

SonicWALL Security Appliances

SonicOS Enhanced 3.2

Administrator's Guide

SONICWALL



Table of Contents

Table of Contents	iii
Preface	xvii
Copyright Notice	xvii
Trademarks	xvii
Limited Warranty	xviii
About this Guide	xix
Organization of this Guide	xix
Guide Conventions	xxii
SonicWALL Technical Support	xxiii
More Information on SonicWALL Products	xxiii

PART 1: Introduction

Chapter 1: Common Criteria Guide	27
Introduction	27
Overview of Common Criteria Operation	27
Use of GUI Interface for Local Management	28
Related Documents	29
SonicOS Enhanced 3.2 Administrator's Guide	29
SonicOS Log Events Reference Guide	32
Chapter 2: Introduction	33
SonicOS Enhanced 3.2	33
What's New in SonicOS Enhanced 3.2	33
What's New in SonicOS Enhanced 3.1	34
SonicWALL Management Interface	37
Navigating the Management Interface	37
Status Bar	38
Applying Changes	38
Navigating Tables	39
Common Icons in the Management Interface	39
Getting Help	39
Logging Out	40

PART 2: System

Chapter 3: Viewing Status Information	43
System > Status	43
Wizards	43
System Messages	44
System Information	44
Latest Alerts	45
Security Services	45
Registering Your SonicWALL Security Appliance	46
Network Interfaces	48

Chapter 4: Managing SonicWALL Licenses	51
System > Licenses	51
Node License Status	51
Security Services Summary	52
Manage Security Services Online	53
Manual Upgrade	54
Manual Upgrade for Closed Environments	54
Chapter 5: Configuring SonicWALL Security Appliance Administration Settings	57
System > Administration	57
Firewall Name	57
Administrator Name & Password	57
Login Security	58
Web Management Settings	58
SSH Management Settings	59
Advanced Management	59
Enabling SNMP Management	59
Enable GMS Management	61
Download URL	63
Chapter 6: Managing Certificates	65
Digital Certificates Overview	65
System > Certificates	66
Certificates and Certificate Requests	66
Certificate Details	67
Importing Certificates	67
Deleting a Certificate	68
Certificate Revocation List (CRL)	69
Generating a Certificate Signing Request	69
Chapter 7: Configuring Time Settings	71
System > Time	71
System Time	72
NTP Settings	72
Chapter 8: Setting Schedules	73
System > Schedules	73
Adding a Schedule	74
Deleting Schedules	75
Chapter 9: Managing SonicWALL Security Appliance Firmware	77
System > Settings	77
Settings	78
Firmware Management	78
SafeMode - Rebooting the SonicWALL Security Appliance	80
FIPS	81
Chapter 10: Using Diagnostic Tools & Restarting the SonicWALL Security Appliance	83
System > Diagnostics	83
Tech Support Report	84
Diagnostic Tools	85
Active Connections Monitor	85
CPU Monitor	86
DNS Name Lookup	87

Find Network Path	87
Packet Trace	88
Ping	89
Process Monitor	90
Real-Time Black List Lookup	90
Reverse Name Resolution	90
Trace Route	91
Web Server Monitor	91
System > Restart.	92

PART 3: Network

Chapter 11: Configuring Interfaces	95
Network > Interfaces	95
Setup Wizard	96
Physical Interfaces	96
Virtual Interfaces (VLAN)	96
SonicOS Enhanced Secure Objects	98
Transparent Mode	98
Interface Settings	99
Interface Traffic Statistics	99
Configuring the F0, F1, X0 - X9, LAN and OPT Interfaces (Static)	100
Configuring Interfaces in Transparent Mode	101
Configuring Wireless Interfaces	103
Configuring the WLAN Interface.	105
Configuring a WAN Interface	106
Configuring the Advanced Settings for the WAN Interface	107
Configuring Modem Settings	109
Connecting the Modem	111
Configuring SonicWALL PortShield™ Interfaces (PRO 1260).	111
Configuring VLAN Sub-Interfaces (PRO 2040, PRO 3060, PRO 4060, PRO 4100, PRO 5060)	113
Deploying VLANs	114
VLAN Integration	116
Chapter 12: Configuring PortShield Interfaces	121
SonicWALL PortShield™ Interfaces	121
Security Services with PortShield.	121
Network > SwitchPorts	122
Overview	122
Using Different Approaches to Configuration	123
Creating a PortShield Interface from the Interfaces Area.	124
Creating a New Zone for the PortShield Interface	128
Refining the PortShield Interface	129
Creating Transparent Mode PortShield Interfaces.	130
Mapping Ports from the Switch Ports Window	134
PortShield Deployment Scenarios.	137
Hospitality.	137
Small Business.	143
Chapter 13: Setting Up WAN Failover and Load Balancing	151
Network > WAN Failover & Load Balancing	151
WAN Failover Caveats	151
Setting Up WAN Failover and Load Balancing.	152
WAN Probe Monitoring.	155

WAN Load Balancing Statistics	157
Chapter 14:Configuring Zones	159
Network > Zones	159
How Zones Work	160
Predefined Zones	161
Security Types	162
Allow Interface Trust	162
Enabling SonicWALL Security Services on Zones	162
The Zone Settings Table	163
Adding a New Zone	164
Deleting a Zone	165
Configuring the WLAN Zone	165
Chapter 15:Configuring DNS Settings	169
Network > DNS	169
Chapter 16:Configuring Address Objects	171
Network > Address Objects	171
Types of Address Objects	171
Address Object Groups	172
Creating and Managing Address Objects	172
Default Address Objects and Groups	173
Adding an Address Object	179
Editing or Deleting an Address Object	180
Creating Group Address Objects	180
Public Server Wizard	181
Chapter 17:Configuring Routes	183
Network > Routing	183
Route Advertisement	184
Route Policies	185
Policy Based Routing	185
Route Policies Table	186
A Route Policy Example	187
Advanced Routing Services	187
Advanced Routing Services (OSPF and RIP)	187
Configuring Advanced Routing Services	194
Chapter 18:Configuring NAT Policies	201
Network > NAT Policies	201
NAT Policies Table	202
NAT Policy Settings Explained	203
NAT Policies Q&A	205
Creating NAT Policies	206
Chapter 19:Managing ARP Traffic	215
Network > ARP	215
Static ARP Entries	216
Secondary Subnets with Static ARP	217
Prohibit Dynamic ARP Entries	218
Navigating and Sorting the ARP Cache Table	219
Navigating and Sorting the ARP Cache Table Entries	219
Flushing the ARP Cache	220

Chapter 20:Setting Up the DHCP Server	221
Network > DHCP Server	221
Enabling the DHCP Server.....	222
DHCP Server Lease Scopes	222
Configuring DHCP Server for Dynamic Ranges.....	223
Configuring Static DHCP Entries	225
Current DHCP Leases	227
Chapter 21:Setting Up Web Proxy Forwarding	229
Network > Web Proxy	229
Configuring Automatic Proxy Forwarding (Web Only)	230
Bypass Proxy Servers Upon Proxy Failure	230
Chapter 22:Using IP Helper	231
Network > IP Helper	231
IP Helper Settings	232
IP Helper Policies	232
Adding an IP Helper Policy.....	232
Editing an IP Helper Policy.....	232
Deleting IP Helper Policies.....	232
Chapter 23:Configuring Dynamic DNS	233
Dynamic DNS Overview	233
Supported DDNS Providers	234
Configuring Dynamic DNS	234
Dynamic DNS Settings Table.....	236

PART 4: Modem

Chapter 24:Viewing Modem Status	241
Modem > Status	241
Modem Status	241
Chapter 25:Configuring Your Modem.....	243
Modem > Settings	243
Modem Settings	243
Dial on Data Categories	243
Management/User Login	244
Profile Settings	244
Modem > Advanced	245
How Does Remotely Triggered Dial-Out Work?.....	245
Configuring Remotely Triggered Dial-Out	246
Chapter 26:Configuring Dialup Profiles	247
Modem > Dialup Profiles	247
Dial-Up Profiles	247
Configuring a Dialup Profile	248
Chat Scripts	251

PART 5: Wireless

Chapter 27:Viewing WLAN Settings, Statistics, and Station Status.....	255
Considerations for Using Wireless Connections	256
Recommendations for Optimal Wireless Performance	256

Adjusting the Antennas	257
Wireless Node Count Enforcement	257
MAC Filter List	257
WiFiSec Enforcement	257
Wireless > Status	258
WLAN Settings	258
WLAN Statistics	259
Station Status	260
Chapter 28:Configuring Wireless Settings	261
Wireless > Settings	261
Wireless Radio Mode	261
Wireless Settings	261
Secure Wireless Bridging	262
Configuring a Secure Wireless Bridge	263
Chapter 29:Configuring WEP/WPA Encryption	269
Wireless > WEP/WPA Encryption	269
WEP Encryption Settings	270
WEP Encryption Keys	270
WPA Encryption Settings	270
Chapter 30:Configuring Advanced Wireless Settings	273
Wireless > Advanced	273
Beaconing & SSID Controls	273
Advanced Radio Settings	274
Chapter 31:Configuring MAC Filter List	275
Wireless > MAC Filter List	275
Chapter 32:Configuring Wireless IDS	277
Wireless > IDS	277
PART 6: SonicPoint	
Chapter 33:Managing SonicPoints	283
SonicPoint > SonicPoints	283
Before Managing SonicPoints	283
SonicPoint Provisioning Profiles	284
Configuring a SonicPoint Profile	285
Updating SonicPoint Settings	288
Updating SonicPoint Firmware	289
Automatic Provisioning (SDP & SSPP)	289
SonicPoint States	290
Chapter 34:Viewing Station Status	291
SonicPoint > Station Status	291
Event and Statistics Reporting	291
Chapter 35:Using and Configuring IDS	295
SonicPoint > IDS	295
Detecting SonicPoint Access Points	295
Wireless Intrusion Detection Services	295

PART 7: Firewall

Chapter 36:Configuring Access Rules	301
Firewall > Access Rules	301
Stateful Packet Inspection Default Access Rules Overview.....	302
Using Bandwidth Management with Access Rules Overview	302
Configuration Task List	303
Displaying Access Rules with View Styles.....	303
Configuring Access Rules for a Zone.....	304
Adding Access Rules	305
Editing an Access Rule	308
Deleting an Access Rule	308
Enabling and Disabling an Access Rule.....	308
Displaying Access Rule Traffic Statistics	308
Connection Limiting Overview	308
Access Rule Configuration Examples	309
Enabling Ping	310
Blocking LAN Access for Specific Services	310
Enabling Bandwidth Management on an Access Rule.....	310
Chapter 37:Configuring Advanced Access Rule Settings	311
Firewall > Advanced	311
Detection Prevention	312
Dynamic Ports	312
Source Routed Packets	312
Connections	312
Access Rule Service Options.....	312
IP and UDP Checksum Enforcement.....	312
UDP	313
Chapter 38:Configuring TCP Settings	315
Firewall > TCP Settings	315
TCP Traffic Statistics	315
TCP Settings	316
Working with SYN/RST/FIN Flood Protection	317
Understanding a TCP Handshake	318
SYN Flood Protection Methods	318
Working with SYN Flood Protection Features	319
Working with SYN Flood Protection Modes	320
Working with SYN Proxy Options.....	320
Working with SYN/RST/FIN Blacklisting	321
SYN, RST, and FIN Flood Statistics.....	322
Chapter 39:Configuring Firewall Services	325
Firewall > Services	325
Default Services Overview	326
Custom Services Configuration Task List	326
Supported Protocols.....	327
Adding Custom Services	327
Adding a Custom Services Group	329
Chapter 40:Configuring Multicast Settings	331
Firewall > Multicast	331
Multicast Snooping	332

Multicast Policies	332
IGMP State Table	333
Enabling Multicast on LAN-dedicated Interfaces	333
Enabling Multicast Through a VPN	334
Chapter 41:Monitoring Active Connections	337
Firewall > Connections Monitor	337
Viewing Connections	338
Filtering Connections Viewed	339
Chapter 42:Managing Quality of Service	341
Working with QoS	341
Classification	341
Marking	342
Conditioning	343
802.1p and DSCP QoS	344
Enabling 802.1p	344
DSCP Marking	347
Bandwidth Management	354
Outbound Bandwidth Management	356
Algorithm for Outbound Bandwidth Management	357
Example of Outbound BWM	359
Inbound Bandwidth Management	360
Algorithm for Inbound Bandwidth Management	361
Credit Based Processing	361
Example of Inbound Bandwidth Management	362
BWM with WAN load balancing	362
Glossary	363
PART 8: VoIP	
Chapter 43:Configuring VoIP Support	369
VoIP Overview	369
What is VoIP?	369
VoIP Security	369
VoIP Protocols	370
SonicWALL's VoIP Capabilities	371
VoIP Security	372
VoIP Network	372
VoIP Network Interoperability	373
Supported VoIP Protocols	374
How SonicOS Handles VoIP Calls	376
Configuring SonicWALL VoIP Features	378
Supported Interfaces	378
Configuration Tasks	378
General VoIP Configuration	379
Configuring BWM and QoS	382
Configuring VoIP Logging	388
VoIP Deployment Scenarios	389
Generic Deployment Scenario	389
Deployment Scenario 1: Point-to-Point VoIP Service	390
Deployment Scenario 2: Public VoIP Service	391
Deployment Scenario 3: Trusted VoIP Service	392

PART 9: VPN

Chapter 44:Configuring VPN Policies	395
VPN > Settings	395
VPN Overview	395
VPN Types	396
VPN Security	397
Configuring VPNs in SonicOS Enhanced	399
Planning Your VPN	400
VPN Policy Wizard	406
VPN Global Settings	406
VPN Policies	406
Currently Active VPN Tunnels	407
Configuring GroupVPN Policies	408
Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone	409
Configuring GroupVPN with IKE using 3rd Party Certificates	412
Exporting a VPN Client Policy	415
Site-to-Site VPN Configurations	416
Creating Site-to-Site VPN Policies	417
Configuring a VPN Policy with IKE using Preshared Secret	417
Configuring a VPN Policy using Manual Key	422
Configuring a VPN Policy with IKE using a Third Party Certificate	426
VPN Auto-Added Access Rule Control	430
Chapter 45:Configuring Advanced VPN Settings	431
VPN > Advanced	431
Advanced VPN Settings	431
Chapter 46:Configuring DHCP Over VPN	435
VPN > DHCP over VPN	435
DHCP Relay Mode	435
Configuring the Central Gateway for DHCP Over VPN	436
Configuring DHCP over VPN Remote Gateway	437
Current DHCP over VPN Leases	439
Chapter 47:Configuring L2TP Server	441
VPN > L2TP Server	441
Configuring the L2TP Server	442

PART 10: Users

Chapter 48:Managing User Status and Authentication Settings	447
Users > Status	447
User > Settings	448
User Login Settings	448
Configuring RADIUS Authentication	449
Configuring LDAP / Active Directory / eDirectory Authentication	452
Configuring LDAP integration in SonicOS Enhanced	453
Configuring the SonicWALL Appliance for LDAP	454
RADIUS with LDAP for user groups	462
User Session Settings	462
Other Global User Settings	463
Acceptable Use Policy	464

Chapter 49:Managing Local Users and Local Groups	465
User > Local Users	465
Viewing Local Users	466
Adding Local Users	466
Editing Local Users	467
Users > Local Groups	468
Creating a Local Group	469
Chapter 50:Managing Guest Services and Guest Accounts	471
Users > Guest Services	471
Global Guest Settings	472
Guest Profiles	472
Users > Guest Accounts	474
Viewing Guest Account Statistics	474
Adding Guest Accounts	475
Enabling Guest Accounts	477
Enabling Auto-prune for Guest Accounts	477
Printing Account Details.	477
Users > Guest Status	478
Logging Accounts off the Appliance	478

PART 11: Hardware Failover

Chapter 51:Setting Up Hardware Failover	483
Hardware Failover > Settings	483
How Hardware Failover Works	483
Before Configuring Hardware Failover	484
Configuring Hardware Failover	487
Synchronizing Firmware	489
Monitoring Links	489
Hardware Failover Status	490

PART 12: Security Services

Chapter 52:Managing SonicWALL Security Services	493
SonicWALL Security Services	493
Security Services Summary	494
Managing Security Services Online.	495
Security Services Settings.	496
Security Services Information	496
Update Signature Manually	497
Activating Security Services	498
Chapter 53:Configuring SonicWALL Content Filtering Service	499
Security Services > Content Filter	499
SonicWALL Content Filtering Service	499
Content Filter Status	500
Content Filter Type	501
Restrict Web Features.	502
Trusted Domains	502
CFS Exclusion List	503
Message to Display when Blocking.	503

Configuring SonicWALL Filter Properties	503
Custom List	503
Consent	505
Chapter 54:Activating SonicWALL Network Anti-Virus	507
Security Services > Anti-Virus	507
Activating SonicWALL Network Anti-Virus	508
Activating a SonicWALL Network Anti-Virus FREE TRIAL	509
Configuring Network Anti-Virus Service	510
Security Services > E-mail Filter	511
Chapter 55:Managing SonicWALL Gateway Anti-Virus Service	513
SonicWALL's Unified Threat Management Solution	513
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Features	514
SonicWALL Gateway Anti-Virus Overview	515
SonicWALL GAV Multi-Layered Approach	516
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Activation	520
Creating a mySonicWALL.com Account	521
Registering Your SonicWALL Security Appliance	522
Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License	523
Activating FREE TRIALS	524
Chapter 56:Activating Intrusion Prevention Service	535
SonicWALL's Unified Threat Management Solution	535
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Features	536
SonicWALL Intrusion Prevention Service Overview	537
SonicWALL Deep Packet Inspection	537
How SonicWALL's Deep Packet Inspection Works	538
SonicWALL IPS Terminology	538
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Activation	539
Creating a mySonicWALL.com Account	540
Registering Your SonicWALL Security Appliance	540
Activating FREE TRIALS	541
Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License	542
Setting Up SonicWALL Intrusion Prevention Service Protection	543
Enabling SonicWALL IPS	543
Specifying Global Attack Level Protection	543
Applying SonicWALL IPS Protection on Zones	544
Chapter 57:Activating Anti-Spyware Service	545
SonicWALL's Unified Threat Management Solution	545
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Features	546
SonicWALL Anti-Spyware Service Overview	547
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Activation	548
Creating a mySonicWALL.com Account	548
Registering Your SonicWALL Security Appliance	549
Activating FREE TRIALS	550
Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License	550
Setting Up SonicWALL Anti-Spyware Service Protection	551
Applying SonicWALL Anti-Spyware Protection on Zones	552

Chapter 58:Configuring SonicWALL Real-Time Blacklist	553
SMTP Real-Time Black List Filtering	553
Security Services > RBL Filter	554
Adding RBL Services.	554
User-Defined SMTP Server Lists	555
Chapter 59:Configuring SonicWALL Global Security Client	557
Security Services > Global Security Client	557
Global Security Client Features.	558
How SonicWALL Global Security Client Works.	559
Global Security Client Licensing	560
Activating Global Security Client Licenses on Your SonicWALL.	560
Configuring Security Policies for Global Security Clients	561
PART 13: Log	
Chapter 60:Managing Log Events	565
Log > View	565
Log View Table	566
Refresh	566
Clear Log	566
Export Log	567
E-mail Log	567
Filtering Log Records Viewed	567
Log Event Messages	568
Chapter 61:Configuring Log Categories	569
Log > Categories	569
Log Priority	569
Log Categories	570
Chapter 62:Configuring Syslog Settings	575
Log > Syslog	575
Syslog Settings	576
Syslog Servers	576
Chapter 63:Configuring Log Automation	577
Log > Automation	577
E-mail Log Automation	578
Mail Server Settings	578
Chapter 64:Configuring Name Resolution	579
Log > Name Resolution	579
Selecting Name Resolution Settings	579
Specifying the DNS Server	580
Chapter 65:Generating Log Reports	581
Log > Reports	581
Data Collection	582
View Data	582
Chapter 66:Activating SonicWALL ViewPoint	585
Log > ViewPoint	585
Activating ViewPoint	586

Enabling ViewPoint Settings 587

PART 14: Wizards

Chapter 67:Configuring Internet Connectivity Using the Setup Wizard..... 591
 Internet Connectivity Using the Setup Wizard..... 591
 Using the Setup Wizard 591
 Wireless Deployment Scenarios 592
 Configuring a Static IP Address with NAT Enabled 593
 Configuring DHCP Networking Mode..... 601
 Configuring NAT Enabled with PPPoE..... 609
 Configuring PPTP Network Mode 617

Chapter 68:Configuring a Public Server with the Wizard 627
 Create a Server with the Public Server Wizard 627

Chapter 69:Configuring VPN Policies with the VPN Policy Wizard..... 631
 Configuring GroupVPN using the VPN Policy Wizard 631
 Using the VPN Policy Wizard..... 631
 Connecting the Global VPN Clients 634
 Configuring a Site-to-Site VPN using the VPN Wizard 635
 Using the VPN Wizard to Configure Preshared Secret 635

Chapter 70:Configuring Your Wireless Network with the Wireless Wizard . 641
 Using the Wireless Wizard 641
 Configuring Additional Wireless Features 645

Chapter 71:Configuring PortShield Interfaces Using the Setup Wizard 647
 Internet Connectivity Using the Setup Wizard..... 647
 Using the PortShield Wizard 647
 Configuring a Static IP Address with NAT Enabled 648

Index..... 655

Preface

Copyright Notice

© 2006 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.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

eDirectory and NetWare are registered trademarks of Novell, Inc.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

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.

About this Guide

Welcome to the *SonicWALL SonicOS Enhanced 3.1 Administrator's Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS Enhanced 3.1 for the SonicWALL TZ 170 SP Wireless, PRO 1260, PRO 4060, and PRO 5060 and available as an upgrade for the SonicWALL TZ 170 SP, TZ 170 Wireless, PRO 1260, PRO 2040, and PRO 3060 security appliances.



Note: Always check <<http://www.sonicwall.com/services/documentation.html>> for the latest version of this manual as well as other SonicWALL products and services documentation.

Organization of this Guide

The SonicOS Enhanced 3.1 Administrator's Guide organization is structured into the following parts that follow the SonicWALL Web Management Interface structure. Within these parts, individual chapters correspond to SonicWALL security appliance management interface layout.

Part 1 Introduction

This part provides an overview of new SonicWALL SonicOS Enhanced features, guide conventions, support information, and an overview of the SonicWALL security appliance management interface.

Part 2 System

This part covers a variety of SonicWALL security appliance controls for managing system status information, registering the SonicWALL security appliance, activating and managing SonicWALL Security Services licenses, configuring SonicWALL security appliance local and remote management options, managing firmware versions and preferences, and using included diagnostics tools for troubleshooting.

Part 3 Network

This part covers configuring the SonicWALL security appliance for your network environment. The **Network** section of the SonicWALL Management Interface includes:

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

Part 4 Modem (TZ 170 SP and TZ 170 SP Wireless)

The part covers the configuration of the SonicWALL security appliance's built in modem for use as the primary or when the WAN zone Ethernet connection is unavailable.

Part 5 Wireless (TZ 170 Wireless and TZ 170 SP Wireless)

The part covers the configuration of the built-in 802.11b/g antennas for the SonicWALL TZ 170 Wireless and SonicWALL TZ 170 SP Wireless security appliances.

Part 6 SonicPoint

The part covers the configuration of the SonicWALL security appliance for provisioning and managing SonicWALL SonicPoints as part of a SonicWALL Distributed Wireless Solution.

Part 7 Firewall

This part covers tools for managing how the SonicWALL security appliance handles traffic through the the firewall.

Part 8 VoIP

This part provides instructions for configuring the SonicWALL security appliance to support H.323 or SIP Voice over IP (VoIP) connections.

Part 9 VPN

This part covers how to create VPN policies on the SonicWALL security appliance to support SonicWALL Global VPN Clients as well as creating site-to-site VPN policies for connecting offices running SonicWALL security appliances.

Part 10 Users

This part covers how to configure the SonicWALL security appliance for user level authentication as well as manage guest services for managed SonicPoints.

Part 11 Hardware Failover

This part explains how to configure the SonicWALL security appliance for failover to another SonicWALL security appliance in the event of hardware failure.

Part 12 Security Services

This part includes an overview of available SonicWALL Security Services as well as instructions for activating the service, including FREE trials. These subscription-based services include SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service, SonicWALL Content Filtering Service, SonicWALL Network Anti-Virus, and well as other services.

Part 13 Log

This part covers managing the SonicWALL security appliance's enhanced logging, alerting, and reporting features. The SonicWALL security appliance's logging features provide a comprehensive set of log categories for monitoring security and network activities.

Part 14 Wizards

This part walks you through using the SonicWALL Configuration Wizards for configuring the SonicWALL security appliance for LAN to WAN (Internet) connectivity, settings up public servers for Internet connectivity behind the firewall, and setting GroupVPN and site-to-site VPN policies for establishing VPN connections for remote SonicWALL Global VPN Client users or remote offices with a SonicWALL security appliance for LAN to LAN connections.

The SonicWALL Configuration Wizards in SonicOS Enhanced 3.1 include:

- 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 **Wireless Wizard** takes you step by step through the configuration of your WLAN. The **Wireless Wizard** is only available for SonicWALL TZ 170 Wireless and TZ 170 SP Wireless security appliances.
- The **Public Server Wizard** takes you step by step through adding a server to your network, such as a mail server or a web server. The wizard automates much of the configuration you need to establish security and access for the server.
- The **VPN Policy Wizard** steps you through the configuration of Group VPNs and site-to-site VPNs.

Guide Conventions

The following Conventions used in this guide are as follows:

Convention	Use
Bold	Highlights items you can select on the SonicWALL security appliance 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.*



Cross Reference: *Provides a pointer to related information in the Administrator's Guide or other resources.*

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <http://www.sonicwall.com/support/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/support/contact.html> for the latest technical support telephone numbers.

More Information on SonicWALL Products

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

Current Documentation

Check the SonicWALL documentation Web site for that latest versions of this manual and all other SonicWALL product documentation.

<http://www.sonicwall.com/support/documentation.html>

PART

1

Introduction

Common Criteria Guide

Introduction

The purpose of this chapter is to define the Common Criteria-compliant operation of SonicWALL Internet Security Appliances.

Common Criteria is an information technology (IT) validation scheme adopted by the National Information Assurance Partnership (NIAP). NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NIAP has established the Common Criteria Evaluation Validated Scheme (CCEVS) to validate IT products. Common Criteria is also referred to as ISO 15408.

SonicWALL Internet Security Appliances have been validated to Common Criteria Evaluation Assurance Level (EAL) 2 using the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999.

Overview of Common Criteria Operation

The Common Criteria evaluated configuration of SonicWALL Internet Security Appliances uses only the firewall services of the device. The VPN services of the device are not included in the Common Criteria evaluated configuration. The Common Criteria evaluated configuration includes all features except those that are explicitly excluded.

The following features are not included in the Common Criteria evaluated configuration:

- VPN
- IPsec or L2TP
- LDAP or RADIUS user authentication
- Security Services
 - ◆ Content Filtering Service
 - ◆ Network Anti-Virus
 - ◆ E-mail Filter
 - ◆ Anti-Spyware
 - ◆ RBL Filter
 - ◆ Global Security Client
 - ◆ Intrusion Prevention System

- ◆ Gateway Anti-Virus
- GMS Remote Management
- Syslog Logging
- SonicPoint
- Hardware Failover

Before installing the SonicWALL Internet Security Appliance, the device should be examined for evidence of tampering. Each device includes a tamper-evident seal to prevent access to the inside of the unit. Verify that the tamper evident seal is intact. If there is a sign of tampering, contact SonicWALL Support Services by phone at 888.777.1476 or 408.752.7819.

The GUI management interface is used to administer the device. The use of the GUI management interface is discussed in the *“Use of GUI Interface for Local Management”* section below.

The Common Criteria evaluated configuration only supports SonicOS v3.2 Enhanced. You can verify that the device is running SonicOS v3.2 Enhanced from the **System -> Status** page of the management GUI under the **System Information** table, **Firmware Version** entry.

If the device ships with SonicOS v3.2 Standard, it must first be upgraded to SonicOS v3.2 Enhanced. The Common Criteria evaluated configuration does not support the evaluation version of SonicOS v3.2 Enhanced. If the device is running an evaluation version of SonicOS v3.2 Enhanced (which can be identified by the presence of **Evaluation Edition** at the top right corner of the management GUI screen, it must first be upgraded to SonicOS v3.2 Enhanced.

Use of GUI Interface for Local Management

This section describes the use of the SonicWALL Graphical User Interface (GUI) interface for local management. Using the red cross-over cable supplied with SonicWALL Internet Security Appliances and a management PC, the SonicWALL GUI can be used for local configuration. This provides a secure way of administering the device without the possibility of traffic between the management PC and device being captured or traced. Following the instructions below will insure that only the management PC, directly connected to the device, can be used for management.

Follow the instructions in the SonicOS Getting Started Guide section 2, Connecting the Network Cables, to connect a management PC to the device.

Follow the instructions in the SonicOS Getting Started Guide section 2, Configuring Your Management Station and Accessing The Management Interface to access the management interface of the device

Select an interface to be used as the local management interface. For example, on a PRO series appliance, select X2 or X3.

Use the Add button on the **Network -> Zones** page to add a “Local Management” with a Security Type of Trusted. On the **Network -> Interfaces** page, configure the local management interface. Set the Zone to “Local Management”. Set the IP Address to 192.168.1.1. Set the Subnet Mask to 255.255.255.0. Enable HTTP Management. Log out from the GUI management interface using the Logout button.

Connect the red cross-over cable to the local interface. Configure the management PC's IP address to be 192.168.1.2 with a netmask of 255.255.255.0. Use the management PC's browser to access the device's management interface at <http://192.168.1.2>.

Use the Configure icon on the **Network -> Interfaces** page to configure the LAN interface. Disable HTTP and HTTPS management.

Do not enable HTTP or HTTPS management on any interface other than the local management interface. HTTP and HTTPS management is disabled on all other interfaces by default.

The management PC can now be used to locally administer the device in a secure manner.

Related Documents

Several other SonicWALL documents provide information relating to the Common Criteria evaluated configuration of SonicWALL Internet Security Appliances. Those documents are described here.

SonicOS Enhanced 3.2 Administrator's Guide

The SonicOS Enhanced 3.2 Administrator's Guide provides procedures for configuring network, firewall, administrator management, and logging on SonicWALL Internet Security Appliances.

Table 1: SonicOS Enhanced 3.2 Administrator's Guide Contents

Chapter Number	Chapter Title	Description
Part 1 Introduction		
Chapter 1	Common Criteria Guide	
Chapter 2	Introduction	Describes new features and provides instructions on using the management interface.
Part 2 System		
Chapter 3	Viewing Status Information	Describes of SonicWALL security appliance status information, configuration wizards, and how to register the SonicWALL security appliance.
Chapter 4	Managing SonicWALL Licenses	Describes managing SonicWALL Security Service activation licenses and appliance node upgrade licenses.
Chapter 5	Configuring SonicWALL Security Appliance Administration Settings	Describes configuration of SonicWALL security appliance for local and remote administration.
Chapter 7	Configuring Time Settings	Describes the configuration of system time settings.
Chapter 8	Setting Schedules	Describes the configuration of schedule objects for enforcing schedule times for a variety of security policies.
Chapter 9	Managing SonicWALL Security Appliance Firmware	Describes the updating of SonicWALL security appliance firmware and the backing up of configuration preferences.
Chapter 10	Using Diagnostic Tools and Restarting the SonicWALL Security Appliance	Describes the use diagnostic tools for network troubleshooting, how to restart the SonicWALL security appliance, and how to create a tech support report.
Part 3 Network		
Chapter 11	Configuring Interfaces	Describes the configuration of logical interfaces for network connectivity.
Chapter 12	Setting Up WAN Failover and Load Balancing	Describes the configuration of a secondary WAN interface for backup and load balancing.
Chapter 13	Configuring Zones	Describes the configuration of security zones.
Chapter 14	Configuring DNS Settings	Describes the specification of DNS servers for name resolution

Table 1: SonicOS Enhanced 3.2 Administrator's Guide Contents

Chapter Number	Chapter Title	Description
Chapter 15	Configuring Address Objects	Describes the configuration of host, network, and address range objects.
Chapter 16	Configuring Routes	Describes the configuration of routing policies.
Chapter 17	Configuring NAT Policies	Describes the configuration of NAT policies.
Chapter 18	Managing ARP Traffic	Describes the management of ARP traffic and the configuration of static mappings
Chapter 19	Setting Up the DHCP Server	Describes the configuration of the SonicWALL security appliance's DHCP server.
Chapter 20	Using IP Helper	Describes the configuration of forwarding DHCP requests from SonicWALL security appliance interfaces to a centralized DHCP server.
Chapter 21	Setting UP Web Proxy Forwarding	Describes the configuration of forwarding all Web proxy requests to a network proxy server.
Chapter 22	Configuring Dynamic DNS	Describes the configuration of the SonicWALL security appliance to dynamically register with a DDNS provider.
Part 4 Modem		
Chapter 23	Viewing Modem Status	Describes modem status information.
Chapter 24	Configuring Modem Settings	Describes the configuration of modem settings.
Chapter 25	Configuring Dialup Profiles	Describes the configuration of dialup profiles for WAN connectivity.
Part 5 Wireless		
Chapter 26	Viewing WLAN Settings, Statistics, and Station Status	Describes WLAN status information.
Chapter 27	Configuring Wireless Settings	Describes the configuration of the SonicWALL security appliance radio mode settings.
Chapter 28	Configuring WEP/WPA Encryption	Describes the configuration of WEP and WPA encryption.
Chapter 29	Configuring Advanced Wireless Settings	Describes the configuration of beaconing, SSID, and advanced radio settings.
Chapter 30	Configuring a MAC Filter List	Describes the configuration of client MAC addresses for authentication.
Chapter 31	Configuring Wireless IDS	Describes the configuration of wireless intrusion detection services.
Part 7 Firewall		
Chapter 35	Configuring Access Rules	Describes the configuration of firewall access rules.
Chapter 36	Configuring Advanced Rules Settings	Describes the configuration of advanced access rule settings.
Chapter 37	Configuring TCP Settings	Describes the configuration of TCP traffic management settings.
Chapter 38	Configuring Firewall Services	Describes the configuration of custom services access rules.
Chapter 39	Configuring Multicast Settings	Describes the configuration of multicast traffic on the SonicWALL security appliance

Table 1: SonicOS Enhanced 3.2 Administrator's Guide Contents

Chapter Number	Chapter Title	Description
Chapter 40	Monitoring Active Connections	Describes the configuration of status information on active connections.
Part 8 VoIP		
Chapter 41	Configuring VoIP Support	Describes the configuration of VoIP support on the SonicWALL security appliance.
Part 10 Users		
Chapter 46	Managing User Status and Authentication	Describes the configuration of user authentication using the SonicWALL security appliance's local database, RADIUS, or LDAP.
Chapter 47	Managing Local Users and Local Groups	Describes the configuration of the SonicWALL security appliance's local database for user authentication and the creation of user groups.
Chapter 48	Managing Guest Services and Guest Accounts	Describes the configuration of temporary guest accounts and services for guest network users.
Part 13 Log		
Chapter 57	Managing Log Events	Describes the management of log events.
Chapter 58	Configuring Log Categories	Describes the configuration of logging functions.
Chapter 59	Configuring Syslog Settings	Describes the configuration of the SonicWALL security appliance to capture and send logs to external Syslog servers.
Chapter 60	Configuring Log Automation	Describes the configuration of the SonicWALL security appliance to send log files and alerts using e-mail.
Chapter 61	Configuring Name Resolution	Describes the configuration of name servers used to resolve IP addresses and server names in log reports.
Chapter 62	Generating Log Reports	Describes the generation of simplified reports based on a rolling analysis of the event log.
Chapter 63	Activating SonicWALL ViewPoint	Describes the activation of SonicWALL ViewPoint Web-based, graphical reporting application.
Part 14 Wizards		
Chapter 64	Configuring Internet Connectivity Using the Setup Wizard	Describes the configuration of SonicWALL security appliance for Internet connectivity using the Setup Wizard.
Chapter 65	Configuring a Public Server Using the Public Server Wizard	Describes the configuration of Internet access to public servers behind the SonicWALL security appliance using the Public Server Wizard.
Chapter 66	Configuring VPN Policies Using the VPN Policy Wizard	Describes the configuration of VPN policies for SonicWALL security appliance using the VPN Policy Wizard.
Chapter 67	Configuring PortShield Interfaces	Configuring PortShield Interfaces Using the Setup Wizard

SonicOS Log Events Reference Guide

During the operation of a SonicWALL security appliance, SonicOS software sends log event messages to the console. Event logging automatically begins when the SonicWALL security appliance is powered on and configured. SonicOS v3.2 Enhanced supports a traffic log containing entries with multiple fields.

Log event messages provide operational informational and debugging information to help you diagnose problems with communication lines, internal hardware, or your firmware configuration.



Note: Not all log event messages indicate operational issues with your SonicWALL security appliance.

The **Log > View** console display provides log event messages including the following fields for alert notification:

- **Time**—Displays the hour and minute the event occurred.
- **Priority**—Displays the level urgency for the event.
- **Category**—Displays the event type.
- **Message**—Displays a description of the event.
- **Source**—Displays the source IP address of incoming IP packet.
- **Destination**—Displays the destination IP address of incoming IP packet.
- **Note**—Displays displays additional information specific to a particular event occurrence.
- **Rule**—Displays the source and destination zones for the access rule. This field provides a link to the access rule defined in the **Firewall' > Access Rules** page.

The display fields for a log event message provides you with data to verify your configurations, trouble-shoot your security appliance, and track IP traffic.

Introduction

SonicOS Enhanced 3.2

SonicOS Enhanced 3.2 is the most powerful SonicOS operating system designed for the SonicWALL TZ 170 SP Wireless, PRO 1260, PRO 4060, the PRO 4100, and the PRO 5060, and available as an upgrade for the SonicWALL TZ 170 SP, TZ 170 Wireless, PRO 2040, and PRO 3060 security appliances.

What's New in SonicOS Enhanced 3.2

SonicOS Enhanced 3.2 includes these new features:

- **DoS Flood Enhancements** - SonicOS now detects and prevents Denial of Service Flood attacks that use RST and FIN packets in addition to SYN packets.
- **GAV 2.0 Enhancements** - SonicWALL GAV now supports HTTP clientless notification, scanning of uuencoded emails, configuring policy settings for individual protocols.
- **IKE v2 Support (Preshared Keys)** - IKE version 2 is a new protocol for negotiating and establishing SAs. IKE v2 features improved security, a simplified architecture, and enhanced support for remote users. In addition, IKE v2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKE V2 greatly reduces the number of message exchanges needed to establish an SA over IKE v1 Main Mode, while being more secure and flexible than IKE v1 Aggressive Mode.
- **LDAP Enhancements** - Lightweight Directory Access Protocol (LDAP) defines a directory services structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. In addition to RADIUS and the local user database, SonicOS Enhanced supports LDAP, Microsoft Active Directory (AD), and Novell eDirectory directory services for user authentication.
- **Manual Signature Import Integration** - SonicWALL security appliances that are deployed in network environments with limited Internet connectivity or in closed, secure environments can now manually update the signature file for Security Services (GAV, Anti-Spyware, and IPS).
- **One-to-Many NAT Load Balancing** - SonicOS Enhanced will now persistently load balance the translated destination within one-to-many NAT policies using the original source IP address as the key to persistence. For example, SonicWALL security appliances can load balance multiple SonicWALL SSL-VPN appliances, while still maintaining session persistence by always balancing clients to the correct destination SSL-VPN. Figure 1 shows a sample topology and configuration.
- **RIPv2 and OSPF Support on SonicWALL PRO 2040 and PRO 3060** - The SonicWALL PRO 2040 and PRO 3060 now support the RIPv2 and OSPF advanced routing protocols.

- **Remotely Triggered Dial-out** - Network administrators can now remotely instruct SonicWALL security appliances to initiate a modem dial-out session, which enhances remote administration of SonicWALL security appliances with dial-up connectivity.
- **SSH Support** - SonicOS Enhanced now supports Secure Shell (SSH) remote management that can be configured on a per interface basis for secure remote access to the command line interface.
- **SSL-VPN WLAN Enforcement** - Allows administrators to configure automatic redirection of WLAN users to a SonicWALL SSL-VPN appliance for securing wireless traffic with SSL-VPN proxies and NetExtender.
- **VoIP SIP Back to Back User Agent Support** - SonicWALL Security Appliances now support SIP VoIP calls where the SonicWALL security Appliance can see both legs of the call. Note that B2BUA mode does not support deployments where the proxy server is on the DMZ.
- **VLAN Support on SonicWALL PRO 2040 and PRO 3060** - VLANs are now available on the SonicWALL PRO 2040 and PRO 3060, which provide improved security through network segmentation.
- **VPN CLI Support** - SonicOS now supports VPN configuration using the CLI.
- **VPN Logging Enhancements** - VPN logging has been expanded to include detailed and descriptive log event messages for all types and phases of VPN negotiations and exchanges.
- **Web Server Improvements** - The SonicOS graphical user interface (GUI) is now 50% faster.

What's New in SonicOS Enhanced 3.1

SonicOS Enhanced 3.1 includes these new operating system features:

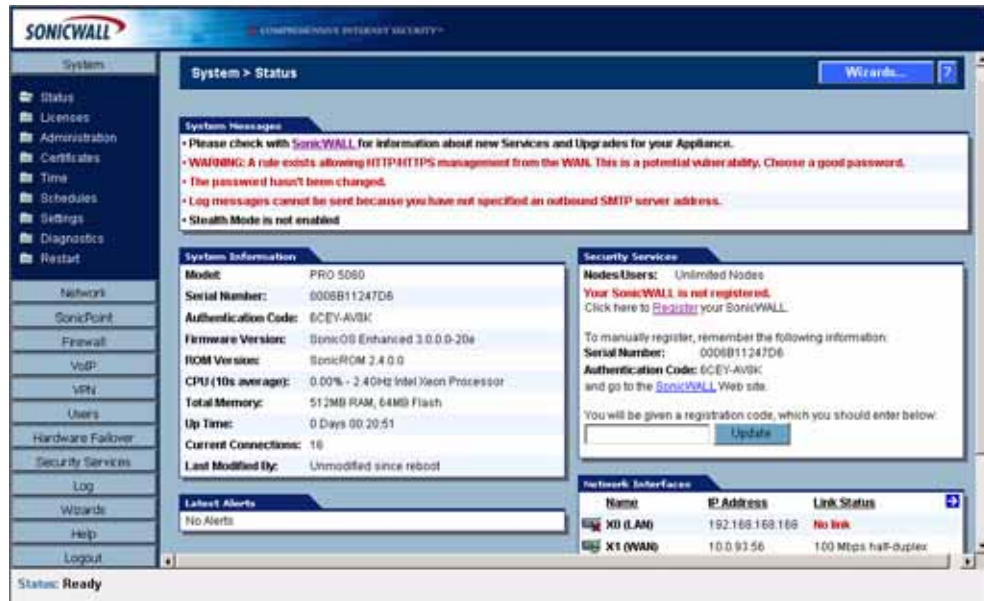
- **Real-Time Gateway Anti Virus** - Delivers per packet virus scanning using Deep Packet Inspection v2.0 engine. The Real-Time Gateway Anti-Virus feature supports scanning the following message delivery protocols:
 - ♦ HyperText Transport Protocol (HTTP)
 - ♦ Simple Mail Transfer Protocol (SMTP)
 - ♦ Internet Message Access Protocol (IMAP)
 - ♦ Post Office Protocol 3 (POP3)
 - ♦ File Transfer Protocol (FTP)
 - ♦ Transmission Control Protocol (TCP) packet streams
- **Support for Intrusion Prevention Services v2.0** - Provides an updated Data Packet Inspection (DPI) engine that powers both Intrusion Prevention Service and Gateway Anti-Virus. The IPS version 2.0 engine includes the following feature enhancements:
 - ♦ **IP Fragmentation** - Provides the ability to either disallow IP fragments or to reassemble IP fragments for full application layer inspection.
 - ♦ **Checksum Validation** - Provides the ability to detect and prevent invalid IP, ICMP, TCP, and UDP checksums.
 - ♦ **Global IP Exclusion List** - Provides the ability to configure a range of IP addresses to exclude specified network traffic from IPS evaluation.
 - ♦ **Log Redundancy** - Provides the ability to configure per-category and per-signature log redundancy filter settings.
 - ♦ **Dynamic Categorization** - Groups and displays signatures automatically in expandable category views. Category maintenance is performed through automated signature updates.
 - ♦ **Category and Signature: User and Group Controls** - Allows signatures and category policies to be applied at the user or group level, overriding global settings.
 - ♦ **Category and Signature: Apply Policies for IP Address Ranges** - Allows network policies to be applied to a single IP address or an IP address range.

- ♦ **Category and Signature Scheduling** - Control the application of signatures and category policies using Schedule Objects.
- **AD and LDAP Support** - Provides the ability to natively query one or more Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) directory servers for incoming User-Level Authentication (ULA), Wireless Guest Service (WGS), VPN tunnel, and Global VPN Client (GVC) connections.
- **802.1q VLAN Support** - Provides the ability to recognize and segregate traffic based on Virtual LAN (VLAN) IDs. Provides support to add subinterfaces on the VLAN trunk interface so that the SonicWALL security appliance is able to route network traffic between VLANs. The 802.1q VLAN support feature is currently only supported on the SonicWALL PRO 4060 and SonicWALL PRO 5060 security appliances.
- **Advanced Routing Services** - Provides the ability to perform Routing Information Protocol version 1 (RIPv1), RIPv2, and Open Shortest Path First (OSPF) routing on all interfaces and subinterfaces on a SonicWALL security appliance, while retaining the ability to broadcast active VPN tunnels during routing updates. The Advanced Routing support feature is currently only supported on the SonicWALL PRO 4060 and SonicWALL PRO 5060 security appliances.
- **Dynamic DNS** - Enables the SonicWALL device to dynamically register its WAN IP address with a DDNS service provider.
- **Real-Time Monitoring** - Includes the following monitoring tools:
 - ♦ **CPU Monitor** allows you to generate CPU utilization reports in a customizable histogram format.
 - ♦ **Process Monitor** allows you to generate reports on current running processes.
 - ♦ **Active Connections Monitor** allows you to generate reports on current active network connections.
- **DHCP Server Enhancements** - Includes expanded hash tables for resource management, accelerated duplicate-address detection, and improved Dynamic Host Configuration Protocol (DHCP) Server internal-database maintenance management.
- **Static ARP Support** - Enables you to create static Address Resolution Protocol (ARP) entries, create MAC address to IP address bindings, and to publish static ARP entries for use in a secondary network subnet.
- **Virtual Adapter Static IP Support** - Provides support for static IP addressing of Global VPN Client (GVC) virtual adapters.
- **Expanded Logging** - Includes additional logging capabilities to provide expanded flexibility. You can export the log into plain text or CSV values. Logging categories are dramatically expanded, the logs conform to Syslog severity levels so you can set the SonicWALL security appliance to only log alerts and messages of specified levels. And you can independently specify which categories are logged to the internal log. When directing logs to external Syslog servers, you can rate-limit the messages based on events-per-second or maximum bytes-per-second, so that external Syslog servers do not become overwhelmed.
- **SMTP RBL** - Support for using DNS to query Real-Time Black List (RBL) services that track well-known spam and open-relay SMTP servers, and to deny SMTP connections from servers that appear on the lists.
- **SYN Cookie/Other TCP Enhancements** - SYN Flood denial of service attack protection based on reliable and resource efficient SYN cookies. Scrutinizing evaluation of all TCP parameters to ensure validity of packets, and to provide an additional layer of protection against malicious network activity.
- **Connection Limiting** - Provides the ability to prevent resource exhaustion by defining a percentage of the total number of allowable connections through the firewall which may be allocated to a particular type of connection, as defined by Access Rules.
- **Lightweight Hotspot Messaging** - Broad support for external authentication backend systems for wireless hotspot services. (TZ 170 Wireless only).

- **Wireless Radio Operating Schedule** - The ability to create a schedule to control the operation of the wireless radio in the TZ 170 class of wireless products and the SonicPoint.
- **Wireless IDS Scheduled Scan** - The ability to create a schedule to control the Intrusion Detection Services scanning function of the wireless radios.
- **WiFiSec Exception List** - Flexible control of services that can bypass WiFiSec enforcement. Can be configured, for example, to allow NT Domain logons to occur prior to GVC tunnel establishment. (TZ 170 Wireless only)
- **Wireless Guest Services Real-Time Session Timer** - Granularly tracks WGS session timers based on login and logout events, allowing the session time to accurately reflect real-time use.
- **Group Address Object for Policy Based Routing** - Support for Group Address Objects as source or destination selectors in Policy Based Routing.
- **Separate CCK and OFDM 2.4GHz Tuning** - Provides separate controls for 802.11b and 802.11g power levels on the 2.4GHz radio on SonicPoints.
- **VPN Auto-Added Access Rule Control** - It is now possible to control the creation of auto-added Access Rules when creating VPN Policies.
- **User Interface Changes** - The SonicWALL management interface includes the following changes:
 - **System > Status** page now shows **Last Modified** by information.
 - **Firewall > Schedules** has been relocated to **System > Schedules**.
 - **VPN > Local Certificates** and **VPN > CA Certificates** have been merged and moved to the **System > Certificates** page.
 - **TCP Checksum Validation** and **TCP Connection Timeout** settings have been moved from the **Firewall > Advanced** page to the **Firewall > TCP Settings** page.
- **SonicSetup** - A stand-alone Win32 executable for discovery of SonicWALL security appliances, automatic synchronization of client and SonicWALL security appliance IP addressing, hardware diagnostics, validation of ROM, firmware and preferences, ROM and firmware recovery, and restoration of factory defaults.

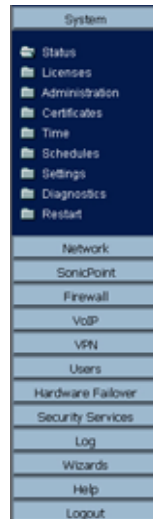
SonicWALL Management Interface

The SonicWALL security appliance's Web-based management interface provides a easy-to-use graphical interface for configuring your SonicWALL security appliance. The following provides an overview of the key management interface objects.



Navigating the Management Interface

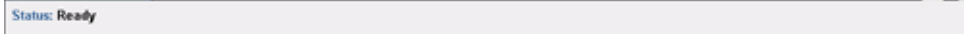
Navigating the SonicWALL management interface includes a hierarchy of menu buttons on the navigation bar (left side of your browser window). When you click a menu button, related management functions are displayed as submenu items in the navigation bar.



To navigate to a submenu page, click the link. When you click a menu button, the first submenu item page is displayed. The first submenu page is automatically displayed when you click the menu button. For example, when you click the **Network** button, the **Network > Settings** page is displayed.

Status Bar

The **Status** bar at the bottom of the management interface window displays the status of actions executed in the SonicWALL management interface.

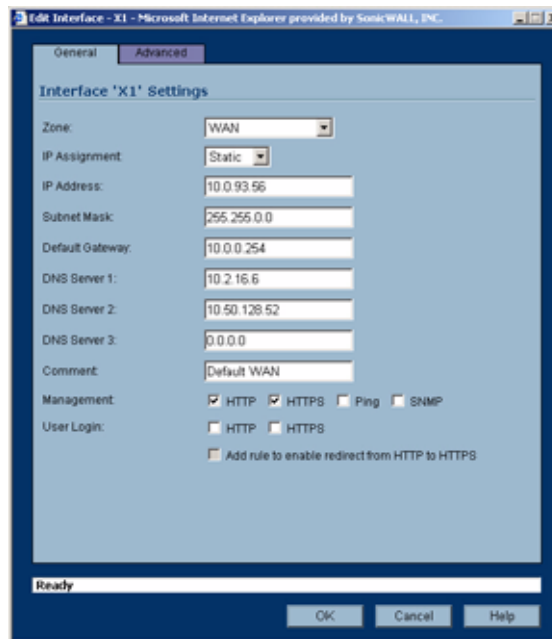


Applying Changes

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 security appliance.

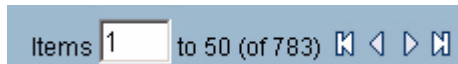


Navigating Tables

Navigate tables in the management interface with large number of entries by using the navigation buttons located on the upper right top corner of the table.

#	Time	Message	Source	Destination	Notes	Rule
1	10/14/2004 09:51:44.094	Web management request allowed	10.0.202.62, 1765, WAN	192.168.168.168, 443, LAN	TCP HTTPS	
2	10/14/2004 09:51:06.784	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
3	10/14/2004 09:50:07.352	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
4	10/14/2004 09:49:08.788	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
5	10/14/2004 09:48:09.176	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
6	10/14/2004 09:47:10.484	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
7	10/14/2004 09:46:11.896	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
8	10/14/2004 09:45:12.176	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
9	10/14/2004 09:44:12.672	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
10	10/14/2004 09:43:14.032	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
11	10/14/2004 09:42:14.384	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
12	10/14/2004 09:41:14.736	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
13	10/14/2004 09:40:16.048	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
14	10/14/2004 09:39:32.560	Web management request allowed	10.0.202.62, 1734, WAN	192.168.168.168, 443, LAN	TCP HTTPS	
15	10/14/2004 09:39:17.560	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
16	10/14/2004 09:38:18.912	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	

The table navigation bar includes buttons for moving through table pages.




Common Icons in the Management Interface

The following describe the functions of common icons used in the SonicWALL management interface:


Clicking on the edit  icon displays a window for editing the settings.

Clicking on the delete  icon deletes a table entry

Moving the pointer over the comment  icon displays text from a **Comment** field entry.

Getting Help

Each SonicWALL security appliance includes Web-based on-line 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: Accessing the SonicWALL security appliance online help requires an active Internet connection.

Logging Out

The **Logout** button at the bottom of the menu bar terminates the management interface session and displays the authentication page for logging into the SonicWALL security appliance.



PART

2

System

Viewing Status Information

System > Status

The **System > Status** page provides a comprehensive collection of information and links to help you manage your SonicWALL security appliance and SonicWALL Security Services licenses. It includes status information about your SonicWALL security appliance organized into five sections: **System Messages**, **System Information**, **Security Services**, **Latest Alerts**, and **Network Interfaces** as well as the **Wizards** button for accessing the **SonicWALL Configuration Wizard**.

The screenshot displays the 'System > Status' page with the following sections:

- System Messages:**
 - Please check with [SonicWALL](#) for information about new Services and Upgrades for your Appliance.
 - Log messages cannot be sent because you have not specified an outbound SMTP server address.
- System Information:**
 - Model: PRO 2040 Enhanced
 - Serial Number: 0006B111A2C4
 - Authentication Code: Y24Y-LJGH
 - Firmware Version: SonicOS Enhanced 3.2.0.0-21e
 - ROM Version: SonicROM 2.1.0.0
 - CPU (10s average): 0.50% - 800MHz VIA C3 Processor
 - Total Memory: 128MB RAM, 64MB Flash
 - System Time: 01/23/2006 17:21:50
 - Up Time: 2 Days 23:07:23
 - Current Connections: 344
 - Last Modified By: 192.168.168.65:X0 01/22/2006 03:18:58
 - Registration Code: HVEBWD8B
- Security Services:**

Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 20 Licenses (0 in use)
CF S (Content Filter)	Licensed
Network Anti-Virus	Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
E-Mail Filter	Licensed
ViewPoint	Licensed
- Latest Alerts:**

Date/Time	Message
01/23/2006 14:36:43	Possible port scan dropped
01/23/2006 13:54:09	Possible port scan dropped
01/23/2006 13:54:07	Possible port scan dropped
01/23/2006 12:20:24	Administrator login denied due to bad credentials
01/23/2006 10:50:49	Possible port scan dropped
- Network Interfaces:**

Name	IP Address	Link Status
X0 (LAN)	192.168.168.168	100 Mbps half-duplex
X1 (WAN)	68.35.78.194	100 Mbps full-duplex
X2 (WLAN)	172.16.31.1	100 Mbps full-duplex
X3 (LAN)	192.100.100.1	No link

Wizards

The **Wizards** button on the **System > Status** page provides access to the **SonicWALL Configuration Wizard**, which allows you to easily configure the SonicWALL security appliance using the following sub-wizards:

- **Setup Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to secure your Internet (WAN) and LAN connections.

- **Public Server Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to provide public access to an internal server, such as a Web or E-mail server.
- **VPN Wizard** - This wizard helps you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept VPN connections from SonicWALL Global VPN Clients.
- **Wireless Wizard** - (SonicWALL TZ 170 Wireless and SonicWALL TZ 170 SP Wireless only), this wizard helps you select a wireless deployment mode and configure the radio settings of the built-in 802.11b/g antennas.



Cross Reference: For more information on using the SonicWALL Configuration Wizard, see Part 11 Wizards.

System Messages

Any information considered relating to possible problems with configurations on the SonicWALL security appliance such as password, log messages, as well as notifications of SonicWALL Security Services offers, new firmware notifications, and upcoming Security Service s expirations are displayed in the **System Messages** section.

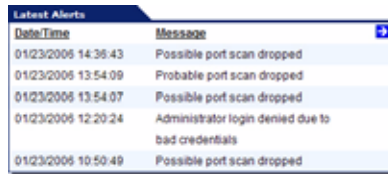
System Information

The following information is displayed in this section:

- **Model** - type of SonicWALL security appliance product
- **Serial Number** - also the MAC address of the SonicWALL security appliance
- **Authentication Code** - the alphanumeric code used to authenticate the SonicWALL security appliance on the registration database at <https://www.mysonicwall.com>.
- **Firmware Version** - the firmware version loaded on the SonicWALL security appliance.
- **ROM Version** - indicates the ROM version.
- **CPU** - displays the average CPU usage over the last 10 seconds and the type of the SonicWALL security appliance processor.
- **Total Memory** - indicates the amount of RAM and flash memory.
- **System Time** - The time registered on the internal clock on the SonicWALL appliance.
- **Up Time** - the length of time, in days, hours, and seconds the SonicWALL security appliance is active.
- **Current Connections** - the number of network connections currently existing on the SonicWALL security appliance.
- **Last Modified By** - The IP address of the user who last modified the system and the time stamp of the last modification.
- **Registration Code** - the registration code is generated when your SonicWALL security appliance is registered at <http://www.mysonicwall.com>.

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.



Date/Time	Message
01/23/2006 14:36:43	Possible port scan dropped
01/23/2006 13:54:09	Probable port scan dropped
01/23/2006 13:54:07	Possible port scan dropped
01/23/2006 12:20:24	Administrator login denied due to bad credentials
01/23/2006 10:50:49	Possible port scan dropped



Cross Reference: For more information on SonicWALL security appliance logging, see *Part 10 Log*.

Security Services

If your SonicWALL security appliance is not registered at mySonicWALL.com, the following message is displayed in the **Security Services** folder: **Your SonicWALL security appliance is not registered.** Click [here](#) to Register your SonicWALL security appliance. You need a mySonicWALL.com account to register your SonicWALL security appliance or activate security services. You can create a mySonicWALL.com account directly from the SonicWALL management interface.



Security Services

Nodes/Users: Unlimited Nodes
Your SonicWALL is not registered.
 Click here to [Register](#) your SonicWALL.

To manually register, remember the following information:
Serial Number: 0008B1135A84
Authentication Code: T778-Y437
 and go to the [SonicWALL](#) Web site.

You will be given a registration code, which you should enter below:

If your SonicWALL security appliance is registered 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-based management interface. SonicWALL Security Services and SonicWALL security appliance registration is managed by mySonicWALL.com.



Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 20 Licenses (0 in use)
CFS (Content Filter)	Licensed
Network Anti-Virus	Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
E-Mail Filter	Licensed
ViewPoint	Licensed

Cross Reference: Refer to *Part 13 Security Services* for more information on SonicWALL Security Services and activating them on the SonicWALL security appliance.

Registering Your SonicWALL Security Appliance

Once you have established your Internet connection, it is recommended you register your SonicWALL security appliance. Registering your SonicWALL security appliance provides the following benefits:

- Try a FREE 30-day trial of SonicWALL Intrusion Prevention Service, SonicWALL Gateway Anti-Virus, Content Filtering Service, and Network Anti-Virus.
- Activate SonicWALL security services and upgrades
- Access SonicOS firmware updates
- Get SonicWALL technical support

Before You Register

If your SonicWALL security appliance is not registered, the following message is displayed in the **Security Services** folder on the **System > Status** page in the SonicWALL management interface: **Your SonicWALL is not registered. Click here to [Register](#) your SonicWALL.** You need a mySonicWALL.com account to register the SonicWALL security appliance.

If your SonicWALL security appliance is connected to the Internet, you can create a mySonicWALL.com account and register your SonicWALL security appliance directly from the SonicWALL management interface. If you already have a mySonicWALL.com account, you can register the SonicWALL security appliance directly from the management interface.

Your mySonicWALL.com account is accessible from any Internet connection by pointing your Web browser to [<https://www.mysonicwall.com>](https://www.mysonicwall.com). mySonicWALL.com uses the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information.



Alert: Make sure the **Time Zone** and **DNS** settings on your SonicWALL security appliance are correct when you register the device. See SonicWALL Setup Wizard instructions for instructions on using the **Setup Wizard** to set the **Time Zone** and **DNS** settings.



Note: mySonicWALL.com registration information is not sold or shared with any other company.

You can also register your security appliance at the [<https://www.mysonicwall.com>](https://www.mysonicwall.com) site by using the **Serial Number** and **Authentication Code** displayed in the **Security Services** section. Click the **SonicWALL** link to access your mySonicWALL.com account. You will be given a registration code after you have registered your security appliance. Enter the registration code in the field below **You will be given a registration code, which you should enter below** heading, then click **Update**.

Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL management interface.

To create a mySonicWALL.com account from the SonicWALL management interface:

- 1 In the **Security Services** section on the **System > Status** page, click the **Register** link in **Your SonicWALL is not registered. Click here to [Register](#) your SonicWALL.**



- Click the [here](#) link in **If you do not have a mySonicWALL account, please click here to create one** on the **mySonicWALL Login** page.

- In the **MySonicWALL Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields in the mySonicWALL.com account form. All fields marked with an * are required fields.



Note: Remember your username and password to access your mySonicWALL.com account.

- Click **Submit** after completing the **MySonicWALL Account** form.
- When the mySonicWALL.com server has finished processing your account, a page is displayed confirming your account has been created. Click **Continue**.
- Congratulations! Your mySonicWALL.com account is activated. Now you need to log into mySonicWALL.com from the management appliance to register your SonicWALL security appliance.

Registering Your SonicWALL Security Appliance

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

- In the **Security Services** section on the **System > Status** page, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL**. The **mySonicWALL Login** page is displayed.

- In the **mySonicWALL.com Login** page, enter your mySonicWALL.com username and password in the **User Name** and **Password** fields and click **Submit**.
- The next several pages inform you about free trials available to you for SonicWALL's Security Services:
 - ♦ **Gateway Anti-Virus** - protects your entire network from viruses
 - ♦ **Network Anti-Virus** - protects computers on your network from viruses
 - ♦ **Premium Content Filtering Service** - protects your network and improves productivity by limiting access to unproductive and inappropriate Web sites
 - ♦ **Intrusion Prevention Service** - protects your network from Trojans, worms, and application layer attacks.

Click **Continue** on each page.

- At the top of the Product Survey page, enter a friendly name for your SonicWALL security appliance in the **Friendly name** field, and complete the optional product survey.
- Click **Submit**.

- 6 When the mySonicWALL.com server has finished processing your registration, a page is displayed confirming your SonicWALL security appliance is registered.
- 7 Click **Continue**. The **Manage Services Online** table on the **System > Licenses** page displayed.

Network Interfaces

Network Interfaces displays information about the interfaces for your SonicWALL security appliance. Clicking the blue arrow displays the **Network > Interfaces** page for configuring your **Network** settings. The available interfaces displayed in the Network Interfaces section depends on the SonicWALL security appliance model.

SonicWALL PRO 1260

- **WAN** - IP address, network speed and devices connected to the WAN interface.
- **OPT (Unassigned)** - user definable interface.
- **1 - 24** - user-defined interfaces.

SonicWALL PRO 2040

- **(X0) LAN** - IP address and network speed.
- **(X1) WAN** - IP address, network speed and devices connected to the WAN interface.
- **X2 - X3** - user-defined interfaces.

SonicWALL PRO 3060/PRO 4060

- **(X0) LAN** - IP address and network speed.
- **(X1) WAN** - IP address, network speed and devices connected to the WAN interface.
- **X2 - X5** - user-defined interfaces.

SonicWALL PRO 4100

The SonicWALL PRO 4100 interfaces support up to 1 Gbps.

- **(X0) LAN** - IP address and network speed.
- **(X1) WAN** - IP address, network speed and devices connected to the WAN interface.
- **X2 - X10** - user-defined interfaces.

SonicWALL PRO 5060 (Copper)

The SonicWALL PRO 5060 interfaces support up to 1 Gbps.

- **(X0) LAN** - IP address and network speed.
- **(X1) WAN** - IP address, network speed and devices connected to the WAN interface.
- **X2 - X5** - user-defined interfaces.

SonicWALL PRO 5060 (Fiber)

The SonicWALL PRO 5060 interfaces support up to 1 Gbps.

- **(X0) default LAN** - IP address and network speed. (LAN may be changed to F0)
- **(X1) default WAN** - IP address, network speed and devices connected to the WAN interface. (WAN may be changed to F1)
- **X2 - X3** - user-defined copper interfaces (10/100/1000).
- **F0 - F1** - user-defined fiber-optic interfaces (100/1000).

SonicWALL TZ 170

- **LAN (LAN)** - IP address and network speed.
- **WAN (WAN)** - IP address, network speed and devices connected to the WAN interface.
- **OPT (Unassigned)** - user definable interface.

SonicWALL TZ 170 SP

- **LAN (LAN)** - IP address and network speed.
- **WAN (WAN)** - IP address, network speed and devices connected to the WAN interface.
- **OPT (Unassigned)** - user definable interface.
- **Modem (WAN)** - IP address, connection status.

SonicWALL TZ 170 Wireless

- **LAN (LAN)** - IP address and network speed.
- **WAN (WAN)** - IP address, network speed and devices connected to the WAN interface.
- **OPT (Unassigned)** - user definable interface.
- **WLAN (WLAN)** - IP address and network speed.

SonicWALL TZ 170 SP Wireless

- **LAN (LAN)** - IP address and network speed.
- **WAN (WAN)** - IP address, network speed and devices connected to the WAN interface.
- **OPT (Unassigned)** - user definable interface.
- **Modem (WAN)** - IP address, connection status.
- **WLAN (WLAN)** - IP address and network speed.

Managing SonicWALL Licenses

System > Licenses

The **System > Licenses** page provides links to activate, upgrade, or renew SonicWALL Security Services licenses. From this page in the SonicWALL Management Interface, you can manage all the SonicWALL Security Services licensed for your SonicWALL security appliance. The information listed in the **Security Services Summary** table is updated from your mySonicWALL.com account. The **System > Licenses** page also includes links to FREE trials of SonicWALL Security Services.

Node License Status

A node is a computer or other device connected to your LAN with an IP address.

If your SonicWALL security appliance is licensed for unlimited nodes, the **Node License Status** section displays the message: **The SonicWALL is licensed for unlimited Nodes/Users**. No other settings are displayed.

If your SonicWALL security appliance is not licensed for unlimited nodes, the **Node License Status** table lists how many nodes your security appliance is licensed to have connected at any one time, how many nodes are currently connected, and how many nodes you have in your **Node License Exclusion List**.




The **Currently Licensed Nodes** table lists details on each node connected to your security appliance.

MAC Address	IP Address	Interface	Name	Exclude
00 0a 5f e5 25 fe	192.168.168.1	LAN	N/A	<input type="checkbox"/>

Excluding a Node

When you exclude a node, you block it from connecting to your network through the security appliance. Excluding a node creates an address object for that IP address and assigns it to the Node License Exclusion List address group.

To exclude a node:

- 1 Select the node you want to exclude in the **Currently Licensed Nodes** table on the **System > Licenses** page, and click the  icon in the **Exclude** column for that node.
- 2 A warning displays, saying that excluding this node will create an address object for it and place it in the **License Exclusion List** address group. Click **OK** to exclude the node.

You can manage the **License Exclusion List** group and address objects in the **Network > Address Objects** page of the management interface. Click the **Node License Exclusion List** link to jump to the **Network > Address Objects** page. See **Chapter 16, Configuring Address Objects** for instructions on managing address objects.

Security Services Summary

The **Security Services Summary** table lists the available and activated security services on the SonicWALL security appliance.

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
Network Anti-Virus	Expired	100	
Intrusion Prevention Service	Expired		
Gateway Antivirus	Not Licensed		
Server Anti-Virus	Not Licensed		
CFB Standard	Expired		
Premium Content Filtering Service	Free Trial		05 May 2005
E-Mail Filtering Service	Not Licensed		
VPN	Licensed		
Global VPN Client	Not Licensed		
Global VPN Client Enterprise	Licensed	2000	
SonicOS Enhanced	Licensed		
Global Security Client	Not Licensed		
ViewPoint	Licensed		

The **Security Service** column lists all the available SonicWALL Security Services and upgrades available for the SonicWALL security appliance. 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 **Expiration** column displays the expiration date for any Licensed Security Service.

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



Cross Reference: For more information on SonicWALL Security Services, see **Part 12, “Security Services”**.

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 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.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	100	04 Aug 2004
Intrusion Prevention Service	Expired		Renew		06 Jun 2004
Gateway AntiVirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
CFS Standard	Expired		Renew		05 Jun 2004
CFS Premium Service	Free Trial		Renew		06 May 2005
E-Mail Filtering Service	Not Licensed				
VPN	Licensed				
Global VPN Client	Not Licensed		Activate		
Global VPN Client Enterprise	Licensed		Upgrade Share	2000	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Licensed				

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**.



Manual Upgrade for Closed Environments

If your SonicWALL security appliance is deployed in a high security environment that does not allow direct Internet connectivity from the SonicWALL security appliance, you can enter the encrypted license key information from <http://www.mysonicwall.com> manually on the **System > Licenses** page in the SonicWALL Management Interface.



Note: Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your SonicWALL security appliance.

From a Computer Connected to the Internet

1. Make sure you have an account at <http://www.mysonicwall.com> and your SonicWALL security appliance is registered to the account before proceeding.
2. After logging into www.mysonicwall.com, click on your registered SonicWALL security appliance listed in **Registered SonicWALL Products**.
3. Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected SonicWALL security appliance and activated Security Services. Copy the Keyset text for pasting into the **System > Licenses** page or print the page if you plan to manually type in the Keyset into the SonicWALL security appliance.

From the Management Interface of your SonicWALL Security Appliance

4. Make sure your SonicWALL security appliance is running SonicOS Standard or Enhanced 2.1 (or higher).
5. Paste (or type) the Keyset (from the step 3) into the Keyset field in the **Manual Upgrade** section of the **System > Licenses** page (SonicOS).
6. Click the **Submit** or the **Apply** button to update your SonicWALL security appliance. The status field at the bottom of the page displays The configuration has been updated.
7. You can generate the **System > Diagnostics > Tech Support Report** to verify the upgrade details.



Note: After the manual upgrade, the **System > Licenses** page does not contain any registration and upgrade information.



Tip: The warning message: **SonicWALL Registration Update Needed. Please update your registration information** remains on the **System > Status** page after you have registered your SonicWALL security appliance. Ignore this message.

Configuring SonicWALL Security Appliance Administration Settings

System > Administration

The System Administration page provides settings for the configuration of SonicWALL security appliance for secure and remote management. You can manage the SonicWALL using a variety of methods, including HTTPS, SNMP or SonicWALL Global Management System (SonicWALL GMS).

Firewall Name

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

Administrator Name & Password

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, type the new name in the **Administrator Name** field. Click **Apply** for the changes to take effect on the SonicWALL.

Changing the Administrator Password

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



Tip: *It's recommended you change the default password "**password**" to your own custom password.*

Login Security

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

- ✓ **Tip:** *If the Administrator Inactivity Timeout is extended beyond 5 minutes, you should end every management session by clicking Logout to prevent unauthorized access to the SonicWALL security appliance's Management Interface.*

Enable Administrator/User Lockout

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

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

Web Management Settings

The screenshot shows the 'Web Management Settings' page. It includes the following fields and values:

- HTTP Port: 80
- HTTPS Port: 443
- Certificate Selection: Use Selfsigned Certificate
- Certificate Common Name: 192.168.168.168
- Table Size: 50 items per page

A 'Delete cookies' button is located to the right of the HTTP Port field.

The SonicWALL security appliance can be managed using HTTP or HTTPS and a Web browser. Both HTTP and HTTPS are enabled by default. The default port for HTTP is port 80, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Apply**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWALL security appliance. For example, if you configure the port to be 76, then you must type <LAN IP Address>:76 into the Web browser, i.e. <http://192.168.168.1:76>. The default port for HTTPS management is **443**.

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

The **Certificate Selection** menu allows you to use a self-signed certificate (**Use Self-signed Certificate**), which allows you to continue using a certificate without downloading a new one each time you log into the SonicWALL security appliance. You can also choose **Import Certificate** to select an imported certificate from the **System > Certificates** page to use for authentication to the management interface.

The **Delete Cookies** button removes all browser cookies saved by the SonicWALL appliance. Deleting cookies will cause you to lose any unsaved changes made in the Management interface.

Changing the Default Size for SonicWALL Management Interface Tables

The SonicWALL Management Interface allows you to control the display of large tables of information across all tables in the management Interface. You can change the default table page size in all tables displayed in the SonicWALL Management Interface from the default 50 items per page to any size ranging from 1 to 5,000 items.

To change the default table size:

- 1 Enter the maximum table size number in the **Table Size** field.
- 2 Click **Apply**.

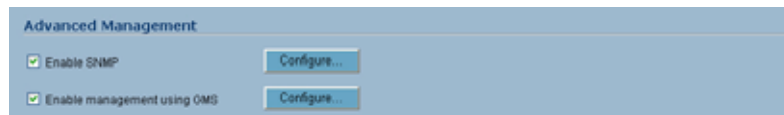
SSH Management Settings



If you use SSH to manage the SonicWALL appliance, you can change the SSH port for additional security. The default SSH port is **22**.

Advanced Management

You can manage the SonicWALL security appliance using SNMP or SonicWALL Global Management System. The following sections explain how to configure the SonicWALL for management by these two options.



Cross Reference: For more information on SonicWALL Global Management System, go to <http://www.sonicwall.com>.

Enabling SNMP Management

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 security appliance and receive notification of critical events as they occur on the network. The SonicWALL security appliance supports SNMP v1/v2c and all relevant Management Information Base II (MIB) groups except **egg** and **at**. The SonicWALL security appliance 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.

Configuring SNMP Management

To enable SNMP on the SonicWALL security appliance, log into the Management interface and click **System**, then Administration. Select the **Enable SNMP** checkbox, and then click **Configure**. The **Configure SNMP** window is displayed.

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

Configuring Log/Log Settings for SNMP

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

Configuring SNMP as a Service and Adding Rules

By default, the SonicWALL security appliance 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.



Cross Reference: For instructions on adding services and rules to the SonicWALL security appliance, see *Part 5 Firewall*.

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

Enable GMS Management

You can configure the SonicWALL security appliance to be managed by SonicWALL Global Management System (SonicWALL GMS).

Configuring the SonicWALL Security Appliance for GMS Management

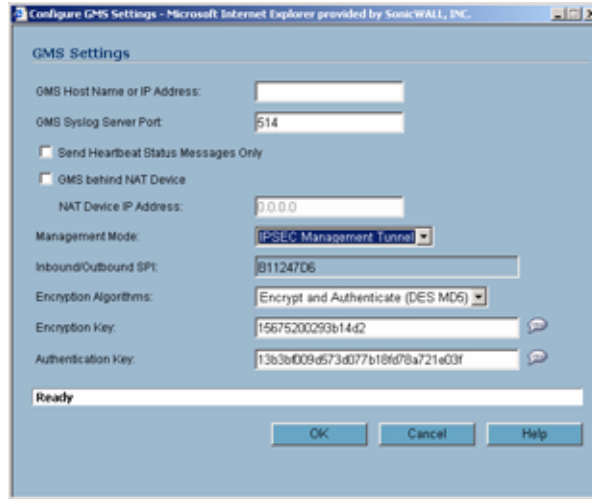
To configure the SonicWALL security appliance for GMS management:

- 1 Select the **Enable Management using GMS** checkbox, then click **Configure**. The **Configure GMS Settings** window is displayed.

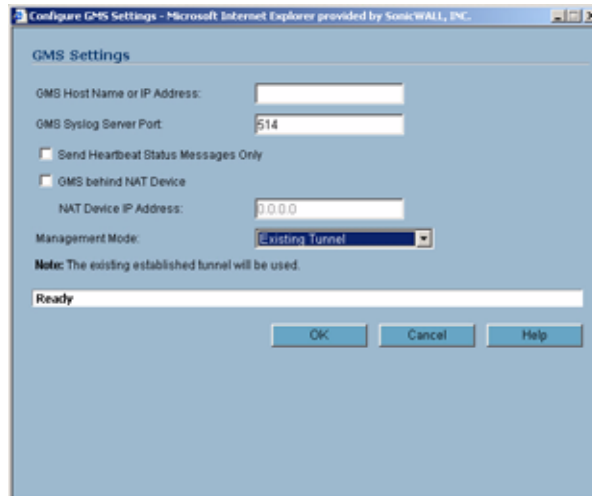
- 2 Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
- 3 Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.
- 4 Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.
-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

IPSEC Management Tunnel - Selecting this option allows the SonicWALL security appliance to be managed over an IPsec VPN tunnel to the GMS management console. The default IPsec VPN settings are displayed. Select **GMS behind NAT Device** if applicable to the GMS installation, and

enter the IP address in the **NAT Device IP Address** field. The default VPN policy settings are displayed at the bottom of the **Configure GMS Settings** window.

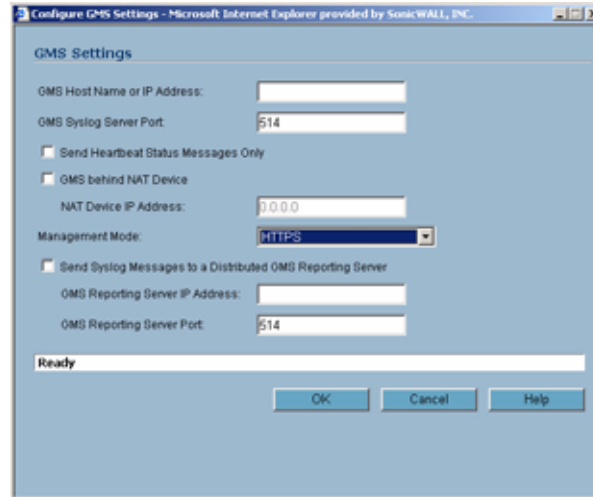


Existing Tunnel - If this option is selected, the GMS server and the SonicWALL security appliance already have an existing VPN tunnel over the connection. Enter the GMS host name or IP address in the **GMS Host Name or IP Address** field. Enter the port number in the **Syslog Server Port** field.



HTTPS - If this option is selected, HTTPS management is allowed from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The SonicWALL security appliance also sends encrypted syslog packets and SNMP traps using 3DES and the SonicWALL security

appliance administrator's password. The following configuration settings for HTTPS management mode are displayed:



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

Send Syslog Messages to a Distributed GMS Reporting Server - Sends regular heartbeat messages to both the GMS Primary and Standby Agent IP address. The regular heartbeat messages are sent to the specified GMS reporting server and the reporting server port.

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

7 Click **OK**.

Download URL

VPN Client Download URL

SonicWALL Global VPN Client (GVC) and SonicWALL Global Security Client (GSC) allow users to connect securely to your network using the GroupVPN Policy on the port they are connecting to. GVC or the VPN client portion of GSC are required for a user to connect to the GroupVPN Policy. Depending on how you have set up your VPN policies, if a user does not have the latest GVC or GSC software installed, the user will be directed to a URL to download the latest GVC or GSC software.

The **Download URL** section provides a field for entering the URL address of a site for downloading the SonicWALL Global VPN Client application, when a user is prompted to use the Global VPN Client for access to the network.



The default URL <http://help.mysonicwall.com/applications/vpnclient> displays the SonicWALL Global VPN Client download site. You can point to any URL where you provide the SonicWALL Global VPN Client application.

SonicPoint Download URL (TZ 170 Series and PRO 1260)

The TZ 170 series and PRO 1260 security appliances do not contain the SonicOS firmware embedded locally on the security appliance's memory. Therefore, if you are managing SonicPoints from a TZ 170 or PRO 1260 running SonicOS 3.1 or newer, the security appliance will download the SonicPoint image at startup for distribution to connected SonicPoint devices. The image is downloaded from software.sonicwall.com or from the URL you specify in the **SonicPoint Download URL** field.

The downloaded SonicPoint firmware image is signed with SonicWALL's certificate to ensure integrity.

The default location is *software.sonicwall.com/applications/sonicpoint/*

If the TZ 170 or PRO 1260 running SonicOS Enhanced 3.1 and requiring SonicPoint support does not have Internet access, you can download the SonicPoint image from mysonicwall.com and host it on a local web-server. In this case, enter the URL for the local server in the **SonicPoint Download URL** field.

The image shows two side-by-side screenshots of the SonicPoint configuration interface. Both screenshots have a blue header with the text 'Download URL'. Each screenshot contains two input fields: 'VPN Client Download URL (http://):' and 'SonicPoint Download URL (http://):'. In the left screenshot, the first field contains 'help.mysonicwall.com/applications/vpnclient/' and the second field contains 'software.sonicwall.com/applications/sonicpoint/'. In the right screenshot, the first field contains 'help.mysonicwall.com/applications/vpnclient/' and the second field contains '10.50.165.2/sonicpoint/'. Below each input field is a yellow comment box with the text: 'Note: The last character must be a slash'.



Note: The specified path must always end in a '/' (trailing slash). The filename should not be specified.

Managing Certificates

Digital Certificates Overview

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWALL has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

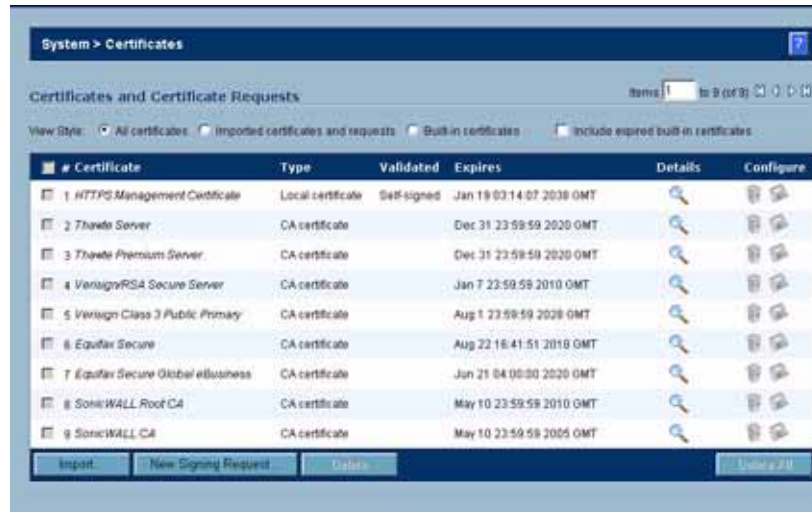
A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

SonicWALL security appliances interoperate with any X.509v3-compliant provider of Certificates. SonicWALL security appliances have been tested with the following vendors of Certificate Authority Certificates:

- Entrust
- Microsoft
- OpenCA
- OpenSSL
- VeriSign

System > Certificates

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the SonicWALL security appliance to validate your Local Certificates. You import the valid CA certificate into the SonicWALL security appliance using the **System > Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates.







Certificates and Certificate Requests

The **Certificate and Certificate Requests** section provides all the settings for managing CA and Local Certificates.

The **View Style** menu allows you to display your certificates in the **Certificates and Certificate Requests** table based on the following criteria:

- **All Certificates** - displays all certificates and certificate requests.
- **Imported certificates and requests** - displays all imported certificates and generated certificate requests.
- **Built-in certificates** - displays all certificates included with the SonicWALL security appliance.
- **Include expired and built-in certificates** - displays all expired and built-in certificates.

The **Certificates and Certificate Requests** table displays the following information about your certificates:

- **Certificate** - the name of the certificate.
- **Type** - the type of certificate, which can include CA or Local.
- **Validated** - the validation information.
- **Expires** - the date and time the certificate expires.
- **Details** - the details of the certificate. Moving the pointer over the  icon displays the details of the certificate.
- **Configure** - Displays the  edit and delete  icons for editing or deleting a certificate entry. Also displays the  Import icon to import either certificate revocation lists (for CA certificates) or signed certificates (for Pending requests).

Certificate Details

Clicking on the icon in the **Details** column of the **Certificates and Certificate Requests** table lists information about the certificate, which may include the following, depending on the type of certificate:

- **Certificate Issuer**
- **Subject Distinguished Name**
- **Certificate Serial Number**
- **Valid from**
- **Expires On**
- **Status** (for Pending requests and local certificates)
- **CRL Status** (for Certificate Authority certificates)

The details shown in the **Details** mouseover popup depend on the type of certificate. **Certificate Issuer**, **Certificate Serial Number**, **Valid from**, and **Expires On** are not shown for Pending requests since this information is generated by the Certificate provider. Similarly, **CRL Status** information is shown only for CA certificates and varies depending on the CA certificate configuration.

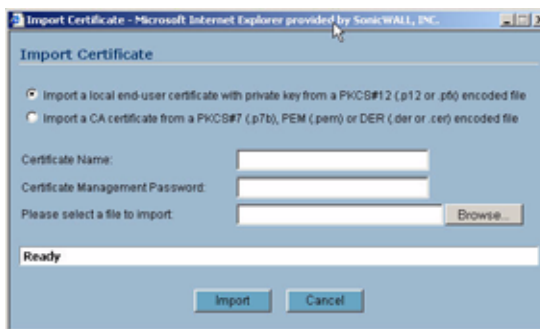
Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates may also be imported to verify Local Certificates and peer Certificates used in IKE negotiation.

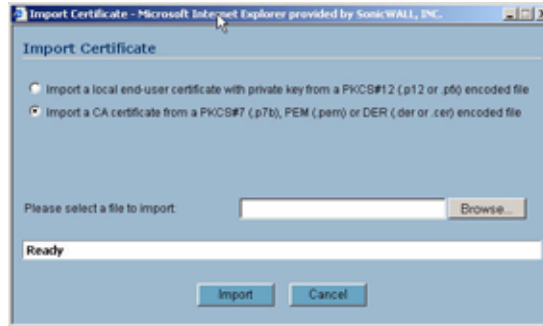
Importing a Certificate Authority Certificate


To import a certificate from a certificate authority, perform these steps:

- 1 Click **Import**. The **Import Certificate** window is displayed.



- 2 Select **Import a CA certificate from a PKCS#7 (*.p7b) or DER (.der or .cer) encoded file**. The **Import Certificate** window settings change.

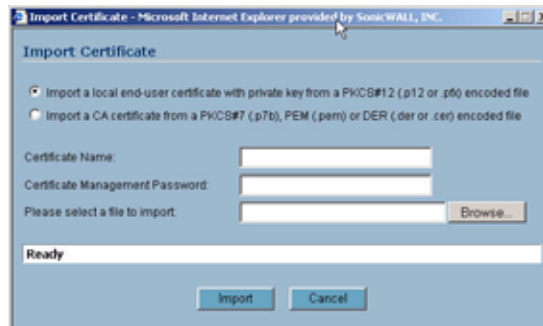



- 3 Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.
- 4 Click **Import** to import the certificate into the SonicWALL security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.
- 5 Moving your pointer to the  icon in the **Details** column displays the certificate details information.

Importing a Local Certificate

To import a local certificate, perform these steps:

- 1 Click **Import**. The **Import Certificate** window is displayed.



- 2 Enter a certificate name in the **Certificate Name** field.
- 3 Enter the password used by your Certificate Authority to encrypt the PKCS#12 file in the **Certificate Management Password** field.
- 4 Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.
- 5 Click **Import** to import the certificate into the SonicWALL security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.
- 6 Moving your pointer to  icon in the **Details** column displays the certificate details information.

Deleting a Certificate

To delete the certificate, click the delete icon. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

Certificate Revocation List (CRL)

A **Certificate Revocation List (CRL)** is a way to check the validity of an existing certificate. A certificate may be invalid for several reasons:

- The status of the entity identified by the Certificate has changed in some way (for example, an employee has left the company).
- The private key associated with a Certificate was stolen or compromised.
- A new certificate was issued that takes precedence over the old certificate.

If a certificate is invalid, the CA may publish the certificate on a **Certificate Revocation List** at a given interval, or on an online server in a X.509 v3 database using Online Certificate Status Protocol (OCSP). Consult your CA provider for specific details on locating a CRL file or URL.



Tip: The SonicWALL security appliance supports obtaining the CRL via HTTP or manually downloading the list.

Importing a CRL

You can import the CRL by manually downloading the CRL and then importing it into the SonicWALL security appliance.

- 1 Click on the Import certificate revocation list icon . The Import CRL window is displayed.

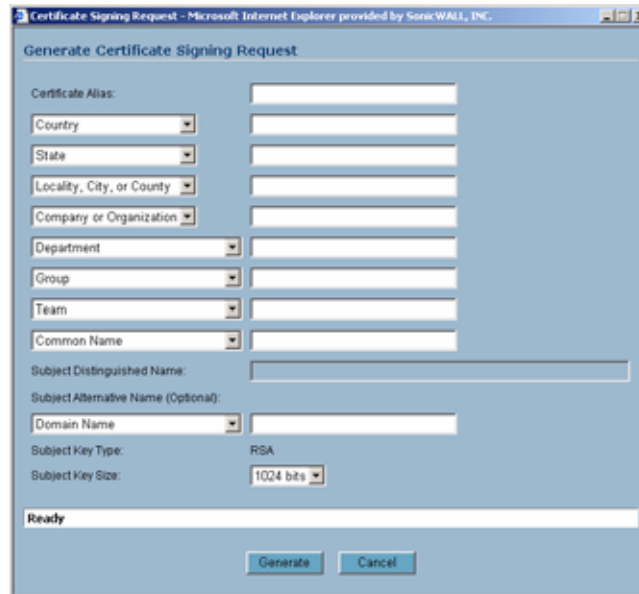
- 2 You can import the CRL from the certificate file by selecting **Import CRL directly from a PEM (.pem) or DER (.der or .cer) encoded file**, and entering the path in the Select a CRL file to import field or click the **Browse** button to navigate to the file, click **Open**, then click **Import**.
- 3 You can also enter the URL location of the CRL by entering the address in the **Enter CRL's location (URL)** field, and then click **Import**. The CRL is downloaded automatically at intervals determined by the CA service. Certificates are checked against the CRL by the SonicWALL security appliance for validity when they are used.
- 4 By default, if no CRL is available, a Certificate is presumed to be valid if it passes all other checks (such as validity dates and signatures). To require that Certificates be checked against a valid CRL, enable the **Invalidate Certificates and Security Associations if CRL import or processing fails** setting.

Generating a Certificate Signing Request

To generate a local certificate, follow these steps:

✓ **Tip:** You should create a *Certificate Policy* to be used in conjunction with local certificates. A *Certificate Policy* determines the authentication requirements and the authority limits required for the validation of a certificate.

- 1 Click the **New Signing Request** button. The Certificate Signing Request window is displayed.



- 2 In the **Generate Certificate Signing Request** section, enter an alias name for the certificate in the **Certificate Alias** field.
- 3 Select the Request field type from the menu, then enter information for the certificate in the Request fields. As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.
You can also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**.
- 4 The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.
- 5 Select a Subject Key size from the **Subject Key Size** menu.



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

- 6 Click **Generate** to create a certificate signing request file. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.
- 7 Click **Export** to download the file to your computer, then click **Save** to save it to a directory on your computer.

You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

Configuring Time Settings

System > Time

The **System > Time** page defines the time and date settings to time stamp log events, to automatically update SonicWALL Security Services, and for other internal purposes.

The screenshot shows the 'System > Time' configuration page. At the top right are 'Apply', 'Cancel', and a help icon. The 'System Time' section includes: 'Time (h:mm:ss)' set to 14:06:22; 'Date' set to December 8, 2004; 'Time Zone' set to Pacific Time (US & Canada) (GMT-8:00). Below these are four checkboxes: 'Set time automatically using NTP' (checked), 'Automatically adjust clock for daylight saving time' (checked), 'Display UTC in logs (instead of local time)' (unchecked), and 'Display date in International format' (unchecked). The 'NTP Settings' section has an 'Update Interval (minutes)' field set to 60. Below is an 'NTP Server' table with 'No Entries', an 'Add...' button, and a 'Delete #B' button. A note at the bottom states: 'Note: An internal NTP list is used by default, and the above list is optional.'

By default, the SonicWALL security appliance 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.

System Time

To select your time zone and automatically update the time, choose the time zone from the **Time Zone** menu. **Set time automatically using NTP** is activated by default to use NTP (Network Time Protocol) servers from an internal list to set time automatically. **Automatically adjust clock for daylight saving changes** is also activated by default to enable automatic adjustments for daylight savings time.

If you want to set your time manually, uncheck **Set time automatically using NTP**. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus.

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

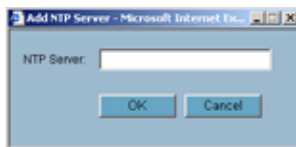
Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.

✓ **Tip:** *The SonicWALL security appliance uses 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 security appliance clock. You can also configure **Update Interval (minutes)** for the NTP server to update the SonicWALL security appliance. The default value is 60 minutes.

To add an NTP server to the SonicWALL security appliance configuration

- 1 Click **Add**. The **Add NTP Server** window is displayed.




- 2 Type the IP address of an NTP server in the **NTP Server** field.
- 3 Click **OK**.
- 4 Click **Apply** on the **System > Time** page to update the SonicWALL security appliance.

To delete an NTP server, highlight the IP address and click **Delete**. Or, click **Delete All** to delete all servers.

Setting Schedules

System > Schedules

The **System > Schedules** page allows you to create and manage schedule objects for enforcing schedule times for a variety of SonicWALL security appliance features.

Name	Days Of Week	Time	Configure
Work Hours	M-T-W-Th-F	08:00-17:00	 
After Hours	M-T-W-Th-F	00:00-00:00	 
	M-T-W-Th-F	17:00-24:00	 
	SA-SU	00:00-24:00	 
Weekend Hours	SA-SU	00:00-24:00	 

Add Delete

The **Schedules** table displays all your predefined and custom schedules. In the **Schedules** table, there are three default schedules: **Work Hours**, **After Hours**, and **Weekend Hours**. You can modify

these schedule by clicking on the edit icon in the **Configure** column to display the **Edit Schedule** window.



Note: You cannot delete the default **Work Hours**, **After Hours**, or **Weekend Hours** schedules.

You apply schedule objects for the specific security feature. For example, if you add an access rule in the **Firewall > Access Rules** page, the **Add Rule** window provides a drop down menu of all the available schedule objects you created in the **System > Schedules** page.

A schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a + (expand) button appears next to the schedule name. Clicking the + button expands the schedule to display all the day and time entries for the schedule.

Adding a Schedule

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



- 1 Enter a name for the schedule in the **Name** field.
- 2 Select the days of the week to apply to the schedule or select **All**.
- 3 Enter the time of day for the schedule to begin in the **Start** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
- 4 Enter the time of day for the schedule to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
- 5 Click **Add**.
- 6 Click **OK** to add the schedule to the **Schedules** table.

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

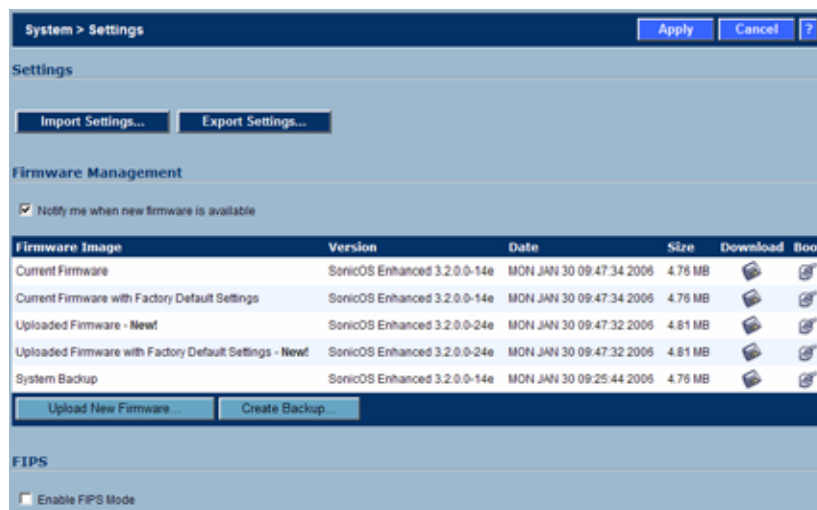
Deleting Schedules

To delete individual schedule objects you created, select the checkbox next to the schedule entry, the **Delete** button becomes enabled. Click **Delete**. To delete all schedule objects you created, select the checkbox next to **Name** column header to select all schedules. Click **Delete**.

Managing SonicWALL Security Appliance Firmware

System > Settings

This **System > Settings** page allows you to manage your SonicWALL security appliance's SonicOS versions and preferences.



The screenshot displays the 'System > Settings' interface. At the top, there are 'Apply', 'Cancel', and a help icon. Below this is the 'Settings' section with 'Import Settings...' and 'Export Settings...' buttons. The 'Firmware Management' section includes a checked checkbox for 'Notify me when new firmware is available'. A table lists the following firmware images:

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 3.2.0.0-14e	MON JAN 30 09:47:34 2006	4.76 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 3.2.0.0-14e	MON JAN 30 09:47:34 2006	4.76 MB		
Uploaded Firmware - New!	SonicOS Enhanced 3.2.0.0-24e	MON JAN 30 09:47:32 2006	4.81 MB		
Uploaded Firmware with Factory Default Settings - New!	SonicOS Enhanced 3.2.0.0-24e	MON JAN 30 09:47:32 2006	4.81 MB		
System Backup	SonicOS Enhanced 3.2.0.0-14e	MON JAN 30 09:25:44 2006	4.76 MB		

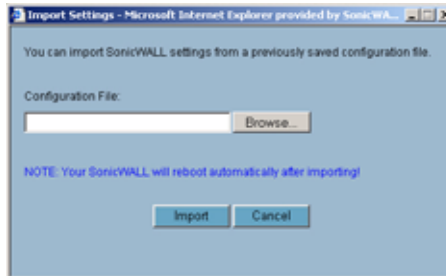
Below the table are 'Upload New Firmware...' and 'Create Backup...' buttons. The 'FIPS' section at the bottom has an unchecked checkbox for 'Enable FIPS Mode'.

Settings

Import Settings

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

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

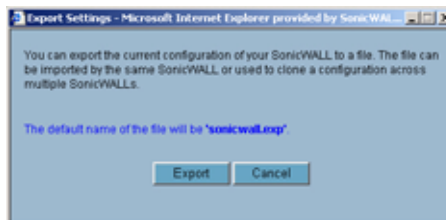


- 2 Click **Browse** to locate the file which has a *.exp file name extension.
- 3 Select the preferences file.
- 4 Click **Import**, and restart the firewall.

Export Settings

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

- 1 Click **Export Settings**. The **Export Settings** window is displayed.



- 2 Click **Export**.
- 3 Click **Save**, and then select a location to save the file. The file is named “sonicwall.exp” but can be renamed.
- 4 Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the SonicWALL security appliance 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.
- Easily return your SonicWALL security appliance to the previous system state.



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

Automatic Notification of New Firmware

To receive automatic notification of new firmware, select the **Notify me when new firmware is available** check box. If you enable this feature, the SonicWALL security appliance 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**



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

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

Firmware Management Table

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 3.2.0.0-14a	MON JAN 30 09:47:34 2006	4.76 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 3.2.0.0-14a	MON JAN 30 09:47:34 2006	4.76 MB		
Uploaded Firmware - New!	SonicOS Enhanced 3.2.0.0-24a	MON JAN 30 09:47:32 2006	4.81 MB		
Uploaded Firmware with Factory Default Settings - New!	SonicOS Enhanced 3.2.0.0-24a	MON JAN 30 09:47:32 2006	4.81 MB		
System Backup	SonicOS Enhanced 3.2.0.0-14a	MON JAN 30 09:25:44 2006	4.76 MB		

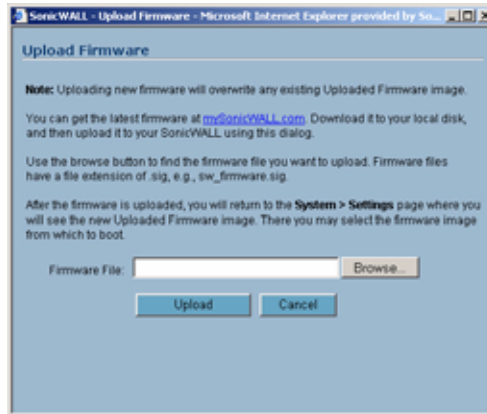
The Firmware Management table displays the following information:

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

- ▲ **Alert:** Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the **Current Firmware** image. On the TZ 170, the uploaded firmware images are removed from the table after rebooting the SonicWALL security appliance.
- ▲ **Alert:** When uploading firmware to the SonicWALL security appliance, 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.

Updating Firmware Manually

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



Creating a Backup Firmware Image

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

SafeMode - Rebooting the SonicWALL Security Appliance

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 security appliance into SafeMode. SafeMode allows you to select the firmware version to load and reboot the SonicWALL security appliance.

To access the SonicWALL security appliance using SafeMode, press the Reset button for 1 second. After the SonicWALL security appliance reboots, open your Web browser and enter the current IP address of the SonicWALL security appliance 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 security appliance.
- Upload and download system settings to the SonicWALL security appliance.
- Boot to your choice of firmware options.
- Create a system backup file.
- Return your SonicWALL security appliance to a previous system state.

System Information

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

Firmware Management

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

- **Firmware Image** - In this column, five types of firmware images are listed:
 - **Current Firmware**, firmware currently loaded on the SonicWALL security appliance
 - **Current Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
 - **Current Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**.
 - **Uploaded Firmware**, the last version uploaded from mysonicwall.com
 - **Uploaded Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
 - **Uploaded Firmware with Backup Settings** - 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 security appliance 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 security appliance.

FIPS

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWALL security appliance supports FIPS 140-2 Compliant security. Among the FIPS-compliant features of the SonicWALL security appliance include PRNG based on SHA-1 and only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1).

Select **Enable FIPS Mode** to enable the SonicWALL security appliance to comply with FIPS. When you check this setting, a dialog box is displayed with the following message: **Warning! Modifying the FIPS mode will disconnect all users and restart the device. Click OK to proceed.**

Click **OK** to reboot the security appliance in FIPS mode. A second warning displays. Click **Yes** to continue rebooting.

To return to normal operation, uncheck the **Enable FIPS Mode** check box and reboot the SonicWALL security appliance into non-FIPS mode.

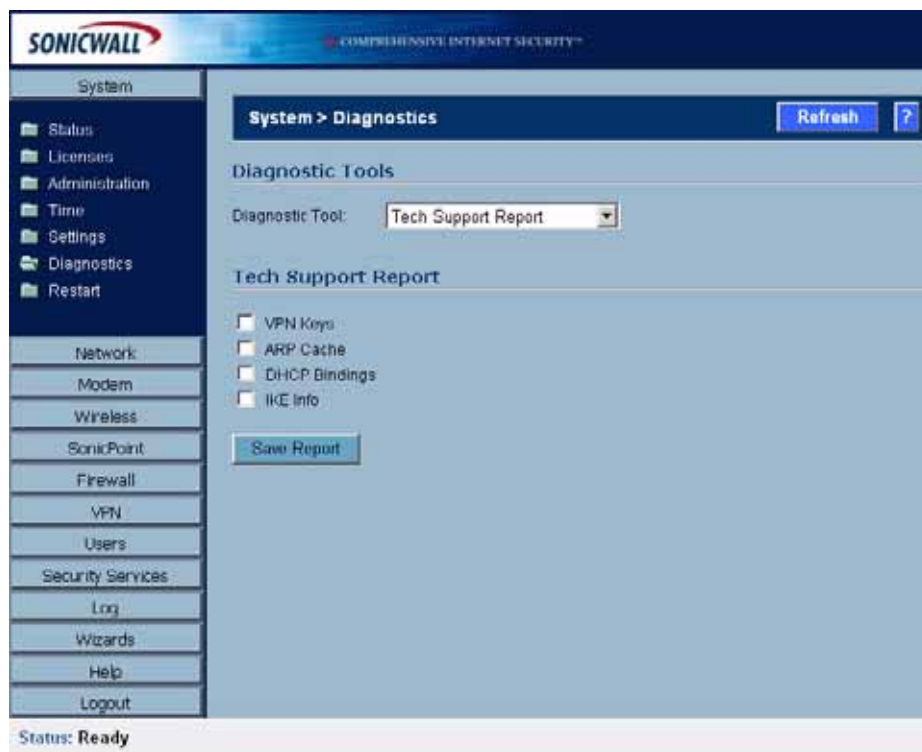


Alert: When using the SonicWALL security appliance for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWALL security appliance must remain in place and untouched.

Using Diagnostic Tools & Restarting the SonicWALL Security Appliance

System > Diagnostics

The **System > Diagnostics** page provides several diagnostic tools which help troubleshoot network problems as well as Active Connections, CPU and Process Monitors.



Tech Support Report

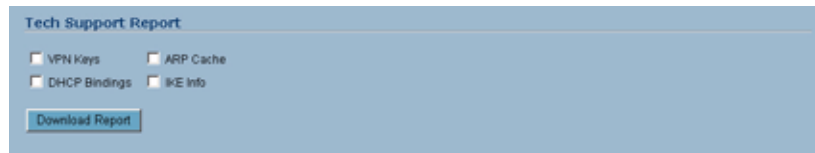
The **Tech Support Report** generates a detailed report of the SonicWALL security appliance configuration and status, and saves it to the local hard disk using the **Download Report** button. This file can then be e-mailed to SonicWALL Technical Support to help assist with a problem.



Alert: You must register your SonicWALL security appliance on mySonicWALL.com to receive technical support.

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

Generating a Tech Support Report



- 1 In the **Tech Support Report** section, select any of the following four report options:
 - **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 security appliance DHCP server.
 - **IKE Info** - saves current information about active IKE configurations.
- 2 Click **Download Report** to save the file to your system. When you click **Download Report**, a warning message is displayed.
- 3 Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.



Diagnostic Tools

You select the diagnostic tool from the **Diagnostic Tools** menu in the **Diagnostic Tool** section of the **System > Diagnostics** page. The following diagnostic tools are available:

- “Active Connections Monitor” on page 85
- “CPU Monitor” on page 86
- “DNS Name Lookup” on page 87
- “Find Network Path” on page 87
- “Packet Trace” on page 88
- “Ping” on page 89
- “Process Monitor” on page 90
- “Real-Time Black List Lookup” on page 90
- “Reverse Name Resolution” on page 90
- “Trace Route” on page 91
- “Web Server Monitor” on page 91

Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the SonicWALL security appliance. Click on a column heading to sort by that column.

Active Connections Monitor

Items 1 to 14 (of 14)

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.62	1849	192.168.168.168	443	TCP	WAN	LAN	1046	1592
2	10.0.202.62	1850	192.168.168.168	443	TCP	WAN	LAN	894	1508
3	10.0.202.62	1851	192.168.168.168	443	TCP	WAN	LAN	1359	2617
4	10.0.202.62	1852	192.168.168.168	443	TCP	WAN	LAN	374	310
5	10.0.202.62	1853	192.168.168.168	443	TCP	WAN	LAN	1354	11644
6	10.0.202.62	1854	192.168.168.168	443	TCP	WAN	LAN	1037	8571
7	10.0.202.62	1855	192.168.168.168	443	TCP	WAN	LAN	951	4943
8	10.0.202.62	1856	192.168.168.168	443	TCP	WAN	LAN	898	955
9	10.0.202.62	1857	192.168.168.168	443	TCP	WAN	LAN	1228	18125
10	10.0.202.62	1858	192.168.168.168	443	TCP	WAN	LAN	1080	9983
11	10.0.202.62	1859	192.168.168.168	443	TCP	WAN	LAN	943	2629
12	10.0.202.62	1860	192.168.168.168	443	TCP	WAN	LAN	1909	48179
13	10.0.202.62	1861	192.168.168.168	443	TCP	WAN	LAN	948	2511
14	10.0.202.62	1862	192.168.168.168	443	TCP	WAN	LAN	992	488

Active Connections Monitor Settings

Active Connections Monitor Settings

Filter	Value	Group Filters
Source IP:	192.168.168.1	<input checked="" type="checkbox"/>
Destination IP:	10.0.93.31	<input checked="" type="checkbox"/>
Destination Port:		<input type="checkbox"/>
Protocol:	TCP(6)	<input type="checkbox"/>
Filter Logic: (Source IP && Destination IP) && Destination Port && Protocol		
Apply Filters		Export Results

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface**, and **Dst Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

Source IP AND Destination IP

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

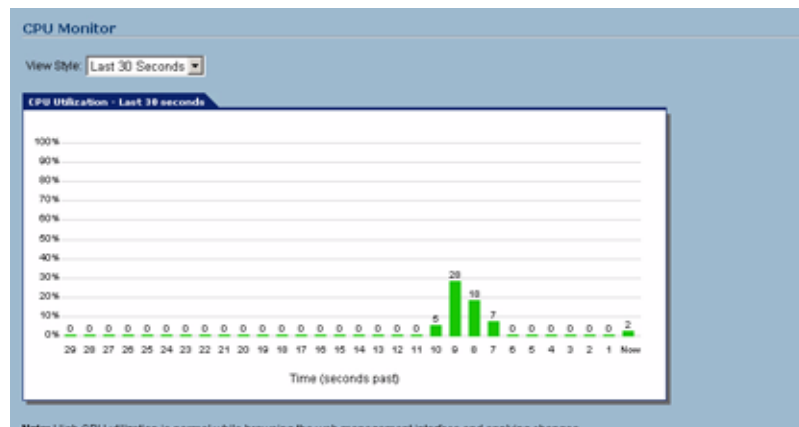
(Source IP OR Destination IP) AND Protocol

Click **Apply Filter** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

CPU Monitor

The **CPU Monitor** diagnostic tool shows real-time CPU utilization in second, minute, hour, and day intervals (historical data does not persist across reboots).



Note: High CPU utilization is normal during Web-management page rendering, and while saving preferences to flash. Utilization by these tasks is an indication that available resources are being efficiently used rather than sitting idle. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and never experience starvation.

DNS Name Lookup

The SonicWALL security appliance 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 security appliance 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 security appliance. 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 LAN or WAN ports. This can diagnose a network configuration problem on the SonicWALL security appliance. For example, if the SonicWALL security appliance indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured.

The screenshot shows the 'Diagnostic Tools' section of the SonicWALL web interface. Under 'Diagnostic Tool', 'Find Network Path' is selected. Below this, the 'Find Network Path' section has an input field for 'Find location of this IP address' containing '10.0.93.25' and a 'Go' button. The 'Result' section displays the following information:

```

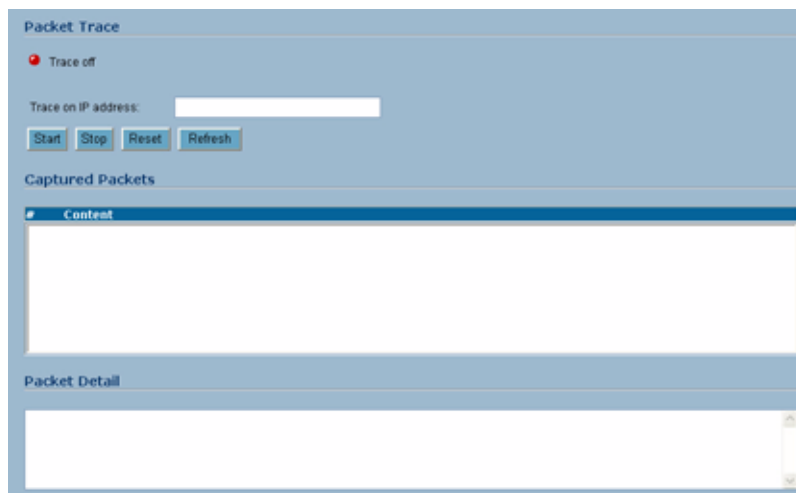
10.0.93.25 is located on the WAN
It is reached through the router at 207.88.91.85
It is reached through ethernet address 00:09:B6:5D:14:06

```

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.

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 security appliance, 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 security appliance 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 security appliance 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 security appliance 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 security appliance 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 security appliance 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 security appliance 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 security appliance 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 security appliance 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.

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 security appliance 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 security appliance returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Process Monitor

Process Monitor shows individual system processes, their CPU utilization, and their system time.

The screenshot shows the 'Process Monitor' tool interface. At the top, there is a dropdown menu for 'Diagnostic Tool' set to 'Process Monitor'. Below this is a table with the following columns: #, Name, Function, Priority, Totals (secs), and Current% (secs). The table lists 16 processes.

#	Name	Function	Priority	Totals (secs)	Current% (secs)
1	!ResetSwitc	-7fc0c50	245	0.00%	0.00
2	!ExcTask	-78c79e70	0	0.00%	0.00
3	!LogTask	-79e04e44	0	0.00%	0.00
4	!NetTask	-7fcada0	50	0.40%	8.62
5	!ChkCable	-78e779c	200	0.00%	0.00
6	!SmpTmr	-79d51e28	200	0.00%	0.00
7	!Smpd	-79d51bb4	150	0.00%	0.00
8	!SysMonitor	-7fc38fc	0	0.00%	0.00
9	!SchedulerTask	-7fc4880	97	0.55%	131.63
10	!RandSeedTask	-79e09f18	200	0.00%	0.00
11	!MainLogTask	-79e3ab4	48	0.00%	0.30
12	!TODTask	-7842168	200	0.00%	0.00
13	!AlertLed	-78e5460	40	0.00%	0.00
14	!MyAppTask	-79d1668	47	0.00%	0.00
15	!WebMain	-79d67790	48	0.00%	0.00
16	!TmrTask	-799cb2c	10	0.00%	0.00

Real-Time Black List Lookup

The **Real-Time Black List Lookup** tool allow you to test SMTP IP addresses, RBL services, or DNS servers. Enter an IP address in the **IP Address** field, a FQDN for the RBL in the **RBL Domain** field and DNS server information in the **DNS Server** field. Click **Go**.

The screenshot shows the 'Real-time Black List Lookup' tool interface. It has a dropdown menu for 'Diagnostic Tool' set to 'Real-time Black List Lookup'. Below this are three input fields: 'IP Address:', 'RBL Domain:', and 'DNS Server:'. A 'Go' button is located to the right of the 'DNS Server' field.

Reverse Name Resolution

The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.

The screenshot shows the 'Reverse Name Resolution' tool interface. It has a dropdown menu for 'Diagnostic Tool' set to 'Reverse Name Resolution'. Below this are three input fields for DNS servers: 'Log Resolution DNS Server 1:', 'Log Resolution DNS Server 2:', and 'Log Resolution DNS Server 3:'. The first two fields contain the IP addresses '206.13.28.12' and '4.2.2.2' respectively. The third field contains '0.0.0.0'. There is also a 'Reverse Lookup the IP Address:' field and a 'Go' button.

Enter an IP address in the **Reverse Lookup the IP Address** field, and it checks all DNS servers configured for your security appliance to resolve the IP address into a server name.

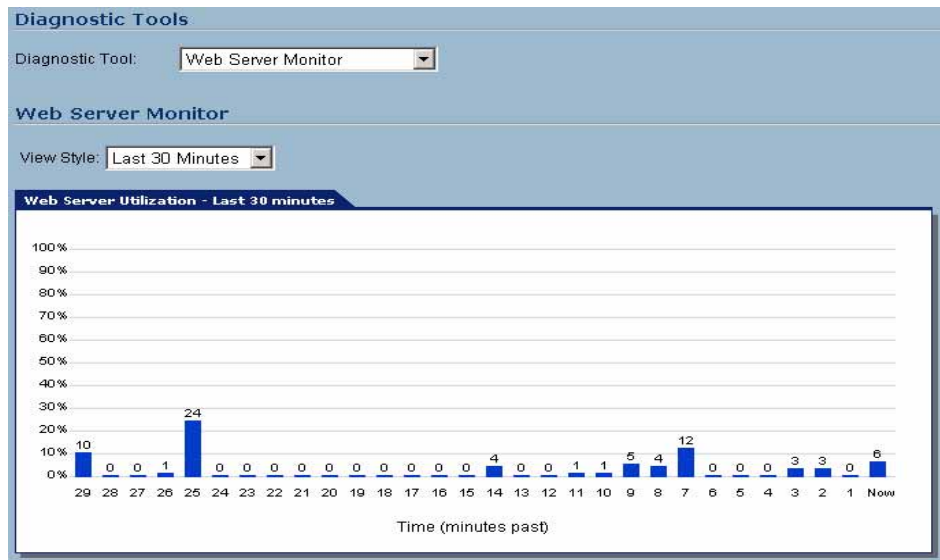
Trace Route

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

Type the IP address or domain name of the destination host. For example, type yahoo.com and click **Go**. A second window is displayed with each hop to the destination host. By following the route, you can diagnose where the connection fails between the SonicWALL security appliance and the destination.

Web Server Monitor

The **Web Server Monitor** tool displays the CPU utilization of the web server over several periods of time. The time frame of the Web Server Monitor can be changed by selecting one of the following options in the **View Style** pulldown menu: last 30 seconds, last 30 minutes, last 24 hours, or last 30 days.



System > Restart

The SonicWALL security appliance can be restarted from the Web Management interface. Click **System > Restart** to display the Restart page.



Click **Restart...** and then click **Yes** to confirm the restart.

The SonicWALL security appliance 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.

PART

3

Network

Configuring Interfaces

Network > Interfaces

The **Network > Interfaces** page includes interface objects that are directly linked to physical interfaces. The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. Physical interface objects include the LAN, WAN, OPT, and depending on which SonicWALL security appliance you have, Modem and WLAN ports in the SonicWALL security appliance.

The screenshot displays the 'Network > Interfaces' configuration page. At the top, there are buttons for 'Setup Wizard...' and 'Clear Statistics'. Below this is the 'Interface Settings' section, which contains a table with columns for Name, Zone, IP Address, Subnet Mask, IP Assignment, Status, Comment, and Configure. The table lists five interfaces: X0 (LAN), X1 (WAN), X2 (Unassigned), X3 (Unassigned), and X5 (Unassigned). Below the table is an 'Add Interface...' button. The bottom section is 'Interface Traffic Statistics', which contains a table with columns for Traffic Statistic and interfaces X0 through X5. The traffic statistics table shows data for Rx Unicast Packets, Rx Broadcast Packets, Rx Bytes, Tx Unicast Packets, Tx Broadcast Packets, and Tx Bytes for each interface.

Network > Interfaces							
Interface Settings							
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	10.0.93.56	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X4	WLAN	0.0.0.0	255.255.255.0	Static	No link		
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

Interface Traffic Statistics						
Traffic Statistic	X0	X1	X2	X3	X4	X5
Rx Unicast Packets:	0	1675	0	0	0	0
Rx Broadcast Packets:	0	57632	0	0	0	0
Rx Bytes:	0	5616064	0	0	0	0
Tx Unicast Packets:	0	1981	0	0	0	0
Tx Broadcast Packets:	0	6	0	0	0	0
Tx Bytes:	0	1291546	0	0	0	0

Setup Wizard

The **Setup Wizard** button accesses the **Setup Wizard**. The Setup Wizard walks you through step-by-step the configuration of the SonicWALL security appliance for Internet connectivity.



Cross Reference: For Setup Wizard instructions, see Chapter 67: “Configuring Internet Connectivity Using the Setup Wizard”.

Physical Interfaces

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



Cross Reference: For more information on zones, see Chapter 14: “Configuring Zones”.

The first two interfaces, LAN and WAN are fixed interfaces, permanently bound to the Trusted and Untrusted Zone types. The TZ 170 series appliances can also have two special interfaces for Modem and WLAN. The remaining Interfaces can be configured and bound to any Zone type, depending on your SonicWALL security appliance:

Permanently Assigned Interfaces

- SonicWALL PRO series: **X0** - The default LAN interface (In the PRO 5060 Fiber this can be changed to (F0).
- SonicWALL TZ 170 series: **LAN** - The single LAN interface includes all five LAN ports on the back of the TZ 170 series appliances.
- SonicWALL PRO 1260: **LAN** - The single LAN interface includes all twenty four numbered ports and the uplink port on the front of the PRO 1260 security appliance. These can be assigned to separate PortShield groups.
- SonicWALL PRO series: **X1** - The default WAN interface (In the PRO 5060 Fiber this can be changed to (F1).
- SonicWALL PRO 1260 and SonicWALL TZ 170 series: **WAN**
- SonicWALL TZ 170 SP and SonicWALL TZ 170 SP Wireless: **Modem**
- SonicWALL TZ 170 Wireless and SonicWALL TZ 170 SP Wireless: **WLAN**

User-definable Interfaces

- SonicWALL PRO 4100 security appliances include eight user-definable interfaces, **X2** through **X9**.
- SonicWALL PRO 3060/PRO 4060/PRO 5060 security appliances include four user-definable interfaces, **X2** through **X5**.
- SonicWALL PRO 2040 security appliance includes two user-definable interfaces, **X2** and **X3**.
- SonicWALL PRO 1260 security appliance includes one user definable interface, **OPT**. The 24 **LAN** ports can be effectively redefined by assigning them to portshield groups.
- SonicWALL TZ 170 family security appliances include one user definable interface, **OPT**.

Virtual Interfaces (VLAN)

On the SonicWALL PRO 2040, PRO 3060, PRO 4060, PRO 4100, and SonicWALL PRO 5060 security appliances, virtual Interfaces are sub-interfaces assigned to a physical interface. Virtual interfaces allow you to have more than one interface on one physical connection.

Virtual interfaces provide many of the same features as physical interfaces, including Zone assignment, DHCP Server, and NAT and Access Rule controls.

Virtual Local Area Networks (VLANs) can be described as a 'tag-based LAN multiplexing technology' because through the use of IP header tagging, VLANs can simulate multiple LAN's within a single physical LAN. Just as two physically distinct, disconnected LAN's are wholly separate from one another, so too are two different VLANs, however the two VLANs can exist on the very same wire. VLANs require VLAN aware networking devices to offer this kind of virtualization – switches, routers and firewalls that have the ability to recognize, process, remove and insert VLAN tags in accordance with the network's design and security policies.

VLANs are useful for a number of different reasons, most of which are predicated on the VLANs ability to provide logical rather than physical broadcast domain, or LAN boundaries. This works both to segment larger physical LAN's into smaller virtual LAN's, as well as to bring physically disparate LAN's together into a logically contiguous virtual LAN. The benefits of this include:

- Increased performance – Creating smaller, logically partitioned broadcast domains decreases overall network utilization, sending broadcasts only where they need to be sent, thus leaving more available bandwidth for application traffic.
- Decreased costs – Historically, broadcast segmentation was performed with routers, requiring additional hardware and configuration. With VLANs, the functional role of the router is reversed – rather than being used for the purposes of inhibiting communications, it is used to facilitate communications between separate VLANs as needed.
- Virtual workgroups – Workgroups are logical units that commonly share information, such as a Marketing department or an Engineering department. For reasons of efficiency, broadcast domain boundaries should be created such that they align with these functional workgroups, but that is not always possible: Engineering and Marketing users might be commingled, sharing the same floor (and the same workgroup switch) in a building, or just the opposite – the Engineering team might be spread across an entire campus. Attempting to solve this with complex feats of wiring can be expensive and impossible to maintain with constant adds and moves. VLANs allow for switches to be quickly reconfigured so that logical network alignment can remain consistent with workgroup requirements.
- Security – Hosts on one VLAN cannot communicate with hosts on another VLAN unless some networking device facilitates communication between them.

Sub-Interfaces

VLAN support on SonicOS Enhanced is achieved by means of sub-interfaces, which are logical interfaces nested beneath a physical interface. Every unique VLAN ID requires its own sub-interface. For reasons of security and control, SonicOS does not participate in any VLAN trunking protocols, but instead requires that each VLAN that is to be supported be configured and assigned appropriate security characteristics.



Note: *Dynamic VLAN Trunking protocols, such as VTP (VLAN Trunking Protocol) or GVRP (Generic VLAN Registration Protocol), should not be used on trunk links from other devices connected to the SonicWALL.*

Trunk links from VLAN capable switches are supported by declaring the relevant VLAN ID's as a sub-interface on the SonicWALL, and configuring them in much the same way that a physical interface would be configured. In other words, only those VLANs which are defined as sub-interfaces will be handled by the SonicWALL, the rest will be discarded as uninteresting. This method also allows the parent physical interface on the SonicWALL to which a trunk link is connected to operate as a conventional interface, providing support for any native (untagged) VLAN traffic that might also exist on the same link. Alternatively, the parent interface may remain in an 'unassigned' state.

VLAN sub-interfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN,

DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN sub-interfaces at this time are VPN policy binding, WAN dynamic client support, and multicast support. The PRO 2040 supports up to 100 sub-interfaces, the PRO 3060 and PRO 4060 support up to 200 sub-interfaces, and the PRO 4100 and PRO 5060 support up to 400 sub-interfaces.

Interface Settings							
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	10.0.93.49	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
X2	LAN	192.168.169.1	255.255.255.0	Static	No link	Second LAN	
X2/V10	Marketing LAN	10.100.10.1	255.255.255.0	Static	VLAN Sub-Interface	Marketing Subnet	
X3	DMZ	10.200.100.1	255.255.255.0	Static	No link	DMZ	
X3/V10	sonicwallDMZ	10.200.200.1	255.255.255.0	Static	VLAN Sub-Interface	DMZ Subnet	
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X4/V10	Engineering LAN	10.50.100.1	255.255.255.0	Static	VLAN Sub-Interface	Engineering Subnet	
X4/V20	Engineering LAN	10.50.150.1	255.255.255.0	Static	VLAN Sub-Interface	Engineering Subnet	
X4/V30	Engineering LAN	10.50.200.1	255.255.255.0	Static	VLAN Sub-Interface	Engineering Subnet	
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

SonicOS Enhanced Secure Objects

The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. This structure is based on secure objects, which are utilized by rules and policies within SonicOS Enhanced. Physical interface objects include the LAN1 through LAN5, WAN, OPT, Modem and WLAN ports. Address objects comprise a host, a network, a range of addresses, or a MAC address.



Note: The **LAN1** through **LAN5** ports on a TZ 170 series security appliance are managed as a single interface, and share the same IP address and, if you enable the internal DHCP Server, they share the same DHCP address range. Essentially, the five LAN ports are a five-port switch for the LAN interface.



Secured objects include interface objects that are directly linked to physical interfaces and managed in the **Network > Interfaces** page. Address objects are defined in the **Network > Address Objects** page. Service and Scheduling objects are defined in the **Firewall** section of the SonicWALL security appliance Management Interface, and User objects are defined in the **Users** section of the SonicWALL security appliance Management Interface.

Zones are the hierarchical apex of SonicOS Enhanced's secure objects architecture. SonicOS Enhanced includes pre-defined zones as well as allow you to define your own zones. Predefined zones include LAN, DMZ, WAN, WLAN, and Custom. Zones can include multiple interfaces, however, the WAN Zone is restricted to a total of two interfaces. Within the WAN zone, either one or both WAN interfaces can be actively passing traffic depending on the WAN Failover and Load-Balancing configuration on the **Network > WAN Failover & LB** page.



Cross Reference: For more information on WAN Failover and Load Balancing on the SonicWALL security appliance, see Chapter 10 Setting Up Network WAN Failover and Load Balancing.

At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

Transparent Mode

Transparent Mode in SonicOS Enhanced uses interfaces as the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing.

Interface Settings

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

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	10.0.93.56	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X4	WLAN	0.0.0.0	255.255.255.0	Static	No link		
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

- **Name** - listed as **F0, F1, X0** through **X9, LAN, WAN, WLAN, Modem**, or **OPT** depending on your SonicWALL security appliance model.
- **Zone** - LAN, DMZ/OPT, WAN, and WLAN are listed by default. As zones are configured, the names are listed in this column.
- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - the network mask assigned to the subnet.
- **IP Assignment** - you can select
 - ♦ **F0, X0, or LAN: Static or Transparent**
 - ♦ **F1, X1, or WAN: DHCP, Static, PPPoE, PPTP, or L2TP**
 - ♦ **X2 - X9, X1** (on PRO 5060 Fiber only), or **OPT**: The selection of IP assignment depends on the zone assigned to the user-defined port:
 - **LAN, DMZ**, or a custom zone of Trusted type: **Static or Transparent**
 - **WAN** or a custom zone of Untrusted type: **DHCP, Static, PPPoE, PPTP, or L2TP**
 - **WLAN** or a custom Wireless zone: static IP only (no IP Assignment list)
 - ♦ **Modem**: static or dynamic, set through the Dial-up Profile. See **Chapter 26, Configuring Dialup Profiles** for instructions on creating Dial-up Profiles.
 - ♦ **WLAN**: static IP only (no IP Assignment list)
- **Status** - the link status and speed.
- **Comment** - any user-defined comments.
- **Configure** - click the **Configure** icon to display the **Edit Interface** window, which allows you to configure the settings for the specified interface.



Alert: You cannot change the Zones in the Edit Interface window for the **X0, LAN, WAN, Modem**, and **WLAN** interfaces.

Interface Traffic Statistics

The **Interface Traffic Statistics** table lists received and transmitted information for all configured interfaces.

Traffic Statistics	X0	X1	X2	X3	X4	X5
Rx Unicast Packets:	0	3847	0	0	0	0
Rx Broadcast Packets:	0	120920	0	0	0	0
Rx Bytes:	0	19095193	0	0	0	0
Tx Unicast Packets:	0	4755	0	0	0	0
Tx Broadcast Packets:	0	19	0	0	0	0
Tx Bytes:	0	3722726	0	0	0	0

The following information is displayed for all SonicWALL security appliance interfaces:

- **Rx Unicast Packets** - indicates the number of point-to-point communications received by the interface.
- **Rx Broadcast Packets** - indicates the number of multipoint communications received by the interface.
- **RX Bytes** - indicates the volume of data, in bytes, received by the interface.
- **Tx Unicast Packets** - indicates the number of point-to-point communications transmitted by the interface.
- **Tx Broadcast Bytes** - indicates the number of mutlipoint communications received by the interface.
- **Tx Bytes** - indicates the volume of data, in bytes, transmitted by the interface.

To clear the current statistics, click the **Clear Statistics** button at the top right of the **Network > Interfaces** page.



Configuring the F0, F1, X0 - X9, LAN and OPT Interfaces (Static)

Static means you assign a fixed IP address to the interface.

- 1 Click on the **Configure** icon  in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.

You can configure **F0, F1, X0** through **X9, LAN**, or **OPT**.

If you select **OPT**, select **LAN, WAN, DMZ, WLAN**, a custom zone, or **Create new zone** for **Zone**.

If you want to create a new zone, select **Create new zone**. The **Add Zone** window is displayed. See **Chapter 14, Configuring Zones** for instructions on adding a zone.

- 2 Select a Zone to assign to the interface. You can select **LAN, WAN, DMZ, WLAN**, or a custom zone.
- 3 Select **Static** from the **IP Assignment** menu.
- 4 Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.



Note: You cannot enter an IP address that is in the same subnet as another zone.

- 5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- 6 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP, HTTPS, SSH, Ping**, and/or **SNMP**.
- 7 If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
- 8 Click **OK**.



Note: The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.



The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.



Alert: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.


Configuring Interfaces in Transparent Mode

Transparent Mode enables the SonicWALL security appliance to bridge the WAN subnet onto an internal interface. You can configure the following interfaces in Transparent Mode

- TZ family and PRO 1260: **Lan** and **Opt**
- PRO family, **X0, X2 - X9, F0**



Note: You cannot configure the **X1** or **WAN** interface in Transparent mode.

- 1 Click on the **Configure** icon  in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
- 2 Select an interface.
If you select a configurable interface, select **LAN** or **DMZ** for **Zone**.

If you want to create a new zone for the configurable interface, select **Create a new zone**. The **Add Zone** window is displayed. See **Chapter 14, Configuring Zones** for instructions on adding a zone.

- 3 Select **Transparent Mode** from the **IP Assignment** menu.



- 4 From the **Transparent Range** menu, select an address object that contains the range of IP addresses you want to have access through this interface. The address range must be within the WAN zone and must not include the WAN interface IP address. If you do not have an address object configured that meets your needs:
 - a In the **Transparent Range** menu, select **Create New Address Object**.
 - b In the **Add Address Object** window, enter a name for the address range.
 - a For **Zone Assignment**, select WAN
 - b For **Type**, select:
 - Host if you want only one network device to connect to this interface.
 - Range to specify a range of IP addresses by entering beginning and ending value of the range.
 - Network to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.
 - c Enter the IP address of the host, the beginning and ending address of the range, or the IP address and subnet mask of the network.
 - d Click **OK** to create the address object and return to the **Edit Interface** window.

- a For **Zone Assignment**, select WAN
- b For **Type**, select:
 - Host if you want only one network device to connect to this interface.
 - Range to specify a range of IP addresses by entering beginning and ending value of the range.
 - Network to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.

- a For **Zone Assignment**, select WAN

- b For **Type**, select:
 - Host if you want only one network device to connect to this interface.
 - Range to specify a range of IP addresses by entering beginning and ending value of the range.
 - Network to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.

- Host if you want only one network device to connect to this interface.

- Range to specify a range of IP addresses by entering beginning and ending value of the range.

- Network to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.

- c Enter the IP address of the host, the beginning and ending address of the range, or the IP address and subnet mask of the network.

- d Click **OK** to create the address object and return to the **Edit Interface** window.

See **Chapter 16, Configuring Address Objects** for more information.

- 5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

- 6 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **Ping**, and/or **SNMP**.

- 7 If you want to allow selected users with limited management rights to log directly into the security appliance through this interface, select **HTTP** and/or **HTTPS** in **User Login**.

- 8 Click **OK**.



Note: The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex ()
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.


Check **Enable Multicast Support** to allow multicast reception on this interface.



Alert: *If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.*

Configuring Wireless Interfaces

A Wireless interface is an interface that has been assigned to a Wireless zone and is used to support SonicWALL SonicPoint secure access points.

- 1 Click on the **Configure** icon  in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.

You can configure **X2** through **X9**, **Opt**, a VLAN sub-interface or a PortShield interface.

- 2 In the **Zone** list, select WLAN or a custom Wireless zone.
- 3 Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.



Note: *The upper limit of the subnet mask is determined by the number of SonicPoints you select in the SonicPoint Limit field. If you are configuring several interfaces or sub-interfaces as Wireless interfaces, you may want to use a smaller subnet (higher) to limit the number of potential DHCP leases available on the interface. Otherwise, if you use a class C subnet (subnet mask of 255.255.255.0) for each Wireless interface you may exceed the limit of DHCP leases available on the security appliance.*

- 4 In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface.

This value determines the highest subnet mask you can enter in the **Subnet Mask** field. The following table shows the subnet mask limit for each **SonicPoint Limit** selection and the number of DHCP leases available on the interface if you enter the maximum allowed subnet mask.

Available Client IPs assumes 1 IP for the SonicWALL gateway interface, in addition to the presence of the maximum number of SonicPoints allowed on this interface, each consuming an IP address.

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IPs	Available Client IPs
No SonicPoints	30bits – 255.255.255.252	2	2
2 SonicPoints	29bits – 255.255.255.248	6	3

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IPs	Available Client IPs
4 SonicPoints	29bits – 255.255.255.248	6	1
8 SonicPoints	28bits – 255.255.255.240	14	5
16 SonicPoints (PRO 4060, PRO 4100, and PRO 5060 only)	27bits – 255.255.255.224	30	13
32 SonicPoints (PRO 5060 only)	26bits – 255.255.255.192	62	29



Note: The above table depicts the maximum subnet mask sizes allowed. You can still use class-full subnetting (class A, class B, or class C) or any variable length subnet mask that you wish on WLAN interfaces. You are encouraged to use a smaller subnet mask (e.g. 24bit class C - 255.255.255.0 - 254 total usable IPs), thus allocating more IP addressing space to clients if you have the need to support larger numbers of wireless clients.

- 5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- 6 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **Ping**, and/or **SNMP**.
- 7 If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
- 8 Click **OK**.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.



The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex



Alert: *If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.*

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

Check **Enable 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see **Chapter 42, Managing Quality of Service**.

Configuring the WLAN Interface

The WLAN interface is only available on the TZ 170 Wireless and TZ 170 SP Wireless.

You can only configure the WLAN interface with a static IP address.

- 1 Click on the **Notepad** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
- 2 Select the **WLAN** interface. If you want to create a new zone for the interface, select **Create a new zone**. The **Add Zone** window is displayed. See Chapter 11 for instructions on adding a zone.
- 3 Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.
- 4 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- 5 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **Ping**, and/or **SNMP**.
- 6 If you want to allow selected users with limited management rights, select **HTTP** and/or **HTTPS** in **User Login**.
- 7 Click **OK**.



Note: *The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.*

Configuring Advanced Settings for the Interface

Check **Enable Multicast Support** to allow multicast reception on this interface.

Configuring a WAN Interface

Configuring the WAN interface enables Internet connect connectivity. You can configure up to two WAN interfaces on the SonicWALL security appliance.

- 1 Click on the **Notepad** icon in the **Configure** column for the **F1, WAN, X1** or **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
- 2 If you're configuring an Unassigned Interface, select **WAN** from the **Zone** menu. If you selected the **Default WAN** Interface, **WAN** is already selected in the **Zone** menu.



- 3 Select one of the following WAN Network Addressing Mode from the **IP Assignment** menu. Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.

Static - configures the SonicWALL for a network that uses static IP addresses.

DHCP - 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.

PPPoE - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If desktop software and a username and password is required by your ISP, select NAT with PPPoE. This protocol is typically found when using a DSL modem.

PPTP - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.

L2TP - uses IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.



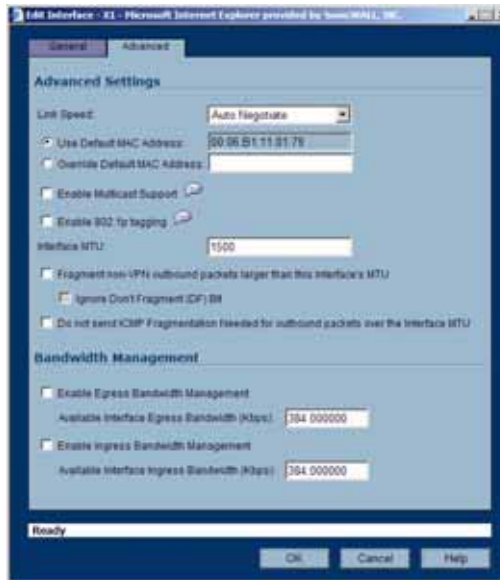
Note: For Windows clients, L2TP is supported by Windows 2000 and Windows XP. If you are running other versions of Windows, you must use PPTP as your tunneling protocol.

- 4 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTPS**, **Ping**, and/or **SNMP**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.
- 5 If you want to allow selected users with limited management rights to log directly into the security appliance from this interface, select **HTTP** and/or **HTTPS** in **User Login**.
- 6 Check **Add rule to enable redirect from HTTP to HTTPS**, if you want an HTTP connection automatically redirected to a secure HTTPS connection to the SonicWALL security appliance management interface.

7 After completing the WAN configuration for your Network Addressing Mode, click **OK**

Configuring the Advanced Settings for the WAN Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC Address, setting up bandwidth management, and creating a default NAT policy automatically.



Ethernet Settings

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.



Alert: *If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.*

Check **Enable Multicast Support** to allow multicast reception on this interface.

Check **Enable 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see **Chapter 42, Managing Quality of Service**.

You can also specify any of these additional **Ethernet Settings**:

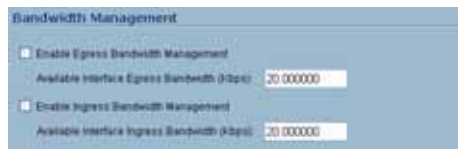
- **Interface MTU** - Specifies the largest packet size that the interface can forward without fragmenting the packet.
- **Fragment non-VPN outbound packets larger than this Interface's MTU** - Specifies all non-VPN outbound packets larger than this Interface's MTU be fragmented. Specifying the fragmenting of VPN outbound packets is set in the **VPN > Advanced** page.
- **Ignore Don't Fragment (DF) Bit** - Overrides DF bits in packets.
- **Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU** - blocks notification that this interface can receive fragmented packets.

Bandwidth Management

SonicOS Enhanced can apply bandwidth management to both egress (outbound) and ingress (inbound) traffic on the WAN interface. Outbound bandwidth management is done using Class Based Queuing. Inbound Bandwidth Management is done by implementing ACK delay algorithm that uses TCP's intrinsic behavior to control the traffic.

Class Based Queuing (CBQ) provides guaranteed and maximum bandwidth Quality of Service (QoS) for the SonicWALL security appliance. Every packet destined to the WAN interface is queued in the corresponding priority queue. The scheduler then dequeues the packets and transmits it on the link depending on the guaranteed bandwidth for the flow and the available link bandwidth.

Use the Bandwidth Management section of the **Edit Interface** screen to enable or disable the ingress and egress bandwidth management. Egress and Ingress available link bandwidth can be used to configure the upstream and downstream connection speeds.



The **Bandwidth Management** section allows you to specify the available outbound bandwidth for this interface in Kbps.

- **Enable Egress Bandwidth Management** - Enables outbound bandwidth management.
 - ♦ **Available Interface Egress Bandwidth (Kbps)** - Specifies the available bandwidth for this interface in Kbps.
- **Enable Ingress Bandwidth Management** - Enables inbound bandwidth management.
 - ♦ **Available Interface Ingress Bandwidth (Kbps)** - Specifies the available bandwidth for this interface in Kbps.

NAT Policy Settings

Selecting **Create default NAT Policy automatically** translates the Source Address of packets from the **Default LAN** (Primary LAN) to your new **WAN** Interface.



Cross Reference: For more information on NAT Policies, see *Chapter 15 Configuring Network NAT Policies*.

Configuring Modem Settings

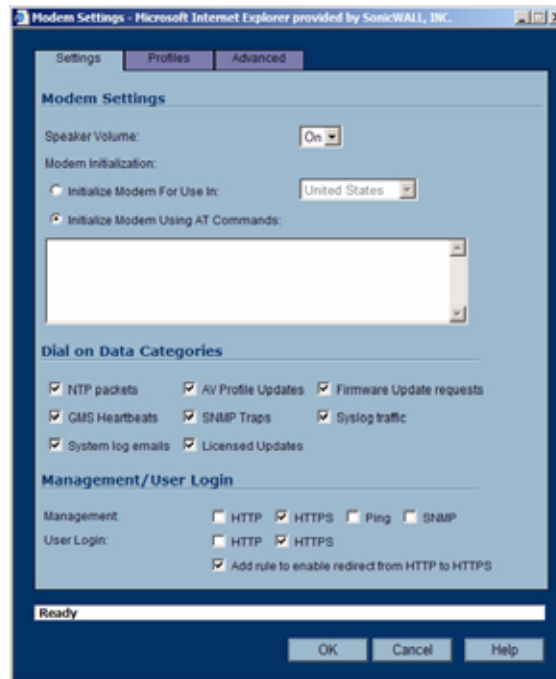
The SonicWALL TZ 170 SP and TZ 170 SP Wireless security appliances include a built-in modem. You can use the modem as your primary WAN connection, or as an automatic backup for your WAN.



Note: Before configuring the Modem interface, you must create at least one Dial-up Profile. See **Chapter 26, Configuring Dialup Profiles** for instructions on creating Dial-up Profiles.

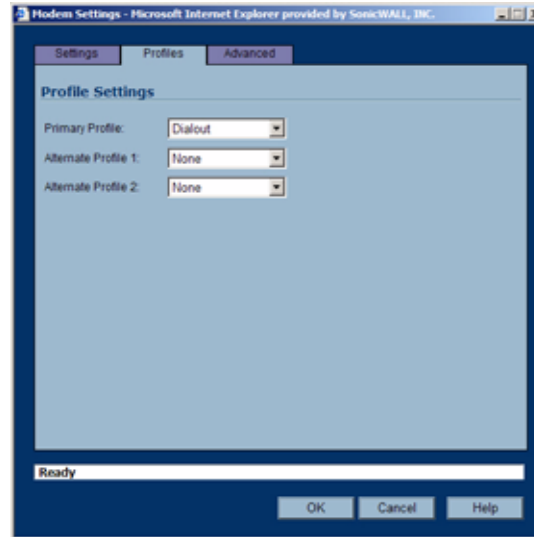
Set up the Modem Interface

- 1 Click on the edit  icon in the **Configure** column for the **Modem** interface.

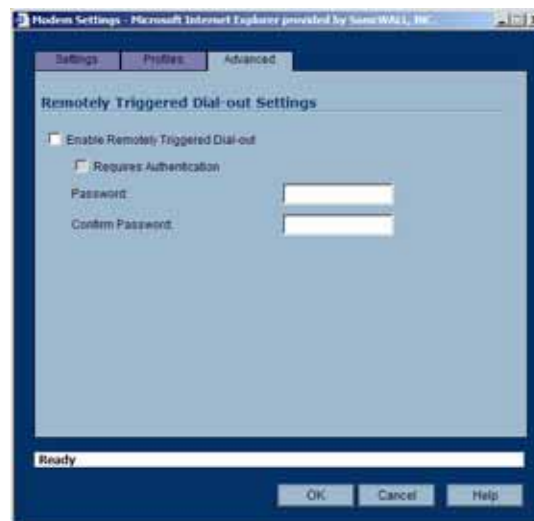


- 2 In the **Modem Settings** page, configure the following settings:
 - ♦ **Speaker Volume** - Select whether you want the modem's speaker turned on or off. The default value is **On**.
 - ♦ **Modem Initialization** - Select **Initialize Modem For Use In** and select the country from the drop-down menu. **United States** is selected by default. If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands (for modem initialization)** field. AT commands are instructions used to control a modem such as **ATS7=30** (allows up to 30 seconds to wait for a dial tone), **ATS8=2** (sets the amount of time the modem pauses when it encounters a comma (",") in the string).
- 3 Specify the **Dial on Data Categories** you want the SonicWALL security appliance modem to detect for outbound data before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWALL security appliance security applications. You can select from the following data categories:
 - ♦ **NTP packets**
 - ♦ **GMS Heartbeats**
 - ♦ **System log e-mails**
 - ♦ **AV Profile Updates**
 - ♦ **SNMP Traps**
 - ♦ **Licensed Updates**

- ◆ **Firmware Update requests**
 - ◆ **Syslog traffic**
- 4 Select any of the supported management protocol(s) for management of the SonicWALL security appliance from the **Modem** interface: **HTTPS**, **Ping**, and/or **SNMP**. Select **Add rule to enable redirect from HTTP to HTTPS** to allow the SonicWALL to automatically convert HTTP requests to HTTPS requests for added security.
 - 5 Click the **Profile** tab.



- 6 For **Primary Profile**, select a dialing profile. If you have an alternative profile, select the profile from the **Alternate Profile 1** menu. If the **Primary Profile** cannot establish a connection, the SonicWALL security appliance uses the **Alternate Profile 1** profile to access the modem and establish a connection. If you have an additional alternate profile, select it from the **Alternate Profile 2** menu.
- 7 Click the **Advanced** tab.



- 8 The Remotely Triggered Dial-out feature allows you to remotely manage the SonicWALL appliance via the WAN interface when the modem is the only WAN connection. When this feature is enabled, you can dial in to the modem's phone number remotely, and that will trigger the modem to dial out. Check **Enable Remotely Triggered Dial-out** to enable the modem to respond to remote management requests.

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- ◆ The dial profile is configured for **dial-on-data**.
 - ◆ The SonicWALL Security Appliance is configured to be managed using HTTPS, so that the device can be accessed remotely.
 - ◆ Enter a value in the **Enable Max Connection Time (minutes)** field. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.
- 9 If you want the remotely triggered dial-out to require a password, check **Requires Authentication**, enter the password into the **Password** field, and reenter the password in the **Confirm Password** field.
- 10 Click **OK**.

Connecting the Modem

If you need to use the modem as your primary WAN interface, you can connect it now: In the **Network > Interfaces** page click **Connect** on the same line as the Modem interface.

Configuring SonicWALL PortShield™ Interfaces (PRO 1260)

SonicWALL PortShield™ is a feature of the SonicWALL PRO 1260 security appliance running SonicOS Enhanced 3.1 or newer.

PortShield architecture enables you to configure any or all of the 24 LAN switch ports on the PRO 1260 into separate security zones, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each security zone has its own wire-speed switch ports that enjoy the protection of a dedicated, deep packet inspection firewall.

Adding a PortShield Interface

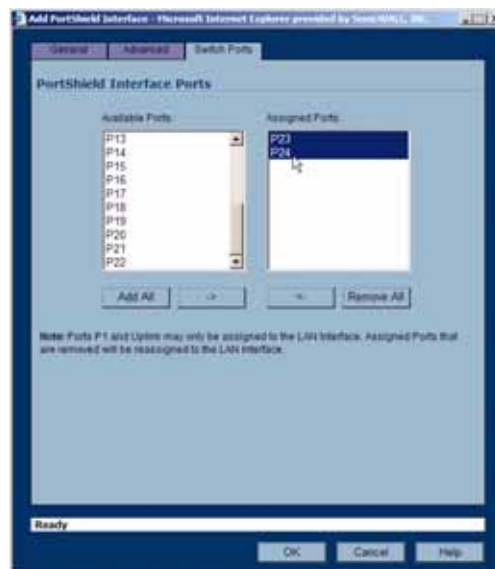
To add a PortShield interface:

- 1 In the **Network > Interfaces** page, click Add Interface.
- 2 Configure the Wireless_Access interface:
 - ◆ **Zone:** The zone assigned to this interface
 - ◆ **PortShield Interface Name:** The name of the interface
 - ◆ **IP Address:** An appropriate IP address that does not conflict with another address range.

- ◆ **Subnet Mask:** 255.255.255.0 is the default



- 3 In the **Switch Ports** tab, assign ports 23 and 24 to the Wireless_Access PortShield interface



Configuring VLAN Sub-Interfaces (PRO 2040, PRO 3060, PRO 4060, PRO 4100, PRO 5060)

When you add a VLAN sub-interface, you need to assign it to a Zone, assign it a VLAN Tag, and assign it to a physical interface. Based on your zone assignment, you configure the VLAN sub-interface the same way you configure a physical interface for the same zone.

Adding a virtual interface

- 1 In the left-navigation menu click on **Network** and then **Interfaces** to display the **Network > Interfaces** page.
- 2 At the bottom of the Interface Settings table, click Add Interface. The Edit Interface window displays.



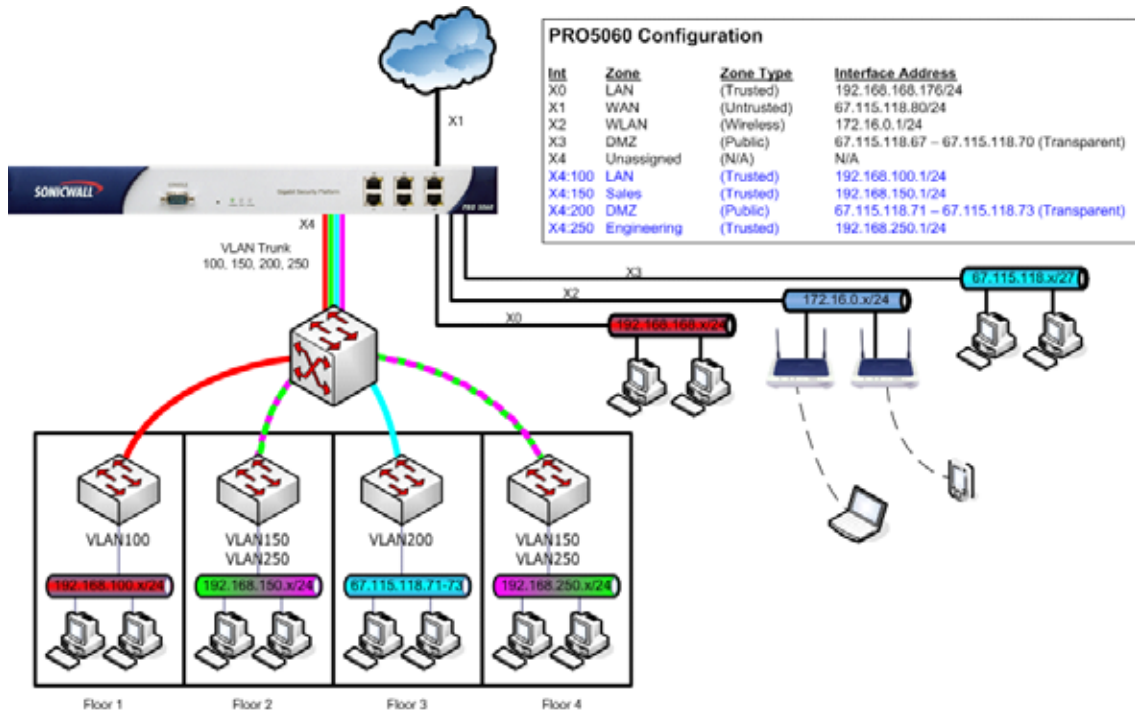
- 3 Select a Zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a custom zone. The zone assignment does not have to be the same as the parent (physical) interface. In fact, the parent interface can even remain **Unassigned**.

Your configuration choices for the network settings of the sub-interface depend on the zone you select.

- **LAN, DMZ**, or a custom zone of Trusted type: **Static** or **Transparent**
 - **WAN** or a custom zone of Untrusted type: static IP only (no IP Assignment list).
 - **WLAN** or a custom Wireless zone: static IP only (no IP Assignment list).
- 4 Assign a VLAN tag (ID) to the sub-interface. Valid VLAN ID's are 1 to 4095, although some switches reserve VLAN 1 for native VLAN designation. You will need to create a VLAN sub-interface with a corresponding VLAN ID for each VLAN you wish to secure with your security appliance.
 - 5 Declare the parent (physical) interface to which this sub-interface will belong. There is no per-interface limit to the number of sub-interfaces you can assign – you may assign sub-interfaces up to the system limit (100 for the PRO 2040, 300 for the PRO 3060 and PRO 4060, 400 for the PRO 4100 and PRO 5060).
 - 6 Configure the sub-interface network settings based on the zone you selected. See the interface configuration instructions earlier in this chapter:
 - ◆ **Configuring the F0, F1, X0 - X9, LAN and OPT Interfaces (Static)**
 - ◆ **Configuring Interfaces in Transparent Mode**
 - ◆ **Configuring the WLAN Interface**
 - ◆ **Configuring a WAN Interface**
 - ◆ **Configuring the Advanced Settings for the WAN Interface**
 - 7 Select the management and user-login methods for the sub-interface.
 - 8 Click **OK**.

Deploying VLANs

The following examples illustrate some typical deployments of a VLAN within a corporate network.



The above illustration depicts a sample VLAN implementation as might be employed by one location of a geographically redundant online retailer. The network has a PRO 5060 and a core switch located in the same server room. Also in the server room are dedicated management workstations and shared file servers connected to X0 (LAN Zone) of the PRO 5060. A small collection of publicly available FTP and mail servers are connected to X3 (DMZ) which is operating in transparent mode using a block of addresses from the WAN. Attached to X2 (WLAN) are a series of SonicPoints which have been located throughout the four floors of the building. On each of the four floors is a 48 port workgroup switch, connected back to the core switch with gigabit Ethernet links.

The switch on Floor 1 provides connectivity to the company's technical support and IT departments, and while most of their network communications occur within their broadcast domain, they require regular access to the rest of the network, particularly to the servers connected to X0. All 48 ports on the switch are assigned to VLAN 100.

Floors 2 and 4 contain mixed groups of users, primarily from the Sales and Engineering teams. Ports to which Engineering users are connected are assigned to VLAN 250, and ports to which Sales and other users are connected are assigned to VLAN 150. Each group has dedicated servers, with appropriate VLAN assignments, and both groups communicate regularly with the servers connected to X0.

Floor 3 houses the company's main public server farm, with dozens of load balanced web-servers. The load-balancers present three public facing IP addresses, and distribute the traffic among the real servers. The public facing interfaces of the load-balancers are connected to 6 ports on the switch, which have been assigned to VLAN 200. The remainder of the switch ports have been assigned to VLAN 210, and have connected to them the real servers and the internal interfaces of the load-balancers. The only network access to these servers is through the load-balancers.

The core switch is layer 3 capable, but rather than routing between the VLANs it trunks VLANs 100, 150, 200, and 250 to the PRO 5060 with a single gigabit connection to X4. Since most of the workgroups' traffic remains within the workgroup, the bandwidth capacity of this approach proves adequate, although if their utilization continues to grow, they can trunk VLAN 100 and 200 via one link to X4 and trunk VLAN 150 and 250 via a second link to X5, thus doubling their effective capacity.

DHCP Services can be enabled on all physical interfaces and all VLAN sub-interfaces, allowing clients to automatically obtain addressing:

#	Type	Lease Scope	Interface	Details	Enable	Configure
1	Dynamic	Range: 172.16.0.2 - 172.16.0.230	X2		<input checked="" type="checkbox"/>	
2	Dynamic	Range: 192.168.100.2 - 192.168.100.254	X4.V100		<input checked="" type="checkbox"/>	
3	Dynamic	Range: 192.168.150.2 - 192.168.150.254	X4.V150		<input checked="" type="checkbox"/>	
4	Dynamic	Range: 192.168.158.1 - 192.168.158.157	X0		<input checked="" type="checkbox"/>	
5	Dynamic	Range: 192.168.250.2 - 192.168.250.254	X4.V250		<input checked="" type="checkbox"/>	
6	Dynamic	Range: 67.115.118.67 - 67.115.118.70	X3		<input checked="" type="checkbox"/>	
7	Dynamic	Range: 67.115.118.71 - 67.115.118.73	X4.V200		<input checked="" type="checkbox"/>	

The screenshot below shows the SonicOS interface configuration required to support the above scenario (the + and - icons can be used to expand and collapse the interface trees):

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.176	255.255.255.0	Static	No link	Default LAN	
X1	WAN	67.115.118.80	255.255.255.224	Static	100 Mbps half-duplex	Default WAN	
X2	WLAN	172.16.0.1	255.255.255.0	Static	No link		
X3	DMZ	67.115.118.80	255.255.255.224	Transparent Mode	No link		
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	100 Mbps full-duplex		
X4.V100	LAN	192.168.100.1	255.255.255.0	Static	VLAN Sub-interface		
X4.V150	Sales	192.168.150.1	255.255.255.0	Static	VLAN Sub-interface		
X4.V200	DMZ	67.115.118.80	255.255.255.224	Transparent Mode	VLAN Sub-interface		
X4.V250	Engineering	192.168.250.1	255.255.255.0	Static	VLAN Sub-interface		
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

VLAN Integration

When a packet with a VLAN tag arrives on a physical interface, the VLAN ID is evaluated to determine if it is supported. The VLAN tag is stripped, and packet processing continues as it would for any other traffic. A simplified view of the inbound and outbound packet path includes the following potentially reiterative steps (refer to the SonicOS Enhanced State Diagram for a more complete reference):

- IP validation and reassembly
- Decapsulation (802.1q, PPP)
- Decryption
- Connection cache lookup and management
- Route policy lookup
- NAT Policy lookup
- Access Rule (policy) lookup
- Bandwidth management
- NAT translation
- Advanced Packet Handling (as applicable)
 - ◆ TCP validation
 - ◆ Management traffic handling
 - ◆ Content Filtering
 - ◆ Transformations and flow analysis: H.323, SIP, RTSP, ILS/LDAP, FTP, Oracle, NetBIOS, Real Audio, TFTP
 - ◆ IPS and GAV

At this point, if the packet has been validated as acceptable traffic, it is forwarded to its destination. The packet egress path includes:

- Encryption
- Encapsulation
- IP fragmentation

On egress, if the route policy lookup determines that the gateway interface is a VLAN sub-interface, the packet is tagged (encapsulated) with the appropriate VLAN ID header. The creation of VLAN sub-interfaces automatically updates the SonicWALL's routing policy table:

Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
24.0.0.0	24.0.0.0	Any	0.0.0.0	24.0.0.0	20	1		
24.0.0.0	0.0.0.0	Any	0.0.0.0	X0	20	2		
Any	255.255.255.0	Any	0.0.0.0	X0	20	3		
Any	Default Gateway	Any	0.0.0.0	X0	20	4		
Any	conf1.0/24	Any	0.0.0.0	24.0.0.0	20	5		
Any	conf7.0/24	Any	0.0.0.0	X3	20	5		
Any	WAN Primary Subnet	Any	0.0.0.0	X0	20	7		
Any	LAN Primary Subnet	Any	0.0.0.0	X0	20	9		
Any	X2 Subnet	Any	0.0.0.0	X2	20	9		
Any	24.0.0.0 Subnet	Any	0.0.0.0	24.0.0.0	20	10		
Any	24.0.0.0 Subnet	Any	0.0.0.0	24.0.0.0	20	11		
Any	24.0.0.0 Subnet	Any	0.0.0.0	24.0.0.0	20	12		
Any	WAN Primary Subnet	Any	Default Gateway	X0	20	13		
Any	0.0.0.0/0	Any	10.50.165.1	X0	20	14		

The auto-creation of NAT policies, Access Rules with regard to VLAN sub-interfaces behave exactly the same as with physical interfaces. Customization of the rules and policies that govern the traffic between VLANs can be performed with customary SonicOS ease and efficiency.

When creating a zone (either as part of general administration, or as a step in creating a sub-interface), a checkbox will be presented on the Zone creation page to control the auto-creation of a GroupVPN for that zone. By default, only newly created Wireless type zones will have 'Create GroupVPN for this Zone' enabled, although the option can be enabled for other Zone types by selecting the checkbox during creation.

General

General Settings

Name: Sales

Security Type: Trusted

Allow Interface Trust

Enforce Content Filtering Service

Enforce Network Anti-Virus Service

Enable Gateway Anti-Virus Service

Enable IPS

Enforce Global Security Clients

Create GroupVPN for this Zone

Ready

OK Cancel

Management of security services between VLAN sub-interfaces is accomplished at the Zone level. All security services are configurable and applicable to zones comprising physical interfaces, VLAN sub-interfaces, or combinations of physical and VLAN sub-interfaces.

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	IPS	GSC	Configure
LAN	Trusted	X0, X4:V100	✓	✓		✓	✓		
WAN	Untrusted	X1				✓	✓		
DMZ	Public	X3, X4:V200	✓	✓					
VPN	Encrypted	N/A							
MULTICAST	Untrusted	N/A							
VLAN	Wireless	X2							
Sales	Trusted	X4:V150	✓			✓	✓		
Engineering	Trusted	X4:V250	✓			✓	✓		

Gateway Anti-Virus and Intrusion Prevention Services between the different workgroups can easily be employed with the use of VLAN segmentation, obviating the need for dedicated physical interfaces for each protected segment:

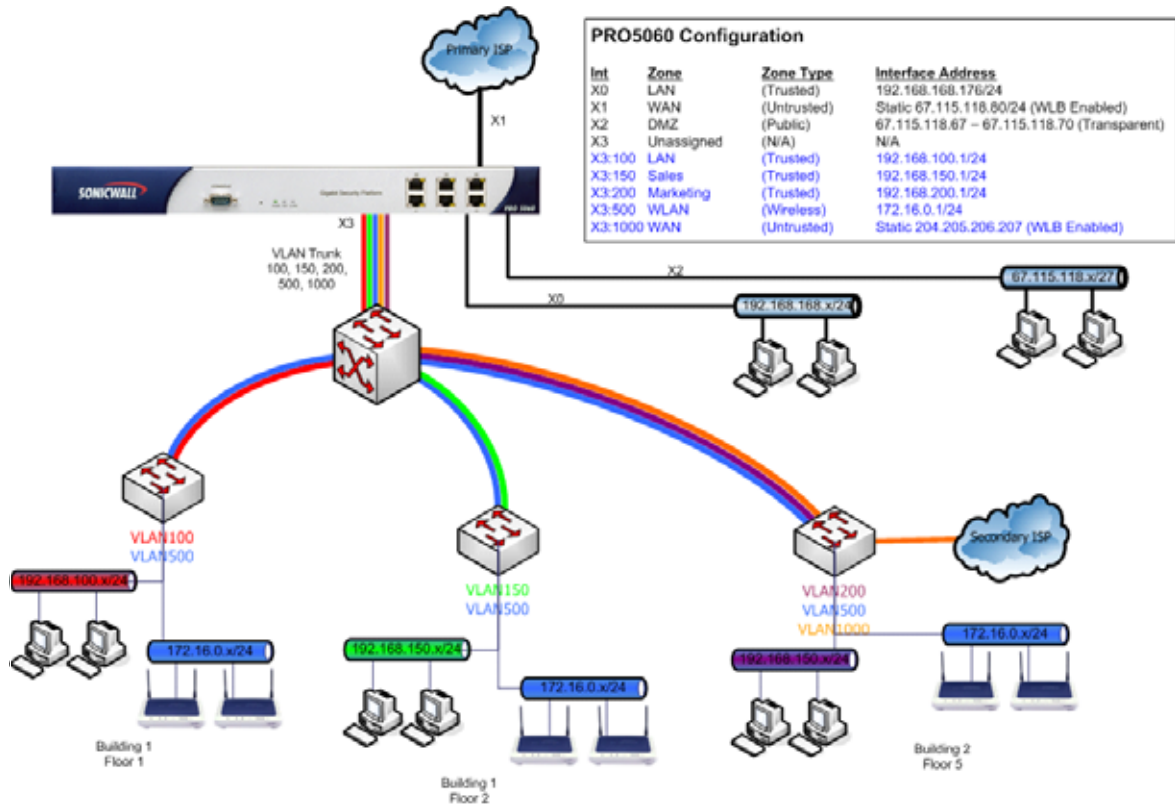
Gateway AV protection between X4:V100 (LAN) and X0 (LAN) with host name resolution:

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	10/08/2004 11:07:17.112	Alert	Security Services	Gateway Anti-Virus Alert: Yankee.6 disabled	192.168.168.10, 80, X0, LAPMOOSE	192.168.100.239, 1349, X0, MOOSE		

IPS Detection between X4:V150 (Sales) and X0 (LAN) with host name resolution:

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	10/08/2004 11:13:22.160	Alert	Intrusion Prevention	IPS Detection Alert ICMP Echo Reply, SID: 316, Priority: Low	192.168.168.10, 8, LAPMOOSE	192.168.150.241, 512, MOOSE		

VLAN support enables organizations to offer meaningful internal security (as opposed to simple packet filtering) between various workgroups, and between workgroups and server farms without having to use dedicated physical interfaces on the SonicWALL. The robust VLAN support of SonicOS Enhanced allows for extremely flexible configurations, such as:



Here the ability to assign VLAN sub-interfaces to the WAN Zone, and to use the WAN client mode (only Static addressing is supported on VLAN sub-interfaces assigned to the WAN Zone) is illustrated, along with the ability to support WAN Load-balancing and failover. Also demonstrated is the distribution of SonicPoints throughout the network by means of connecting them to access mode VLAN ports on workgroup switches. These switches are then backhauled to the core switch, which then connects all the VLANs to the PRO 5060 via a trunk link.

Configuring PortShield Interfaces

SonicWALL PortShield™ Interfaces

SonicWALL PortShield™ is a feature of the SonicWALL PRO 1260 security appliance running SonicOS Enhanced 3.1 or newer.

PortShield architecture enables you to configure some or all of the 24 LAN switch ports on the PRO 1260 into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed switch ports that enjoy the protection of a dedicated, deep packet inspection firewall.



Note: *Port 1 and the Uplink port are the only ports from which you can establish a SonicOS management session with the device.*

You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface. For example, if you assign ports 4 through 12 to a PortShield interface, ports 1 through 3, ports 13 through 24, and the uplink port are all assigned to the LAN interface.



Note: *Port 1 and the Uplink port can not be assigned to a PortShield interface. They can only be LAN interface. The OPT and WAN ports can not be assigned to a PortShield interface.*

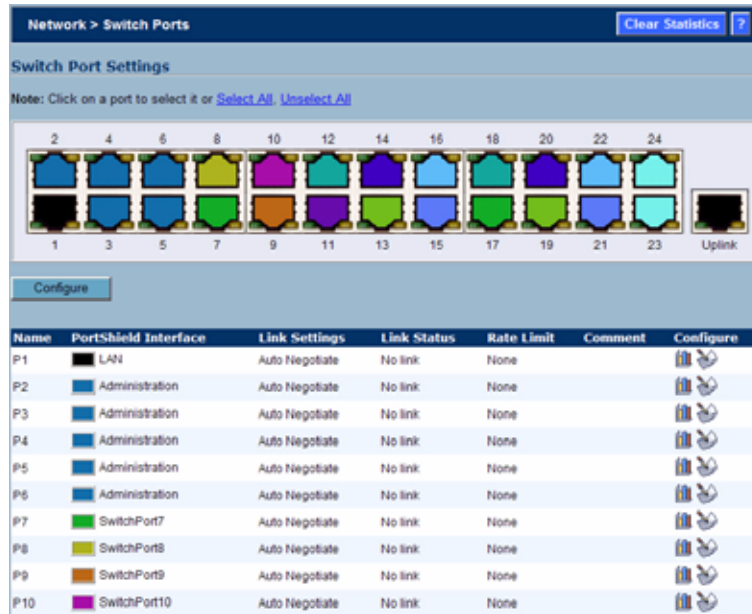
Security Services with PortShield

When you enable SonicWALL Security Services, such as Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS), the services inspect traffic between different PortShield interfaces and not traffic between ports within the same PortShield interface.

For example: If ports 2 and 3 are assigned to the SwitchPort1 interface and ports 4 and 5 are assigned to the SwitchPort2 interface, traffic between port 2 and port 3 will not be inspected by Security Services. Traffic between port 2 and port 4 will be inspected.

Network > SwitchPorts

The Network > SwitchPorts page allows you to manage the assignments of ports to PortShield interfaces.



The screenshot shows the 'Network > Switch Ports' configuration page. At the top, there's a 'Clear Statistics' button and a help icon. Below that is the 'Switch Port Settings' section with a note: 'Click on a port to select it or [Select All](#) [Unselect All](#)'. A grid of 24 ports is displayed, with ports 1-23 numbered and an 'Uplink' port. A 'Configure' button is below the grid. Below the grid is a table with the following data:

Name	PortShield Interface	Link Settings	Link Status	Rate Limit	Comment	Configure
P1	LAN	Auto Negotiate	No link	None		
P2	Administration	Auto Negotiate	No link	None		
P3	Administration	Auto Negotiate	No link	None		
P4	Administration	Auto Negotiate	No link	None		
P5	Administration	Auto Negotiate	No link	None		
P6	Administration	Auto Negotiate	No link	None		
P7	SwitchPort7	Auto Negotiate	No link	None		
P8	SwitchPort8	Auto Negotiate	No link	None		
P9	SwitchPort9	Auto Negotiate	No link	None		
P10	SwitchPort10	Auto Negotiate	No link	None		

Overview

A PortShield interface is a virtual interface with a set of ports assigned to it. There are two IP assignment methods you can deploy to create PortShield interfaces. They are Static and Transparent modes. The following two sections describe each.

Working in Static Mode

When you create a PortShield interface in Static Mode, you manually create an explicit address to be applied to the PortShield interface. All ports mapped to the interface are identified by this address. Static mode is available on interfaces assigned to Trusted, Public, or Wireless zones.



Note: When you create a PortShield interface in Static Mode, make sure the IP address you assign to the interface is not already in use by another PortShield interface.

Working in Transparent Mode

Transparent Mode addressing allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.



Note: Make sure the IP address you assign to the PortShield interface is within the WAN subnetwork.

When you create a PortShield interface in Transparent Mode, you create a range of addresses to be applied to the PortShield interface. You include these addresses in one entity called an Address Object. Address Objects allow for entities to be defined one time and to be re-used in multiple referential instances throughout the SonicOS interface. When you create a PortShield interface using an address object, all ports mapped to the interface are identified by any of the addresses specified in the address range.



Note: Each statically addressed PortShield interface must be on a unique subnet. You can not overlap PortShield interfaces across multiple subnetworks.

Using Different Approaches to Configuration

Note there are four ways to approach configuration of PortShield interface. They are:

- By going into the Interfaces environment and clicking the Add PortShield Interface button.
- By going into the Switch Ports environment and clicking on port icons in an interactive graphic of the SonicWALL PRO 1260 switch.
- By going into the Switch Ports environment and clicking on the pen and paper icon in the Configure column of the switch ports list.
- By using the PortShield interface wizard and clicking on options presented in the wizard screens.

To create a PortShield interface using the first method, you perform the following tasks:

- 1 Access the SonicWALL PRO 1260 device.
- 2 Create and add a PortShield interface to the list of interfaces. The PortShield interface is a virtual interface that you are adding to segment and control traffic for the 25-port managed SonicWALL PRO 1260 switch. After you select a zone, you select a series of ports that you want to assign to the PortShield interface.
- 3 Go to the Switch Port environment and perform either per-port or multiple-port extra configuration.

To create a PortShield interface using the second and third methods, you perform the following tasks:

- 1 Access the SonicWALL PRO 1260 device.
- 2 Create and add a PortShield interface to the list of interfaces.
- 3 Go to the Switch Port environment and assign ports to the PortShield interface you have already created.
 - ♦ For the second method, you select ports from the device graphic.
 - ♦ For third method, you click on the pen and paper icon and select ports from the same dialog boxes you work in the Interface environment.
- 4 Perform per-port or multiple-port extra configuration.

To create a PortShield interface using the fourth method, you perform the following tasks:

- 1 Access the SonicWALL PRO 1260 device.
- 2 From the Wizards environment go to the PortShield interface wizard.
- 3 Navigate through the wizard screens, selecting and verifying one of the options presented for switch partitioning which divides the ports up into various amounts.
- 4 Creating and Adding a PortShield Interface

Creating a PortShield Interface from the Interfaces Area

Before creating and adding a PortShield interface, think about why you are creating it and what role it will play in your network. To create and add a PortShield interface to the list of interfaces, perform the following steps:

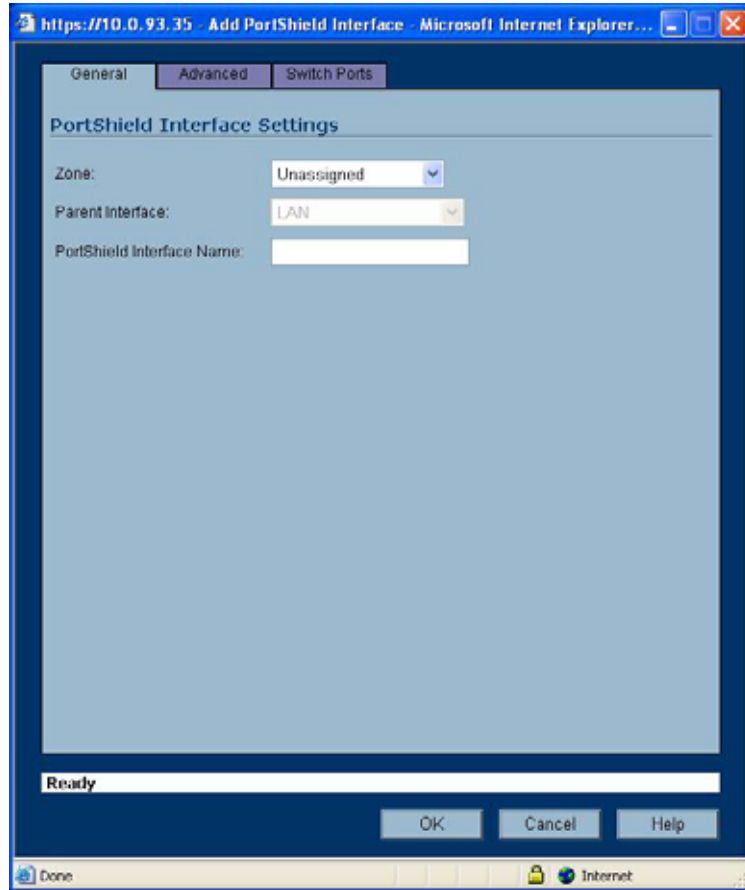
- 1 Log into the switch.
- 2 Click on the Interfaces option. The management software displays the Interfaces Settings screen.

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment
LAN	LAN	192.168.168.168	255.255.255.0	Static	100 Mbps full-duplex	Default LAN
My 2nd LAN	LAN	10.1.1.1	255.255.255.0	Static	Switch PortShield Interface	
Sales Group	LAN	10.1.2.1	255.255.255.0	Static	Switch PortShield Interface	
WLAN Group	WLAN	1.2.3.4	255.255.255.0	Static	Switch PortShield Interface	
silly goose	WLAN	5.5.5.5	255.255.255.0	Static	Switch PortShield Interface	
bob_test_interface	LAN	1.1.1.100	255.255.255.0	Static	Switch PortShield Interface	
Sales	Sales	172.16.1.1	255.255.255.0	Static	Switch PortShield Interface	Sales Port
test_interface_1	LAN	10.10.10.200	255.255.255.0	Static	Switch PortShield Interface	
bob_test_interface_0	LAN	10.10.20.200	255.255.255.0	Static	Switch PortShield Interface	
WAN	WAN	10.0.93.35	255.255.0.0	Static	100 Mbps half-duplex	Default WAN
OPT	Unassigned	0.0.0.0	0.0.0.0	N/A	No link	

- 3 Note the interfaces in the list contain the following columns of information:

Column	Description
Name	A string that identifies the interface.
Zone	The zone to which the interface maps.
IP Address	The IP address assigned to the interface.
Subnet Mask	The subnetwork mask value assigned to the IP address to indicate a range of addresses.
IP Assignment	The method in which the interface obtains its IP address: Static. Manually creating an explicit address to which you will map ports. Transparent. Allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address will be the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.
Status	Aggregate Ethernet Link port(s) status or Ethernet Link port(s) status summary, indicating the currently active highest speed and duplex properties.
Comment	A note about the interface.
Configure	Contains two icons. One icon is a grouping of books that displays traffic statistics when you hover the mouse cursor over it. The other icon is a pen and paper that enables you to launch an interface configuration session.

- 4 Click the Add PortShield interface Settings button. The management software displays the Add Port Shield dialog box.



- 5 Click the Zone list box and click on a zone type option to which you want to map the interface. Default zones are:

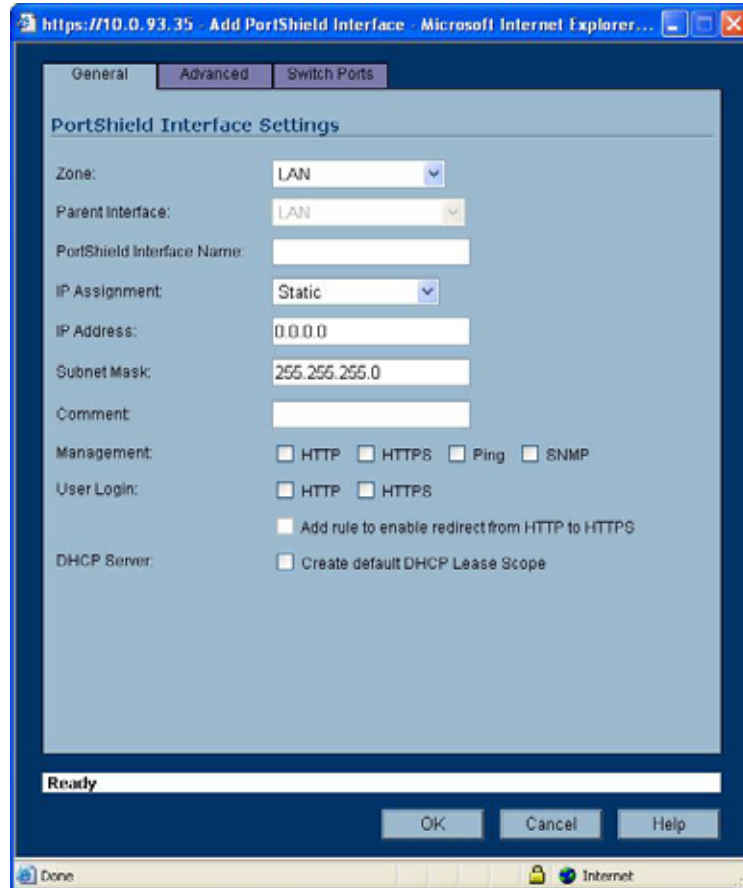
- ◆ LAN
- ◆ DMZ
- ◆ WLAN
- ◆ Unassigned

If you want to create another zone, go to the section [Creating a New Zone for the PortShield Interface](#).



Note: You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

- 6 After you select a zone option, the management software displays a more expanded version of the PortShield Interface Settings dialog box.

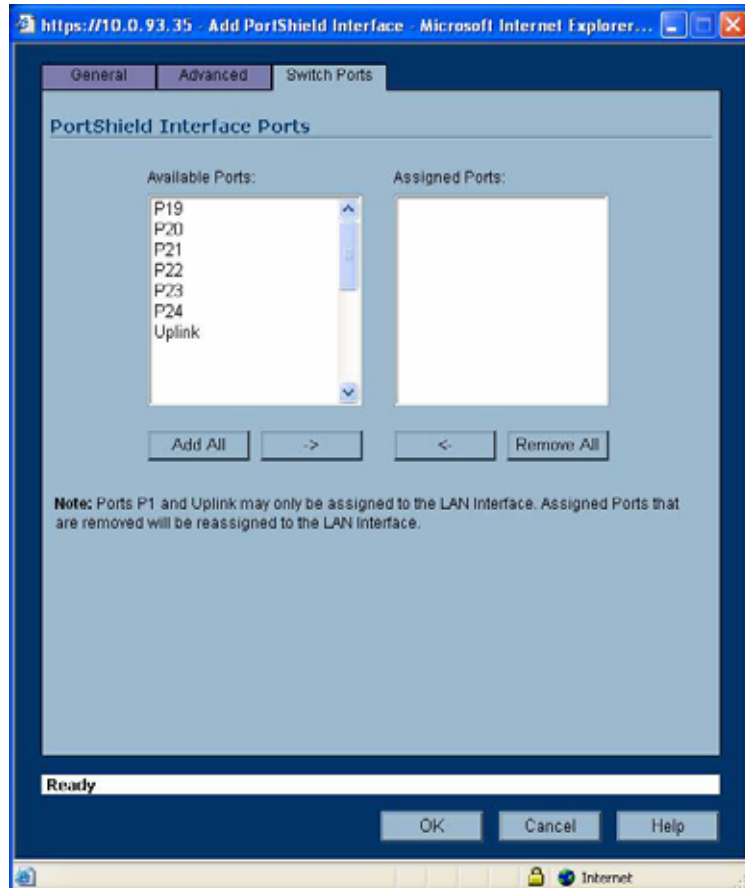


- 7 Type a string in the PortShield Interface Name field.
- 8 Click on the IP Assignment list box and click on either Static or Transparent. Static indicates the interface obtains its IP address manually. Transparent mode allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address will be the same as the WAN interface IP address.
- 9 Type an available IP address in the IP Address field.
- 10 If you want to specify a range of IP addresses different than the one allowed by the subnetwork mask 255.255.255.0 (Class C network), type in the desired subnetwork mask value in the Subnet Mask field.
- 11 Click on a checkbox in the Management area to indicate the desired management protocol type. The options are:
 - ◆ HTTP
 - ◆ HTTPS
 - ◆ Ping
 - ◆ SNMP
- 12 Click on a checkbox in the User Login area. This is a special feature that enables you to set up a Web access environment so you can enforce User Level Authentication. For more detail, see **Chapter 12, Configuring PortShield Interfaces**.
- 13 Click on the Create Default DHCP Lease Scope in the DHCP Server field to indicate that the amount of time allowed for an IP address issued by DHCP will be the default.



Note: This option only appears when creating a PortShield interface, not when editing an existing PortShield interface. You can make changes to the interface's DHCP settings after creating an interface from the DHCP Server environment (Network>DHCP Server).

- 14 Click on the Switch Ports tab. The management software displays the PortShield Interface dialog box.

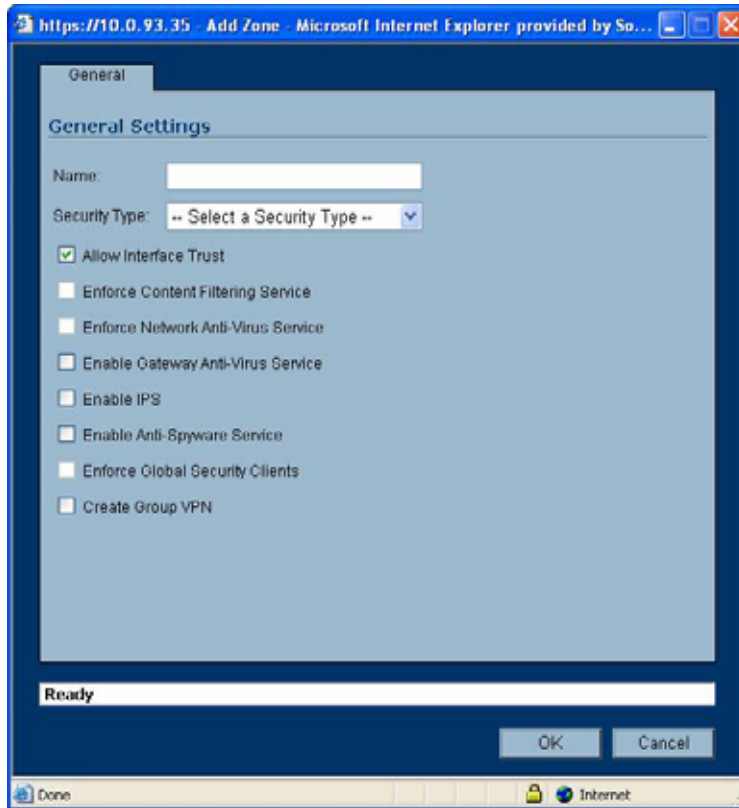


- 15 In the Available Ports list, click on the port numbers you want to assign to the PortShield interface and click on the right arrow (->) button to move them into the Assigned Ports list.
- 16 Click Ok. The management software adds the PortShield interface to the interface list.

Creating a New Zone for the PortShield Interface

You may want to create a zone for a PortShield interface that has different attributes to it than any of the default zones provide. To create a new zone for a PortShield interface, perform the following:

- 1 Click on the Zone list box and click on the Create new zone option. The management software displays the General Settings dialog box.



- 2 Type a string in the Name field that will identify the new zone.
- 3 Click on the Security Type list box and click on a security type option that will classify the zone as having a certain level of access. The choices are:
 - ♦ **Trusted.** This security type offers the highest level of security, indicating that only trust, indicating that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the device. The LAN zone is always Trusted.
 - ♦ **Public.** This security type offers a higher level of security than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the device and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN.
 - ♦ **Wireless.** This security type applies to the WLAN zone or any zone where the only interface to the network consists of SonicWALL SonicPoint devices. You typical use WiFiSec to secure traffic in a wireless zone.
- 4 After selecting the security level for the PortShield interface, click on one of the checkboxes that enables a security service for the zone. The following table details:

Checkbox	Description
Allow Interface Trust	Automates the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance.
Enforce Content Filtering Service	Enforces protection and productivity policies for organizations to reduce legal and privacy risks while minimizing administration overhead.
Enforce Network Anti-Virus Service	Enables network-level inspection of email, Web traffic, file transfers, various stream-based protocols, instant messaging, and peer-to-peer applications to detect and clean malicious code, viruses, and worms.

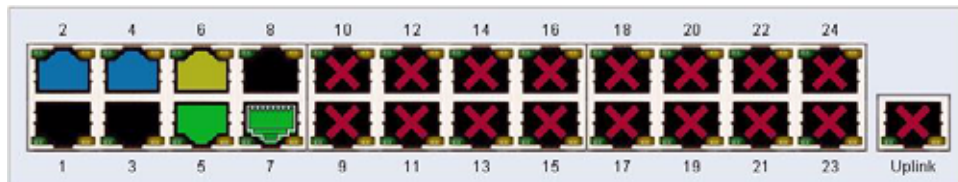
Checkbox	Description
Enable Gateway Anti-Virus Service	Enables gateway-level inspection of email, Web traffic, file transfers, various stream-based protocols, instant messaging, and peer-to-peer applications to detect and clean malicious code, viruses, and worms.
Enable IPS	Enables Intrusion Prevention Service which provides a configurable, high-performance deep packet inspection architecture using parallel searching algorithms through the application layer to deliver complete Web and E-Mail attack prevention.
Enable Anti-Spyware Service	Enables spyware protection which prevents malicious spyware from infecting networks by blocking related installations at the gateway and disrupting background communications from existing spyware programs.
Enforce Global Security Clients	Enables the application of the SonicWALL Global Security Client that delivers comprehensive desktop security for remote/mobile workers and corporate networks.
Create Group VPNs	Enables group VPN creation.

5 Click Ok.

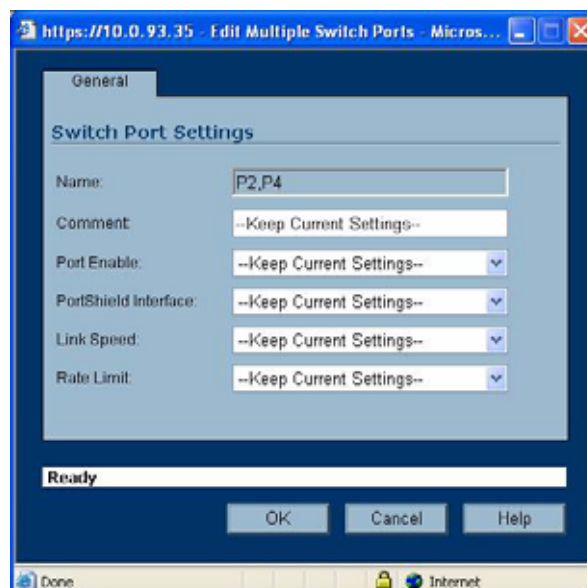
Refining the PortShield Interface

You can refine a PortShield interface group in the Switch Ports environment. To refine a PortShield interface group, perform the following steps:

- 1 Log in to the device.
- 2 Click on the Switch Ports option. The management software displays two major items:
 - ♦ a list of all interfaces including PortShield interfaces. Note the ports you have selected are parts of the PortShield interface you just created.
 - ♦ an interactive graphic of the ports on the switch



- 3 If there are more ports you want to add to the PortShield interface, in the interactive switch ports graphic, click on the ports you want to include in the PortShield interface group.
- 4 Click the Configure button. The management software displays the Edit Multiple Switch Ports dialog box. You can refine your settings in this dialog box.



- 5 Note that the name of the PortShield interface group will be assigned by default.
- 6 Click on the Port Enable list box and click on either the Enable or Disable option to either activate or deactivate the interfaces in the PortShield interface group.
- 7 Click on the PortShield interface list box and click on the PortShield interface you created in the previous procedure.
- 8 Click on the Link Speed list box and click on a throughput speed you want to assign the interface. The choices are:
 - ◆ Auto negotiate
 - ◆ 100Mbps Full Duplex
 - ◆ 100 Mbps Half Duplex
 - ◆ 10 Mbps Full Duplex
 - ◆ 10 Mbps Half Duplex



Note: Do not change this setting from the default of Auto negotiate unless your system requires you to do so. Also, note that for any setting involving the Full Duplex feature to work properly, be sure to configure Full Duplex on both ends of the link. By not having Full Duplex configured on both ends, a duplex mismatch occurs, causing throughput loss.

- 9 Click on the Rate Limit option and click on a value. The rate limit value enables you to throttle traffic coming into the switch. Remember, these values apply to inbound traffic only. The rate limit choices are:
 - ◆ 64 Kbps
 - ◆ 128 Kbps
 - ◆ 256 Kbps
 - ◆ 512 Kbps
 - ◆ 1 Mbps
 - ◆ 4 Mbps
 - ◆ 10 Mbps
 - ◆ 20 Mbps
- 10 Click Ok. Wait for a few seconds. The system then will incorporate the changes you made to the PortShield interface Group and add it back to the switch ports list.

Creating Transparent Mode PortShield Interfaces

You may find it useful to create address objects to bundle addresses into address objects and reference these objects when creating a PortShield interface. Address objects allow for entities to be defined one time and to be reused in multiple referential instances throughout SonicOS. The PortShield interface creation environment provides a convenient way to reference address objects.

The following example takes a network with a series of addresses in the range 67.115.118.80/24 and divides it into three PortShield Interfaces, mapping each to the following ports and address objects:

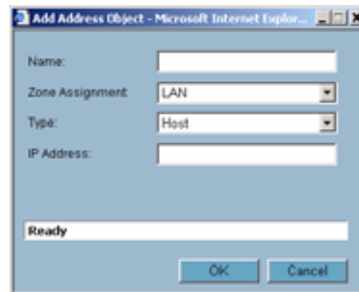
PortShield Interface	Port Numbers Mapped	Address Object Type	Address(es)
portshield1	5	Address Object Host	67.115.118.90/32
portshield2	12, 13, 14	Address Object Range	67.115.118.100-67.115.118.102
portshield3	16, 20	Address Object Host Group	67.115.118.200, 67.115.118.210, 67.115.118.212, 67.115.118.220, 67,115,118,230

To create these PortShield interfaces, using the prescribed address objects, perform the following steps:

- 1 Log in to the device.
- 2 Click on the Networks->Interfaces option. The management software displays the Interfaces Settings screen.
- 3 Click the Add PortShield Interface button. The management software displays the Add Port Shield dialog box.
- 4 Click the Zone list box and click on a zone type option to which you want to map the interface. For this exercise, click the LAN option. After you select a zone option, the management software displays a more expanded version of the PortShield Interface Settings dialog box. Only interfaces assigned to Trusted and Public zones can operate in Transparent mode.
- 5 Type a string in the PortShield Interface Name field.
- 6 Click on the IP Assignment list box and click the Transparent Mode option.



- 7 Click on the Transparent Range list box and click on the Create new address object option. The management software displays the Add Address Object dialog box.



- 8 Fill out the fields as detailed in the next three sections to create the three different types of address objects. The three scenarios presuppose you are in the 67.115.118.0 subnetwork.

Creating a Transparent Mode PortShield Interface with a Host Address Object

To assign the Host Address Object 67.115.118.90 to portshield1, perform the following steps:

- 1 Type the string portshield1 in the Name field to identify the address object.
- 2 Click the Zone Assignment list box and click the LAN option.
- 3 Click the Type list box and click the Host option to make the address object apply to a single IP address. Note the Host option is the default option in the list box.
- 4 Type 67.115.118.90 in the IP Address field. The management software presupposes a subnetwork mask of 255.255.255.255 (67.115.118.90/32). Note that because of this assumption, the software does not display a field for a subnetwork mask. Also, the field does not allow you to type enough a /32 notation as part of the address.
- 5 Click Ok. The management software displays the General tab of the Port Shield dialog box.
- 6 Click the Switch Ports tab. The management software displays the Switch Ports tab.
- 7 Click on P5 in the Available Ports list and click the right arrow (->) button to move the port into the Assigned Ports list.
- 8 Click Ok. The management software displays the Interfaces list displaying the new PortShield interface in the list. Note it displays the name, zone, IP address, subnetwork mask, IP assignment method, status, and comment, and link type status information about the address object you created (portshield1).



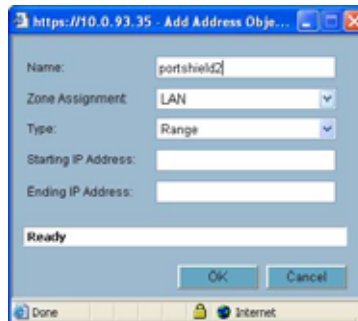
Note: Note that the IP address is the actual subnetwork address, not the specific address you entered. In this example, the address is 67.115.118.0 and not 67.115.118.90. This is because in Transparent mode, the interface appears to users as having the same address as the gateway. Therefore your explicit address is invisible or transparent to internet users. It lets you keep assigned IP addresses in the WAN subnet while protecting those hosts with full SonicWALL firewall protection (including services, etc.).

- 9 Click on the Switch Ports option in the left navigation pane.
- 10 In the graphic of the switch, view port number 5 and verify that the port is colored blue.
- 11 In the switch port list, view the PortShield Interface column for P5 (port 5) and verify that the interface listed is portshield1.
- 12 Refine the configuration of the PortShield Interface. For details, go to the section, [Refining the PortShield Interface](#).

Creating a PortShield Using an Address Object Containing an Address Range

To assign a Range Address Object with addresses extending from 67.115.118.100 to 67.115.118.102 to portshield2, perform the following steps:

- 1 Type the string portshield2 in the Name field to identify the address object.
- 2 Click the Zone Assignment list box and click the LAN option.
- 3 Click the Type list box and click the Range option to make the address object apply to a range of addresses. The management software displays new fields in the Add Address Object dialog box.



- 4 Note the Starting IP Address and Ending IP Address fields in the dialog box.
- 5 Type 67.115.118.100 in the Starting IP Address field to establish this address as the minimum value in the range.
- 6 Type 67.115.118.102 in the Ending IP Address field to establish this address as the maximum value in the range.
- 7 Click Ok. The management software displays the General tab of the Port Shield dialog box.
- 8 Click the Switch Ports tab. The management software displays the Switch Ports tab.
- 9 Holding down the shift key, click on P12, P13, and P14, in the Available Ports list and click the right arrow (->) button to move the port into the Assigned Ports list.
- 10 Click Ok. Note it displays the name, zone, IP address, subnetwork mask, IP assignment method, status, comment, and link type status detail about the address object you created (portshield2).
- 11 Click on the Switch Ports option in the left navigation pane.
- 12 In the graphic of the switch, view port numbers 12, 13, and 14, and verify the port is colored blue.
- 13 In the switch port list, view the PortShield Interface column for P12, P13, and P14 (ports 12, 13, 14) and verify that the interface listed is portshield2.
- 14 Refine the configuration of the PortShield Interface. For details, go to the section, [Refining the PortShield Interface](#).

Creating a Transparent Mode PortShield Interface with a Group Address Object

To assign a Group Address Object with addresses 67.115.118.200, 67.115.118.210, 67.115.118.212, 67.115.118.220, and 67.115.118.230 to portshield3, perform the following steps:

- 1 To add a Group Address Object, you need to go to the Address Objects window under Networks > Address Objects.

Click on the Add button in the Address Objects list in the window. SonicOS displays the Add Address Object dialog box as shown in the following figure:



- 2 Enter the string portshield3 in the Name field.
- 3 Select Network from the Type menu.
- 4 Enter 67.115.118.200 in the network IP address and 255.255.255.0 in the Netmask field.
- 5 Click on the Zone Assignment list box and click on LAN.
- 6 Click Ok. The Management Software displays the Address Objects window displaying the new portshield3 in the address group list.
- 7 Repeat the procedure with the same settings for the following IP addresses: 67.115.118.210, 67.115.118.212, 67.115.118.220, and 67.115.118.230. Make sure the name of the address object for each address is portshield3. When you finish creating these address objects, you will only see portshield3 displayed in the address group list.
- 8 Go back to the Add PortShield Interface dialog box and create an interface called portshield3 with a LAN zone, using a Transparent Mode address assignment type and select portshield3 from the Transparent Range list of existing address groups.
- 9 Click on the Switch Port tab and add the ports 16 and 20 to the address object.
- 10 Click OK. SonicOS displays the group address object portshield3 in the Interfaces list.
- 11 Note the Network and Netmask fields in the dialog box.
- 12 In the graphic of the switch, view port numbers 16 and 20, and verify that the port is colored blue.
- 13 In the switch port list, view the PortShield Interface column for P16 and P20 (ports 16 and 20) and verify that the interface listed is portshield3.
- 14 Refine the configuration of the PortShield Interface. For details, go to the section, [Refining the PortShield Interface](#).

Mapping Ports from the Switch Ports Window

Another way to create a PortShield interface is to configure the interface in the Interfaces window and then assign ports to it in the Switch Ports window. Approaching it this way assumes you created a PortShield interface first and then selected the ports from the device ports graphic and selected the existing interface. This provides several advantages:

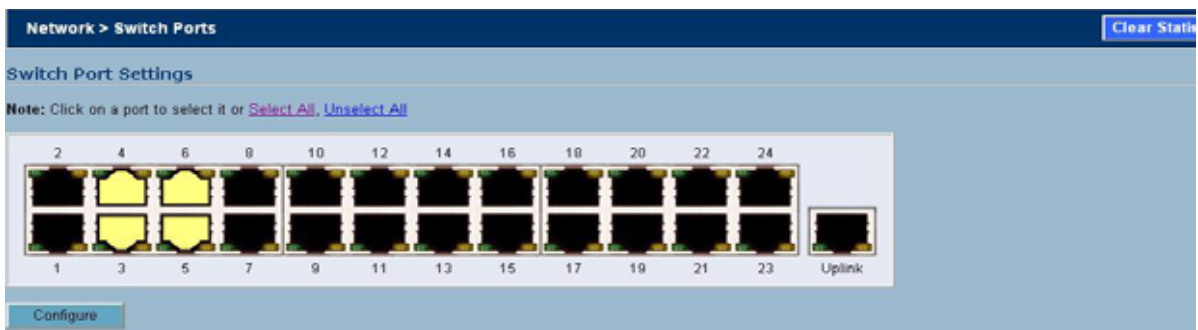
- ◆ enables you to easily visualize the actual locations of ports.
- ◆ separating the task of creating the interface, helps you focus more on how you want to separate the ports into different domains.

To select ports and apply them to a previously configured interface, perform the following steps:

- 1 Create a PortShield interface following the steps in the section [Overview](#), but do not map ports to it by going into the Switch Ports tab.
- 2 Click the Networks option in the navigation pane and then click the Switch Ports option. SonicOS displays the Switch Ports window.
- 3 Note the color of the ports. While you can map any port, no matter what its color, to an interface, you should be aware of whether it has been selected for use in another PortShield interface.
 - ◆ From the device graphic, see if any of the ports you want to select appear in black or another color. If they are black, they are unused by another PortShield interface. If they are another color, they are in use. Just be cognizant of ones that are being used and what impact your remapping the port will have on the existing interface.
 - ◆ From the Switch Ports list, see if any of the ports in the PortShield Interface list have been selected as a PortShield interface.

Be cognizant of ones that are being used and what impact your remapping the port will have on the existing interface.

- 4 On the Device Graphic, click on ports 4, 5, 6, and 7. The selected port graphics appear as yellow as shown in the following figure (if you are viewing this document in color).

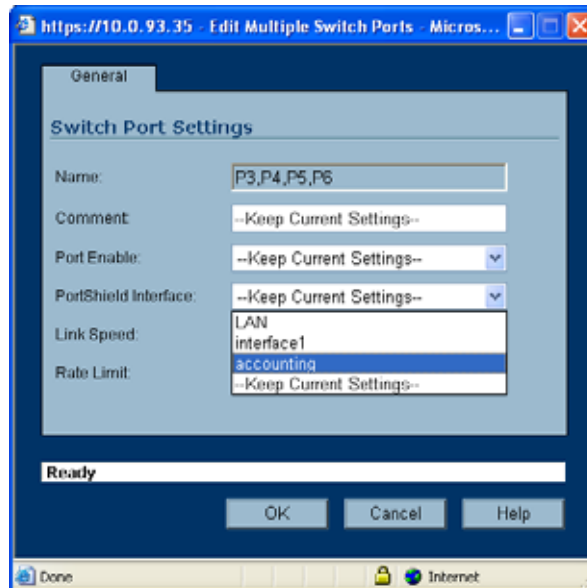


- 5 Click the Configure button. SonicOS displays the Switch Port Settings dialog box as shown in the following figure.



Note the Name field displays the ports you selected (P3, P4, P5, P6).

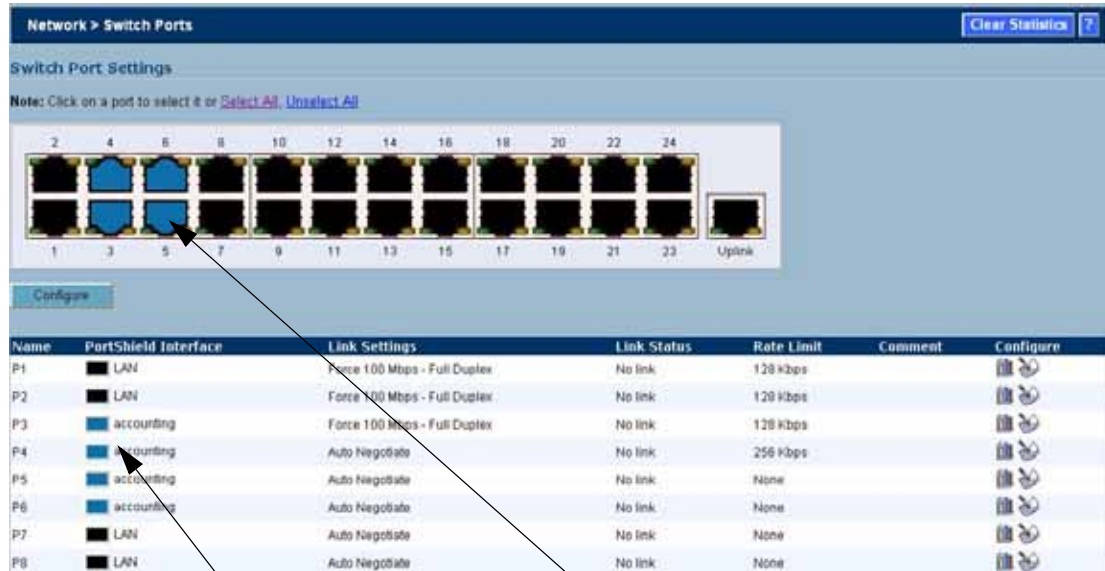
- 6 Click on the PortShield Interface list box as shown in the following figure.



Note the list contains the entry called Accounting. This is the host address object you created.

- 7 Click on the Accounting entry. By selecting this entry, you mapped ports 3, 4, 5, and 6 to the Accounting entry.
- 8 Click Ok. Wait a moment.

SonicOS displays the Switch Ports dialog box, displaying the results of your session as shown the following figure.



PortShield Interface Assignments for Ports 3, 4,

Ports 3, 4, 5, 6 in Device

9 Verify the PortShield interface port mappings.

- ◆ In the device graphic, note SonicOS changed the color of ports 3, 4, 5, and 6 from black to blue, indicating you successfully mapped them to a PortShield interface.
- ◆ In the Switch Ports list, view the PortShield Interface column for ports 3, 4, 5, and 6. This column now displays a blue-colored icon and the accounting string for P3, P4, P5, and P6, indicating these ports are now mapped to the accounting PortShield interface.

PortShield Deployment Scenarios

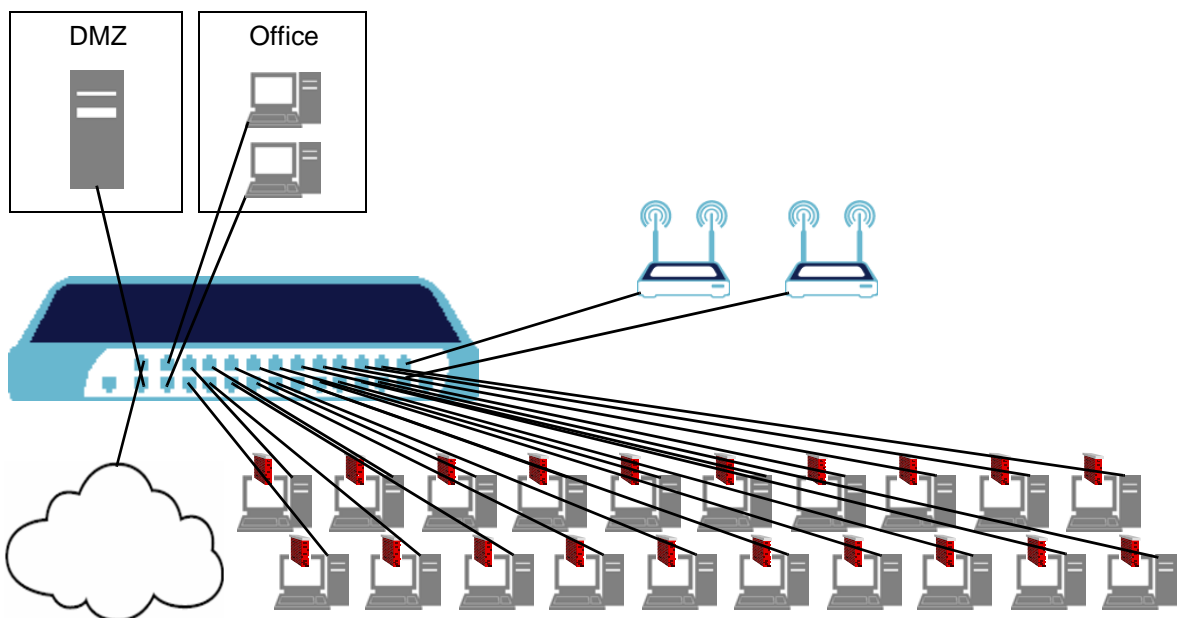
The following examples show different ways you can use PortShield interfaces in a network.

Hospitality

A PRO 1260 with PortShield can be used in a small hotel or apartment setting. For example, an apartment complex with 20 apartments could have a PortShield group for each individual room, two sonicpoints to give wireless access to residents, a small office LAN, and a mail and web server in a DMZ. With all SonicWALL Security Services enabled, the network behaves as if each apartment had a separate firewall.



Note: The easiest way to configure this example is to use the PortShield Wizard. Configure it to have 24 PortShield interfaces, with one port each. Then reconfigure the LAN to include 2 ports and reconfigure the wireless group to include 2 ports. For more details on the PortShield Wizard, see the appropriate wizard chapter.



Configuration Details

This example has the uses the following zones and PortShield interfaces:

Zones

- **LAN:** Default LAN zone configuration.
 - ◆ Used for Office PortShield Group.
 - ◆ All SonicWALL Security Services enabled.
- **Residents:** A custom zone for the General Users PortShield group. Residents is a Wireless zone with SonicPoint Enforcement disabled so it can be used like a LAN with mixed wired and wireless clients.
 - ◆ Used for the Residents PortShield group.
 - ◆ Zone Type: Wireless
 - ◆ All SonicWALL Security Services enabled.
 - ◆ **Only allow traffic generated by a SonicPoint** is not checked, disabling SonicPoint Enforcement. This setting allows the zone to be used for both wired and wireless traffic.

- ◆ **Enable Wireless Guest Services** is checked. With SonicPoint enforcement disabled, this enables both wired and wireless guest services.
- ◆ **Enable Dynamic Address Translation (DAT)** is checked. With SonicPoint enforcement disabled, this enables DAT for both wired and wireless guests.
- **DMZ:** Default DMZ zone configuration.
 - ◆ Used for Opt port.
 - ◆ All SonicWALL Security Services enabled.

PortShield Groups

The small business example uses six PortShield interfaces.

- **LAN:** for office use
 - ◆ LAN zone
 - ◆ 2 ports, 1 - 2. These ports are assigned to LAN by not assigning them to another PortShield interface.
 - ◆ 2 desktop workstations
 - ◆ no wireless access
- **Resident1** through **Resident20**
 - ◆ Resident custom Wireless zone with SonicPoint enforcement disabled
 - ◆ 1 port for each PortShield interface, from 3 to 24
 - ◆ One outlet in apartment
 - ◆ Wireless Guest Services enabled--both wireless and wired
- **Wireless_Access**
 - ◆ Resident custom Wireless zone with SonicPoint enforcement disabled
 - ◆ 2 ports, 23 - 24
 - ◆ Two SonicPoints connected, covering the whole complex and providing seamless roaming.
 - ◆ Wireless Guest Services enabled

Total 24 ports.

Configuring the Hospitality Example Deployment

Configuring the hospitality example deployment involves the following procedures:

- **Configure the SonicPoint Profile**
- **Configure the Zones**
- **Configure the PortShield Interfaces with the PortShield Wizard**
- **Set Up the DMZ**

Configure the SonicPoint Profile

This example uses two SonicPoints to grant wireless access to users throughout the complex. Residents can log in with their accounts, and guest users can log in using Wireless Guest Services. The SonicPoint profile contains the settings that the security appliance automatically applies to all connected SonicPoints.

Follow the procedures in **Chapter 33, Managing SonicPoints** and configure the SonicPoint profile. Keep the defaults except where appropriate for your installation. Set the SSID for both 802.11a and 802.11g radios to a name that identifies the apartment complex or hotel, for example, "SonicWALL Arms Resident Internet"

Configure the Zones

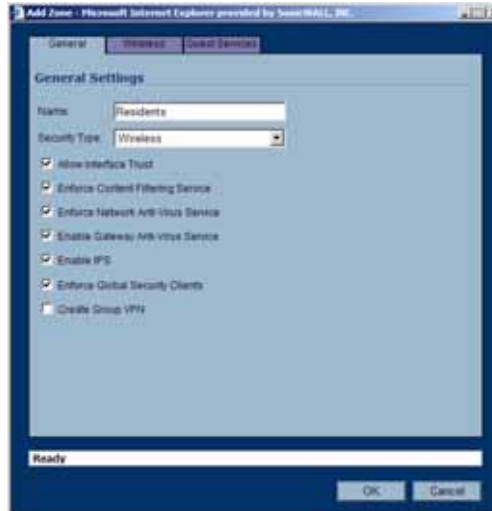
This example uses three zones inside its network, LAN, DMZ, and a custom zone, Residents. Residents is a Wireless zone with SonicPoint Enforcement disabled, thus allowing both wireless and wired access. Guest services is enabled, allowing both wired and wireless guest users access to the internet.

Configure the three Zones used in this example. Follow the procedures in **Chapter 14, Configuring Zones**.

LAN and **DMZ**: Leave the default configuration for these two zones.

Residents: Configure the Residents zone with the following values:

- **General** tab settings:
 - ◆ **Name**: Residents
 - ◆ **Security Type**: Wireless. Select Wireless so you can use the same context for the both the individual wired connections and the SonicPoints.
 - ◆ **Allow Interface Trust**: Checked
 - ◆ **Enforce Content Filtering Service**: Checked
 - ◆ **Enforce Network Anti-Virus Service**: Checked
 - ◆ **Enable Gateway Anti-Virus Service**: Checked
 - ◆ **Enable IPS**: Checked
 - ◆ **Enforce Global Security Clients**: Only check if you want to require SonicWALL Global Security Client for your residents to log into the network
 - ◆ **Create Group VPN**: Only Check if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.



- **Wireless** tab settings:
 - ◆ **Only allow traffic generated by a SonicPoint**: Leave this option unchecked. This disables SonicPoint enforcement, allowing both wired and wireless connections through this zone.
 - ◆ **WiFiSec Enforcement**: Only check this option if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.

- ◆ **SonicPoint Provisioning Profile:** Select the SonicPoint profile you configured. The settings in this profile will automatically be applied to the SonicPoints you set up for wireless access.



- **Guest Services** tab settings:
 - ◆ **Enable Wireless Guest Services:** Check this option to enable access to the internet for guest users who do not have resident accounts.
 - ◆ **Enable Dynamic Address Translation (DAT):** Check this option to enable guest users to connect without having to change their internet connection settings. See **Chapter 14, Configuring Zones** for more information on DAT.
 - ◆ **Custom Authentication Page:** Only check this option if you want to create a custom login page for guest users.



Configure the PortShield Interfaces with the PortShield Wizard

In this example, twenty apartments each have their own PortShield interface. Each of the twenty PortShield interfaces has a single port assigned to it. In addition, two ports are assigned to a Wireless PortShield interface for the SonicPoints. The Office has two ports assigned to the LAN interface.

The easiest way to configure this is to use the PortShield Wizard and then modify the configuration as follows:

Use the wizard to configure 24 separate PortShield interfaces with one port each:



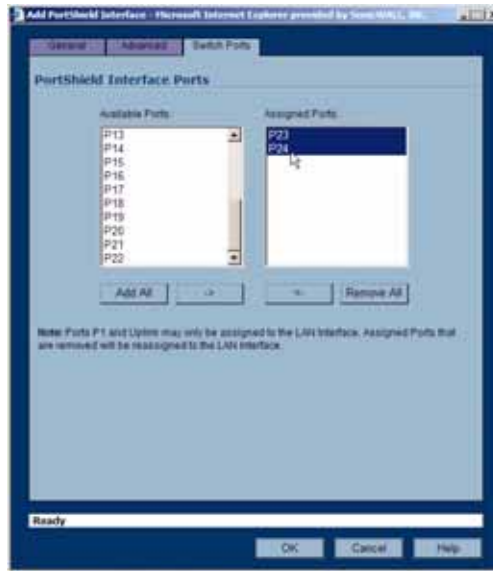
- 1 Launch the PortShield Wizard
- 2 Select 24 PortShield interfaces with one port each
- 3 Select to configure the PortShield interfaces automatically
- 4 Create the interfaces.

Create the **Wireless_Access** PortShield interface for the SonicPoints

- 1 In the **Network > Interfaces** page, click Add Interface.
- 2 Configure the Wireless_Access interface:
 - ♦ **Zone:** Residents
 - ♦ **PortShield Interface Name:** Wireless_Access
 - ♦ **IP Address:** 172.16.31.1 (or an appropriate address)
 - ♦ **Subnet Mask:** 255.255.255.0

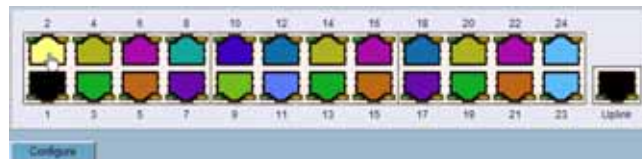


- 3 In the **Switch Ports** tab, assign ports 23 and 24 to the Wireless_Access PortShield interface

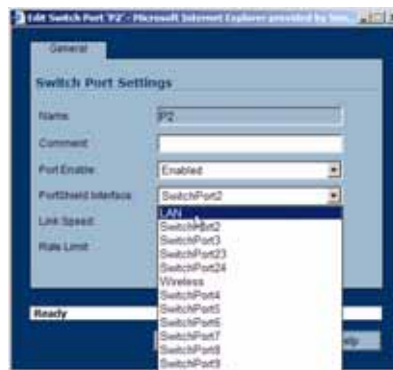


Use the **Network > Switch Ports** page to remove port 2 to the LAN interface

- 1 In the **Network > Switch Ports** page, select port 2 and click **Configure**.



- 2 In the **Edit Switch Port** page, Select **LAN** for the **PortShield interface**.



Set Up the DMZ

This example uses the Opt port as a DMZ for a mail and web server.

- 1 In the **Network > Interfaces** page, configure the Opt interface.
- 2 Select DMZ for zone.
- 3 Specify an appropriate IP address and netmask.

Small Business

One good example deployment for PortShield interface groups is a small business office, with 25 or fewer clients on the network. PortShield allows the business to separate its network into contexts.

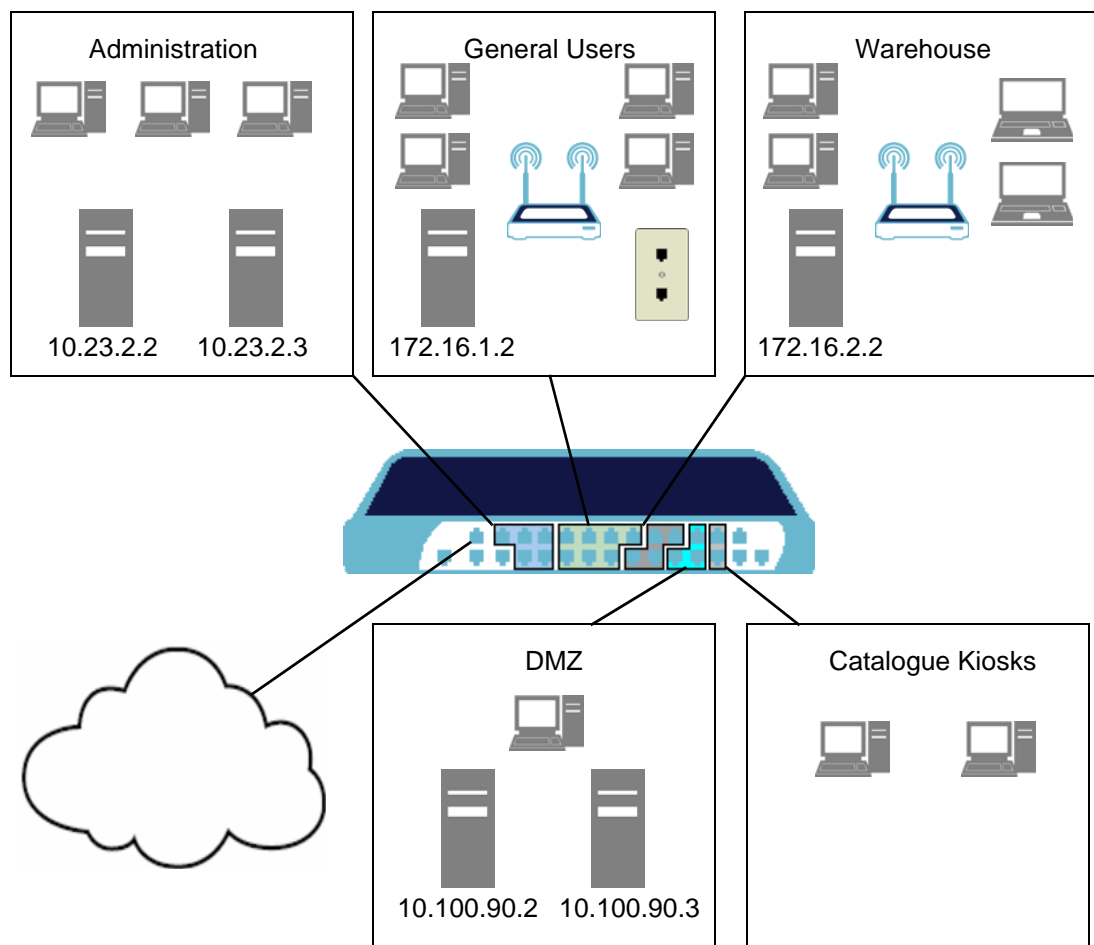
In this example, the network is divided into five zones, each served by a PortShield interface:

- Administration (including Accounting and Payroll) is on the LAN zone.
- General users in a custom Wireless zone. With SonicPoint Enforcement disabled, users in the company can have both wired and wireless access to the network. Wireless Guest Services is enabled to allow visitors to have both wired and wireless access to the Internet without access to the corporate network.
- Warehouse in a custom Wireless zone with SonicPoint Enforcement disabled. The warehouse has two stationary computers and warehouse users also have wireless access for handheld devices.
- The company has a DMZ for their mail server and Web server.
- Catalog kiosks are set up in the main building for customers to use. They are in a separate Kiosk zone.

All zones have the full array of SonicWALL Security Services enabled.



Note: In the example, the ports are assigned to the PortShield groups in sequential order. However, you can assign any combination of ports to a group. If the company needs to expand the Administration group, they can add a combination of ports to a group. For example, if the company needs to expand, they can add either of the unused ports 23 or 24.



Small Business Example Configuration Details

Zones

- **LAN:** Default LAN zone configuration.
 - ♦ Used for Administration PortShield group.
 - ♦ All SonicWALL Security Services enabled.
- **General:** A custom zone for the General Users PortShield interface. General is a Wireless zone with SonicPoint Enforcement disabled so it can be used like a LAN with mixed wired and wireless clients.
 - ♦ Used for the General Users PortShield group.
 - ♦ Zone Type: Wireless.
 - ♦ All SonicWALL Security Services enabled.
 - ♦ Only allow traffic generated by a SonicPoint is not checked, disabling SonicPoint Enforcement. This setting allows the zone to be used for both wired and wireless traffic.
 - ♦ **Enable Wireless Guest Services** is checked. With SonicPoint enforcement disabled, this enables both wired and Wireless Guest Services.
 - ♦ **Enable Dynamic Address Translation (DAT)** is checked. With SonicPoint enforcement disabled, this enables DAT for both wired and Wireless Guest Services.
- **Warehouse:** A custom zone for the Warehouse PortShield interface. General is a Wireless zone with SonicPoint Enforcement disabled so it can be used like a LAN with mixed wired and wireless clients.
 - ♦ Zone Type: Wireless.
 - ♦ All Security services enabled.
 - ♦ **Only allow traffic generated by a SonicPoint** is not checked, disabling SonicPoint Enforcement. This setting allows the zone to be used for both wired and wireless traffic.
 - ♦ **Enable Wireless Guest Services** is not checked. Guest services is not enabled for the Warehouse zone.
- **DMZ:** Default DMZ zone configuration.
 - ♦ Used for DMZ PortShield Group.
 - ♦ All SonicWALL Security Services enabled.
- **Catalog:** Copy of DMZ zone configuration.
 - ♦ Used for Kiosk PortShield.
 - ♦ All SonicWALL Security Services enabled.

PortShield Groups

The small business example uses six PortShield interfaces.

- **Administration:** for business office use, HR, Accounting, and Billing departments
 - ♦ LAN zone
 - ♦ 5 ports, 2 - 6
 - ♦ 10.100.23.0 subnet
 - ♦ Accounting, Billing, HR, etc.
 - ♦ Accounting Server 10.100.23.2
 - ♦ HR Server 10.100.23.3
 - ♦ 3 desktop workstations
 - ♦ no wireless access

- **General Users**
 - ♦ General custom Wireless zone with SonicPoint enforcement disabled
 - ♦ 7 ports, 7 - 13.
 - ♦ 172.16.1.0 subnet.
 - ♦ 4 desktops.
 - ♦ Server for sales software 172.16.1.2.
 - ♦ One SonicPoint for wireless access for employees.
 - ♦ Wireless Guest Services enabled--both wireless and wired.
 - ♦ One Guest port in conference room.
- **Warehouse**
 - ♦ Warehouse PortShield Group interface.
 - ♦ 4 ports, 14 - 17.
 - ♦ 172.16.2.0 subnet.
 - ♦ Mixed wired and wireless access.
 - ♦ Wireless Guest Services not enabled.
 - ♦ 2 fixed stationary computers.
 - ♦ 1 SonicPoint.
 - ♦ Wireless zone with SonicPoint enforcement disabled.
 - ♦ Inventory server 172.16.2.2.
- **DMZ:** for e-mail and Web and e-commerce Servers.
 - ♦ 3 ports, 18 - 20.
 - ♦ 10.100.90.0 subnet.
 - ♦ No Wireless Access.
 - ♦ Wireless Guest Services not enabled.
 - ♦ Mail Server 10.100.90.2.
 - ♦ Web Server 10.100.90.3.
 - ♦ Management station for servers - DHCP.
- **Kiosk:** for customer catalog kiosks.
 - ♦ 2 ports, 21 - 22.
 - ♦ 2 fixed stations with showing web interface of product catalog.
 - ♦ No Wireless Access.
 - ♦ Wireless Guest Services not enabled.

Total ports used: 21 - leaves 3 ports unassigned.

Configuring the Small Business Example Deployment

Configuring the Small Business example deployment involves the following procedures:

- **Configure the SonicPoint Profile**
- **Configure the Zones**
- **Configure the PortShield Interfaces with the PortShield Wizard**

Configure the SonicPoint Profile

This example uses a SonicPoint in the main office to grant wireless access to users throughout the company and a SonicPoint in the warehouse for wireless access from handheld devices like bar-code

readers. WiFiSec is enforced so employees must log in with a VPN client. Guest access is available through the SonicPoint in the General zone.

Follow the procedures in **Chapter 33, Managing SonicPoints** and configure the SonicPoint profile. Keep the defaults except where appropriate for your installation. Set the SSID for both 802.11a and 802.11g radios to a name that identifies the network.

Configure the Zones

This example uses five zones inside its network, LAN, DMZ, General, Warehouse, and Catalog.

Configure the five Zones used in this example. Follow the procedures in **Chapter 14, Configuring Zones**.

LAN and DMZ: Leave the default configuration for these two zones.

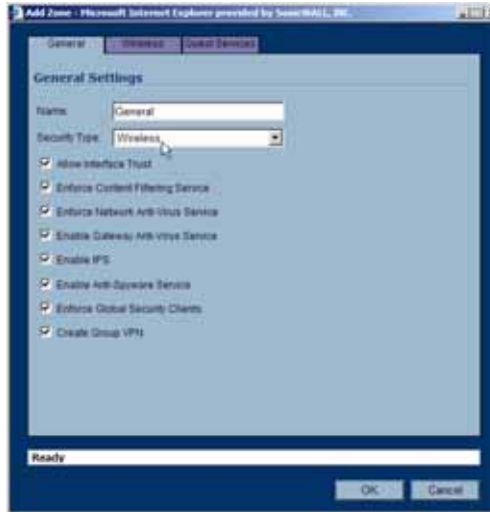
General: Configure the General zone with the following values:

- **General** tab settings:
 - ♦ **Name:** General
 - ♦ **Security Type:** **Wireless.** Select Wireless so you can use the same context for both wired connections and the SonicPoints.
 - ♦ **Allow Interface Trust:** Checked
 - ♦ **Enforce Content Filtering Service:** Checked
 - ♦ **Enforce Network Anti-Virus Service:** Checked
 - ♦ **Enable Gateway Anti-Virus Service:** Checked
 - ♦ **Enable IPS:** Checked
 - ♦ **Enforce Global Security Clients:** Check to manage SonicWALL Global Security Client settings
 - ♦ **Create Group VPN:** Check to provide a GroupVPN policy for users to log into when you enforce WiFiSec security.



- **Wireless** tab settings:
 - ♦ **Only allow traffic generated by a SonicPoint:** Leave this option unchecked. This disables SonicPoint enforcement, allowing both wired and wireless connections through this zone.
 - ♦ **WiFiSec Enforcement:** Only check this option if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.

- ◆ **SonicPoint Provisioning Profile:** Select the SonicPoint profile you configured. The settings in this profile will automatically be applied to the SonicPoints you set up for wireless access.



- **Guest Services** tab settings:
 - ◆ **Enable Wireless Guest Services:** Check this option to enable access to the internet for guest users.
 - ◆ **Enable Dynamic Address Translation (DAT):** Check this option to enable guest users to connect without having to change their internet connection settings. See **Chapter 14, Configuring Zones** for more information on DAT.
 - ◆ **Custom Authentication Page:** Only check this option if you want to create a custom login page for guest users.



Warehouse: Configure the Warehouse zone with the following values:

- **General** tab settings:
 - ◆ **Name:** Warehouse
 - ◆ **Security Type:** **Wireless.** Select Wireless so you can use the same contexts for both wired connections and the SonicPoints.
 - ◆ **Allow Interface Trust:** Checked
 - ◆ **Enforce Content Filtering Service:** Checked
 - ◆ **Enforce Network Anti-Virus Service:** Checked

- ◆ **Enable Gateway Anti-Virus Service:** Checked
- ◆ **Enable IPS:** Checked
- ◆ **Enforce Global Security Clients:** Check to manage SonicWALL Global Security Client settings
- ◆ **Create Group VPN:** Check to provide a GroupVPN policy for users to log into when you enforce WiFiSec security.
- **Wireless** tab settings:
 - ◆ **Only allow traffic generated by a SonicPoint:** Leave this option unchecked. This disables SonicPoint enforcement, allowing both wired and wireless connections through this zone.
 - ◆ **WiFiSec Enforcement:** Only check this option if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.
 - ◆ **SonicPoint Provisioning Profile:** Select the SonicPoint profile you configured. The settings in this profile will automatically be applied to the SonicPoints you set up for wireless access.
- **Guest Services** tab settings:
 - ◆ **Enable Wireless Guest Services:** Unchecked to disable Guest Services.

Catalog: Configure the Catalog zone with the following values:

- **General** tab settings:
 - ◆ **Name:** Catalog
 - ◆ **Security Type:** Public.
 - ◆ **Allow Interface Trust:** Unchecked
 - ◆ **Enforce Content Filtering Service:** Checked
 - ◆ **Enforce Network Anti-Virus Service:** Checked
 - ◆ **Enable Gateway Anti-Virus Service:** Checked
 - ◆ **Enable IPS:** Checked
 - ◆ **Enforce Global Security Clients:** Unchecked
 - ◆ **Create Group VPN:** Unchecked

Configure the PortShield Interfaces

In this example, there are four PortShield interfaces, one assigned to the LAN zone, two assigned to Wireless zones (General and Warehouse) and one assigned to the Kiosk zone which is similar to a DMZ.

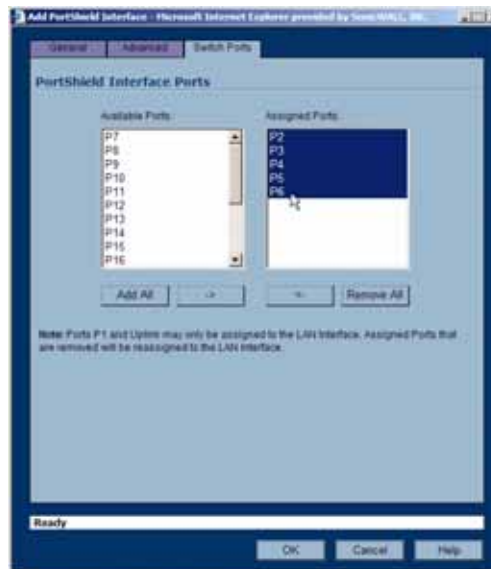
Create the **Administration** PortShield interface:

- 1 In the **Network > Interfaces** page, click Add Interface.
- 2 Configure the interface:
 - ◆ **Zone:** LAN
 - ◆ **PortShield Interface Name:** Administration
 - ◆ **IP Address:** 10.100.23.1 (or an appropriate address)

- ◆ **Subnet Mask:** 255.255.255.0



- 3 In the **Switch Ports** tab, assign ports 2 through 6 to the Administration PortShield interface.



Create the **General Users** PortShield interface:

- 1 In the **Network > Interfaces** page, click Add Interface.
- 2 Configure the interface:
 - ◆ **Zone:** General Users
 - ◆ **PortShield Interface Name:** General Users
 - ◆ **IP Address:** 172.16.1.1
 - ◆ **Subnet Mask:** 255.255.255.0
- 3 In the **Switch Ports** tab, assign ports 7 through 13 to the General Users PortShield interface.

Create the **Warehouse** PortShield interface:

- 1 In the **Network > Interfaces** page, click Add Interface.
- 2 Configure the interface:
 - ◆ **Zone:** Warehouse
 - ◆ **PortShield Interface Name:** Warehouse
 - ◆ **IP Address:** 172.16.2.1
 - ◆ **Subnet Mask:** 255.255.255.0
- 3 In the **Switch Ports** tab, assign ports 14 through 17 to the Warehouse PortShield interface.

Create the **DMZ** PortShield interface:

- 1 In the **Network > Interfaces** page, click Add Interface.
- 2 Configure the interface:
 - ◆ **Zone:** DMZ
 - ◆ **PortShield Interface Name:** DMZ
 - ◆ **IP Address:** 10.100.90.1
 - ◆ **Subnet Mask:** 255.255.255.0
- 3 In the **Switch Ports** tab, assign ports 18 through 20 to the DMZ PortShield interface.

Create the **Kiosk** PortShield interface:

- 1 In the **Network > Interfaces** page, click Add Interface.
- 2 Configure the interface:
 - ◆ **Zone:** Catalog
 - ◆ **PortShield Interface Name:** Kiosk
 - ◆ **IP Address:** 10.100.100.1
 - ◆ **Subnet Mask:** 255.255.255.0
- 3 In the **Switch Ports** tab, assign ports 21 and 22 to the Kiosk PortShield interface.



Tip: An alternative to configuring the Administration PortShield interface is to leave the ports unassigned. That way, they are automatically part of the LAN interface.

Setting Up WAN Failover and Load Balancing

Network > WAN Failover & Load Balancing

WAN Failover and Load Balancing allows you to designate the modem interface or one of the user-assigned interfaces as a Secondary or backup WAN port. The modem or secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through the secondary WAN port if the primary WAN port is down and/or unavailable. In this chapter, this feature is referred to as *basic failover*. This allows the SonicWALL security appliance to maintain a persistent connection for WAN port traffic by failing over to the modem or secondary WAN port. The primary and secondary WAN ports can also be used in a more dynamic active/active setup, where the administrator can choose a method of dividing outbound traffic flows between the Primary fixed WAN port and the user-assigned Secondary WAN port. This latter feature is referred to as *load balancing*.

WAN Failover Caveats

- WAN Failover and Load-Balancing applies to outbound-initiated traffic only; it cannot be used to perform inbound load-balancing functions, such as what a content switching or load-balancing appliance provides.
- Make sure that the SonicWALL security appliance has the proper NAT policies for the Secondary WAN interface an incorrect or missing NAT Policy for the Secondary WAN port is the most common problem seen when configuring WAN Failover & Load-Balancing.
- The Primary and Secondary WAN ports cannot be on the same IP subnet; each WAN connection must be on unique IP subnets in order to work properly
- You cannot use the WAN failover feature if you have configured the SonicWALL security appliance to use Transparent Mode in the **Network > Settings** page.

About Source and Destination IP Address Binding

When you establish a connection with a WAN, you can create multiple interfaces, dividing up the task load over these interfaces. There are both Primary and Secondary WAN interfaces. This task distribution model maintains high performance, ensuring that one interface does not become an impasse to the point where it blocks traffic from passing. This process is WAN Load Balancing.

While WAN Load Balancing addresses performance challenges, it can create other problems, including losing track of sessions. Session confusion can occur because some applications fail to

adequately track multiple user sessions load-balanced on multiple interfaces. These applications treat incoming packets as originating from different users because they use IP addresses to differentiate user sessions instead of application-layer user identification tags.

To ensure that you have proper connectivity in all applications, SonicWALL provides a feature called Source and Destination IP Addresses Binding, a solution that maintains a consistent mapping of traffic flows with a single outbound WAN interface.

Setting Up WAN Failover and Load Balancing

The following are the steps to configuring WAN Failover and Load Balancing on the SonicWALL security appliance:

- 1 [Configuring an Interface as a Secondary WAN Port](#)
- 2 [Creating a NAT Policy for the Secondary WAN Port](#)
- 3 [Activating WAN Failover and Selecting the Load Balancing Method](#)
- 4 [Configuring WAN Failover to the Modem](#)
- 5 [Configuring WAN Interface Monitoring](#)
- 6 [Configuring WAN Probe Monitoring](#)

Configuring an Interface as a Secondary WAN Port

On **Network > Interfaces** page, configure the chosen port to be in WAN zone, and enter in the correct address settings provided by the Secondary ISP. In the example, the SonicWALL security appliance is acquiring its secondary WAN address dynamically from ISP #2, using DHCP. Any interface added to the WAN zone by default creates a NAT Policy allowing internal LAN subnets to NAT out this Secondary WAN interface.

Creating a NAT Policy for the Secondary WAN Port

You need to create a NAT policy on your SonicWALL for WAN Failover. Follow these steps to create a NAT policy on your SonicWALL using the **OPT** interface:

- 1 Select **Network > NAT Policies**.
- 2 Click **Add**. The **Add NAT Policy** window is displayed.
- 3 Select **Any** from the **Original Source** menu.
- 4 Select **OPT IP** from the **Translated Source** menu.
- 5 Select **Any** from the **Original Destination** menu.
- 6 Select **Original** from the **Translated Destination** menu.
- 7 Select **Any** from the **Original Service** menu.
- 8 Select **Original** from the **Translated Service** menu.
- 9 Select **LAN** from the **Inbound Interface** menu.
- 10 Select **OPT** interface from the **Outbound Interface** menu.
- 11 Make sure the **Enable** setting is checked.
- 12 Click **OK**.

Activating WAN Failover and Selecting the Load Balancing Method

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

- 1 On **Network > WAN Failover & LB** page, select **Enable Load Balancing**.

The screenshot shows the 'Network > WAN Failover & Load Balancing' configuration page. The 'Ethernet WAN Failover & Load Balancing' section is active. The 'Primary WAN Interface' is set to 'WAN' and the 'Secondary WAN Interface' is set to 'None'. The 'Enable Load Balancing' checkbox is checked. Under 'Basic Active/Passive Failover', the 'Preempt and failback to Primary WAN when possible' checkbox is checked. Other methods like 'Per Connection Round-Robin', 'Spillover-Based', and 'Percentage-Based' are not selected. The 'WAN Load Balancing Statistics' table shows the following data:

WAN Load Balancing Statistics		
WAN Interface Statistics	WAN	Modem
Link Status:	Link Up	Link Down
Load Balancing State:	Active - Available	Adm'n Down
Probe Main Target:	Disabled	Disabled
Probe Alternate Target:	Disabled	Disabled
New Connections:	0	0
Total Connections:	0	0
Rx Unicast Packets:	3421581	0
Rx Bytes:	305000943	0
Tx Unicast Packets:	3557	0
Tx Bytes:	2241910	0
Tx Current Percentage:	100	0
Tx Current Throughput (Mbps):	1	0

- 2 If there are multiple possible secondary WAN interfaces, select an interface from the **Secondary WAN Interface**.
- 3 Select a load balancing method. By default, the SonicWALL will select **Basic Active/Passive Failover** as the method, but there are four load balancing methods available:

This close-up screenshot shows the 'Basic Active/Passive Failover' section of the configuration page. The 'Preempt and failback to Primary WAN when possible' checkbox is checked. Other options like 'Per Connection Round-Robin', 'Spillover-Based', and 'Percentage-Based' are not selected. The 'Primary WAN Percentage' is set to 100 and the 'Secondary WAN Percentage' is set to 0.

- ◆ **Basic Active/Passive Failover:** When this setting is selected, the SonicWALL security appliance only sends traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. The SonicWALL security appliance is set to use this as the default load balancing method. If the Primary WAN fails, then the SonicWALL security appliance reverts to this method instead of the ones described below. This mode will automatically return back to using the Primary WAN interface once it has been restored (preempt mode).

This item has an associated **Preempt and fail back to Primary WAN when possible** checkbox. When this checkbox is selected, the SonicWALL security appliance switches back to sending its traffic across the Primary WAN interface when it resumes responding to the SonicWALL security appliance's checks (the WAN's physical link is restored, or the logical probe targets on the WAN port resume responding).

- ◆ **Per Destination Round-Robin:** When this setting is selected, the SonicWALL security appliance load-balances outgoing traffic on a per-destination basis. This is a simple load balancing method and, though not very granular, allows you to utilize both links in a basic fashion (instead of the method above, which does not utilize the capability of the Secondary WAN until the Primary WAN has failed). The SonicWALL security appliance needs to examine outbound flows for uniqueness in source IP and destination IP and make the determination as to which interface to send the traffic out of and accept it back on. Please note this feature will be overridden by specific static route entries.
- ◆ **Spillover-Based:** When this settings is selected, the user can specify when the SonicWALL security appliance starts sending traffic through the Secondary WAN interface. This method allows you to control when and if the Secondary interface is used. This method is used if you do not want outbound traffic sent across the Secondary WAN unless the Primary WAN is overloaded.

Specify the maximum allowed bandwidth on the primary WAN interface in the **Send traffic to Secondary WAN interface when bandwidth exceeds _ kbs** field. The SonicWALL security appliance has a non-Management Interface exposed hold timer set to 20 seconds – if the sustained outbound traffic across the Primary WAN interface exceeds the administrator defined Kbps, then the SonicWALL security appliance spills outbound traffic to the Secondary WAN interface (on a per-destination basis). Please note this feature will be overridden by specific static route entries.

- ◆ **Percentage-Based:** When this setting is selected, you can specify the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces. This method allows you to actively utilize both Primary and Secondary WAN interfaces. Only one entry box is required (percentage for Primary WAN) The management interface automatically populates the non-user-editable entry box with the remaining percentage assigned to the Secondary WAN interface. Please note this feature will be overridden by specific static route entries.
 - **Use Source and Destination IP Address Binding:** When you are using percentage-based load balancing, this checkbox enables you to maintain a consistent mapping of traffic flows with a single outbound WAN interface, regardless of the percentage of traffic through that interface. Therefore, the outbound IP address of the connection remains consistent. However the percentage of traffic in each WAN interface may not match the percentage you specify in the **Primary WAN Percentage** field.

This method uses only the source IP address and the destination IP address to determine when to bind a connection to a single interface and ignores all other information, such as source and destination TCP port numbers.

4 Click **Apply**.

Configuring WAN Failover to the Modem

If you are using the Modem as a backup connection for your WAN, enable WAN failover to the modem. If your primary WAN connection fails, the TZ 170 SP Wireless will automatically try to connect with the modem. It will then monitor the WAN port, and switch back when it has a reliable connection again.



To configure WAN failover to the modem:

- 1 In the navigation column on the left, click on **Network**, and then click on **WAN Failover & LB**.
- 2 In the **Network > WAN Failover & Load Balancing** page, check the **Enable Load Balancing** box.
- 3 Check the **Enable Dial-Up Wan Failover** box.
- 4 Click **Apply** in the upper right corner of the **Network > WAN Failover & Load Balancing** page.

Configuring WAN Interface Monitoring

under the **WAN Interface Monitoring** heading, you can customize how the SonicWALL security appliance monitors the WAN interface:

- Enter a number between 5 and 300, in the **Check Interface Every _ Seconds** field. The default value is **5** seconds.
- In the **Deactivate Interface after _ missed intervals**, enter a number between 1 and 10. The default value is **3**, which means the interface is considered inactive after 3 consecutive unsuccessful attempts.
- Enter a number between 1 and 10 in the **Reactivate Interface after _ successful intervals**. The default value is 3, which means the interface is considered active after 3 consecutive successful attempts.

WAN Probe Monitoring

If Probe Monitoring is not activated, the SonicWALL security appliance performs physical monitoring only on the Primary and Secondary WAN interfaces, meaning it only marks a WAN interface as failed if the interface is disconnected or stops receiving an Ethernet-layer signal. This is not an assured means of link monitoring, because it does not address most failure scenarios (for example, routing issues with your ISP or an upstream router that is no longer passing traffic). If the WAN interface is connected to a hub or switch, and the router providing the connection to the ISP (also connected to this hub or switch) were to fail, the SonicWALL will continue to believe the WAN link is usable, because the connection to the hub or switch is good.

Enabling probe monitoring on the **Network > WAN Failover & Load Balancing** page instructs the SonicWALL security appliance to perform logical checks of upstream targets to ensure that the line is indeed usable, eliminating this potential problem, as well as continue to do physical monitoring. Under the default probe monitoring configuration, the SonicWALL performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring, because service interruption may be occurring farther upstream. If your ISP is experiencing problems in its routing infrastructure, a successful ICMP ping of their router causes the SonicWALL security appliance to believe the line is usable, when in fact it may not be able to pass traffic to and from the public Internet at all.

To perform reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port. TCP is preferred because many devices on the public Internet now actively drop or block ICMP requests. If you specify two targets for each WAN interface, you can logically link the two probe targets such that if either one fails the line will go down, or that both must fail for the line to be considered down. Using the latter method, you can configure a sort of 'deep check' to see if the line is truly usable – for instance, you could set first probe target of your ISP's router interface using ICMP (assuming they allow this), and then do a secondary probe target of a DNS server on the public Internet using TCP Port 53. With this method, if the ICMP probe of the ISP's router fails but the farther upstream continues to respond, the SonicWALL security appliance assumes the link is usable and continue to send traffic across it.

Configuring WAN Probe Monitoring

To configure WAN probe monitoring, follow these steps:

- 1 On the **Network > WAN Failover & Load Balancing** page, under the **WAN Interface Monitoring** heading, check the **Enable Probe Monitoring** box.



- 2 Check the **Respond to Probes** box to have the SonicWALL security appliance respond to SonicWALL TCP probes received on any of its WAN ports. Do not check this box if the SonicWALL security appliance should not respond to TCP probes.
- 3 Check the **Any TCP-SYN to Port** box to instruct the SonicWALL security appliance to respond to TCP probes to the specified port number without validating them first. The **Any TCP-SYN to Port** box should only be checked when receiving TCP probes from SonicWALL security appliances running SonicOS Standard or older, legacy SonicWALL security appliances.



Note: If there is a NAT device between the two devices sending and receiving TCP probes, the **Any TCP-SYN to Port** box must be checked, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.

- 4 Click on the **Configure** button. The **Configure WAN Probe Monitoring** window is displayed.



- 5 In the **Primary WAN Probe Settings** menu, select one of the following options:
 - ◆ **Probe succeeds when either Main Target or Alternate Target responds**
 - ◆ **Probe succeeds when both Main Target and Alternative Target respond**
 - ◆ **Probe succeeds when Main Target responds**
 - ◆ **Succeeds Always (no probing)**
- 6 Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.

7 Enter the IP address of the target device in the **IP Address** field.

8 Enter a port number in the **Port** field.



Note: If there is a NAT device between the two devices sending and receiving TCP probes, the **Any TCP-SYN to Port** box must be checked, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.

9 Check the **SNWL?** box if the target device is a SonicWALL security appliance. Do not check the **SNWL?** box for third-party devices, as the TCP probes may not work consistently.

10 Configure the **Secondary WAN Probe Settings**, which provide the same options as the **Primary WAN Probe Settings**.

11 If you are using the Modem as a backup connection for your WAN, configure the **Dialup WAN Probe Settings**, which provide the same options as the **Primary WAN Probe Settings**.

12 Click **OK**.



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



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

WAN Load Balancing Statistics

The **WAN Load Balancing Statistics** table displays the following WAN Interface statistics for the SonicWALL:

WAN Load Balancing Statistics		
WAN interface Statistics	X1	X4
Link Status:	Link Up	Link Down
Load Balancing State:	Active - Available	Failover
Probe Main Target:	No probing	No probing
Probe Alternate Target:	No probing	No probing
New Connections:	1539	0
Total Connections:	40356	0
Rx Unicast Packets:	17912	0
Rx Bytes:	112520961	0
Tx Unicast Packets:	21080	0
Tx Bytes:	11177641	0
Tx Current Percentage:	0	0
Tx Current Throughput (KB/s):	31	0

- **Link Status**
- **Load Balancing State**
- **Probe Monitoring**
- **New Connections**
- **Total Connections**
- **Rx Unicast Packets**
- **Rx Bytes**
- **Tx Unicast Packets**
- **Tx Bytes**

- **Tx Current Percentage**
- **Tx Current Throughput (KB/s)**

Click the **Clear Statistic** button on the top right of the **Network > WAN Failover & Load Balancing** page to clear information from the **WAN Load Balancing Statistics** table.

Configuring Zones

Network > Zones

A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.



Cross Reference: For more information on configuring interfaces, see **Chapter 11, Configuring Interfaces**.

SonicOS Enhanced zones allows you to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN tunnels, which is a feature that users have long requested. SonicWALL security appliances can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zone.

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure
LAN	Trusted	X0	✓			✓	✓	✓		⊞ ⊞ ⊞
WAN	Untrusted	X1				✓	✓	✓		⊞ ⊞ ⊞
DMZ	Public	X2	✓	✓						⊞ ⊞ ⊞
VPN	Encrypted	N/A								⊞ ⊞ ⊞
MULTICAST	Untrusted	N/A								⊞ ⊞ ⊞
WLAN	Wireless	N/A								⊞ ⊞ ⊞

How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a doorperson on the way out of each room. This doorperson is the inter-zone/intra-zone security policy, and the doorperson's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (i.e. the security policy lets them), they can leave the room via the door (the interface).

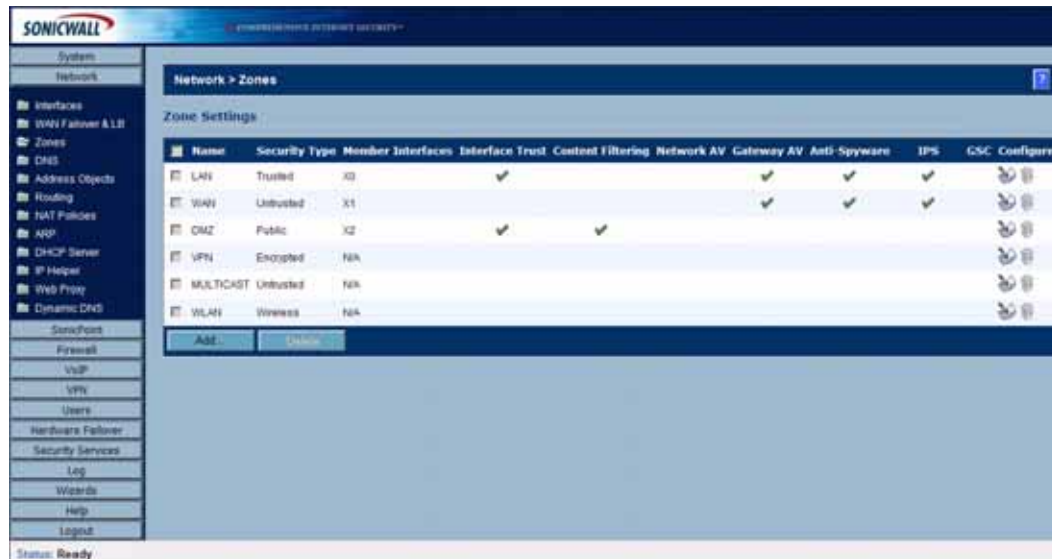
Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they've been told to do so (i.e. only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN load balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also don't recognize each other, in order to speak with someone in another group, the users must ask the doorperson (the security policy) to point out which person in the other group is the one with whom they wish to speak. The doorperson has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people will wish to visit remote offices, and people may arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The doorperson can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.

Predefined Zones

The predefined zones on your the SonicWALL security appliance depend on the device. The following are all the SonicWALL security appliance's predefined security zones:



Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	Anti-Spyware	IPS	CSC	Configure
LAN	Trusted	X0	✓			✓	✓	✓		
WAN	Untrusted	X1				✓	✓	✓		
DMZ	Public	X2	✓	✓						
VPN	Encrypted	N/A								
MULTICAST	Untrusted	N/A								
WLAN	Wireless	N/A								

The pre-defined security zones on the SonicWALL security appliance are not modifiable and are defined as follows:

- **WAN:** This zone can consist of either one or two interfaces. If you're using the security appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
- **LAN:** This zone can consist of one to five interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity.
- **DMZ:** This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on you network design.
- **VPN:** This virtual zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical interface.
- **MULTICAST:** This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.
- **WLAN:** This zone provides support to SonicWALL SonicPoints. When assigned to the Opt port, it enforces SonicPoint Enforcement, automatically dropping all packets received from non-SonicPoint devices. The WLAN zone supports SonicPoint Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoints. It also supports SonicWALL Simple Provisioning Protocol to configure SonicPoints using profiles.

In a TZ 170 Wireless or TZ 170 SP Wireless, The **WLAN** zone is assigned to the **WLAN** interface (built-in antennas). The **WLAN** zone works with the built-in 802.11b/g antennas when assigned to the **WLAN** interface, and does not enforce SonicPoint Enforcement, SDP, or SSPP.



Note: Even though you may group interfaces together into one security zone, this does not preclude you from addressing a single interface within the Zone.

Security Types

Each zone has a security type, which defines the level of trust given to that zone. There are five security types:

- **Trusted:** Trusted is a security type that provides the highest level of trust--meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the security appliance. The LAN zone is always Trusted.
- **Encrypted:** Encrypted is a security type used exclusively by the VPN Zone. All traffic to and from an Encrypted zone is encrypted.
- **Wireless:** Wireless is a security type applied to the WLAN zone or any zone where the only interface to the network consists of SonicWALL SonicPoint devices. You typically use WiFiSec to secure traffic in a Wireless zone. The Wireless security type is designed specifically for use with SonicPoint devices. Placing an interface in a Wireless Zone activates SDP (SonicWALL Discovery Protocol) and SSPP (SonicWALL Simple Provisioning Protocol) on that interface for automatic discovery and provisioning of SonicPoint devices. Only traffic that passes through a SonicPoint is allowed through a Wireless zone; all other traffic is dropped.
- **Public:** A Public security type offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default traffic from DMZ to LAN is denied. But traffic from LAN to ANY is allowed. This means only LAN initiated connections will have traffic between DMZ and LAN. The DMZ will only have default access to the WAN, not the LAN.
- **Untrusted:** The Untrusted security type represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the security appliance. By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.

Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** window automates the creation of Access Rules to allow traffic to flow between the Interfaces of a zone instance. For example, if the LAN Zone has both the **LAN** and **OPT** interfaces assigned to it, checking **Allow Interface Trust** on the LAN Zone creates the necessary Access Rules to allow hosts on these Interfaces to communicate with each other.

Enabling SonicWALL Security Services on Zones

You can enable SonicWALL Security Services for traffic across zones. For example, you can enable SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable the following SonicWALL Security Services on zones:

- **Enforce Content Filtering Service** - enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
- **Enforce Network Anti-Virus Service** - enforces anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Gateway Anti-Virus** - enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable IPS** - enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.

- **Enable Anti-Spyware Service** - enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enforce Global Security Clients** - enforces security policies for Global Security Clients on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN** - creates a GroupVPN policy for the Zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck **Create Group VPN**, the GroupVPN policy is removed from the **VPN > Settings** page.

The Zone Settings Table

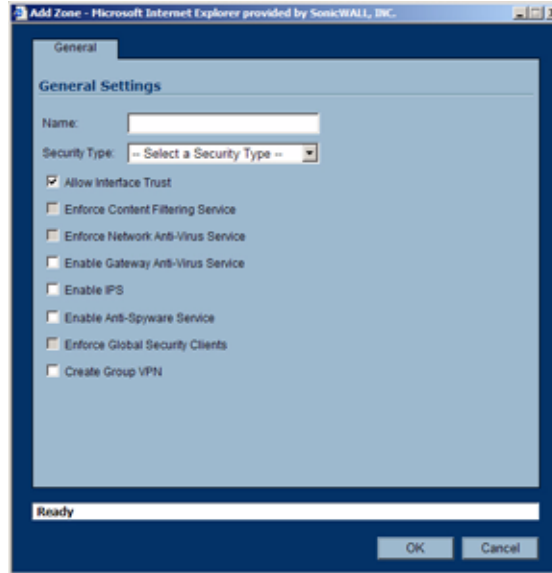
The **Zone Settings** table displays a listing of all the SonicWALL security appliance default pre-defined zones as well as any zones you create. The table displays the following status information about each zone configuration:

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure
LAN	Trusted	X0	✓			✓	✓	✓		
WAN	Untrusted	X1				✓	✓	✓		
DMZ	Public	X2	✓	✓						
VPN	Encrypted	N/A								
MULTICAST	Untrusted	N/A								
WLAN	Wireless	N/A								

- **Name:** Lists the name of the zone. The predefined **LAN**, **WAN**, **WLAN**, **VPN**, and **Encrypted** zone names cannot be changed.
- **Security Type:** Displays the security type: **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**.
- **Member Interfaces:** Displays the interfaces that are members of the zone. VLAN sub-interfaces are denoted by the name of the physical interface and the VLAN tag number, for example: "X3:V100".
- **Interface Trust:** A check mark indicates the **Allow Interface Trust** setting is enabled for the zone.
- **Content Filtering:** A check mark indicates SonicWALL Content Filtering Service is enabled for traffic coming in and going out of the zone.
- **Network Anti-Virus:** A check mark indicates SonicWALL Network Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWALL Network Anti-Virus manages an anti-virus client application on all clients on the zone.
- **Gateway Anti-Virus:** A check mark indicates SonicWALL Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
- **Anti-Spyware Service** - A check mark indicates SonicWALL Anti-Spyware detection and prevention is enabled for traffic through interfaces in the zone.
- **IPS:** A check mark indicates SonicWALL Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
- **GSC:** A check mark indicates SonicWALL Global Security Client is enabled for clients connecting to the zone.
- **Configure:** Clicking the Notepad icon displays the Edit Zone window. Clicking the Trashcan icon deletes the zone. The Trashcan icon is dimmed for the predefined zones. You cannot delete these zones.

Adding a New Zone

To add a new Zone, click **Add** under the **Zone Settings** table. The **Add Zone** window is displayed.




- 1 Type a name for the new zone in the **Name** field.
- 2 Select a security type **Trusted**, **Public** or **Wireless** from the **Security Type** menu. Use **Trusted** for Zones that you want to assign the highest level of trust, such as internal LAN segments. Use **Public** for Zones with a lower level of trust requirements, such as a DMZ Interface. Use **Wireless** for the WLAN interface.
- 3 If you want to allow intra-zone communications, select **Allow Interface Trust**. If not, select the **Allow Interface Trust** checkbox.
- 4 Select any of the SonicWALL Security Services you want to enforce on the zone. You can select:
 - ♦ **SonicWALL Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
 - ♦ **SonicWALL Enforce Network Anti-Virus Service** - Enforces network anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones, using the SonicWALL Network Anti-Virus client on your network hosts
 - ♦ **Enable Gateway Anti-Virus Service** - Enforces gateway anti-virus protection on your SonicWALL security appliance for all clients connecting to this zone. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
 - ♦ **SonicWALL Intrusion Protection Service (IPS)** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
 - ♦ **Enable Anti-Spyware Service** - enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
 - ♦ **Enforce Global Security Clients** - Requires clients to use the SonicWALL Global Security Client (GSC) to secure their local machine. Causes GSC settings to be pushed from the security appliance to the network hosts.
 - ♦ **Create Group VPN** - Automatically creates a SonicWALL GroupVPN Policy for this zone. You can customize the GroupVPN Policy in the **VPN > Settings** page.




Alert: *Unsetting the **Create Group VPN** checkbox will remove any corresponding GroupVPN policy.*

- 5 Click **OK**. The new zone is now added to the SonicWALL security appliance.

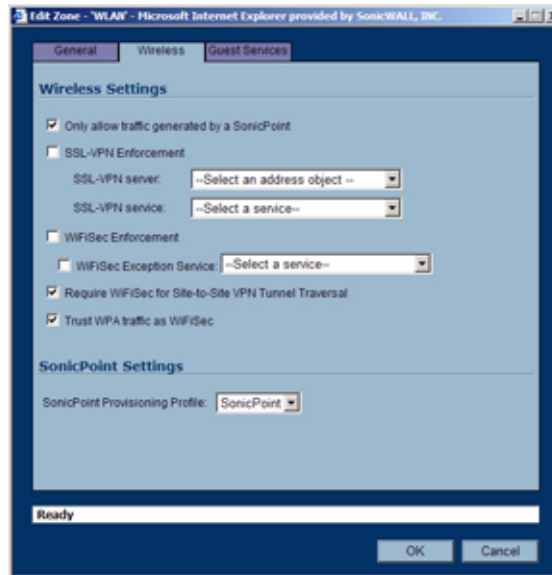
Deleting a Zone

You can delete a user-created zone by clicking the Trashcan icon  in the **Configure** column. The Trashcan icon is unavailable for the predefined Zones (LAN, WAN, DMZ, VPN, WLAN, and MULTICAST). You cannot delete these zones. Any zones that you create can be deleted.

Configuring the WLAN Zone

- 1 Click the Edit icon  for the WLAN zone. The **Edit Zone** window is displayed.
- 2 In the **General** tab, select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the Interfaces of a zone instance. For example, if the LAN Zone has both the **LAN** and **OPT** interfaces assigned to it, checking **Allow Interface Trust** on the LAN Zone creates the necessary Access Rules to allow hosts on these Interfaces to communicate with each other.
- 3 Select any of the following settings to enable the SonicWALL Security Services on the WLAN zone:
 - ♦ **Enforce Content Filtering Service** - enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
 - ♦ **Enforce Network Anti-Virus Service** - enforces managed anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. SonicWALL Network Anti-Virus manages an anti-virus client application on all clients on the zone.
 - ♦ **Enable Gateway Anti-Virus** - enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
 - ♦ **Enable IPS** - enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
 - ♦ **Enable Anti-Spyware Service** - enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
 - ♦ **Enforce Global Security Clients** - enforces security policies for Global Security Clients on multiple interfaces in the same Trusted, Public or WLAN zones.
 - ♦ **Create Group VPN** - creates a GroupVPN policy for the Zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck Create Group VPN, the GroupVPN policy is removed from the **VPN > Settings** page.

- 4 Click the **Wireless** tab.



- 5 In the **Wireless Settings** section, check **Only allow traffic generated by a SonicPoint** to allow only traffic from SonicWALL SonicPoints to enter the WLAN Zone interface. This allows maximum security of your WLAN. Uncheck this option if you want to allow any traffic on your WLAN Zone regardless of whether or not it is from a wireless connection.



Tip: Uncheck **Only allow traffic generated by a SonicPoint** and use the zone on a wired interface to allow guest services on that interface.

- 6 Select **SSL-VPN Enforcement** to require that all traffic that enters into the WLAN Zone be authenticated through a SonicWALL SSL-VPN appliance.

If you select both **SSL-VPN Enforcement**, and **WiFiSec Enforcement**, the Wireless zone will allow traffic authenticated by either a SSL-VPN or an IPsec VPN.

- 7 In the **SSL-VPN Server** list, select an address object to direct traffic to the SonicWALL SSL-VPN appliance. You can select:

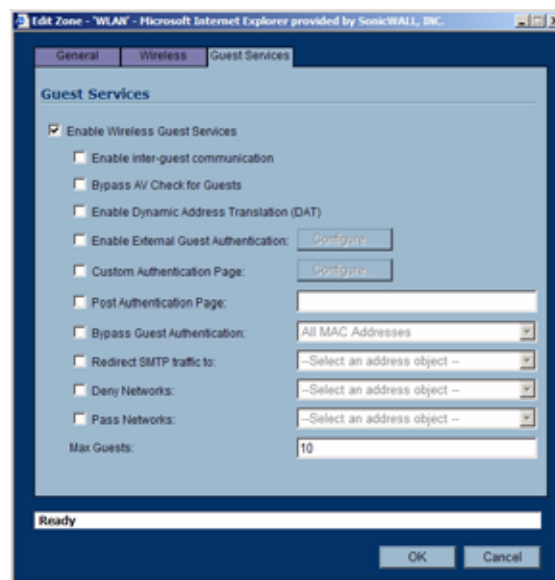
- ◆ **Create new address object...**
- ◆ **Default Gateway**
- ◆ **Secondary Default Gateway**
- ◆ **X0 IP**
- ◆ **X1 IP**
- ◆ **X2 IP**
- ◆ **X3 IP**
- ◆ **X4 IP**
- ◆ **X5 IP**

- 8 In the **SSL-VPN Service** list, select the service or group of services you want to allow for clients authenticated through the SSL-VPN.

- 9 Select **WiFiSec Enforcement** to require that all traffic that enters into the WLAN Zone interface be either IPsec traffic, WPA traffic, or both. With **WiFiSec Enforcement** enabled, all non-guest wireless clients connected to SonicPoints attached to an interface belonging to a Zone on which WiFiSec is enforced are required to use the strong security of IPsec. The VPN connection inherent in WiFiSec terminates at the "WLAN GroupVPN", which you can configure independently of "WAN GroupVPN" or other Zone GroupVPN instances.

If you select both **WiFiSec Enforcement**, and **SSL-VPN Enforcement**, the Wireless zone will allow traffic authenticated by either a SSL-VPN or an IPsec VPN.

- 10 If you have enabled **WiFiSec Enforcement**, you can specify services that are allowed to bypass the WiFiSec enforcement by checking **WiFiSec Exception Service** and then selecting the service you want to exempt from WiFiSec enforcement.
- 11 If you have enabled **WiFiSec Enforcement**, you can select **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** to require WiFiSec security for all wireless connections through the WLAN zone that are part of a site-to-site VPN.
- 12 Select **Trust WPA traffic as WiFiSec** to accept WPA as an allowable alternative to IPsec. Both WPA-PSK (Pre-shared key) and WPA-EAP (Extensible Authentication Protocol using an external 802.1x/EAP capable RADIUS server) will be supported on SonicPoints.
- 13 Under the **SonicPoint Settings** heading, select the **SonicPoint Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.
- 14 Click the **Guest Services** tab. You can choose from the following configuration options for Wireless Guest Services:



- ◆ **Enable Wireless Guest Services** - enables guest services on the WLAN zone.
- ◆ **Enable inter-guest communication** - allows guests connecting to SonicPoints in this WLAN Zone to communicate directly and wirelessly with each other.
- ◆ **Bypass AV Check for Guests** - allows guest traffic to bypass Anti-Virus protection.
- ◆ **Enable Dynamic Address Translation (DAT)** - Wireless Guest Services (WGS) provides spur of the moment “hotspot” access to wireless-capable guests and visitors. For easy connectivity, WGS allows wireless users to authenticate and associate, obtain IP settings from the TZ 170 Wireless DHCP services, and authenticate using any web-browser. Without DAT, if a WGS user is not a DHCP client, but instead has static IP settings incompatible with the TZ 170 Wireless WLAN network settings, network connectivity is prevented until the user’s settings change to compatible values. Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the TZ 170 Wireless to support any IP addressing scheme for WGS users. For example, the TZ 170 Wireless WLAN interface is configured with its default address of 172.16.31.1, and one WGS client has a static IP Address of 192.168.0.10 and a default gateway of 192.168.0.1, while another has a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables network communication for both of these clients.
- ◆ **Enable External Guest Authentication** - requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.



Note: Refer to the SonicWALL *Lightweight Hotspot Messaging Tech Note* available at the SonicWALL documentation Web site <<http://www.sonicwall.com/services/documentation.html>> for complete configuration of the **Enable External Guest Authentication** feature.

- ◆ **Custom Authentication Page** - redirects users to a custom authentication page when they first connect to a SonicPoint in the WLAN zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
- ◆ **Post Authentication Page** - directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
- ◆ **Bypass Guest Authentication** - allows a SonicPoint running WGS to integrate into environments already using some form of user-level authentication. This feature automates the WGS authentication process, allowing wireless users to reach WGS resources without requiring authentication. This feature should only be used when unrestricted WGS access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
- ◆ **Redirect SMTP traffic to** - redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
- ◆ **Deny Networks** - blocks traffic from the networks you name. Select the subnet, address group, or IP address to block traffic from.
- ◆ **Pass Networks** - automatically allows traffic through the WLAN zone from the networks you select.
- ◆ **Max Guests** - specifies the maximum number of guest users allowed to connect to the WLAN zone. The default is 10.

15 Click **OK** to apply these settings to the WLAN zone.

Configuring DNS Settings

Network > DNS

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses.

The **Network > DNS** page allows you to manually configure your DNS settings, if necessary.



In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields. Click **Apply** to save your changes.

To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Apply** to save your changes.

The screenshot shows the 'Network > DNS' configuration window. At the top right, there are 'Apply', 'Cancel', and a help icon. The main section is titled 'DNS Settings'. There are two radio button options: 'Specify DNS Servers Manually' (which is unselected) and 'Inherit DNS Settings Dynamically from WAN Zone' (which is selected). Under the 'Specify DNS Servers Manually' option, there are three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', all containing the value '0.0.0.0'. Under the 'Inherit DNS Settings Dynamically from WAN Zone' option, there are three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', containing the values '10.2.16.6', '10.50.128.52', and '0.0.0.0' respectively.

Configuring Address Objects

Network > Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS Enhanced. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web-Server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called “My Web Server” as a Host Address Object with an IP address of 67.115.118.80. This Address Object, “My Web Server” can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

Types of Address Objects

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host** – Host Address Objects define a single host by its IP address. The netmask for a Host Address Object will automatically be set to 32 bit (255.255.255.255) to identify it as a single host. For example, “My Web Server” with an IP address of “67.115.118.110” and a default netmask of “255.255.255.255”
- **Range** – Range Address Objects define a range of contiguous IP addresses. No netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32 bit-masked Host object. For example “My Public Servers” with an IP address starting value of “67.115.118.66” and an ending value of “67.115.118.90”. All 25 individual host addresses in this range would be comprised by this Range Address Object.
- **Network** – Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network Address Objects must be defined by the network’s address and a corresponding netmask. For example “My Public Network” with a Network Value of “67.115.118.64” and a Netmask of “255.255.255.224” would comprise addresses from 67.115.118.64 through to 67.115.118.95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable.
- **MAC Address** – MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address. MAC Addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48 bit values that are expressed in 6 byte hex-notation. For

example “My Access Point” with a MAC address of “00:06:01:AB:02:CD”. MAC Address objects are used by various components of Wireless configurations throughout SonicOS.

Address Object Groups

SonicOS Enhanced has the ability to group Address Objects into Address Object Groups. Groups of Address Objects can be defined to introduce further referential efficiencies. Groups can comprise any combination of Host, Range, or Network Address Objects. MAC Address Objects should be grouped separately, although they can safely be added to Groups of IP-based Address Objects, where they will be ignored when their reference is contextually irrelevant (e.g. in a NAT Policy). For example “My Public Group” can contain Host Address Object “My Web Server” and Range Address Object “My Public Servers”, effectively representing IP Addresses 67.115.118.66 to 67.115.118.90 and IP Address 67.115.118.110.

Creating and Managing Address Objects

The **Network > Address Objects** page allows you to create and manage your Address Objects.

#	Name	Address Detail	Type	Zone	Configure
1	LAN Subnets		Group		
2	Firewalled Subnets		Group		
3	LAN Interface IP		Group		
4	WAN Subnets		Group		
5	WAN Interface IP		Group		
6	DMZ Subnets		Group		
7	DMZ Interface IP		Group		
8	WLAN Subnets		Group		
9	WLAN Interface IP		Group		
10	All WAN IP		Group		
11	All Interface IP		Group		
12	All LAN Management IP		Group		
13	All WAN Management IP		Group		

You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** - displays all configured Address Objects.
- **Custom Address Objects** - displays Address Objects with custom properties.
- **Default Address Objects** - displays Address Objects configured by default on the SonicWALL security appliance.

Sorting Address Objects allows you to quickly and easily locate Address Objects configured on the SonicWALL security appliance.



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

Navigating and Sorting the Address Objects and Address Groups Entries









The Address Objects and Address Groups tables provides easy pagination for viewing a large number of address objects and groups. You can navigate a large number of entries listed in the Address Objects or Address Groups tables by using the navigation control bar located at the top right of the tables. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Default Address Objects and Groups

The **Default Address Objects** view displays the default **Address Objects** and **Address Groups** for your SonicWALL security appliance. The **Default Address Objects** entries cannot be modified or deleted. Therefore, the **Notepad** (Edit) and **Trashcan** (delete) icons are dimmed. The following lists the default **Address Objects** and **Address Groups** for the TZ 170 SP Wireless.

#	Name	Address Detail	Type	Zone	Configure
1	LAN Primary IP	192.168.168.0/255.255.255.255	Host	LAN	 
2	LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN	 
3	WAN Primary IP	10.0.93.31/255.255.255.255	Host	WAN	 
4	WAN Primary Subnet	10.0.93.0/255.255.255.0	Network	WAN	 
5	OPT IP	172.16.32.0/255.255.255.255	Host	WLAN	 
6	OPT Subnet	172.16.32.0/255.255.255.0	Network	WLAN	 
7	Modem IP	0.0.0.0/255.255.255.255	Host	WAN	 
8	Modem Subnet	0.0.0.0.0.0.0	Network	WAN	 
9	WLAN IP	172.16.31.1/255.255.255.255	Host	WLAN	 
10	WLAN Subnet	172.16.31.0/255.255.255.0	Network	WLAN	 
11	Default Gateway	10.0.0.254/255.255.255.255	Host	WAN	 
12	Secondary Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	 
13	WLAN RemoteAccess Networks	0.0.0.0.0.0.0	Network	VPN	 
14	Dial-Up Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	 
15	SonicPoint 00:02:8f:e0:09:72	00:02:8f:e0:09:72	MAC Address	WLAN	 
16	Bite_B	10.30.30.0/255.255.255.255	Host	LAN	 
17	Access Point 00:06:b1:12:4b:a1	00:06:b1:12:4b:a1	MAC Address	WLAN	 

SonicWALL PRO 5060

Default Address Objects

- X0 IP
- X0 Subnet
- X1 IP Host
- X1 Subnet
- X2 IP
- X2 Subnet

- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- LAN Interface IP
- WAN Subnets
- WAN Interface IP
- DMZ Subnets
- DMZ Interface IP
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- Custom Subnets
- Custom Interface IP
- All SonicPoints
- All Authorized Access Points
- WLAN Subnets
- WLAN Interface IP
- All SonicPoints
- All Authorized Access Points
- Node License Exclusion List
- RBL User White List
- RBL User Black List
- Default SonicPoint ACL Allow Group
- Default SonicPoint ACL Deny Group
- All X0 Management IP

SonicWALL PRO 4060

Default Address Objects

- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet

- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- WAN Remote Access Networks
- VPN DHCP Clients
- LAN Remote Access Networks
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- WAN Subnets
- DMZ Subnets
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- All SonicPoints
- All Authorized Access Points
- LAN Interface IP
- WAN Interface IP
- DMZ Interface IP
- WLAN Subnets
- WLAN Interface IP
- Wireless2 Subnets
- Wireless2 Interface IP
- All SonicPoints
- All Authorized Access Points
- Node License Exclusion List
- RBL User White List
- RBL User Black List
- Default SonicPoint ACL Allow Group
- Default SonicPoint ACL Deny Group
- All X0 Management IP

SonicWALL PRO 3060

Default Address Objects

- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- WAN Remote Access Networks
- VPN DHCP Clients
- LAN Remote Access Networks
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- WAN Subnets
- DMZ Subnets
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- All SonicPoints
- All Authorized Access Points
- LAN Interface IP
- WAN Interface IP
- DMZ Interface IP
- WLAN Subnets
- WLAN Interface IP
- Wireless2 Subnets
- Wireless2 Interface IP
- All SonicPoints
- All Authorized Access Points
- Node License Exclusion List
- RBL User White List

- RBL User Black List
- Default SonicPoint ACL Allow Group
- Default SonicPoint ACL Deny Group
- All X0 Management IP

SonicWALL PRO 2040

Default Address Objects

- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- WAN Remote Access Networks
- VPN DHCP Clients
- LAN Remote Access Networks
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- WAN Subnets
- DMZ Subnets
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- All SonicPoints
- All Authorized Access Points
- LAN Interface IP
- WAN Interface IP
- DMZ Interface IP
- WLAN Subnets
- WLAN Interface IP
- Wireless2 Subnets

- Wireless2 Interface IP
- All SonicPoints
- All Authorized Access Points
- Node License Exclusion List
- RBL User White List
- RBL User Black List
- Default SonicPoint ACL Allow Group
- Default SonicPoint ACL Deny Group
- All X0 Management IP

#	Name	Address Detail	Type	Zone	Configure
1	LAN Primary IP	192.168.168.168/255.255.255.255	Host	LAN	
2	LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN	
3	WAN Primary IP	10.0.93.31/255.255.255.255	Host	WAN	
4	WAN Primary Subnet	10.0.93.0/255.255.255.0	Network	WAN	
5	OPT IP	172.16.32.1/255.255.255.255	Host	WLAN	
6	OPT Subnet	172.16.32.0/255.255.255.0	Network	WLAN	
7	Modem IP	0.0.0.0/255.255.255.255	Host	WAN	
8	Modem Subnet	0.0.0.0.0.0.0	Network	WAN	
9	WLAN IP	172.16.31.1/255.255.255.255	Host	WLAN	
10	WLAN Subnet	172.16.31.0/255.255.255.0	Network	WLAN	
11	Default Gateway	10.0.0.254/255.255.255.255	Host	WAN	
12	Secondary Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	
13	WLAN RemoteAccess Networks	0.0.0.0.0.0.0	Network	VPN	
14	Dial-Up Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	
15	SonicPoint 00:02:8f:a0:00:72	00:02:8f:a0:00:72	MAC Address	WLAN	
16	Site_B	10.30.30.0/255.255.255.255	Host	LAN	
17	Access Point 00:06:b1:12:4b:a1	00:06:b1:12:4b:a1	MAC Address	WLAN	

SonicWALL TZ 170 Series

Default Address Objects

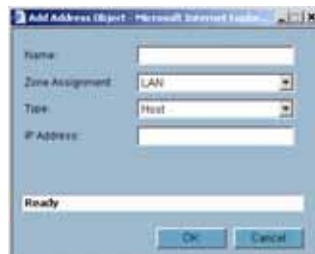
- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- OPT IP
- OPT Subnet
- Modem IP
- Modem Subnet
- WLAN IP
- WLAN Subnet
- Default Gateway
- Secondary Default Gateway
- WLAN RemoteAccess Networks
- Dial-Up Default Gateway (TZ 170 SP and TZ 170 SP Wireless only)
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- LAN Interface IP
- WAN Subnets
- WAN Interface IP
- DMZ Subnets
- DMZ Interface
- WLAN Subnets
- WLAN Interface IP
- All WAN IP
- All Interface IP
- All LAN Management IP
- All WAN Management IP
- All SonicPoints
- All Authorized Access Points
- Default ACL Allow Group
- Default ACL Deny Group
- Node License Exclusion List


Adding an Address Object

To add an **Address Object**, click **Add** button under the **Address Objects** table in the **All Address Objects** or **Custom Address Objects** views to display the **Add Address Object** window.



- 1 Enter a name for the Network Object in the **Name** field.
- 2 Select **Host** or **Range** or **Network** from the **Type** menu.
- 3 If you select **Host**, enter the IP address and netmask in the **IP Address** and **Netmask** fields.
- 4 If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
- 5 If you selected Network, enter the network IP address and netmask in the **Network** and **Netmask** fields.
- 6 Select the zone to assign to the Address Object from the **Zone Assignment** menu. You can choose **LAN**, **WAN**, **DMZ**, or **VPN**.

Editing or Deleting an Address Object

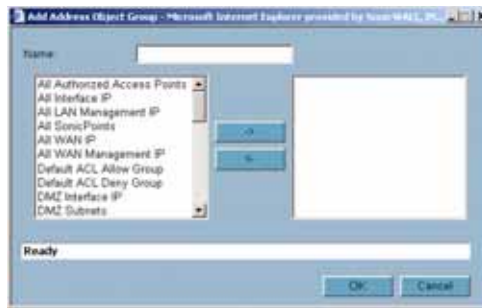
To edit an Address Object, click the edit icon  in the **Configure** column in the **Address Objects** table. The **Edit Address Object** window is displayed, which has the same settings as the **Add Address Object** window.

To delete an Address Object, click the Delete icon  in the **Configure** column for the Address Object you want to delete. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Object. To delete multiple active Address Objects, select them and click the **Delete** button.

Creating Group Address Objects

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


To add a Group of Address Objects, click **Add Group** to display the **Add Address Object Group** window.




- 1 Create a name for the group in the **Name** field.
- 2 Select the Address Object from the list and click the right arrow. It is added to the group. Clicking while pressing the Ctrl key allows you to select multiple objects.
- 3 Click **OK**.

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

Editing or Deleting Address Groups

To edit a group, click the edit icon  in the **Configure** column of the **Address Groups** table. The **Edit Address Object Group** window is displayed. Make your changes and then click **OK**.

To delete a group, click on the Delete icon  in the **Configure** column to delete an individual Address Group. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Group. To delete multiple active Address Groups, select them and click the **Delete** button.

Public Server Wizard

SonicOS Enhanced includes the **Public Server Wizard** to automate the process of configuring the SonicWALL security appliance for handling public servers. For example, if you have an e-mail and Web servers on your network for access from users on the Internet.



The **Public Server Wizard** allows you to select or define the server type (HTTP, FTP, Mail), the private (external) address objects, and the public (internal) address objects. Once the server type, private and public network objects are configured, the wizard creates the correct NAT Policies and Access Rule entries on the security appliance for the server. You can use the SonicWALL Management Interface for additional configuration options.



Cross Reference: See **Part 14, Wizards** for more information on configuring the SonicWALL security appliance using wizards.

Configuring Routes

Network > Routing

If you have routers on your interfaces, you can configure static routes on the SonicWALL security appliance on the **Network > Routing** page. You can create static routing policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables.

Route Advertisement

Interface (Zone)	Status	Configure
LAN (LAN)	Disabled	
WAN (WAN)	Disabled	
OPT (WLAN)	Disabled	
Modem (WAN)	Disabled	
WLAN (WLAN)	Disabled	

Route Policies

View 10 items (1 to 10 of 10) |

View 0/0: All Policies Custom Policies Default Policies

ID	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	255.255.255.255/32	Any	0.0.0.0	LAN	20	1		
2	Any	Default Gateway	Any	0.0.0.0	WAN	20	2		
3	Any	LAN Primary Subnet	Any	0.0.0.0	LAN	20	3		
4	Any	OPT Subnet	Any	0.0.0.0	OPT	20	4		
5	Any	WLAN Subnet	Any	0.0.0.0	WLAN	20	5		
6	Any	WAN Primary Subnet	Any	0.0.0.0	WAN	20	6		
7	Any	OPT DAT Subnet	Any	0.0.0.0	OPT	20	7		
8	Any	WLAN DAT Subnet	Any	0.0.0.0	WLAN	20	8		
9	WAN Primary Subnet	Any	Any	Default Gateway	WAN	20	9		
10	Any	0.0.0.0/0	Any	10.0.0.254	WAN	20	10		

Buttons: Add, Remove, Delete All

Status: Ready

Route Advertisement

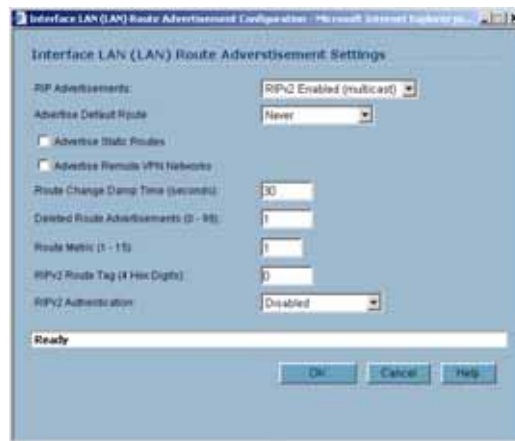
The SonicWALL security appliance uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the SonicWALL security appliance and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or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

Interface (Zone)	Status	Configure
LAN (LAN)	Disabled	
WAN (WAN)	Disabled	
OPT (WLAN)	Disabled	
Modem (WAN)	Disabled	
WLAN (WLAN)	Disabled	

Route Advertisement Configuration

To enable Route Advertisement for an Interface, follow these steps:

- 1 Click the **Notepad** icon in the **Configure** column for the interface. The **Route Advertisement Configuration** window is displayed.



- 2 Select one of the following types of RIP Advertisements:
 - ♦ **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
 - ♦ **RIPv2 Enabled (multicast)** - to send route advertisements using multicasting (a single data packet to specific nodes on the network).
 - ♦ **RIPv2 Enabled (broadcast)** - to send route advertisements using broadcasting (a single data packet to all nodes on the network).
- 3 In the **Advertise Default Route** menu, select **Never**, or **When WAN is up**, or **Always**.
- 4 Enable **Advertise Static Routes** if you have static routes configured on the SonicWALL security appliance, enable this feature to exclude them from Route Advertisement.
- 5 Enable **Advertise Remote VPN Networks** if you want to advertise VPN networks.
- 6 Enter a value in seconds between advertisements broadcasted over a network in the **Route Change Damp Time (seconds)** field. The default value is **30** seconds. A lower value corresponds with a higher volume of broadcast traffic over the network. The **Route Change Damp Time**

- (seconds)** setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of temporary change in the VPN tunnel status.
- 7 Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99)** field. The default value is **1**.
 - 8 Enter a value from 1 to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address.
 - 9 If RIPv2 is selected from the Route Advertisements menu, you can enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.
 - 10 If you want to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** menu:
 - ♦ **User defined** - Enter 4 hex digits in the Authentication Type (4 hex digits) field. Enter 32 hex digits in the Authentication Data (32 Hex Digits) field.
 - ♦ **Cleartext Password** - Enter a password in the Authentication Password (Max 16 Chars) field. A maximum of 16 characters can be used to define a password.
 - ♦ **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication Key-Id (0-255) field. Enter a 32 hex digit value for the Authentication Key (32 hex digits) field, or use the generated key.
 - 11 Click **OK**.

Route Policies

SonicOS Enhanced provides Policy Based Routing (PBR) to provide more flexible and granular traffic handling capabilities.

Policy Based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satisfies most static requirements, but is limited to forwarding based only on destination addressing.

Policy Based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS Enhanced PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

A metric is a weighted cost assigned to static and dynamic routes. Metrics have a value between 0 and 255. Lower metrics are considered better and take precedence over higher costs. SonicOS Enhanced adheres to Cisco defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

Metric Value	Description
1	Static Route
5	EIGRP Summary
20	External BGP
90	EIGRP

Metric Value	Description
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
Internal	BGP

Route Policies Table

You can change the view your route policies in the **Route Policies** table by selecting one of the view settings in the **View Style** menu.

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	255.255.255.255/32	Any	0.0.0.0	LAN	20	1		
2	Any	Default Gateway	Any	0.0.0.0	WAN	20	2		
3	Any	LAN Primary Subnet	Any	0.0.0.0	LAN	20	3		
4	Any	OPT Subnet	Any	0.0.0.0	OPT	20	4		
5	Any	WLAN Subnet	Any	0.0.0.0	WLAN	20	5		
6	Any	WAN Primary Subnet	Any	0.0.0.0	WAN	20	6		
7	Any	OPT DAT Subnet	Any	0.0.0.0	OPT	20	7		
8	Any	WLAN DAT Subnet	Any	0.0.0.0	WLAN	20	8		
9	WAN Primary Subnet	Any	Any	Default Gateway	WAN	20	9		
10	Any	0.0.0.0/0	Any	10.0.0.254	WAN	20	10		

All Policies displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **Route Policies** table provides easy pagination for viewing a large number of routing policies. You can navigate a large number of routing policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific routing policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

A Route Policy Example

The following example walks you through creating a route policy for two simultaneously active WAN interfaces. For this example, a secondary WAN interface needs to be setup on the **OPT** interface and configured with the settings from your ISP. Next, configure the security appliance for load balancing by checking the **Enable Load Balancing** on the **Network > WAN Failover & LB** page. For this example, choose **Per Connection Round-Robin** as the load balancing method in the **Network > WAN Failover & LB** page. Click **Apply** to save your changes on the **Network > WAN Failover & LB** page.

- 1 Click the **Add** button under the Route Policies table. The **Add Route Policy** window is displayed.



- 2 Create a routing policy that directs all **LAN Subnet** sources to **Any** destinations for **HTTP** service out of the **Default Gateway** via the **WAN** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force http out primary** into the **Comment** field. Click **OK**.
- 3 Create a second routing policy that directs all **LAN Subnet** sources to **Any** destinations for **Telnet** service out of the **Secondary Default Gateway** via the **Opt** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force telnet out backup** into the **Comment** field. Click **OK**.

These two policy-based routes force all sources from the LAN subnet to always go out the primary WAN when using any HTTP-based application, and forces all sources from the LAN subnet to always go out the backup WAN when using any Telnet-based application.

To test the HTTP policy-based route, from a computer attached to the LAN interface, access the public Web site <http://www.whatismyip.com> and <http://whatismyip.everdot.org>. Both sites display the primary WAN interface's IP address and not the secondary WAN interface.

To test the Telnet policy-based route, telnet to route-server.exodus.net and when logged in, issue the `who` command. It displays the IP address (or resolved FQDN) of the WAN IP address of the secondary WAN interface and not the primary WAN interface.

Advanced Routing Services

Advanced Routing Services (OSPF and RIP)

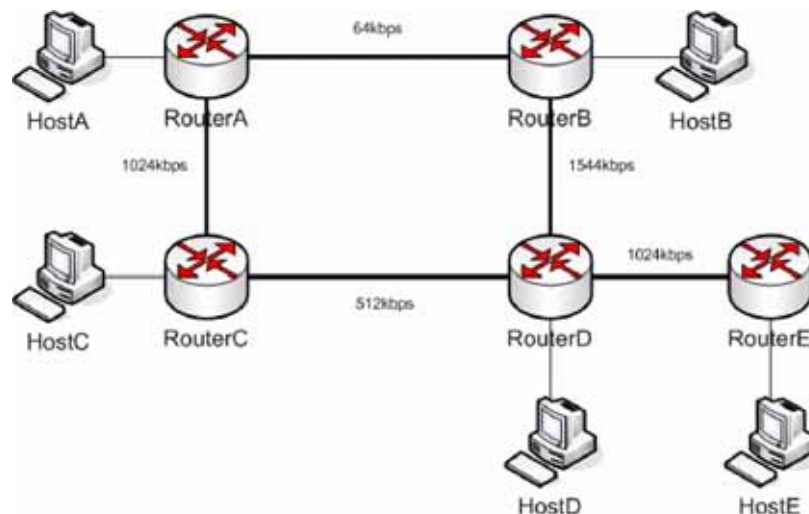
In addition to Policy Based Routing and RIP advertising, SonicOS Enhanced running on the PRO4060 and PRO5060 offers the option of enabling Advanced Routing Services (ARS). Advanced Routing Services provides full advertising and listening support for the Routing Information Protocol (RIPv1 - RFC1058) and (RIPv2 - RFC2453), and Open Shortest Path First (OSPFv2 - RFC2328).

Advanced Routing Service should only be enabled by those environments requiring support for either or both of these dynamic routing protocols.

RIP and OSPF are Interior Gateway Protocols (IGP) that are both widely used by networks of various sizes to automate the process of route distribution. RIP is commonly used within smaller networks, while OSPF is used by larger networks, although network size should not be the only factor used to determine the appropriateness of one protocol over the other – network speed, interoperability requirements, and relative overall complexity, for example, should also be considered. RIPv1 and RIPv2 are both supported by ARS, the largest differences between the two being that RIPv2 supports VLSM (Variable Length Subnet Masks), authentication, and routing updates. The following table illustrates the major differences between RIPv1, RIPv2, and OSPFv2:

	RIPv1	RIPv2	OSPFv2
Protocol metrics	Distance Vector	Distance Vector	Link State
Maximum Hops	15	15	Unlimited
Routing table updates	Full table broadcast periodically, slower convergence	Full table broadcast or multicast periodically, slower convergence	Link state advertisement multicasts, triggered by changes, fast convergence
Subnet Sizes Supported	Only class-based (a/b/c) subnets support	Class-based only	VLSM
Autonomous system topology	Indivisible and flat	Indivisible and flat	Area based, allowing for segmentation and aggregation

- Protocol Type – Distance Vector protocols such as RIP base routing metrics exclusively on hop counts, while Link state protocols such as OSPF consider the state of the link when determining metrics. For example, OSPF determines interface metrics by dividing its reference bandwidth (100mbits by default) by the interface speed – the faster the link, the lower the cost and the more preferable the path. Consider the following example network:



In the above sample network, if Host A wanted to reach Host B, with RIP, the lowest cost route would be from Router A to Router B, across the relatively slow 64kbps link. With OSPF, the cost

from Router A to Router B would be 1562, while the cost from Router A to Router C to Router D to Router B would be 364 (see the Cost section in OSPF concepts later), making it the preferred route.

- Maximum Hops – RIP imposes a hop count of 15 to help prevent routing loops which can occur when bad (e.g. stale) routing information is broadcast and propagated through a network either due to misconfiguration, or slow convergence. Consider if the link between Router D and Router E failed in the diagram above, and there were no safeguards in place:
 - ♦ Router A's routing information states that it can reach Network E through Router B or Router C with a metric of 3.
 - ♦ When the link between Router D and Router E fail, and Router A broadcasts its routing information, Router B and Router C determine that they can reach Network E through Router A with a metric of 4.
 - ♦ Router B and Router C broadcast this information, and it is received by Router D which then determines it can reach Network E through Router B or Router C with a metric of 5.
 - ♦ This loop continues until the hop count of 16 (infinity) is reached.

Other measures against this sort of situation are also commonly employed by RIP, including:

- ♦ Split-Horizon – A preventative mechanism where routing information learned through an interface is not sent back out the same interface. This generally works well on broadcast links, but not on non-broadcast links such as Frame Relay, where a single link can commonly be used to reach two separate autonomous systems.
- ♦ Poison reverse – Also known as route poisoning, an extension of split-horizon where a network is advertised with a metric of 16 (unreachable), helping to ensure that incorrect alternative routes aren't propagated.

OSPF does not have to impose a hop count limit because it does not advertise entire routing tables, rather it generally only sends link state updates when changes occur. This is a significant advantage in larger networks in that it converges more quickly, produces less update traffic, and supports an unlimited number of hops.

- Routing table updates – As mentioned above, the practice of sending an entire routing table introduces the problems of slower convergences, higher bandwidth utilization, and increased potential for stale routing information. RIPv1 broadcasts its entire routing table at a prescribed interval (usually every 30 seconds), RIPv2 can either broadcast or multicast, and OSPF multicasts only link state updates whenever a change to the network fabric occurs. OSPF has a further advantage of using designated routers (DR) in forming adjacencies in multiple-access networks (more on these concepts later) so that updates don't have to be sent to the entire network.
- Subnet sizes supported – RIPv1 was first implemented when networks were strictly class A, class B, and class C (and later D and E):
 - ♦ Class A – 1.0.0.0 to 126.0.0.0 (0.0.0.0 and 127.0.0.0 are reserved)
 - Leftmost bit 0; 7 network bits; 24 host bits
 - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8 bit classful netmask)
 - 126 Class A networks, 16,777,214 hosts each
 - ♦ Class B - 128.0.0.0 to 191.255.0.0
 - Leftmost bits 10; 14 network bits; 16 host bits
 - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16 bit classful netmask)
 - 16,384 Class B networks, 65,532 hosts each
 - ♦ Class C – 192.0.0.0 to 223.255.255.0
 - Leftmost bits 110; 21 network bits; 8 host bits
 - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24 bit classful netmask)
 - 2,097,152 Class Cs networks, 254 hosts each
 - ♦ Class D - 224.0.0.0 to 239.255.255.255 (multicast)

- Leftmost bits 1110; 28 multicast address bits
- 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
- ◆ Class E - 240.0.0.0 to 255.255.255.255 (reserved)
 - Leftmost bits 1111; 28 reserved address bits
 - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

This method of address allocation proved to be very inefficient because it provided no flexibility, neither in the way of segmentation (subnetting) or aggregation (supernetting, or CIDR – classless inter-domain routing) by means of VLSM – variable length subnet masks.

VLSM, supported by RIPv2 and OSPF, allows for classless representation of networks to break larger networks into smaller networks:

For example, take the classful 10.0.0.0/8 network, and assign it a /24 netmask. This subnetting allocates an additional 16 bits from the host range to the network range ($24-8=16$). To calculate the number of additional networks this subnetting provides, raise 2 to the number of additional bits: $2^{16}=65,536$. Thus, rather than having a single network with 16.7 million hosts (usually more than most LAN's require) it is possible to have 65,536 networks, each with 254 usable hosts.

VLSM also allows for route aggregation (CIDR):

For example, if you had 8 class C networks: 192.168.0.0/24 through 192.168.7.0/24, rather than having to have a separate route statement to each of them, it would be possible to provide a single route to 192.168.0.0/21 which would encompass them all.

This ability, in addition to providing more efficient and flexible allocation of IP address space, also allows routing tables and routing updates to be kept smaller.

- Autonomous system topologies – An autonomous system (AS) is a collection of routers that are under common administrative control, and that share the same routing characteristics. When a group of autonomous systems share routing information, they are commonly referred to as a confederation of autonomous systems. (RFC1930 and RFC975 address these concepts in much greater detail). In simple terms, an AS is a logical distinction that encompasses physical network elements based on the commonness of their configurations.

With regard to RIP and OSPF, RIP autonomous systems cannot be segmented, and all routing information must be advertised (broadcast) through the entire AS. This can become difficult to manage and can result in excessive routing information traffic. OSPF, on the other hand, employs the concept of Areas, and allows for logically, manageable segmentation to control the sharing of information within an AS. OSPF areas begin with the backbone area (area 0 or 0.0.0.0), and all other areas must connect to this backbone area (although there are exceptions). This ability to segment the routing AS helps to ensure that it never becomes too large to manage, or too computationally intensive for the routers to handle.

OSPF Terms

OSPF is substantially more complicated to configure and maintain than RIP. The following concepts are critical to understanding an OSPF routing environment:

- Link state – As it pertains to OSPF, a link is an egress interface on a router, and the state describes characteristics of that interface, such as its cost. Link states are sent in the form of Link State Advertisements (LSA) which are contained within Link State Update (LSU) packets, one of five types of OSPF packets.
- Cost – A quantification of the overhead required to send a packet along a particular link. Cost is calculated by dividing a reference bandwidth (usually 100mbit, or 10^8 bit) by an interface's speed. The lower the cost, the more preferable the link. Some common path costs:

Interface	Divided by 10^8 (100mbit) = OSPF Cost
Fast Ethernet	1
Ethernet	10
T1 (1.544mbit)	64
DSL (1mbit)	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

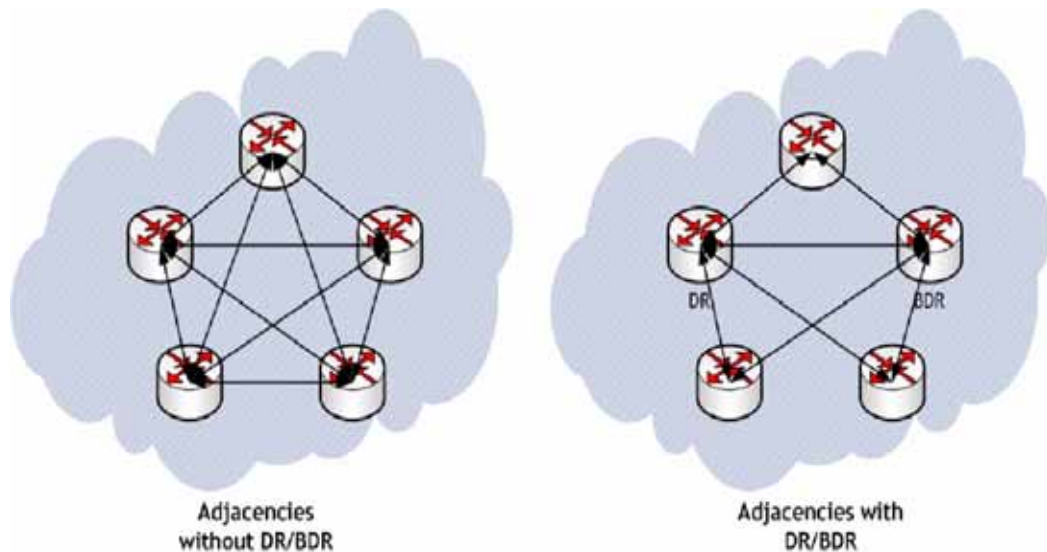
- Area – The network comprising the group of OSPF routers intended to share a common Link State Database. OSPF networks are built around the backbone area (area 0, or 0.0.0.0) and all other areas must connect to the backbone area (unless virtual links are used, which is generally discouraged). Area assignment is interface specific on an OSPF router; in other words, a router with multiple interfaces can have those interfaces configured for the same or different areas.
- Neighbors – OSPF routers on a common network segment have the potential to become neighbors by means of sending Hello packets. Hello packets act as a form of advertisement and identification, and if two OSPF routers share a common set of certain characteristics, they will become neighbors upon seeing their own router ID in the other router's Hello packet. Hello packets are also used in the *DR* (Designated Router) and *BDR* (Backup Designated Router) election process. For two routers to become neighbors, the characteristics that they must have in common are:
 - ♦ Area-ID – An area ID identifies an OSPF *area* with a 32 bit value, and is generally represented in an IP address format. OSPF requires at a minimum the backbone area, area 0 (or 0.0.0.0) for operation.
 - ♦ Authentication – Authentication types can generally be set to none, simple text, or MD5. When using simple text, it should only be used for identification purposes, since it is sent in the clear. For security, MD5 should be used.
 - ♦ Timer intervals – 'Hello' and 'Dead' intervals must be the same. The Hello interval specifies the number of seconds between Hello packets (as a Keepalive function), and the Dead interval specifies the number of seconds after which a router will be considered unavailable if a Hello is not received.
 - ♦ Stub area flag – A *Stub area* is an area that only requires a single point of egress, and therefore does not require a full list of external link advertisements. The stub area flag on two potential neighbors must be the same to avoid inappropriate link state exchanges.

Another factor that affects neighboring is the kind of network. OSPF recognizes three network types:

- ♦ Broadcast – For example, Ethernet. In broadcast networks, neighboring can be established with all other routers in the broadcast domain.
- ♦ Point to Point – For example, serial links. In point to point (or point to multipoint) networks, neighboring can be established with the router at the other end of the link.
- ♦ NBMA (non-broadcast multiple access) – For example, frame relay. In NBMA networks, neighbors must be explicitly declared.
- Link State Database – The Link State Database is composed of the LSA's sent and received by *neighboring* OSPF routers that have created *adjacencies* within an *area*. The database, once complete, will contain all the link state information for a given area, at which time the Shortest Path First (SPF) algorithm will be applied to determine the optimal route to all connected networks based on cost. The SPF algorithm employs the Dijkstra pathfinding algorithm, which essentially regards all routers as vertices in a graph, and computes the cost between each vertex.

- Adjacencies – OSPF routers exchange LSA's with adjacent routers to create the LSDB. Adjacencies are created in different fashions depending on the network type (see Neighbors section above). Generally, the network type is broadcast (e.g. Ethernet) so adjacencies are formed by the exchanging OSPF packets in a handshake-like fashion (see OSPF Packet types below). To minimize the amount of information exchanged between adjacent routers, segments (broadcast domains) with multiple OSPF routers elect a Designated Router (DR) and a Backup Designated Router (BDR) using Hello packets.
- DR (Designated Router) – On multi-access segments, OSPF routers elect a DR and a BDR, and all other routers on the segment create adjacencies with the DR and the BDR. DR election is based on a router's OSPF Priority, which is a configurable value from 0 (not eligible for DR) to 255. The router with the highest priority becomes the DR. In the event of a priority tie, the router with the highest Router ID (based on interface addressing) wins. Once a router is the DR, its role is uncontested, until it becomes unavailable.

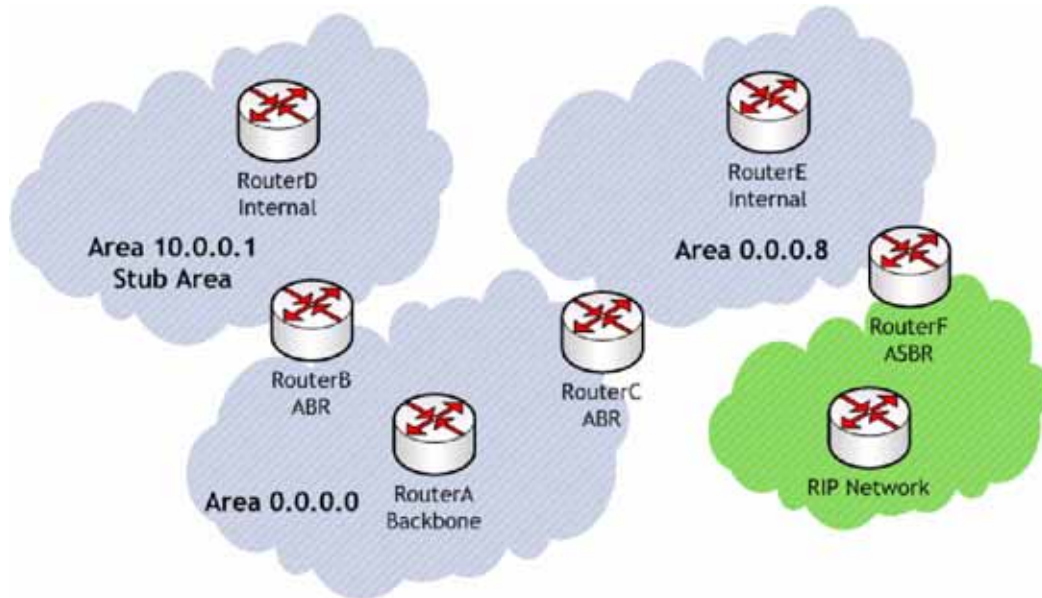
LSA's are then exchanged within LSU's across these adjacencies rather than between each possible pairing combination of routers on the segment. Link state updates are sent by non-DR routers to the multicast address 224.0.0.6, the RFC1583 assigned 'OSPFIGP Designated Routers' address. They are also flooded by DR routers to the multicast address 224.0.0.5 'OSPFIGP All Routers' for all routers to receives the LSA's.



- OSPF Packet types – The five types of OSPF packets are:
 - ♦ Hello (OSPF type 1) – Sent at a certain interval to establish and maintain relationships with neighboring OSPF routers, and elect Designated Routers. (*Sent during the initialization and the 2-WAY phases on LSDB synchronization*).
 - ♦ Database Description (OSPF type 2) – Sent between OSPF routers during the creation of an adjacency. *During the Exstart phase of LSDB synchronization*, DD packets establish an ISN (initial sequence number) used to track LSA's, and they establish a master/slave relationship between neighboring OSPF routers. *In the Exchange phase of LSDB synchronization*, they contain short versions of Link State Advertisements. Because DD exchanges can span multiple packets, they are exchanged in a poll (master) and response (slave) fashion to ensure completeness.
 - ♦ Link State Request (OSPF type 3) – *During the Loading phase of LSDB synchronization*, LSR packets are sent to request database updates from a neighbor. This is the final step in the establishment of an adjacency.
 - ♦ Link State Update (OSPF type 4) – Sent in response to Link State Requests, LSU packets flood adjacencies with Link State Advertisements to achieve LSDB synchronization.

- ♦ Link State Acknowledgement (OSPF type 5) – To ensure reliability of LSA flooding, all updates are acknowledged.
- Link State Advertisements (LSA) – There are 7 types of LSA's:
 - ♦ Type 1 (Router Link Advertisements) - Sent by an OSPF router to describe the links to each area to which it belongs. Type 1 LSA's are only flooded into a router's area.
 - ♦ Type 2 (Network Links Advertisements) – Sent by the DR for an area describing the set of routers within the network. Type 2 LSA's are only flooded into a router's area.
 - ♦ Type 3 (Summary Link Advertisements) – Sent across areas by ABR's (Area Border Routers) to describe the networks within an area. Type 3 LSA's are also used for route aggregation purposes, and are not sent to Totally Stubby Areas.
 - ♦ Type 4 (AS Summary Link Advertisements) – Sent across areas by ABR's to describe networks within a different AS. Type 4 LSA's are not sent to Stub Areas.
 - ♦ Type 5 (AS External Link Advertisements) – Sent by ASBR (Autonomous System Boundary Routers) to describe routes to networks in a different AS. Type 5 LSA's are not sent to Stub Areas. There are two types of External Link Advertisements:
 - External Type 1 - Type 1 packets add the internal link cost to the external link cost when calculating a link's metric. A Type 1 route is always preferred over a Type 2 route to the same destination.
 - External Type 2 - Type 2 packets only use the external link cost to determine the metric. Type 2 is generally used when there is only one path to an external AS.
 - ♦ Type 6 (Multicast OSPF) - Spooky. See RFC1584.
 - ♦ Type 7 (NSSA AS External Link Advertisements) – Sent by ASBR's that are part of an NSSA (see 'Stub Area').
- Stub Area – A stub area is an area that only requires one path, rather than an optimal path. This can be an area with only a single point of egress, or it can be an area where SPF optimization is not necessary. All routers in a stub area must be configured as stub routers, and rather than receiving the full state database, and computing the SPF tree, they will receive only a summary link information. There are different type of stub area:
 - ♦ Stub area – The standard stub area receives all LSA's except for LSA type 5 (AS External Link advertisement). This helps to keep the LSDB smaller, and reduces the computational overhead on the router.
 - ♦ Totally Stubby Area – A special type of stub area into which LSA types 3 (Summary Links), 4 (AS Summary Links) and 5 are not passed. Only intra-area routes, and a default route are advertised into totally stubby areas.
 - ♦ NSSA (Not So Stubby Area) – Described by RFC3101, NSSA is a hybrid stub area that allows external routes to be flooded within the NSSA area using type 7 LSA's (NSSA AS External Routes), but does not accept type 5 LSA's from other areas. NSSA's are useful when connecting a remote site running a different IGP (such as RIP) to an OSPF site, where the remote site's routes do not need to be distributed back to the main OSPF site. An NSSA ABR (Area Border Router) also has the ability to translate type 7 to type 5 LSA's (this is possible only from the SonicOS Enhanced CLI).

- Router Types – OSPF recognizes 4 types of routers, based on their roles:



- ♦ IR (Internal Router) - A router whose interfaces are all contained within the same area. An internal router's LSDB only contains information about its own area.
- ♦ ABR (Area Border Router) – A router with interfaces in multiple areas. An ABR maintains LSDB's for each area to which it is connected, one of which is typically the backbone.
- ♦ Backbone Router – A router with an interface connected to area 0, the backbone.
- ♦ ASBR (Autonomous System Boundary Router) – A router with an interface connected to a non-OSPF AS (such as a RIP network) which advertises external routing information from that AS into the OSPF AS.

Configuring Advanced Routing Services



Note: ARS is a fully featured multi-protocol routing suite. The sheer number of configurable options and parameters provided is incongruous with the simplicity of a graphical user interface. Rather than limiting the functionality of ARS, an abbreviated representation of its capabilities has been rendered in the GUI, providing control over the most germane routing features, while the full command suite is available via the CLI. The ARS CLI can be accessed from an authenticated CLI session, and contains 3 modules:

- **route ars-nsm** – The Advanced Routing Services Network Services Module. This component provides control over core router functionality, such as interface bindings and redistributable routes.
- **route ars-rip** – The RIP module. Provides control over the RIP router.
- **route ars-ospf** – The OSPF module. Provides control over the OSPF router.

In general, all of the functionality needed to integrate the SonicWALL into most RIP and OSPF environments is available through the web-based GUI. The additional capabilities of the CLI will make more advanced configurations possible. Please refer to the appendix for the full set of ARS CLI commands.

By default, Advanced Routing Services are disabled, and must be enabled to be made available. At the top of the 'Network>Routing' page, is a checkbox 'Use Advanced Routing'. Toggling the state of

this checkbox will require a reboot for the changes to take effect. When the SonicWALL is running in Advanced Routing mode, the top of the 'Network>Routing' page will look as follows:

Interface (Zone)	RIP	Configure RIP	OSFPv2	Configure OSFP	OSFP Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Disabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (RA)	RIP Disabled		OSPF Disabled		
X3 (RA)	RIP Disabled		OSPF Disabled		
X3:V1 (DMZ)	RIP Disabled		OSPF Disabled		
X4 (MLAN)	RIP Disabled		OSPF Disabled		
X5 (RA)	RIP Disabled		OSPF Disabled		

The operation of the RIP and OSPF routing protocols is interface dependent. Each interface and virtual sub-interface can have RIP and OSPF settings configured separately, and each interface can run both RIP and OSPF routers.

Apply the following metric to default routes received from Advanced Routing protocols:

Configuring RIP

To configure RIP routing on an interface, select the (Configure) icon in the interface's row under the "Configure RIP" column. This will launch the following window:

RIP Modes

- Disabled – RIP is disabled on this interface
- Send and Receive – The RIP router on this interface will send updates and process received updates.
- Send Only – The RIP router on this interface will only send updates, and will not process received updates. This is similar to the basic routing implementation.

- Receive Only – The RIP router on this interface will only process received updates.
- Passive – The RIP router on this interface will not process received updates, and will only send updates to neighboring RIP routers specified with the CLI 'neighbor' command. This mode should only be used when configuring advanced RIP options from the ars-rip CLI.

Receive (Available in 'Send and Receive' and 'Receive Only' modes)

- RIPv1 – Receive only *broadcast* RIPv1 packets.
- RIPv2 – Receive only *multicast* RIPv2 packets. RIPv2 packets are sent by multicast, although some implementations of RIP routers (including basic routing on SonicWALL devices) have the ability to send RIPv2 in either broadcast or multicast formats.



Note: Be sure the device sending RIPv2 updates uses multicast mode, or the updates will not be processed by the ars-rip router.

Send (Available in 'Send and Receive' and 'Send Only' modes)

- RIPv1 – Send *broadcast* RIPv1 packets.
- RIPv2 - v1 compatible – Send *multicast* RIPv2 packets that are compatible with RIPv1.
- RIPv2 – Send *multicast* RIPv2 packets.

Split Horizon – Enabling Split Horizon will suppress the inclusion of routes sent in updates to routers from which they were learned. This is a common RIP mechanism for preventing routing loops. See the 'maximum hops' entry at the start of Advanced Routing Services section.

Poisoned Reverse – Poison reverse is an optional mode of Split Horizon operation. Rather than suppressing the inclusion of learned routes, the routes are sent with a metric of infinity (16) thus indicating that they are unreachable. See the 'maximum hops' entry at the start of Advanced Routing Services section.

Use Password – Enables the use of a plain-text password on this interface, up to 16 alpha-numeric characters long, for identification.

Default Metric – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, OSPF, or VPN) routing information sources. The default value (undefined) is 1 and the maximum is 15.

Administrative Distance – The administrative distance value is used by routers in selecting a path when there is more than one route to a destination, with the smaller distance being preferred. The default value is 120, minimum is 1, and maximum is 255.

Originate Default Route – This checkbox enables or disables the advertising of the SonicWALL's default route into the RIP system.

Redistribute Static Routes – Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

Redistribute Connected Networks - Enables or disables the advertising of locally connected networks into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

Redistribute OSPF Routes - Enables or disables the advertising of routes learned via OSPF into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

Redistribute Remote VPN Networks - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

Routes learned via RIP will appear in the Route Policies table as 'OSPR or RIP routes':

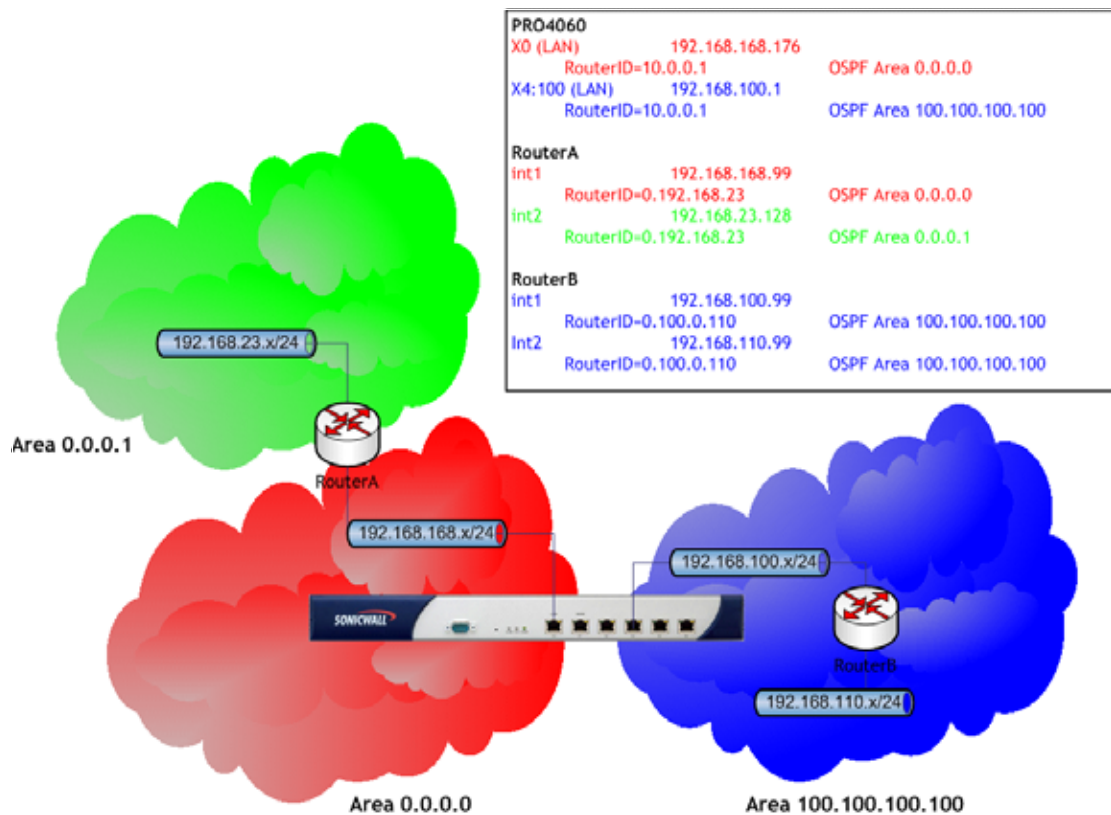
<input type="checkbox"/>	4	Any	88.182.95.84/27	Any	10.50.165.1	X2	120	4		
<input type="checkbox"/>	5	Any	LAN Primary Subnet	Any	0.0.0.0	X0			Comment	X0 OSPF or RIP Route

Configuring OSPF




Note: OSPF design concepts are beyond the scope of this document. The following section describes how to configure a SonicWALL to integrate into an OSPF network, be it existing or newly implemented, but it does not offer design guidelines. For terms used throughout this section, refer to the 'OSPF Terms' section above.

Consider the following simple example network:



The diagram illustrates an OSPF network where the backbone (area 0.0.0.0) comprises the X0 interface on the SonicWALL and the int1 interface on Router A. Two additional areas, 0.0.0.1 and 100.100.100.100 are connected, respectively, to the backbone via interface int2 on ABR Router A, and via the X4:100 VLAN sub-interface on the SonicWALL.

To configure OSPF routing on the X0 and the X4:100 interfaces, select the  (Configure) icon in the interface's row under the "Configure OSPF" column. This will launch the following window:

OSPFv2 Setting

- Disabled – OSPF Router is disabled on this interface
- Enabled – OSPF Router is enabled on this interface
- Passive – The OSPF router is enabled on this interface, but only advertises connected networks using type 1 LSA's (Router Link Advertisements) into the local area. This is different from the 'Redistribute Connected Networks' options, which would cause the OSPF router to behave as an ASBR, and to use type 5 LSA's (AS External Link Advertisement) to flood the advertisements into all non-stub areas. See the 'OSPF Terms' section for more information.

Dead Interval – The period after with an entry in the LSDB is removed if not Hello is received. The default is 40 seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

Hello Interval – The period of time between Hello packets. The default is 10 seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

Authentication - Be sure this setting agrees with the other OSPF routers on the segment for successful neighbor establishment.

- Disabled – No authentication is used on this interface.
- Simple Password – A plain-text password is used for identification purposes by the OSPF router on this interface.
- Message Digest – An MD5 hash is used to securely identify the OSPF router on this interface.

OSPF Area – The OSPF Area can be represented in either IP or decimal notation. For example, you may represent the area connected to X4:100 as either 100.100.100.100 or 1684300900.

OSPFv2 Area Type – See the 'OSPF Terms' section above for a more detailed description of these settings.

- Normal – Receives and sends all applicable LSA types.
- Stub Area – Does not receive type 5 LSA's (AS External Link Advertisements)
- Totally Stubby Area – Does not receive LSA types 3, 4, or 5.
- Not So Stubby Area – Receives type 7 LSA's (NSSA AS External Routes).

Interface Cost – Specifies the overhead of sending packets across this interface. The default value is 10, generally used to indicate an Ethernet interface. The minimum value is 1 (e.g. Fast Ethernet) and the maximum value is 65,535 (e.g. pudding).

Router Priority – The router priority value is used in determining the Designated Router (DR) for a segment. The higher the value, the higher the priority. In the event of a priority tie, the Router ID will act as the tie-breaker. Setting a value of 0 makes the OSPF router on this interface ineligible for DR status. The default value is 1, and the maximum value is 255.

OSPF Router ID – The Router ID can be any value, represented in IP address notation. It is unrelated to the any of the IP addresses on the SonicWALL, and can be set to any *unique* value within your OSPF network.

ABR Type – Allows for the specification of the topology with which this OSPF router will be participating, for the sake of compatibility. The options are:

- Standard – Full RFC2328 compliant ABR OSPF operation.
- Cisco – For interoperating with Cisco's ABR behavior, which expects the backbone to be configured and active before setting the ABR flag.
- IBM – For interoperating with IBM's ABR behavior, which expects the backbone to be configured before settings the ABR flag.
- Shortcut – A 'shortcut area' enables traffic to go through the non-backbone area with a lower metric whether or not the ABR router is attached to area 0.

Default Metric – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, RIP, or VPN) routing information sources. The default value (undefined) is 1 and the maximum is 16,777,214.

Originate Default Route – Controls the advertising of the SonicWALL security appliance's default route into the OSPF system on this interface. The options are:

- Never – Disables advertisement of the default route into the OSPF system.
- When WAN is up – Advertises the default route into the OSPF system when the WAN is online. The default route is always advertised as an External Type 2 using LSA Type 5.
- Always – Enables advertisement of the default route into the OSPF system. The default route is always advertised as an External Type 2 using LSA Type 5.



Note: *The following applies to all Redistributed routes: The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting. An optional route tag value can be added to help other routers identify this redistributed route (the default tag value is 0). The redistributed route advertisement will be an LSA Type 5, and the type may be selected as either Type 1 (adds the internal link cost) or Type 2 (only uses the external link cost).*

Redistribute Static Routes – Enables or disables the advertising of static (Policy Based Routing) routes into the OSPF system.

Redistribute Connected Networks - Enables or disables the advertising of locally connected networks into the OSPF system.

Redistribute RIP Routes - Enables or disables the advertising of routes learned via RIP into the OSPF system.

Redistribute Remote VPN Networks - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system.

The Routing Protocols section will show the status of all active OSPF routers by interface:

Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Enabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (WLAN)	RIP Disabled		OSPF Disabled		
X3 (LAN)	RIP Disabled		OSPF Disabled		
X4 (WAN)	RIP Disabled		OSPF Disabled		
▶ X4-V100 (LAN)	RIP Disabled		OSPF Enabled		
▶ X4-V150 (Sales)	RIP Disabled		OSPF Disabled		
▶ X4-V250 (Engineering)	RIP Disabled		OSPF Disabled		
X5 (WAN)	RIP Disabled		OSPF Disabled		

The and Status LED's indicate whether or not there are active neighbors, and can be clicked on for more detail:

Router-ID	Current State	Priority	IP Address
0.192.168.23	Full / DR	1	192.168.168.99

The Routing Policies section will show routes learned by OSPF as 'OSPF or RIP Routes':

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	192.168.110.0/24	Any	192.168.100.99		110	11		
2	Any	192.168.23.0/24	Any	192.168.168.99	X1	110	10		
3	Any	WAN Primary Subnet	Any	0.0.0.0	X1				

Configuring NAT Policies

Network > NAT Policies

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to allow all systems connected to the **LAN** interface to perform many-to-one NAT using the IP address of the **WAN** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. This chapter explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with an the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester's IP address, the protocol information of the requestor, and the destination's IP address. The NAT Policies engine in SonicOS Enhanced can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 NAT Policies on a SonicWALL security appliance running SonicOS Enhanced, and they can be as granular as you need. It's also possible to create multiple NAT policies for the same object – for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

NAT Policies Table

The **NAT Policies** table allows you to view your NAT Policies by **Custom Policies**, **Default Policies**, or **All Policies**.

#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound				
1	Any	Original	X3/V100 IP	Original	HTTPS Management	Original	X3/V100	X3/V100	1		✓	
2	Any	Original	X3/V100 IP	Original	HTTP Management	Original	X3/V100	X3/V100	2		✓	
3	All Interface IP	X1 IP	Any	Original	Any	Original	Any	X1	3		✓	
4	Any	Original	X3/V20 IP	Original	HTTPS Management	Original	X3/V20	X3/V20	4		✓	
5	Any	Original	X3/V20 IP	Original	HTTP Management	Original	X3/V20	X3/V20	5		✓	
6	Any	Original	X4 IP	Original	HTTPS Management	Original	X4	X4	6		✓	
7	Any	Original	X4 IP	Original	HTTP Management	Original	X4	X4	7		✓	
8	Any	Original	X1 IP	Original	HTTPS Management	Original	X1	X1	8		✓	
9	Any	Original	X1 IP	Original	HTTP Management	Original	X1	X1	9		✓	
10	Any	Original	X0 IP	Original	Ping	Original	X0	X0	10		✓	
11	Any	Original	X0 IP	Original	HTTPS Management	Original	X0	X0	11		✓	
12	Any	Original	X0 IP	Original	HTTP Management	Original	X0	X0	12		✓	
13	Any	X1 IP	Any	Original	Any	Original	X3/V100	X1	13		✗	
14	Any	X1 IP	Any	Original	Any	Original	X3/V20	X1	14		✗	
15	Any	X1 IP	Any	Original	Any	Original	X4	X1	15		✗	
16	Any	X1 IP	Any	Original	Any	Original	X0	X1	16		✗	
17	Any	Original	Any	Original	Any	Original	Any	Any	17		✓	

#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound				
1	WAN Interface IP	Original	Any	Original	WE	Original	Any	Any	1		✓	
2	Any	Original	WAN Interface IP	Original	WE	Original	Any	Any	2		✓	
3	WAN Interface IP	Original	Any	Original	WE	Original	Any	Any	3		✓	
4	Any	Original	WAN Interface IP	Original	WE	Original	Any	Any	4		✓	
5	Any	Original	GPT IP	Original	HTTPS Management	Original	GPT	GPT	5		✓	
6	Any	Original	GPT IP	Original	HTTP Management	Original	GPT	GPT	6		✓	
7	Any	Original	WAN Poman IP	Original	SNMP	Original	WAN	WAN	7		✓	
8	Any	Original	WAN Poman IP	Original	Ping	Original	WAN	WAN	8		✓	

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



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

Navigating and Sorting NAT Policy Entries

You can change the view your route policies in the **NAT Policies** table by selecting one of the view settings in the **View Style** menu. **All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **NAT Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed in the **#** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

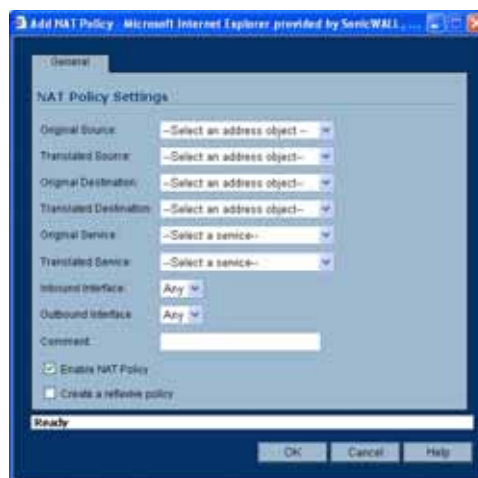
Moving your pointer over the Comment icon in the **Configure** column of **NAT Policies** table displays the comments entered in the **Comments** field of the **Add NAT Policy** window.

Moving your pointer over the Statistics icon in the **Configure** column of **NAT Policies** table displays traffic statistics for the NAT policy.

Clicking the Delete icon (trashcan) deletes the NAT Policy entry. If the icon is dimmed, the NAT Policy is a default entry and you cannot delete it.

NAT Policy Settings Explained

The following explains the settings used to create a NAT policy entry in the **Add NAT Policy** or **Edit NAT Policy** windows.



Click the **Add** button in the **Network > NAT Policies** page to display the **Add NAT Policy** window to create a new NAT policy or click the Edit icon in the **Configure** column for the NAT policy you want to edit to display the **Edit NAT Policy** window.

- **Original Source:** This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the SonicWALL security appliance, whether it's across interfaces, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects. These entries can be single host entries, address ranges, or IP subnets.
- **Translated Source:** This drop-down menu setting is what the SonicWALL security appliance translates the specified **Original Source** to as it exits the SonicWALL security appliance, whether it's to another interface, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects entries. These entries can be single host entries, address ranges, or IP subnets.
- **Original Destination:** This drop-down menu setting is used to identify the Destination IP address(es) in the packet crossing the SonicWALL security appliance, whether it be across interfaces, or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Any** since the destination of the packet is not being changed, but the source is being changed. However, these Address Object entries can be single host entries, address ranges, or IP subnets.
- **Translated Destination:** This drop-down menu setting is what the SonicWALL translates the specified **Original Destination** to as it exits the SonicWALL security appliance, whether it's to another interface, or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Original**, since the destination of the packet is not being changed, but the source is being changed. However, these Address Objects entries can be single host entries, address ranges, or IP subnets.
- **Original Service:** This drop-down menu setting is used to identify the IP service in the packet crossing the SonicWALL security appliance, whether it's across interfaces, or into/out-of VPN tunnels. You can use the default services on the SonicWALL, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.
- **Translated Service:** This drop-down menu setting is what the SonicWALL security appliance translates the **Original Service** to as it exits the SonicWALL security appliance, whether it be to another interface, or into/out-of VPN tunnels. You can use the default services in the SonicWALL security appliance, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.
- **Inbound Interface:** This drop-down menu setting is used to specify the entry interface of the packet. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces.
- **Outbound Interface:** This drop-down is used to specify the exit interface of the packet once the NAT policy has been applied. This field is mainly used for specifying which WAN interface to apply the translation to. Of all fields in NAT policy, this one has the most potential for confusion. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces. Also, as noted in the Quick Q&A' section of this chapter, when creating inbound 1-2-1 NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.
- **Comment:** This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Network > NAT Policies** page by running the mouse over the text balloon next to the NAT policy entry. Your comment appears in a pop-up window as long as the mouse is over the text balloon.
- **Enable NAT Policy:** By default, this box is checked, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, uncheck this box.
- **Create a reflective policy:** When you check this box, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** window is automatically created.

NAT Policies Q&A

Why is it necessary to specify 'Any' as the destination interface for inbound 1-2-1 NAT policies?

It may seem counter-intuitive to do this, given that other types of NAT policies require you to specify the destination interface, but for this type of NAT policy, this is what is necessary. The SonicWALL security appliance uses this field during the NAT Policy lookup and validates it against the packet that it receives, but if this is set to some internal interface such as LAN, the lookup fails because at that point, the SonicWALL security appliance does not know that the packet is going to LAN. It's not until after the SonicWALL security appliance performs the NAT Policy lookup that it knows that the packet is going to LAN. At the precise time that the SonicWALL security appliance does the NAT Policy lookup, the packet looks like it is going from WAN -> WAN (or whatever interface it is coming in on), since doing a route lookup on the NAT Public address returns the Public interface.

Can I manually order the NAT Policies?

No, the SonicWALL security appliance automatically orders them, depending on the granularity of the rule. This means that you can create NAT policy entries for the same objects, if each policy has more granularity than the existing policy. For example, you can create a NAT policy to translate all LAN systems to the WAN IP Address, then create a policy saying that a specific system on that LAN use a different IP address, and additionally, create a policy saying that specific use another IP address when using HTTP.

Can I have multiple NAT policies for the same objects?

Yes – please read the section above.

What are the NAT 'System Polices'?

On the **Network > NAT Policies** page, notice a radio button labeled **System Polices**. If you choose this radio button, the NAT Polices page displays all of the default, auto-created NAT policies for the SonicWALL security appliance. These policies are default settings for the SonicWALL security appliance to operate properly, and cannot be deleted. For this reason, they are listed in their own section, in order to make the user-created NAT policies easier to browse. If you wish to see user-created NAT policies along with the default NAT policies, simply check the radio button next to 'All Policies'.

Can I write NAT policies for VPN traffic?

Yes, this is possible if both sides of the VPN tunnel are SonicWALL security policies running SonicOS Enhanced firmware. Please refer to the technote **SonicOS Enhanced NAT VPN Overlap** for instructions on how to perform NAT on traffic entering and exiting VPN tunnels. Available at <http://www.sonicwall.com/services/documentation.html>.

Why do I have to write two policies for 1-2-1 traffic?

With the new NAT engine, it's necessary to write two policies – one to allow incoming requests to the destination public IP address to reach the destination private IP address (uninitiated inbound), and one to allow the source private IP address to be remapped to the source public IP address (initiated outbound). It takes a bit more work, but it's a lot more flexible.

Creating NAT Policies

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

For this chapter, the examples use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **LAN**
- 67.115.118.64/27 IP subnet on interface **WAN**
- 192.168.30.0/24 IP subnet on interface **Opt**
- **LAN** IP address is 192.168.10.1
- **WAN** IP address is 67.115.118.68
- **Opt** 'Sales' IP address is 192.168.30.1
- Webserver's "private" address at 192.168.30.200
- Webserver's "public" address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Creating a Many-to-One NAT Policy

Many-to-One is the most common NAT policy on a SonicWALL security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you're taking an internal "private" IP subnet and translating all outgoing requests into the IP address of the SonicWALL security appliance WAN port, such that the destination sees the request as coming from the IP address of the SonicWALL security appliance WAN port, and not from the internal private IP address.

This policy is easy to set up and activate. From the Management Interface, go to the **Network > NAT Policies** page and click on the **Add** button. The **Add NAT Policy** window is displayed for adding the policy. To create a NAT policy to allow all systems on the **Opt** interface to initiate traffic using the SonicWALL security appliance's WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** Opt Subnet
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. This policy can be duplicated for subnets behind the other interfaces of the SonicWALL security appliance – just replace the **Original Source** with the subnet behind that interface, adjust the source interface, and add another NAT policy.

Creating a Many-to-Many NAT Policy

The Many-to-Many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the SonicWALL security appliance to utilize several addresses to perform the dynamic translation. Thus allowing a much higher number of concurrent the SonicWALL security appliance to perform up to a half-million concurrent connections across the interfaces.

This policy is easy to set up and activate. You first need to go to the **Network > Address Objects** and click on the **Add** button at the bottom of the screen. When the **Add Address Object** window appears, enter in a description for the range in the **Name** field, choose **Range** from the drop-down menu, enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields, and select **WAN** as the zone from the **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Select **Network > NAT Policies** and click on the **Add** button. The Add NAT Policy window is displayed. To create a NAT policy to allow the systems on the LAN interface to initiate traffic using the public range addresses, choose the following from the drop-down menus:

- **Original Source:** LAN Primary Subnet
- **Translated Source:** public_range
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** LAN
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance dynamically maps outgoing traffic using the four available IP addresses in the range we created.

You can test the dynamic mapping by installing several systems on the LAN interface at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public website <http://www.whatismyip.com> from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

Creating a One-to-One NAT Policy for Outbound Traffic

One-to-One NAT for outbound traffic is another common NAT policy on a SonicWALL security appliance for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this one-to-one NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it's paired with a reflective (mirror) policy that allows any system from the public Internet to access the server, along with a matching firewall access rule that permits this. Reflective NAT policies are covered in the next section.

This policy is easy to set up and activate. Select **Network > Address Objects** and click on the **Add** button at the bottom of the screen. In the **Add Address Object** window, enter a description for server's private IP address in the **Name** field. Choose **Host** from the **Type** menu, enter the server's private IP address in the **IP Address** field, and select the zone that the server assigned from the **Zone Assignment** menu. Click **OK**. Then, create another object in the **Add Address Object** window

for the server's public IP address and with the correct values, and select **WAN** from **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Next, select **Network > NAT Policies** and click on the **Add** button to display the **Add NAT Policy** window. To create a NAT policy to allow the webserver to initiate traffic to the public Internet using its mapped public IP address, choose the following from the drop-down menus:

- **Original Source:** webserver_private_ip
- **Translated Source:** webserver_public_ip
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Checked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface.

You can test the one-to-one mapping by opening up a web browser on the server and accessing the public website <http://www.whatismyip.com>. The website should display the public IP address we attached to the private IP address in the NAT policy we just created.

Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)

This is the mirror policy for the one created in the previous section when you check **Create a reflective policy**. It allows you to translate an external public IP addresses into an internal private IP address. This NAT policy, when paired with a 'permit' access policy, allows any source to connect to the internal server using the public IP address; the SonicWALL security appliance handles the translation between the private and public address. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive via the WAN interface.

Below, you create the entry as well as the rule to allow HTTP access to the server. You need to create the access policy that allows anyone to make HTTP connections to the webserver via the webserver's public IP address.



Note: *With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.*

Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your server in). Click on the 'Add...' button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action:** Allow
- **Service:** HTTP
- **Source:** Any
- **Destination:** webserver_public_ip
- **Users Allowed:** All

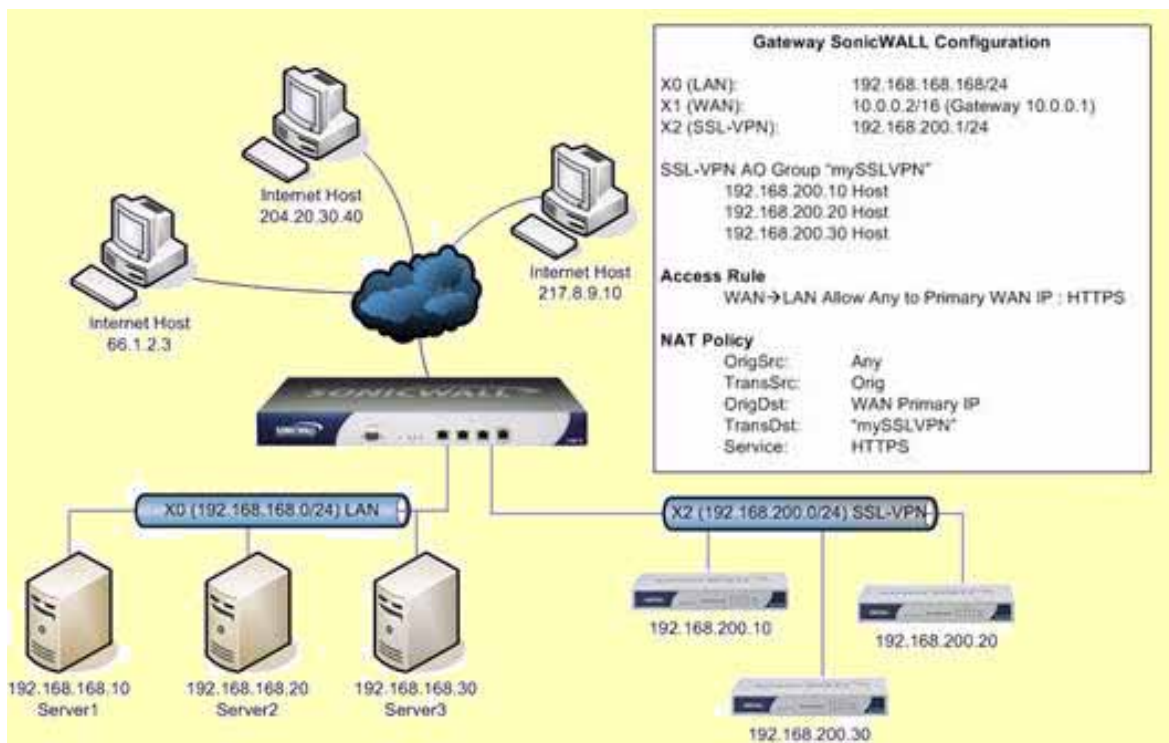
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

When you are done, attempt to access the webserver's public IP address using a system located on the public Internet. You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Configuring One-to-Many NAT Load Balancing

One-to-Many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, SonicWALL security appliances can load balance multiple SonicWALL SSL-VPN appliances, while still maintaining session persistence by always balancing clients to the correct destination SSL-VPN. Figure 18.1 shows a sample topology and configuration.

Figure 18.1 **One-to-Many NAT Load Balancing Topology and Configuration**



To configure One-to-Many NAT load balancing, first go to the **Firewall > Access Rules** page and choose the policy for **WAN** to **LAN**. Click on the **Add...** button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action:** Allow
- **Service:** HTTPS
- **Source:** Any
- **Destination:** WAN Primary IP
- **Users Allowed:** All
- **Schedule:** Always on
- **Comment:** Descriptive text, such as SSLVPN LB
- **Logging:** checked
- **Allow Fragmented Packets:** unchecked

Next, create the following NAT policy by selecting **Network > NAT Policies** and clicking on the **Add...** button:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** Select **Create new address object...** to bring up the **Add Address Object** screen.
 - ♦ **Name:** A descriptive name, such as mySSLVPN
 - ♦ **Zone assignment:** LAN
 - ♦ **Type:** Host
 - ♦ **IP Address:** The network IP address for the devices to be load balanced (in the topology shown in Figure 18.1, this is 192.168.200.1)
- **Original Service:** HTTPS
- **Translated Service:** HTTPS
- **Inbound Interface:** Any
- **Outbound Interface:** Any
- **Comment:** Descriptive text, such as SSLVPN LB
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In the example below, you modify the NAT policy and rule created in the previous section to allow public users to connect to the private webserver on its public IP address, but via a different port (TCP 9000), instead of the standard HTTP port (TCP 80).

First, you need to create a custom service for the different port. Go to the **Firewall > Custom Services** page and select the **Add** button. When the pop-up screen appears, give your custom service a name such as "webserver_public_port", enter in "9000" as the starting and ending port, and choose "TCP(6)" as the protocol. When done, click on the **OK** button to save the custom service.

Next, you modify the NAT policy created in the previous section that allowed any public user to connect to the webserver on its public IP address. Go to the **Network > NAT Policies** menu and click on the Edit button next to this NAT policy. The Edit NAT Policy window is displayed for editing the policy. Edit the NAT policy so that it includes the following from the drop-down menus:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** webserver_public_ip
- **Translated Destination:** webserver_private_ip
- **Original Service:** webserver_public_port (or whatever you named it above)
- **Translated Service:** HTTP
- **Inbound Interface:** WAN
- **Outbound Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked



Note: Make sure you chose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it's actually the correct thing to do (if you try to specify the interface, you get an error).

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface, and translates the requested protocol (TCP 9000) to the server's actual listening port (TCP 80).

Finally, you're going to modify the firewall access rule created in the previous section to allow any public user to connect to the webserver on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).



Note: With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** section and choose the policy for the **WAN to Sales** zone intersection (or, whatever zone you put your server in). Click on the **Configure** button to bring up the previously created policy. When the pop-up appears, edit in the following values:

- **Action:** Allow
- **Service:** webserver_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** webserver_public_ip
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

When you're done, attempt to access the webserver's public IP address using a system located on the public Internet on the new custom port (example: <http://67.115.118.70:9000>). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a SonicWALL security appliance running SonicOS Enhanced – it allows you to use the WAN IP address of the SonicWALL security appliance to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the SonicWALL security appliance's WAN interface.

Below, you create the programming to provide public access to two internal web servers via the SonicWALL security appliances WAN IP address; each is tied to a unique custom port. In the following examples, you set up two, but it's possible to create more than these as long as the ports are all unique.

In this section, we have five tasks to complete:

- 1 Create two custom service objects for the unique public ports the servers respond on.
- 2 Create two address objects for the servers' private IP addresses.
- 3 Create two NAT entries to allow the two servers to initiate traffic to the public Internet.
- 4 Create two NAT entries to map the custom ports to the actual listening ports, and to map the private IP addresses to the SonicWALL's WAN IP address.

- 5 Create two access rule entries to allow any public user to connect to both servers via the SonicWALL's WAN IP address and the servers' respective unique custom ports.

First, you need to create a custom service for the different port. Go to the **Firewall > Custom Services** page and click on the Add button. When the pop-up screen appears, give your custom services names such as "servone_public_port" and "servtwo_public_port", enter in "9100" and "9200" as the starting and ending port, and choose "TCP(6)" as the protocol. When done, click on the **OK** button to save the custom services.

Second, to go to the **Network > Address Objects** and click on the **Add** button at the bottom of the page. In the **Add Address Objects** window, enter in a description for server's private IP addresses, choose 'Host' from the drop-down box, enter the server's private IP addresses, and select the zone that the servers are in. When done, click on the 'OK' button to create the range object.

Third, from the SonicWALL's management GUI, go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create a NAT policy to allow the two servers to initiate traffic to the public Internet using the SonicWALL security appliance's WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** servone_private_ip
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** servtwo_private_ip
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the servers' private IP addresses to the public IP address when it initiates traffic out the WAN interface.

Fourth, go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create the NAT policies to map the custom ports to the servers' real listening

ports and to map the SonicWALL's WAN IP address to the servers' private addresses, choose the following from the drop-down boxes:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servone_private_ip
- **Original Service:** servone_public_port
- **Translated Service:** HTTP
- **Inbound Interface:** WAN
- **Outbound Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servtwo_private_ip
- **Original Service:** servtwo_public_port
- **Translated Service:** HTTP
- **Source Interface:** WAN
- **Destination Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked



Note: Make sure you choose 'Any' as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it's actually the correct thing to do (if you try to specify the interface, you get an error).

When done, click on the 'OK' button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface.

Fifth, you need to create the access rules that allows anyone from the public Internet to access the two webservers using the custom ports and the SonicWALL security appliance's WAN IP address.



Note: With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS 2.0 Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your servers in). Click on the 'Add...' button to bring up the pop-up window to create the policies. When the pop-up appears, enter the following values:

- **Action:** Allow
- **Service:** servone_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP Address

- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

And:

- **Action:** Allow
- **Service:** servtwo_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP Address
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

When you're done, attempt to access the web servers via the SonicWALL's WAN IP address using a system located on the public Internet on the new custom port (example: <http://67.115.118.70:9100> and <http://67.115.118.70:9200>). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Managing ARP Traffic

Network > ARP

Network > ARP Flush ARP Cache... Apply Cancel ?

Static ARP Entries

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
1	192.168.50.1	00:06:b1:04:00:e5	X2	✓		

Add... Delete Delete All...

ARP Settings

ARP Cache entry timeout (minutes):

ARP Cache Items 1 to 7 (of 7)

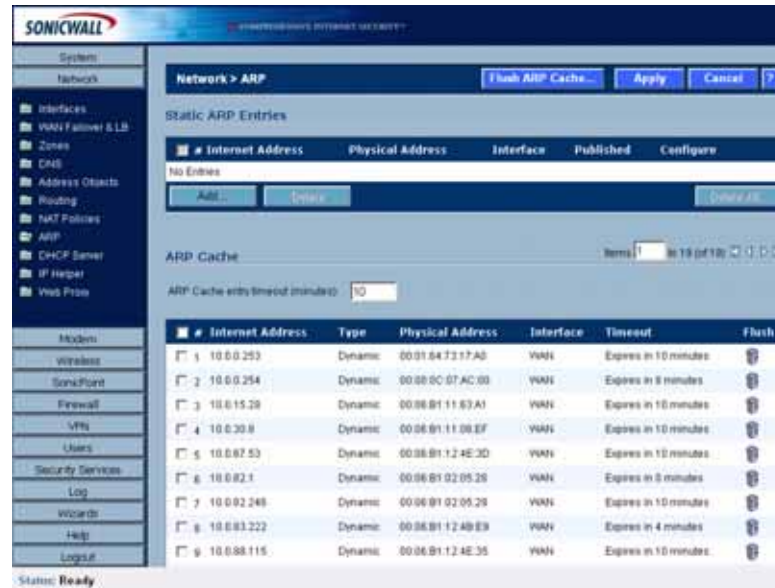
#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	10.0.93.56	Static	00:06:B1:12:47:D7	X1	Permanent published	
2	10.0.202.118	Dynamic	00:00:56:84:99:C8	X1	Expires in 10 minutes	
3	172.31.20.1	Static	00:06:B1:12:47:D9	X3/V20	Permanent published	
4	175.31.16.1	Static	00:06:B1:12:47:DA	X4	Permanent published	
5	192.168.50.1	Static	00:06:B1:04:00:E5	X2	Permanent published	
6	192.168.100.1	Static	00:06:B1:12:47:D9	X3/V100	Permanent published	
7	192.168.168.168	Static	00:06:B1:12:47:D6	X0	Permanent published	

Flush Flush ARP Cache...

ARP Statistics: ARP Statistics: 7 entries, 1381 lookups, 6 failures, 1363 hits, 12 misses, 99% hit rate

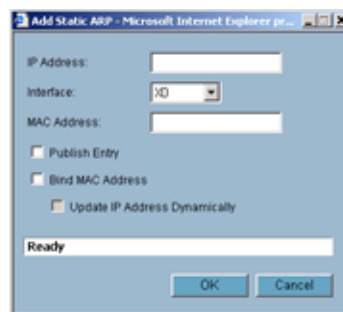
ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize

the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.



Static ARP Entries

The Static ARP feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses, but also provides the following capabilities:



- Publish Entry** - Enabling the **Publish Entry** option in the **Add Static ARP** window causes the SonicWALL device to respond to ARP queries for the specified IP address with the specified MAC address. This can be used, for example, to have the SonicWALL device reply for a secondary IP address on a particular interface by adding the MAC address of the SonicWALL. See the Secondary Subnet section that follows.
- Bind MAC Address** - Enabling the **Bind MAC Address** option in the **Add Static ARP** window binds the MAC address specified to the designated IP address and interface. This can be used to ensure that a particular workstation (as recognized by the network card's unique MAC address) can only be used on a specified interface on the SonicWALL. Once the MAC address is bound to an interface, the SonicWALL will not respond to that MAC address on any other interface. It will also remove any dynamically cached references to that MAC address that might have been present, and it will prohibit additional (non-unique) static mappings of that MAC address.
- Update IP Address Dynamically** - The **Update IP Address Dynamically** setting in the Add Static ARP window is a sub-feature of the **Bind MAC Address** option. This allows for a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing. Enabling this option will blur the IP Address field, and will populate the ARP Cache with the IP Address allocated by the SonicWALL's internal DHCP server, or by the external DHCP server if IP Helper is in use.

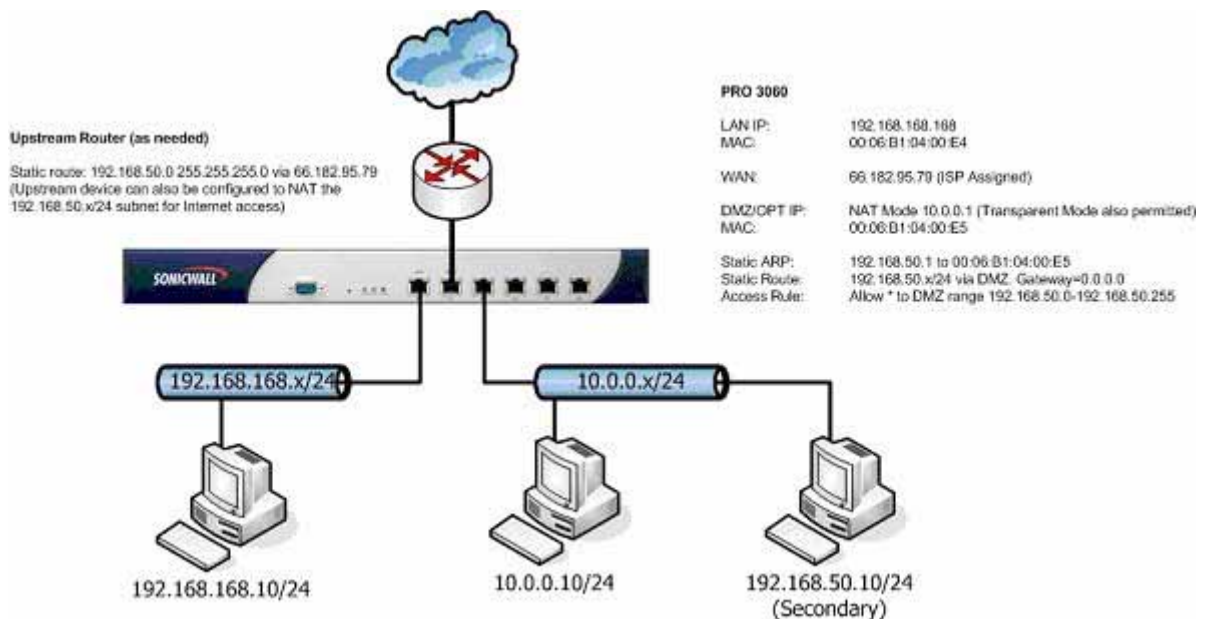
Secondary Subnets with Static ARP

The Static ARP feature allows for secondary subnets to be added on other interfaces, and without the addition of automatic NAT rules.

Adding a Secondary Subnet using the Static ARP Method

- 1 Add a 'published' static ARP entry for the gateway address that will be used for the secondary subnet, assigning it the MAC address of the SonicWALL interface to which it will be connected.
- 2 Add a static route for that subnet, so that the SonicWALL regards it as valid traffic, and knows to which interface to route that subnet's traffic.
- 3 Add Access Rules to allow traffic destined for that subnet to traverse the correct network interface.
- 4 Optional: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

Consider the following network example:



To support the above configuration, first create a published static ARP entry for 192.168.50.1, the address which will serve as the gateway for the secondary subnet, and associate it with the DMZ/OPT interface. From the **Network > ARP** page, select the **Add** button in the **Static ARP Entries** section, and add the following entry:

Add Static ARP - Microsoft Internet Explorer pr...

IP Address: 192.168.50.1
 Interface: X2
 MAC Address: 00:06:b1:04:00:e5
 Publish Entry
 Bind MAC Address
 Update IP Address Dynamically
 Ready
 OK Cancel

The entry will appear in the table as follows:

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
1	192.168.50.1	00:06:b1:04:00:e5	X2	<input checked="" type="checkbox"/>		

Navigate to the **Network > Routing** page, and add a static route for the 192.168.50.0/24 network as follows:

Destination Network: 192.168.50.0
 Subnet Mask: 255.255.255.0
 Default Gateway: 0.0.0.0
 Interface: OPT

The entry will appear in the table as follows:

Destination Network	Subnet Mask	Gateway	Interface	Configure
192.168.50.0	255.255.255.0	0.0.0.0	OPT	

To allow the traffic to reach the 192.168.50.0/24 subnet, and to allow the 192.168.50.0/24 subnet to reach the hosts on the LAN, navigate to the **Firewall > Access Rules** page, and add the following Access Rule:

Prohibit Dynamic ARP Entries

Enabling this feature on an interface will prevent that interface from dynamically adding ARP entries. This is offered as a security mechanism to statically and strictly define the MAC addresses of hosts that will be permitted to operate on a particular interface.

ARP Cache entry timeout (minutes): 20
 Prohibit Dynamic ARP Entries: LAN WAN DMZ



Alert: Misuse or misconfiguration of this feature can render the SonicWALL inaccessible and recoverable only by restoring factory defaults. Be certain to understand the behavior of this feature, and to have properly configured static ARP entries for allowed hosts prior to applying any 'prohibit dynamic ARP entry' settings.

A typical use for this feature would be prohibiting dynamic ARP on the WAN interface, after adding a static ARP entry for the upstream router. This will help to ensure that the router will be the only host allowed on the WAN interface.

After adding the static ARP entry for the router, mark the checkbox next to the WAN interface in the 'Prohibit dynamic ARP entries' area. Click the **OK** button in the alert dialog to proceed. The setting will not take effect until the **Apply** button at the top of the page is selected.

Navigating and Sorting the ARP Cache Table

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table.

#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	10.0.0.254	Dynamic	00:00:0C:07:AC:00	WAN	expires in 6 mins	
2	10.0.88.123	Dynamic	00:06:B1:11:05:FA	WAN	expires in 10 mins	
3	10.0.92.2	Dynamic	00:06:B1:12:44:B3	WAN	expires in 10 mins	
4	10.0.93.24	Dynamic	00:06:B1:12:51:4D	WAN	expires in 10 mins	
5	10.0.93.52	Static	00:06:B1:13:5A:C0	WAN	permanent published	
6	10.0.93.52	Static	00:06:B1:13:5A:C0	OPT	permanent published	
7	10.0.202.82	Dynamic	00:B0:D0:5A:5D:69	WAN	expires in 10 mins	
8	192.168.168.168	Static	00:06:B1:13:5A:BE	LAN	permanent published	

ARP Statistics: ARP Statistics: 8 entries, 1129 lookups, 797 failures, 330 hits, 2 misses, 99% hit rate

Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Navigating and Sorting the ARP Cache Table Entries

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per

page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP** Cache to clear the information.

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

Setting Up the DHCP Server

Network > DHCP Server

The SonicWALL security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. The **Network > DHCP Server** page includes settings for configuring the SonicWALL security appliance's DHCP server.

Network > DHCP Server Apply Cancel ?

DHCP Server Settings

Enable DHCP Server
 Enable Conflict Detection

DHCP Server Lease Scopes Items 1 to 2 (of 2)

View Style: All Dynamic Static

#	Type	Lease Scope	Interface	Details	Enable	Configure
1	Dynamic	Range: 172.16.31.2 - 172.16.31.252	X2		<input checked="" type="checkbox"/>	
2	Dynamic	Range: 192.168.168.1 - 192.168.168.167	X0		<input checked="" type="checkbox"/>	

Add Dynamic Add Static Delete Delete All

Current DHCP Leases Items 1 to 2 (of 2)

#	IP Address	Ethernet Address	Type	Delete
1	172.16.31.233	00:12:17:81:BB:FC	Dynamic	
2	192.168.168.20	00:0D:5E:E5:35:FC	Dynamic	

Delete Delete All

Current: 2, Available Dynamic: 416, Available Static: 0, Total: 418

You can use the SonicWALL security appliance's DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure the **Enable DHCP Server** checkbox is unchecked.

The number of address ranges and IP addresses the SonicWALL DHCP server can assign depends on the model, operating system, and licenses of the SonicWALL security appliance. For example, on a SonicWALL TZ 170 SP Wireless running SonicOS Enhanced, the SonicWALL DHCP Server can assign a total of 64 address ranges with 64 IP addresses each or a total of 4,096 IP addresses.


Enabling the DHCP Server

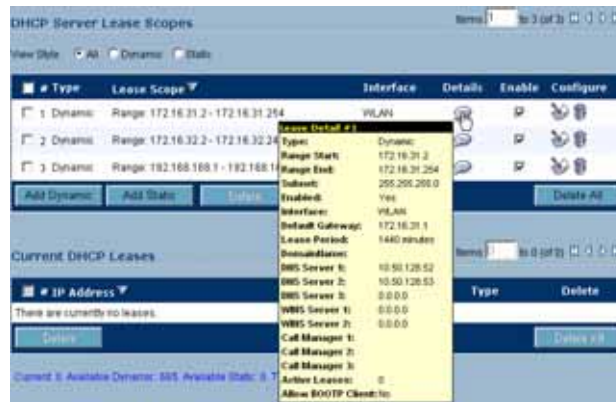
If you want to use the SonicWALL security appliance's DHCP server, select **Enable DHCP Server** on the **Network > DHCP Server** page.


Select **Enable Conflict Detection** to turn on automatic DHCP scope conflict detection on each zone.

DHCP Server Lease Scopes

The DHCP **Server Lease Scopes** table displays the currently configured DHCP IP ranges. The table shows:

- **Type:** Dynamic or Static
- **Lease Scope:** The IP address range, for example **172.16.31.2 - 172.16.31.254**
- **Interface:** The Interface the range is assigned to--**LAN**, **OPT**, or **WLAN**
- **Details:** Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the Details icon 



- **Enable:** Check the box in the Enable column to enable the DHCP range. Uncheck it to disable the range
- **Configure:** Click the configure icon  to configure the DHCP range

Configuring DHCP Server for Dynamic Ranges

To configure DHCP server for dynamic IP address ranges, follow these instructions:

- 1 In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Dynamic**. The **Dynamic Ranges Configuration** window is displayed.



General

- 2 In the **General** page, make sure the **Enable this DHCP Range** is checked, if you want to enable this range.
- 3 Select the interface from the Interface menu. The IP addresses are in the same private subnet as the selected interface.



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

- 4 Use the default IP address range entries for the interface in the **Range Start** and **Range End** fields or type in your own IP address range.
- 5 Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
- 6 Select the gateway from the **Gateway Preferences** menu. The interface IP address is the default value, but you can select **Other** and type a different IP address for the gateway.
- 7 If you select the interface IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to type the **Default Gateway** and **Subnet Mask** information into the fields.
- 8 Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.

DNS/WINS

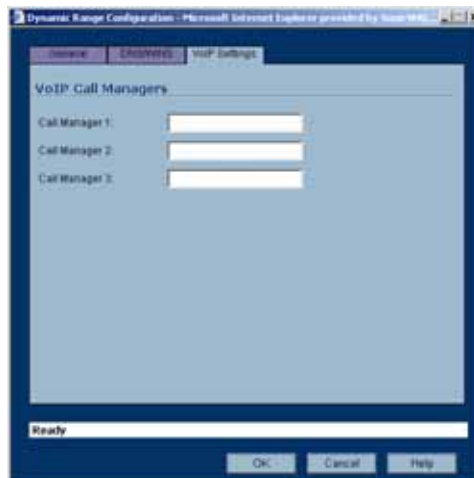
- 9 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



- 10 If you have a domain name for the DNS server, type it in the **Domain Name** field.
- 11 **Inherit DNS Settings Dynamically using SonicWALL's DNS Settings** automatically populates the DNS and WINS settings with the settings in the **Network > DNS** page. This option is selected by default.
- 12 If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.
- 13 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can add an additional WINS server.

VoIP Settings

- 14 Click on the **VoIP Settings** tab. The **VoIP Settings** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.



- 15 Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.
- 16 Click **OK** to add the settings to the SonicWALL security appliance.
- 17 Click **Apply** for the settings to take effect on the SonicWALL security appliance.



Cross Reference: For more information on VoIP support features on the SonicWALL security appliance, see Chapter 28 Configuring VoIP Support.

Configuring Static DHCP Entries

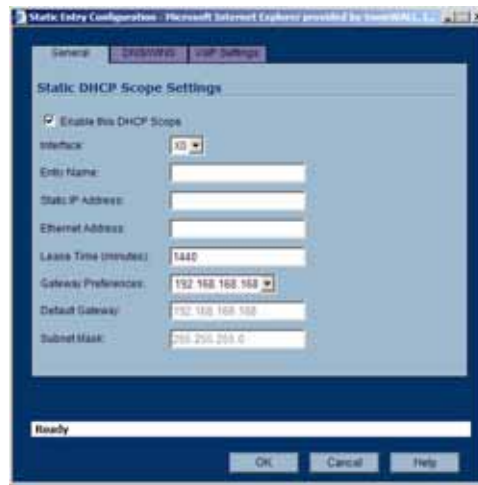
Static entries are IP addresses assigned to servers requiring permanent IP settings.



Note: Static DHCP entries should not be configured for computers with IP addresses configured in Network

To configure static entries, follow these steps:

- 1 In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Static**. The **Static Entry Configuration** window is displayed.



General

- 2 In the **General** tab, make sure the **Enable this DHCP Entry** is checked, if you want to enable this range.
- 3 Select the interface from the Interface menu. The IP addresses are in the same private subnet as the selected interface.
- 4 Enter a name for the static DNS entry in the **Entry Name** field.
- 5 Type the device IP address in the **Static IP Address** field.
- 6 Type the device Ethernet (MAC) address in the **Ethernet Address** field.
- 7 Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
- 8 Select the gateway from the **Gateway Preferences** menu. The interface IP address is the default value, but you can select **Other** and type a different IP address for the gateway.
- 9 If you select the SonicWALL security appliance LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to type the **Default Gateway** and information into the fields.

DNS/WINS

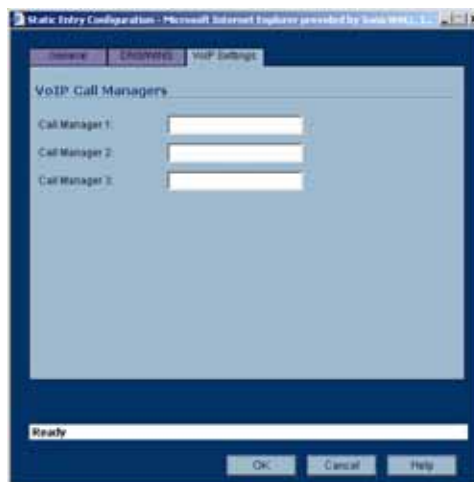
- 10 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



- 11 If you have a domain name for the DNS Server, type it in the **Domain Name** field.
- 12 **Inherit DNS Settings Dynamically from the SonicWALL's DNS settings** is selected by default. When selected, the DNS Server IP fields are unavailable.
- 13 If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.
- 14 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can specify an additional WINS server.

VoIP Settings

- 15 Click on the **VoIP Settings** tab. The **VoIP Settings** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.



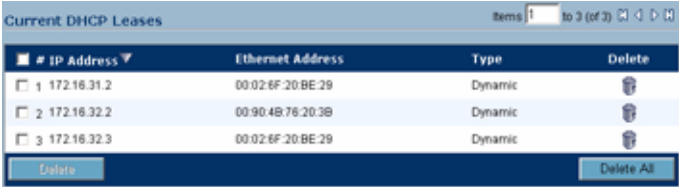
- 16 Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.
- 17 Click **OK** to add the settings to the SonicWALL.
- 18 Click **Apply** for the settings to take effect on the SonicWALL.








For more information on VoIP support features on the SonicWALL security appliance, see Chapter 28 Configuring VoIP Support.

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the **IP Address**, the **Ethernet Address**, and the **Type** of binding (Dynamic, Dynamic BOOTP, or Static BOOTP).



#	IP Address	Ethernet Address	Type	Delete
1	172.16.31.2	00:02:6F:20:BE:29	Dynamic	
2	172.16.32.2	00:90:4B:76:20:3B	Dynamic	
3	172.16.32.3	00:02:6F:20:BE:29	Dynamic	

To delete a binding, which frees the IP address on the DHCP server, click the Delete icon  next to the entry. For example, use the Delete icon  to remove a host when it has been removed from the network, and you need to reuse its IP address.

Setting Up Web Proxy Forwarding

Network > Web Proxy

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests. Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

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



The screenshot shows the configuration page for 'Automatic Proxy Forwarding (Web Only)'. The page title is 'Network > Web Proxy' with 'Apply', 'Cancel', and '?' buttons. The configuration fields are:

- Proxy Web Server (name or IP address): [Text input field]
- Proxy Web Server Port: [Text input field with '0' entered]
- Bypass Proxy Servers Upon Proxy Server Failure
- Forward Public Zone Client Requests to Proxy Server

Configuring Automatic Proxy Forwarding (Web Only)



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

To configure a Proxy Web sever, select the **Network > Web Proxy** page.

- 1 Connect your Web proxy server to a hub, and connect the hub to the SonicWALL security appliance WAN port.
- 2 Type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
- 3 Type the proxy IP port in the **Proxy Web Server Port** field.
- 4 To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
- 5 Select **Forward DMZ Client Requests to Proxy Server** if you have clients configured on the DMZ.
- 6 Click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

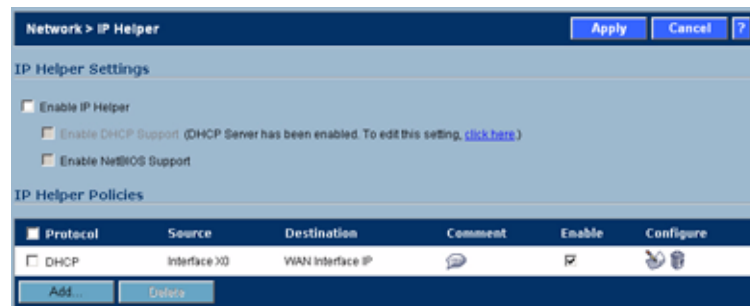
Bypass Proxy Servers Upon Proxy Failure

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

Using IP Helper

Network > IP Helper

The IP Helper allows the SonicWALL security appliance to forward DHCP requests originating from the interfaces on a SonicWALL security appliance to a centralized DHCP server on the behalf of the requesting client. IP Helper is used extensively in routed VLAN environments where a DHCP server is not available for each interface, or where the layer 3 routing mechanism is not capable of acting as a DHCP server itself. The IP Helper also allows NetBIOS broadcasts to be forwarded with DHCP client requests.



For more information on IP Helper, refer to the IP Helper technote at:
http://www.sonicwall.com/support/pdfs/technotes/ip_helper_on_sonicos_enhanced.pdf

IP Helper Settings

- **Enable IP Helper** - enables IP Helper features.
- **Enable DHCP Support** - enables DHCP forwarding from the SonicWALL security appliance to your central DHCP server. If the DHCP server has been enabled, the message “**DHCP Server has been enabled. To edit this setting, click here.**” is displayed. Clicking the link displays the **Network > DHCP Server** page.

▲ **Alert:** *The SonicWALL DHCP Server feature must be disabled before you can enable DHCP Support on the IP Helper. The **Enable DHCP Support** checkbox is greyed out until the DHCP Server setting is disabled.*

- **Enable NetBIOS Support** - enables NetBIOS broadcast forwarding with the DHCP requests. NetBIOS is required to allow Windows operating systems to browse for resources on a network.

IP Helper Policies

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

Adding an IP Helper Policy

- 1 Click the **Add** button under the **IP Helper Policies** table. The **Add IP Helper Policy** window is displayed.



- 2 The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.
- 3 Select **DHCP** or **NetBIOS** from the **Protocol** menu.
- 4 Select a source Interface or Zone from the **From** menu.
- 5 Select a destination IP address or subnet from the **To** menu or select **Create a new network** to create a new **Address Object**.
- 6 Enter an optional comment in the **Comment** field.
- 7 Click **OK** to add the policy to the **IP Helper Policies** table.

Editing an IP Helper Policy

Click the **Notepad** icon in the **Configure** column of the **IP Helper Policies** table to display the **Edit IP Helper** window, which includes the same settings as the **Add IP Helper Policy** window.

Deleting IP Helper Policies

Click the Trashcan icon to delete the individual IP Helper policy entry. Click the **Delete** button to delete all the selected IP Helper policies in the **IP Helper Policies** table.

Configuring Dynamic DNS

Dynamic DNS Overview

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, if a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and could result in your DDNS account getting locked out. Please refer to the use policies posted on the provider's pages, and abide by the guidelines. SonicWALL does not provide technical support for DDNS providers - the providers themselves must be contacted.

Profile Name	Domain	Provider	Status	Enabled	Online	Configure
DDNS Example	example.sonicwall.com	DynDNS.org		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS currently supports the following services from four Dynamic DNS providers:

- [Dyndns.org](http://www.dyndns.org) <<http://www.dyndns.org>> - SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from Dyndns.org.
- [Changeip.com](http://www.changeip.com) <<http://www.changeip.com>> - A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
- [No-ip.com](http://www.no-ip.com) <<http://www.no-ip.com>> - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
- [Yi.org](http://www.yi.org) <<http://www.yi.org>> - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the yi.org administrative page for dynamic updates to occur properly.

Additional Services offered by Dynamic DNS Providers

Some common additional services offered by Dynamic DNS providers include:

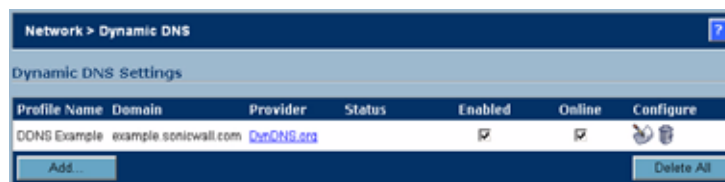
- **Wildcards** - allows for wildcard references to sub-domains. For example, if you register yourdomain.dyndns.org, your site would be reachable at *.yourdomain.dyndyn.org, e.g. server.yourdomain.dyndyn.org, www.yourdomain.dyndyn.org, ftp.yourdomain.dyndyn.org, etc.
- **Mail Exchangers** - Creates MX record entries for your domain so that SMTP servers can locate it via DNS and send mail. Note: inbound SMTP is frequently blocked by ISPs - please check with your provider before attempting to host a mail server.
- **Backup MX** (offered by dyndns.org, yi.org) - Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
- **Groups** - Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
- **Off-Line IP Address** - Allows for the specification of an alternative address for your registered hostnames in the event that the primary registered IP is offline.

Configuring Dynamic DNS

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed above. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email.

After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS.

The **Network > Dynamic DNS** page provides the settings for configuring the SonicWALL security appliance to use your DDNS service.



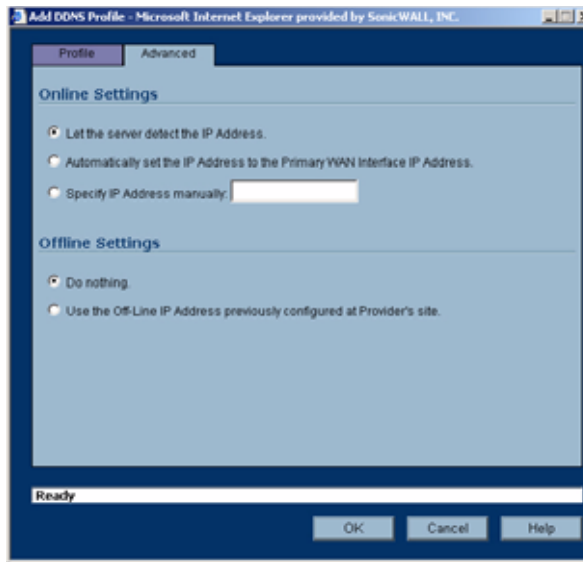
To configure Dynamic DNS on the SonicWALL security appliance, perform these steps:

- 1 From the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** window is displayed.



- 2 If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the SonicWALL security appliance takes the actions defined in the **Online Settings** section on the **Advanced** tab.
- 3 If **Use Online Settings** is checked, the profile is administratively online.
- 4 Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table.
- 5 In the **Profile** page, select the **Provider** from the drop-down list at the top of the page. *DynDNS.org* and *changeip.com* use HTTPS, while *yi.org* and *no-ip.com* use HTTP. This example uses *DynDNS.org*. DynDNS.org requires the selection of a service. This example assumes you have created a dynamic service record with dynDNS.org.
- 6 Enter your dynDNS.org username and password in the **User Name** and **Password** fields.
- 7 Enter the fully qualified domain name (FQDN) of the hostname you registered with dynDNS.org. Make sure you provide the same hostname and domain as you configured.
- 8 When using *DynDNS.org*, select the **Service Type** from the drop-down list that corresponds to your type of service through DynDNS.org. The options are:
 - ♦ **Dynamic** - A free Dynamic DNS service.
 - ♦ **Custom** - A managed primary DNS solution that provides a unified primary/secondary DNS service and a web-based interface. Supports both dynamic and static IP addresses.
 - ♦ **Static** - A free DNS service for static IP addresses.
- 9 When using *DynDNS.org*, you may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field. Check **Backup MX** if this is the backup mail exchanger.

10 Click the **Advanced** tab. You can typically leave the default settings on this page.



11 The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:

Let the server detect IP Address - The dynamic DNS provider determines the IP address based upon the source address of the connection. This is the most common setting.

Automatically set IP Address to the Primary WAN Interface IP Address - This will cause the SonicWALL device to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.

Specify IP Address manually - Allows for the IP address to be registered to be manually specified and asserted.

12 The **Off-line Settings** section controls what IP Address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the SonicWALL. The options are:

Do nothing - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.

Use the Off-Line IP Address previously configured at Providers site - If your provider supports manual configuration of **Off-Line Settings**, you can select this option to use those settings when this profile is taken administratively offline.

13 Click **OK**.



Dynamic DNS Settings Table

The **Dynamic DNS Settings** table provides a table view of configured DDNS profiles.

Profile Name	Domain	Provider	Status	Enabled	Offline	Configure
profile2	msocler.bndns.org	comcast.net	Online: 07:10:10:00:00 at 11/01/2004 11:03:26	☑	☑	⚙️
profile1	msocler.dns.biz	comcast.com	Online: 06:10:00:79:00 at 11/01/2004 11:21:32	☑	☑	⚙️

Dynamic DNS Settings table includes the following columns:

- **Profile Name** - The name assigned to the DDNS entry during its creation. This can be any value, and is used only for identification.
- **Domain** - The fully qualified domain name (FQDN) of the DDNS entry.
- **Provider** - The DDNS provider with whom the entry is registered.

- **Status** - The last reported/current status of the DDNS entry. Possible states are:
 - ♦ **Online** - The DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
 - ♦ **Taken Offline Locally** - The DDNS entry is administratively offline. If the entry is Enabled, the action configured in the Offline Settings section of the Advanced tab is taken.
 - ♦ **Abuse** - The DDNS provider has considered the type or frequency of updates to be abusive. Please check with the DDNS provider's guidelines to determine what is considered abuse.
 - ♦ **No IP change** - abuse possible - A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates will only occur when address or state changes occur. Manual or forced should only be made when absolutely necessary, such as when registered information is incorrect.
 - ♦ **Disabled** - The account has been disabled because of a configuration error or a policy violation. Check the profile's settings, and verify the DDNS account status with the provider.
 - ♦ **Invalid Account** - The account information provided is not valid. Check the profile's settings, and verify the DDNS account status with the provider.
 - ♦ **Network Error** - Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
 - ♦ **Provider Error** - The DDNS provider is unable to perform the requested action at this time. Check the profile's settings, and verify the DDNS account status with the provider. Try the action again later.
 - ♦ **Not Donator Account** - Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Please check with the provider for more details on which services may require payment or donation.
- **Enabled** - When selected, this profile is administratively enabled, and the SonicWALL will take the **Online Settings** action that is configured on the **Advanced** tab. This setting can also be controlled using the **Enable this DDNS Profile** checkbox in the entry's **Profile** tab. Deselecting this checkbox will disable the profile, and no communications with the DDNS provider will occur for this profile until the profile is again enabled.
- **Online** - When selected, this profile is administratively online. The setting can also be controlled using the **Use Online Settings** checkbox on the entry's **Profile** tab. Deselecting this checkbox while the profile is enabled will take the profile offline, and the SonicWALL will take the **Offline Settings** action that is configured on the **Advanced** tab.
- **Configure** - Includes the edit  icon for configuring the DDNS profile settings, and the delete  icon for deleting the DDNS profile entry.

PART

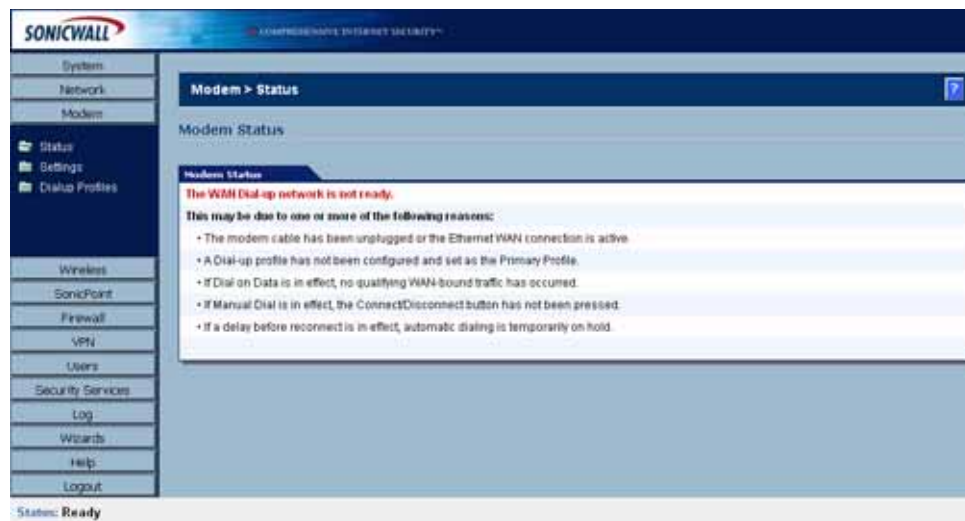
4

Modem

Viewing Modem Status

Modem > Status

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



Modem Status

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

- **WAN Gateway (Router) Address**
- **WAN IP (NAT Public) Address**
- **WAN Subnet Mask**
- **DNS Server 1**
- **DNS Server 2**
- **DNS Server 3**

- **Current Active Dial-Up Profile (id)**
- **Current Connection Speed**

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

When the modem is active, the network settings from the ISP are used for WAN access. If you select **Chapter 25, Configuring Your Modem**, a message is displayed reminding you that the modem is active and the current network settings are displayed on the Modem > Status page.

Configuring Your Modem

Modem > Settings

The **Modem > Settings** page allows you to configure modem settings, specify dial on data categories, select management and user login options, and select the primary and alternate modem profiles.

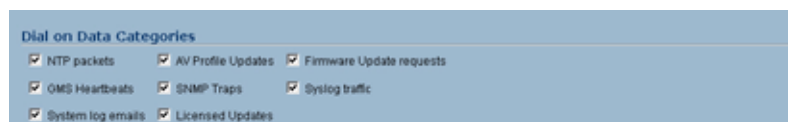
Modem Settings



Speaker Volume - Select whether you want the modem's speaker turned on or off. The default value is **On**.

Modem Initialization - Select **Initialize Modem For Use In** and select the country from the drop-down menu. **United States** is selected by default. If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands (for modem initialization)** field. AT commands are instructions used to control a modem such as `ATS7=30` (allows up to 30 seconds to wait for a dial tone), `ATS8=2` (sets the amount of time the modem pauses when it encounters a comma (",") in the string).

Dial on Data Categories



The **Dial on Data Categories** settings allow you to specify the outbound data that is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWALL security appliance security applications.

The **Dial on Data Categories** include:

- **NTP packets**
- **GMS Heartbeats**
- **System log e-mails**
- **AV Profile Updates**
- **SNMP Traps**
- **Licensed Updates**
- **Firmware Update requests**
- **Syslog traffic**

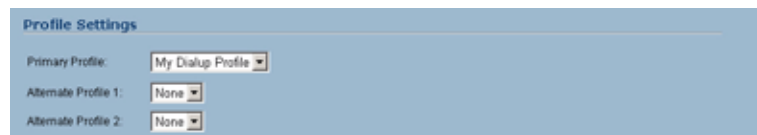
Management/User Login



The **Management/User Login** section allows you to enable remote management of the SonicWALL security appliance or user login from the **Modem** interface. You can select any of the supported management protocol(s): **HTTPS**, **Ping**, and/or **SNMP**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to allow the SonicWALL to automatically convert HTTP requests to HTTPS requests for added security.

Profile Settings



Select the profile you want to use for the primary profile from the **Primary Profile** menu that the SonicWALL security appliance uses to access the modem. If you have enabled **Manual Dial** for the **Primary Profile**, the **Alternate Profile 1** is not used.

Select the secondary profile from the **Alternate Profile 1** menu. If the **Primary Profile** cannot establish a connection, the SonicWALL security appliance uses the **Alternate Profile 1** profile to access the modem and establish a connection. If you have an additional alternate profile, select it from the **Alternate Profile 2** menu.



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

To create a Dialup Profile, see **Chapter 26, Configuring Dialup Profiles**.

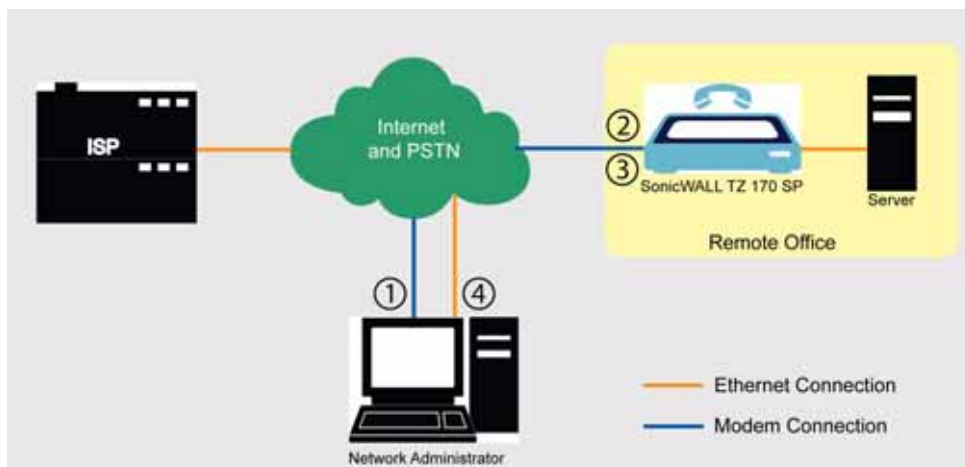
Modem > Advanced

The **Modem > Advanced** page is used to configure the Remotely Triggered Dial-Out feature, which is applicable to deployments of the SonicWALL TZ 170 SP that do not have available Ethernet connections, and where the SonicWALL TZ 170 SP is managed remotely. In these deployments, the modem is used for WAN connectivity. The Remotely Triggered Dial-Out feature enables network administrators to remotely initiate a WAN modem connection from a SonicWALL TZ 170 SP.

How Does Remotely Triggered Dial-Out Work?

Figure 25.1 shows a typical deployment that uses the Remotely Triggered Dial-Out feature.

Figure 25.1 Remotely Triggered Dial-Out Call Flow



The following process describes how a Remotely Triggered Dial-Out call functions:

- 1 The network administrator initiates a modem connection to the SonicWALL TZ 170 SP located at the remote office.
- 2 If the SonicWALL TZ 170 SP is configured to authenticate the incoming call, it prompts the network administrator to enter a password. Once the call is authenticated, the SonicWALL TZ 170 SP terminates the call.

Note: After 3 incorrect password attempts, the SonicWALL TZ170 SP terminates a Remotely Triggered Dial-out authentication session. Each password attempt is allowed a maximum of 60 seconds. If a dial-out session is terminated, the SonicWALL TZ170 SP can be called again for another Remotely Triggered Dial-out authentication session.

- 3 The SonicWALL TZ170 SP then initiates a modem connection to its dial-up ISP, based on the configured dial profile.
- 4 The network administrator accesses the SonicWALL TZ 170 SP web management interface to perform the required tasks.

Note: If LAN- to-WAN traffic on the SonicWALL TZ 170 SP generates a dial-out request at the same time as a Remotely Triggered Dial-out session is being authenticated, the Remotely Triggered Dial-out session is terminated and the SonicWALL TZ170 SP initiates its own dial-out session.

Configuring Remotely Triggered Dial-Out

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The dial profile is configured for **dial-on-data**.
- The SonicWALL Security Appliance is configured to be managed using HTTPS, so that the device can be accessed remotely.
- Enter a value in the **Enable Max Connection Time (minutes)** field. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out, go the **Modem > Advanced** screen.

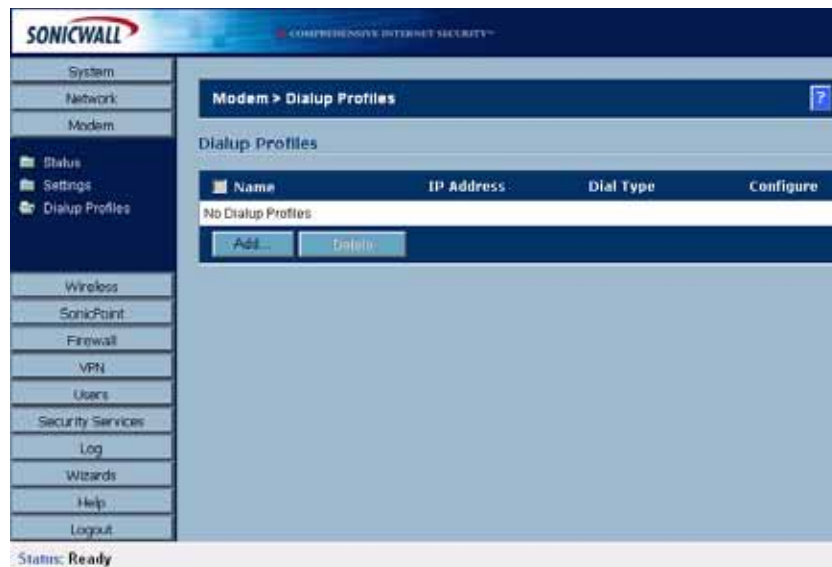
The screenshot shows the SonicWALL web interface. The top header includes the SonicWALL logo and the text 'COMPREHENSIVE INTERNET SECURITY'. A left-hand navigation menu lists various system settings: System, Network, Modem, Status, Settings, Advanced, Dialup Profiles, Wireless, SonicPoint, Firewall, VoIP, VPN, Users, Security Services, Log, Wizards, Help, and Logout. The main content area is titled 'Modem > Advanced' and contains the 'Remotely Triggered Dial-out Settings' section. This section includes three checkboxes: 'Enable Remotely Triggered Dial-out' (checked), 'Requires Authentication' (checked), and 'Enable Max Connection Time (minutes)'. Below the 'Requires Authentication' checkbox are two password input fields labeled 'Password:' and 'Confirm Password:'. The interface also features 'Apply', 'Cancel', and '?' buttons in the top right corner.

- 1 Check the **Enable dialback** checkbox.
- 2 (Optional) To authenticate the remote call, check the **Requires authentication** checkbox and enter the password in the **Password:** and **Confirm Password:** fields.

Configuring Dialup Profiles

Modem > Dialup Profiles

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



✓ **Tip:** The SonicWALL security appliance supports a maximum of 10 configuration profiles.

Dial-Up Profiles

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

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

- **Configure** - clicking the edit icon allows you to edit the profile. Clicking on the delete icon deletes the profile.

Configuring a Dialup Profile

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



Once you create your profiles, you can then configure specify which profiles to use for WAN failover or Internet access.

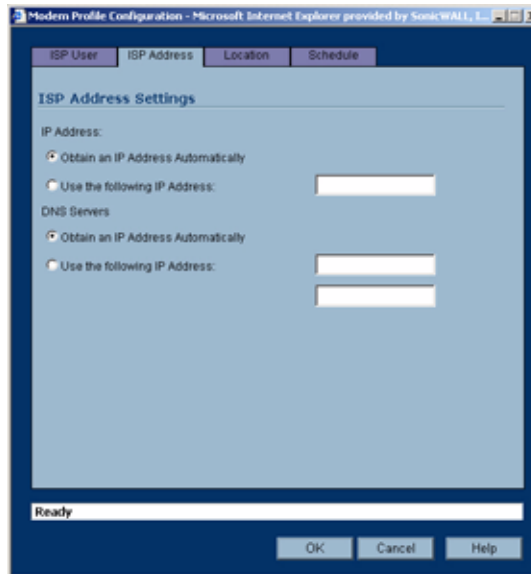
To configure your ISP settings, you must obtain your Internet information from your dial-up Internet Service Provider.

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

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

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

8 Click the **ISP Address** tab.



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



- 12 In the **Dial Type** menu select one of the following options:
- ♦ **Persistent Connection** - By selecting **Persistent Connection**, the modem stays connected unless you click the Disconnect button on the **Network > Settings** page. If **Enable Dial-Up Wan Failover** is selected on the **Network > WAN Failover & Load Balancing** page, the modem dials automatically when a WAN connection fails. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.

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



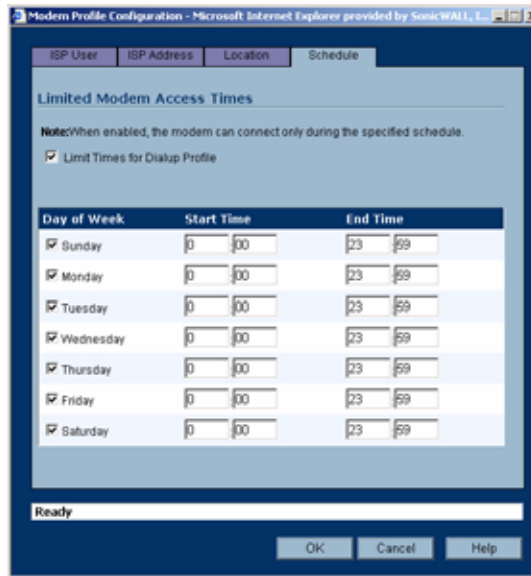
Alert: *If you are configuring two dial-up profiles for WAN failover, the modem behavior should be the same for each profile. For example, if your Primary Profile uses Persistent Connection, your Secondary Profile should also use Persistent Connection.*



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

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

21 Click the **Schedule** tab.



- 22 If you want to specify scheduled times the modem can connect, select **Limit Times for Dialup Profile**. Enter times for each day in 24-hour format that you want the modem to be able to make a connection.
- 23 Click **OK** to add the dial-up profile to the SonicWALL security appliance. The Dialup Profile appears in the **Dialup Profiles** table.

Chat Scripts

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

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

```
ABORT `NO DIALTONE`
ABORT `BUSY`
ABOR `NO CARRIER`
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

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

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

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

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

Custom Chat Scripts

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

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

A custom chat script can look like the following script:

```
ABORT `NO CARRIER`
ABORT `NO DIALTONE`
ABORT `BUSY`
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername: \L
assword: \P
```



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

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

PART

5

Wireless

Viewing WLAN Settings, Statistics, and Station Status

The SonicWALL TZ 170 Wireless and TZ 170 SP Wireless support two wireless protocols called IEEE 802.11b and 802.11g, commonly known as Wi-Fi, and send data via radio transmissions. The SonicWALL TZ 170 Wireless combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the TZ 170 Wireless offers the flexibility of wireless without compromising network security.



Note: *The information in this chapter refers to the wireless features of the TZ 170 Wireless and TZ 170 SP Wireless security appliances running SonicOS Enhanced. When the text in this chapter refers to the TZ 170 Wireless, the information applies to both security appliances.*

Typically, the TZ 170 Wireless is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the TZ 170 Wireless also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the TZ 170 Wireless, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the TZ 170 Wireless. It is also at this layer that the TZ 170 Wireless has the capability of enforcing WiFiSec, an IPsec-based VPN overlay for wireless networking. As wireless network traffic successfully passes through these layers, it is then passed to the VPN-NAT-Stateful firewall layer where WiFiSec termination, address translation, and access rules are applied. If all of the security criteria is met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- DMZ or other zone on Opt port
- VPN tunnel

The screenshot shows the SonicWall management interface. On the left is a navigation menu with options like System, Network, Modern, Wireless, Status, Settings, WEP/WPA Encryption, Advanced, MAC Filter List, IDS, SonicPoint, Firewall, VPN, Users, Security Services, Log, Wizards, Help, and Logout. The main content area is titled 'Wireless > Status' and includes a 'Clear Statistics' button. Below this is the 'Access Point 'sonicwall' Status' section, which is divided into two panels: 'WLAN Settings' and 'WLAN Statistics'.

WLAN Settings:

- WLAN: Enabled
- WiFiSec Enforcement: Enabled
- SSID: sonicwall
- MAC Address (BSSID): 00:08:01:12:4D:FC
- WLAN IP Address: 172.18.31.1
- WLAN Subnet Mask: 255.255.255.0
- Regulatory Domain: FCC - North America
- Channel: AutoChannel - Currently Channel 1
- Radio Tx Rate: 54 Mbps
- Radio Tx Power: High
- Authentication Type: Disabled
- MAC Filter List: Disabled
- Wireless Guest Services: Disabled
- Intrusion Detection: Enabled
- Wireless Firmware: 1.0.4.3
- Associated Stations: 1 of 32 maximum
- Radio Mode: 2.4GHz 802.11bg Mixed

WLAN Statistics:

Wireless Statistics	Bx	Tx
Unicast Frames	31	1088
Multicast Frames	69	78
Fragments	0	0
Total Packets	100	82
Total Bytes	12697	6695
Errors	N/A	4042
Single Retry Frames	N/A	0
Multiple Retry Frames	N/A	0
Retry Limit Exceeded	N/A	0
Discards	2151282444	0
Discards Bad WEP Key	0	N/A
FCS Errors	141991	N/A
Frames Received	1263664	N/A
Frames Aborted	53483	N/A
Frames Aborted Phy	555265	N/A
Duplicate Frames	0	N/A

Below the statistics is the 'Station Status' table:

Station	MAC Address	Authenticated	Associated	AD	Signal	Timeout	Configure
1	00:90:4B:76:20:3B	Authenticated	Associated	25	94%	48s	

At the bottom of the station status table is a 'Delete All' button. The status bar at the very bottom of the interface shows 'Status: Ready'.

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the TZ 170 Wireless is a firewall and has NAT capabilities which provides security, and you can use WiFiSec to secure data transmissions.

Recommendations for Optimal Wireless Performance

- Place the TZ 170 Wireless near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the TZ 170 Wireless and the receiving points such as PCs or laptops.
- Try to place the TZ 170 Wireless in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.

- Building construction can make a difference on wireless performance. Avoid placing the TZ 170 Wireless near walls, fireplaces, or other large solid objects. Placing the TZ 170 Wireless near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the TZ 170 Wireless is installed near these types of materials.
- Installing the TZ 170 Wireless in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the TZ 170 Wireless. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the TZ 170 Wireless.

Adjusting the Antennas

The antennas on the TZ 170 Wireless can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the TZ 170 Wireless, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the SonicWALL GroupVPN are not counted towards the node enforcement on the SonicWALL. Only users on the LAN and non-Wireless zones on the Opt port are counted towards the node limit.

The Station Status table lists all the wireless nodes connected.

MAC Filter List

The SonicWALL TZ 170 Wireless networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

WiFiSec Enforcement

Enabling **WiFiSec Enforcement** on the TZ 170 Wireless enforces the use of IPsec-based VPN for access from the WLAN to the WAN or LAN, and provides access from the WLAN to the WAN independent of WGS. Access from one wireless client to another is configured on the **Wireless > Advanced** page where you can disable or enable access between wireless clients.

WiFiSec uses the easy provisioning capabilities of the SonicWALL Global VPN client making it easy for experienced and inexperienced administrators to implement on the network. The level of interaction between the Global VPN Client and the user depends on the WiFiSec options selected by the administrator. WiFiSec IPsec terminates on the WLAN/LAN port, and is configured using the Group VPN Security Policy including noneditable parameters specifically for wireless access.

Wireless > Status

The **Wireless > Status** page provides status information for wireless network, including **WLAN Settings**, **WLAN Statistics**, and **Station Status**.

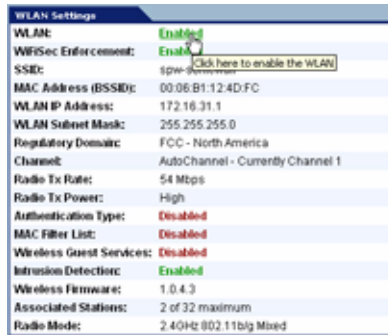


The **Wireless > Status** page has three tables:

- **WLAN Settings**
- **WLAN Statistics**
- **Station Status**

WLAN Settings

The **WLAN Settings** table lists the configuration information for the built-in radio. All configurable settings in the **WLAN Settings** table are hyperlinks to their respective pages for configuration. Enabled features are displayed in green, and disabled features are displayed in red. Click on a setting to go the page in the Management Interface where you can configure that setting.



WLAN Settings

WLAN Settings	Value
WLAN:	Enabled or Disabled
WiFiSec Enforcement:	Enabled or Disabled
SSID:	Wireless network identification information
MAC Address (BSSID):	Serial Number of the TZ 170 Wireless
WLAN IP Address:	IP address of the WLAN port
WLAN Subnet Mask:	Subnet information
Regulatory Domain	FCC - North America for domestic appliances ETSI - Europe for international appliances
Channel	Channel Number selected for transmitting wireless signal
Radio Tx Rate	Network speed in Mbps
Radio Tx Power	Current power level of the radio signal transmission
Authentication Type	Encryption settings for the radio, or Disabled--see the Wireless > WEP/WPA Encryption page
MAC Filter List:	Enabled or Disabled
Wireless Guest Services	Enabled or Disabled
Intrusion Detection	Enabled or Disabled
Wireless Firmware:	Firmware version on the radio card
Associated Stations:	Number of clients associated with the TZ 170 Wireless
Radio Mode	Current power level of the radio signal transmission

WLAN Statistics




WLAN Statistics: The **WLAN Statistics** table lists all of the traffic sent and received through the WLAN. The **Wireless Statistics** column lists the kinds of traffic recorded, the **Rx** column lists received traffic, and the **Tx** column lists transmitted traffic.

Wireless Statistics	Rx/TX
Unicast Frames	Number of frames received and transmitted
Multicast Frames	Total number of frames received and transmitted as broadcast or multicast. Typically a lower number than Unicast frames.
Fragments	Total number of fragmented frames received and sent. This is a general indication of activity at this wireless device.
Total Packets	Total number of packets received and transmitted.
Total Bytes	Total number of bytes received and transmitted.
Errors	Number of times a transmission resulted in an error.




Wireless Statistics	Rx/TX
Signal Retry Frames	Number of messages retransmitted a single time being acknowledged by the receiving device. Retransmission is normal for 802.11b to quickly recover from lost messages.
Multiple Retry Frames	Number of messages retransmitted multiple times before acknowledgement by the receiving device. A relatively high value can indicate interference or a heavy wireless data load.
Retry Limit Exceeded	Number of messages undelivered after the maximum number of transmissions. Along with Discards, it can indicate a wireless network under heavy interference or excessive load of wireless data traffic.
Discards	Number of messages untransmitted due to congestion. Normally, the messages are temporarily stored in an internal buffer until transmitted. When the buffer is full, frames are discarded until the buffer is cleared. When the number is high, it may indicate a wireless network with a heavy load of traffic.
Discards: Bad WEP Key	Number of times a received message was discarded because it could not be decrypted. This could indicate mismatched keys or one device does not support encryption or does not have encryption enabled.
FCS Errors	Number of received frames or frame parts containing an erroneous checksum requiring deletion. Messages are recovered using ACK and retransmitted by the sending device.
Frames Received	Total number of frames received.
Frames Aborted	Total number of frames aborted while receiving
Frames Aborted Phy	Total number of frames aborted
Duplicate Frames	Number or duplicate frames received.

Station Status

The **Station Status** table displays information about wireless connections associated with the TZ 170 Wireless.

Station	MAC Address	Authenticated	Associated	AID	Signal	Timeout	Configure
1	00:06:B1:12:4D:FC	Authenticated	Associated	56	0%	60s	  

Delete All

- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated** - status of 802.11b authentication
- **Associated** - status of 802.11b association
- **AID** - Association ID, assigned by the security appliance
- **Signal** - strength of the radio signal
- **Timeout** - number of seconds left on the session
- **Configure**
 - ♦  - configure power management on the wireless network card of this station, if enabled.
 - ♦  - block the station from the security appliance and add it to the Deny MAC Filter List.
 - ♦  - dissociate the station from the security appliance.

Configuring Wireless Settings

Wireless > Settings

The **Wireless > Settings** page allows you to configure your wireless settings.

On the **Wireless>Settings** page, you can enable or disable the WLAN port by selecting or clearing the **Enable WLAN** checkbox.



Wireless Radio Mode

Select either **Access Point** to configure the SonicWALL as the default gateway on your network or select **Wireless Bridge** from the **Radio Role** menu to configure the SonicWALL to act as an intermediary wireless device.



Note: WPA support is only available in Access Point Mode. WPA support is not available in Wireless Bridge Mode.

Wireless Settings

Enable WLAN Radio: Check this checkbox to turn the radio on, and enable wireless networking. Click **Apply** in the top right corner of the administrative interface to have this setting take effect.

Schedule: The schedule determines when the radio is on to send and receive data. The default value is **Always on**. The Schedule list displays the schedule objects you create and manage in the **System > Schedule** page. The default choices are:

- **Always on**
- **M-T-W-TH-F 08:00-17:00**
- **M-T-W-TH-F 00:00-08:00**
- **M-T-W-TH-F 17:00-24:00**
- **SA-SU 00:00-24:00**
- **SA-SU 00:00-24:00**

SSID: The default value, **sonicwall**, for the SSID can be changed to any alphanumeric value with a maximum of 32 characters.

Radio Mode: Select your preferred radio mode from the **Radio Mode** menu. The TZ 170 Wireless supports the following modes:

- **2.4GHz 802.11b/g Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.
- **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **802.11b Only** - Select this mode if only 802.11b clients access your wireless network.

Regulatory: Specifies the regulatory domain--the country whose radio broadcasting rules the security appliance must obey. **FCC - North America** is displayed as the **Regulatory Domain**. This field is determined by the ROM code, and cannot be changed by the user.

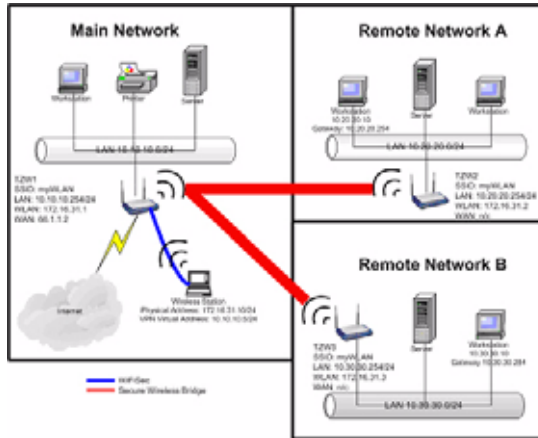
Country Code: Specifies the country whose radio broadcasting rules the security appliance must obey.

Channel: Select the channel for transmitting the wireless signal from the **Channel** menu. An **AutoChannel** setting allows the TZ 170 Wireless to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. AutoChannel is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.

Secure Wireless Bridging

Wireless Bridging is a feature that allows two or more physically separated networks to be joined over a wireless connection. The TZ 170 Wireless provides this capability by shifting the radio mode at remote networks from **Access Point** mode to **Wireless Bridge** mode. Operating in Wireless Bridge

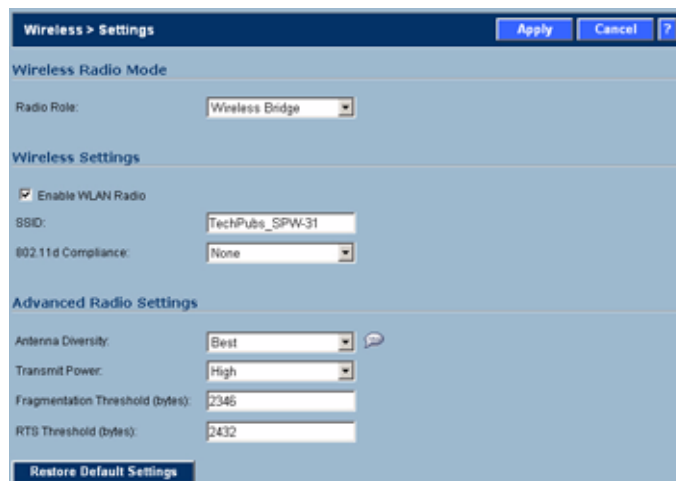
mode, the TZ 170 Wireless connects to another TZ 170 Wireless acting as an access point, and allows communications between the connected networks via the wireless bridge.



Secure Wireless Bridging employs a WiFiSec VPN policy, providing security to all communications between the wireless networks. Previous bridging solutions offered no encryption, or at best, WEP encryption.

Configuring a Secure Wireless Bridge

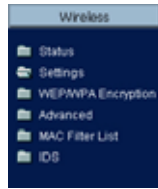
When switching from **Access Point** mode to **Wireless Bridge** mode, all clients are disconnected, and the navigation panel on the left changes to reflect the new mode of operation.



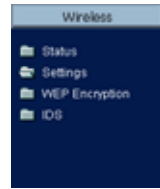
To configure a secure wireless bridge, follow these steps:

- 1 Click **Wireless**, then **Settings**.


- 2 In the **Wireless Radio Mode** section, select **Wireless Bridge** from the **Radio Role** menu. The TZ 170 Wireless updates the interface. The left-navigation menu changes to reflect the choices that apply to configuring a secure wireless bridge.



Wireless Menu
Access Point Mode



Wireless Menu
Wireless Bridge Mode

- 3 In the left-navigation menu, click **Status** under **Wireless**. Any available access point is displayed at the bottom of the **Status** page. Click the **Connect** icon  to establish a wireless bridge to another TZ 170 Wireless.
- 4 In the left-navigation menu, click **Settings** under **Wireless**. Configure the WLAN settings for the wireless connection as follows:
 - a Configure the SSID on all TZ 170 Wireless to the SSID of the Access Point.
 - b Configure the WLAN for all TZ 170 Wireless must be on the same subnet.
 - c LAN IP address for all TZ 170 Wireless must be on different subnets.

For example, in the previous network diagram, the TZ 170 Wireless are configured as follows:

- SSID on all three TZ 170 Wireless are set to “myWLAN”.
- WLAN addressing for all the TZ 170 Wireless's connected via Wireless Bridge must place the WLAN interfaces on the same subnet: 172.16.31.1 for TZ 170 Wireless1, 172.16.31.2 for TZ 170 Wireless2, and 172.16.31.3 for TZ 170 Wireless3.
- TZ 170 Wireless4 must have a different subnet on the WLAN, such as 172.16.32.X/24.
- LAN addressing for all TZ 170 Wireless connected via Wireless Bridge must place the LAN interfaces on different subnets: 10.10.10.x/24 for TZ 170 Wireless1, 10.20.20.x/24 for TZ 170 Wireless2, and 10.30.30.x/24 for TZ 170 Wireless3.
- LAN addressing for TZ 170 Wireless4 must be the same as TZ 170 Wireless3.
- To facilitate Virtual Adapter addressing, the TZ 170 Wireless4 can be set to forward DHCP requests to TZ 170 Wireless3.
- When a TZ 170 Wireless is in Wireless Bridge mode, the channel cannot be configured. TZ 170 Wireless2 and TZ 170 Wireless3 operate on the channel of the connecting Access Point TZ 170 Wireless. For example, TZ 170 Wireless1 is on channel 1.
- A Bridge Mode TZ 170 Wireless cannot simultaneously support wireless client connections. Access Point services at Remote Site B are provided by a second TZ 170 Wireless (4). The channel of operation is set 5 apart from the channel inherited by the TZ 170 Wireless3. For example, Access Point TZ 170 Wireless1 is set to channel 1, then Bridge Mode TZ 170 Wireless3 inherits channel 1. Access Point TZ 170 Wireless4 should be set to channel 6.

Network Settings for the Example Network

Device	Mode	SSID	Channel	LAN IP Address	WLAN IP Address
TZ 170 Wireless1	Access Point	myWLAN	1	10.10.10.254/24	172.16.31.1/24
TZ 170 Wireless2	Wireless Bridge	myWLAN	1 (auto)	10.20.20.254/24	172.16.31.2/24
TZ 170 Wireless3	Wireless Bridge	myWLAN	1 (auto)	10.30.30.254/24	172.16.31.3/24
TZ 170 Wireless4	Access Point	otherWLAN	6	10.30.30.253/24	172.16.31.1/24

Wireless Bridging (without WiFiSec)

To provide compatibility with other non-WiFiSec wireless access points, the TZ 170 Wireless supports a non-secure form of wireless bridging, but insecure wireless communications should only be employed when data is non-sensitive. By default, **WiFiSec Enforcement** is enabled on **Wireless Settings** for **Wireless Bridge** Mode. To connect to a non-WiFiSec access point, this checkbox must be disabled. Since VPN tunnels are not established in non-secure Wireless Bridging deployments, traffic routes must be clearly defined for both the Access Point and the Bridge Mode sites:

- The default route on the Bridge Mode TZ 170 Wireless must from the WLAN interface to the WLAN interface of the connecting Access Point TZ 170 Wireless.
 - Referring to the example above, the default route on TZ 170 Wireless2 and TZ 170 Wireless3 is set via their WLAN interfaces to 172.16.31.1.
- Static routes must be entered on the Access Point TZ 170 Wireless to route back to the LAN subnets of the Bridge Mode TZ 170 Wireless.
 - Referring to the example network, TZ 170 Wireless1 must have static routes to 10.20.20.x/24 via 172.16.31.2 and to 10.30.30.x/24 via 172.16.31.3

Configuring VPN Policies for the Access Point and Wireless Bridge

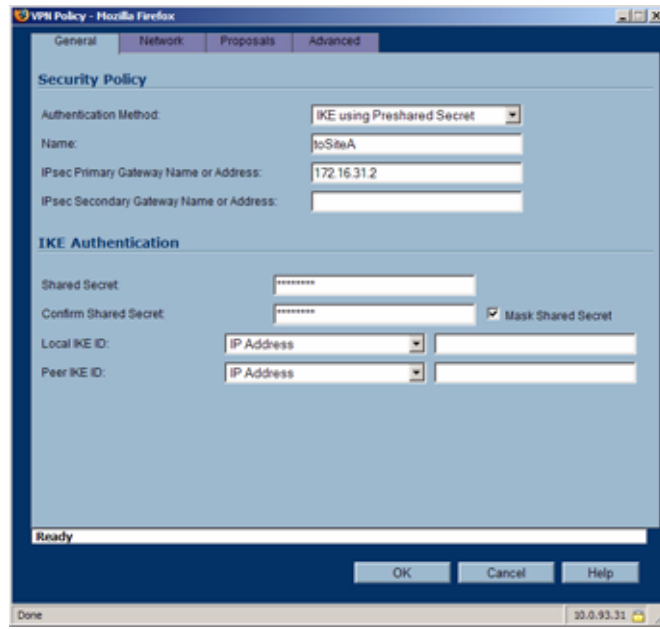
Access Point

After Wireless Settings are defined, the WiFiSec connections (VPN Policies) must be configured. The VPN Policies are defined as would any other site-to-site VPN policy, typically with the following in mind:

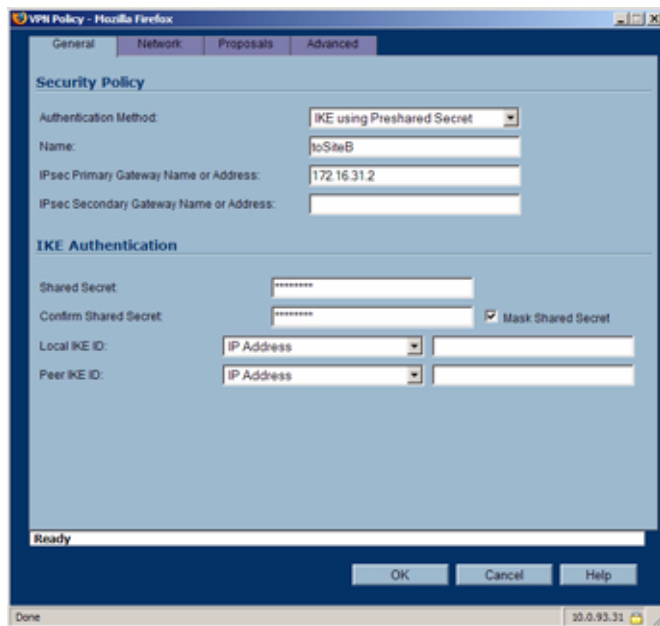
- The Access Point TZ 170 Wireless must specify the destination networks of the remote sites.
- The Access Point TZ 170 Wireless must specify its LAN management IP address as the **Default LAN Gateway** under the **Advanced** tab.
- The Wireless Bridge Mode TZ 170 Wireless must be configured to use the tunnel as the default route for all internet traffic.

Referring to the example network, the Access Point TZ 170 Wireless has the following two VPN Policies defined:

- One policy to the Site_A address object at 10.20.20.0:

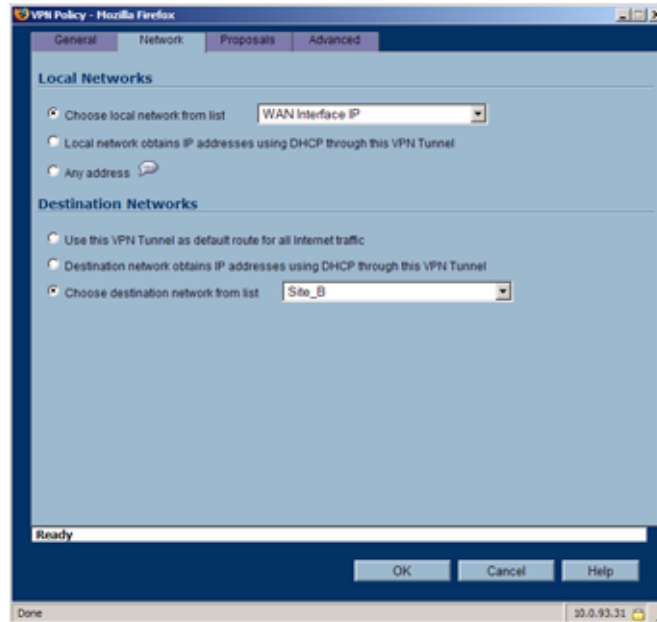


- One policy to the Site_B address object at 10.30.30.0:

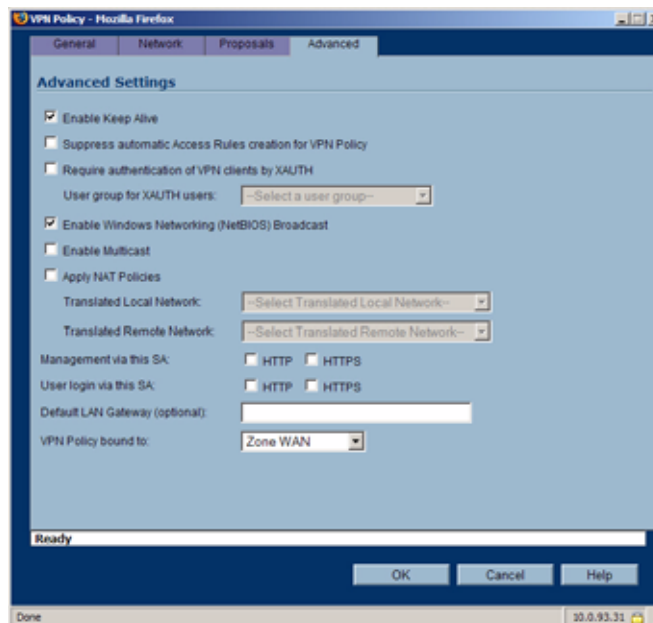


Configuration for VPN Policies

1. Click **Network**.
2. Under **Local Networks**, select **Choose local network from list** and select **LAN Interface IP**.
3. Under **Destination Networks**, select **Choose destination network from list** and select or create an address object for the destination (Site_A - 10.20.20.0 or Site_B - 10.30.30.0 in the example).



4. Click **Advanced**.
5. Select **Enable Keep Alive**.
6. Select **Enable Windows Networking (NetBIOS) Broadcast**.
7. Click **OK** to close the window, and then click **Apply** for the settings to take effect on the SonicWALL.



Wireless Bridge VPN Policy

The Wireless Bridge VPN Policy is configured as follows:

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

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

Configuring WEP/WPA Encryption

Wireless > WEP/WPA Encryption

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

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

Wi-Fi Protected Access (WPA) provides much greater security than WEP. WPA has two authentication modes:

- WPA-PSK (Pre-Shared Key) uses a pre-shared key, similar to IKE.
- WPA-EAP (External Authentication Protocol) requires a separate authentication protocol, such as RADIUS, be used to authenticate all users.



WEP Encryption Settings

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

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

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

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

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

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

WEP Encryption Keys

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

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

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

WPA Encryption Settings

WPA supports two protocols for storing and generating keys:

- *Extensible Authentication Protocol (EAP)*: EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.
- *Pre-Shared Key (PSK)*: PSK allows WPA to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.



Note: WPA support is only available in Access Point Mode. WPA support is not available in Bridge Mode.

WPA-PSK Settings

The screenshot shows the 'Wireless > WEP/WPA Encryption' configuration window. The 'Authentication Type' dropdown is set to 'WPA-PSK'. Under the 'WPA Settings' section, 'Cipher Type' is set to 'TKIP', 'Group Key Update' is set to 'By Timeout', and 'Interval (seconds)' is set to '86400'. Under the 'Preshared Key Settings (PSK)' section, there is a text input field for 'Passphrase'.

Encryption Mode: In the **Authentication Type** field, select **WPA-PSK**.

WPA Settings:

- **Cipher Type:** select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update:** Select the how to determine when to update the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.
- **Packet Threshold:** If you selected **By Packet**, select the number (x 1000) of packets to pass before generating a new group key.

Preshared Key Settings (PSK)

- **Passphrase:** Enter the passphrase from which the key is generated.

Click **Apply** in the top right corner to apply your WPA settings.

WPA-EAP Settings

The screenshot shows the 'Wireless > WEP/WPA Encryption' configuration window. The 'Authentication Type' dropdown is set to 'WPA-EAP'. Under the 'WPA Settings' section, 'Cipher Type' is set to 'TKIP', 'Group Key Update' is set to 'By Timeout', and 'Interval (seconds)' is set to '86400'. Under the 'Extensible Authentication Protocol Settings (EAP)' section, there are input fields for 'Radius Server 1 IP', 'Port', 'Radius Server 1 Secret', 'Radius Server 2 IP', 'Port', and 'Radius Server 2 Secret'.

Encryption Mode: In the **Authentication Type** field, select **WPA-EAP**.

WPA Settings:

- **Cipher Type:** select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.

- **Group Key Update:** Select the how to determine when to update the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.
- **Packet Threshold:** If you selected **By Packet**, select the number (x 1000) of packets to pass before generating a new group key.

Extensible Authentication Protocol Settings (PSK)

- **Radius Server 1 IP and Port:** Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret:** Enter the password for access to Radius Server
- **Radius Server 2 IP and Port:** Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret:** Enter the password for access to Radius Server

Click **Apply** in the top right corner to apply your WPA settings.

Configuring Advanced Wireless Settings

Wireless > Advanced

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



Beaconing & SSID Controls

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

Advanced Radio Settings

The TZ 170 Wireless employs dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the TZ 170 Wireless, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal.

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

The **Antenna Diversity** setting determines which antenna the TZ 170 Wireless uses to send and receive data. You can select:

- **Best:** This is the default setting. When **Best** is selected, the TZ 170 Wireless automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
- **1:** Select **1** to restrict the TZ 170 Wireless to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the console port. You can disconnect antenna 2 when using only antenna 1.
- **2:** Select **2** to restrict the TZ 170 Wireless to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the power supply. You can disconnect antenna 1 when using only antenna 2.



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

1. Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.
2. The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
3. The **RTS Threshold (bytes)** is 2432 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
4. The default value for the **DTIM Interval** is 3. Increasing the DTIM Interval value allows you to conserve power more effectively.
5. The **Station Timeout (seconds)** is 300 seconds by default. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Station Timeout (seconds)** field.
6. Set the **Maximum Client Associations** to limit the number of stations that can connect wirelessly at one time. The default is 32.

Click **Restore Default Settings** to return the radio settings to the default settings. Click **Apply** in the top right corner of the page to apply your changes to the security appliance.

Configuring MAC Filter List

Wireless > MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the TZ 170 Wireless. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card.

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



Allow or Deny Specific Resources

The MAC **Allow List** contains groups of address objects for network resources that the security appliance allows to connect via the WLAN, regardless of the selections in the deny list.

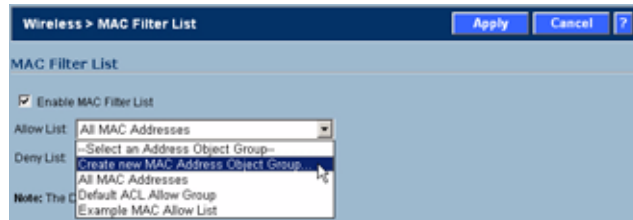
The MAC **Deny List** contains groups of address objects for network resources that the security appliance denies to connect via the WLAN, regardless of the selections in the deny list.

The items in the list are address object groups--defined groups of objects that represent specific IP addresses or ranges of addresses that can be used throughout the Management Interface to specify network resources. An address object group can contain other address object groups.

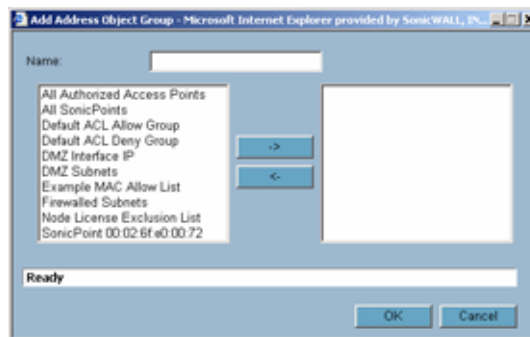
The Allow List and Deny List are also address object groups.

You can create individual objects in the **Wireless > Mac Filter List** page:

- 1 In the **Allow List** or **Deny List** box, select Create New MAC Address Object Group.



- 2 In the Add Address Object Group box, enter a name for the new group
- 3 In the left column, select the groups or individual address objects you want to allow or deny. You can use **Ctrl-click** select more than one item.
- 4 Click the -> button to add the items to the group.



- 5 Click **OK** to create the group and add it to the **Allow List** or **Deny List**.

Configuring Wireless IDS

Wireless > IDS

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

Wireless Bridge IDS

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

MAC Address (BSSID)	SSID	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
00:06:B1:12:4B:A1	TechPubs_TZ170W	1	SonicWALL	100 - Excellent	54 Mbps	
00:40:10:58:60:29	dtelehow	1	SonicWALL	80 - Excellent	11 Mbps	
00:02:8F:2E:21:34	voip1	1	Senao	75 - Very good	54 Mbps	
00:06:B1:12:4C:F7	depwall-one	1	SonicWALL	70 - Very good	54 Mbps	
00:50:E8:02:05:8E	VSI-BC	1	Unknown	70 - Very good	54 Mbps	
00:06:B1:12:4C:11	local_tz170w_102	1	SonicWALL	80 - Excellent	54 Mbps	
00:06:B1:13:5A:89	sonicwall	1	SonicWALL	78 - Very good	54 Mbps	
00:02:8F:2E:21:FA	sp0	1	Senao	83 - Excellent	54 Mbps	

Access Point IDS

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

MAC Address (BSSID)	SSID	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
00:02:8F:2E:20:C4	sonicwall	3	Senao	79 - Very good	54 Mbps	
00:06:B1:12:4C:20	sonicwall	1	SonicWALL	88 - Excellent	54 Mbps	
00:06:B1:12:4D:F0	sonicwall	4	SonicWALL	78 - Very good	54 Mbps	
00:02:8F:2E:20:F8	sonicwall	3	Senao	78 - Very good	54 Mbps	
00:02:8F:2E:21:CC	sonicwall	1	Senao	81 - Excellent	54 Mbps	
00:06:B1:12:71:6B	SWBETA	1	SonicWALL	75 - Very good	54 Mbps	

Enable Client Null Probing

Enabling this setting allows the TZ 170 Wireless to detect and log Null Probes, such as those used by Netstumbler and other similar tools.

Association Flood Detection

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

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

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

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

Intrusion Detection Settings

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

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


Enable Rouge Access Point Detection is enabled by default. The **Authorized Access Points** menu allows you to specify **All Authorized Access Points**, **Create new MAC Address Object Group**, or **Select an Address Object Group**.

The **Authorized Access Points** menu allows you to specify which access points the SonicWALL security appliance will considered authorized when it performs a scan. You can select **All Authorized Access Points** to allow all SonicPoints, or you can select **Create new MAC Address Object Group** to create an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group.

Select **Create Address Object Group** to add a new group of MAC address objects to the list.

Discovered Access Points

The **Discovered Access Points** table displays information on every access point that can be detected by all your SonicPoints or on a individual SonicPoint basis:

- **MAC Address (BSSID):** The MAC address of the radio interface of the detected access point.
- **SSID:** The radio SSID of the access point.
- **Channel:** The radio channel used by the access point.
- **Manufacturer:** The manufacturer of the access point. SonicPoints will show a manufacturer of either SonicWALL or Senao.
- **Signal Strength:** The strength of the detected radio signal
- **Max Rate:** The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize:** Click the icon  in the **Authorize** column to add the access point to the address object group of authorized access points.

Scanning for Access Points


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

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



Alert: *The **Scan Now** feature causes a brief disruption in service. If this is a concern, wait and use the **Scan Now** feature at a time when no clients are active, or the potential for disruption becomes acceptable.*

Authorizing Access Points on Your Network

Access Points detected by the TZ 170 Wireless are regarded as rogues until they are identified to the TZ 170 Wireless as authorized for operation. To authorize an access point, select it in the list of access points discovered by the TZ 170 Wireless scanning feature, and add it clicking the **Authorize** icon .

PART

6

SonicPoint

Managing SonicPoints

SonicPoint > SonicPoints

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances running SonicOS Enhanced 3.0 or greater to provide wireless access throughout your enterprise.

The SonicPoint section of the Management Interface lets you manage the SonicPoints connected to your system.

The screenshot displays the SonicWALL Management Interface for SonicPoints. It is divided into two main sections: SonicPoint Provisioning Profiles and SonicPoints.

SonicPoint Provisioning Profiles: This section shows a table with columns for Name Prefix, Applied Zone, 802.11a Radio, 802.11g Radio, and Configure. A single profile is listed with Name Prefix 'SonicPoint', Applied Zone 'WLAN', and both radio channels set to 'AutoChannel'. Below the table are 'Add', 'Delete', and 'Delete All' buttons.

SonicPoints: This section shows a table with columns for Name, Interface, Network Settings, Status, 802.11a Radio, 802.11g Radio, Enable, and Configure. A single SonicPoint is listed with Name 'SonicPoint00072 X4 (WLAN)', Interface 'X4 (WLAN)', IP '175.31.16.223', MAC '00:02:6f:e0:00:72', and Status 'Rebooting'. Below the table are 'Delete' and 'Delete All' buttons.

Note: All Operational SonicPoints are upgraded to SonicPoint Firmware Version 3.0.0.0. Download

Before Managing SonicPoints

Before you can manage SonicPoints in the Management Interface, you must first:

- Configure your SonicPoint Provisioning Profiles
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign an interface to the Wireless zone.
- Attach the SonicPoints to the interfaces in the Wireless zone.
- Test SonicPoints

SonicPoint Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

SonicOS includes a default SonicPoint profile, named SonicPoint. You can modify this profile or create a new one.


The default SonicPoint profile has the following settings:

802.11a Radio		802.11g Radio	
Enable 802.11a Radio	Yes - Always on	Enable 802.11g Radio	Yes - Always on
SSID	SonicWALL	SSID	SonicWALL
Radio Mode	54Mbps - 802.11a	Radio Mode	2.4 GHz 54Mbps - 802.11g
Channel	AutoChannel	Channel	AutoChannel
ACL Enforcement	Disabled	ACL Enforcement	Disabled
Authentication Type	WEP - Both Open System & Shared Key	Authentication Type	WEP - Both Open System & Shared Key
Schedule IDS Scan	Disabled	Schedule IDS Scan	Disabled
Data Rate	Best	Data Rate	Best
Antenna Diversity	Best	Antenna Diversity	Best

Configuring a SonicPoint Profile

You can add any number of SonicPoint profiles. To configure a SonicPoint provisioning profile:

- 1 To add a new profile click **Add** below the list of SonicPoint provisioning profiles

To edit an existing profile, select the profile and click the edit icon  in the same line as the profile you are editing.

- 2 In the **General** tab of the Add Profile window, specify:



- ♦ **Enable SonicPoint:** Check this to automatically enable each SonicPoint when it is provisioned with this profile.
 - ♦ **Name Prefix:** Enter a prefix for the names of all SonicPoints connected to this zone. When each SonicPoint is provisioned it is given a name that consists of the name prefix and a unique number, for example: "SonicPoint 126008."
 - ♦ **Country Code:** Select the country where you are operating the SonicPoints. The country code determines which regulatory domain the radio operation falls under.
- 3 In the **802.11g** tab, Configure the radio settings for the 802.11g (2.4GHz band) radio:

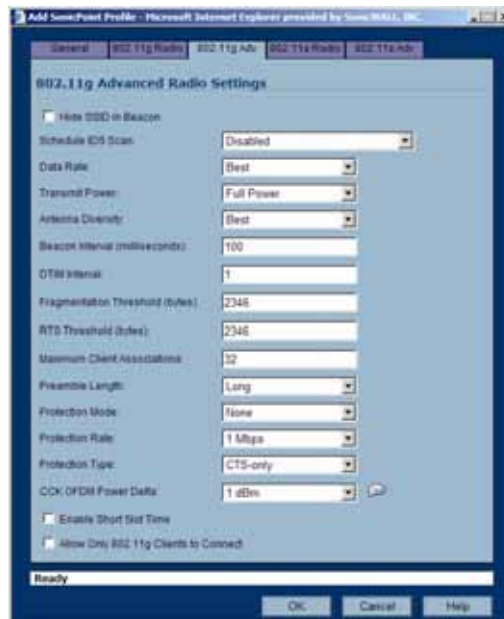


- ◆ **Enable 802.11g Radio:** Check this to automatically enable the 802.11g radio bands on all SonicPoints provisioned with this profile.
- ◆ Select a schedule to determine when the radio is enabled. The default is **Always on**. you can create and manage Schedule objects in the **System > Schedules** page of the management interface.
- ◆ **SSID:** Enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.



Note: *If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.*

- ◆ **Radio Mode:** Select the speed of the wireless connection. You can choose **11Mbps - 802.11b**, **54 Mbps - 802.11g**, or **108 Mbps - Turbo G** mode. If you choose Turbo mode, all users in your company must use wireless access cards from the same manufacturer.
 - ◆ **Channel:** Select the channel the radio will operate on. The default is **AutoChannel**, which automatically selects the channel with the least interference. Use AutoChannel unless you have a specific reason to use or avoid specific channels.
 - ◆ **ACL Enforcement:** Select this to enforce Access Control by allowing or denying traffic from specific devices. Select a MAC address group from the **Allow List** to automatically allow traffic from all devices with MAC address in the group. Select a MAC address group from the **Deny List** to automatically deny traffic from all devices with MAC address in the group. The deny list is enforced before the Allow list.
 - ◆ **Authentication Type:** Select the method of authentication for your wireless network. You can select **WEP - Both (Open System & Shared Key)**, **WEP - Open System**, **WEP - Shared Key**, **WPA - PSK**, or **WPA - EAP**.
 - ◆ **WEP Key Mode:** Select the size of the encryption key.
 - ◆ **Default Key:** Select which key in the list below is the default key, which will be tried first when trying to authenticate a user.
 - ◆ **Key Entry:** Select whether the key is alphanumeric or hexadecimal.
 - ◆ **Key 1 - Key 4:** Enter the encryption keys for WEP encryption. Enter the most likely to be used in the field you selected as the default key.
- 4 In the **802.11g Advanced** tab, configure the performance settings for the 802.11g radio. For most 802.11g advanced options, the default settings give optimum performance.



- ◆ **Hide SSID in Beacon:** Check this option to have the SSID broadcast as part of the wireless beacon, rather than as a separate broadcast.

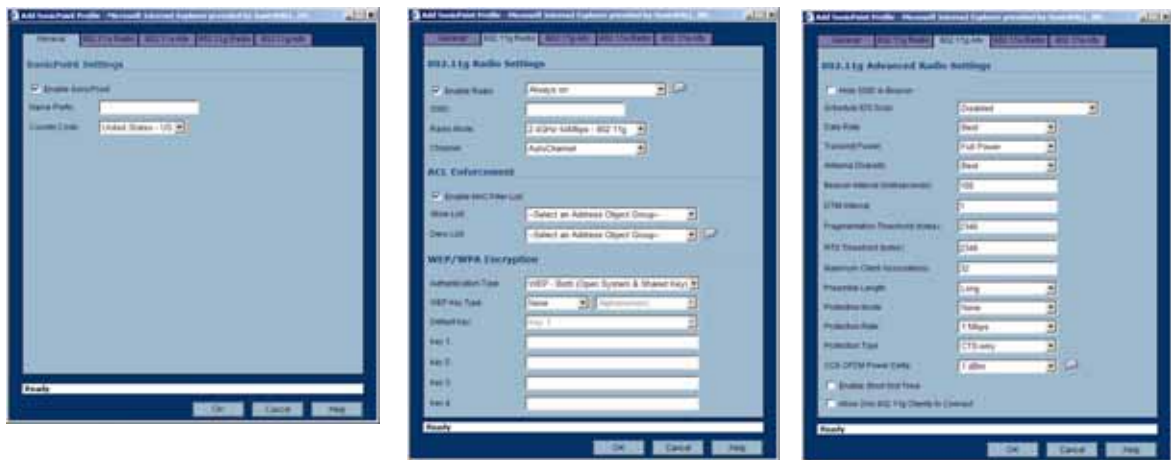
- ♦ **Schedule IDS Scan:** Select a time when there are fewer demands on the wireless network to schedule an Intrusion Detection Service (IDS) scan to minimize the inconvenience of dropped wireless connections.
 - ♦ **Data Rate:** Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. You can select: **Best, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, or 54 Mbps.**
 - ♦ **Transmit Power:** Select the transmission power. Transmission power effects the range of the SonicPoint. You can select: **Full Power, Half (-3 dB), Quarter (-6 dB), Eighth (-9 dB), or Minimum.**
 - ♦ **Antenna Diversity:** The **Antenna Diversity** setting determines which antenna the SonicPoint uses to send and receive data. You can select:
 - **Best:** This is the default setting. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
 - **1:** Select **1** to restrict the SonicPoint to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the power supply.
 - **2:** Select **2** to restrict the SonicPoint to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the console port.
 - ♦ **Beacon Interval (milliseconds):** Enter the number of milliseconds between sending out a wireless beacon.
 - ♦ **DTIM Interval:** Enter the interval in milliseconds.
 - ♦ **Fragmentation Threshold (bytes):** Enter the number of bytes of fragmented data you want the network to allow.
 - ♦ **RTS Threshold (bytes):** Enter the number of bytes.
 - ♦ **Maximum Client Associations:** Enter the maximum number of clients you want the SonicPoint to support on this radio at one time.
 - ♦ **Preamble Length:** Select the length of the preamble--the initial wireless communication send when associating with a wireless host. You can select **Long** or **Short**.
 - ♦ **Protection Mode:** Select the CTS or RTS protection. Select **None, Always, or Auto.** **None** is the default.
 - ♦ **Protection Rate:** Select the speed for the CTS or RTS protection, **1 Mbps, 2 Mbps, 5 Mbps, or 11 Mbps.**
 - ♦ **Protection Type:** Select the type of protection, **CTS-only** or **RTS-CTS.**
 - ♦ **CCK OFDM Power Delta:** Select the difference in radio transmit power you will allow between the 802.11b and 802.11g modes: 0 dBm, 1 dBm, or 2 dBm.
 - ♦ **Enable Short Slot Time:** Allow clients to disassociate and reassociate more quickly.
 - ♦ **Allow Only 802.11g Clients to Connect:** Use this if you are using Turbo G mode and therefore are not allowing 802.11b clients to connect.
- 5 Configure the settings in the **802.11a Radio** and **802.11a Advanced** tabs. These settings affect the operation of the 802.11a radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.
- The settings in the **802.11a Radio** and **802.11a Advanced** tabs are similar to the settings in the **802.11g Radio** and **802.11g Advanced** tabs. Follow the instructions in step 3 and step 4 in this procedure to configure the 802.11a radio.

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP Address 192.168.1.20, username: admin, password: password). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint does locate, or is located by a peer SonicOS device, via the SonicWALL Discovery Protocol, an encrypted exchange between the two units will ensue wherein the profile assigned to the relevant Wireless Zone will be used to automatically configure (provision) the newly added SonicPoint unit.

#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
1	SonicPointe00072	OPT (WLAN)	IP: 0.0.0.247 MAC: 00:02:8F:e0:00:72	Initializing	SSID: sonicwall Channel: AutoChannel	SSID: sonicwall Channel: AutoChannel	<input type="checkbox"/>	

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and Zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant Zone to configure the 2.4GHz and 5GHz radio settings.



Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- Via manual configuration changes – Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its Zone.
- Via un-provisioning – Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a Zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Updating SonicPoint Settings

You can change the settings of any individual SonicPoint list on the **Wireless > SonicPoints** page.

Edit SonicPoint settings

To edit the settings of an individual SonicPoint:

- 1 Under SonicPoint Settings, click the Edit icon in the same line as the SonicPoint you want to edit.
- 2 In Edit SonicPoint screen, make the changes you want. The Edit SonicPoint screen has the following tabs:

- ◆ **General**
- ◆ **802.11a Radio**
- ◆ **802.11a Advanced**
- ◆ **802.11g Radio**
- ◆ **802.11g Advanced**

The options on these tabs are the same as the Add SonicPoint Profile screen. See [Configuring a SonicPoint Profile](#) for instructions on configuring these settings.

- 3 Click **OK** to apply these settings.

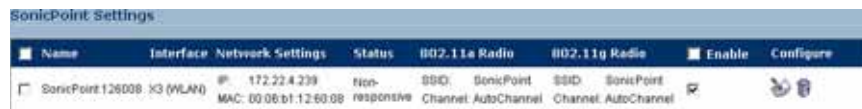
Synchronize SonicPoints

Click **Synchronize SonicPoints** at the top of the **SonicPoint > SonicPoints** page to update the settings for each SonicPoint reported on the page. When you click **Synchronize SonicPoints**, SonicOS polls all connected SonicPoints and displays updated settings on the page.

Enable and Disable Individual SonicPoints

You can enable or disable individual SonicPoints on the **SonicPoint > SonicPoints** page:

- 1 Check the box under Enable to enable the SonicPoint, uncheck the box to disable it.



- 2 Click **Apply** at the top of the **SonicPoint > SonicPoints** page to apply this setting to the SonicPoint.

Updating SonicPoint Firmware

SonicOS Enhanced contains an image of the SonicPoint firmware. When you connect a SonicPoint to a security appliance running SonicOS Enhanced, the appliance checks the version of the SonicPoint's firmware, and automatically updates it, if necessary.

Automatic Provisioning (SDP & SSPP)

The SonicWALL Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS Enhanced 3.0 and higher. SDP is the foundation for the automatic provisioning of SonicPoint units via the following messages:

- **Advertisement** – SonicPoint devices without a peer will periodically and on startup announce or advertise themselves via a broadcast. The advertisement will include information that will be used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device will then report the state of all peered SonicPoints, and will take configuration actions as needed.
- **Discovery** – SonicOS devices will periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- **Configure Directive** – A unicast message from a SonicOS device to a specific SonicPoint unit to establish encryption keys for provisioning, and to set the parameters for and to engage configuration mode.
- **Configure Acknowledgement** – A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive** – A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If via the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (e.g. on calculating a checksum mismatch, or when a firmware update is available), the Configure directive will engage a 3DES encrypted, reliable TCP based SonicWALL Simple Provisioning Protocol (SSPP) channel. The SonicOS device will then send the update to the SonicPoint via this channel, and the SonicPoint will restart with the updated configuration. State information will be provided by the SonicPoint, and will be viewable on the SonicOS device throughout the entire discovery and provisioning process.

SonicPoint States

SonicPoint devices can function in and report the following states:

- **Initializing** – The state when a SonicPoint starts up and advertises itself via SDP prior to it entering into an operational or stand-alone mode.
- **Operational** – Once the SonicPoint has peered with a SonicOS device and has its configuration validated, it will enter into a operational state, and will be ready for clients.
- **Provisioning** – If the SonicPoint configuration requires an update, the SonicOS device will engage an SSPP channel to update the SonicPoint. During this brief process it will enter the provisioning state.
- **Safemode** – Safemode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into Safemode returns its configuration to defaults, disables the radios, and disables SDP. The SonicPoint must then be rebooted to enter either a stand-alone, or some other functional state.
- **Non-Responsive** – If a SonicOS device loses communications with a previously peered SonicPoint, it will report its state as non-responsive. It will remain in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.
- **Updating Firmware** – If the SonicOS device detects that it has a firmware update available for a SonicPoint, it will use SSPP to update the SonicPoint's firmware.
- **Over-Limit** – By default, up to 2 SonicPoint devices can be attached to the Wireless Zone interface on a SonicWALL TZ 170. If more than 2 units are detected, the over-limit devices will report an over-limit state, and will not enter an operational mode. The number can be reduced from 2 as needed.
- **Rebooting** – After a firmware or configuration update, the SonicPoint will announce that it is about to reboot, and will then do so.
- **Firmware failed** – If a firmware update fails, the SonicPoint will report the failure, and will then reboot.
- **Provision failed** – In the unlikely event that a provision attempt from a SonicOS device fails, the SonicPoint will report the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.
- **Stand-alone Mode (not reported)** – If a SonicPoint device cannot find or be found by a SonicOS device to peer with, it will enter a stand-alone mode of operation. This will engage the SonicPoint's internal GUI (which is otherwise disabled) and will allow it to be configured as a conventional Access Point. If at any time it is placed on the same layer 2 segment as a SonicOS device that is sending Discovery packets, it will leave stand-alone mode, and will enter into a managed mode. The stand-alone configuration will be retained.

Viewing Station Status

SonicPoint > Station Status

Event and Statistics Reporting

The **SonicPoint > Station Status** page reports on the statistics of each SonicPoint








The screenshot shows the 'SonicPoint > Station Status' page. At the top right is a 'Refresh' button. Below the title, there is a 'Station Status' section with a 'View Style' dropdown set to 'SonicPoint' and a 'View Style' dropdown set to 'All SonicPoints'. A table lists the status of wireless clients. The table has columns: #, SonicPoint, Station, MAC Address, Status, Type, SSID, AID, Connect Rate, Tx Rate, Signal Strength, and Statistics. The table is divided by SonicPoint. The first SonicPoint is 'SonicPoint e00072 - Status was updated 00:00:03 ago'. It lists two clients:

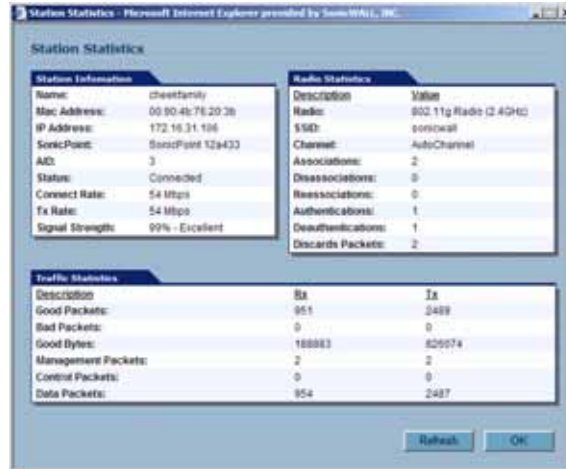
#	SonicPoint	Station	MAC Address	Status	Type	SSID	AID	Connect Rate	Tx Rate	Signal Strength	Statistics
1	SonicPoint e00072		00:02:ef:20:be:29	Connected	50Hz	1_sonicwall	1	54 Mbps	6 Mbps	78% - Very Good	
2	SonicPoint e00072	172.16.32.2	00:90:4b:76:20:3b	Connected	2.4GHz	1_sonicwall	1	1 Mbps	48 Mbps	100% - Excellent	

The table lists entries for each wireless client connected to each SonicPoint. The sections of the table are divided by SonicPoint. Under each SonicPoint, is the list of all clients currently connected to it.

Click the **Refresh** button in the top right corner to refresh the list.

By default, the page displays the first 50 entries found. Click the First Page , Previous Page , Next Page , and Last Page  icons to navigate if you need to view more than 50 entries.

Click on the Statistics icon  to see a detailed report for an individual station. Each SonicPoint device reports for both radios, and for each station, the following information to its SonicOS peer:



Station Information		Radio Statistics	
Name:	chertfamily	Description:	Radio
Mac Address:	00:90:4b:76:20:2b	Radio:	802.11g Radio (2.4GHz)
IP Address:	172.16.31.196	SSI:	sonicwall
SonicPoint:	SonicPoint 12a433	Channel:	AutoChannel
AID:	3	Associations:	2
Status:	Connected	Disassociations:	0
Connect Rate:	54 Mbps	Reassociations:	0
Tx Rate:	54 Mbps	Authentications:	1
Signal Strength:	99% - Excellent	Deauthentications:	1
		Discards Packets:	2

Traffic Statistics		
Description	Rx	Tx
Good Packets:	951	3489
Bad Packets:	0	0
Good Bytes:	188883	825574
Management Packets:	2	2
Control Packets:	0	0
Data Packets:	954	2487

- MAC Address – The client's (Station's) hardware address
- Station State – The state of the station. States can include:
 - ♦ None – No state information yet exists for the station
 - ♦ Authenticated – The station has successfully authenticated.
 - ♦ Associated – The station is associated.
 - ♦ Joined – The station has joined the ESSID.
 - ♦ Connected – The station is connected (joined, authenticated or associated).
 - ♦ Up – An Access Point state, indicating that the Access Point is up and running.
 - ♦ Down – An Access Point state, indicating that the Access Point is not running.
- Associations – Total number of Associations since power up.
- Dis-Associations – Total number of Dis-Associations.
- Re-Associations – Total number of Re-Associations.
- Authentications – Number of Authentications.
- De-Authentications – Number of De-Authentications.
- Good Frames Received – Total number of good frames received.
- Good Frames Transmitted – Total number of good frames transmitted.
- Error in Receive Frames – Total number of error frames received.
- Error in Transmit Frames – Total number of error frames transmitted.
- Discarded Frames – Total number of frames discarded. Discarded frames are generally a sign of network congestion.
- Total Bytes received – Total number of bytes received.
- Total Bytes Transmitted – Total number of bytes transmitted.
- Management Frames Received – Total number of Management frames received. Management Frames include:
 - ♦ Association request
 - ♦ Association response
 - ♦ Re-association request
 - ♦ Re-association response
 - ♦ Probe request
 - ♦ Probe response

- ◆ Beacon frame
- ◆ ATIM message
- ◆ Disassociation
- ◆ Authentication
- ◆ De-authentication
- Management Frames Transmitted – Total number of Management frames transmitted.
- Control Frames Received – Total number of Control frames received. Control frames include:
 - ◆ RTS – Request to Send
 - ◆ CTS – Clear to Send
 - ◆ ACK – Positive Acknowledgement
- Control Frames Transmitted – Total number of Control frames transmitted.
- Data Frames Received – Total number of Data frames received.
- Data Frames Transmitted – Total number of Data frames transmitted.

Using and Configuring IDS

SonicPoint > IDS

Detecting SonicPoint Access Points

You can have many wireless access points within reach of the signal of the SonicPoints on your network. The **SonicPoint > IDS** page reports on all access points the TZ 170 Wireless can find by scanning the 802.11a and 802.11g radio bands.

The screenshot shows the 'SonicPoint > IDS' configuration page. Under 'Intrusion Detection Settings', the 'Enable Rogue Access Point Detection' checkbox is checked, and the 'Authorized Access Points' dropdown is set to 'All Authorized Access Points'. Below this, the 'Discovered Access Points' section shows a table of detected APs. The table has columns for #, SonicPoint, MAC Address (BSSID), SSID, Type, Channel, Manufacturer, Signal Strength, Max Rate, and Authorize. A note above the table states 'SonicPoint e00072 - The last scan was performed 1 Day 01:31:06 ago' and there is a '- Perform SonicPoint Scan -' button.

#	SonicPoint	MAC Address (BSSID)	SSID	Type	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
1	SonicPoint e00072	00:06:b1:12:71:8a	SYBETA	5GHz	56	SonicWALL	39% - Fair	54 Mbps	
2	SonicPoint e00072	00:02:8f:2e:21:f9	sonicwall	5GHz	58	Benao	60% - Very Good	54 Mbps	
3	SonicPoint e00072	00:02:8f:2e:21:df	sonicwall	5GHz	60	Benao	78% - Very Good	54 Mbps	
4	SonicPoint e00072	00:02:8f:2e:20:cd	Atheros Wireless Network	5GHz	60	Benao	60% - Very Good	54 Mbps	
5	SonicPoint e00072	00:02:8f:2e:20:bf	ctsavePRO2040SPa	5GHz	64	Benao	78% - Very Good	54 Mbps	
6	SonicPoint e00072	00:02:8f:2e:21:f1	sonicwall	5GHz	64	Benao	39% - Fair	54 Mbps	
7	SonicPoint e00072	00:0d:ac:6c:4f:26	olivea	5GHz	36	Cisco	39% - Fair	54 Mbps	
8	SonicPoint e00072	00:02:8f:2e:21:cb	sonicwall	5GHz	38	Benao	60% - Very Good	54 Mbps	
9	SonicPoint e00072	00:06:b1:12:71:94	sonicwall	5GHz	40	SonicWALL	78% - Very Good	54 Mbps	

Wireless Intrusion Detection Services

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

Intrusion Detection Settings

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

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

Check **Enable Rogue Access Point Detection** to enable the security appliance to search for rogue access points.

The **Authorized Access Points** list determines which access points the security appliance will considered authorized when it performs a scan. You can select **All Authorized Access Points** to allow all SonicPoints, or you can select an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group.

Select Create Address Object Group to add a new group of MAC address objects to the list.



Cross Reference: See **Chapter 16, Configuring Address Objects** for instructions on creating address objects and address object groups.

Scanning for Access Points

Active scanning occurs when the security appliance starts up, and at any time **Scan All** is clicked on the **SonicPoint > IDS** page. When the security appliance performs a scan, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

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



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

You can also scan on a SonicPoint by SonicPoint basis by choosing from the following options in the Perform SonicWALL Scan menu on the header for the individual SonicPoint:

- **Scan Both Radios**
- **Scan 802.11a Radio (5GHz)**
- **Scan 802.11g Radio (2.4GHZ)**

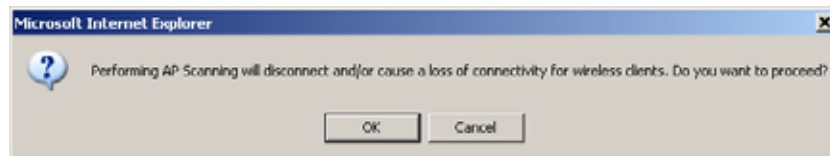
Discovered Access Points

The Discovered Access points displays information on every access point that can be detected by the SonicPoint radio:

- **SonicPoint:** The SonicPoint that detected the access point.
- **MAC Address (BSSID):** The MAC address of the radio interface of the detected access point.
- **SSID:** The radio SSID of the access point.
- **Type:** The range of radio bands used by the access point, 2.4 GHz or 5 GHz.
- **Channel:** The radio channel used by the access point.
- **Manufacturer:** The manufacturer of the access point. SonicPoints will show a manufacturer of either *SonicWALL* or *Senao*.
- **Signal Strength:** The strength of the detected radio signal
- **Max Rate:** The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize:** Click the Authorize icon to add the access point to the address object group of authorized access points.

View Style

If you have more than one SonicPoint, you can select an individual device from the **SonicPoint** list to limit the **Discovered Access Points** table to display only scan results from that SonicPoint. Select **All SonicPoints** to display scan results from all SonicPoints.



Authorizing Access Points on Your Network

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

P A R T

7

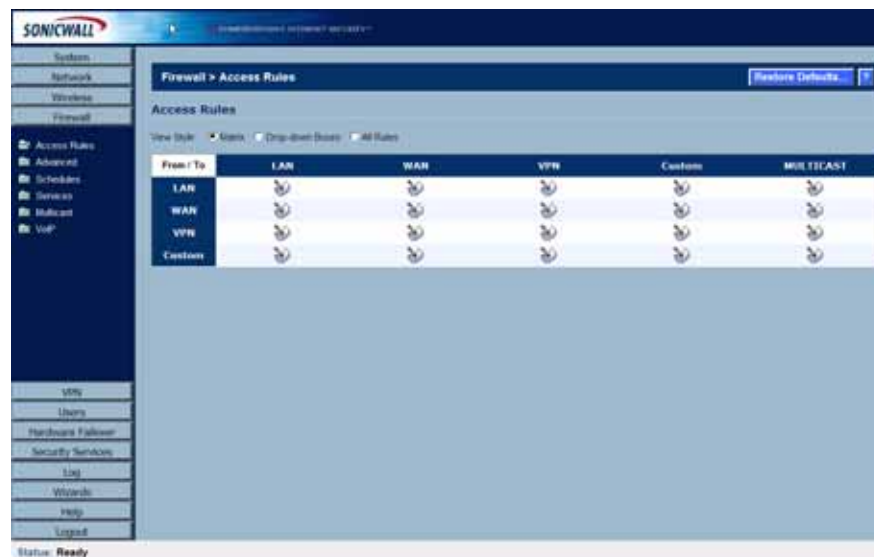
Firewall

Configuring Access Rules

Firewall > Access Rules

This chapter provides an overview on your SonicWALL security appliance stateful packet inspection default access rules and configuration examples to customize your access rules to meet your business requirements.

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



The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

Stateful Packet Inspection Default Access Rules Overview

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

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

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

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWALL security appliance. Network access rules take precedence, and can override the SonicWALL security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWALL security appliance default setting of allowing this type of traffic.



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

Using Bandwidth Management with Access Rules Overview

Bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. All other packets will be queued in the default queue and will be sent in a First In and First Out (FIFO) manner (a storage method that retrieves the item stored for the longest time).

Example Scenario

If you create an access rule for outbound mail traffic (such as SMTP) and enable bandwidth management with the following parameters:

- Guaranteed bandwidth of 20 percent
- Maximum bandwidth of 40 percent
- Priority of 0 (zero)

The outbound SMTP traffic is guaranteed 20 percent of available bandwidth available to it and can get as much as 40 percent of available bandwidth. If this is the only access rule using bandwidth management, it has priority over all other access rules on the SonicWALL security appliance. Other access rules use the remaining bandwidth (minus 20 percent of bandwidth, or greater than minus 20 percent and less than minus 40 percent of bandwidth).



Note: *Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.*

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


Configuration Task List

This section provides a list of the following configuration tasks:

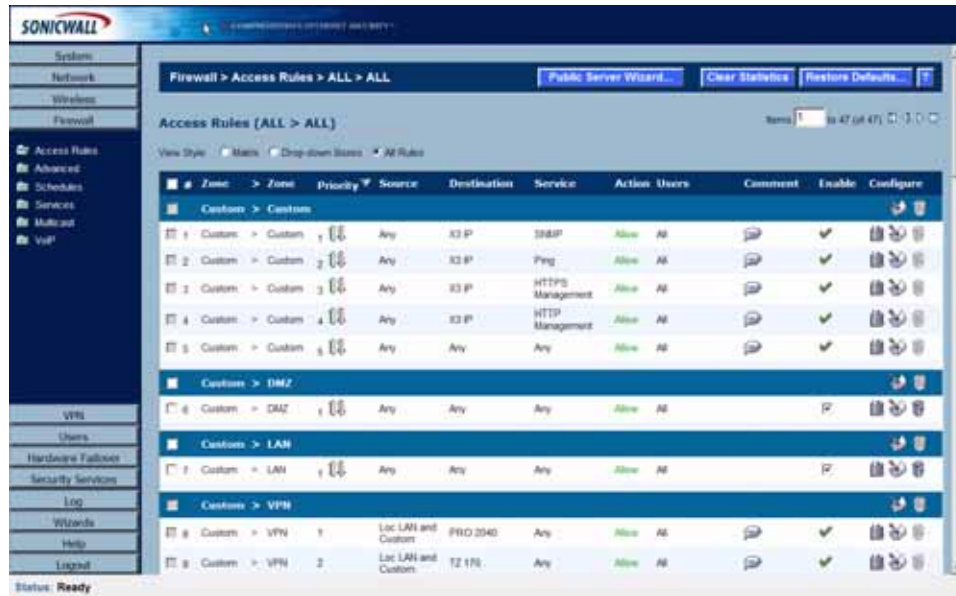
- Displaying Access Rules with View Styles
- Configuring Access Rules for a Zone
- Adding Access Rules
- Editing an Access Rule
- Deleting an Access Rule
- Enabling and Disabling an Access Rule
- Displaying Access Rule Traffic Statistics
- Access Rule Configuration Examples

Displaying Access Rules with View Styles

Access rules can be displayed in multiple views using SonicOS Enhanced. You can select the type of view from the selections in the **View Style** section. The following **View Styles** are available:

- **All Rules** - Select **All Rules** to display all access rules configured on the SonicWALL security appliance.
 - **Matrix** - Displays as **From/To** with **LAN, WAN, VPN**, or other interface in the **From** row, and **LAN, WAN, VPN**, or other interface in the **To** column. Select the **Edit** icon  in the table cell to view the access rules.
 - **Drop-down Boxes** - Displays two pull-down menus: **From Zone** and **To Zone**. Select an interface from the **From Zone** menu and select an interface from the **To Zone** menu. Click **OK** and access rules defined for the two interfaces are displayed.
- ✓ **Tip:** You can also view access rules by Zones. Use the *Option* checkboxes in the **From Zone** and **To Zone** column. Select **LAN, WAN, VPN, ALL** from the **From Zone** column. And then select **LAN, WAN, VPN, ALL** from the **To Zone** column. Click **OK** to display the access rules.

Each view displays a table of defined network access rules. For example, selecting **All Rules** displays all the network access rules for all zones.



Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone, select a zone from the **Matrix**, **Drop-down Boxes**, or **All Rules** view.



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

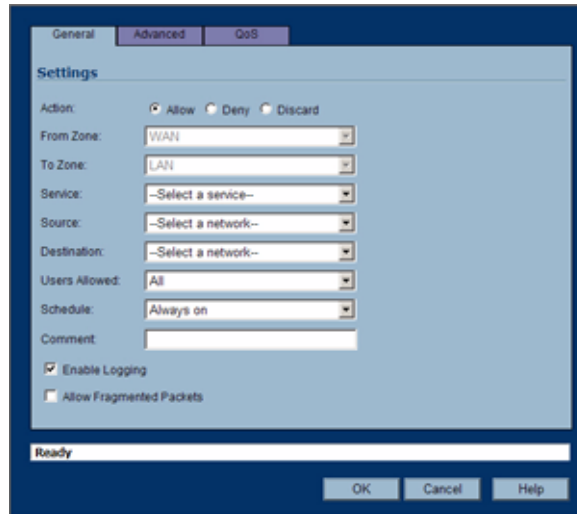
You can change the priority ranking of an access rule by clicking the **Arrows** icon in the Priority column. The Change Priority window is displayed. Enter the new priority number (1-10) in the **Priority** field, and click **OK**.

✓ **Tip:** If the **Trashcan** or **Notepad** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

Adding Access Rules

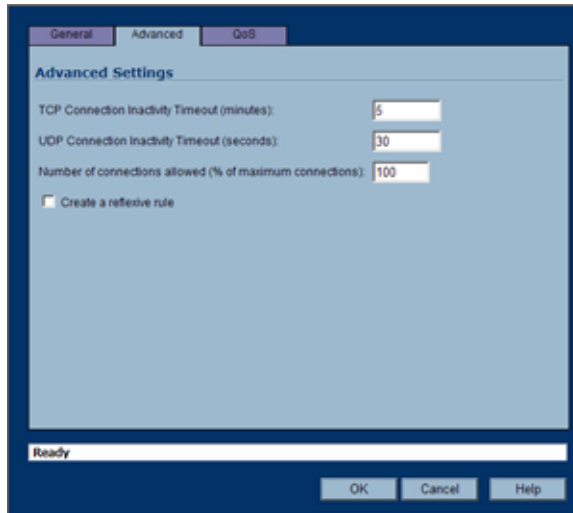
To add access rules to the SonicWALL security appliance, perform the following steps:

1. Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.



2. In the **General** tab, select **Allow | Deny | Discard** from the **Action** list to permit or block IP traffic.
3. Select the from and to zones from the **From Zone** and **To Zone** menus.
4. Select the service or group of services affected by the access rule from the **Service** list. The **Default** service encompasses all IP services.
If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
5. Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
6. If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, type the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, type * in the **Address Range Begin** field.
7. Select the destination of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
8. From the **Users Allowed** menu, add the user or user group affected by the access rule.
9. Select a schedule from the **Schedule** menu. The default schedule is **Always on**.
10. Enter any comments to help identify the access rule in the **Comments** field.
11. Do not select the **Allow Fragmented Packets** check box. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. Because hackers exploit IP fragmentation in Denial of Service (DoS) attacks, the SonicWALL security appliance blocks fragmented packets by default. You can override the default configuration to allow fragmented packets over PPTP or IPsec.

12. Click on the **Advanced** tab.



13. If you would like for the access rule to timeout after a period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **5** minutes.

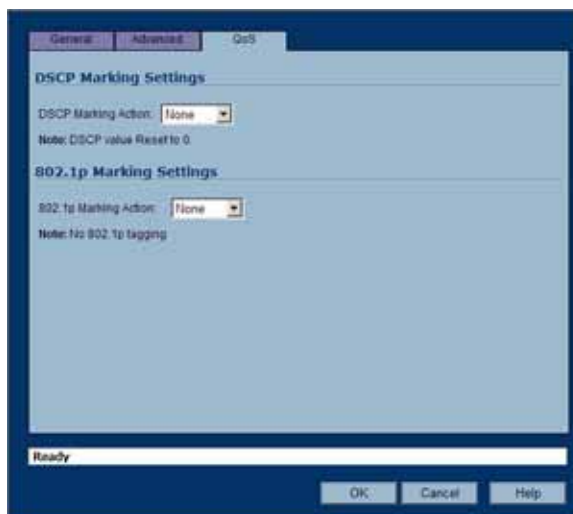
14. If you would like for the access rule to timeout after a period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.

15. Specify the number of connections allowed as a percent of maximum number of connections allowed by the SonicWALL security appliance in the **Number of connections allowed (% of maximum connections)** field. Refer to [Connection Limiting Overview on page 308](#) for more information on connection limiting.

16. Select **Create a reflexive rule** if you want to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object.

17. Click on the **QoS** tab if you want to apply DSCP or 802.1p Quality of Service management to traffic governed by this rule.

See [Chapter 42, Managing Quality of Service](#) for more information on managing QoS marking in access rules.



18. Under **DSCP Marking Settings** select the **DSCP Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **Preserve** is the default.

- ◆ **None:** DSCP values in packets are reset to 0.
 - ◆ **Preserve:** DSCP values in packets will remain unaltered.
 - ◆ **Explicit:** Set the DSCP value to the value you select in the **Explicit DSCP Value** field. This is a numeric value between 0 and 63. Some of the standard values are:
 - **0** - Best effort/Default (default)
 - **8** - Class 1
 - **10** - Class 1, Gold (AF11)
 - **12** - Class 1, Silver (AF12)
 - **14** - Class 1, Bronze (AF13)
 - **16** - Class 2
 - **18** - Class 2, Gold (AF21)
 - **20** - Class 2, Silver (AF22)
 - **22** - Class 2, Bronze (AF23)
 - **24** - Class 3
 - **26** - Class 3, Gold (AF31)
 - **27** - Class 3, Silver (AF32)
 - **30** - Class 3, Bronze (AF33)
 - **32** - Class 4
 - **34** - Class 4, Gold (AF41)
 - **36** - Class 4, Silver (AF42)
 - **38** - Class 4, Bronze (AF43)
 - **40** - Express Forwarding
 - **46** - Expedited Forwarding (EF)
 - **48** - Control
 - **56** - Control
 - ◆ **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [Chapter 42, Managing Quality of Service](#) for instructions on configuring the QoS Mapping. If you select Map, you can select **Allow 802.1p Marking to override DSCP values**.
19. Under **802.1p Marking Settings** select the **802.1p Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **None** is the default.
- ◆ **None:** No 802.1p tagging is added to the packets.
 - ◆ **Preserve:** 802.1p values in packets will remain unaltered.
 - ◆ **Explicit:** Set the 802.1p value to the value you select in the Explicit 802.1p Value field. This is a numeric value between 0 and 7. The standard values are:
 - **0** - Best effort (default)
 - **1** - Background
 - **2** - Spare
 - **3** - Excellent effort
 - **4** - Controlled load
 - **5** - Video (<100ms latency)
 - **6** - Voice (<10ms latency)
 - **7** - Network control
 - ◆ **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [Chapter 42, Managing Quality of Service](#) for instructions on configuring the QoS Mapping.

20. Click **OK** to add the rule.



Tip: Although custom access rules can be created that allow inbound IP traffic, the SonicWALL security appliance does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.

Editing an Access Rule

To display the **Edit Rule** window (includes the same settings as the **Add Rule** window), click the **Notepad** icon.

Deleting an Access Rule

To delete the individual access rule, click on the **Trashcan** icon. To delete all the checkbox selected access rules, click the **Delete** button.

Enabling and Disabling an Access Rule

To enable or disable an access rule, click the **Enable** checkbox.

Restoring Access Rules to Default Zone Settings

To remove all end-user configured access rules for a zone, click the **Default** button. This will restore the access rules for the selected zone to the default access rules initially setup on the SonicWALL security appliance.

Displaying Access Rule Traffic Statistics

Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

Connection Limiting Overview

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such SonicOS features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the SonicWALL using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted ->Untrusted traffic (i.e. LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

The following table delineates the connection-cache size of currently available SonicWALL devices running SonicOS Enhanced (numbers are subject to change):

SonicWALL Security Appliance	Connection Cache Maximum
TZ 150	2,048
TZ 170 (all versions)	6,144
PRO 1260	6,144
PRO 2040	32,768
PRO 3060	131,072
PRO 4060	524,288
PRO 4100	600,000
PRO 5060	750,000

In addition to mitigating the propagation of worms and viruses, Connection limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, connection limiting can be used to protect publicly available servers (e.g. web-servers) by limiting the number of legitimate inbound connections permitted to the server (i.e. to protect the server against the Slashdot-effect). This is different from SYN flood protection which attempts to detect and prevent partially-open or spoofed TCP connection. This will be most applicable for Untrusted'Trusted traffic, but it can be applied to any Zone'Zone traffic as needed.

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The above figures show the default LAN ->WAN setting, where all available resources may be allocated to LAN->WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (e.g. FTP traffic to any destination on the WAN), or to prioritize important traffic (e.g. HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).



Note: It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (i.e. Address Objects and Service Objects) are permissible.

Access Rule Configuration Examples

This section provides configuration examples on adding network access rules:

- Enabling Ping
- Blocking LAN Access for Specific Services
- Enabling Bandwidth Management on an Access Rule

Enabling Ping

This section provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your SonicWALL security appliance does not allow traffic initiated from the DMZ to reach the LAN. Once you have placed one of your interfaces into the DMZ zone, then from the **Firewall > Access Rules** window, perform the following steps to configure an access rule that allow devices in the DMZ to send ping requests and receive ping responses from devices in the LAN.

1. Click **Add** to launch the **Add Rule** window.
2. Select the **Allow** radio button.
3. From the **Service** menu, select **Ping**.
4. From the **Source** menu, select **DMZ Subnets**.
5. From the **Destination** menu, select **LAN Subnets**.
6. Click **OK**.

Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

Perform the following steps to configure an access rule blocking LAN access to NNTP servers based on a schedule:

1. Click **Add** to launch the **Add** window.
2. Select **Deny** from the **Action** settings.
3. Select **NNTP** from the **Service** menu. If the service is not listed in the list, you must to add it in the **Add Service** window.
4. Select **Any** from the **Source** menu.
5. Select **WAN** from the **Destination** menu.
6. Select the schedule from the **Schedule** menu.
7. Enter any comments in the **Comment** field.
8. Click **OK**.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the Funnel icon are configured for bandwidth management.



Tip: Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For more information on Bandwidth Management see [Bandwidth Management on page 354 in Chapter 42, Managing Quality of Service](#).

Configuring Advanced Access Rule Settings

Firewall > Advanced

To configure advanced access rule options, select **Firewall > Advanced** under Firewall. The **Advanced Rule Options** page is displayed.



The **Advanced Rule Options** includes the following firewall configuration option groups:

- **Detection Prevention**
- **Dynamic Ports**
- **Source Routed Packets**
- **Connections**
- **Access Rule Service Options**
- **IP and UDP Checksum Enforcement**
- **UDP**

Detection Prevention

- **Enable Stealth Mode** - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to *blocked inbound connection requests*. Stealth Mode makes your security appliance essentially invisible to hackers.
- **Randomize IP ID** - Select Randomize IP ID to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.
- **Decrement IP TTL for forwarded traffic** - Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Select this option to decrease the TTL value for packets that have been forwarded and therefore have already been in the network for some time.
- **Never generate ICMP Time-Exceeded packets** - The SonicWALL appliance generates Time-Exceeded packets to report when it has dropped a packet because its TTL value has decreased to zero. Select this option if you don’t want the SonicWALL appliance to generate these reporting packets.

Dynamic Ports

- **Enable support for Oracle (SQLNet)** - Select if you have Oracle applications on your network.
- **Enable support for Windows Messenger** - Select this option to support special SIP messaging used in Windows Messenger on the Windows XP.
- **Enable RTSP Transformations** - Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

Source Routed Packets

Drop Source Routed Packets is selected by default. Clear the check box if you are testing traffic between two specific hosts and you are using source routing.

Connections

Check **Disable Anti-Spyware, Gateway AV and IPS Engine (increases maximum SPI connections)** if you want to enable more connections at the expense of the Gateway Anti-Virus and Intrusion Prevention services.

Access Rule Service Options

Force inbound and outbound FTP data connections to use default port 20 - The default configuration allows FTP connections from port 20 but remaps outbound traffic to a port such as 1024. If the check box is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.

IP and UDP Checksum Enforcement

- **Enable IP header checksum enforcement** - Select this to enforce IP header checksums.
- **Enable UDP checksum enforcement** - Select this to enforce IP header checksums.

UDP

Enter the number of seconds of idle time you want to allow before UDP connections time out in the **Default UDP Connection Timeout (seconds)** field. This value is overridden by the UDP Connection timeout you set for individual rules.

Configuring TCP Settings

Firewall > TCP Settings

The TCP Settings lets you view statistics on TCP Traffic through the security appliance and manage TCP traffic settings. The page is divided into three sections

- TCP Traffic Statistics
- TCP Settings
- SYN/RST/FIN Flood Protection

TCP Traffic Statistics

The TCP Traffic Statistics table provides statistics on the following:

- **Connections Opened** – Incremented when a TCP connection initiator sends a SYN, or a TCP connection responder receives a SYN.
- **Connections Closed** – Incremented when a TCP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
- **Connections Refused** – Incremented when a RST is encountered, and the responder is in a SYN_RCVD state.
- **Connections Aborted** – Incremented when a RST is encountered, and the responder is in some state other than SYN_RCVD.
- **Total TCP Packets** – Incremented with every processed TCP packet.
- **Validated Packets Passed** – Incremented under the following conditions:
 - ♦ When a TCP packet passes checksum validation (while TCP checksum validation is enabled)
 - ♦ When a valid SYN packet is encountered (while SYN Flood protection is enabled)
 - ♦ When a SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).
- **Corrupted Packets Dropped** - Incremented under the following conditions:
 - ♦ When TCP checksum fails validation (while TCP checksum validation is enabled)
 - ♦ When the TCP SACK Permitted (Selective Acknowledgement, see RFC1072) option is encountered, but the calculated option length is incorrect.
 - ♦ When the TCP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect.

- ◆ When the TCP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes.
- ◆ When the TCP option length is determined to be invalid.
- ◆ When the TCP header length is calculated to be less than the minimum of 20 bytes.
- ◆ When the TCP header length is calculated to be greater than the packet's data length.
- **Invalid Flag Packets Dropped** - Incremented under the following conditions:
 - ◆ When a non-SYN packet is received that cannot be located in the connection-cache (while SYN Flood protection is disabled).
 - ◆ When a packet with flags other than SYN, RST+ACK or SYN+ACK is received during session establishment (while SYN Flood protection is enabled).
 - TCP XMAS Scan will be logged if the packet has FIN, URG, and PSH flags set
 - TCP FIN Scan will be logged if the packet has the FIN flag set
 - TCP Null Scan will be logged if the packet has no flags set
 - ◆ When a new TCP connection initiation is attempted with something other than just the SYN flag set.
 - ◆ When a packet with the SYN flag set is received within an established TCP session.
 - ◆ When a packet without the ACK flag set is received within an established TCP session.
- **Invalid Sequence Packets Dropped** – Incremented under the following conditions:
 - ◆ When a packet within an established connection is received where the sequence number is less than the connection's oldest unacknowledged sequence
 - ◆ When a packet within an established connection is received where the sequence number is greater than the connection's oldest unacknowledged sequence + the connection's last advertised window size.
- **Invalid Acknowledgement Packets Dropped** - Incremented under the following conditions:
 - ◆ When a packet is received with the ACK flag set, and with neither the RST or SYN flags set, but the SYN Cookie is determined to be invalid (while SYN Flood protection is enabled)
 - ◆ When a packet's ACK value (adjusted by the sequence number randomization offset) is less than the connection's oldest unacknowledged sequence number.
 - ◆ When a packet's ACK value (adjusted by the sequence number randomization offset) is greater than the connection's next expected sequence number.

TCP Settings



The TCP Settings section allows you to:

- **Enable TCP Stateful Inspection** – Enabling TCP stateful inspection requires that all TCP connections rigidly adhere to the following TCP setup requirements:
 - ◆ TCP session establishment involves a three-way handshake between two hosts and consists of the following:
 - Initiator --> SYN --> Responder
 - Initiator <-- SYN/ACK <-- Responder

- Initiator --> ACK --> Responder
- (Session established)

After the initial SYN, it is permissible for a Client to send a RST or a SYN, or for the Server to send a SYN-ACK or a RST. Any other kind of TCP flags are generally considered invalid, or potentially malicious. The 'Enable TCP Stateful Inspection' option enforces these guidelines, and drops any traffic that violates them.



Note: *Some legitimate TCP/IP stack implementations do not abide by these rules, and require that 'Enable TCP Stateful Inspection' be disabled. For the sake of compatibility with these implementations, the 'Enable TCP Stateful Inspection' option is disabled by default, but can be enabled to heighten security, or if there is no concern of potential incompatibilities.*

- **Enable TCP Checksum Validation** – If an invalid TCP checksum is calculated, the packet will be dropped.
- **Default TCP Connection Timeout** – The default time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection will be cleared by the SonicWALL. The default value is 5 minutes, the minimum value is 1 minute, and the maximum value is 999 minutes. Note: Setting excessively long connection time-outs will slow the reclamation of stale resources, and in extreme cases could lead to exhaustion of the connection cache.
- **Maximum Segment Lifetime (seconds)** – Determines the number of seconds that any TCP packet is valid before it expires. This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME_WAIT state to ensure that the proper FIN / ACK exchange has occurred to cleanly close the TCP connection.
 - ◆ Default value: 8 seconds
 - ◆ Minimum value: 1 second
 - ◆ Maximum value: 60 seconds

Working with SYN/RST/FIN Flood Protection

SYN/RST/FIN Flood protection helps to protect hosts behind the SonicWALL from Denial of Service (DoS) or Distributed DoS attacks that attempt to consume the host's available resources by creating one of the following attack mechanisms:

- sending TCP SYN packets, RST packets, or FIN packets with invalid or spoofed IP addresses
- creating excessive numbers of half-opened TCP connections.

A SYN Flood attack is considered to be in progress if the number of unanswered SYN/ACK packets sent by the SonicWALL (half-opened TCP connections) exceeds the threshold set in the "Flood rate until attack logged (unanswered SYN/ACK packets per second)" field. The default value for the field is 20, the minimum is 5, and the maximum is 999,999.

Understanding a TCP Handshake

A typical TCP handshake (simplified) begins with an initiator sending a TCP SYN packet with a 32-bit sequence (SEQ_i) number. The responder then sends a SYN/ACK packet acknowledging the received sequence by sending an ACK equal to SEQ_i+1 and a random, 32-bit sequence number (SEQ_r). The responder also maintains state awaiting an ACK from the initiator. The initiator's ACK packet should contain the next sequence (SEQ_i+1) along with an acknowledgment of the sequence it received from the responder (by sending an ACK equal to SEQ_r+1). The exchange looks as follows:

- 1 Initiator -> SYN (SEQ_i=0001234567, ACK_i=0) -> Responder
- 2 Initiator <- SYN/ACK (SEQ_r=3987654321, ACK_r=0001234568) <- Responder
- 3 Initiator -> ACK (SEQ_i=0001234568, ACK_i=3987654322) -> Responder

Because the responder has to maintain state on all half-opened TCP connections, it is possible for memory depletion to occur if SYNs come in faster than they can be processed or cleared by the responder. A half-opened TCP connection did not transition to an established state through the completion of the three-way handshake. When the SonicWALL is between the initiator and the responder, it effectively becomes the responder, brokering, or *proxying*, the TCP connection to the actual responder (private host) it is protecting.

SYN Flood Protection Methods

The following sections detail some SYN Flood protection methods.

SYN Flood Protection Using Stateless Cookies

The method of SYN flood protection employed starting with SonicOS Enhanced 3.1 uses stateless SYN Cookies, which increase reliability of SYN Flood detection, and also improves overall resource utilization on the SonicWALL. With stateless SYN Cookies, the SonicWALL does not have to maintain state on half-opened connections. Instead, it uses a cryptographic calculation (rather than randomness) to arrive at SEQ_r.

Layer-Specific SYN Flood Protection Methods

SonicOS 3.1 and newer provides several protections against SYN Floods generated from two different environments: trusted (internal) or untrusted (external) networks. Attacks from *untrusted* WAN networks usually occur on one or more servers protected by the firewall. Attacks from the *trusted* LAN networks occur as a result of a virus infection inside one or more of the trusted networks, generating attacks on one or more local or remote hosts.

To provide a firewall defense to both attack scenarios, SonicOS Enhanced 3.1 and newer provides two separate SYN Flood protection mechanisms on two different layers. Each gathers and displays SYN Flood statistics and generates log messages for significant SYN Flood events.

- **SYN Proxy (Layer 3)** – This mechanism shields servers inside the trusted network from WAN-based SYN flood attacks, using a SYN Proxy implementation to verify the WAN clients before forwarding their connection requests to the protected server. You can enable SYN Proxy only on WAN interfaces.
- **SYN Blacklisting (Layer 2)** – This mechanism blocks specific devices from generating or forwarding SYN flood attacks. You can enable SYN Blacklisting on any interface.

Understanding SYN Watchlists

The internal architecture of both SYN Flood protection mechanisms is based on a single list of Ethernet addresses that are the most active devices sending initial SYN packets to the firewall. This list is called a *SYN watchlist*. Because this list contains Ethernet addresses, the device tracks all SYN

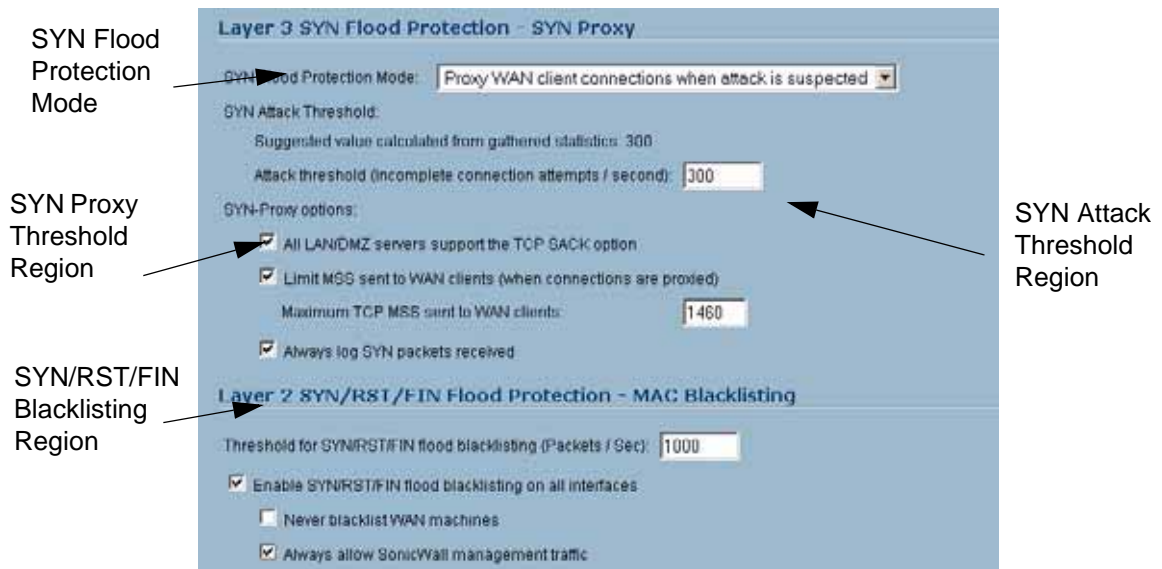
traffic based on the address of the device forwarding the SYN packet, without considering the IP source or destination address.

Each watchlist entry contains a value called a *hit count*. The hit count value increments when the device receives the an initial SYN packet from a corresponding device. The hit count decrements when the TCP three-way handshake completes. The hit count for any particular device generally equals the number of half-open connections pending since the last time the device reset the hit count. The device default for resetting a hit count is once a second.

The thresholds for logging, SYN Proxy, and SYN Blacklisting are all compared to the hit count values when determining if a log message or state change is necessary. When a SYN Flood attack occurs, the number of pending half-open connections from the device forwarding the attacking packets increases substantially because of the spoofed connection attempts. When you set the attack thresholds correctly, normal traffic flow produces few attack warnings, but the same thresholds detect and deflect attacks before they result in serious network degradation.

Working with SYN Flood Protection Features

To configure SYN Flood Protection features, go to the Layer 3 SYN Flood Protection - SYN Proxy portion of the Firewall > TCP Settings window that appears as shown in the following figure.



Note that this region contains four regions:

- SYN Flood Protection Mode
- SYN Attack Threshold
- SYN Proxy Options
- SYN/RST/FIN Blacklisting

Each contains various types of SYN Flood Protection. The following sections describe these features.

Working with SYN Flood Protection Modes

A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection:

Watch and Report Possible SYN Floods – This option enables the device to monitor SYN traffic on all interfaces on the device and to log suspected SYN flood activity that exceeds a packet count threshold. The feature does not turn on the SYN Proxy on the device so the device forwards the TCP three-way handshake without modification. This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high risk environment.

Proxy WAN Client Connections When Attack is Suspected – This option enables the device to enable the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second surpasses a specified threshold. This method ensures the device continues to process valid traffic during the attack and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring or until the device blacklists all of them using the SYN Blacklisting feature. This is the intermediate level of SYN Flood protection. Select this option if your network experiences SYN Flood attacks from internal or external sources.

Always Proxy WAN Client Connections – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. Note that this is an extreme security measure and directs the device to respond to port scans on all TCP ports because the SYN Proxy feature forces the device to respond to all TCP SYN connection attempts. This can degrade performance and can generate a false positive. Select this option only if your network is in a high risk environment.

Working with SYN Attack Threshold

The SYN Attack Threshold region of the SYN Flood Protection region, provides limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold.

Note the two options in the section:

Use the 300 Value Calculated from Gathered Statistics – Sets the threshold for the number of incomplete connection attempts per second before the device drops packets at the default value of 300.

Attack Threshold (Incomplete Connection Attempts/Second) – Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 999,999.

Working with SYN Proxy Options

When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server will respond to the TCP options normally provided on SYN/ACK packets.

To provide more control over the options sent to WAN clients when in SYN Proxy mode, you can configure the following two objects:

SACK (Selective Acknowledgment) – This parameter controls whether or not Selective ACK is enabled. With SACK enabled, a packet or series of packets can be dropped, and the receiver informs the sender which data has been received and where holes may exist in the data.

MSS (Minimum Segment Size) – This sets the threshold for the size of TCP segments, preventing a segment that is too large to be sent to the targeted server. For example, if the server is an IPsec gateway, it may need to limit the MSS it received to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment, enables you to control the manufactured MSS value sent to WAN clients.

The SYN Proxy Threshold region contains the following options:

All LAN/DMZ servers support the TCP SACK option – This checkbox enables Selective ACK where a packet can be dropped and the receiving device indicates which packets it received. Enable this checkbox only when you know that all servers covered by the firewall accessed from the WAN support the SACK option.

Limit MSS sent to WAN clients (when connections are proxied) – Enables you to enter the maximum Minimum Segment Size value. If you specify an override value for the default of 1460, this indicates that a segment of that size or smaller will be sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.

Maximum TCP MSS sent to WAN clients. The value of the MSS. The default is 1460.



Note: *When using Proxy WAN client connections, remember to set these options conservatively since they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can proceed during an attack.*

Working with SYN/RST/FIN Blacklisting

The SYN/RST/FIN Blacklisting feature is a list that contains devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.

The SYN/RST/FIN Blacklisting region contains the following options:

Threshold for SYN/RST/FIN flood blacklisting (SYNs / Sec) – The maximum number of SYN, RST, and FIN packets allowed per second. The default is 1,000. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.

Enable SYN/RST/FIN flood blacklisting on all interfaces – This checkbox enables the blacklisting feature on all interfaces on the firewall.

Never blacklist WAN machines – This checkbox ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it unchecked may interrupt traffic to and from the firewall's WAN ports.

Always allow SonicWall management traffic – This checkbox causes IP traffic from a blacklisted device targeting the firewall’s WAN IP addresses to not be filtered. This allows management traffic, and routing protocols to maintain connectivity through a blacklisted device.

SYN, RST, and FIN Flood Statistics

You can view SYN, RST and FIN Flood statistics in the lower half of the TCP Traffic Statistics list as shown in the following figure.

TCP Traffic Statistics	
Connections Opened	320
Connections Closed	314
Connections Refused	2
Connections Aborted	10
Connection Handshake Errors	0
Total TCP Packets	6299
Validated Packets Passed	6298
Malformed Packets Dropped	0
Invalid Flag Packets Dropped	1
Invalid Sequence Packets Dropped	0
Invalid Acknowledgement Packets Dropped	0
Max Incomplete WAN Connections / sec	2
Average Incomplete WAN Connections / sec	0
SYN Floods In Progress	0
RST Floods In Progress	0
FIN Floods In Progress	0
Total SYN, RST or FIN Floods Detected	0
TCP Connection SYN-Proxy State (WAN only)	OFF
Current SYN-Blacklisted Machines	0
Current RST-Blacklisted Machines	0
Current FIN-Blacklisted Machines	0
Total SYN-Blacklisting Events	0
Total RST-Blacklisting Events	0
Total FIN-Blacklisting Events	0
Total SYN Blacklist Packets Rejected	0
Total RST Blacklist Packets Rejected	0
Total FIN Blacklist Packets Rejected	0
Invalid SYN Flood Cookies Received	0

SYN, RST, and FIN Flood Related Statistics (Bottom seventeen)

The following are SYN Flood statistics.

Column	Description
Max Incomplete WAN Connections / sec	The maximum number of pending embryonic half-open connections recorded since the firewall has been up (or since the last time the TCP statistics were cleared).
Average Incomplete WAN Connections / sec	The average number of pending embryonic half-open connections, based on the total number of samples since bootup (or the last TCP statistics reset).
SYN Floods in Progress	The number of individual forwarding devices that are currently exceeding either SYN Flood threshold.
RST Floods in Progress	The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
FIN Floods in Progress	The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
Total SYN, RST, or FIN Floods Detected	The total number of events in which a forwarding device has exceeded the lower of either the SYN attack threshold or the SYN/RST/FIN flood blacklisting threshold.

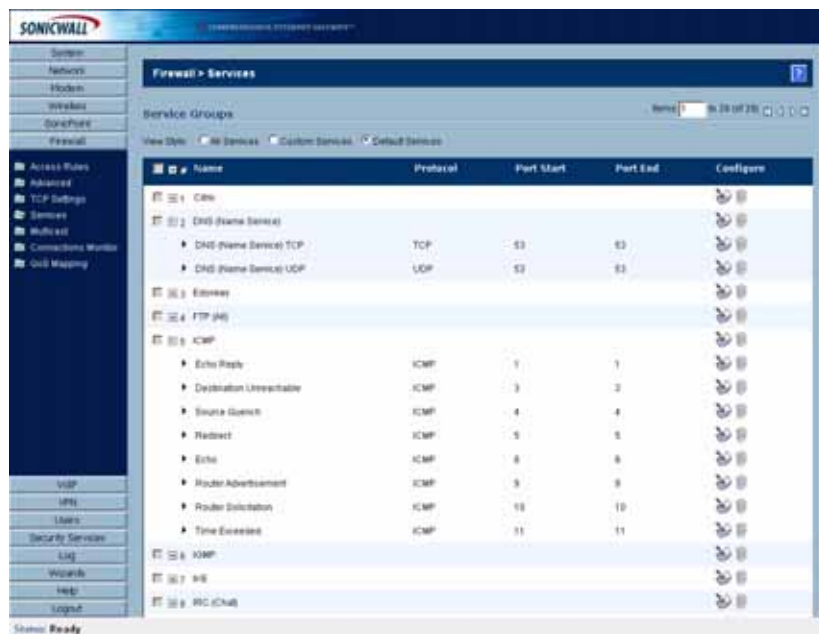
Column	Description
TCP Connection SYN-Proxy State (WAN only)	Indicates whether or not Proxy-Mode is currently on the WAN interfaces.
Current SYN-Blacklisted Machines	The number of devices currently on the SYN blacklist.
Current RST-Blacklisted Machines	The number of devices currently on the RST blacklist.
Current FIN-Blacklisted Machines	The number of devices currently on the FIN blacklist.
Total SYN-Blacklisting Events	The total number of instances any device has been placed on the SYN blacklist.
Total RST-Blacklisting Events	The total number of instances any device has been placed on the RST blacklist.
Total FIN-Blacklisting Events	The total number of instances any device has been placed on the FIN blacklist.
Total SYN Blacklist Packets Rejected	The total number of packets dropped because of the SYN blacklist.
Total RST Blacklist Packets Rejected	The total number of packets dropped because of the RST blacklist.
Total FIN Blacklist Packets Rejected	The total number of packets dropped because of the FIN blacklist.
Invalid SYN Flood Cookies Received	The total number of invalid SYN flood cookies received.

Configuring Firewall Services

Firewall > Services

SonicOS Enhanced supports an expanded IP protocol support to allow users to create services and access rules based on these protocols. See “Supported Protocols” on page 327 for a complete listing of support IP protocols.

Services are used by the SonicWALL security appliance to configure network access rules for allowing or denying traffic to the network. The SonicWALL security appliance includes **Default Services**. Default Services are predefined services that are not editable. And you can also create **Custom Services** to configure firewall services to meet your specific business requirements.



Selecting **All Services** from **View Style** displays both **Custom Services** and **Default Services**.

The screenshot shows the 'Firewall > Services' configuration page. At the top, there is a 'Service Groups' section with a 'View Style' dropdown set to 'All Services'. Below this is a table with the following columns: #, Name, Protocol, Port Start, Port End, and Configure. The table lists 8 service groups:

#	Name	Protocol	Port Start	Port End	Configure
1	Cbitx				[Notepad/Trashcan icons]
2	DNS (Name Service)				[Notepad/Trashcan icons]
3	Edonkey				[Notepad/Trashcan icons]
4	Filemaker				[Notepad/Trashcan icons]
5	ICMP				[Notepad/Trashcan icons]
6	IGMP				[Notepad/Trashcan icons]
7	IKE				[Notepad/Trashcan icons]
8	IRC (Chat)				[Notepad/Trashcan icons]

Default Services Overview

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

- **Name**—the name of the service
- **Protocol**—the protocol of the service
- **Port Start**—the starting port number for the service
- **Port End**—the ending port number for the service
- **Configure**—Displays the unavailable Notepad and Trashcan icon (default services cannot be edited or deleted, you will need to add a new service for the Notepad and Trashcan icons to become available).

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

Custom Services Configuration Task List

The following list provides configuration tasks for Custom Services:

- Adding Custom Services
- Editing Custom Services
- Deleting Custom Services
- Editing Custom Services Groups
- Deleting Custom Services Groups

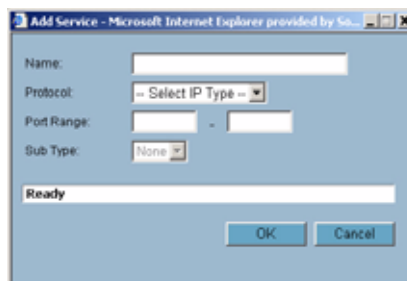
Supported Protocols

The following IP protocols are available for custom services:

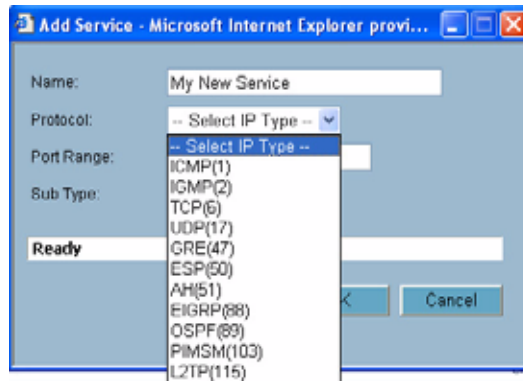
- ♦ **ICMP (1)**—(Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
- ♦ **IGMP (2)**—(Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
- ♦ **TCP (6)**—(Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
- ♦ **UDP (17)**—(User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
- ♦ **GRE (47)**—(Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP internetwork.
- ♦ **ESP (50)**—(Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
- ♦ **AH (51)**—(Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
- ♦ **EIGRP (88)**—(Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
- ♦ **OSPF (89)**—(Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- ♦ **PIMSM (103)**—(Protocol Independent Multicast Sparse Mode) One of two PIM operational modes (dense and sparse). PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
- ♦ **L2TP (115)**—(Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Custom Services

All custom services you create are listed in the **Custom Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement. If a protocol is not listed in the **Default Services** table, you can add it to the Custom Services table by clicking **Add**.




- 1 Enter the name of the service in the **Name** field.
- 2 Select the type of IP protocol from the **Protocol** pull-down menu.




- 3 Enter the Port Range or IP protocol Sub Type depending on your IP protocol selection:
 - ◆ For TCP and UDP protocols, specify the Port Range. You will not need to specify a Sub Type.
 - ◆ For ICMP, IGMP, OSPF and PIMSM protocols, select from the Sub Type pull-down menu for sub types.
 - ◆ For the remaining protocols, you will not need to specify a Port Range or Sub Type.
- 4 Click **OK**. The service appears in the **Custom Services** table.

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

Editing Custom Services

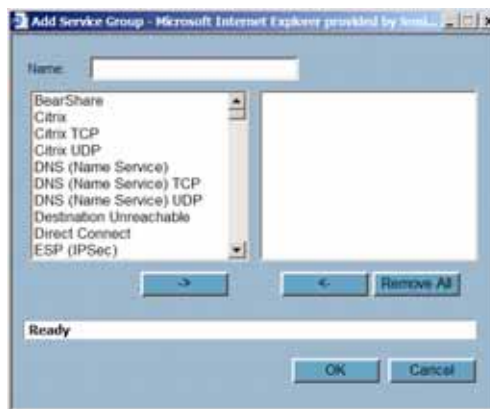
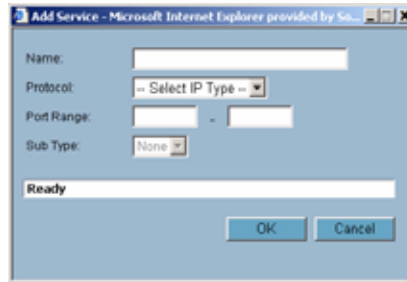
Click the **Edit** icon  under **Configure** to edit the service in the **Edit Service** window, which includes the same configuration settings as the **Add Service** window.

Deleting Custom Services

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

Adding a Custom Services Group


You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a Custom Service Group. To create a **Custom Services Group**, click **Add Group**.




- 1 Enter a name for the custom group in the name field.
- 2 Select individual services from the list in the left column. You can also select multiple services by pressing the **Ctrl** key and clicking on the services.
- 3 Click **- >** to add the services to the group.
- 4 To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.
- 5 Click **< -** to remove the services.
- 6 When you are finished, click **OK** to add the group to **Custom Services Groups**.

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

Editing Custom Services Groups

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

Deleting Custom Services Groups

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

Configuring Multicast Settings

Firewall > Multicast

Multicasting, also called IP multicasting, is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and videoconferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In multicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

The **Firewall > Multicast** page allows you to manage multicast traffic on the SonicWALL security appliance.



Multicast Snooping

This section provides configuration tasks for Multicast Snooping.

- **Enable Multicast** - This checkbox is disabled by default. Select this checkbox to support multicast traffic.
- **Require IGMP Membership reports for multicast data forwarding** - This checkbox is enabled by default. Select this checkbox to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP.
- **Multicast state table entry timeout (minutes)** - This field has a default of 5. The value range for this field is 5 to 60 (minutes). Update the default timer value of 5 in the following conditions:
 - ♦ You suspect membership queries or reports are being lost on the network.
 - ♦ You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
 - ♦ You want to synchronize the timing with an IGMP router.

Multicast Policies

This section provides configuration tasks for Multicast Policies.

- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses. Receiving all multicast addresses may cause your network to experience performance degradation.
- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the pull-down menu, select **Create a new multicast object** or **Create new multicast group**.



Note: Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from 224.0.0.1 to 239.255.255.255 can be bound to the MULTICAST zone.

To create a multicast address object:

- 1 In the **Enable reception for the following multicast addresses** list, select **Create new multicast object**.
- 2 In the Add Address Object window, configure:

- ◆ **Name:** The name of the address object.
- ◆ **Zone Assignment:** Select **MULTICAST**
- ◆ **Type:** Select Host, Range, Network, or MAC
- ◆ **IP Address:** If you selected Host or Network, the IP address of the host or network. The IP address must be in the range for multicast, 224.0.0.0 to 239.255.255.255.
- ◆ **Netmask:** If you selected Network, the netmask for the network.
- ◆ **Starting IP Address and Ending IP Address:** If you selected Range, the starting and ending IP address for the address range. The IP addresses must be in the range for multicast, 224.0.0.1 to 239.255.255.255.

IGMP State Table

This section provides descriptions of the fields in the **IGMP State** table.



- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as **LAN**) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—Provides the amount of time left before the IGMP entry will be flushed. This is calculated by subtracting the “**Multicast state table entry timeout (minutes)**” value, which has the default value of 5 minutes, and the elapsed time since the multicast address was added.
- **Flush** and **Flush All** buttons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

Enabling Multicast on LAN-dedicated Interfaces

Perform the following steps to enable multicast support on LAN-dedicated interfaces.

- 1 Enable multicast support on your SonicWALL security appliance. In the **Firewall > Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception of all multicast addresses**.
- 2 Enable multicast support on LAN interfaces. In the **Network > Interfaces** setting, click on the ‘**Configure**’ icon for the LAN interface. In the **Edit Interface - LAN** page, click on the **Enable Multicast Support** checkbox.

Perform the following steps to enable multicast support for address objects over a VPN tunnel.

- 3 Enable multicast support on your SonicWALL security appliance. In the **Firewall > Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception for the following multicast addresses** and select from the pull-down menu, **Create new multicast address object....**
- 4 Create a multicast address object. In the Add Address Object window, enter the following information for your address object:
 - ◆ **Name**
 - ◆ **Zone Assignment:** <LAN, WAN, DMZ, VPN, MULTICAST, WLAN, or a custom zone>
 - ◆ **Type:** <Host, Range, Network>
 - If you select **Host**, you will need to enter an **IP address**.

- If you select **Range**, you will need to enter a **Starting IP Address** and an **Ending IP Address**.
 - If you select **Network**, you will need to enter a description of the **Network** and a **Netmask**.
 - If you select **MAC**, you will need to enter a **MAC Address**.
- 5 Enable multicast support on the VPN policy for your GroupVPN. In the **VPN > Settings** firmware setting, click on the “**Configure**” icon to edit your GroupVPN’s VPN policy.
 - 6 In the **VPN Policy** window, select the **Advanced** tab. At the **Advanced** tab, select the **Enable Multicast** checkbox.

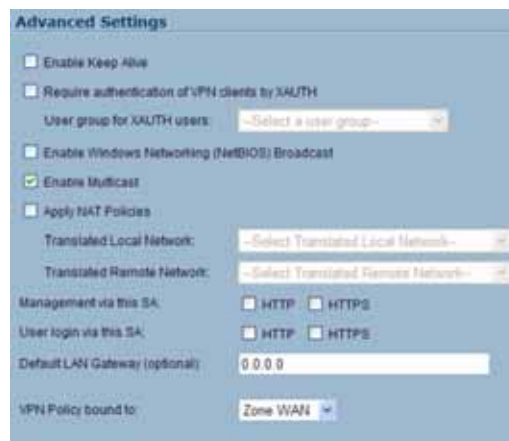
Enabling Multicast Through a VPN

To enable multicast across the WAN through a VPN, follow:

- 1 Enable multicast globally. On the **Firewall > Multicast** page, check the **Enable Multicast** checkbox, and click the **Apply** button for each security appliance.
- 2 Enable multicast support on each individual interface that will be participating in the multicast network. On the **Network > Interfaces** page for each interface on all security appliances participating, go to the **Edit Interface: Advanced** tab, and select the **Enable Multicast Support** checkbox.



- 3 Enable multicast on the VPN policies between the security appliances. From the **VPN > Settings** page, **Advanced** tab for each policy, select the **Enable Multicast** checkbox.



4 The resulting Access Rules should look as follows:

#	Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
MULTICAST										
15	LAN	MULTICAST 1	Any	Any	IGMP	Allow	All		<input checked="" type="checkbox"/>	
17	LAN	MULTICAST 2	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	
18	WAN	MULTICAST 1	Any	Any	Membership Query	Allow	All		<input checked="" type="checkbox"/>	
19	WAN	MULTICAST 2	Any	Any	IGMP	Deny	All		<input checked="" type="checkbox"/>	
20	WAN	MULTICAST 3	Any	Any	Any	Deny	All		<input checked="" type="checkbox"/>	
21	DMZ	MULTICAST 1	Any	Any	Membership Query	Allow	All		<input checked="" type="checkbox"/>	
22	DMZ	MULTICAST 2	Any	Any	IGMP	Deny	All		<input checked="" type="checkbox"/>	
23	DMZ	MULTICAST 3	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	
24	VPN	MULTICAST 1	Any	Any	IGMP	Allow	All		<input checked="" type="checkbox"/>	
25	VPN	MULTICAST 2	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	
26	WLAN	MULTICAST 1	Any	Any	Membership Query	Allow	All		<input checked="" type="checkbox"/>	
27	WLAN	MULTICAST 2	Any	Any	IGMP	Deny	All		<input checked="" type="checkbox"/>	
28	WLAN	MULTICAST 3	Any	Any	Any	Deny	All		<input checked="" type="checkbox"/>	

Notice that the default WLAN/MULTICAST access rule for IGMP traffic is set to 'DENY'. This will need to be changed to 'ALLOW' on all participating appliances to enable multicast, if they have multicast clients on their WLAN zones.

5 Make sure the tunnels are active between the sites, and start the multicast server application and client applications. As multicast data is sent from the multicast server to the multicast group (224.0.0.0 through 239.255.255.255), the SonicWALL security appliance will query its IGMP state table for that group to determine where to deliver that data. Similarly, when the appliance receives that data at the VPN Zone, it will query its IGMP State Table to determine where it should deliver the data.

The IGMP State Tables (upon updating) should provide information similar to the following:

#	Multicast Group Address	Interface/ Vpn Tunnel	IGMP Version	Time Remaining	Flush
1	224.15.16.17	OPT	V3	3 minute 52 second	
2	224.15.16.17	LAN	V2	3 minute 35 second	

This indicates that there is a multicast client on the **OPT** interface, and across the vpnMcastServer tunnel for the 224.15.16.17 group.



Note: By selecting "Enable reception of all multicast addresses", you might see entries other than those you are expecting to see when viewing your IGMP State Table. These are caused by other multicast applications that might be running on your hosts.

Monitoring Active Connections

Firewall > Connections Monitor

The **Firewall > Connections Monitor** page displays details on all active connections to the security appliance.

Firewall > Connections Monitor Refresh ?

Active Connections Monitor Settings

Filter	Value	Group Filters
Source IP:	<input type="text"/>	<input type="checkbox"/>
Destination IP:	<input type="text"/>	<input type="checkbox"/>
Destination Port:	<input type="text"/>	<input type="checkbox"/>
Protocol:	All Protocols	<input type="checkbox"/>
Src Interface:	All Interfaces	<input type="checkbox"/>
Dst Interface:	All Interfaces	<input type="checkbox"/>

Filter Logic: Source IP && Destination IP && Destination Port && Protocol && Src Interface && Dst Interface

Apply Filters Reset Filters Export Results

Active Connections Monitor Items 1 to 2 (of 2) < >

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.118	1936	10.0.93.32	443	TCP	WAN	WAN	1032	2262
2	10.0.202.118	1937	10.0.93.32	443	TCP	WAN	WAN	983	404

Viewing Connections

The connections are listed in the **Active Connections Monitor** table.

The screenshot shows a table titled "Active Connections Monitor" with 13 rows of data. The table has columns for #, Source IP, Source Port, Destination IP, Destination Port, Protocol, Src Interface, Dst Interface, Tx Bytes, and Rx Bytes. All connections are TCP and use WAN for both source and destination interfaces.

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.118	2149	10.0.93.32	443	TCP	WAN	WAN	1004	937
2	10.0.202.118	2158	10.0.93.32	443	TCP	WAN	WAN	1005	1393
3	10.0.202.118	2154	10.0.93.32	443	TCP	WAN	WAN	1002	542
4	10.0.202.118	2152	10.0.93.32	443	TCP	WAN	WAN	1049	2485
5	10.0.202.118	2151	10.0.93.32	443	TCP	WAN	WAN	1186	12532
6	10.0.202.118	2159	10.0.93.32	443	TCP	WAN	WAN	1071	404
7	10.0.202.118	2150	10.0.93.32	443	TCP	WAN	WAN	1426	27548
8	10.0.202.118	2157	10.0.93.32	443	TCP	WAN	WAN	1005	1370
9	10.0.202.118	2156	10.0.93.32	443	TCP	WAN	WAN	1005	1411
10	10.0.202.118	2147	10.0.93.32	443	TCP	WAN	WAN	1531	23322
11	10.0.202.118	2148	10.0.93.32	443	TCP	WAN	WAN	1143	9107
12	10.0.202.118	2153	10.0.93.32	443	TCP	WAN	WAN	1739	48015
13	10.0.202.118	2155	10.0.93.32	443	TCP	WAN	WAN	1006	1435

The table lists:

- **Source IP**
- **Source Port**
- **Destination IP**
- **Destination Port**
- **Protocol**
- **Src Interface**
- **Dst Interface**
- **Tx Bytes**
- **Rx Bytes**

Click on a column heading to sort by that column.

Filtering Connections Viewed

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Src Interface**, **Dst Interface**, and **Protocol**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

Filter	Value	Group Filters
Source IP:	<input type="text" value="192.168.168.1"/>	<input checked="" type="checkbox"/>
Destination IP:	<input type="text" value="10.16.31.2"/>	<input checked="" type="checkbox"/>
Destination Port:	<input type="text"/>	<input type="checkbox"/>
Protocol:	<input type="text" value="TCP(6)"/>	<input type="checkbox"/>
Src Interface:	<input type="text" value="LAN"/>	<input type="checkbox"/>
Dst Interface:	<input type="text" value="WLAN"/>	<input type="checkbox"/>
Filter Logic:	(Source IP Destination IP) && Destination Port && Protocol && Src Interface && Dst Interface	
<input type="button" value="Apply Filters"/>		<input type="button" value="Reset Filters"/>
<input type="button" value="Export Results..."/>		

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

Source IP AND Destination IP

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

(Source IP OR Destination IP) AND Protocol

Click **Apply Filter** to apply the filter immediately to the **Active Connections** table. Click **Reset** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

Managing Quality of Service

Working with QoS

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

This section contains the following subsections:

- [“Classification” section on page 341](#)
- [“Marking” section on page 342](#)
- [“Conditioning” section on page 343](#)

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS Enhanced uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicOS Enhanced 3.1 and later adds the ability to recognize, map, modify, and generate the industry-standard external CoS designators, DSCP and 802.1p (refer to the [“802.1p and DSCP QoS” section on page 344](#)).

Once identified, or classified, it can be managed. Management can be performed internally by SonicOS' BWM, which is perfectly effective as long as the network is a fully contained autonomous system. Once external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth (e.g. the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM will work exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. Once SonicOS Enhanced classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; thus they too can participate in providing QoS.



Note: *Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations will not be able to recognize 802.1p tags, and could drop tagged traffic.*

Although DSCP will not cause compatibility issues, many service providers will simply strip or ignore the DSCP tags, disregarding the code points.

If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider – some offer fee-based support for QoS using these CoS methods.

Marking

Once the traffic has been classified, if it is to be handled by QoS capable external systems (e.g. CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

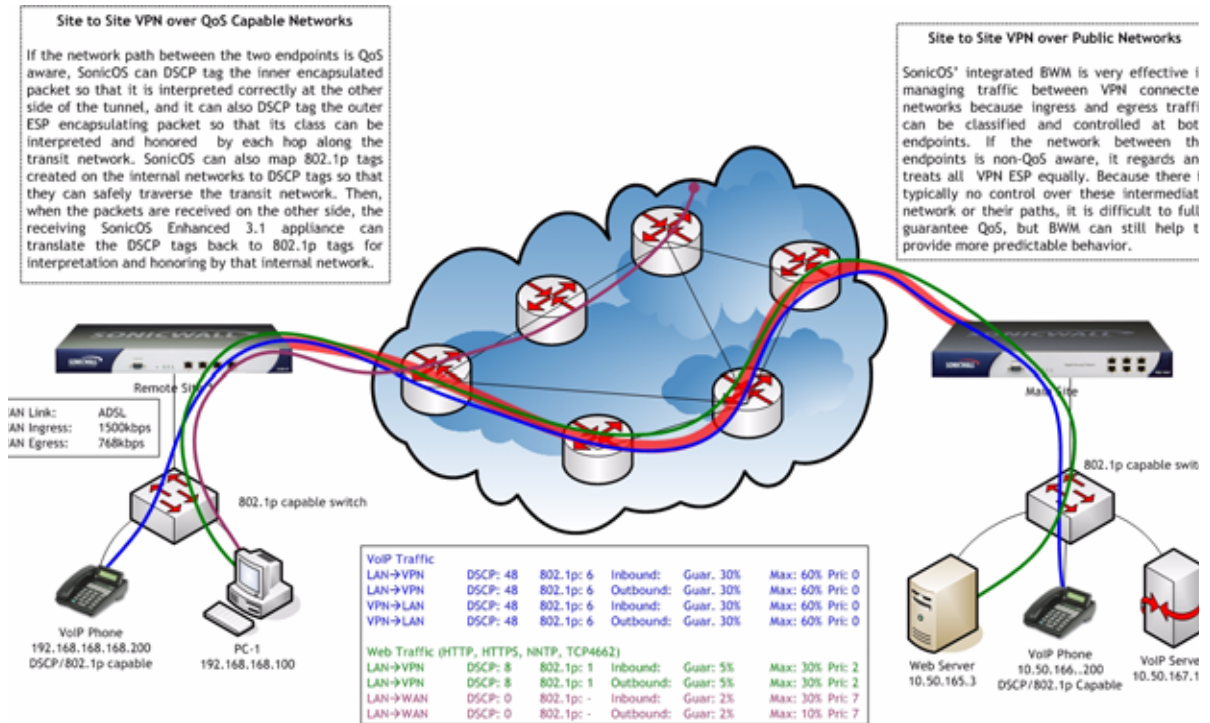
DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it will rarely mistreat or discard the packet.

The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p will only work with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (i.e. WAN links) was introduced in the form of **802.1p to DSCP mapping**.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS Enhanced, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS Enhanced appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to the [“802.1p and DSCP QoS” section on page 344](#) for more information.

Conditioning

Finally, the traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM), detailed in the [“Bandwidth Management” section on page 354](#). SonicOS’s BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to the [Example Scenario](#) in the [“Example Scenario” section on page 346](#) for a description of contention issues.



To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP. SonicOS Enhanced has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

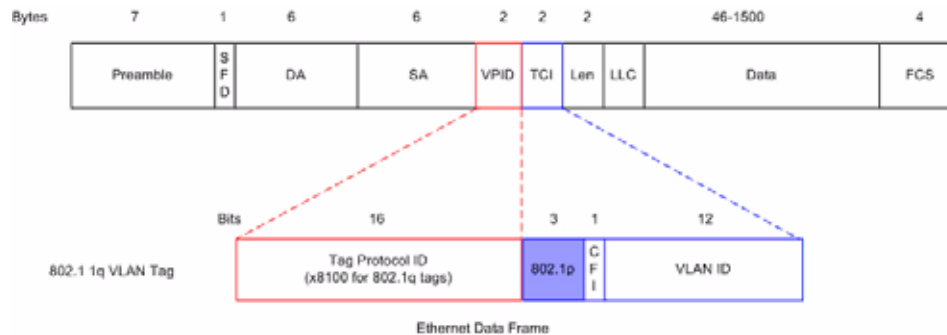
The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

802.1p and DSCP QoS

The following sections detail the 802.1p standard and DSCP QoS.

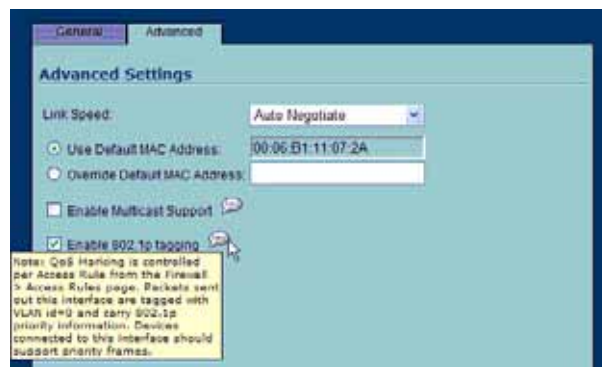
Enabling 802.1p

SonicOS Enhanced 3.1 and higher supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3 bits of an additional 16 bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:



- **TPID:** Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ethertype of 0x8100 for tagged traffic.
- **802.1p:** The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- **CFI:** Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VLAN ID:** VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12 bits and allows for the identification of 4,096 (2^{12}) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any SonicWALL appliance including the TZ 170 Series, PRO 2040, PRO 3060, PRO 4060, and PRO 5060.



Note: 802.1p tagging is not currently supported on the on the PRO 1260.

Although **Enable 802.1p tagging** does not appear as an option on VLAN sub-interfaces on the PRO 4060 and PRO 5060, the 802.1p field is already present within the 802.1q tags of VLAN sub-interfaces. The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of **None** will reset existing 802.1p tags to **0**, unless otherwise configured (see [“Managing QoS Marking” section on page 350](#) for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS will bear VLAN ID 0.

802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment’s documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** tab of the **Properties** page of your network card. If your card supports 802.1p, it will list it as **802.1p QoS**, **802.1p Support**, **QoS Packet Tagging** or something similar:



To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

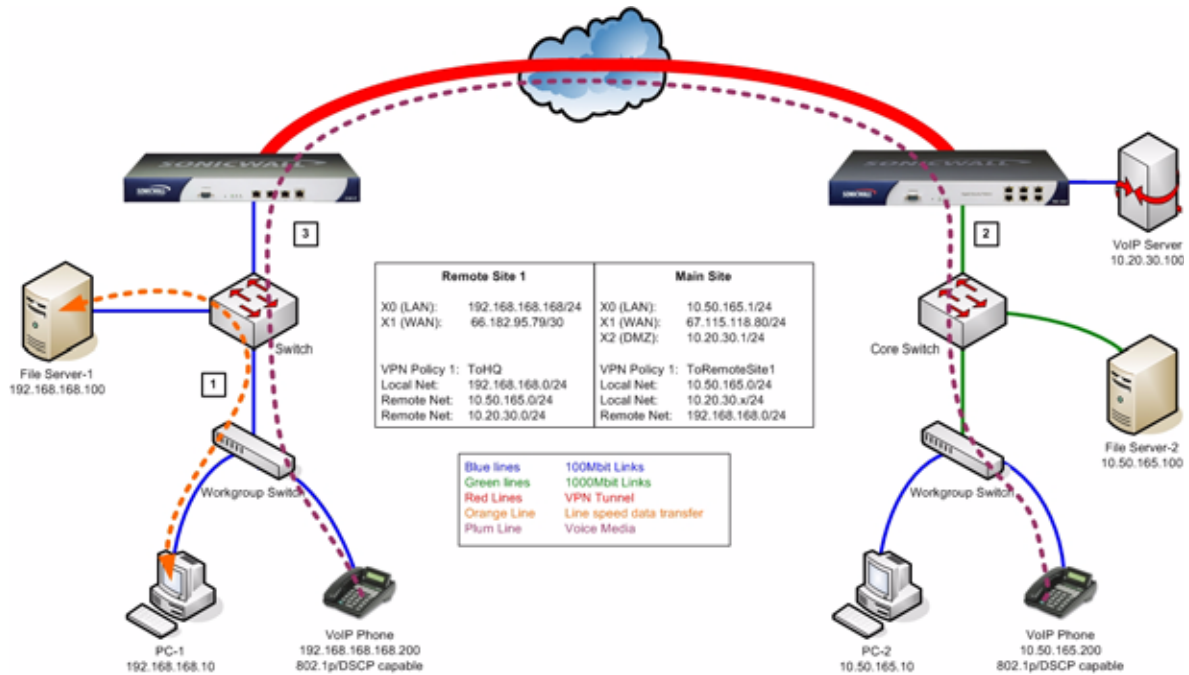


Note: *If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.*

It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on to [“Managing QoS Marking” section on page 350](#), it is important to introduce ‘DSCP Marking’ because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists.

Example Scenario



In the scenario above, we have **Remote Site 1** connected to 'Main Site' by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1. PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.
2. At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone 10.50.165.200 initiates a call to the person at VoIP phone 192.168.168.200. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.
 - a If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.
 - b If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

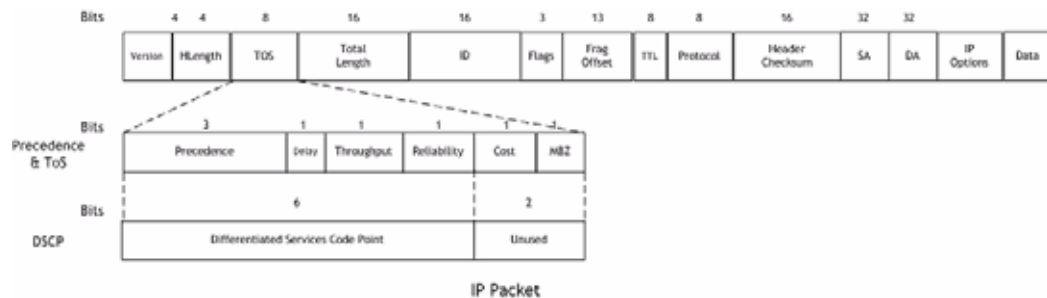
So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

- In our above scenario, the firewall at the Main Site assigns a DSCP tag (e.g. value **48**) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWALL, mapping the DSCP tag back to an 802.1p tag.
- The receiving SonicWALL at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the SonicWALL, it will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6 bits of the 8 bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Since DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP will simply ignore the tags, or at worst, they will reset the tag value to 0.



The above diagram depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

The following table shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-
26	Class 3, gold (AF31)	3 (Flash – 011)	T
27	Class 3, silver (AF32)	3 (Flash – 011)	D
30	Class 3, bronze (AF33)	3 (Flash – 011)	D, T

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
32	Class 4	4 (Flash Override – 100)	-
34	Class 4, gold (AF41)	4 (Flash Override – 100)	T
36	Class 4, silver (AF42)	4 (Flash Override – 100)	D
38	Class 4, bronze (AF43)	4 (Flash Override – 100)	D, T
40	Express forwarding	5 (CRITIC/ECP – 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/ECP – 101)	D, T
48	Control	6 (Internet Control – 110)	-
56	Control	7 (Network Control – 111)	-

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the QoS tab, and can be used in conjunction with 802.1p marking, as well as with SonicOS' internal bandwidth management.

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS Enhanced provides a replay window of 64 packets, i.e. if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (e.g. VoIP), and some that is DSCP tagged low-priority, or untagged/best-effort (e.g. FTP), your service provider will prioritize the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWALL's anti-replay defenses.

If symptoms of such a scenario emerge (e.g. excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (e.g. the VoIP network) on their own subnet.

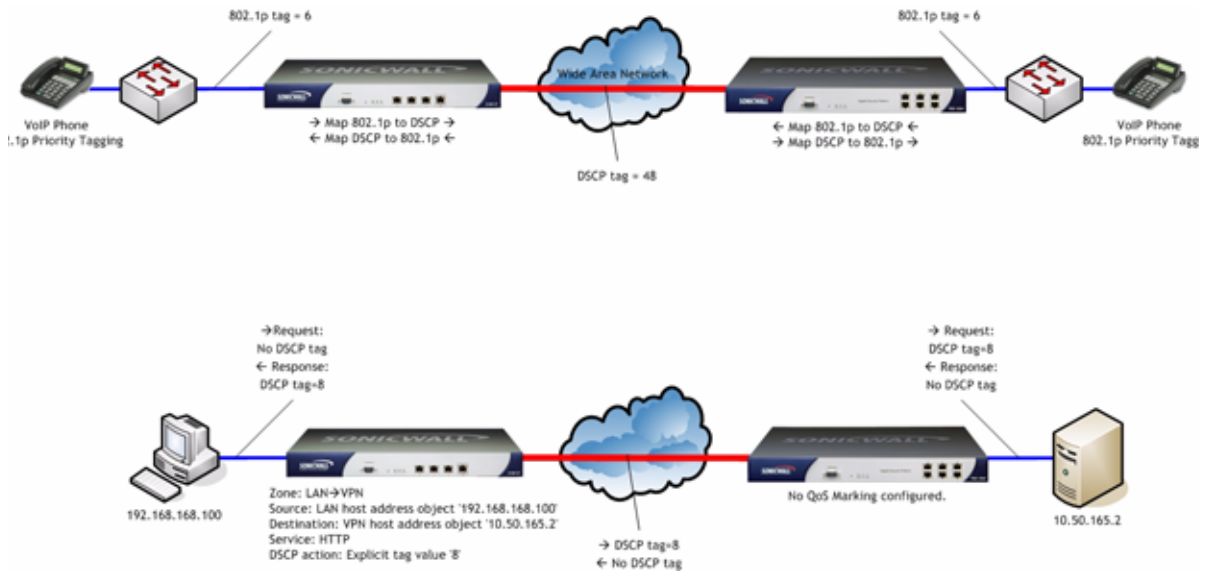


Configure for 802.1p CoS 4 – Controlled load

If you want to change the inbound mapping of DSCP tag **15** from its default 802.1p mapping of **1** to an 802.1p mapping of **2**, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping will give the error **DSCP range already exists or overlaps with another range**. First, you will have to remove **15** from its current end-range mapping to 802.1p CoS **1** (changing the end-range mapping of 802.1p CoS **1** to DSCP **14**), then you can assign DSCP **15** to the start-range mapping on 802.1p CoS **2**:

QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (e.g. WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side:



Note: Mapping will not occur until you assign **Map** as an action of the QoS tab of an Access Rule. The mapping table only defines the correspondence that will be employed by an Access Rule's Map action.

802.1p Class Of Service	To DSCP	From DSCP Range	Configure
0 - Best effort	0 - Best effort/Default	0-7	
1 - Background	8 - Class 1	8-15	
2 - Spare	16 - Class 2	16-23	
3 - Excellent effort	24 - Class 3	24-31	
4 - Controlled load	32 - Class 4	32-39	
5 - Video ($\leq 100\text{ms}$ latency)	40 - Express forwarding	40-47	
6 - Voice ($\leq 10\text{ms}$ latency)	48 - Control	48-55	
7 - Network control	56 - Control	56-63	

[Reset QoS Settings...](#)

For example, according to the default table, an 802.1p tag with a value of **2** will be outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** will be inbound mapped to an 802.1p value of **5**.

Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag 4 from its default DSCP value of 32 to a DSCP value of 43, you can click the **Configure** icon for 4 – **Controlled load** and select the new **To DSCP** value from the drop-down box:



802.1p CoS 1 end-range remap

802.1p CoS 2 start-range remap

You can restore the default mappings by clicking the **Reset QoS Settings** button.

Managing QoS Marking

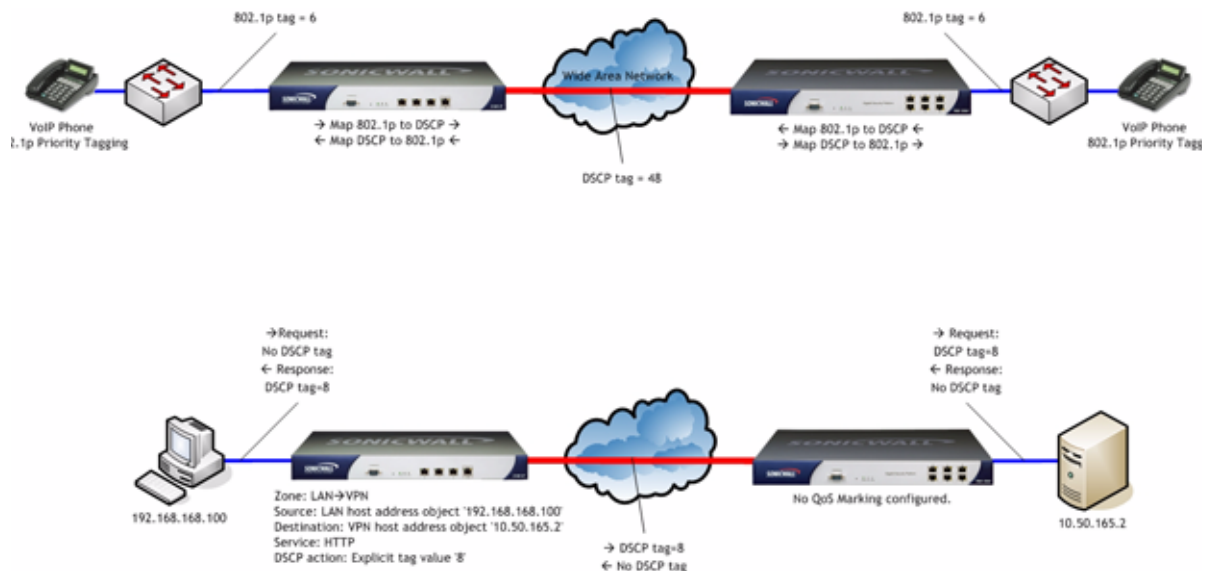
QoS marking is configured from the **QoS** tab of Access Rules under the **Firewall > Access Rules** page of the management interface. Both 802.1p and DSCP marking as managed by SonicOS Enhanced Access Rules provide 4 actions: None, Preserve, Explicit, and Map. The default action for DSCP is **Preserve** and the default action for 802.1p is **None**.

The following table describes the behavior of each action on both methods of marking:

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN sub-interface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the Preserve , Explicit , or Map action should be defined for this class of traffic.
Preserve	Existing 802.1p tag will be preserved.	Existing DSCP tag value will be preserved.	

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented.	If either the 802.1p or the DSCP action is set to Explicit while the other is set to Map , the explicit assignment occurs first, and then the other is mapped according to that assignment.
Map	The mapping setting defined in the Firewall > QoS Mapping page will be used to map from a DSCP tag to an 802.1p tag.	The mapping setting defined in the Firewall > QoS Mapping page will be used to map from an 802.1 tag to a DSCP tag. An additional checkbox will be presented to Allow 802.1p Marking to override DSCP values . Selecting this checkbox will assert the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If Map is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped to the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped to the DSCP tag.

For example, refer to the following figure which provides a bi-directional DSCP tag action.



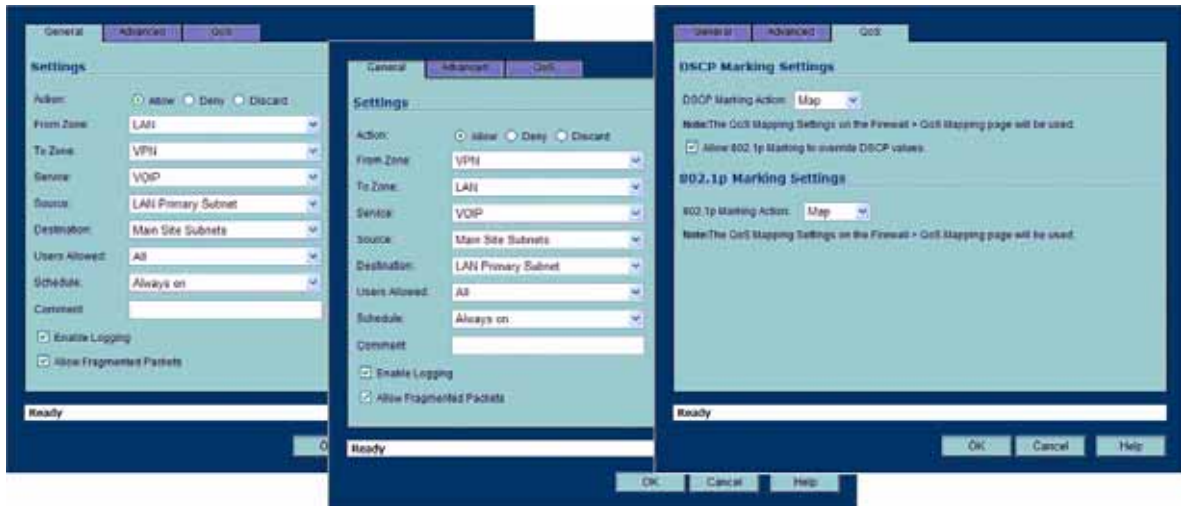
HTTP access from a web-browser on 192.168.168.100 to the web-server on 10.50.165.2 will result in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to 10.50.165.2, they will bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to 192.168.168.100 (beginning with the very first SYN/ACK packet) the Access Rule will tag the response packets delivered to 192.168.168.100 with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN Zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than None.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWALL interfaces, you can begin configuring Access Rules to manage 802.1p tags.

Referring to the following figure, the **Remote Site 1** network could have two Access Rules configured as follows:

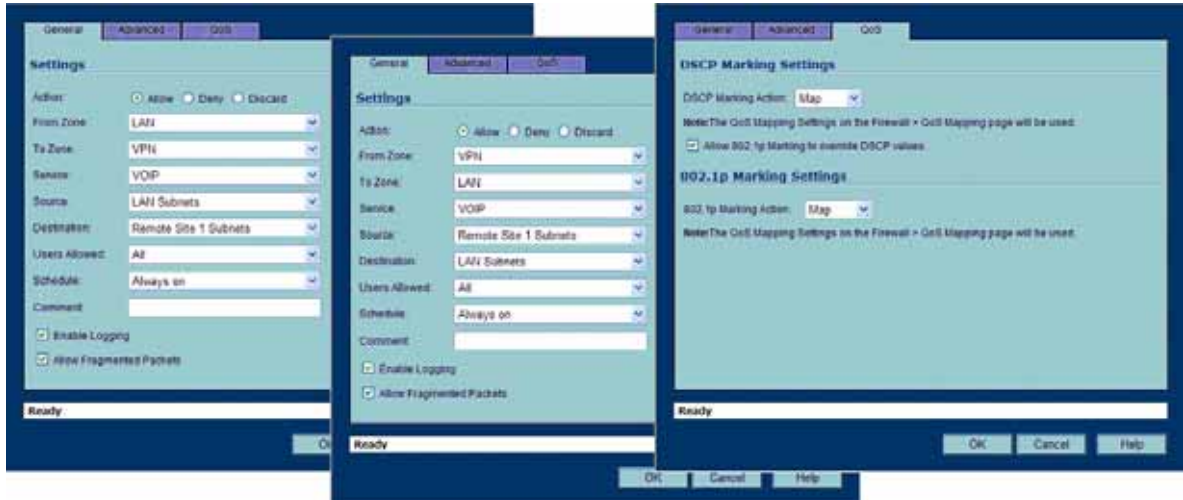


The first Access Rule (governing **LAN>VPN**) would have the following effects:

- **VoIP** traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to **Main Site Subnets** would be evaluated for both DSCP and 802.1p tags.
 - ♦ The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in the [“Managing QoS Marking” section on page 350](#).
 - ♦ Sent traffic containing only an 802.1p tag (e.g. CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
 - ♦ Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
 - ♦ Sent traffic containing only a DSCP tag (e.g. CoS = 48) would have the DSCP value preserved on both inner and outer packets.
 - ♦ Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
 - ♦ Sent traffic containing only both an 802.1p tag (e.g. CoS = 6) and a DSCP tag (e.g. CoS = 63) would give precedence to the 802.1p tag, and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Access Rule (VPN>LAN), we'll look at the Access Rules configured at the Main Site:



VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone will not have any 802.1p tags, only DSCP tags.

- ◆ Traffic exiting the tunnel containing a DSCP tag (e.g. CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Mapping** settings (e.g. CoS = 6) by the SonicWALL at the Main Site.
- ◆ Assuming returned traffic has been 802.1p tagged (e.g. CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- ◆ Assuming returned traffic has been DSCP tagged (e.g. CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- ◆ Assuming returned traffic has been both 802.1p tagged (e.g. CoS = 6) and DSCP tagged (e.g. CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

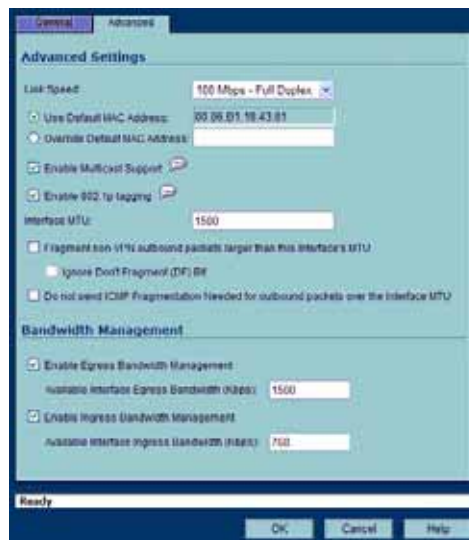
Bandwidth Management

SonicOS Enhanced offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) bandwidth management (BWM) interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public Zones (e.g. LAN and DMZ) destined to Untrusted and Encrypted Zones (e.g. WAN and VPN). Inbound BWM can be applied to traffic sourced from Untrusted and Encrypted Zones destined to Trusted and Public Zones.



Note: Although BWM is a fully integrated QoS system, wherein classification and shaping is performed on the single SonicWALL appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (i.e. layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the SonicWALL even after it has already shaped the traffic.

BWM configurations begin by enabling BWM on the relevant WAN interface, and declaring the interface's available bandwidth in Kbps (Kilobits per second). This is performed from the **Network > Interfaces** page by selecting the **Configure** icon for the WAN interface, and navigating to the **Advanced** tab:



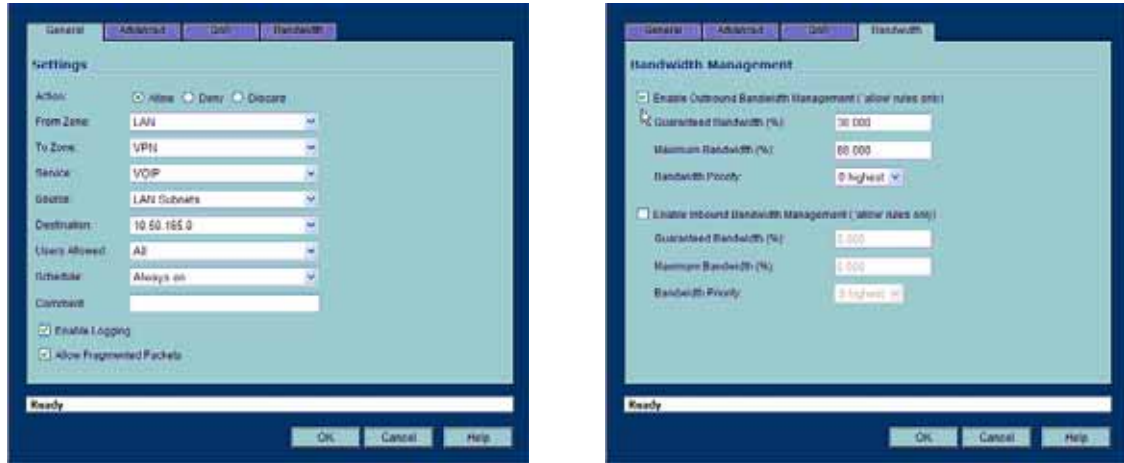
Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interface, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 (Gigabit). The speed declared should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.



Note: Once BWM has been enabled on an interface, and a link speed has been defined, traffic traversing that link will be throttled—both inbound and outbound—to the declared values, even if no Access Rules are configured with BWM settings.

Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a **Bandwidth** tab will appear on Access Rules. The Bandwidth tab will present either

Inbound settings, **Outbound** settings, or both, depending on what was enabled on the WAN interface:



The configuration on the **General** tab will classify the traffic. In the above example, which assumes no other configured BWM rules, traffic from the LAN (Trusted) Zone's **LAN Subnets** destined to the VPN (Encrypted) Zone's **10.50.165.0** remote subnet, consisting of Service Group **VOIP** will be guaranteed 30% of the declared bandwidth (30% of 1500Kbps = 450Kbps), but it will not be permitted to exceed 80% (80% of 1500Kbps = 1200Kbps), leaving 300Kbps for other traffic.

Declaration Limits

Bandwidth Management rules each consume memory for packet queuing, so the number of allowed queued packets and rules on SonicOS Enhanced is limited by platform (values are subject to change):

Platform	RAM	Max Queued Packets	Max Outbound BWM Rules	Max Inbound BWM Rules	Total BWM Rules
TZ 170 Family	64MB	220	20	20	40
PRO 1260	64MB	220	20	20	40
PRO 2040	128MB	520	25	25	50
PRO 3060	256MB	2080	100	100	200
PRO 4060	256MB	2080	100	100	200
PRO 5060	512MB	6240	100	100	200



Note: Consider the following about bandwidth management

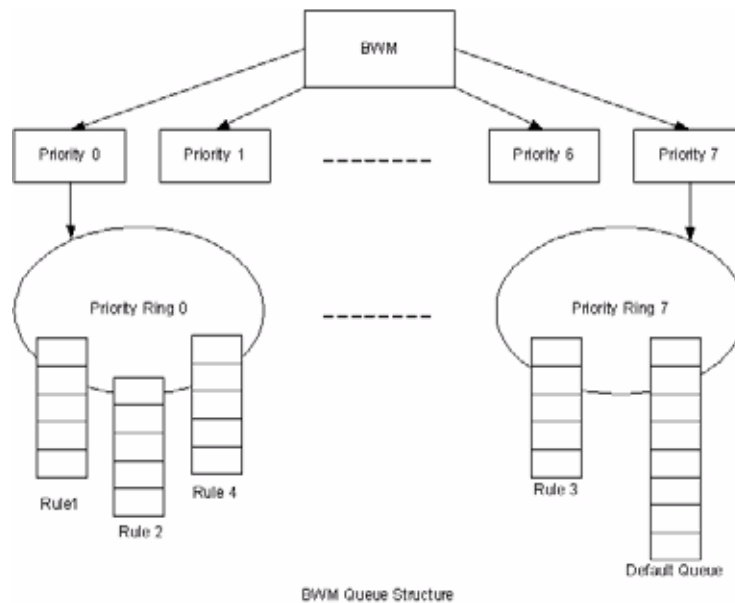
- The grand total of all declared Guaranteed Bandwidth percentages across all BWM rules cannot exceed 100%, since it is not possible to guarantee greater than 100% of the available bandwidth.
- The grand total of all Maximum Bandwidth values must be equal to or greater than the total Guaranteed Bandwidth.
- The grand total of all Maximum Bandwidth values may exceed 100% (e.g. every BWM rule may specify 100% Maximum Bandwidth, if no explicit throttling is required).

Outbound Bandwidth Management

Bandwidth Management as employed by SonicOS Enhanced is based on an amalgamation of queue management and congestion avoidance techniques, but in empirical practice it most closely resembles Class Base Queuing (CBQ), as defined by Sally Floyd and Van Jacobson in **Link-sharing and Resource Management Models for Packet Networks**, while incorporating elements of RFC2309 **Recommendations on Queue Management and Congestion Avoidance in the Internet** and various credit-based flow control theory. The overarching goals of the SonicOS BWM scheme are:

- **Simplicity** – The processing overhead must be consistently and appreciably less than average packet transmission times.
- **Robustness** – The scheduler must perform well under predictable and unpredictable traffic conditions, and must not introduce undesirable side effects such as traffic bursts or synchronization issues.
- **Fairness** – The sharing of available bandwidth should be commensurate with the defined management scheme, particularly in the presence of poorly behaving or **greedy** traffic.

The available bandwidth on a WAN link is tracked by means of adjusting a link credit (token) pool for each packet sent. Providing that the link hasn't reached a point of saturation, the prioritized queues are deemed eligible for processing.



Like CBQ, SonicOS BWM is based on a class structure, where traffic queues are classified according to Access Rules—for example SSH, Telnet, or HTTP—and then scheduled according to their prescribed priority. Each participating Access Rule is assigned three values: Guaranteed bandwidth, Maximum bandwidth, and Bandwidth priority. Scheduling prioritization is achieved by assignment to one of eight priority rings, starting at 0 (zero) for the highest priority, and descending to 7 (seven) for the lowest priority. The resulting queuing hierarchy can be best thought of as a node tree structure that is always one level deep, where all nodes are leaf nodes, containing no children.

Queue processing utilizes a time division scheme of approximately 1/256th of a second per time-slice. Within a time-slice, evaluation begins with priority 0 queues, and on a packet-by-packet basis transmission eligibility is determined by measuring the packet's length against the queue credit pool. If sufficient credit is available, the packet is transmitted and the queue and link credit pools are decremented accordingly. As long as packets remain in the queue, and as long as Guaranteed link and queue credits are available, packets from that queue will continue to be processed. When Guaranteed queue credits are depleted, the next queue in that priority ring is processed. The same

process is repeated for the remaining priority rings, and upon completing priority ring 7 begins again with priority ring 0.

The scheduling for excess bandwidth is strict priority, with per-packet round-robin within each priority. In other words, if there is excess bandwidth for a given time-slice all the queues within that priority ring would take turns sending packets until the excess was depleted, and then processing would move to the next priority ring.

This credit based method obviates the need for CBQ's concept of **overlimit**, and addresses one of the largest problems of traditional CBQ, namely, **bursty** behavior (which can easily flood downstream devices and links). This more prudent approach spares SonicOS the wasted CPU cycles that would normally be incurred by the need for re-transmission due to the saturation of downstream devices, as well as avoiding other congestive and degrading behaviors such as TCP slow-start (see Sally Floyd's **Limited Slow-Start for TCP with Large Congestion Windows**), and Global Synchronization (as described in RFC 2884):

Queue management algorithms traditionally manage the length of packet queues in the router by dropping packets only when the buffer overflows. A maximum length for each queue is configured. The router will accept packets till this maximum size is exceeded, at which point it will drop incoming packets. New packets are accepted when buffer space allows. This technique is known as Tail Drop. This method has served the Internet well for years, but has the several drawbacks. Since all arriving packets (from all flows) are dropped when the buffer overflows, this interacts badly with the congestion control mechanism of TCP. A cycle is formed with a burst of drops after the maximum queue size is exceeded, followed by a period of underutilization at the router as end systems back off. End systems then increase their windows simultaneously up to a point where a burst of drops happens again. This phenomenon is called Global Synchronization. It leads to poor link utilization and lower overall throughput. Another problem with Tail Drop is that a single connection or a few flows could monopolize the queue space, in some circumstances. This results in a lock out phenomenon leading to synchronization or other timing effects. Lastly, one of the major drawbacks of Tail Drop is that queues remain full for long periods of time. One of the major goals of queue management is to reduce the steady state queue size.

Algorithm for Outbound Bandwidth Management

Each packet through the SonicWALL is initially classified as either a **Real Time** or a **Firewall** packet. Firewall packets are user-generated packets that always pass through the BWM module. Real time packets are usually firewall generated packets that are not processed by the BWM module, and are implicitly given the highest priority. Real Time (firewall generated) packets include:

- WAN Load Balancing Probe
- ISAKMP
- Web CFS
- PPTP and L2TP control packets
- DHCP
- ARP Packets
- Web Sense
- Syslog
- NTP
- Security Services (AV, signature updates, license manager)

Outbound BWM Packet Processing Path

- a Determine that the packet is bound for the WAN Zone.
- b Determine that the packet is classifiable as a Firewall packet.
- c Match the packet to an Access Rule to determine BWM setting.
- d Queue the packet in the appropriate rule queue.

Guaranteed Bandwidth Processing

This algorithm depicts how all the policies use up the GBW.

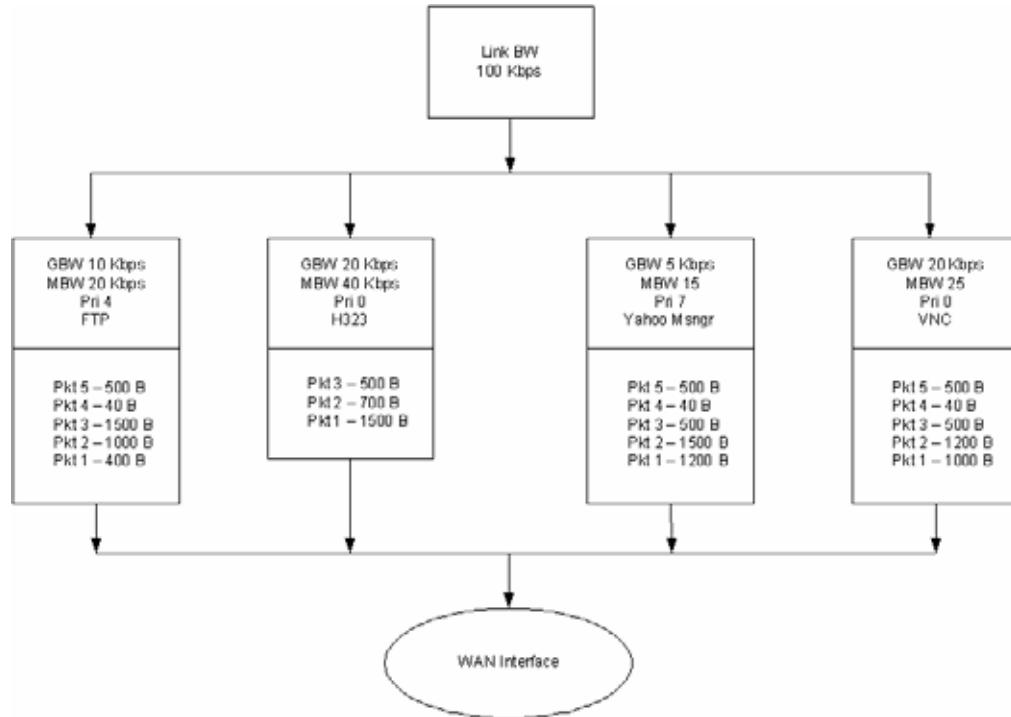
- a Start with a link credit equal to available link BW.
- b Initialize the class credit with configured GBW for the rule.
- c If that packet length is less than or equal to the class credit, transmit the packet and deduct the length from class credit and link credit.
- d Choose the next packet from queue and repeat step c until class credit is lesser or rule queue is empty.
- e Choose the next rule queue and repeat steps b through d.

Maximum Bandwidth Processing

This algorithm depicts how the unutilized link BW is used up by the policies. We start with the highest priority ring and transmit packets from all the rule queues in a round robin fashion until link credit is exhausted or all queues are empty. Then we move on to the next lowest priority ring and repeat the same.

- a Start with the link credit equal to the left over link BW after GBW utilization.
- b Choose the highest priority ring.
- c Initialize class credit to (MBW - GBW).
- d Check if the length of a packet from the rule queue is below class credit as well as link credit.
- e If yes, transmit the packet and deduct the length from class credit and link credit.
- f Choose the next rule queue and repeat steps c thru f until link credit gets exhausted or this priority ring has all its queues empty.
- g Choose the next lowest priority ring and repeat steps c thru f.

Example of Outbound BWM



The above diagram shows 4 policies are configured for OBWM with a link capacity of 100 Kbps. This means that the link capacity is 12800 Bytes/sec. Below table gives the BWM values for each rule in Bytes per second.

BWM values	FTP	H323	Yahoo Messenger	VNC
GBW	1280	2560	640	2560
MBW	2560	5120	1920	3200

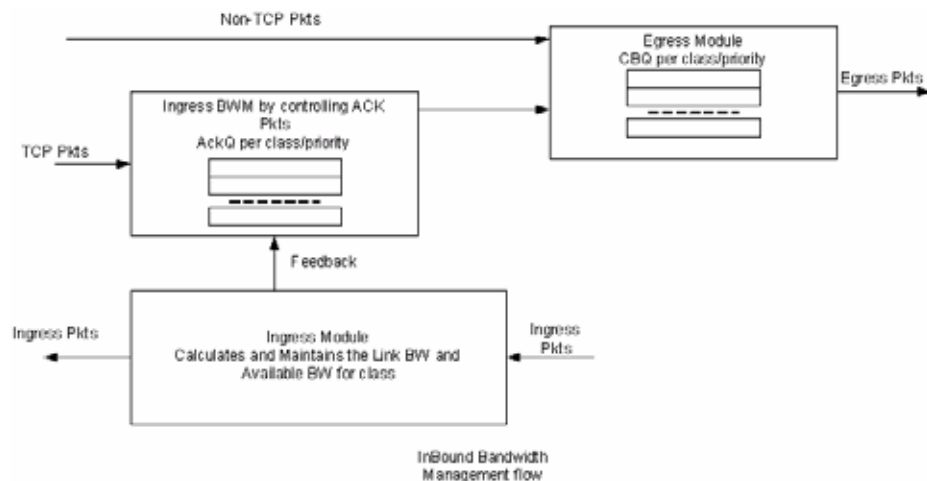
- a For GBW processing, we start with the first queue in the rule queue list which is FTP. Link credit is 12800 and class credit is 1280. Pkt1 of 400B is sent out on the WAN link and link credit becomes 12400 and class credit becomes 880. Pkt2 is not sent out because there is not enough class credit to send 1500 Bytes. The remaining class credit is carried over to the next time slice.
- b We move on to the next rule queue in this list which is for H323. Pkt1 of 1500B is sent out and link credit becomes 10900 and class credit for H323 becomes 1060. Pkt2 is also sent from queue hence link credit = 10200 and class credit = 360. Pkt3 is not sent since there is not enough class credit. The remaining class credit is carried over to the next time slice.
- c Now we move onto Yahoo Messenger queue. Since Pkt1 cannot be accommodated with its class credit of 640 Bytes, no packets are processed from this queue. However, its class credit is carried over to the next time slice.
- d From VNC queue, Pkt1 and Pkt2 are sent out leaving link credit = 8000 and class credit = 360. Class credit is carried over.
- e Since all the queues have been processed for GBW we now move onto use up the left over link credit of 8000.
- f Start off with the highest priority ring 0 and process all queues in this priority in a round robin fashion. H323 has Pkt3 of 500B which is sent since it can use up to max = 2560 (MBW-GBW). Now Link credit = 7500 and max = 2060.

- g Move to the next queue in this priority ring which is VNC queue. Pkt3 of 500B is sent out leaving link credit = 7000B and class max = 140 (MBW-GBW - 500).
- h Move to the next queue in this priority ring. Since H323 queue is empty already we move to the next queue which is VNC again.
- i From VNC queue Pkt4 of 40B is sent out leaving link credit = 6960 and class max = 100. Pkt5 of 500B is not sent since class max is not enough.
- j Now we move onto next lower priority queue. Since priority rings 1 thru 3 are empty we choose priority ring 4 which has the rule queue for FTP. Pkt2 of 1000B is sent which leaves with link credit = 6000 and class max = 280. Since there are no other queues in this priority, FTP queue is processed again. But since class max is not enough for Pkt3 of 1500B it is not sent.
- k Move to the next lower priority ring which is 7 for Yahoo Messenger. Pkt1 of 1200B is sent leaving link credit = 4800 and class max = 80. Since no other queues exist in this priority, this queue is processed again. Pkt2 of 1500B is not sent since it cannot be accommodated with max = 80.
- l At this point, all the queues under all priority rings are processed for the current time slice.

Inbound Bandwidth Management

Inbound BWM can be used to shape inbound TCP and UDP traffic. TCP's intrinsic flow control behavior is used to manage ingress bandwidth. To manage inbound UDP traffic, CBQ is used by the ingress module to queue the incoming packets. TCP rate is inherently controlled by the rate of receipt of ACKs; i.e. TCP sends out packets out on the network at the same rate as it receives ACKs. For IBWM, the sending rate of a TCP source will be reduced by controlling the rate of ACKs to the source. By delaying an ACK to the source, round-trip time (RTT) for the flow is increased, thus reducing the source's sending rate.

An ingress module monitors and records the ingress rate for each traffic class. It also monitors the egress ACKs and queues them if the ingress rate has to be reduced. According to ingress BW availability and average rate, the ACKs will be released.



Algorithm for Inbound Bandwidth Management

IBWM maintains eight priority rings, where each priority ring has one queue for a rule that has IBWM enabled. The IBWM pool is processed from the highest to lowest priority ring further shaping the traffic. IBWM employs three key algorithms:

Ingress Rate Update

This algorithm processes each packet from the WAN and updates the ingress rate of the class to which it belongs. It also marks the traffic class if it has over utilized the link.

- a Determine that the packet is from the WAN zone and is a firewall packet.
- b Add the packet length to the sum of packet lengths received so far in the current time slice. Deduct the minimum of (GBW, packet length) from link's credit.
- c If the sum is greater than the class's credit, mark the class to be over utilizing the link.
- d If the packet length is greater than the link's credit, mark the link as well as the class to be over utilized.

Egress ACK monitor

This algorithm depicts how the egress ACKs are monitored and processed.

- a Determine that the packet is to the WAN zone and is a TCP ACK.
- b If class or interface is marked as over utilizing, queue the packet in the appropriate ingress rule queue.

Process ACKs

This algorithm is used to update the BW parameters per class according to the amount of BW usage in the previous time slice. Amount of BW usage is given by the total number of bytes received for the class in the previous time slice. The algorithm is also used to process the packets from the ingress module queues according to the available credit for the class.

Credit Based Processing

A class will be in debt when its BW usage is more than the GBW for a particular time slice. All the egress ACKs for the class are then queued until the debt is reduced to zero. At each successive time slice, debt is deducted by GBW and if link BW is left, (MBW – GBW) is also deducted.

Compute BW usage in the previous time slice:

- a Compute average ingress rate using the amount of BW usage by the class.
- b If the BW usage is more than the class credit, record the difference as debt. If link BW is left over, deduct (MBW - GBW) from debt.

Compute the class and link credit for the current time slice:

- c If the class is in debt, deduct GBW from debt and also from link's credit, indicating that the class has already used up its GBW for the current time slice.
- d If class is not in debt and there are packets arriving for this class, accumulate link credit; i.e. add GBW to credit at each time slice.
- e Class is marked as over utilizing if debt is nonzero.

Process packets from ingress pool from highest priority ring to lowest priority ring:

- f Record class credit as remaining credit.
- g If remaining credit is greater than or equal to average rate, process the ACK packet and deduct average rate from remaining credit.
- h Repeat g until remaining credit is not enough or the ingress ACK queue is empty.
- i Repeat steps f thru h for the next rule queue in the ring.
- j Repeat steps f thru i for the next lowest priority ring.

Example of Inbound Bandwidth Management

Consider a class with GBW = 5 Kbps, MBW = 10 Kbps and Link BW = 100 Kbps. In terms of bytes\second we have GBW=640, excess BW = (MBW - GBW) = 640 and link BW = 12800.

No.	Ingress	Egress	Credit	Debt	Rate	Link BW	#Acks
1.	0	0	640	0	0	12800	0
2.	1300	0	620	0	1300	12780	0
2a.	0	40	620	0	1300	12780	1
3.	0	0	1260	0	1300	12800	1
4.	0	0	1900	0	1300	12800	0

- a Class credit starts with 640. In row 2, 1300 bytes are received for this class in the previous time slice. Since it is more than the class credit, debt = 20 (1300-GBW-excess BW). For the current time slice class credit = 620 (GBW - debt), debt = 0 and link BW = 12780 since 20 bytes of debt is already used up from GBW for the class.
- b Row 2a shows an egress ACK for the class. Since class credit is less than the rate this packet is queued in the appropriate ingress queue. And it will not be processed until class credit is at least equal to the rate.
- c In the following time slices, class credit gets accumulated until it matches the rate. Hence, after two time slices class credit becomes 1900 (620 + 640 + 640). The queued ACK packet is process from the ingress pool at this point.

In row 2a, an ACK packet is received that needs to be sent to the TCP source on the WAN zone. Sending this ACK immediately would have caused the TCP source to send more packets immediately. By queuing the ACK and sending it only after the class credit reaches the average rate, we have reduced the TCP's sending rate; i.e. by doing this we have slowed down the ingress rate.

BWM with WAN load balancing

BWM with WAN load balancing works in the following manner:

- a If two interfaces are configured as WAN and load balancing is NOT enabled, BWM is only applied to the primary WAN interface.
- b If two interfaces are configured as WAN and load balancing is enabled:
 - For Active/Passive Failover, BWM is done only on the active WAN interface.
 - For Round Robin and Ratio options, link capacity is the sum of available BW for primary and secondary WAN interface and BWM is done on both interfaces.
 - For Spill Over option, link capacity is Primary's available BW and BWM is done on primary interface before the spill over occurs. And after the spill over occurs, the secondary interface's capacity is used and BWM is done on the secondary WAN interface.

Glossary

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16 bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks.
- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWALL employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic. Important terminologies used within SonicWALL's BWM implementation include:
 - **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
 - **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.
 - **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth.
 - **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism.
 - **Priority** – An additional dimension used in the classification of traffic. SonicOS uses 8 priority rings (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority ring.
 - **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic's sensitivity to delay, latency, or packet loss. Classification within SonicOS Enhanced uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
 - **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (e.g. prioritized queuing, low latency, etc.) as defined by the QoS system administrator.
 - **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.
 - **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.
 - **DiffServ** – Differentiated Services. A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently include at a minimum **Default, Assured**

Forwarding, and **Expedited Forwarding**. Refer to the [“DSCP Marking” section on page 347](#) for more information.

- **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
- **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
- **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.
- **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.
- **DSCP** – (Differentiate Services Code Points) – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.
- **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.
- **IntServ** – Integrated Services, as defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by SonicOS. The most common implementation of IntServ is RSVP.
- **Mapping** – Mapping, with regard to SonicOS' implementation of QoS, is the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for the purpose as preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules.
- **Marking** – Also known as **tagging** or **coloring** – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination.

- **MPLS** - Multi Protocol Label Switching. A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including SonicWALL appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.
- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.
- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.
- **Queuing** – To effectively make use of a link’s available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety of methods and algorithms to ensure that the higher priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:
 - **FIFO** – First In First Out. A very simple, undiscriminating queue where the first packet in is the first packet to be processed.
 - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets’ IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.
 - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
 - **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by SonicOS’ BWM.
- **RSVP** – Resource Reservation Protocol. An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (e.g. delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ’s RSVP is quite different from DiffServ’s DSCP, the two can interoperate. RSVP is not supported by SonicOS.
- **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.
- **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ’s code point values.

PART

8

VoIP

Configuring VoIP Support

This chapter contains the following sections:

- “VoIP Overview” on page 369
- “SonicWALL’s VoIP Capabilities” on page 371
- “Configuring SonicWALL VoIP Features” on page 378
- “VoIP Deployment Scenarios” on page 389

VoIP Overview

This section provides an overview of VoIP. It contains the following sections:

- “What is VoIP?” on page 369
- “VoIP Security” on page 369
- “VoIP Protocols” on page 370

What is VoIP?

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

VoIP Security

Companies implementing VoIP technologies in an effort to cut communication costs and extend corporate voice services to a distributed workforce face security risks associated with the convergence of voice and data networks. VoIP security and network integrity are an essential part of any VoIP deployment.

The same security threats that plague data networks today are inherited by VoIP but the addition of VoIP as an application on the network makes those threats even more dangerous. By adding VoIP components to your network, you're also adding new security requirements.

VoIP encompasses a number of complex standards that leave the door open for bugs and vulnerabilities within the software implementation. The same types of bugs and vulnerabilities that hamper every operating system and application available today also apply to VoIP equipment. Many of today's VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems.

Firewall Requirements for VoIP

VoIP is more complicated than standard TCP/UDP-based applications. Because of the complexities of VoIP signaling and protocols, as well as inconsistencies that are introduced when a firewall modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard firewall. Here are a few of the reasons why.

- **VoIP operates using two separate protocols** - A signaling protocol (between the client and VoIP Server) and a media protocol (between the clients). Port/IP address pairs used by the media protocols (RTP/RTCP) for each session are negotiated dynamically by the signaling protocols. Firewalls need to dynamically track and maintain this information, securely opening selected ports for the sessions and closing them at the appropriate time.
- **Multiple media ports are dynamically negotiated through the signaling session** - negotiations of the media ports are contained in the payload of the signaling protocols (IP address and port information). Firewalls need to perform deep packet inspection on each packet to acquire the information and dynamically maintain the sessions, thus demanding extra firewall processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A firewall supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT firewalls adjust their NAT bindings frequently, and may arbitrarily close the pinholes that allow inbound packets to pass into the network they protect, eliminating the service provider's ability to send inbound calls to the customer. To effectively support VoIP it is necessary for a NAT firewall to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the firewall.
- **Firewalls need to process the signaling protocol suites consisting of different message formats used by different VoIP systems** - Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

To overcome many of the hurdles introduced by the complexities of VoIP and NAT, vendors are offering Session Border Controllers (SBCs). An SBC sits on the Internet side of a firewall and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signalling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled firewalls. SonicWALL security appliances are VoIP enabled firewalls that eliminate the need for an SBC on your network.

VoIP Protocols

VoIP technologies are built on two primary protocols, H.323 and SIP.

H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It's a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet. H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

H.323 uses a combination of TCP and UDP for signaling and ASN.1 for message encoding. H.323v1 was released in 1996 and H.323v5 was released in 2003. As the older standard, H.323 was embraced by many early VoIP players.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC.
- **Gatekeepers** - Performs services for call setup and tear down, and registering H.323 terminals for communications. Includes:
 - ♦ Address translation.
 - ♦ Registration, admission control, and status (RAS).
 - ♦ Internet Locator Service (ILS) also falls into this category (although it is not part of H.323). ILS uses LDAP (Lightweight Directory Access Protocol) rather than H.323 messages.
- **Multipoint control units (MCUs)** - Conference control and data distribution for multipoint communications between terminals.
- **Gateways** - Interoperation between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN).

SIP

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports 'presence' and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

A SIP network is composed of the following logical entities:

- **User Agent (UA)** - Initiates, receives and terminates calls.
- **Proxy Server** - Acts on behalf of UA in forwarding or responding to requests. A Proxy Server can fork requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.
- **Redirect Server** - Responds to request but does not forward requests.
- **Registration Server** - Handles UA authentication and registration.

SonicWALL's VoIP Capabilities

The following sections describe SonicWALL's integrated VoIP service:

- "VoIP Security" on page 372
- "VoIP Network" on page 372
- "VoIP Network Interoperability" on page 373
- "Supported VoIP Protocols" on page 374
- "How SonicOS Handles VoIP Calls" on page 376

VoIP Security

- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the firewall ensures all traffic is legitimate. Packets that exploit implementation flaws, causing effects such as buffer overflows in the target device, are the weapons of choice for many attackers. SonicWALL security appliances detect and discard malformed and invalid packets before they reach their intended target.
- **Application-layer protection for VoIP protocols** - Full protection from application-level VoIP exploits through SonicWALL Intrusion Prevention Service (IPS). IPS integrates a configurable, high performance scanning engine with a dynamically updated and provisioned database of attack and vulnerability signatures to protect networks against sophisticated Trojans and polymorphic threats. SonicWALL extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers.
- **DoS and DDoS attack protection** - Prevention of DoS and DDoS attacks, such as the SYN Flood, Ping of Death, and LAND (IP) attack, which are designed to disable a network or service.
 - ♦ Validating packet sequence for VoIP signaling packets using TCP to disallow out of sequence and retransmitted packets beyond window.
 - ♦ Using randomized TCP sequence numbers (generated by a cryptographic random number generator during connection setup) and validating the flow of data within each TCP session to prevent replay and data insertion attacks.
 - ♦ Ensures that attackers cannot overwhelm a server by attempting to open many TCP/IP connections (which are never fully established-usually due to a spoofed source address) by using SYN Flood protection.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.
- **Encrypted VoIP Device Support** - SonicWALL supports VoIP devices capable of using encryption to protect the media exchange within a VoIP conversation or secure VoIP devices that do not support encrypted media using IPsec VPNs to protect VoIP calls.
- **Application-Layer Protection** - SonicWALL delivers full protection from application-level VoIP exploits through SonicWALL Intrusion Prevention Service (IPS). SonicWALL IPS is built on a configurable, high performance Deep Packet Inspection engine that provides extended protection of key network services including VoIP, Windows services, and DNS. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

VoIP Network

- **VoIP over Wireless LAN (WLAN)** - SonicWALL extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. All of the security features provided to VoIP devices attached to a wired network behind a SonicWALL are also provided to VoIP devices using a wireless network.

Note: SonicWALL's Secure Wireless Solution includes the network enablers to extend secure VoIP communications over wireless networks. Refer to the SonicWALL Secure Wireless Network Integrated Solutions Guide available on the SonicWALL Web site <<http://www.sonicwall.com>> for complete information.

- **Bandwidth Management (BWM) and Quality-of-Service (QoS)** - Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. BWM is integrated into SonicWALL Quality of Service (QoS) features to provide predictability that is vital for certain types of applications.
- **WAN redundancy and load balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary or backup WAN port. This secondary WAN port can be used in a

simple active/passive setup, where traffic is only routed through it if the primary WAN port is down or unavailable. Load balancing can be performed by splitting the routing of traffic based on destination.

- **High availability** - High availability is provided by SonicOS hardware failover, which ensures reliable, continuous connectivity in the event of a system failure.

VoIP Network Interoperability

- **Plug-and-protect support for VoIP devices** - With SonicOS, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected. Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a SonicWALL security appliance.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicOS to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the firewall can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.
- **Support for dynamic setup and tracking of media streams** - SonicOS tracks each VoIP call from the first signaling packet requesting a call setup, to the point where the call ends. Only based on the successful call progress are additional ports opened (for additional signaling and media exchange) between the calling and called party.
Media ports that are negotiated as part of the call setup are dynamically assigned by the firewall. Subsequent calls, even between the same parties, will use different ports, thwarting an attacker who may be monitoring specific ports. Required media ports are only opened when the call is fully connected, and are shut down upon call termination. Traffic that tries to use the ports outside of the call is dropped, providing added protection to the VoIP devices behind the firewall.
- **Validation of headers for all media packets** - SonicOS examines and monitors the headers within media packets to allow detection and discarding of out-of-sequence and retransmitted packets (beyond window). Also, by ensuring that a valid header exists, invalid media packets are detected and discarded. By tracking the media streams as well as the signaling, SonicWALL provides protection for the entire VoIP session.
- **Configurable inactivity timeouts for signaling and media** - In order to ensure that dropped VoIP connections do not stay open indefinitely, SonicOS monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle for more than the configured timeout are shut down to prevent potential security holes.
- **SonicOS allows the administrator to control incoming calls** - By requiring that all incoming calls are authorized and authenticated by the H.323 Gatekeeper or SIP Proxy, SonicOS can block unauthorized and spam calls. This allows the administrator to be sure that the VoIP network is being used only for those calls authorized by the company.
- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicOS offers extensive monitoring and troubleshooting tools:
 - ♦ Dynamic live reporting of active VoIP calls, indicating the caller and called parties, and bandwidth used.
 - ♦ Audit logs of all VoIP calls, indicating caller and called parties, call duration, and total bandwidth used. Logging of abnormal packets seen (such as a bad response) with details of the parties involved and condition seen.
 - ♦ Detailed syslog reports and ViewPoint reports for VoIP signaling and media streams. SonicWALL ViewPoint is a Web-based graphical reporting tool that provides detailed and comprehensive reports of your security and network activities based on syslog data streams received from the firewall. Reports can be generated about virtually any aspect of firewall activity, including individual user or group usage patterns and events on specific firewalls or groups of firewalls, types and times of attacks, resource consumption and constraints, etc.

Supported VoIP Protocols

SonicWALL security appliances support transformations for the following protocols.

H.323

SonicOS provides the following support for H.323:

- VoIP devices running all versions of H.323 (currently 1 through to 5) are supported
- Microsoft's LDAP-based Internet Locator Service (ILS)
- Discovery of the Gatekeeper by LAN H.323 terminals using multicast
- Stateful monitoring and processing of Gatekeeper registration, admission, and status (RAS) messages
- Support for H.323 terminals that use encryption for the media streams
- DHCP Option 150. The SonicWALL DHCP Server can be configured to return the address of a VoIP specific TFTP server to DHCP clients
- In addition to H.323 support, SonicOS supports VoIP devices using the following additional ITU standards:
 - ◆ T.120 for application sharing, electronic white-boarding, file exchange, and chat
 - ◆ H.239 to allow multiple channels for delivering audio, video and data
 - ◆ H.281 for Far End Camera Control (FECC)

SIP

SonicOS provides the following support for SIP:

- ◆ Base SIP standard (both RFC 2543 and RFC 3261)
- ◆ SIP INFO method (RFC 2976)
- ◆ Reliability of provisional responses in SIP (RFC 3262)
- ◆ SIP specific event notification (RFC 3265)
- ◆ SIP UPDATE method (RFC 3311)
- ◆ DHCP option for SIP servers (RFC 3361)
- ◆ SIP extension for instant messaging (RFC 3428)
- ◆ SIP REFER method (RFC 3515)
- ◆ Extension to SIP for symmetric response routing (RFC 3581)

SonicWALL VoIP Vendor Interoperability

The following is a partial list of devices from leading manufacturers with which SonicWALL VoIP interoperates.

H.323	SIP
Soft-Phones: Avaya Microsoft NetMeeting OpenPhone PolyCom SJLabs SJ Phone Zultys	Soft-Phones: Apple iChat Avaya Microsoft MSN Messenger Nortel Multimedia PC Client PingTel Instant Xpressa PolyCom Siemens SCS Client SJLabs SJPhone XTen X-Lite Ubiquity SIP User Agent Zultys
Telephones/VideoPhones: Avaya Cisco D-Link PolyCom Sony Zultys	Telephones/ATAs: Avaya Cisco Grandstream BudgetOne Mitel Packet8 ATA PingTel Xpressa PolyCom PolyCom Pulver Innovations WiSIP SoundPoint Zultys
Gatekeepers: Cisco OpenH323 Gatekeeper	SIP Proxies/Services: Cisco SIP Proxy Server Brekeke Software OnDo SIP Proxy Packet8 Siemens SCS SIP Proxy Vonage
Gateway: Cisco	

CODECS

SonicOS supports media streams from any CODEC - Media streams carry audio and video signals that have been processed by a hardware/software CODEC (COder/DECoder) within the VoIP device. CODECs use coding and compression techniques to reduce the amount of data required to represent audio/video signals. Some examples of CODECs are:

- H.264, H.263, and H.261 for video
- MPEG4, G.711, G.722, G.723, G.728, G.729 for audio

VoIP Protocols that SonicOS Does Not Perform Deep Packet Inspection on

SonicWALL security appliances do not currently support deep packet inspection for the following protocols; therefore, these protocols should only be used in non-NAT environments.

- Proprietary extensions to H.323 or SIP
- MGCP
- Megaco/H.248

- Cisco Skinny Client Control Protocol (SCCP)
- IP-QSIG
- Proprietary protocols (Mitel's MiNET, 3Com NBX, etc.)

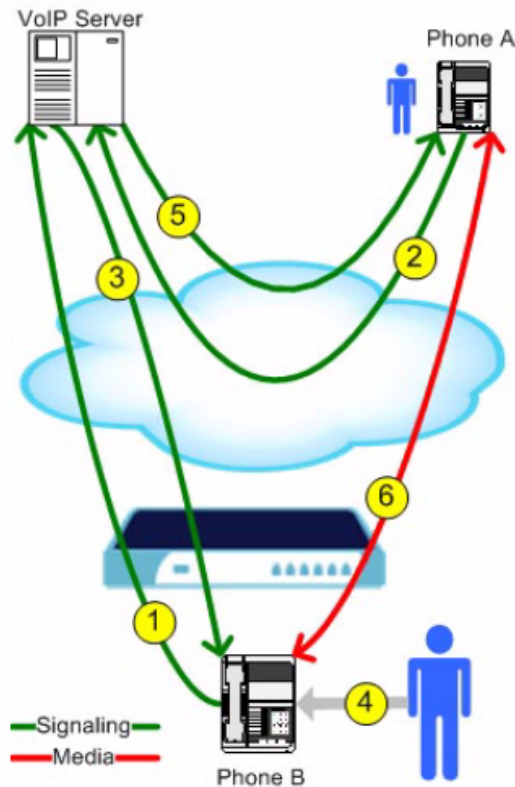
How SonicOS Handles VoIP Calls

SonicOS provides an efficient and secure solution for all VoIP call scenarios. The following are examples of how SonicOS handles VoIP call flows.

Incoming Calls

The following figure shows the sequence of events that occurs during an incoming call.

Figure 43.1 Incoming VoIP Call Flow



The following describes the sequence of events shown in Figure 42.1:

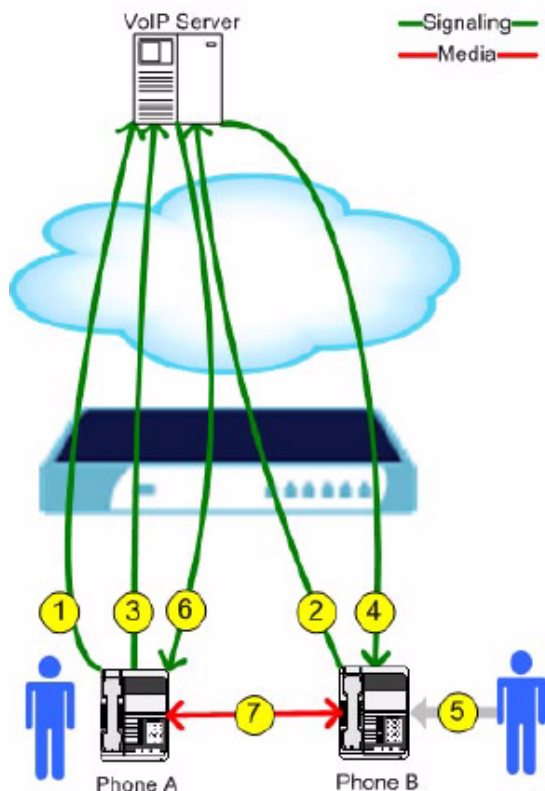
1. **Phone B registers with VoIP server** - The SonicWALL security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between phone B's private IP address and the firewall's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a firewall and has a private IP address—it associates phone B with the firewall's public IP address.
2. **Phone A initiates a call to phone B** - Phone A initiates a call to phone B using a phone number or alias. When sending this information to the VoIP server, it also provides details about the media types and formats it can support as well as the corresponding IP addresses and ports.
3. **VoIP Server validates the call request and sends the request to phone B**. The VoIP server sends the call request to the firewall's public IP address. When it reaches the firewall, SonicOS validates the source and content of the request. The firewall then determines phone B's private IP address.

4. **Phone B rings and is answered.** When phone B is answered, it returns information to the VoIP server for the media types and formats it supports as well as the corresponding IP addresses and ports. SonicOS translates this private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP server returns phone B media IP information to phone A.** Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.
6. **Phone A and phone B exchange audio/video/data through the VoIP server.** Using the internal database, SonicOS ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

Local Calls

The following figure shows the sequence of events that occurs during a local VoIP call.

Figure 43.2 Local VoIP Call Flow



The following describes the sequence of events shown in Figure 42.2:

1. **Phones A and B register with VoIP server** - The SonicWALL security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between the phones' private IP addresses and the firewall's public IP address. The VoIP server is unaware that the phones are behind a firewall. It associates the same IP address for both phones, but different port numbers.
2. **Phone A initiates a call to phone B by sending a request to the VoIP server** - Even though they are behind the same firewall, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. The firewall then determines phone B's private IP address.

4. **Phone B rings and is answered** - When phone B is answered, the firewall translate its private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP Server returns phone B media IP information to phone A** - Both the called and calling party information within the messages are translated by SonicOS back to the private addresses and ports for phone A and phone B.
6. **Phone A and phone B directly exchange audio/video/data** - The SonicWALL security appliance routes traffic directly between the two phones over the LAN. Directly connecting the two phones reduces the bandwidth requirements for transmitting data to the VoIP server and eliminates the need for the SonicWALL security appliance to perform address translation.

Configuring SonicWALL VoIP Features

Configuring the SonicWALL security appliance for VoIP deployments builds on your basic network configuration in the SonicWALL management interface. This chapter assumes the SonicWALL security appliance is configured for your network environment.

Supported Interfaces

VoIP devices are supported on the following SonicOS Zones:

- Trusted zones (LAN, VPN)
- Untrusted zones (WAN)
- Public zones (DMZ)
- Wireless zones (WLAN)

Configuration Tasks

- “General VoIP Configuration” on page 379
 - ♦ “Configuring Consistent Network Address Translation (NAT)” on page 379
 - ♦ “Configuring SIP Settings” on page 380
 - ♦ “Configuring H.323 Transformations” on page 381
- “Configuring BWM and QoS” on page 382
 - ♦ “Bandwidth Management” on page 382
 - ♦ “Quality of Service” on page 382
 - ♦ “Configuring Bandwidth on the WAN Interface” on page 383
 - ♦ “Configuring VoIP Access Rules” on page 383
 - ♦ “Using the Public Server Wizard” on page 386
- “Configuring VoIP Logging” on page 388

General VoIP Configuration

SonicOS includes the VoIP configuration settings on the **VoIP > Settings** page. This page is divided into three configuration settings sections: **General Settings**, **SIP Settings**, and **H.323 Settings**.

Configuring Consistent Network Address Translation (NAT)

Consistent NAT enhances standard NAT policy to provide greater compatibility with peer-to-peer applications that require a consistent IP address to connect to, such as VoIP. Consistent NAT uses an MD5 hashing method to consistently assign the same mapped public IP address and UDP Port pair to each internal private IP address and port pair.

For example, NAT could translate the private (LAN) IP address and port pairs, 192.116.168.10/50650 and 192.116.168.20/50655 into public (WAN) IP/port pairs as follows:

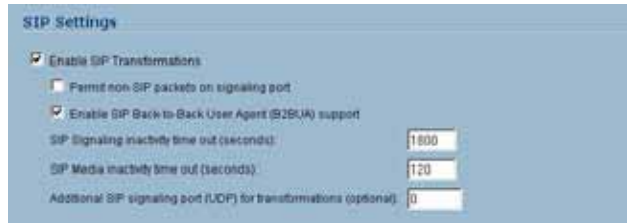
Private IP/Port	Translated Public IP/Port
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

With Consistent NAT enabled, all subsequent requests from either host 192.116.168.10 or 192.116.168.20 using the same ports illustrated in the previous result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

To enable Consistent NAT, select the **Enable Consistent NAT** setting and click **Apply**. This checkbox is disabled by default.

Note: *Enabling Consistent NAT causes a slight decrease in overall security, because of the increased predictability of the address and port pairs. Most UDP-based applications are compatible with traditional NAT. Therefore, do not enable Consistent NAT unless your network uses applications that require it.*

Configuring SIP Settings



By default, SIP clients use their private IP address in the SIP Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the SonicWALL security appliance and SIP clients are on the private (LAN) side behind the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

Selecting **Enable SIP Transformations** transforms SIP messages between LAN (trusted) and WAN/DMZ (untrusted). You need to check this setting when you want the SonicWALL security appliance to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the SonicWALL and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the SonicWALL. Selecting **Enable SIP Transformations** enables the SonicWALL to go through each SIP message and change the private IP address and assigned port. **Enable SIP Transformation** also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select **Enable SIP Transformations** to transform the SIP messages.

Tip: In general, you should check the **Enable SIP Transformations** box unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa.

Selecting **Permit non-SIP packets on signaling port** enables applications such as Apple iChat and MSN Messenger, which use the SIP signaling port for additional proprietary messages. Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic. This checkbox is disabled by default.

The **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be enabled when the SonicWALL security appliance can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN). This setting should only be enabled when the SIP Proxy Server is being used as a B2BUA.

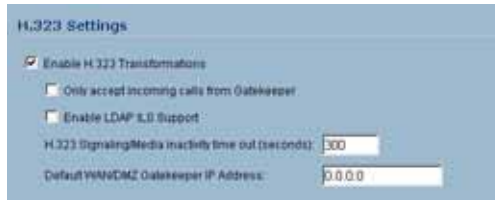
Tip: If there is not the possibility of the SonicWALL security appliance seeing both legs of voice calls (for example, when calls will only be made to and received from phones on the WAN), the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be disabled to avoid unnecessary CPU usage.

SIP Signaling inactivity time out (seconds) and **SIP Media inactivity time out (seconds)** define the amount of time a call can be idle (no traffic exchanged) before the SonicWALL security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **SIP Signaling inactivity time out** is 1800 seconds (30 minutes). The default time value for **SIP Media inactivity time out** is 120 seconds (2 minutes).

The **Additional SIP signaling port (UDP) for transformations** setting allows you to specify a non-standard UDP port used to carry SIP signaling traffic. Normally, SIP signaling traffic is carried on UDP port 5060. However, a number of commercial VOIP services use different ports, such as 1560. Using this setting, the security appliance performs SIP transformation on these non-standard ports.

Tip: Vonage's VoIP service uses UDP port 5061.

Configuring H.323 Transformations



Select **Enable H.323 Transformation** in the **H.323 Settings** section and click **Apply** to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWALL security appliance. The SonicWALL security appliance performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Disable the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the SonicWALL security appliance.

Select **Only accept incoming calls from Gatekeeper** to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper will refuse calls that fail authentication.

Select **Enable LDAP ILS Support** to enable Microsoft NetMeeting users to locate and connect to users for conferencing and collaboration over the Internet.

The **H.323 Signaling/Media inactivity time out (seconds)** field specifies the amount of time a call can be idle before the SonicWALL security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **H.323 Signaling/Media inactivity time out** is 300 seconds (5 minutes).

The **Default WAN/DMZ Gatekeeper IP Address** field has a default value of 0.0.0.0. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices to discover the Gatekeeper using the multicast address 224.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices will go through the configured multicast handling.

Configuring BWM and QoS

One of the greatest challenges for VoIP is ensuring high speech quality over an IP network. IP was designed primarily for asynchronous data traffic, which can tolerate delay. VoIP, however, is very sensitive to delay and packet loss. Managing access and prioritizing traffic are important requirements for ensuring high-quality, real-time VoIP communications.

SonicWALL's integrated Bandwidth Management (BWM) and Quality of Service (QoS) features provide the tools for managing the reliability and quality of your VoIP communications.

Bandwidth Management

SonicOS offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) management interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public Zones (such as LAN and DMZ) destined to Untrusted and Encrypted Zones (such as WAN and VPN). Inbound bandwidth management can be applied to traffic sourced from Untrusted and Encrypted Zones destined to Trusted and Public Zones.

Enabling bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.

Quality of Service

QoS encompasses a number of methods intended to provide predictable network behavior and performance. Network predictability is vital to VoIP and other mission critical applications. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

SonicOS includes QoS features that adds the ability to recognize, map, modify and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators.

Note: For more information on QoS and BWM, see [Chapter 42, Managing Quality of Service](#). Refer to the *Configuring QoS and BWM Feature Module* for complete BWM and QoS configuration instructions. Available on the SonicWALL Web site <www.sonicwall.com/support/documentation.html>

Configuring Bandwidth on the WAN Interface

BWM configurations begin by enabling BWM on the relevant WAN interface, and specifying the interface's available bandwidth in Kbps. This is performed from the **Network > Interfaces** page by selecting the **Configure** icon for the WAN interface, and navigating to the **Advanced** tab:



Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interface, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 (Gigabit). The bandwidth specified should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.

Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a **Bandwidth** tab will appear on Access Rules. See the following [“Configuring VoIP Access Rules”](#) section for more information.

To configure Bandwidth Management on the SonicWALL security appliance:

1. Select **Network > Interfaces**.
2. Click the Edit icon in the Configure column in the **WAN (X1)** line of the Interfaces table. The **Edit Interface** window is displayed.
3. Click the **Advanced** tab.
4. Check **Enable Egress** (Outbound) **Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Egress Bandwidth Management** field.
5. Check **Enable Ingress** (Inbound) **Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Ingress Bandwidth Management** field.
6. Click **OK**.

Configuring VoIP Access Rules

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. Additional network access rules can be defined to extend or override the default access rules.

If you are defining VoIP access for client to use a VoIP service provider from the WAN, you configure network access rules between source and destination interface or zones to enable clients behind the firewall to send and receive VoIP calls.

If your SIP Proxy or H.323 Gateway is located behind the firewall, you can use the SonicWALL **Public Server Wizard** to automatically configure access rules.

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

Configuring VoIP Access Rules

Note: You must select *Bandwidth Management* on the **Network > Interfaces** page for the **WAN** interface before you can configure bandwidth management for network access rules.

- To add access rules for VoIP traffic on the SonicWALL security appliance:
Go to the **Firewall > Access Rules** page, and under **View Style** click **All Rules**.
- Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.

The screenshot shows the 'Add Rule' dialog box in the SonicWALL management interface. The 'General' tab is active, and the 'Settings' section is visible. The 'Action' is set to 'Allow'. The 'From Zone' is 'LAN' and the 'To Zone' is 'WAN'. The 'Service' is 'H323 Call Signaling'. The 'Source' is 'LAN Interface IP' and the 'Destination' is 'WAN Interface IP'. The 'Users Allowed' is 'All' and the 'Schedule' is 'Always on'. The 'Comment' is 'VoIP'. The 'Enable Logging' checkbox is checked, and the 'Allow Fragmented Packets' checkbox is unchecked. The status bar at the bottom shows 'Ready'.

- In the **General** tab, select **Allow** from the **Action** list to permit traffic.
- Select the from and to zones from the **From Zone** and **To Zone** menus.
- Select the service or group of services affected by the access rule from the **Service** list.
 - For H.323, select one of the following or select **Create New Group** and add the following services to the group:
 - ◆ H.323 Call Signaling
 - ◆ H.323 Gatekeeper Discovery
 - ◆ H.323 Gatekeeper RAS
 - For SIP, select **SIP**

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

The screenshot shows a configuration window for an address object. The fields are as follows:

Name:	HR phones
Zone Assignment:	LAN
Type:	Range
Starting IP Address:	172.22.54.128
Ending IP Address:	172.22.54.136
Ready	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

7. If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, select **Range** in the **Type**: pulldown menu. Then enter the lowest and highest IP addresses in the range in the **Starting IP Address**: and **Ending IP Address** fields.
8. Select the destination of the traffic affected by the access rule from the **Destination** list. Selecting **Create New Network** displays the **Add Address Object** window.
9. From the **Users Allowed** menu, add the user or user group affected by the access rule.
10. Select a schedule from the **Schedule** menu if you want to allow VoIP access only during specified times. The default schedule is **Always on**. You can specify schedule objects on the **system > Schedules** page.
11. Enter any comments to help identify the access rule in the **Comments** field.
12. Click the **Bandwidth** tab.

The screenshot shows the 'Bandwidth Management' tab with the following settings:

<input checked="" type="checkbox"/> Enable Outbound Bandwidth Management ('allow' rules only)	
Guaranteed Bandwidth (%):	30.000
Maximum Bandwidth (%):	60.000
Bandwidth Priority:	0 highest
<input type="checkbox"/> Enable Inbound Bandwidth Management ('allow' rules only)	
Guaranteed Bandwidth (%):	0.000
Maximum Bandwidth (%):	0.000
Bandwidth Priority:	0 highest
Ready	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

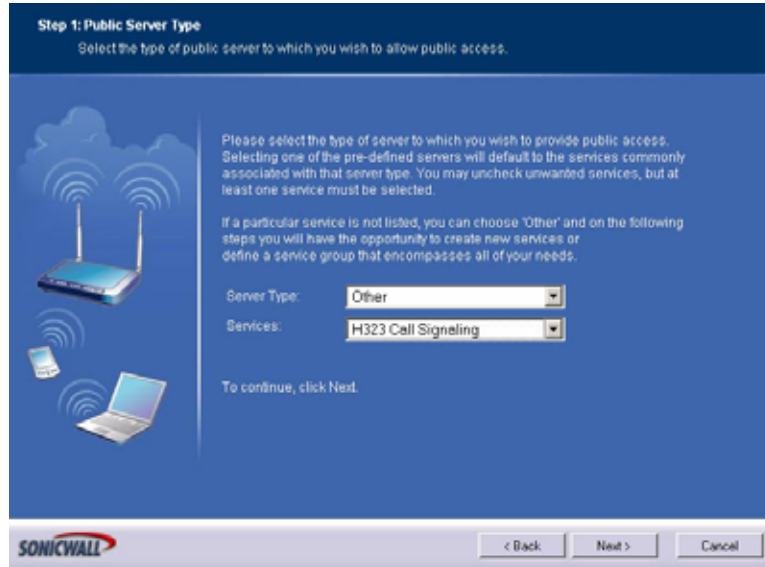
13. Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.
14. Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.
15. Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list. For higher VoIP call quality, ensure VoIP traffic receives HIGH priority.

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

Using the Public Server Wizard

The SonicWALL **Public Server Wizard** provides an easy method for configuring firewall access rules for a SIP Proxy or H.323 Gatekeeper running on your network behind the firewall. Using this wizard performs all the configuration settings you need for VoIP clients to access your VoIP servers.

1. Click **Wizards** on the SonicOS navigation bar.
2. Select **Public Server Wizard** and click **Next**.



3. Select **Other** from the **Server Type** list.

Select **SIP** from the **Services** menu if you're configuring network access for a SIP proxy server from the WAN.

Select **Gatekeeper RAS** if you're configuring network access for a H.323 Gatekeeper from the WAN.

Select **H.323 Call Signaling** for enabling Point-to-Point VoIP calls from the WAN to the LAN.

Click **Next**

Note: SonicWALL recommends **NOT** selecting **VoIP** from the **Services** menu. Selecting this option opens up more TCP/UDP ports than is required, potentially opening up unnecessary security vulnerabilities.

Step 2: Server Private Network Configuration
Enter the server's private (internal) address information.

Please enter a name to identify this server, and the server's private (internal) IP address. A Network object representing the private server will be created, as needed, using the name and IP address information you provide, and will be assigned to the appropriate Zone.

If you enter an IP address that matches an existing Network Object, that object will be renamed with the Server Name you specify here. You may also enter an optional comment to help further identify the server.

If you do not know this information, please contact the server's administrator or your network administrator before continuing.

Server Name:

Server Private IP Address:

Server Comment:

To continue, click Next.

SONICWALL < Back Next > Cancel

4. Enter the name of the server in the **Server Name** field.
5. Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to the zone where the server is located. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs. You can enter optional descriptive text in the Server Comment field.
6. Click **Next**.
7. Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.
8. Click **Next**.

Step 4: Public Server Configuration Summary
Review the settings for your public server.

Please review the settings below and click "Apply" to create the new objects listed below.

Server Address Objects

1. Create 'Huhcorp VoIP Server Private' assigned to LAN Zone for Host 10.1.2.3.
2. Reuse 'WAN Primary IP' address object assigned to WAN Zone for 10.0.93.31.

Server Service Group Object

1. Create 'Huhcorp VoIP Server Services' with H323 Call Signaling Service.

Server NAT Policies

1. Create Inbound Server NAT Policy to rewrite packets to original destination 'WAN Primary IP' to translated destination 'Huhcorp VoIP Server Private'.
2. Create Outbound Server NAT Policy to rewrite packets from 'Huhcorp VoIP Server Private' to translated source 'WAN Primary IP'.
3. Create Loopback NAT Policy to allow access from all internal zones to the server at public IP address 10.0.93.31.

Server Access Rules

1. **WAN > LAN** - Allow 'Any' to 'WAN Primary IP' for Service Group 'Huhcorp VoIP Server Services'. Similar rules will be created from all lower security zones to the LAN zone.

To apply these settings, click Apply. To continue, click Next.

SONICWALL < Back Apply > Cancel

9. The Summary page displays a summary of all the configuration you have performed in the wizard. It should show:
 - **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the LAN zone, the wizard binds the address object to the LAN zone.
 - **Server Service Group Object** - The wizard creates a service group object for the services used by the new server.
 - **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. The wizard also creates a Loopback NAT policy
 - **Server Access Rules** - The wizard creates an access policy allowing all traffic to the WAN Primary IP for the new service.
10. Click **Apply** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your SonicWALL.

✓ **Tip:** *The new IP address used to access the new server, both internally and externally, is displayed in the **URL** field of the **Congratulations** window.*

11. Click **Close** to close the wizard.

Configuring VoIP Logging

You can enable the logging of VoIP events in the SonicWALL security appliance log in the **Log > Categories** page. Log entries are displayed on the **Log > View** page. To enable logging:

1. Select **Log > Categories**.
2. Select **Expanded Categories** from the **View Style** menu in the **Log Categories** section.
3. Locate the **VoIP (VOIP H.323/RAS, H.323/H.225, H.323/H.245 activity)** entry in the table.
4. Select **Log** to enable the display of VoIP log events in on the **Log > View** page.
5. Select **Alerts** to enable the sending of alerts for the category.
6. Select **Syslog** to enable the capture of the log events into the SonicWALL security appliance Syslog.
7. Click **Apply**.

VoIP Deployment Scenarios

SonicWALL security appliances can be deployed VoIP devices can be deployed in a variety of network configurations. This section describes the following deployment scenarios:

- “Generic Deployment Scenario” on page 389
- “Deployment Scenario 1: Point-to-Point VoIP Service” on page 390
- “Deployment Scenario 2: Public VoIP Service” on page 391
- “Deployment Scenario 3: Trusted VoIP Service” on page 392

Generic Deployment Scenario

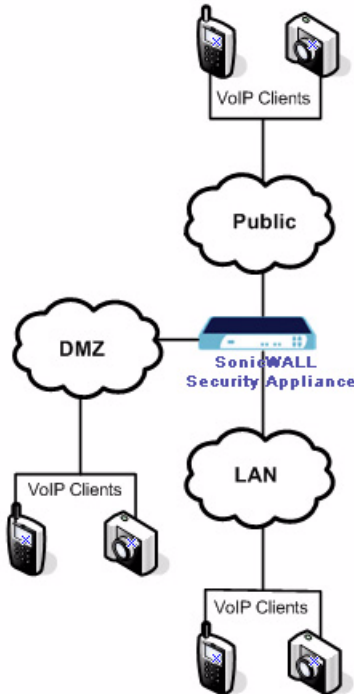
All three of the follow deployment scenarios begin with the following basic configuration procedure:

1. Enable bandwidth management on the WAN interface on **Network > Interfaces**.
2. Configure SIP or H.323 transformations and inactivity settings on **VoIP > Settings**.
3. Configure the DHCP Server on the **Network > DHCP Server** page with static private IP address assignments to VoIP clients.
4. Enable SonicWALL Intrusion Prevention Service to provided application-layer protection for VoIP communications on the **Security Services > Intrusion Prevention** page.
5. Connect VoIP Clients to network.

Deployment Scenario 1: Point-to-Point VoIP Service

The point-to-point VoIP service deployment is common for remote locations or small office environments that use a VoIP end point device connected to the network behind the firewall to receive calls directly from the WAN. The VoIP end point device on the Internet connects to VoIP client device on LAN behind the firewall using the SonicWALL security appliance's Public IP address. The following figure shows a point-to-point VoIP service topology

Figure 43.3 Point-to-Point VoIP Service Topology



This deployment does not require a VoIP server. The Public IP address of the SonicWALL security appliance is used as the main VoIP number for hosts on the network. This requires a static Public IP address or the use of a Dynamic DNS service to make the public address available to callers from the WAN. Incoming call requests are routed through the SonicWALL security appliance using NAT, DHCP Server, and network access rules.

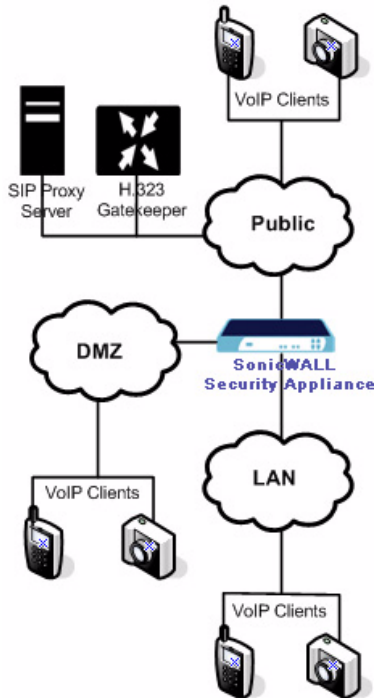
To make multiple devices behind the SonicWALL security appliance accessible from the public side, configure one-to-one NAT. If many-to-one NAT is configured, only one SIP and one NAT device will be accessible from the public side. See [“Chapter 18. Configuring NAT Policies”](#) for more information on NAT.

See the [“Using the Public Server Wizard”](#) section for information on configuring this deployment.

Deployment Scenario 2: Public VoIP Service

The Public VoIP Service deployment uses a VoIP service provider, which maintains the VoIP server (either a SIP Proxy Server or H.323 Gatekeeper). The SonicWALL security appliance public IP address provides the connection from the SIP Proxy Server or H.323 Gatekeeper operated by the VoIP service provider. The following figure shows a public VoIP service topology

Figure 43.4 Public VoIP Service Topology

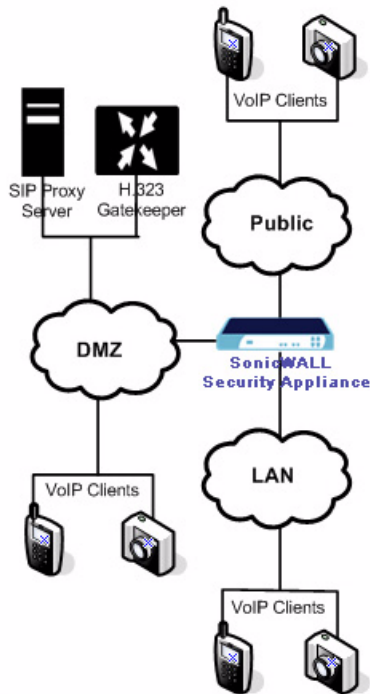


For VoIP clients that register with a server from the WAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration of clients is required. See the [“Using the Public Server Wizard”](#) section for information on configuring this deployment.

Deployment Scenario 3: Trusted VoIP Service

The organization deploys its own VoIP server on a DMZ or LAN to provide in-house VoIP services that are accessible to VoIP clients on the Internet or from local network users behind the security gateway. The following figure shows a trusted VoIP service topology

Figure 43.5 Trusted VoIP Service Topology



For VoIP clients that register with a server on the DMZ or LAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration on the VoIP clients is required.

To make a server on the LAN accessible to clients on the WAN:

1. Define a Host address object with the zone and IP address of the server.
2. Define a NAT policy, mapping traffic coming to the SonicWALL security appliance's public (WAN) IP address and VoIP service (SIP or H.323 Gatekeeper) to the server.
3. Define access rules allowing VoIP service to pass through the firewall.

See the "[Using the Public Server Wizard](#)" section for information on configuring this deployment.

PART

9

VPN

Configuring VPN Policies

VPN > Settings

The **VPN > Settings** page provides the SonicWALL features for configuring your VPN policies. You configure site-to-site VPN policies and GroupVPN policies from this page.

VPN > Settings VPN Policy Wizard... Apply Cancel ?

VPN Global Settings

Enable VPN
Unique Firewall Identifier: 0006B111A2C4

VPN Policies Items 1 to 4 (of 4)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN Group/VPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
2	WLAN Group/VPN			ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
3	Wireless#2 Group/VPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
4	SonicWALL Site-2-Site	64.41.140.167	10.50.0.1 - 10.50.127.255 10.50.128.1 - 10.50.159.255 10.0.0.1 - 10.0.255.255	ESP 3DES HMAC MD5 (IKE)	<input checked="" type="checkbox"/>	

Add Delete Delete All

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed
GroupVPN Policies: 3 Policies Defined, 1 Policies Enabled, 8 Maximum Policies Allowed

Currently Active VPN Tunnels Items 0 to 0 (of 0)

#	Name	Local	Remote	Gateway
No Entries				

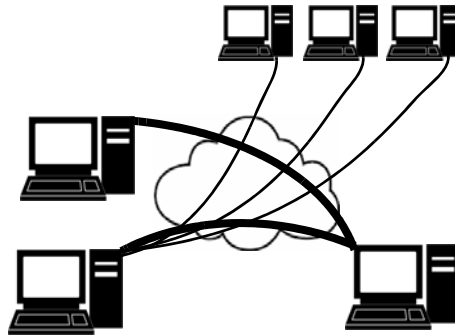
VPN Overview

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public internet. It provides authentication to ensure that the information is going to and from the correct parties. It provides security to protect the information from viewing or tampering en route.

Prior to the invention of Internet Protocol Security (IPsec) and Secure Socket Layer (SSL), secure connections between remote computers or networks required a dedicated line or satellite link. This was both inflexible and expensive.



A VPN creates a connection with similar reliability and security by establishing a secure tunnel through the internet. Because this tunnel is not a physical connection, it is more flexible--you can change it at any time to add more nodes, change the nodes, or remove it altogether. It is also far less costly, because it uses the existing internet infrastructure.



VPN Types

There are two main types of VPN in popular use today:

- **IPsec VPN:** IPsec is a set of protocols for security at the packet processing layer of network communication. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

SonicOS supports the creation and management of IPsec VPNs.

- **SSL VPN:** Secure Socket Layer (SSL) is a protocol for managing the security of a message transmission on the Internet, usually by HTTPS. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SSL VPN uses SSL to secure the VPN tunnel.

One advantage of SSL VPN is that SSL is built into most Web Browsers. No special VPN client software or hardware is required.



Note: SonicWALL makes SSL-VPN devices that you can use in concert with or independently of a SonicWALL UTM appliance running SonicOS. For information on SonicWALL SSL-VPN devices, see the SonicWALL Website: <http://www.sonicwall.com/products/ssl-vpn2000.html>

VPN Security

IPsec VPN traffic is secured in two stages:

- **Authentication:** The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
- **Encryption:** The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN) The exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel. SonicOS Enhanced supports two versions of IKE, version 1 and version 2.

IKE version 1

IKE version 1 uses a two phase process to secure the VPN tunnel.

- **IKE Phase 1** is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption/decryption keys, and establish the secure tunnel.
- **IKE Phase 2** is the negotiation phase. Once authenticated, the two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN and negotiate the number of secure associations (SAs) in the tunnel and their lifetime before requiring renegotiation of the encryption/decryption keys.

IKE Phase 1

In IKE v1, there are two modes of exchanging authentication information: Main Mode and Aggressive Mode.

Main Mode: The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:

- 1 The initiator sends a list of cryptographic algorithms the initiator supports.
- 2 The responder replies with a list of supported cryptographic algorithms.
- 3 The initiator send a public key (part of a Diffie-Helman public/private key pair) for the first mutually supported cryptographic algorithm.
- 4 The responder replies with the public key for the same cryptographic algorithm.
- 5 The initiator sends identity information (usually a certificate).
- 6 The responder replies with identity information.

Aggressive Mode: To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:

- 1 The initiator proposes a cryptographic algorithms to use and sends its public key.
- 2 The responder replies with a public key and identity proof.
- 3 The initiator sends an identification proof.

After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

IKE Phase 2

In IKE phase 2, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encryption Secured Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authentic and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following encryption methods for Traffic through the VPN.

- DES
- 3DES
- AES-128
- AES-192
- AES-256



Note: You can find more information about IKE v1 in the three specifications that define initially define IKE, RFC 2407, RFC 2408, and RFC 2409, available on the web at:

[<http://rfc.net/rfc2407.html>](http://rfc.net/rfc2407.html)

[<http://rfc.net/rfc2408.html>](http://rfc.net/rfc2408.html)

[<http://rfc.net/rfc2409.html>](http://rfc.net/rfc2409.html)

IKEv2

IKE version 2 is a new protocol for negotiating and establishing SAs. IKE v2 features improved security, a simplified architecture, and enhanced support for remote users. In addition, IKE v2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKE V2 greatly reduces the number of message exchanges needed to establish an SA over IKE v1 Main Mode, while being more secure and flexible than IKE v1 Aggressive Mode. This reduces the delays during re-keying. As VPNS grow to include more and more tunnels between multiple nodes or gateways, IKE v2 reduces the number of SAs required per tunnel, thus reducing required bandwidth and housekeeping overhead.

IKE v2 is not compatible with IKE v1. If using IKE v2, all nodes in the VPN must use IKE v2 to establish the tunnels.

SAs in IKE v2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.



Note: There is no restriction on nesting IKE v1 tunnels within an IKE v2 tunnel and visa-versa. For example, if you are connecting to a wireless device using WiFiSec, which uses an IKE v1 tunnel, you can then connect over the internet to a corporate network using a site-to-site VPN tunnel established with IKE v2.

Initialization and Authentication in IKE v2

IKE v2 initializes a VPN tunnel with a pair of message exchanges (two message/response pairs).

- Initialize communication: The first pair of messages (IKE_SA_INIT) negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange.
 - a Initiator sends a list of supported cryptographic algorithms, public keys, and a nonce.
 - b Responder sends the selected cryptographic algorithm, the public key, a nonce, and an authentication request.
- Authenticate: The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first CHILD_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.
 - a Initiator identity proof, such as a shared secret or a certificate, and a request to establish a child SA.
 - b Responder sends the matching identity proof and completes negotiation of a child SA.

Negotiating SAs in IKE v2

This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKE v1. It may be initiated by either end of the SA after the initial exchanges are completed.

All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

Either endpoint may initiate a CREATE_CHILD_SA exchange, so in this section the term “initiator” refers to the endpoint initiating this exchange.

- 1 Initiator sends a child SA offer and, if the data is to be encrypted, the encryption method and the public key.
- 2 Responder sends the accepted child SA offer and, if encryption information was included, a public key.



Note: You can find more information about IKE v2 in the specification, RFC 4306, available on the web at:

[<http://rfc.net/rfc4306.html>](http://rfc.net/rfc4306.html)

Configuring VPNs in SonicOS Enhanced

SonicWALL VPN, based on the industry-standard IPsec VPN implementation, provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWALL Global VPN Client or Global Security Client and SonicWALL GroupVPN on your SonicWALL. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to- network VPN connections.



Note: For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator's Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator's Guide**.

SonicWALL's GroupVPN provides automatic VPN policy provisioning for SonicWALL Global VPN Clients. The GroupVPN feature on the SonicWALL security appliance and the SonicWALL Global VPN Client (part of the Global security Client) dramatically streamline VPN deployment and management. Using SonicWALL's Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information automatically downloads from the SonicWALL

security appliance (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can easily and quickly create a site-to-site VPN policy or a GroupVPN policy for SonicWALL Global Security Clients using the **VPN Policy Wizard**. You can also configure GroupVPN or site-to-site VPN tunnels using the Management Interface. You can define up to four GroupVPN policies, one for each Zone. You can also create multiple site-to-site VPN. The maximum number of policies you can add depends on your SonicWALL model.

Planning Your VPN

Before creating or activating a VPN tunnel, gather the following information. You can print these pages and to use as a planning checklist:

GroupVPN Policy Planning Checklist

On the SonicWALL security appliance:

- **Authentication Method:**
 - IKE using Preshared Secret
 - IKE using 3rd Party Certificates.
- **Shared Secret** if using preshared secret.

- **Gateway Certificate** if using 3rd part certificates. This is a certificate file you have uploaded to your Sonicwall security appliance and plan to distribute to your VPN Clients.

- **Peer ID Type** if using 3rd party certificates: Choose
 - Distinguished Name
 - E-Mail ID
 - Domain name.
- **Peer ID Filter** if using 3rd party certificates.

- **IKE (Phase 1) Proposal:**
 - ♦ **DH Group:**
 - Group 1
 - Group 2
 - Group 5
 - ♦ **Encryption:**
 - DES
 - 3DES
 - AES-128
 - AES-256
 - ♦ **Authentication:**
 - MD5
 - SHA1
 - ♦ **Life Time** (seconds): _____ (default 28800)
- **Ipssec (Phase 2) Proposal**

- ♦ **Protocol:** (ESP only)
- ♦ **Encryption:**
 - DES
 - 3DES
 - AES-128
 - AES-192
 - AES-256
- ♦ **Authentication:**
 - MD5
 - SHA1
- ♦ **Enable Perfect Forward Secrecy**
- ♦ **DH Group** (if perfect forward secrecy is enabled)
 - Group 1
 - Group 2
 - Group 5
- ♦ **Life Time** (seconds): _____ (default 28800)
- **Enable Windows Networking (NetBIOS) Broadcast**
- **Enable Multicast**
- **Management via this SA:**
 - HTTP
 - HTTPS
- **Default Gateway:**
- **Enable OCSP Checking**
 - ♦ **OCSP Responder URL:** _____
- **Require Authentication of VPN Clients via XAUTH**
- **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

- **Allow Unauthenticated VPN Client Access** (the network or subnet you will allow to have access to this VPN without authentication if XAUTH is not selected):

- **Cache XAUTH User Name and Password on Client** (will the client be able to store the user name and password):
 - Never
 - Single Session
 - Always
- **Virtual Adapter settings:**
 - None
 - DHCP Lease
 - DHCP Lease or Manual Configuration
- **Allow Connections to:**
 - This Gateway Only
 - All Secured Gateways
 - Split Tunnels

- Set Default Route as this Gateway
- Require Global Security Client for this Connection
- **Use Default Key for Simple Client Provisioning**
(this allows easier client setup, but is less secure)

On the client

- IP address or Web address of VPN Gateway
- VPN Client:
 - GVC or GSC
 - GSC only (Require Global Security Client checked on security appliance)
- Shared secret, if selected on security appliance:

- Certificate, if selected on security appliance:

- User's user name and password if XAUTH is required on the security appliance.

Site-to-Site VPN Planning Checklist

On the Initiator

Typically, the request for an IKE VPN SA is made from the remote site.

- **Authentication Method:**
 - Manual Key
 - IKE using Preshared Secret
 - IKE using 3rd Party Certificates (not used with IKEv2)
- **Name of this VPN:** _____
- **IPsec Primary Gateway Name or Address:**

- **IPsec Secondary Gateway Name or Address:**

(not used with manual key, not used with IKEv2)
- **IKE Authentication for IKE using Preshared Secret:**
 - ♦ **Shared Secret:** _____
 - ♦ **Local IKE ID:**
 - IP Address _____
 - Domain Name _____
 - Email Address _____
 - SonicWALL Identifier _____
 - ♦ **Peer IKE ID:**
 - IP Address _____
 - Domain Name _____
 - Email Address _____
 - SonicWALL Identifier _____
- **IKE Authentication for IKE using 3rd Party Certificate (not used with IKEv2):**
 - ♦ **Local Certificate:** _____
 - ♦ **Peer IKE ID Type:** _____

- Distinguished name
- E-Mail ID
- Domain name
- ◆ Peer IKE ID: _____
- Local Networks
 - Choose local network from list (select an address object):

 - Local network obtains IP addresses using DHCP through this VPN Tunnel
(not used with IKEv2)
 - Any address
- Destination Networks
 - Use this VPN Tunnel as default route for all Internet traffic
 - Destination network obtains IP addresses using DHCP through this VPN Tunnel
 - Choose destination network from list (select an address object):

- IKE (Phase 1) Proposal:
 - ◆ Exchange:
 - Main Mode
 - Aggressive Mode
 - IKEv2 Mode
 - ◆ DH Group:
 - Group 1
 - Group 2
 - Group 5
 - ◆ Encryption:
 - DES
 - 3DES
 - AES-128
 - AES-192
 - AES-256
 - ◆ Authentication:
 - MD5
 - SHA1
 - ◆ Life Time (seconds): _____ (default 28800)
- Ipsec (Phase 2) Proposal
 - ◆ Protocol:
 - ESP
 - AH
 - ◆ Encryption:
 - DES
 - 3DES
 - AES-128
 - AES-192
 - AES-256

- ◆ **Authentication:**
 - MD5
 - SHA1
- ◆ **Enable Perfect Forward Secrecy**
- ◆ **DH Group** (if perfect forward secrecy is enabled)
 - Group 1
 - Group 2
 - Group 5
- ◆ **Life Time** (seconds): _____ (default 28800)
- **Enable Keep Alive**
- **Suppress automatic Access Rules creation for VPN Policy**
- **Require authentication of VPN clients by XAUTH** (not with IKEv2)
 - ◆ **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

- **Enable Windows Networking (NetBIOS) Broadcast**
- **Enable Multicast**
- **Apply NAT Policies**
 - ◆ **Translated Local Network:** _____
 - ◆ **Translated Remote Network:** _____
- **Enable OCSP Checking** (IKE with 3rd Party Certificate only)
 - ◆ **OCSP Responder URL:** (IKE with 3rd Party Certificate only)

- **Management via this SA:**
 - HTTP
 - HTTPS
- **User login via this SA:**
 - HTTP
 - HTTPS
- **Default LAN Gateway (optional):**
- **VPN Policy bound to:**
 - Interface X0, Interface X1, Interface X2, Interface X3, Interface X4
 - Interface X5, Interface X6, Interface X7, Interface X8, Interface X9
 - Zone WAN
- **Do not send trigger packet during IKE SA negotiation** (IKEv2 only)

On the Responder

The settings on the responder must be the same as on the initiator except:

- **Name** of this VPN: _____
- **IPsec Primary Gateway Name or Address:** not required on the responder
- **IPsec Secondary Gateway Name or Address:** not required on the responder
- **IKE Authentication for IKE using Preshared Secret:**
 - ◆ **Local IKE ID:** (must match Peer IKE ID on initiator)
 - IP Address** _____

- Domain Name _____
- Email Address _____
- SonicWALL Identifier _____
- ◆ Peer IKE ID: (must match Local IKE ID on initiator)
 - IP Address _____
 - Domain Name _____
 - Email Address _____
 - SonicWALL Identifier _____
- IKE Authentication for IKE using 3rd Party Certificate (not used with IKEv2):
 - ◆ Local Certificate: _____
 - ◆ Peer IKE ID Type:
 - Distinguished name
 - E-Mail ID
 - Domain name
 - ◆ Peer IKE ID: _____
- Local Networks (must match Destination Networks on initiator)
 - Choose local network from list (select an address object):

 - Local network obtains IP addresses using DHCP through this VPN Tunnel
(not used with IKEv2)
 - Any address
- Destination Networks (must match Local Networks on initiator)
 - Use this VPN Tunnel as default route for all Internet traffic
 - Destination network obtains IP addresses using DHCP through this VPN Tunnel
 - Choose destination network from list (select an address object):

- Apply NAT Policies
 - ◆ Translated Local Network: (must match Translated Remote Network on initiator)

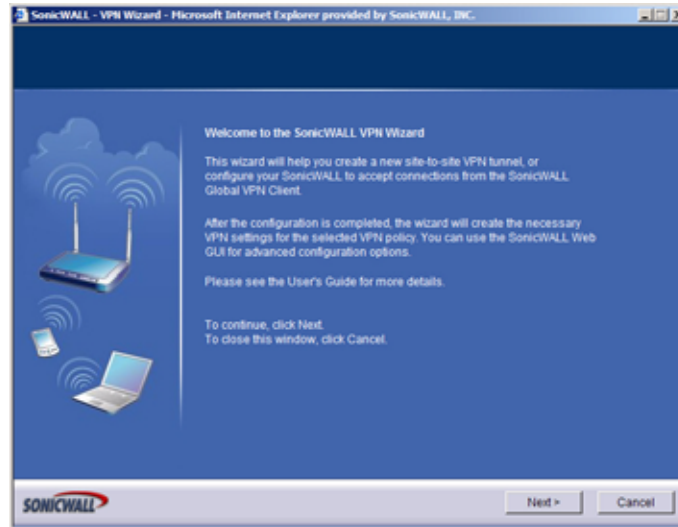
 - ◆ Translated Remote Network (must match Translated Local Network on initiator)

VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN or site-to-site VPN policies on the SonicWALL security appliance. After completing the configuration, the wizard creates the necessary VPN settings for the selected policy. You can use the SonicWALL Management Interface for optional advanced configuration options.



Note: For step-by-step instructions on using the VPN Policy Wizard, see Chapter 50 Configuring VPNs with the VPN Policy Wizard.



VPN Global Settings

The **Global VPN Settings** section of the **VPN > Settings** page displays the following information:



- **Enable VPN** must be selected to allow VPN policies through the SonicWALL security policies.
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWALL. You can change the Identifier, and use it for configuring VPN tunnels.

VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
2	WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
3	Wireless#2 GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
4	SonicWALL Site-2-Site	188.55.155.155	10.10.0.1 - 10.10.127.255 10.10.128.1 - 10.10.159.255 10.1.0.1 - 10.1.255.255	ESP 3DES HMAC MD5 (IKE)	<input checked="" type="checkbox"/>	

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed
 GroupVPN Policies: 3 Policies Defined, 1 Policies Enabled, 8 Maximum Policies Allowed

- **Name:** Displays the default name or user-defined VPN policy name.
- **Gateway:** Displays the IP address of the remote SonicWALL. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations:** Displays the IP addresses of the destination networks.
- **Crypto Suite:** Displays the type of encryption used for the VPN policy.
- **Enable:** Selecting the check box enables the VPN Policy. Clearing the check box disables it.
- **Configure:** Clicking the Edit icon allows you to edit the VPN policy. Clicking the Trashcan allows you to delete the VPN policy. The predefined GroupVPN policies cannot be deleted, so the Trashcan icons are dimmed. GroupVPN policies also have a Disk icon for exporting the VPN policy configuration as a file for local installation by SonicWALL Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table. You can define up to 4 GroupVPN policies, one for each Zone. These GroupVPN policies are listed by default in the VPN Policies table as **WAN GroupVPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on the edit icon in the Configure column for the GroupVPN displays the **VPN Policy** window for configuring the GroupVPN policy.

Below the VPN Policies table are the following buttons:

- **Add** - Accesses the **VPN Policy** window to configure site-to-site VPN policies.
- **Delete** - Deletes the selected (checked box before the VPN policy name in the **Name** column. You cannot delete the GroupVPN policies.
- **Delete All** - Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

Navigating and Sorting the VPN Policies Entries

The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **VPN Policies** table by using the navigation control bar located at the top right of the **VPN Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.


Currently Active VPN Tunnels

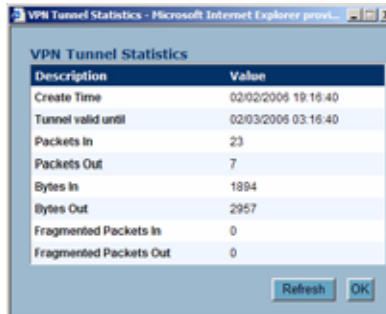
A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the peer gateway IP address.

#	Name	Local	Remote	Gateway
1	WLAN GroupVPN	0.0.0.1 - 255.255.255.255	fcheek	172.16.31.233

Click the **Renegotiate** button to force the VPN Client to renegotiate the VPN tunnel.

Viewing VPN Tunnel Statistics

In the Currently Active VPN Tunnels table, click on the Statistics icon  in the row for a tunnel to view the statistics on that tunnel. The VPN Tunnel Statistics icon displays:



Description	Value
Create Time	02/02/2006 19:16:40
Tunnel valid until	02/03/2006 03:16:40
Packets In	23
Packets Out	7
Bytes In	1894
Bytes Out	2957
Fragmented Packets In	0
Fragmented Packets Out	0

- **Create Time:** The date and time the tunnel came into existence.
- **Tunnel valid until:** The time when the tunnel expires and is force to renegotiate.
- **Packets In:** The number of packets received from this tunnel.
- **Packets Out:** The number of packets sent out from this tunnel.
- **Bytes In:** The number of bytes received from this tunnel.
- **Bytes Out:** The number of bytes sent out from this tunnel.
- **Fragmented Packets In:** The number of fragmented packets received from this tunnel.
- **Fragmented Packets Out:** The number of fragmented packets sent out from this tunnel.

Configuring GroupVPN Policies

SonicWALL **GroupVPN** facilitates the set up and deployment of multiple SonicWALL Global VPN Clients by the SonicWALL security appliance administrator. **GroupVPN** is only available for SonicWALL Global VPN Clients and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.



Cross Reference: For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator's Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator's Guide**.

The default GroupVPN configuration allows you to support SonicWALL Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

SonicWALL supports four GroupVPN policies. You can create GroupVPN policies for the DMZ, LAN, WAN, and WLAN zones. These GroupVPN policies are listed in the VPN policies tables as **WAN Group VPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. For these GroupVPN policies, you can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPsec Keying Mode.



Tip: You can easily create GroupVPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Chapter 51 Configuring VPNs with the SonicWALL VPN Policy Wizard.

The following instructions explain configuring GroupVPN using the SonicWALL Management Interface.



Note: See the **GroupVPN Setup in SonicOS Enhanced** technote on the SonicWALL documentation Web site <http://www.sonicwall.com> for more GroupVPN configuration information.

Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

To configure the WAN GroupVPN, follow these steps:

- 1 Click the Edit icon for the **WAN GroupVPN** entry. The **VPN Policy** window is displayed.

The screenshot shows the 'VPN Policy' window in Microsoft Internet Explorer. The 'General' tab is selected. Under the 'Security Policy' section, the following fields are visible:

- Authentication Method: IKE using Preshared Secret
- Name: WAN GroupVPN
- Shared Secret: BEE817419E703FEE

Buttons for 'OK', 'Cancel', and 'Help' are at the bottom right. A 'Ready' status bar is at the bottom left.

- 2 In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**. A Shared Secret is automatically generated by the SonicWALL security appliance in the **Shared Secret** field, or you can generate your own shared secret. **Shared Secrets** must be minimum of four characters. You cannot change the name of any GroupVPN policy.
- 3 Click the **Proposals** tab to continue the configuration process.

The screenshot shows the 'VPN Policy' window in Microsoft Internet Explorer. The 'Proposals' tab is selected. The configuration is split into two sections:

IKE (Phase 1) Proposal

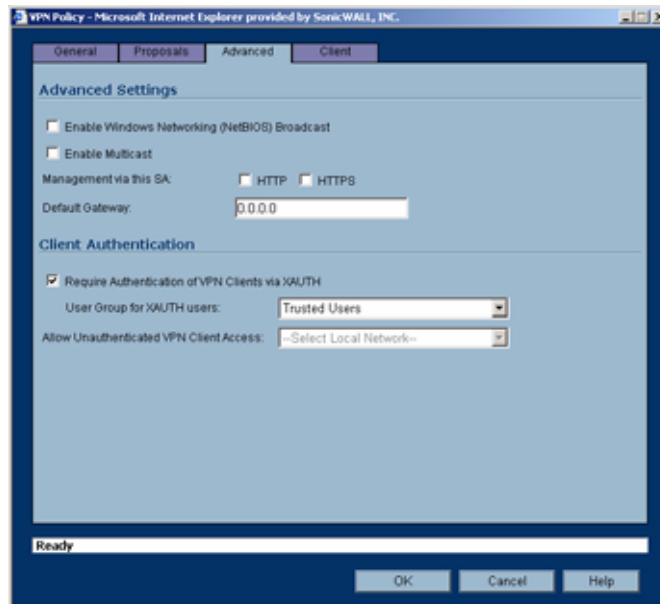
- DH Group: Group 2
- Encryption: 3DES
- Authentication: SHA1
- Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

- Protocol: ESP
- Encryption: 3DES
- Authentication: SHA1
- Enable Perfect Forward Secrecy
- DH Group: Group 1
- Life Time (seconds): 28800

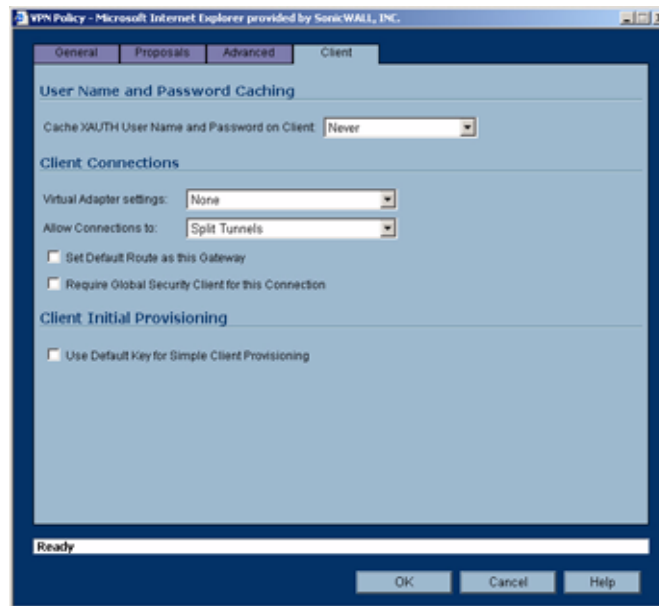
Buttons for 'OK', 'Cancel', and 'Help' are at the bottom right. A 'Ready' status bar is at the bottom left.

- 4 In the **IKE (Phase 1) Proposal** section, use the following settings:
 - ♦ Select the DH Group from the **DH Group** menu.
 - ♦ Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
 - ♦ Select the desired authentication method from the **Authentication** menu.
 - ♦ Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.
- 5 In the **IPsec (Phase 2) Proposal** section, select the following settings:
 - ♦ Select the desired protocol from the **Protocol** menu
 - ♦ Select **3DES, AES-128, or AES-256** from the **Encryption** menu
 - ♦ Select the desired authentication method from the **Authentication** menu
 - ♦ Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.
 - ♦ Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.
- 6 Click the **Advanced** tab.



- 7 Select any of the following optional settings you want to apply to your GroupVPN policy:
 - ♦ **Enable Windows Networking (NetBIOS) broadcast** - allows access to remote network resources by browsing the Windows® Network Neighborhood.
 - ♦ **Enable Multicast** - enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
 - ♦ **Management via this SA:** - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
 - ♦ **Default Gateway** - allows the network administrator to specify the IP address of the default network route for incoming IPsec packets for this VPN policy. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL security appliance. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the SonicWALL looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

- ◆ **Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. The **Trusted users** group is selected by default. You can select another user group or **Everyone** from **User Group for XAUTH users**.
 - ◆ **Allow Unauthenticated VPN Client Access** - allows you to enable unauthenticated VPN client access. If you uncheck **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from menu of predefined options, or select **Create new address object** or **Create new address group** to create a new one.
- 8 Click the **Client** tab, select any of the following settings you want to apply to your GroupVPN policy.



- ◆ **Cache XAUTH User Name and Password on Client** - allows the Global VPN Client to cache the user name and password.
 - **Never** - Global VPN Client is not allowed to cache the username and password. The user will be prompted for a username and password when the connection is enabled, and also every time there is an IKE Phase 1 rekey.
 - **Single Session** - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.
 - **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- ◆ **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it's necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
 - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
 - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
 - **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP

messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

- ◆ **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
 - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
 - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
 - **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- ◆ **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting.
- ◆ **Require Global Security Client for this Connection** - only allows a VPN connection from a remote computer running the SonicWALL Global Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.



Note: For more information on the SonicWALL Global Security Client, see the SonicWALL Global Security Client Administrator's Guide.

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

9 Click **OK**.

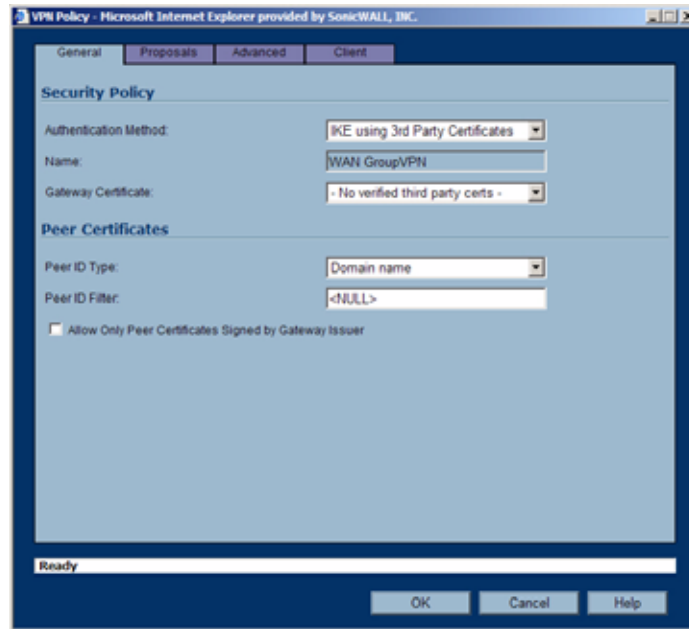
Configuring GroupVPN with IKE using 3rd Party Certificates

To configure GroupVPN with IKE using 3rd Party Certificates, follow these steps:



Warning: Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the SonicWALL.

- 1 In the **VPN > Settings** page click the edit icon under **Configure**. The **VPN Policy** window is displayed.



- 2 In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **Authentication Method** menu. The VPN policy name is **GroupVPN** by default and cannot be changed.
- 3 Select a certificate for the SonicWALL from the **Gateway Certificate** menu.
- 4 Select one of the following Peer ID types from the **Peer ID Type** menu:
 - ♦ **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters * (for more than 1 character) and ? (for a single character). For example, the string *@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string *sv.us.sonicwall.com when **Domain Name** is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.
 - ♦ **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=). Up to three organizational units can be specified. The usage is c=*;o=*;ou=*;ou=*;ou=*;cn=*. The final entry does not need to contain a semi-colon. You must enter at least one entry, i.e. c=us.
- 5 Enter the Peer ID filter in the **Peer ID Filter** field.
- 6 Check **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.
- 7 Click on the **Proposals** tab.
- 8 In the **IKE (Phase 1) Proposal** section, select the following settings:
 - ♦ Select the DH Group from the **DH Group** menu.
 - ♦ Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
 - ♦ Select the desired authentication method from the **Authentication** menu.

- ♦ Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.
- 9 In the **IPsec (Phase 2) Proposal** section, select the following settings:
- ♦ Select the desired protocol from the **Protocol** menu
 - ♦ Select **3DES, AES-128, or AES-256** from the **Encryption** menu
 - ♦ Select the desired authentication method from the **Authentication** menu
 - ♦ Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.
 - ♦ Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.
- 10 Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:
- ♦ **Enable Windows Networking (NetBIOS) broadcast** - allows access to remote network resources by browsing the Windows Network Neighborhood.
 - ♦ **Enable Multicast** - enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
 - ♦ **Management via this SA** - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
 - ♦ **Default Gateway** - used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
 - ♦ **Enable OCSP Checking** and **OCSP Responder URL** - enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See the “[Using OCSP with SonicWALL Security Appliances](#)” section in [Chapter 44, Configuring VPN Policies](#).
 - ♦ **Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
 - ♦ **User group for XAUTH users** - allows you to select a defined user group for authentication.
 - ♦ **All Unauthenticated VPN Client Access** - allows you to specify network segments for unauthenticated Global VPN Client access.
- 11 Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:
- ♦ **Cache XAUTH User Name and Password** - allows the Global VPN Client to cache the user name and password. Select from:
 - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
 - **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
 - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.

- ◆ **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it's necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
 - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
 - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
 - **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.
- ◆ **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
 - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
 - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
 - **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- ◆ **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
- ◆ **Require Global Security Client for this Connection** - only allows a VPN connection from a remote computer running the SonicWALL Global Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.



Note: For more information on the SonicWALL Global Security Client and Distributed Security Client, see the SonicWALL Global Security Client Administrator's Guide.

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

12 Click **OK**.

Exporting a VPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:



Warning: The GroupVPN SA must be enabled on the SonicWALL to export a configuration file.

- 1 Click the **Disk** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Policy** window appears.



- 2 **rcf format is required for SonicWALL Global VPN Clients** is selected by default. Files saved in the rcf format can be password encrypted. The SonicWALL provides a default file name for the configuration file, which you can change.
- 3 Click **Yes**. The **VPN Policy Export** window appears.
- 4 Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.
- 5 Click **Submit**. If you did not enter a password, a message appears confirming your choice.
- 6 Click **OK**. You can change the configuration file before saving.
- 7 Save the file.
- 8 Click **Close**.

The file can be saved to a floppy disk or sent electronically to remote users to configure their Global VPN Clients.

Site-to-Site VPN Configurations

When designing VPN connections, be sure to document all pertinent IP Addressing information and create a network diagram to use as a reference. A sample planning sheet is provided on the next page. The SonicWALL must have a routable WAN IP Address whether it is dynamic or static. In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWALL is configured to connect to another SonicWALL via a VPN tunnel. Or, a SonicWALL is configured to connect via IPsec to another manufacturer's firewall.
- **Hub and Spoke Design** - All SonicWALL VPN gateways are configured to connect to a central SonicWALL (hub), such as a corporate SonicWALL. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWALL.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

See “[Planning Your VPN](#)” on page 400 for a planning sheet to help you set up your VPN.

Creating Site-to-Site VPN Policies

- ✓ **Tip:** You can easily create site-to-site VPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Chapter 51 Configuring VPNs with the SonicWALL VPN Policy Wizard.

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPsec Keying mode VPN policies:

- IKE using Preshared Key
- Manual Key
- IKE using 3rd Party Certificates

- ✓ **Tip:** Use the *VPN Planning Sheet for Site-to-Site VPN Policies* to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.

- ➔ **Cross Reference:** For configuring VPN policies between SonicWALL security appliances running SonicOS Enhanced and SonicWALL security appliances running SonicWALL Firmware version 6.5 (or higher), see the technote: *Creating IKE IPsec VPN Tunnels between SonicWALL Firmware 6.5 and SonicOS Enhanced*, available at the SonicWALL documentation Web site <http://www.sonicwall.com/services/documentation.html>.

Configuring a VPN Policy with IKE using Preshared Secret

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

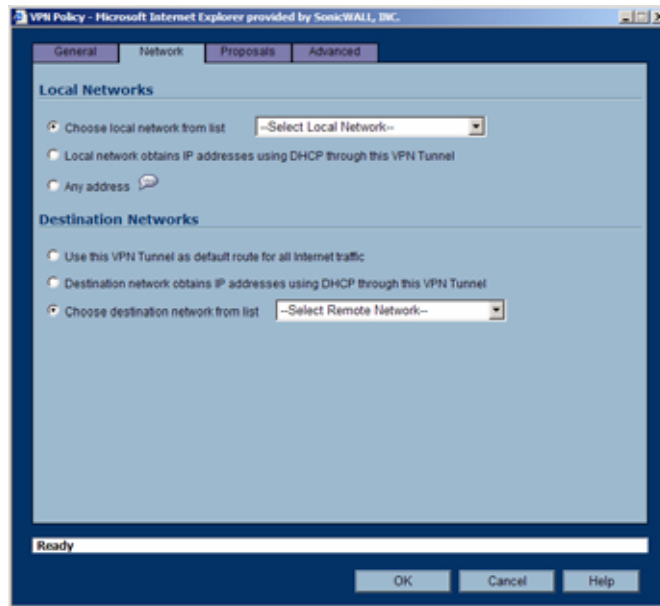
- 1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.

- 2 In the **General** tab, select **IKE using Preshared Secret** from the **Authentication Method** menu.
- 3 Enter a name for the policy in the **Name** field.

- 4 Enter the host name or IP address of the remote connection in the IPsec **Primary Gateway Name or Address** field.
- 5 If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.
- 6 Enter a Shared Secret password to be used to setup the Security Association the **Shared Secret** and **Confirm Shared Secret** fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

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

- 7 Click the **Network** tab.

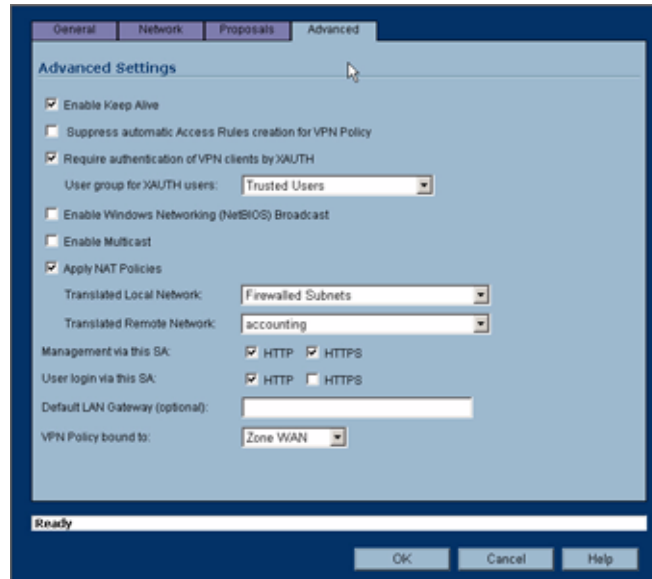


- 8 Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected.
- 9 Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

10 Click **Proposals**.

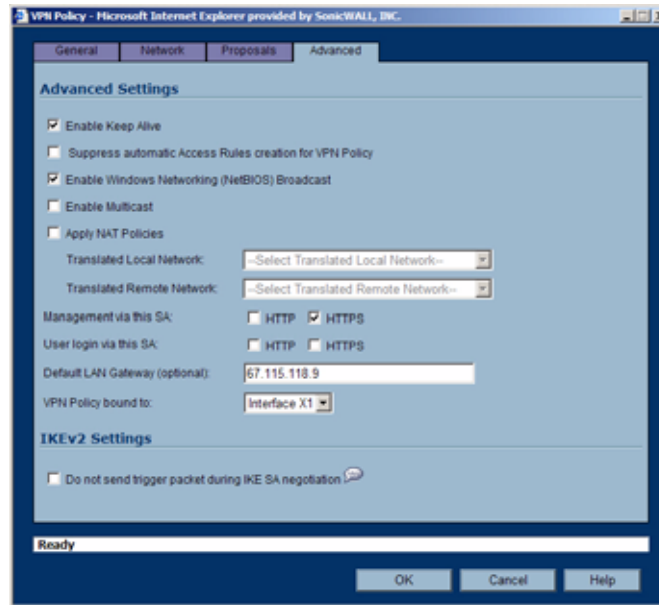
- 11 Under **IKE (Phase 1) Proposal**, select either **Main Mode**, **Aggressive Mode**, or **IKEv2** from the **Exchange** menu. **Aggressive Mode** is generally used when WAN addressing is dynamically assigned. **IKEv2** causes all the negotiation to happen via IKE v2 protocols, rather than using IKE Phase 1 and Phase 2. If you use IKE v2, both ends of the VPN tunnel must use IKE v2.
- 12 Under **IKE (Phase 1) Proposal**, the default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match. You can also choose **AES-128**, **AES-192**, or **AES-256** from the **Authentication** menu instead of 3DES for enhanced authentication security.
- 13 Under **IPsec (Phase 2) Proposal**, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, **DH Group**, and **Lifetime** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.
- 14 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

- ◆ If you selected **Main Mode** or **Aggressive Mode** in the **Proposals** tab:



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or Zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

- ◆ If you selected **IKEv2** in the **Proposals** tab:



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- Select **Suppress automatic Access Rules creation for VPN Policy** to turn off the automatic access rules created between the LAN and VPN zones for this VPN policy.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- Enter the **Default LAN Gateway** if you have more than one gateway and you want this one always to be used first.
- Select an interface or Zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.
- Under **IKEv2 Settings** (visible only if you selected **IKEv2** for **Exchange** on the **Proposals** tab), The **Do not send trigger packet during IKE SA negotiation** checkbox is cleared by default and should only be selected when required for interoperability.

The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations

support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

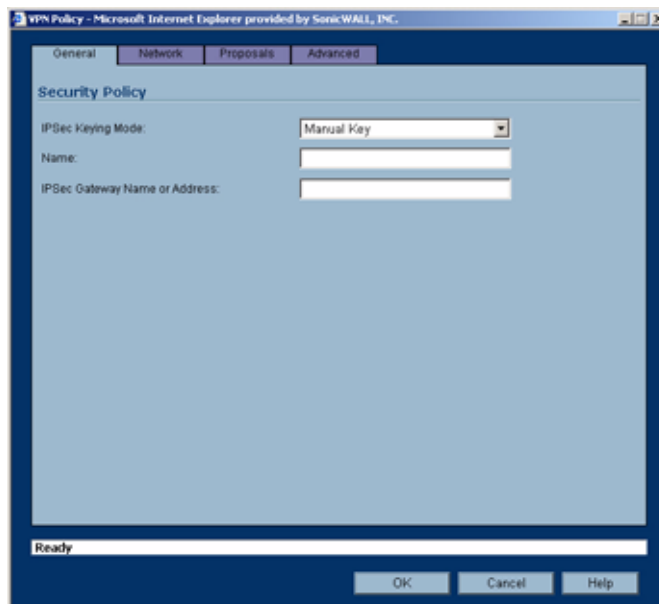
15 Click **OK**.

Configuring a VPN Policy using Manual Key

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

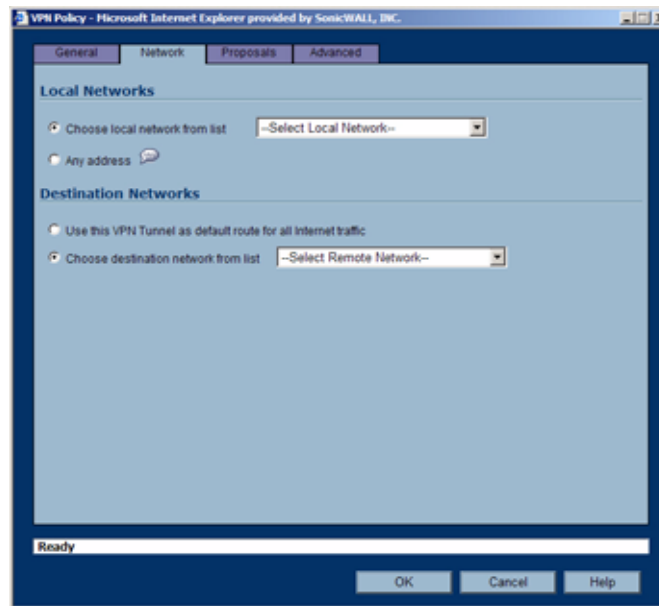
Configuring the Local SonicWALL Security Appliance

- 1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
- 2 In the **General** tab of the **VPN Policy** window, select **Manual Key** from the **IPsec Keying Mode** menu. The **VPN Policy** window displays the manual key options.



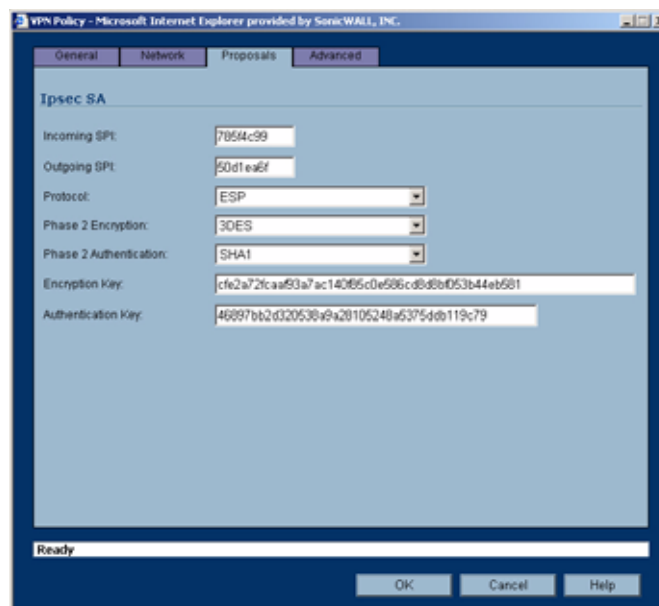
- 3 Enter a name for the policy in the **Name** field.
- 4 Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.

5 Click the **Network** tab.



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

7 Click on the **Proposals** tab.



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



Warning: Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

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



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

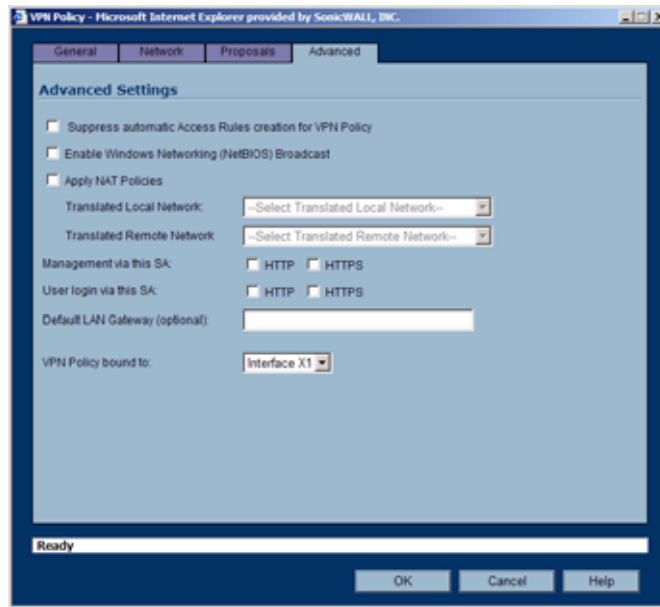
10 Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the SonicWALL.

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



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

12 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.



- ♦ The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
 - ♦ Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
 - ♦ Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
 - ♦ To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**.
 - ♦ Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
 - ♦ If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
 - ♦ Select an interface from the **VPN Policy bound to** menu.
- 13 Click **OK**.
- 14 Click **Apply** on the **VPN > Settings** page to update the VPN Policies.

Configuring the Remote SonicWALL Security Appliance

- 1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
- 2 In the **General** tab, select **Manual Key** from the **IPsec Keying Mode** menu.
- 3 Enter a name for the SA in the **Name** field.
- 4 Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.
- 5 Click the **Network** tab.
- 6 Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.
- 7 Click the **Proposals** tab.
- 8 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcdef) and can range from 3 to 8 characters in length.



Warning: *Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.*

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



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

- 10 Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the remote SonicWALL.
- 11 Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWALL settings.



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

- 12 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:
 - ♦ The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
 - ♦ Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
 - ♦ Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.



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

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

- ◆ If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- ◆ Select an interface from the **VPN Policy bound to** menu.

13 Click **OK**.

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



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

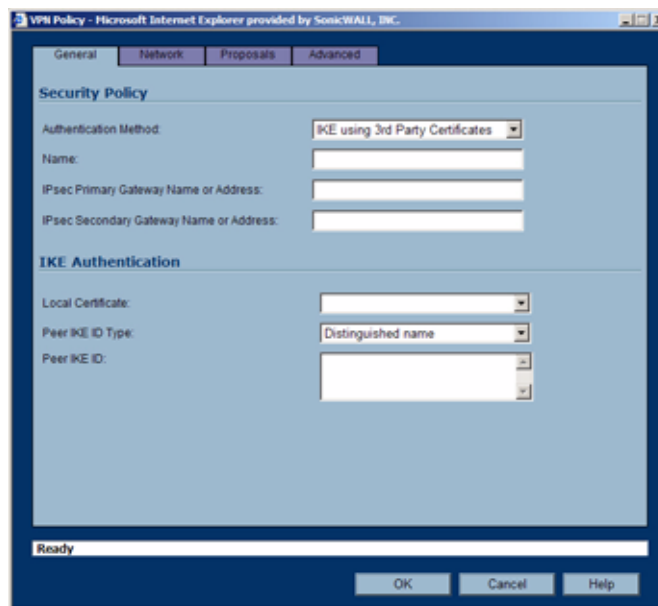
Configuring a VPN Policy with IKE using a Third Party Certificate



Warning: You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate.

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

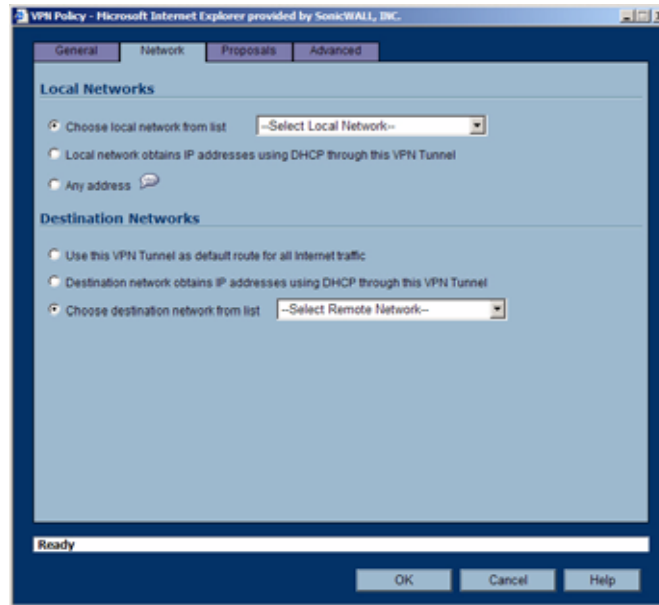
- 1 In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.
- 2 In the **Authentication Method** list in the **General** tab, select **IKE using 3rd Party Certificates**. The **VPN Policy** window displays the 3rd party certificate options.



- 3 Type a Name for the Security Association in the **Name** field.
- 4 Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWALL in the **IPsec Primary Gateway Name or Address** field. If you have a secondary remote SonicWALL, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.
- 5 Under **IKE Authentication**, select a third party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.
- 6 Select one of the following Peer ID types from the **Peer IKE ID Type** menu:
 - ◆ **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card

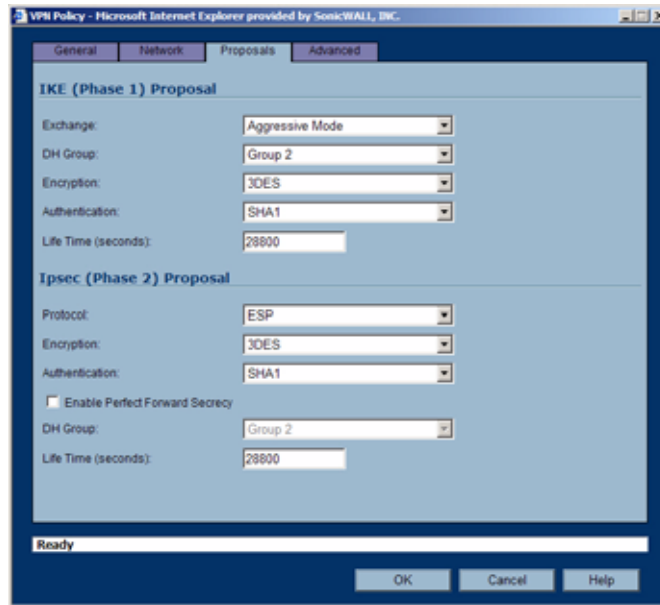
characters * (for more than 1 character) and ? (for a single character). For example, the string *@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string *sv.us.sonicwall.com when **Domain Name** is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.

- ◆ **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=). Up to three organizational units can be specified. The usage is c=*;o=*;ou=*;ou=*;ou=*;cn=*. The final entry does not need to contain a semi-colon. You must enter at least one entry, i.e. c=us.
- 7 Type an ID string in the **Peer IKE ID** field.
 - 8 Click on the **Network** tab.



- 9 Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.
- 10 Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

11 Click the **Proposals** tab.



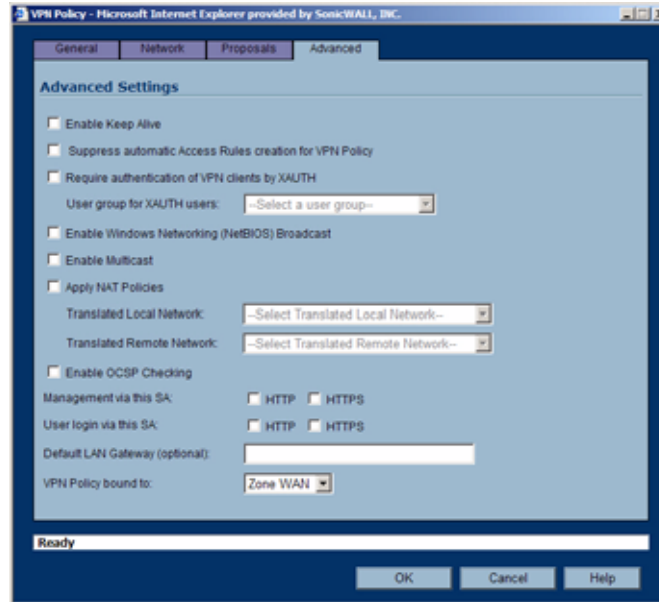
12 In the **IKE (Phase 1) Proposal** section, select the following settings:

- ◆ Select **Main Mode** or **Aggressive Mode** from the **Exchange** menu.
- ◆ Select the desired DH Group from the **DH Group** menu.
- ◆ Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- ◆ Select the desired authentication method from the **Authentication** menu.
- ◆ Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

13 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- ◆ Select the desired protocol from the **Protocol** menu
- ◆ Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu
- ◆ Select the desired authentication method from the **Authentication** menu
- ◆ Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.
- ◆ Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

- 14 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy:



- ◆ Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- ◆ The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- ◆ To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- ◆ Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- ◆ Select **Enable Multicast** to allow multicast traffic through the VPN tunnel.
- ◆ Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- ◆ Select **Enable OCSP Checking** to check VPN certificate status and specify the URL where to check certificate status. See the “[Using OCSP with SonicWALL Security Appliances](#)” section in [Chapter 44, Configuring VPN Policies](#).
- ◆ To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- ◆ If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

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

15 Click **OK**.

VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS Enhanced auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate Zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet 192.168.169.0. The VPN Policy appears as follows:

Name	Gateway	Destinations	Crypto Suite	Enable	Configure
Remote Site 1	87.115.118.80	192.168.169.1 - 192.168.169.255	ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

And the following Access Rules are added for inbound and outbound traffic:

Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
DMZ	1	Firewalled Subnets	Subnet 192.168.169.0	Any	Allow All	All		<input checked="" type="checkbox"/>	
LAN	1	Firewalled Subnets	Subnet 192.168.169.0	Any	Allow All	All		<input checked="" type="checkbox"/>	
VPN	3	Subnet 192.168.169.0	Firewalled Subnets	Any	Allow All	All		<input checked="" type="checkbox"/>	
VPN	3	Subnet 192.168.169.0	Firewalled Subnets	Any	Allow All	All		<input checked="" type="checkbox"/>	

While this is generally a tremendous convenience, there are some instances where it might be preferable to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke sites are addresses using address spaces that can easily be supernetted. For example, assume we wanted to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

```
remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)
```

Creating VPN Policies for each of these remote sites would result in the requisite 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just 4 Access Rules to a supernetted or address range representation of the remote sites (More specific allow or deny Access Rules could be added as needed):

```
remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255) or
remoteRangeAll=Range 10.0.0.0-10.7.207.255
```

To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** window page offers the option to **Auto-Add Access Rules for VPN Policy** setting. By default, the checkbox is selected, meaning the accompanying Access Rules will be automatically created, as they've always been. By deselecting the checkbox upon creating the VPN Policy, the administrator will have the ability and need to create custom Access Rules for VPN traffic.

Configuring Advanced VPN Settings

VPN > Advanced

The **VPN > Advanced** page includes optional settings that affect all VPN policies.

The screenshot shows the 'Advanced VPN Settings' configuration page. The page title is 'VPN > Advanced VPN Settings' with 'Apply', 'Cancel', and a help icon (?) buttons. The settings are as follows:

- Enable IKE Dead Peer Detection
 - Dead Peer Detection Interval (seconds): 60
 - Failure Trigger Level (missed heartbeats): 3
- Enable Dead Peer Detection for Idle vpn sessions
 - Dead Peer Detection Interval for Idle vpn sessions (seconds): 600
- Enable Fragmented Packet Handling
 - Ignore DF (Don't Fragment) Bit
- Enable NAT Traversal
- Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address
- Preserve IKE Port for Pass Through Connections
- Enable OCSP Checking
 - OCSP Responder URL: [text input field]
- Send vpn tunnel traps only when tunnel status changes
- Send IKEv2 Cookie Notify

Advanced VPN Settings

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the SonicWALL.
- **Dead Peer Detection Interval** - Enter the number of seconds between "heartbeats." The default value is 60 seconds.
- **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the SonicWALL security appliance. The SonicWALL security appliance uses a UDP packet protected by Phase 1 Encryption as the heartbeat.

- **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the SonicWALL security appliance after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is 600 seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message “Fragmented IPsec packet dropped”, select this feature. Do not select it until the VPN tunnel is established and in operation.
Ignore DF (Don't Fragment) Bit - when you select **Enable Fragmented Packet Handling**, the **Ignore DF (Don't Fragment) Bit** setting becomes active.
- **Enable NAT Traversal** - Select this setting if a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.
- **Clean up Active Tunnels when Peer Gateway DNS names resolves to a different IP address** - breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Preserve IKE Port for Pass-Through Connections** - preserves UDP 500/4500 source port and IP address information for pass-through VPN connections.
- **Enable OCSP Checking and OCSP Responder URL** - enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See [Using OCSP with SonicWALL Security Appliances](#).
- **Send IKEv2 Cookie Notify** - sends cookies to IKEv2 peers as an authentication tool.

Using OCSP with SonicWALL Security Appliances

Online Certificate Status Protocol (OCSP) allows you to check VPN certificate status without CRLs. This allows timely updates regarding the status of the certificates used on your SonicWALL.

About OCSP

OCSP is designed to augment or replace Certificate Revocation Lists (CRL) in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

Certificate Revocation Lists main disadvantage is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions may or may not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client will not accept the response from the OCSP server.

OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder. OpenCA OCSP Responder is available at <http://www.openca.org/ocspd/>. The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

Loading Certificates to use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the SonicWALL.

- 1 On the **System** -> **Certificates** page, click on the Import button. This will bring up the Import Certificate page.
- 2 Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.

Using OCSP with VPN Policies

The SonicWALL OCSP settings can be configured on a policy level or globally. To configure OCSP checking for individual VPN policies, use the **Advanced** tab of the **VPN Policy** configuration page.

- 1 Select the radio button next to **Enable OCSP Checking**
- 2 Specify the **OCSP Responder URL** of the OCSP server, for example <http://192.168.168.220:2560> where 192.168.168.220 is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.

Configuring DHCP Over VPN

VPN > DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a SonicWALL security appliance to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.



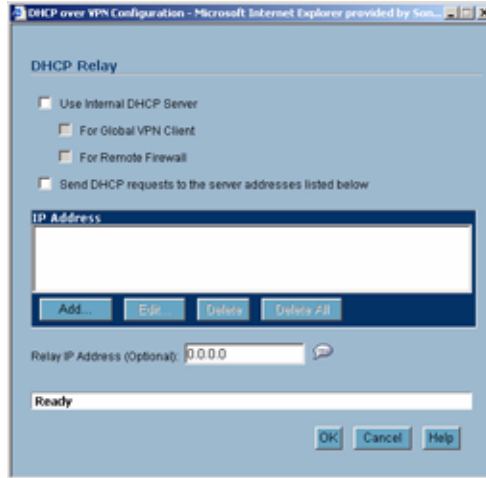
DHCP Relay Mode

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

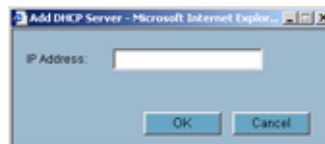
Configuring the Central Gateway for DHCP Over VPN

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

- 1 Select **VPN > DHCP over VPN**.
- 2 Select **Central Gateway** from the **DHCP Relay Mode** menu.
- 3 Click **Configure**. The **DHCP over VPN Configuration** window is displayed.



- 4 Select **Use Internal DHCP Server** to enable the SonicWALL Global VPN Client or a remote firewall or both to use an internal DHCP server to obtain IP addressing information. Check the **For Global VPN Client** checkbox to use the DHCP Server for Global VPN Clients and check the **For Remote Firewall** checkbox for the SonicWALL Global Security Client's firewall.
- 5 If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
- 6 Click **Add**. The **Add DHCP Server** window is displayed.



- 7 Type the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The SonicWALL security appliance now directs DHCP requests to the specified servers.
- 8 Type the IP address of a relay server in the **Relay IP Address (Optional)** field.

To edit an entry in the **IP Address** table, click **Edit**. To delete a DHCP Server, highlight the entry in the **IP Address** table, and click **Delete**. Click **Delete All** to delete all entries.

Configuring DHCP over VPN Remote Gateway

- 1 Select **Remote Gateway** from the **DHCP Relay Mode** menu.
- 2 Click **Configure**. The **DHCP over VPN Configuration** window is displayed.



- 3 In the **General** tab, the VPN policy name is automatically displayed in the Relay DHCP through this VPN Tunnel field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.



Alert: Only VPN policies using IKE can be used as VPN tunnels for DHCP.

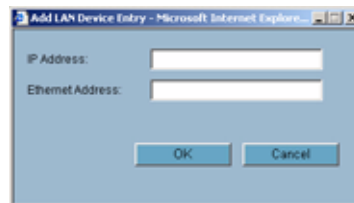
- 4 Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.
- 5 If you enter an IP address in the **Relay IP address** field, this IP address is used as the DHCP Relay Agent IP address in place of the Central Gateway's address, and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this SonicWALL security appliance remotely through the VPN tunnel from behind the Central Gateway.
- 6 If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the SonicWALL security appliance from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.
- 7 If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWALL security appliance blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWALL security appliance to respond to IP spoofs.
- 8 If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function. If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is 2 minutes.

Devices

- 1 To configure devices on your LAN, click the **Devices** tab.

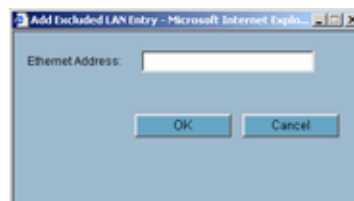


- 2 To configure **Static Devices on the LAN**, click **Add** to display the **Add LAN Device Entry** window, and type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.



An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses. Click **OK**.

- 3 To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** window. Enter the MAC address of the device in the **Ethernet Address** field. Click **OK**.



- 4 Click **OK** to exit the **DHCP over VPN Configuration** window.



Alert: You must configure the local DHCP server on the remote SonicWALL security appliance to assign IP leases to these computers.



Alert: If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.



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

Current DHCP over VPN Leases

The scrolling window shows the details on the current bindings: IP and Ethernet address of the bindings, along with the Lease Time, and Tunnel Name.

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the Trashcan icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

Click **Delete All** to delete all VPN leases.

Configuring L2TP Server

VPN > L2TP Server

The SonicWALL security appliance can terminate L2TP-over-IPsec connections from incoming Microsoft Windows 2000 and Windows XP clients. In situations where running the SonicWALL Global VPN Client is not possible, you can use the SonicWALL L2TP Server to provide secure access to resources behind the SonicWALL security appliances.

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Windows 2000 Operating System.

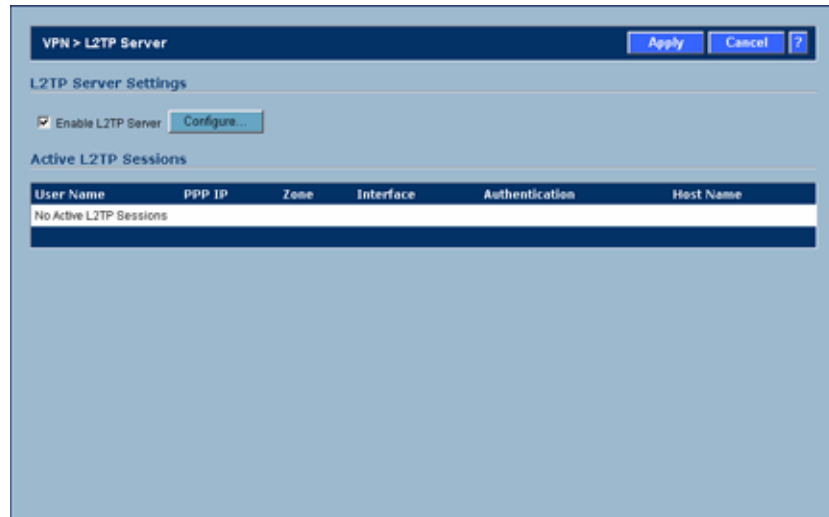
L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.



Cross Reference: For more complete information on configuring the L2TP Server, see the technote **Configuring the L2TP Server in SonicOS** located on the SonicWALL documentation site: <http://www.sonicwall.com/services/documentation.htm>.

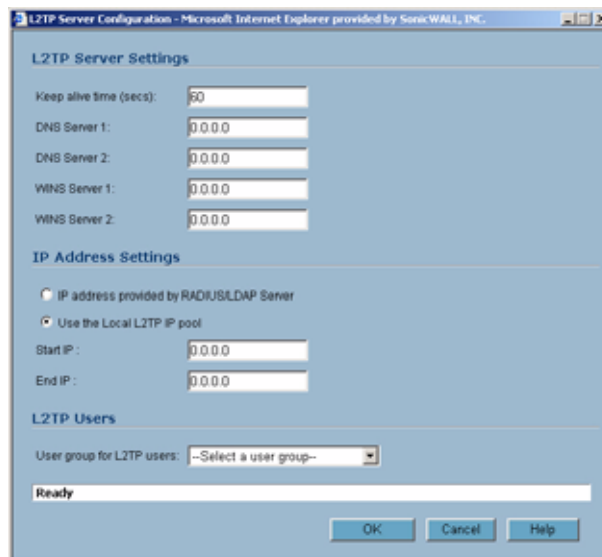
Configuring the L2TP Server

The **VPN > L2TP Server** page provides the settings for configuring the SonicWALL security appliance as a L2TP Server.



To configure the L2TP Server, follow these steps:

- 1 To enable L2TP Server functionality on the SonicWALL security appliance, select **Enable L2TP Server**. Then click **Configure** to display the **L2TP Server Configuration** window.



- 2 Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open. The default is **60** seconds.
- 3 Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.
- 4 Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.
- 5 Select **IP address provided by RADIUS Server** if a RADIUS Server provides IP addressing information to the L2TP clients.

- 6 If the L2TP Server provides IP addresses, select **Use the Local L2TP IP** pool. Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.
- 7 If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu or use **Everyone**.
- 8 Click **OK**.

Currently Active L2TP Sessions

- **User Name** - the user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - the source IP address of the connection.
- **Zone** - the zone used by the L2TP client.
- **Interface** - the type of interface used to access the L2TP Server, whether it's a VPN client or another SonicWALL security appliance.
- **Authentication** - type of authentication used by the L2TP client.
- **Host Name** - the name of the network connecting to the L2TP Server.

PART
10

Users

Managing User Status and Authentication Settings

SonicWALL security appliances provide a mechanism for user level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to bypass content filtering. Also, you can permit only authenticated users to access VPN tunnels and send data across the encrypted connection.

User level authentication can be performed using a local user database, RADIUS, or a combination of the two applications. The local database on the SonicWALL can support up to 1000 users. If you have more than 1000 users, you must use RADIUS for authentication.

Users > Status

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



The screenshot shows the 'Users > Status' page with a table of active user sessions. The table has the following columns: User Name, IP Address, Session Time, Time Remaining, Inactivity Remaining, Settings, and Logout. There is one entry for the user 'admin' with IP address 10.0.202.118, a session time of 0 Minutes, unlimited time remaining, and 60 Minutes of inactivity remaining. A trashcan icon is visible in the Logout column for the admin user.

User Name	IP Address	Session Time	Time Remaining	Inactivity Remaining	Settings	Logout
admin	10.0.202.118	0 Minutes	Unlimited	60 Minutes		

User > Settings

On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network.

The screenshot shows the 'Users > Settings' configuration page. At the top right are 'Apply', 'Cancel', and a help icon. The page is organized into sections:

- User Login Settings:**
 - Authentication Method: LDAP + Local Users (with a 'Configure...' button)
 - Show authentication page for (minutes): 1
 - Redirect users from HTTPS to HTTP on completion of login
- User Session Settings:**
 - Inactivity timeout (minutes): 5
 - Enable login session limit
 - Login session limit (minutes): 30
 - Show user login status window
 - User's login status window sends heartbeat every (seconds): 120
 - Enable disconnected user detection
 - Timeout on heartbeat from user's login status window (minutes): 10
- Other Global User Settings:**
 - Allow these HTTP URLs to bypass user authentication in access rules:
 - Text area containing: -None-
 - Buttons: Add, Remove
- Acceptable Use Policy:**
 - Display on login from:
 - Trusted Zones
 - WAN Zone
 - Public Zones
 - Wireless Zones
 - VPN Zone
 - Window size (pixels): 460 x 310
 - Enable scroll bars on the window
 - Acceptable use policy page content:
 - Large empty text area for policy content

At the bottom, there is a note: 'Note: Acceptable use policy text may include HTML formatting.' and two buttons: 'Example Template' and 'Preview'.

User Login Settings

From the **Authentication Method** list, select the type of user account management your network uses:

- Select **Local Users** to configure users in the local database in the SonicWALL appliance using the **Users > Local Users** and **Users > Local Groups** pages.
- Select **RADIUS** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the SonicWALL. If you select Use RADIUS for user authentication, users must log into the SonicWALL using HTTPS in order to encrypt the password sent to the SonicWALL. If a user attempts to log into the SonicWALL using HTTP, the browser is automatically redirected to HTTPS.
- Select **RADIUS + Local Users** if you want to use both RADIUS and the SonicWALL local user database for authentication.
- Select **LDAP** if you use a Lightweight Directory Access Protocol (LDAP) server, Microsoft Active Directory (AD) server, or Novell eDirectory to maintain all your user account data.
- Select **LDAP + Local Users** if you want to use both LDAP and the SonicWALL local user database for authentication.

In the **Show User Authentication Page for** field, enter the number of minutes a user has to log in before the login page times out. If it times out, a message displays saying they must click before attempting to log in again.



Select **Redirect users from HTTPS to HTTP on completion of login** if you want users to be connected to the network through your SonicWALL appliance via HTTP after logging in via HTTPS. If you have a large number of users logging in via HTTPS, you may want to redirect them to HTTP, because HTTPS consumes more system resources than HTTP. If you unselect this option, you will see a warning dialog.



Configuring RADIUS Authentication

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

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



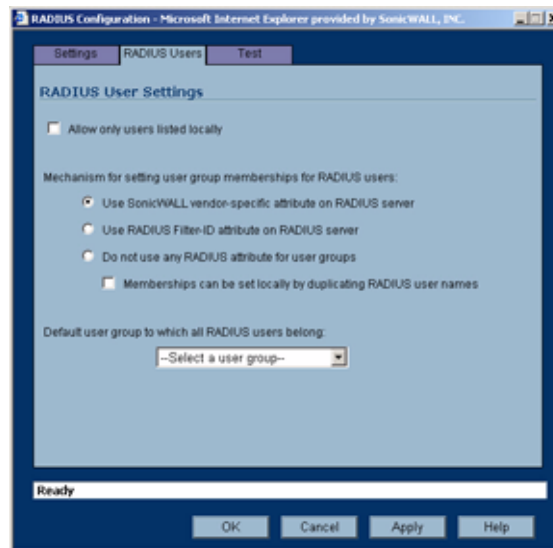
- 2 Define the **RADIUS Server Timeout in Seconds**. The allowable range is 1-60 seconds with a default value of 5.
- 3 Define the number of times the SonicWALL attempts to contact the RADIUS server in the **Retries** field. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, however 3 RADIUS server retries is recommended.

RADIUS Servers

- 1 Specify the settings of the primary RADIUS server in the RADIUS servers section. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.
- 2 Type the IP address of the RADIUS server in the **IP Address** field.
- 3 Type the **Port Number** for the RADIUS server.
- 4 Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
- 5 If there is a secondary RADIUS server, type the appropriate information in the **Secondary Server** section.
- 6 Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.

RADIUS Users

Click the **RADIUS Users** tab



RADIUS Users Settings

Select **Allow only users listed locally** if only the users listed in the SonicWALL database are authenticated using RADIUS.

Select the mechanism used for setting user group memberships for RADIUS users from the following list:

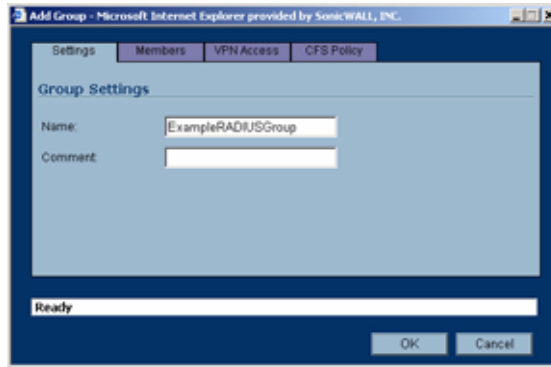
- **Use SonicWALL vendor-specific attribute on RADIUS server:** select to apply specific attributes from the RADIUS server.
- **Use RADIUS Filter-ID attribute on RADIUS server**
- Do not use any RADIUS attributes for user groups

For a shortcut for managing RADIUS user groups, check **Memberships can be set locally by duplicating RADIUS user names**. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database will automatically change to mirror your local changes.

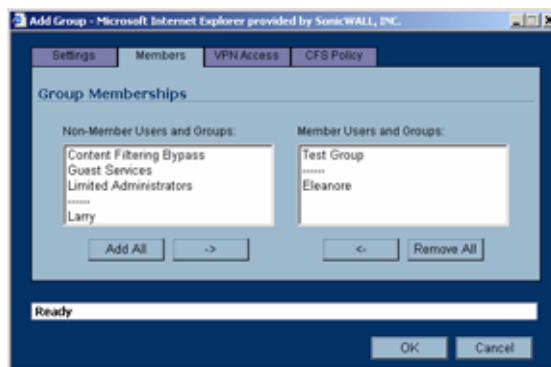
If you have previously configured User Groups on the SonicWALL, select the group from the **Default user group to which all RADIUS user belong** menu.

You can create a new group by choosing **Create a new user group...** from the list:

- 1 Select **Create a new user group...** The Add Group window displays.
- 2 In the **Settings** tab, enter a name for the group. You may enter a descriptive comment as well.

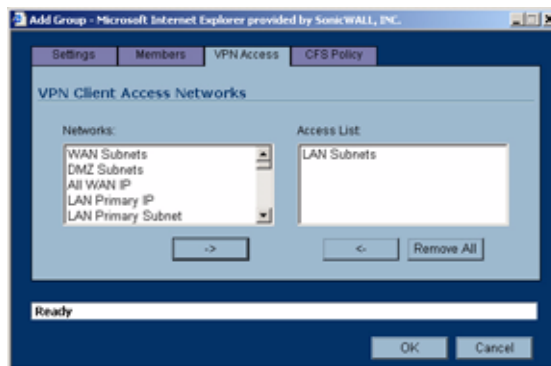


- 3 In the **Members** tab, select the members of the group. Select the users or groups you want to add in the left column and click the -> button. Click **Add All** to add all users and groups.



Note: You can add any group as a member of another group except **Everybody** and **All RADIUS Users**. Be aware of the membership of the groups you add as members of another group.

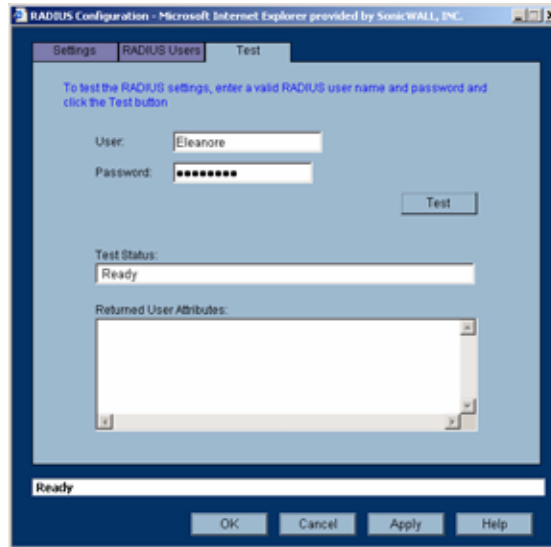
- 4 In the **VPN Access** tab, select the network resources this group will have VPN Access to by default.



- 5 If you have Content Filtering Service (CFS) on your security appliance, you can configure the content filtering policy for this group in the **CFS Policy** tab. See [Chapter 53, Configuring SonicWALL Content Filtering Service](#) for instructions on registering for and managing the SonicWALL Content Filtering Service.

RADIUS Client Test

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



If the validation is successful, the **Status** message changes to **Success**. If the validation fails, the **Status** message changes to **Failure**. Once the SonicWALL has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialogue box.

Configuring LDAP / Active Directory / eDirectory Authentication

Lightweight Directory Access Protocol (LDAP) defines a directory services structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. Several different standards exist that use LDAP to manage user account, group, and permissions. Some are proprietary systems like Microsoft Active Directory which you can manage using LDAP. Some are open standards SAMBA, which are implementations of the LDAP standards. Some are proprietary systems like Novell eDirectory which provide an LDAP API for managing the user repository information.

In addition to RADIUS and the local user database, SonicOS Enhanced supports LDAP, Microsoft Active Directory (AD), and Novell eDirectory directory services for user authentication.

LDAP Directory Services Supported in SonicOS Enhanced

In order to integrate with the most common directory services used in company networks, SonicOS Enhanced supports integration with the following LDAP schemas:

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User-defined schemas

SonicOS Enhanced provides support for directory servers running the following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)
- LDAP Referrals (RFC2251)

LDAP Terms

The following terms are useful when working with LDAP and its variants:

- *Schema* – The schema is the set of rules or the structure that defines the types of data that can be stored in a directory, and how that data can be stored. Data is stored in the form of ‘entries’.
- *Active Directory (AD)* – The Microsoft directory service, commonly used with Windows-based networking. Microsoft Active Directory is compatible with LDAP.
- *eDirectory* – The Novell directory service, used for Novell NetWare-based networking. Novell eDirectory has an LDAP gateway that can be used for management.
- *Entry* – The data that is stored in the LDAP directory. Entries are stored in ‘attribute/value (or name/value) pairs, where the attributes are defined by ‘object classes’. A sample entry would be ‘cn=john’ where ‘cn’ (common name) is the attribute, and ‘john’ is the value.
- *Object class* – Object classes define the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be ‘user’ or ‘group’.

Microsoft Active Directory’s Classes can be browsed at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes_all.asp

- *Object* - In LDAP terminology, the entries in a directory are referred to as objects. For the purposes of the SonicOS implementation of the LDAP client, the critical objects are ‘User’ and ‘Group’ objects. Different implementations of LDAP can refer to these object classes in different fashions, for example, Active Directory refers to the user object as ‘user’ and the group object as ‘group’, while RFC2798 refers to the user object as ‘inetOrgPerson’ and the group object as ‘groupOfNames’.
- *Attribute* - A data item stored in an object in an LDAP directory. Object can have required attributes or allowed attributes. For example, the ‘dc’ attribute is a required attribute of the ‘dcObject’ (domain component) object.
- *dn* - A ‘distinguished name’, which is a globally unique name for a user or other object. It is made up of a number of components, usually starting with a common name (cn) component and ending with a domain specified as two or more domain components (dc). For example, ‘cn=john,cn=users,dc=domain,dc=com’
- *cn* – The ‘common name’ attribute is a required component of many object classes throughout LDAP.
- *ou* – The ‘organizational unit’ attribute is a required component of most LDAP schema implementations.
- *dc* – The ‘domain component’ attribute is commonly found at the root of a distinguished name, and is commonly a required attribute.
- *TLS* – Transport Layer Security is the IETF standardized version of SSL (Secure Sockets Layer). TLS 1.0 is the successor to SSL 3.0.

Configuring LDAP integration in SonicOS Enhanced

Integrating your SonicWALL appliance with an LDAP directory service requires configuring your LDAP server to accept the management, installing the correct certificate on your SonicWALL appliance, and configuring the SonicWALL appliance to use the information from the LDAP Server.

Before you begin

Before beginning your LDAP configuration, you should prepare your LDAP server and your SonicWALL for LDAP over TLS support. This requires:

- Installing a server certificate and your LDAP server.
- Installing a CA (Certificate Authority) certificate for the issuing CA on your SonicWALL appliance.

To perform these tasks in an Active Directory environment:

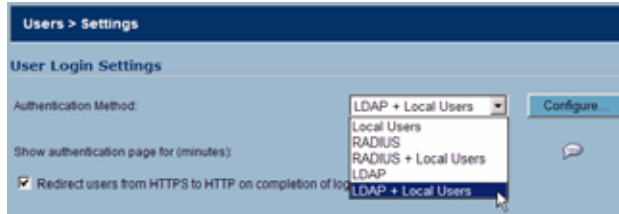
- 1 Configuring the CA on the Active Directory server (skip steps a. through e. if Certificate Services are already installed):
 - a Start>Settings>Control Panel>Add/Remove Programs'
 - b Select 'Add/Remove Windows Components'
 - c Select 'Certificate Services'
 - d Select 'Enterprise Root CA' when prompted.
 - e Enter the requested information. For detailed information on CA setup, see <http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp>
 - f Launch the 'Domain Security Policy' application:
'Start>Run>dcompol.msc'
 - g Open 'Security Settings > Public Key Policies'
 - h Right click on 'Automatic Certificate Request Settings'
 - i Select 'New > Automatic Certificate Request'
 - j Step through the wizard, and select 'Domain Controller' from the list.
- 2 Exporting the CA certificate from the AD server:
 - a Launch the 'Certification Authority' application: *Start>Run>certsrv.msc*
 - b Right click on the CA you created, select 'properties'
 - c On the 'General' tab, click the 'View Certificate' button
 - d From the 'Details' tab, select 'Copy to File'
 - e Step through the wizard, select the 'Base-64 Encoded X.509 (.cer)' format.
 - f Specify a path and filename to which to save the certificate.
- 3 Importing the CA certificate onto the SonicWALL:
 - a Browse to 'System > CA Certificates'
 - b Select 'Add new CA certificate'. Browse to and select the certificate file you just exported
 - c Click the 'Import certificate' button.

Configuring the SonicWALL Appliance for LDAP

The **Users > Settings** page in the administrative interface provides the settings for managing your LDAP integration:

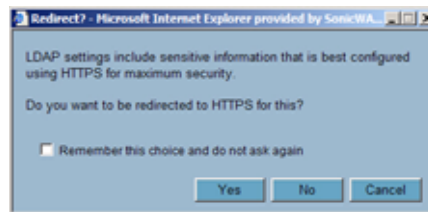
- 1 In the SonicOS administrative interface, open the **Users > Settings** page.

- 2 In the **Authentication Method** list, select either **LDAP** or **LDAP + Local Users**.

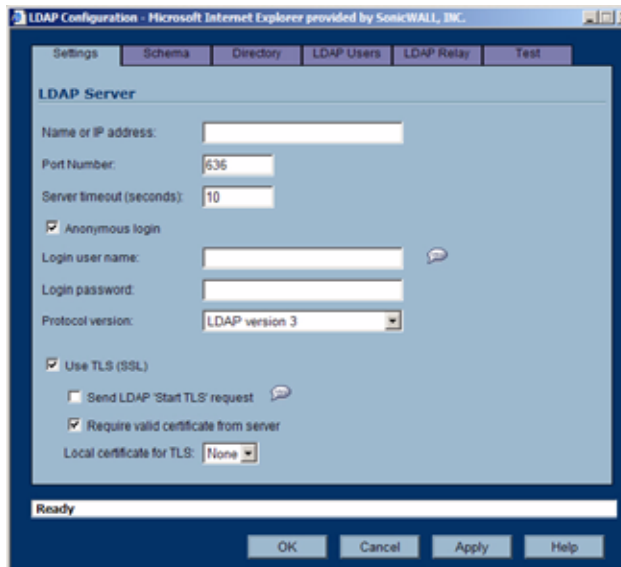


- 3 Click **Configure**.

- 4 If you are connected to your SonicWALL appliance via HTTP rather than HTTPS, you will see dialog box warning you of the sensitive nature of the information stored in directory services offering to change your connection to HTTPS. If you have HTTPS management enabled for the interface you are connected to (recommended), click **Yes**.



- 5 In the Settings tab LDAP Configuration window, configure:

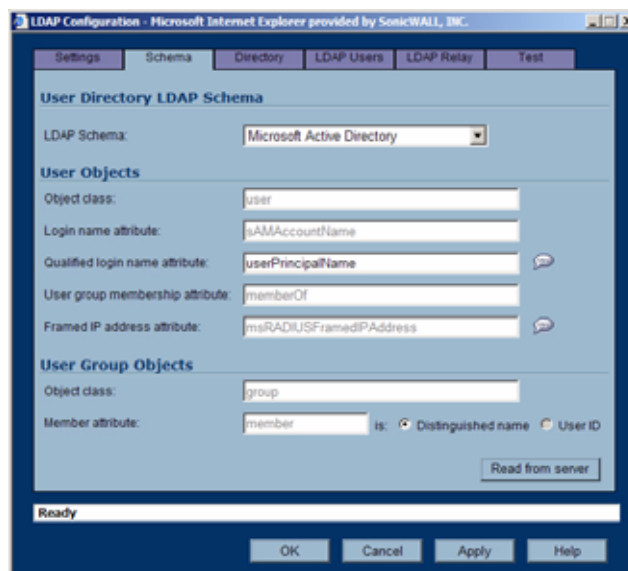


- ◆ **Name or IP Address** – Enter the FQDN or the IP address of the LDAP server against which you wish to authenticate. If using a name, be certain it can be resolved by your DNS server. Also, if using TLS with the ‘Require valid certificate from server’ option, the name provided here must match the name to which the server certificate was issued (i.e. the CN) or the TLS exchange will fail.
- ◆ **Port Number** – The default LDAP over TLS port number is TCP 636. The default LDAP (unencrypted) port number is TCP 389. If you are using a custom listening port on your LDAP server, specify it here.
- ◆ **Server timeout** – The amount of time, in seconds, that the SonicWALL will wait for a response from the LDAP server before timing out. Allowable ranges are 1 to 99999 (in case you’re running your LDAP server on a VIC-20 located on the moon), with a default of 10 seconds.
- ◆ **Anonymous Login** – Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AS generally does not), then you may select this option.

- ◆ **Login name** – Specify a user name which has rights to log in to the LDAP directory. The login name will automatically be presented to the LDAP server in full 'dn' notation. This can be any account with LDAP read privileges (essentially any user account) – Administrative privileges are not required. *Note that this is the user's name, not their login ID (e.g. John Smith rather than jsmith).*
- ◆ **Login password** – The password for the user account specified above.
- ◆ **Protocol version** – Select either LDAPv3 or LDAPv2. Most modern implementations of LDAP, including AD, employ LDAPv3.
- ◆ **Use TLS** – Use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended that TLS be used to protect the username and password information that will be sent across the network. Most modern implementations of LDAP server, including AD, support TLS. Deselecting this default setting will provide an alert which must be accepted to proceed.
- ◆ **Send LDAP 'Start TLS' Request** – Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. AD does not use this option, and it should only be selected if required by your LDAP server.
- ◆ **Require valid certificate from server** – Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWALL and the LDAP server will still use TLS – only without issuance validation.
- ◆ **Local certificate for TLS** – Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (AD does not return passwords). This setting is not required for AD.

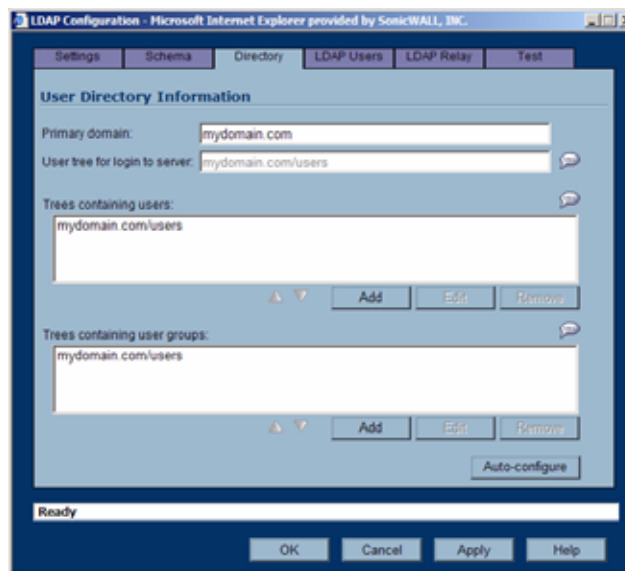
If your network uses multiple LDAP/AD servers with referrals, then select one as the primary server (probably the one that holds the bulk of the users) and use the above settings for that server. It will then refer the SonicWALL on to the other servers for users in domains other than its own. For the SonicWALL to be able to log in to those other servers, each server must have a user configured with the same credentials (user name, password and location in the directory) as per the login to primary server. This may entail creating a special user in the directory for the SonicWALL login. Note that only read access to the directory is required.

6 Select the **Schema** tab:



- ♦ **LDAP Schema** – select **Microsoft Active Directory, RFC2798 inetOrgPerson, RFC2307 Network Information Service, Samba SMB, Novell eDirectory, or user-defined**. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting 'user-defined' will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.
- ♦ **Object class** – this defines which attribute represents the individual user account to which the next two fields apply
- ♦ **Login name attribute** – this defines which attribute is used for login authentication.
 - sAMAccountName** for Microsoft Active Directory
 - inetOrgPerson** for RFC2798 inetOrgPerson
 - posixAccount** for RFC2307 Network Information Service
 - sambaSAMAccount** for Samba SMB
 - inetOrgPerson** for Novell eDirectory
- ♦ **Qualified login name attribute** – if not empty, this specifies an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for Microsoft Active Directory and RFC2798 inetOrgPerson.
- ♦ **User group membership attribute** – this attribute contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- ♦ **Framed IP address attribute** – this attribute can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting via L2TP with the SonicWALL's L2TP server. In future this may also be supported for Global VPN Client. In Active Directory the static IP address is configured on the Dial-in tab of a user's properties.

7 Select the **Directory** tab.



- ♦ **Primary Domain** – specify the user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, e.g. *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

- ♦ **User tree for login to server** – The tree in which the user specified in the ‘Settings’ tab resides. For example, in AD the ‘administrator’ account’s default tree is the same as the user tree.
- ♦ **Trees containing users** – The trees where users commonly reside in the LDAP directory. One default value is provided which can be edited, an up to a total of 64 DN values may be provided, and the SonicWALL search the directory using them all until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- ♦ **Trees containing user groups** – Same as above, only with regard to user group containers, and a maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema’s user object, and are not used with AD.

All the above trees are normally given in URL format but can alternatively be specified as distinguished names (e.g. “myDom.com/Sales/Users” could alternatively be given as the DN “ou=Users,ou=Sales,dc=myDom,dc=com”). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



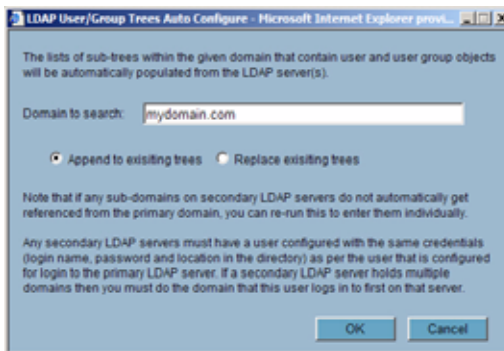
Note: AD has some built-in containers that do not conform (e.g. the DN for the top level Users container is formatted as “cn=Users,dc=...”, using ‘cn’ rather than ‘ou’) but the SonicWALL knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.



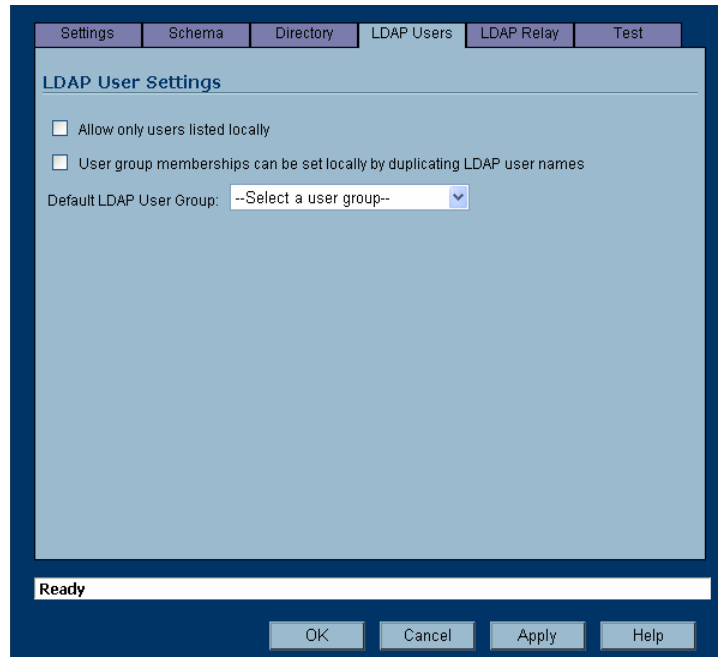
Note: When working with AD, to locate the location of a user in the directory for the ‘User tree for login to server’ field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as `queryad.vbs` in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

- ♦ **Auto-configure** – This causes the SonicWALL to auto-configure the ‘Trees containing users’ and ‘Trees containing user groups’ fields by scanning through the directory/directories looking for all trees that contain user objects. The ‘User tree for login to server’ must first be set, and clicking the Auto-configure button then brings up the following dialog:



- 8 Select whether to append new located trees to the current configuration, or to start from scratch removing all currently configured trees first, and then click OK. Note that it will quite likely locate trees that are not needed for user login and some tidying up afterwards, manually removing such entries, is worth while.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the ‘Domain to search’ accordingly and selecting ‘Append to existing trees’ on each subsequent run.

9 Select the **LDAP Users** tab.

- ◆ **Allow only users listed locally** – Requires that LDAP users also be present in the SonicWALL local user database for logins to be allowed.
- ◆ **User group membership can be set locally by duplicating LDAP user names** – Allows for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- ◆ **Default LDAP User Group** – A default group on the SonicWALL to which LDAP users will belong in addition to group memberships configured on the LDAP server.

Group memberships (and privileges) can also be assigned simply with LDAP. By creating user groups on the LDAP/AD server with the same name as SonicWALL built-in groups (such as 'Guest Services', 'Content Filtering Bypass', 'Limited Administrators') and assigning users to these groups in the directory, or creating user groups on the SonicWALL with the same name as existing LDAP/AD user groups, SonicWALL group memberships will be granted upon successful LDAP authentication.

The SonicWALL appliance can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

10 Select the **LDAP Relay** tab.

The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWALL, with remote satellite sites connected into it via low-end SonicWALL security appliances that may not support LDAP. In that case the central SonicWALL can operate as a RADIUS server for the remote SonicWALLs, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote SonicWALLs running non-enhanced firmware, with this feature the central SonicWALL can return legacy user privilege information to them based on user group memberships learned via LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWALLs.

- ◆ Enable RADIUS to LDAP Relay – Enables this feature.
- ◆ Allow RADIUS clients to connect via - Check the relevant checkboxes and policy rules will be added to allow incoming Radius requests accordingly.
- ◆ RADIUS shared secret - This is a shared secret common to all remote SonicWALLs.
- ◆ User groups for legacy users – These define the user groups that correspond to the legacy ‘Access to VPNs’, ‘Access from VPN client with XAUTH’, ‘Access from L2TP VPN client’ and ‘Allow Internet access (when access is restricted)’ privileges respectively. When a user in one of the given user groups is authenticated, the remote SonicWALL will be informed that the user is to be given the relevant privilege.



Note: The ‘Bypass filters’ and ‘Limited management capabilities’ privileges are returned based on membership to user groups named ‘Content Filtering Bypass’ and ‘Limited Administrators’ – these are not configurable.

11 Select the **Test** tab.

The screenshot shows a 'Test LDAP Settings' dialog box. At the top, there are tabs for 'Settings', 'Schema', 'Directory', 'LDAP Users', 'LDAP Relay', and 'Test'. The 'Test' tab is selected. Below the tabs, there is a title 'Test LDAP Settings' and a blue instruction box: 'To test the LDAP settings, enter a valid LDAP login name and password and click the Test button. Note that this will apply any changes that have been made.' Below this, there are two input fields: 'User:' with the text 'jdoe' and 'Password:' with masked characters. To the right of the password field is a 'Test' button. Below the input fields, there is a 'Test Status:' field containing the text 'LDAP Client Authentication Succeeded'. Underneath that is a 'Returned User Attributes:' section with a scrollable list box containing three entries: 'memberOf: Group1', 'memberOf: Limited Administrators', and 'memberOf: Content Filtering Bypass'. At the bottom of the dialog, there is a 'Ready' status bar and four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

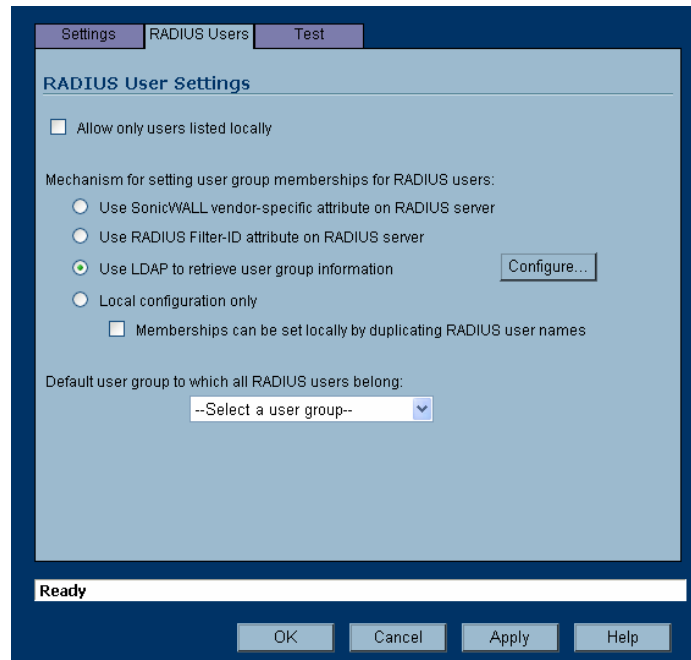
The 'Test' page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

Further Information on LDAP Schemas

- **Microsoft Active Directory:** Schema information is available at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/active_directory_schema.asp and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap_reference.asp
- **RFC2798 InetOrgPerson:** Schema definition and development information is available at <http://rfc.net/rfc2798.html>
- **RFC2307 Network Information Service:** Schema definition and development information is available at <http://rfc.net/rfc2307.html>
- **Samba SMB:** Development information is available at <http://us5.samba.org/samba/>
- **Novell eDirectory:** LDAP integration information is available at <http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/h0000007.html>
- **User-defined schemas:** See the documentation for your LDAP installation. You can also see general information on LDAP at <http://rfc.net/rfc1777.html>

RADIUS with LDAP for user groups

When RADIUS is used for user authentication, there is an option on the RADIUS Users page in the RADIUS configuration to allow LDAP to be selected as the mechanism for setting user group memberships for RADIUS users:



When that is selected, after authenticating a user via RADIUS his/her user group membership information will be looked up via LDAP in the directory on the LDAP/AD server.

Clicking the Configure button launches the LDAP configuration window.

Note that in this case LDAP is not dealing with user passwords and the information that it reads from the directory is normally unrestricted, so operation without TLS could be selected, ignoring the warnings, if TLS is not available (e.g. if certificate services are not installed with Active Directory). However, it must be ensured that security is not compromised by the SonicWALL doing a clear-text login to the LDAP server – e.g. create a user account with read-only access to the directory dedicated for the SonicWALL's use. Do not use the administrator account in this case.

User Session Settings

The settings listed below apply to all users when authenticated through the SonicWALL.

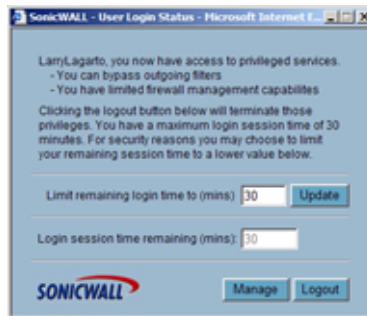
- **Inactivity timeout (minutes):** users can be logged out of the SonicWALL after a preconfigured inactivity time. Enter the number of minutes in this field. The default value is **5** minutes.
- **Enable login session limit:** you can limit the time a user is logged into the SonicWALL by selecting the check box and typing the amount of time, in minutes, in the **Login session limit (minutes)** field. The default value is **30** minutes.

- **Show user login status window:** causes a status window to display with a **Log Out** button during the user's session. The user can click the **Log Out** button to log out of their session.



The **User Login Status** window displays the number of minutes the user has left in the login session. The user can set the remaining time to a smaller number of minutes by entering the number and clicking the **Update** button.

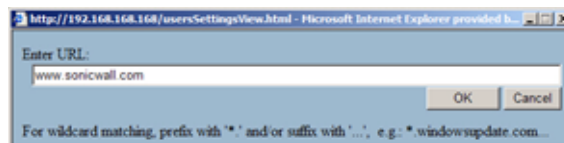
If the user is a member of the Limited Administrators user group, the **User Login Status** window has a **Manage** button the user can click to automatically log into the SonicWALL appliance's management interface. See [Chapter 49, Managing Local Users and Local Groups](#) for information on the Limited Administrators group.



- **User's login status window sends heartbeat every (seconds):** sets the frequency of the heartbeat signal used to detect whether the user still has a valid connection
- **Enable disconnected user detection:** causes the SonicWALL to detect when a user's connection is no longer valid and end the session.
- **Timeout on heartbeat from user's login status window (minutes):** sets the time needed without a reply from the heartbeat before ending the user session.

Other Global User Settings

- **Allow these HTTP URLs to bypass users authentication access rules:** Define a list of URLs users can connect to without authenticating. To add a URL to the list:
 - a Click **Add** below the URL list.
 - b In the **Enter URL** window, enter the top level URL you are adding, for example, `www.sonicwall.com`. All sub directories of that URL are included, such as `www.sonicwall.com/services/documentation.html`. Click on **OK** to add the URL to the list.



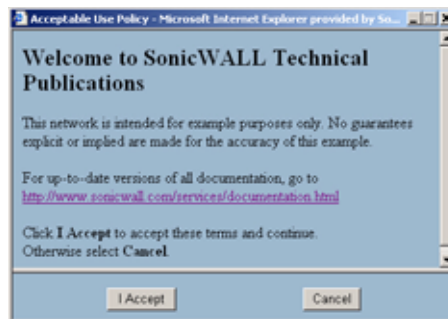
Acceptable Use Policy

An acceptable use policy (AUP) is a policy users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the SonicWALL.

The **Acceptable Use Policy** section allows you to create the AUP message window for users. You can use HTML formatting in the body of your message. Clicking the **Example Template** button creates a preformatted HTML template for your AUP window.

- **Display on login from** - select the network interface(s) you want to display the Acceptable Use Policy page when users login. You can choose **Trusted Zones**, **WAN Zone**, **Public Zones**, **Wireless Zones**, and **VPN Zone** in any combination.
- **Window size (pixels)** - allows you to specify the size of the AUP window defined in pixels. Checking the **Enable scroll bars on the window** allows the user to scroll through the AUP window contents.
- Select **Enable scroll bars on window** to turn on the scroll bars if your content will exceed the display size of the window.

Acceptable use policy page content - enter your Acceptable Use Policy text in the text box. You can include HTML formatting. The page that is displayed to the user includes an **I Accept** button or **Cancel** button for user confirmation.



Click the **Example Template** button to populate the content with the default AUP template, which you can modify:

```
<font face=arial size=3>
<center><b><i>Welcome to the SonicWALL</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>
```

Click "I Accept" only if you wish to accept these terms and continue, or otherwise select "Cancel".

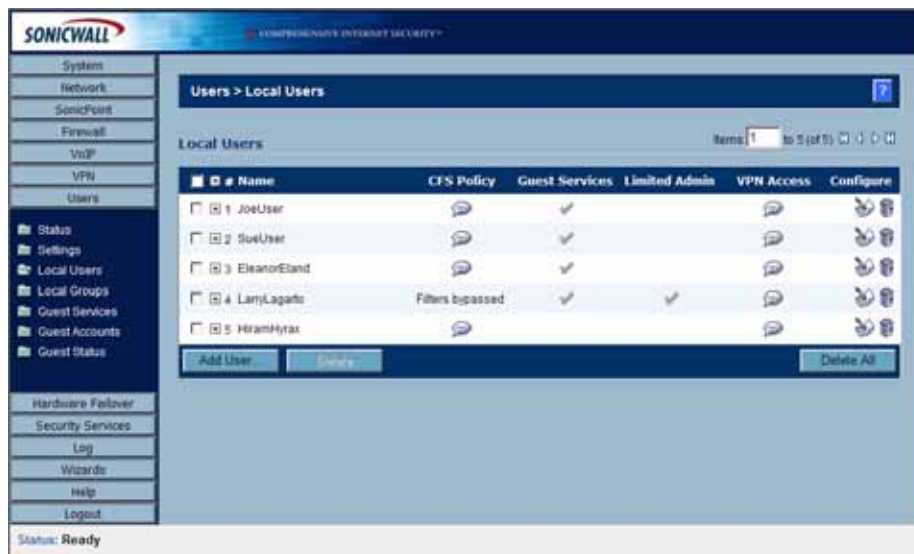
Click the **Preview** button to display your AUP message as it will appear for the user.

Managing Local Users and Local Groups


User > Local Users

Local Users are users stored and managed on the security appliance's local database.

In the **Users > Local Users** page, you can view and manage all local users, add new local users, and edit existing local users.







Viewing Local Users

You can view all the groups a user belongs to on the **Users > Local Users** page. Click on the expand icon  next to a user to view the group memberships for that user.

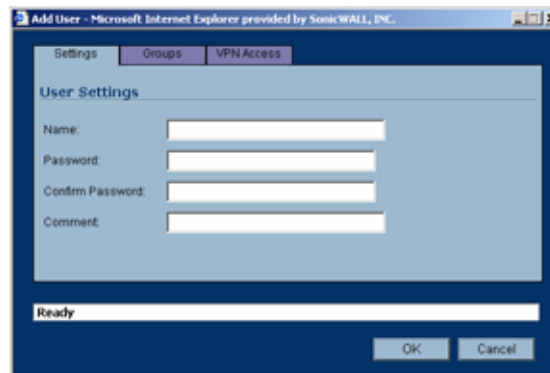


The three columns to the right of the user's name list the privileges the user has. In the expanded view, it displays which group the user gets each privilege from.

- Hover the mouse pointer over the comment icon  in the VPN Access column to view the network resources the user has VPN access to.
- In the expanded view, click the remove icon  under Configure to remove the user from a group.
- Click the edit icon  under Configure to edit the user.
- Click the delete icon  under Configure to delete the user or group in that row.

Adding Local Users

To add local users to the security appliance's internal database. Click **Add User** to display the **Add User** configuration window. Follow the steps below to add users locally.

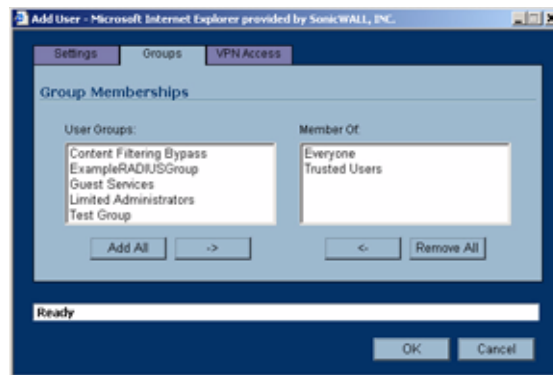


Settings

- 1 Create a user name and type it in the **User Name** field.
- 2 Create a password for the user and type it in the **Password** field. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.
- 3 Confirm the password by retyping it in the **Confirm Password** field.

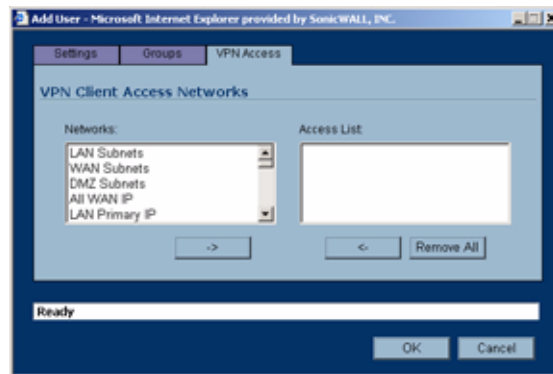
Groups

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



VPN Access

To allow users to access networks using a VPN tunnel, select the network from the **Networks** list and click **->** to move it to the **Access List**.



To remove a network from the **Access List**, select the network and click **<-**. Click **OK** to complete the user configuration.

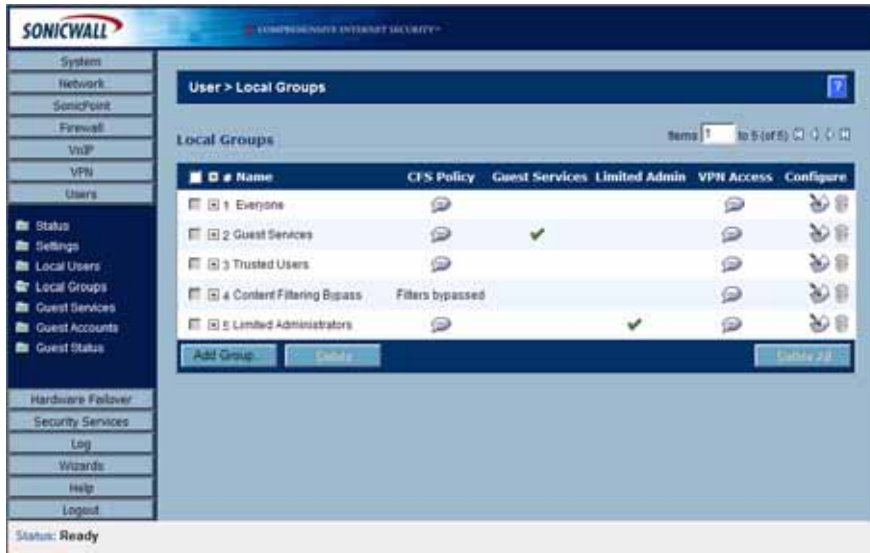
Editing Local Users

You can edit local users from the **Users > Local Users** screen. To edit a local user, in the list of users, click the edit icon in same line as the user you are editing.

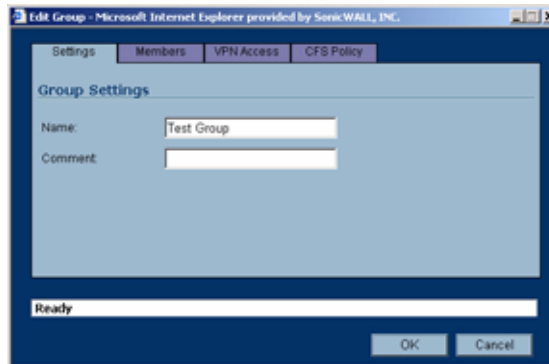
Configure the Settings, Groups, and VPN Access exactly as when adding a new user.

Users > Local Groups

Local groups are displayed in the **Local Groups** table. The table lists **Name**, **CFS Policy**, **Guest Services**, **Limited Admin**, **VPN Access**, and **Configure**.

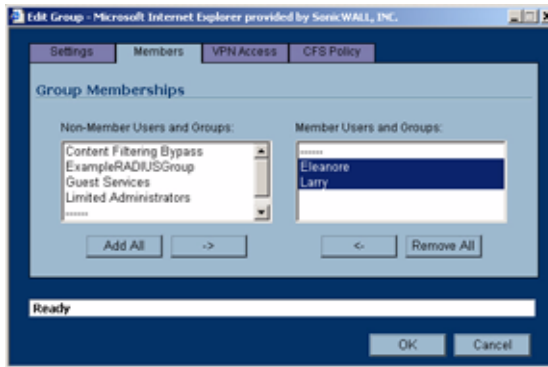


A default group, **Everyone**, is listed in the first row of the table. Click the Notepad icon in the **Configure** column to review or change the settings for **Everyone**.



Creating a Local Group

- 1 Click the **Add Group** button to display the **Add Group** window.
- 2 Create a user name and type it in the **User Name** field.
- 3 To add non-Members Users and Groups, click the **Members** tab. Select the non-member user or group from the **Non-Members Users and Groups** list and click ->.



- 4 To allow users in this group to access networks using a VPN tunnel, click the **VPN Access** tab, select the network from the **Networks** list and click -> to move it to the **Access List**.
- 5 To enforce a custom Content Filtering Service policy for this group, click on the **CFS Policy** tab. Select the CFS policy from the **Policy** menu.



Note: You create custom Content Filtering Service policies in the **Security Services > Content Filter** page. See [Chapter 53, Configuring SonicWALL Content Filtering Service](#).

- 6 Click **OK**.

Managing Guest Services and Guest Accounts

Guest accounts are temporary accounts set up for users to log into your network.

You can create these accounts manually, as needed or generate them in batches. SonicOS includes profiles you can configure in advance to automate configuring guest accounts when you generate them.

Guest accounts are typically limited to a pre-determined life-span. After their life span, by default, the accounts are removed.

Users > Guest Services

Guest Services determine the limits and configuration of the guest accounts. The **Users > Guest Services** page displays a list of Guest Profiles. Guest profiles determine the configuration of guest accounts when they are generated. In the **Users > Guest Services** page, you can add, delete, and configure Guest Profiles. In addition, you can determine if all users who log in to the security appliance see a user login window that displays the amount of time remaining in their current login session.

The screenshot shows the SonicWall SonicOS Administrator's Guide interface. The left sidebar contains a navigation menu with categories like Systems, Network, Wireless, Firewall, VPN, Users, Status, Settings, Local Users, Local Groups, Guest Services, Guest Accounts, Guest Status, Hardware Failover, Security Services, Log, Wizards, Help, and Logout. The main content area is titled 'Users > Guest Services' and includes an 'Apply' button. Below the title, there are 'Global Guest Settings' and a checkbox for 'Show guest login status window with logout button'. The 'Guest Profiles' section contains a table with the following data:

Name	User Name Prefix	Account Lifetime	Session Lifetime	Idle Timeout	Configure
1 Default	guest	7 Days	1 Hour	10 Minutes	[Icons]
2 Wireless Guest	guest	7 Days	1 Hour	10 Minutes	[Icons]

Below the table are 'Add' and 'Delete' buttons. At the bottom of the page, a status message reads: 'Status: The configuration has been updated.'

Global Guest Settings

Check **Show guest login status window with logout button** to display a user login window on the users's workstation whenever the user is logged in. Users must keep this window open during their login session. The window displays the time remaining in their current session. Users can log out but clicking the **Logout** button in the login status window.

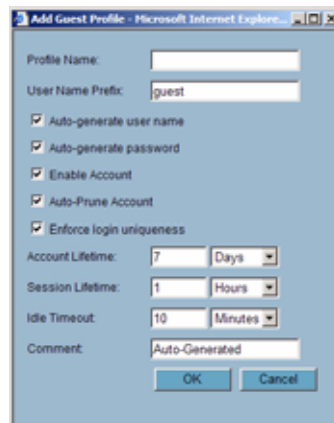


Guest Profiles

The Guest Profiles list shows the profiles you have created and enables you to add, edit, and delete profiles.

To add a profile:

- 1 Click **Add** below the Guest Profile list to display the Add Guest Profile window.



- 2 In the Add Guest Profile window, configure:

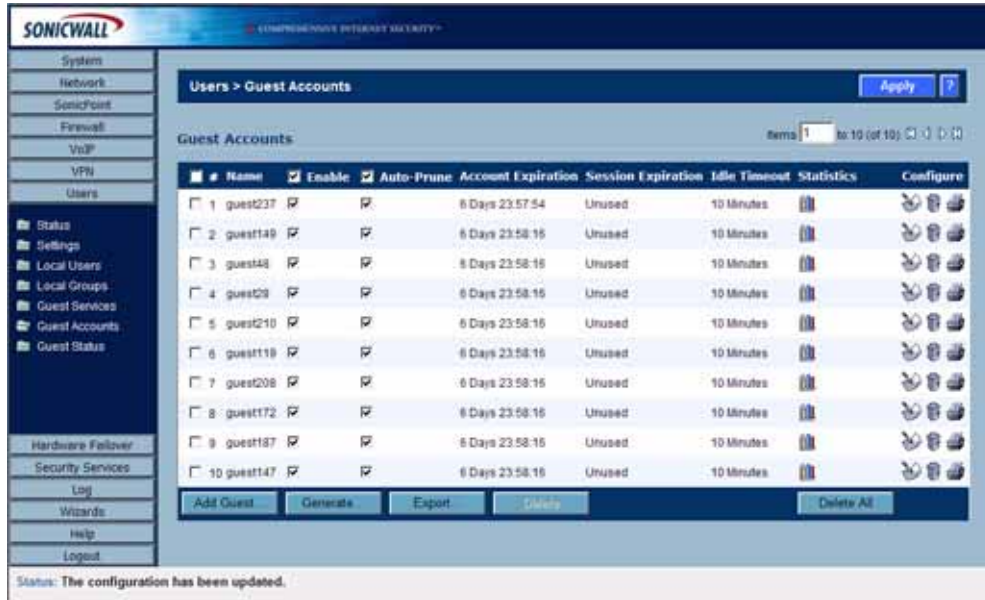
- ◆ **Profile Name:** Enter the name of the profile.
- ◆ **User Name Prefix:** Enter the first part of every user account name generated from this profile.
- ◆ **Auto-generate user name:** Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.
- ◆ **Auto-generate password:** Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- ◆ **Enable Account:** Check this for all guest accounts generated from this profile to be enabled upon creation.
- ◆ **Auto-Prune Account:** Check this to have the account removed from the database after its lifetime expires.
- ◆ **Enforce login uniqueness:** Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you

want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness checkbox.

- ◆ **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
 - ◆ **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**
 - ◆ **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
 - ◆ **Comment:** Any text can be entered as a comment in the **Comment** field.
- 3 Click **OK** to add the profile.

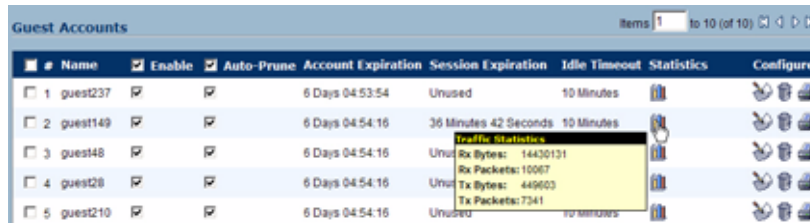
Users > Guest Accounts

The **Users > Guest Accounts** page lists the guest services accounts on the security appliance. In the guest services accounts, you can enable or disable individual accounts, groups of accounts, or all accounts, you can set the Auto-Prune feature for accounts, and you can add, edit, delete, and print accounts.



Viewing Guest Account Statistics

To view statistics on a guest account, hover your mouse over the Statistics icon in the line of the guest account. The statistics window will display the cumulative total bytes and packets sent and received for all completed sessions. Currently active sessions will not be added to the statistics until the guest user logs out.



Adding Guest Accounts

You can add guest accounts individually or generate multiple guest accounts automatically.

To Add an Individual Account:

- 1 Under the list of accounts, click **Add Guest**.

- 2 In the **Settings** tab of the Add Guest Account window configure:
 - ◆ **Profile:** Select the Guest Profile to generate this account from.
 - ◆ **Name:** Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
 - ◆ **Comment:** Enter a descriptive comment.
 - ◆ **Password:** Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
 - ◆ **Confirm Password:** If you did not generate the password, re-enter it.



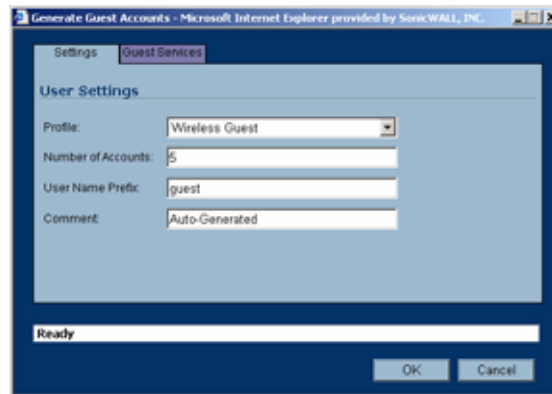
Note: Make a note of the password. Otherwise you will have to reset it.

- 3 In the **Guest Services** tab, configure:
 - ◆ **Enable Guest Services Privilege:** Check this for the account to be enabled upon creation.
 - ◆ **Enforce login uniqueness:** Check this to allow only one instance of this account to log into the security appliance at one time. Leave it unchecked, to allow multiple users to use this account at once.
 - ◆ **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires.
 - ◆ **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
 - ◆ **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
 - ◆ **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

- 4 Click **OK** to generate the account.

To Generate Multiple Accounts

- 1 Under the list of accounts, click **Generate**.



- 2 In the **Settings** tab of the Generate Guest Accounts window configure:
 - ♦ **Profile:** Select the Guest Profile to generate the accounts from.
 - ♦ **Number of Accounts:** Enter the number of accounts to generate.
 - ♦ **User Name Prefix:** Enter the prefix from which account names are generated. For example, if you enter **Guest** the generated accounts will have names like “Guest 123” and “Guest 234”.
 - ♦ **Comment:** Enter a descriptive comment.
- 3 In the **Guest Services** tab, configure:
 - ♦ **Enable Guest Services Privilege:** Check this for the accounts to be enabled upon creation.
 - ♦ **Enforce login uniqueness:** Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
 - ♦ **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires.
 - ♦ **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
 - ♦ **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
 - ♦ **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.
- 4 Click **OK** to generate the accounts.

Enabling Guest Accounts

You can enable or disable any number of accounts at one time. To enable one or more guest accounts:

- 1 Check the box in the **Enable** column next to the name of the account you want to enable. Check the **Enable** box in the table heading to enable all accounts on the page.
- 2 Click on **Apply** in the top right corner of the page.




Enabling Auto-prune for Guest Accounts

You can enable or disable auto-prune for any number of accounts at one time. When auto-prune is enabled, the account is deleted after it expires. To enable auto-prune:

- 1 Check the box in the **Auto-Prune** column next to the name of the account. Check the **Auto-Prune** box in the table heading to enable it on all accounts on the page.
- 2 Click on **Apply** in the top right corner of the page.

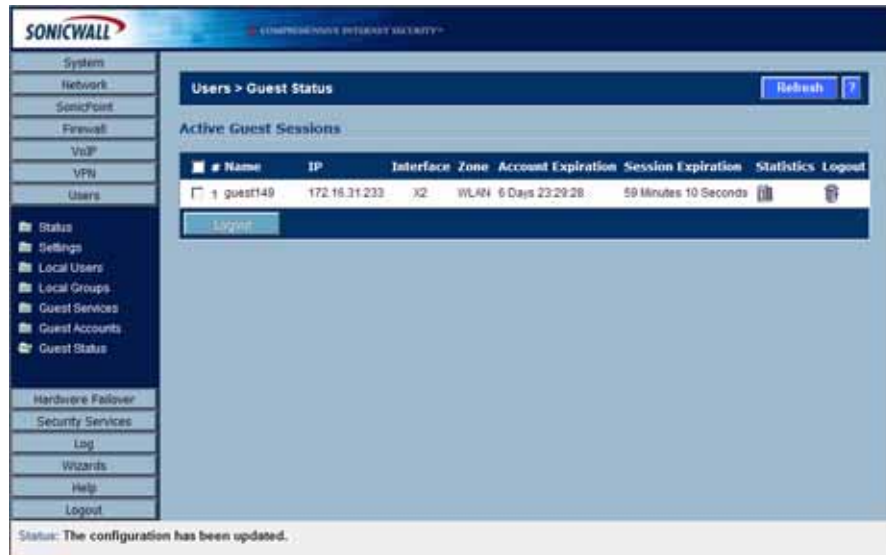
Printing Account Details.

You can print a summary of a guest account. Click the print icon  to launch a summary account report page and send that page to an active printer.

Description	Value
Account Name:	guest341
Password:	pretrbr
Enabled:	Yes
Comment:	Auto-Generated
Created:	FRI MAY 20 12:01:08 2004
Account Expires:	FRI JUN 04 12:01:08 2004
Session Expires:	Unused
Session Lifetime:	1 Hour
Idle Timeout:	10 Minutes

Users > Guest Status

The Guest Status page reports on all the guest accounts currently logged in to the security appliance.



The page lists:

- **Name:** The name of the guest account
- **IP:** The IP address the guest user is connecting to.
- **Interface:** The interface on the security appliance through which the user account is connecting to the appliance. For example, If the guest account is a wireless user connecting through a SonicWALL SonicPoint, and all SonicPoints are connecting to the **OPT** port on the appliance, which is configured as a Wireless Zone, the **Interface** column will list **OPT**.
- **Zone:** The Zone on the security appliance that the guest user is connecting to. For example, a wireless user might be connecting to the **WLAN** zone.
- **Account Expiration:** The date, hour, or minute when the account expires.
- **Session Expiration:** The time when the current session expires.
- **Statistics:** hover your mouse over the **Statistics** icon to view statistics for total received and sent bytes and packets for this guest user's current session.



- **Logout:** Click the Logout icon to log the guest user off of the security appliance.

Click **Refresh** in the top right of the page at any time to update the information in the list.

Logging Accounts off the Appliance

As administrator, you can log users off the security appliance:

- To log an individual user out, click the Logout icon in the **Logout** column for that user.
- To log multiple users out, click the checkbox in the first column to select individual users, or check the checkbox next to the **#** in the table heading to select all the guest users listed on the page. Then click **Logout** below the list.

PART
11

Hardware Failover

Setting Up Hardware Failover

Hardware Failover > Settings

Hardware Failover allows two identical SonicWALL PRO Series security appliances running SonicOS Enhanced to be configured to provide a reliable, continuous connection to the public Internet. In the event of the failure of the Primary SonicWALL, the Backup SonicWALL takes over to secure a reliable connection between the protected network and the Internet.

How Hardware Failover Works

Hardware Failover requires one SonicWALL device configured as the Primary SonicWALL, and an identical SonicWALL device configured as the Backup SonicWALL. During normal operation, the Primary SonicWALL is in an Active state and the Backup SonicWALL in an Idle state. When a failure on the Primary SonicWALL occurs, the Backup SonicWALL transitions to Active mode and assumes the configuration and role of Primary. The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWALL.

SonicWALL security appliance configuration is performed on only the Primary SonicWALL, with no need to perform any configuration on the Backup SonicWALL. The Backup SonicWALL contains a real-time mirrored configuration of the Primary SonicWALL via a dedicated Ethernet link. If the firmware configuration becomes corrupted on the Primary SonicWALL, the Backup SonicWALL

automatically refreshes the Primary SonicWALL with the last-known-good copy of the configuration preferences.

The Primary and Backup SonicWALL appliances have unique MAC addresses and communicate via the X3 interface on the PRO2040 series, and via the X5 interface on the PRO3060/4060/5060 series. The dedicated HF interface link transmits all synchronization information from the Primary SonicWALL to the Backup SonicWALL.

There are two types of synchronization: incremental and complete. If the timestamps are in sync and a change is made on the Active unit, an incremental sync is pushed to the Idle unit. If the timestamps are out of sync and the Idle unit is available, a complete sync is pushed to the Idle unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

Crash Detection

The Hardware Failover feature has a thorough self-diagnostic mechanism for both the Primary and Backup SonicWALL security appliances. The failover to the Backup SonicWALL occurs when critical services are affected, physical (or logical) link detection is detected on monitored interfaces, or when the SonicWALL loses power.

The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the SonicWALL device. The diagnostics check internal system status, system process status, and both internal and external network connectivity. For example, if a network topology has three levels, then diagnostics are performed on the router/switch/hub connectivity on the first, second, and third level. There is a weighting mechanism on both sides to decide which side has better connectivity, used to avoid potential failover looping.

Critical internal system processes such as NAT, VPN, and DHCP (among others) are checked in real time. The failing service is isolated as early as possible, and the failover mechanism repairs it automatically.

Before Configuring Hardware Failover

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

- Hardware Failover is only supported on the SonicWALL PRO 2040, PRO 3060, PRO 4060 and PRO 5060 security appliances running SonicOS Enhanced. It is not supported in any version of SonicOS Standard, or on any SonicWALL TZ 170 series product running the version of SonicOS Enhanced
- The Primary and Backup SonicWALL security appliances must be same hardware model – mixing and matching SonicWALLs of different hardware types is not currently supported.
- The Hardware Failover feature requires three unique LAN IP addresses to operate – the first IP address is used as a virtual gateway IP address, the second is used as the unique LAN IP address for the Primary device, and the third is used as the unique LAN IP address for the Backup device. You have at least one (1) valid, static IP address available from your Internet Service Provider (ISP). Two (2) valid, static IP addresses are required to remotely manage both the primary SonicWALL and the backup SonicWALL.



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

- Each SonicWALL security appliance in the **Hardware Failover** pair must have the same firmware version installed.
- SonicWALL Security Services licenses are not shared between Primary and Backup SonicWALL devices -- the Backup SonicWALL must have separate licenses. Each SonicWALL security appliance in the **Hardware Failover** pair must have the same SonicWALL Security Services

enabled. If the Backup SonicWALL security appliance does not have the same upgrades and subscriptions enabled, these functions are not supported in the event of a failure of the Primary SonicWALL appliance.

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



Tip: *The two SonicWALLs in the Hardware Failover pair send “heartbeats” on their X5 Interfaces—on the PRO3060/4060/5060 series—as a dedicated-HF link. However, the PRO2040 series uses the X3 Interface as the dedicated-HF link.*

- If using new single WAN IP method, please note that the Backup device, when in offline ‘Idle’ mode, will not be able to use NTP to synchronize its internal clock, nor will it be able to contact the backend services licensing servers. It is also unable to perform device registration with the backend licensing servers.
- Hardware Failover can be used with dual WAN ports, but only if both WAN interfaces use static IP addressing; the current firmware does not support either WAN interface using dynamic IP addressing.
- Once Hardware Failover has been configured and activated, upon first preferences synchronization, the Backup SonicWALL security appliance automatically reboots in order to load the mirrored preferences – this is normal behavior.
- At present, the monitor feature utilizes ICMP pings on designated probe targets, and can only be used on interfaces that have been assigned unique IP addresses (at present, LAN and WAN only).
- The Primary and Backup SonicWALL security appliance’s unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.
- The Primary and Backup SonicWALL devices are currently only capable of performing active/passive Hardware Failover – active/active failover is not supported at present.
- Session state is not currently synchronized between the Primary and Backup SonicWALL security appliances. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.
- If shifting a previously assigned interface to act as the Secondary WAN interface, be sure to remove any custom NAT policies that were associated with that interface before configuring it.
- It’s strongly recommended that Primary and Backup SonicWALL security appliances run the exact same version of firmware; system instability may result if firmware versions are out of sync.
- Successful Hardware Failover synchronization is not logged, only failures.
- If you are connecting the Primary and Backup device to an Ethernet switch running the spanning-tree protocol, please be aware that it may be necessary to adjust the link activation time on the switch port that the SonicWALL interfaces connect to. As an example, it would be necessary to activate spantree portfast on a Cisco Catalyst-series switch, for each port connecting to the SonicWALL’s interfaces.
- If you will not be using the unique WAN IP address feature, make sure each entry field is set to ‘0.0.0.0’ – the SonicWALL will report an error if the field is left blank.

Hardware Failover Terminology

- **Primary** - Describes the principal hardware unit itself. The Primary identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.
- **Backup** - Describes the subordinate hardware unit itself. The Backup identifier is a relational designation, and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Backup unit operates in an Idle mode. Upon failure of the Primary unit, the Backup unit will assume the Active role.
- **Active** - Describes the operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Backup hardware unit.
- **Idle** - Describes the passive condition of a hardware unit. The Idle identifier is a logical role that can be assumed by either a Primary or Backup hardware unit. The Idle unit assumes the Active role in the event of determinable failure of the Active unit.
- **Failover** - The actual process in which the Idle unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described throughout the Task List section.
- **Preempt** - Applies to a post-failover condition in which the Primary unit has failed, and the Backup unit has assumed the Active role. Enabling Preempt will cause the Primary unit to seize the Active role from the Backup after the Primary has been restored to a verified operational state.

Initial Hardware Failover Setup

Before you begin the configuration of Hardware Failover on the Primary SonicWALL security appliance, perform the following initial setup procedures.

- On the back of the Backup SonicWALL security appliance, locate the serial number and write the number down. You need to enter this number in the **Hardware Failover>Settings** page.
- Check to make sure the Primary SonicWALL and Backup SonicWALL security appliances are registered, running the same SonicOS Enhanced versions, and running the same SonicWALL Security services.
- Make sure Primary SonicWALL and Backup SonicWALL security appliance's LAN, WAN, and other interfaces are properly configured for seamless failover.
- Connect the X5 ports on the Primary SonicWALL and Backup SonicWALL appliances with a CAT6-rated crossover cable. The Primary and Backup SonicWALL security appliances must have a dedicated connection between each other using the X3 (PRO2040) or X5 (PRO3060/4060/5060) interface. SonicWALL recommends cross-connecting the two together using a CAT5/6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also acceptable.
- Power up the Primary SonicWALL security appliance, and then power on the Backup SonicWALL security appliance.
- Do not make any configuration to the Primary's X3 (PRO 2040) or X5 (PRO 3060/4060/5060) interface; the Hardware Failover programming in an upcoming step takes care of this issue. When done, disconnect the workstation.

Configuring Hardware Failover

The first task in setting up hardware failover after initial setup is configuring the **Hardware Failover>Settings** page on the Primary SonicWALL security appliance. Once you configure hardware failover on the Primary SonicWALL security appliance, you push out the settings to the Backup SonicWALL security appliance.

To configure Hardware Failover on the Primary SonicWALL, perform the following steps:

- 1 Select the **Hardware Failover > Settings** page on the Primary SonicWALL.



- 2 In the **Serial Number** field under **Backup SonicWALL**, enter the Backup SonicWALL's Serial number (this can be found on the back of the device).
- 3 Leave the **Heartbeat Interval (seconds)**, **Failover Trigger Level (missed heartbeats)**, **Probe Interval (seconds)**, and **Election Delay Time (seconds)** timers to their default settings. These timers can be tuned later as necessary for your specific network environment. A description of these timers and their effects are covered in the [“Adjusting Hardware Failover Settings”](#) section.
- 4 Check the **Enable Hardware Failover** and the **Enable Preempt Mode** checkboxes. If everything is configured and cabled correctly, the Primary SonicWALL automatically contacts the Backup SonicWALL over the dedicated link and configures all necessary settings. The Backup SonicWALL then reboots with its new settings and come back online in Idle mode.
- 5 Check the **Generate/Overwrite backup firmware and settings when upgrade firmware** checkbox if you want the SonicWALL to backup the firmware and system settings when upgrading to a new firmware version. This will overwrite the current backup file when the firmware is upgraded. If you prefer to manually manage backup settings, leave this checkbox unchecked.
- 6 Click the **Apply** button to save the changes.

Synchronize Settings

Once you've configured the hardware failover setting on the Primary SonicWALL security appliance, click the **Synchronize Settings** button. You should see a **HA Peer Firewall has been updated** message at the bottom of the Management Interface page. Also note that the Management Interface displays **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that Certificates, CRLs and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the primary and backup units. When Local Certificates are copied to the backup unit, the associated Private Keys are also copied. Because the connection between the primary and backup units is

typically protected, this is generally not a security concern.

Tip: A compromise between the convenience of synchronizing Certificates and the added security of not synchronizing Certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then power off the Primary SonicWALL device. The Backup SonicWALL security appliance should quickly take over.

From your Management Workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet – note that the Backup SonicWALL, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Backup SonicWALL's unique LAN IP address. If this SonicWALL security appliance has not been registered at mySonicWALL.com, register it. The Management Interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the Management Interface. The Management GUI should again display **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure everything is working correctly.

Forcing Transitions

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

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

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

Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the active SonicWALL restarts, the other SonicWALL in the **Hardware Failover** pair takes over operation.



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

Adjusting Hardware Failover Settings

On the **Hardware Failover>Settings** page, there are four user-configurable timers that can be adjusted to suit your network's needs:

- **Heartbeat Interval (seconds)** – This timer is the length of time between status checks. By default this timer is set to 5 seconds; using a longer interval will result in the SonicWALL taking more time to detect when/if failures have occurred.
- **Failover Trigger Level (missed heart beats)** – This timer is the number of heartbeats the SonicWALL will miss before failing over. By default, this time is set to 5 missed heart beats. This timer is linked to the Heartbeat Interval timer – for example, if you set the Heartbeat Interval to 10


- seconds, and the Failover Trigger Level timer to 5, it will be 50 seconds before the SonicWALL fails over.
- **Probe Interval** – This timer controls the path monitoring speed. Path monitoring sends pings to specified IP addresses to monitor that the network critical path is still reachable. The default is 20 seconds, and the allowed range is from 5 to 255 seconds.
 - **Election Delay Time** – This timer can be used to specify an amount of time the SonicWALL will wait to consider an interface up and stable, and is useful when dealing with switch ports that have a spanning-tree delay set.

Synchronizing Firmware

Checking the **Synchronize Firmware Upload and Reboot** checkbox allows the Primary And Backup SonicWALL security appliances in Hardware Failover mode to have firmware uploaded on both devices at once, in staggered sequence to ensure security is always maintained. During the firmware upload and reboot, you are notified via a message dialog box that the firmware is loaded on the Backup SonicWALL security appliance, and then the Primary SonicWALL security appliance. You initiate this process by clicking on the **Synchronize Firmware** button.

Monitoring Links

On the **Hardware Failover > Monitoring** page, you can specify IP addresses that the SonicWALL security appliance performs an ICMP ping on to determine link viability.



The screenshot shows the 'Hardware Failover > Monitoring' configuration page. It features a table titled 'Monitoring Settings' with the following columns: Name, Primary IP Address, Backup IP Address, Probe IP Address, Monitor Interface, Management, and Configure. The table contains four rows of data, each with a name (X0, X1, X2, X3, X4) and corresponding IP addresses. The 'Monitor Interface' and 'Management' columns have checkmarks for X0 and X1, and a gear icon for X2, X3, and X4.

Name	Primary IP Address	Backup IP Address	Probe IP Address	Monitor Interface	Management	Configure
X0	0.0.0.0	0.0.0.0	0.0.0.0	✓	✓	⚙️
X1	0.0.0.0	0.0.0.0	0.0.0.0	✓	✓	⚙️
X2	0.0.0.0	0.0.0.0	0.0.0.0			⚙️
X3	0.0.0.0	0.0.0.0	0.0.0.0			⚙️
X4	0.0.0.0	0.0.0.0	0.0.0.0			⚙️

When using logical monitors, the SonicWALL will ping the defined Probe IP Address target from the Primary as well as the Backup SonicWALL. If both can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWALLs will assume that the problem is with the target, and not the SonicWALLs. But, if one SonicWALL can ping the target but the other SonicWALL cannot, it will failover to the SonicWALL that can ping the target.

Clicking the edit icon in the **Configure** column of the Monitoring Settings table displays the **Edit HA Monitoring** window for monitoring hardware failover for the individual interface.



Hardware Failover Status

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

- Hardware Failover Status** - One method to determine which SonicWALL is active is to check the Hardware Failover Settings Status indicator on the Hardware Failover>Settings page. If the primary SonicWALL is active, the first line in the page indicates that the primary SonicWALL is currently Active. It is also possible to check the status of the backup SonicWALL by logging into the LAN IP Address of the backup SonicWALL. If the primary SonicWALL is operating normally, the status indicates that the backup SonicWALL is currently Idle. If the backup has taken over for the primary, the status indicates that the backup is currently Active. In the event of a failure in the primary SonicWALL, you can access the Management Interface of the backup SonicWALL at the primary SonicWALL LAN IP Address or at the backup SonicWALL LAN IP Address. When the primary SonicWALL restarts after a failure, it is accessible using the third IP address created during configuration. If preempt mode is enabled, the primary SonicWALL becomes the active firewall and the backup firewall returns to Idle status.
- E-mail Alerts Indicating Status Change** - If you have configured the primary SonicWALL to send E-mail alerts, you receive alert e-mails when there is a change in the status of the Hardware Failover pair. For example, when the backup SonicWALL takes over for the primary after a failure, an e-mail alert is sent indicating that the backup has transitioned from Idle to Active. If the primary SonicWALL subsequently resumes operation after that failure, and Preempt Mode has been enabled, the primary SonicWALL takes over and another e-mail alert is sent to the administrator indicating that the primary has preempted the backup.
- View Log** - The SonicWALL also maintains an event log that displays the Hardware Failover events in addition to other status messages and possible security threats. This log may be viewed with a browser using the SonicWALL Management Interface or it may be automatically sent to the administrator's E-mail address. To view the SonicWALL log, click Log on the left side of the management interface.

PART
12

Security Services

Managing SonicWALL Security Services

SonicWALL Security Services

SonicWALL, Inc. offers a variety of subscription-based security services to provide layered security for your network. SonicWALL security services are designed to integrate seamlessly into your network to provide complete protection.

The following subscription-based security services are listed in **Security Services** on the SonicWALL security appliance's management interface:

- SonicWALL Content Filtering Service
- SonicWALL Network Anti-Virus
- SonicWALL Gateway Anti-Virus*
- SonicWALL Intrusion Prevention Service*
- SonicWALL Anti-Spyware*
- SonicWALL E-Mail Filter**
- SonicWALL Global Security Client

**Included as part of the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service unified threat management solution.*

***Included with SonicWALL Network Anti-Virus.*



Tip: After you register your SonicWALL security appliance, you can try FREE TRIAL versions of SonicWALL Content Filtering Service, SonicWALL Network Anti-Virus, SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service, and SonicWALL Anti-Spyware.

You can activate and manage SonicWALL security services directly from the SonicWALL management interface or from <https://www.mySonicWALL.com>.



Note: For more information on SonicWALL security services, please visit <http://www.sonicwall.com>.



Note: Complete product documentation for SonicWALL security services are available on the SonicWALL documentation Web site <http://www.sonicwall.com/support/documentation.html>.

Security Services Summary

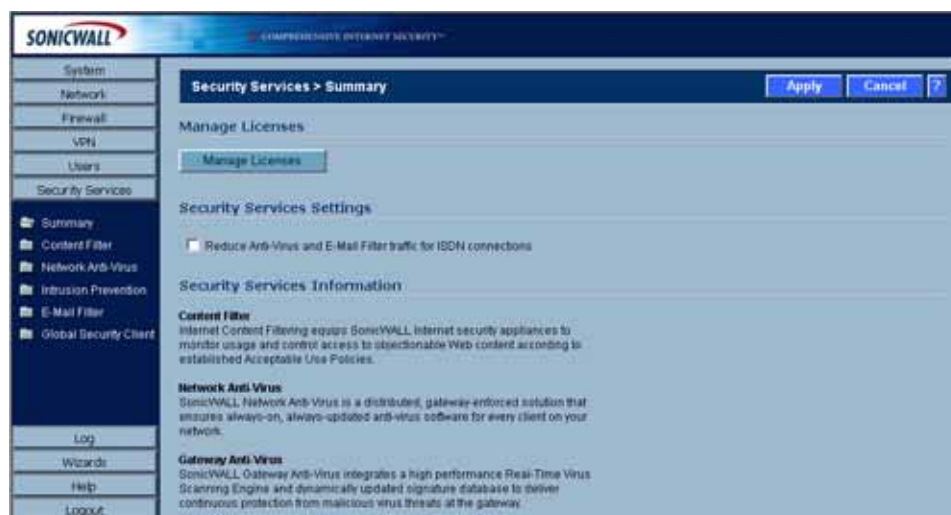
The **Security Services > Summary** page lists the available SonicWALL security services and upgrades for your SonicWALL security appliance and provides access to mySonicWALL.com for activating services using Activation Keys.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Antivirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Licensed		Renew		07 Apr 2006
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

A list of currently available services is displayed in the **Security Services Summary** table. Subscribed services are displayed with **Licensed** in the **Status** column. The service expiration date is displayed in the **Expiration** column. If the service is limited to a number of users, the number is displayed in the **Count** column. If the service is not licensed, **Not Licensed** is displayed in the **Status** column. If the service license has expired, **Expired** is displayed in the Status column.

When you access your mySonicWALL.com account from this page in the SonicWALL management interface, the **Security Services Summary** table changes to the **Manage Services Online** table. This table provides an updated status of your security services and allows you to activate FREE TRIAL versions, and activate or renew security services licenses using Activation Keys.

If your SonicWALL security appliance is not registered, the **Security Services > Summary** page does not include the **Services Summary** table. Your SonicWALL security appliance must be registered to display the **Services Summary** table.



mySonicWALL.com

To activate SonicWALL Security Services, you need to have a mySonicWALL.com account and your SonicWALL security appliance must be registered. Creating a mySonicWALL.com account is easy and free. You can create a mySonicWALL.com account directly from the SonicWALL management interface. Simply complete an online registration form. Once your account is created, you can register SonicWALL security appliances and activate SonicWALL Security Services associated with the SonicWALL security appliance.

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 security appliance
- Try free trials of SonicWALL security services
- Purchase/Activate SonicWALL security service licenses
- Receive SonicWALL firmware and security service updates and alerts
- Manage your SonicWALL security services
- Access SonicWALL Technical Support

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.

Managing Security Services Online

Clicking the **Manage Licenses** button displays the **mySonicWALL.com Login** page for accessing your MySonicWALL.com account licensing information.

Enter your mySonicWALL.com username and password in the **User Name** and **Password** fields, and then click **Submit**. The **System > Licenses** page is displayed with the **Manage Services Online** table.

The information in the **Manage Services Online** table is updated from your mysSonicWALL.com account.

System > Licenses					
Manage Services Online					
Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Antivirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Licensed		Renew		07 Apr 2006
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

If you are already connected to your mysonicwall.com account from the management interface, the **Manage Services Online** table is displayed.

Security Services Settings

- **Synchronize** - Click **Synchronize** to update the licensing and subscription information on the SonicWALL security appliance from your mysonicwall.com account.
- **Reduce Anti-Virus and E-mail Filter traffic for ISDN connections** - Selecting this feature enables the SonicWALL Anti-Virus to only check daily (every 24 hours) for updates and reduces the frequency of outbound traffic for users who do not have an “always on” Internet connection.

Security Services Information

This section includes a brief overview of services available for your SonicWALL security appliance.

Security Services Information
<p>Content Filter Internet Content Filtering equips SonicWALL Internet security appliances to monitor usage and control access to objectionable Web content according to established Acceptable Use Policies.</p>
<p>Network Anti-Virus SonicWALL Network Anti-Virus is a distributed, gateway-enforced solution that ensures always-on, always-updated anti-virus software for every client on your network.</p>
<p>Gateway Anti-Virus SonicWALL Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.</p>
<p>Intrusion Prevention SonicWALL Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. In addition, SonicWALL Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.</p>
<p>E-Mail Filter SonicWALL E-mail Filter enables custom rule configuration for filtering potential virus carrying e-mail attachments.</p>

Update Signature Manually

The Manual Signature Update feature is intended for networks where reliable, broadband Internet connectivity is either not possible or not desirable (for security reasons).

The Manual Signature Update feature provides a method to update the latest signatures at the network administrator's discretion. The network administrator first downloads the signatures from <http://www.mysonicwall.com> to a separate computer, a USB drive, or other media. Then the network administrator uploads the signatures to the SonicWALL security appliance.

The same signature update file can be used to all SonicWALL security appliances that meet the following requirements:

- Devices that are registered to the same mysonicwall.com account
- Devices that belong to the same class of SonicWALL security appliances. There are two classes of SonicWALL security appliances:
 - ◆ The SonicWALL TZ series and the SonicWALL PRO 1260
 - ◆ The SonicWALL PRO series except for the SonicWALL PRO 1260

To manually update signature files, complete the following steps:

- 1 On the **Security Services > Summary** page, scroll to the **Update Signatures Manually** heading at the bottom of the page. Note the Signature File ID for the device

The screenshot shows the SonicWALL Security Services Summary page. The left sidebar contains a navigation menu with the following items: System, Network, Firewall, VPN, Users, Security Services, Summary, Content Filter, Network Anti-Virus, Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware, E-Mail Filter, Log, Wizards, Help, and Logout. The main content area is titled 'COMPREHENSIVE INTERNET SECURITY™' and contains the following sections:

- System:** SonicWALL Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.
- Anti-Spyware:** SonicWALL Anti-Spyware prevents malicious spyware from infecting networks by blocking spyware installation at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- Intrusion Prevention:** SonicWALL Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. In addition, SonicWALL Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.
- E-Mail Filter:** SonicWALL E-mail Filter enables custom rule configuration for filtering potential virus carrying e-mail attachments.

At the bottom of the page, there is a section titled 'Update signatures manually' which includes a text input field for 'Signature File ID' containing the value '2'. Below this field is a paragraph of text: 'If you work in a closed environment or prefer to update AV signatures manually, please download signature updates from mySonicWALL.com to your disk, then import the file.' Below the text is a button labeled 'Import Signatures'.

- 2 Log on to <http://www.mysonicwall.com> using the mysonicwall.com account that was used to register the SonicWALL security appliance.



Note: The signature file can only be used on SonicWALL security appliances that are registered to the mysonicwall.com account that downloaded the signature file.

- 3 Click on **Download Signatures** under the **Downloads** heading.

The screenshot shows the SonicWall mySonicWALL 3.6.11.0 interface. The user is logged in as 'teSt'. The main heading is 'Download Signature Files'. Below this, there is a note: 'Download Signature Files based on the Signature File Id for your Product. This feature is available only when running SonicOS Enhanced version 3.2 or newer.' There are two dropdown menus: 'Signature ID:' with a value of '3' and 'Applicable Products:' with a list of 'PRO 1260', 'PRO 2040', and 'PRO 4060'. Under the heading 'Available Download', there is a link: 'Click here to download the Signature File'. The left navigation menu includes: Home, My Products, My Account, Personal Info, Preferences, My Orders, View Cart, Auto-Renewal, Co termination, Order History, Reports, Downloads, Download Center, My Downloads, Download Signatures, Support, Feedback, Service Requests, Forum, My Training, My Promotions, and Quick Register.

- 4 In the pull down window next to **Signature ID:**, select the appropriate SFID for your SonicWALL security appliance.

- 5 Download the signature update file by clicking on **Click here to download the Signature file**.



Note: *The remaining steps can be performed while disconnected from the Internet.*

- 6 Return to the Security Services > Summary page on the SonicWALL security appliance GUI.
- 7 Click on the **Import Signatures** box.
- 8 In pop-up window that appears, click the **browse** button, and navigate to the location of the signature update file.
- 9 Click **Import**. The signatures are uploaded for the security services that are enabled on the SonicWALL security appliance.

Activating Security Services

To activate a SonicWALL Security Service FREE TRAIL MIX or activate a license using an Activation Key, refer to the specific SonicWALL Security Service chapter in this guide.

Configuring SonicWALL Content Filtering Service

Security Services > Content Filter

The **Security Services > Content Filter** page allows you to configure the SonicWALL Restrict Web Features and Trusted Domains settings, which are included with SonicOS Enhanced. You can activate and configure SonicWALL Content Filtering Service (SonicWALL CFS) as well as two third-party Content Filtering products from the **Security Services > Content Filter** page.

The screenshot displays the 'Security Services > Content Filtering' configuration window. At the top, there are 'Apply', 'Cancel', and '?' buttons. The 'Content Filter Status' section indicates the server is ready and the subscription expires on 05/08/2005. Below this, there is a link for reporting incorrect ratings. The 'Content Filter Type' section shows 'SonicWALL CFS' selected in a dropdown menu, with a 'Configure...' button next to it. A note instructs users to enforce the service per zone from the 'Network > Zones' page. The 'Restrict Web Features' section includes checkboxes for 'ActiveX', 'Java', 'Cookies', 'Access to HTTP Proxy Servers', and 'Known Fraudulent Certificates'. The 'Trusted Domains' section has a checkbox for 'Do not block Java / ActiveX / Cookies to Trusted Domain sites'. At the bottom, there is a table with a 'Name' column and a 'Configure' button, currently showing 'No Entries' with 'Add' and 'Delete All' buttons below it.



SonicWALL Content Filtering Service is a subscription service upgrade. You can try a FREE TRIAL of SonicWALL directly from your SonicWALL management interface. See "Activating a SonicWALL CFS FREE TRIAL" on page 501.



For complete SonicWALL Content Filtering Service documentation, see the SonicWALL Content Filtering Service Standard or Premium Administrator's Guide available at <http://www.sonicwall.com/services/documentation.html>.

SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration

overhead. SonicWALL CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of SonicWALL CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWALL co-location facilities. A rating is returned to the SonicWALL security appliance and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWALL security appliance informing the user that the site has been blocked according to policy.

With SonicWALL CFS, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. SonicWALL CFS automatically updates the filters, making maintenance substantially simpler and less time consuming.

SonicWALL CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL security appliance, a customized message is displayed on the user's screen. SonicWALL security appliance can also be configured to log attempts to access sites on the SonicWALL Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

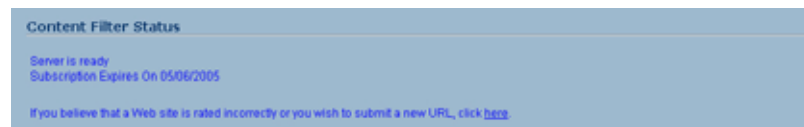
- **SonicWALL CFS Standard** blocks 12 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Standard runs on SonicOS Standard 2.0 (or higher).
- **SonicWALL CFS Premium** blocks 56 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Premium provides network administrators with greater control by automatically and transparently enforces acceptable use policies. It gives administrators the flexibility to enforce custom content filtering policies for groups of users on the network. For example, a school can create one policy for teachers and another for students. SonicWALL CFS Premium Productivity Edition and the SonicWALL CFS Premium Government/Education Edition run on SonicOS Standard 2.1 (or higher) as well as SonicOS Enhanced 2.0 (or higher).



Cross Reference: For complete SonicWALL Content Filtering Service documentation, see the *SonicWALL Content Filtering Service Administrator's Guide* available at <http://www.sonicwall.com/services/documentation.html>

Content Filter Status

If SonicWALL CFS is activated, the **Content Filter Status** section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.



You can also access the **SonicWALL CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.**

If SonicWALL CFS is not activated, you must activate it. If you do not have an Activation Key, you must purchase SonicWALL CFS from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).

Activating SonicWALL CFS

If you have an Activation Key for your SonicWALL CFS subscription, follow these steps to activate SonicWALL CFS:



Alert: You must have a mySonicWALL.com account and your SonicWALL security appliance must be registered to activate SonicWALL Network Anti-Virus.

- 1 Click the **SonicWALL Content Filtering Subscription** link on the **Security Services > Content Filtering** page. The **mySonicWALL.com Login** page is displayed.
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.
- 3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL CFS subscription is activated on your SonicWALL.
- 4 If you activated SonicWALL CFS at mySonicWALL.com, the SonicWALL CFS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL.

Activating a SonicWALL CFS FREE TRIAL

You can try a FREE TRIAL of SonicWALL CFS by following these steps:

- 1 Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- 3 Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL CFS trial subscription is activated on your SonicWALL.
- 4 Select **Security Services > Content Filter** to display the Content Filter page for configuring your SonicWALL Content Filtering Service settings.

Content Filter Type

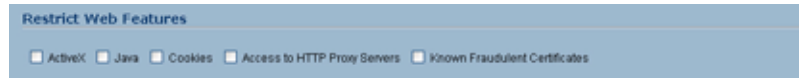
There are three types of content filtering available on the SonicWALL security appliance. These options are available from the **Content Filter Type** menu.

- **SonicWALL CFS** - Selecting **SonicWALL CFS** as the **Content Filter Type** allows you to use the SonicWALL Content Filtering Service that is available as an upgrade. You can obtain more information about SonicWALL Content Filtering Service at <http://www.sonicwall.com/products/cfs.html>
- **N2H2** - N2H2 is a third party content filter software package supported by SonicWALL security appliance.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list supported by SonicWALL security appliance.

Clicking the **Network > Zones** link in **Note: Enforce the Content Filtering per zone from the Network > Zone page**, displays the **Network > Zones** page for enabling SonicWALL Content Filtering Service on network zones.

Restrict Web Features

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



Restrict Web Features are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.
- **Known Fraudulent Certificates** - Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL security appliance blocks the Web content and the files that use these fraudulent certificates. Known fraudulent certificates blocked by SonicWALL security appliance include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

Trusted Domains

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features**.



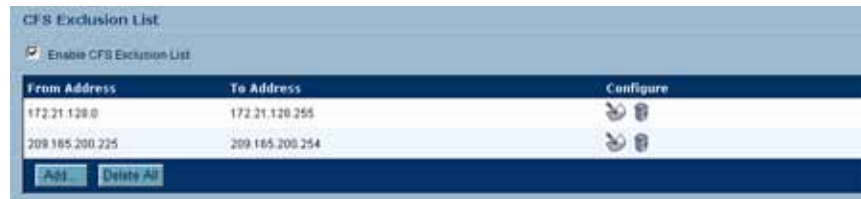
If you trust content on specific domains and want them exempt from **Restrict Web Features**, follow these steps to add them:

- 1 Check the **Don't block Java/ActiveX/Cookies to Trusted Domains** checkbox.
- 2 Click **Add**. The **Add Trusted Domain Entry** window is displayed.
- 3 Enter the trusted domain name in the **Domain Name** field.
- 4 Click **OK**. The trusted domain entry is added to the Trusted Domain table.

To keep the trusted domain entries but enable Restrict Web Features, uncheck **Don't block Java/ActiveX/Cookies to Trusted Domains**. To delete an individual trusted domain, click on the **Trashcan** icon for the entry. To delete all trusted domains, click **Delete All**. To edit a trusted domain entry, click the **Notepad** icon.

CFS Exclusion List

IP address ranges can be manually added to the CFS Exclusion List.



To manually add a range of IP addresses to the CFS Exclusion List, follow these steps:

- 1 Check the **Enable CFS Exclusion List** checkbox.
- 2 Click **Add**. The **Add CFS Range Entry** window is displayed.
- 3 Enter the first IP address in the range in the **IP Address From:** field and the last address in the **IP Address To:** field.
- 4 Click **OK**. The IP address range is added to the CFS Exclusion List.

To keep the CFS Exclusion List entries but temporarily allow access to these sites, uncheck the **Enable CFS Exclusion List** checkbox. To delete an individual trusted domain, click on the **Trashcan** icon for the entry. To delete all trusted domains, click **Delete All**. To edit a trusted domain entry, click the **Notepad** icon.

Message to Display when Blocking

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



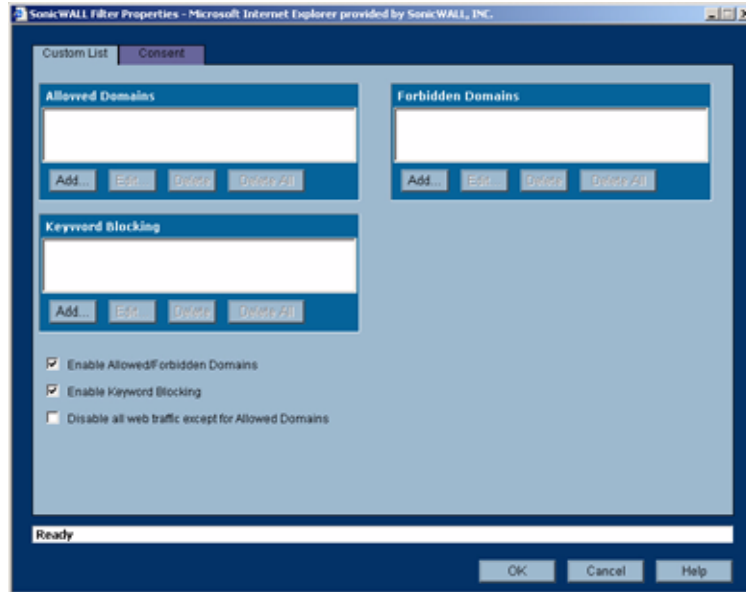
Configuring SonicWALL Filter Properties

You can customize SonicWALL filter features included with SonicOS from the **SonicWALL Filter Properties** window. To display the **SonicWALL Filter Properties** window, select **SonicWALL CFS** from the **Content Filter Type** menu on the **Security Services > Content Filter** page, and click **Configure**. The **SonicWALL Filter Properties** window is displayed.

Custom List

You can customize your URL list to include **Allowed Domains** and **Forbidden Domains**. By customizing your URL list, you can include specific domains to be accessed, blocked, and include

specific keywords to block sites. Select the check box **Enable Allowed/Forbidden Domains** to activate this feature.



To allow access to a Web site that is blocked by the Content Filter List, click **Add**, and enter the host name, such as “www.ok-site.com”, into the Allowed Domains fields. 256 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the **Content Filter Service**, click **Add**, and enter the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 256 entries can be added to the **Forbidden Domains** list.



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

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.

Enable Keyword Blocking

To enable blocking using **Keywords**, select **Enable Keyword Blocking**. Click **Add**, and enter the keyword to block in the **Add Keyword** field, and click **OK**.

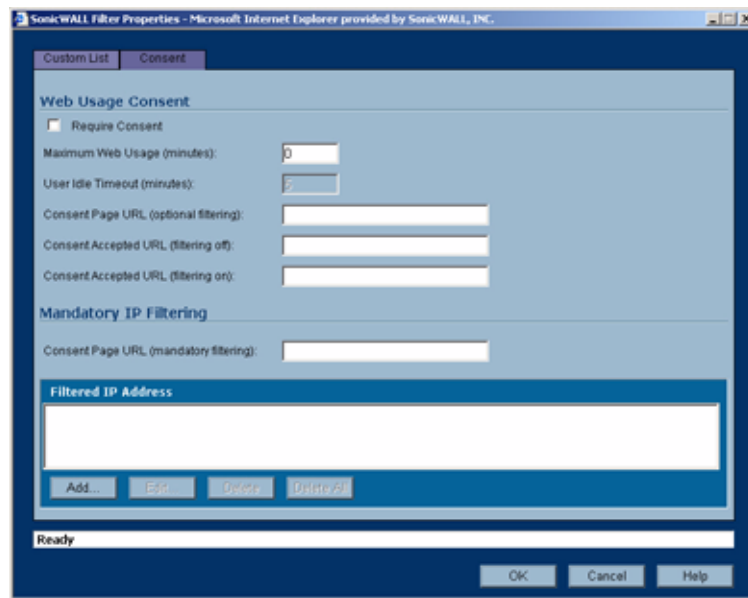
To remove a keyword, select it from the list and click **Delete**. Once the keyword has been removed, the **Status** bar displays **Ready**.

Disable all Web traffic except for Allowed Domains

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

Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed.



To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes)** - In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL security appliance can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.
- **User Idle Timeout (minutes)** - After a period of Web browser inactivity, the SonicWALL security appliance requires the user to agree to the terms outlined in the Consent page before accessing the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the User Idle Timeout section.
- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the SonicWALL security appliance, which, when selected, tell the SonicWALL security appliance 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 network.
- **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 network.

Mandatory Filtered IP Addresses

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

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL security appliance that tells the device that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

Adding a New Address

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

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

Activating SonicWALL Network Anti-Virus

Security Services > Anti-Virus

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses don't have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWALL Network Anti-Virus prevents occurrences like these and offers a new approach to virus protection. SonicWALL security appliance constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the SonicWALL security appliance restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.



Alert: *You must purchase an Anti-Virus subscription to enforce Anti-Virus through the SonicWALL security appliance's Management Interface.*

Activating SonicWALL Network Anti-Virus

If Sonic WALL Network Anti-Virus is not activated, you must activate it.



If you do not have an Activation Key, you must purchase SonicWALL Network Anti-Virus from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).



Cross Reference: For complete SonicWALL Network Anti-Virus documentation, see the SonicWALL Network Anti-Virus Administrator's Guide available at <http://www.sonicwall.com/support/documentation.html>

If you have an Activation Key for your SonicWALL Network Anti-Virus subscription, follow these steps to activate SonicWALL Network Anti-Virus:



Alert: You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Network Anti-Virus.

- 1 Click the **SonicWALL Network Anti-Virus Subscription** link on the **Security Services > Anti-Virus** page. The **mySonicWALL.com Login** page is displayed.
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Network Anti-Virus Subscription** link.

- Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL security appliance.



- If you activated SonicWALL Network Anti-Virus at www.mySonicWALL.com, the SonicWALL Network Anti-Virus activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

Activating a SonicWALL Network Anti-Virus FREE TRIAL

You can try a FREE TRIAL of SonicWALL Network Anti-Virus by following these steps:

- Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
- Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL security appliance.
- Select **Security Services > Anti-Virus** to display the Anti-Virus page for configuring your SonicWALL Network Anti-Virus settings.



Configuring Network Anti-Virus Service

Anti-Virus Policies

The following features are available in the Anti-Virus Policies section:

- **Disable policing from Trusted to Public** - Unchecked, this option enforces anti-virus policies on computers located on Trusted Zones. Choosing this option allows computers on a trusted zone (such as a LAN) to access computers on public zones (such as DMZ), even if anti-virus software is not installed on the LAN computers.
- **Days before forcing update** - This feature defines the maximum number of days may access the Internet before the SonicWALL requires the latest virus date files to be downloaded.
- **Force update on alert** - SonicWALL, Inc. broadcasts virus alerts to all SonicWALL appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the Maximum number of days allowed before forcing update selection. In addition, every virus alert is logged, and an alert message is sent to the administrator.
 - ♦ **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.
 - ♦ **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread.
 - ♦ **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence.

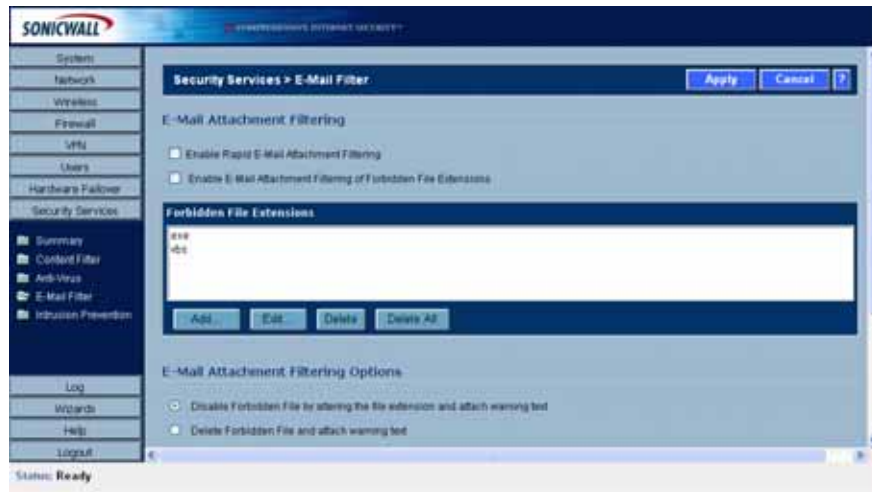
Anti-Virus Enforcement

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

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

Security Services > E-mail Filter

The **E-Mail Filter** allows the administrator to selectively delete or disable inbound e-mail attachments as they pass through the SonicWALL security appliance. This feature provides control over executable files and scripts, and applications sent as e-mail attachments.



Note: E-Mail Filter is included with the Network Anti-Virus service subscription. When you activate SonicWALL Network Anti-Virus, E-Mail Filter is automatically activated.



Cross Reference: For complete SonicWALL Network Anti-Virus documentation including E-Mail Filter, see the SonicWALL Network Anti-Virus Administrator's Guide available at <http://www.sonicwall.com/support/documentation.html>.

Managing SonicWALL Gateway Anti-Virus Service

SonicWALL's Unified Threat Management Solution

SonicWALL Gateway Anti-Virus is included in SonicWALL's unified threat management solution that integrates Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service into an intelligent, real-time network security solution. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers unified threat management directly on the SonicWALL security appliance gateway.

Utilizing a configurable, high-performance deep packet inspection architecture, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service secures the network from the core to the perimeter against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans, and software vulnerabilities, such as buffer overflows, as well as peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code. Because new threats emerge daily and are often unpredictable, the deep packet inspection architecture is constantly updated to deliver the highest protection against an ever-changing threat landscape.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service inspects e-mail, Web traffic, file transfers, a multitude of stream-based protocols, as well as instant messaging and peer-to-peer applications. Because files containing malicious code, viruses and worms can be compressed and therefore inaccessible to conventional solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis. Supported compression formats include ZIP, Deflate and GZIP. As an added layer of security, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection not only against external threats, but also against those originating inside the network.

Unlike other threat management solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service has the capacity to analyze files of any size in real-time without the need to add expensive hardware drive or extra memory. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes a pro-active alerting mechanism that notifies network administrators when a new threat is discovered. Granular policy tools and an intuitive user interface enable administrators to configure a custom set of detection or prevention policies tailored to their specific network environment. Network administrator's can create global policies between security

zones and group attacks by priority, simplifying deployment and management across a distributed network.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Features

- **Integrated Deep Packet Inspection Technology** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service features a configurable, high-performance Deep Packet Inspection architecture that uses parallel searching algorithms up through the application layer to deliver complete application layer, Web and e-mail attack prevention. Parallel processing reduces the impact on the processor and maximizes available memory for exceptional performance on SonicWALL appliances.
- **Spyware Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service prevents malicious spyware from infecting networks by blocking spyware installations at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- **Real-Time AV Gateway Scanning** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent file-based virus and malicious code prevention by scanning in real-time for decompressed and compressed files containing viruses, Trojans, worms and other Internet threats over the corporate network.
- **Powerful Intrusion Prevention** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers complete protection from a comprehensive array of network-based application layer threats by scanning packet payloads for worms, Trojans, software vulnerabilities such as buffer overflows, peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.
- **Scalability and Performance** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes a per packet scanning engine, allowing the SonicWALL unified threat management solution to handle unlimited file size and virtually unlimited concurrent downloads.
- **Day Zero Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service ensures fast time-to-protection by employing a dynamically updated database of signatures created by a combination of SonicWALL's SonicAlert Team and third-party sources.
- **Extensive Signature List** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes an extensive database of thousands of attack and vulnerability signatures written to detect and prevent intrusions, viruses, spyware, worms, Trojans, application exploits, and malicious applications.
- **Distributed Enforcement Architecture** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes a distributed enforcement architecture to deliver automated signature updates, providing real-time protection from emerging threats and lowering total cost of ownership.
- **Inter-zone Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection against malicious code and other threats originating from the Internet or from internal sources. Administrators have the ability to enforce intrusion prevention and anti-virus scanning not only between each network zone and the Internet, but also between internal network zones for added security (Requires SonicOS Enhanced).
- **Advanced File Decompression Technology** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses, Trojans, worms and malware. Supported compression formats include: ZIP, Deflate and GZIP.
- **File-Based Scanning Protocol Support** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers protection for high threat viruses and malware by inspecting the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NETBIOS, instant messaging and peer-to-peer applications, and dozens of

- other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Application Control** - SonicWALL GAV/IPS provides the ability to prevent instant messaging and peer-to-peer file sharing programs from operating through the firewall, closing a potential back door that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
 - **Simplified Deployment and Management** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service allows network administrators to create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.
 - **Granular Management** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides an intuitive user interface and granular policy tools, allowing network administrators to configure a custom set of detection or prevention policies for their specific network environment and reduce the number of false policies while identifying immediate threats.
 - **Logging and Reporting** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service offers comprehensive logging of all intrusion attempts with the ability to filter logs based on priority level, enabling administrators to highlight high priority attacks. Granular reporting based on attack source, destination and type of intrusion is available through SonicWALL ViewPoint and Global Management System.

SonicWALL GAV Enhancements in SonicOS 3.2 Enhanced

The following enhancements have been added to GAV for SonicOS 3.2 Enhanced:

- **HTTP Clientless Notification** - When GAV detects an incoming threat from an HTTP server, GAV redirects users to a page notifying them that the HTTP request was blocked because a threat was detected. Previously, users would only see a blank screen and generally would attempt to re-access the HTTP page.
- **UUdecoding Support** - GAV can now scan emails that are uuencoded for threats.
- **Per Protocol Policy Settings** - GAV administrators can now configure transfer restrictions for individual protocols. Restricting the transfer of password protected zip files, packed executables, and Microsoft Office files containing macros can be configured on a per-protocol basis.

SonicWALL Gateway Anti-Virus Overview

SonicWALL GAV delivers real-time virus protection directly on the SonicWALL security appliance by using SonicWALL's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWALL gateway. Building on SonicWALL's reassembly-free architecture, SonicWALL GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWALL GAV delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

SonicWALL GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based

protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

SonicWALL GAV delivers real-time virus protection directly on the SonicWALL security appliance by using SonicWALL's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWALL gateway. Building on SonicWALL's reassembly-free architecture, SonicWALL GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

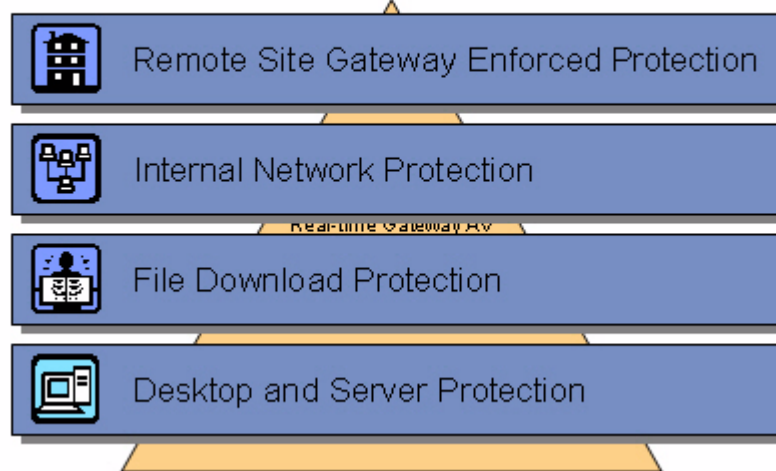
SonicWALL GAV delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

SonicWALL GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

SonicWALL GAV Multi-Layered Approach

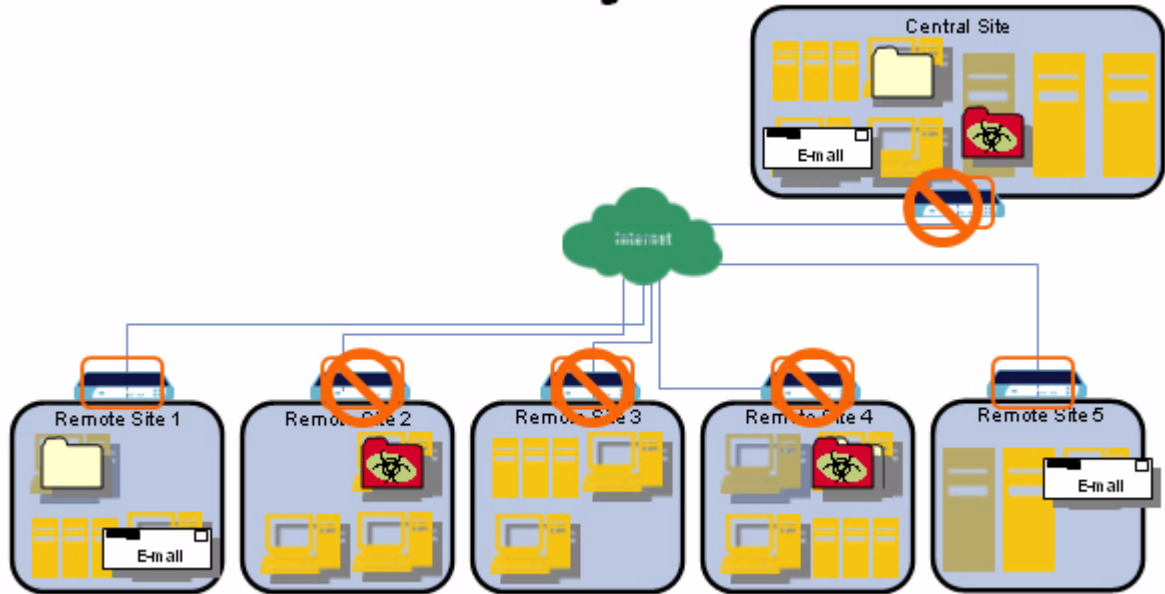
SonicWALL GAV delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, the network, and at remote sites. SonicWALL GAV enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network.

SonicWALL Multi-layered Approach



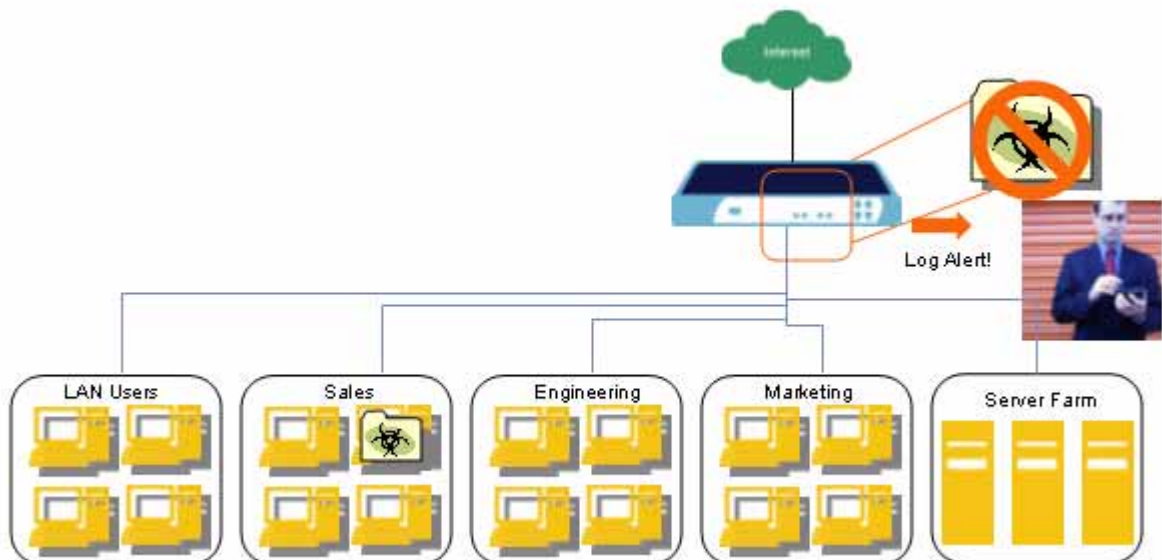
Remote Site Protection

- 1 Users send typical e-mail and files between remote sites and the corporate office.
- 2 SonicWALL GAV scans and analyses files and e-mail messages on the SonicWALL security appliance.
- 3 Viruses are found and blocked before infecting remote desktop.
- 4 Virus is logged and alert is sent to administrator.



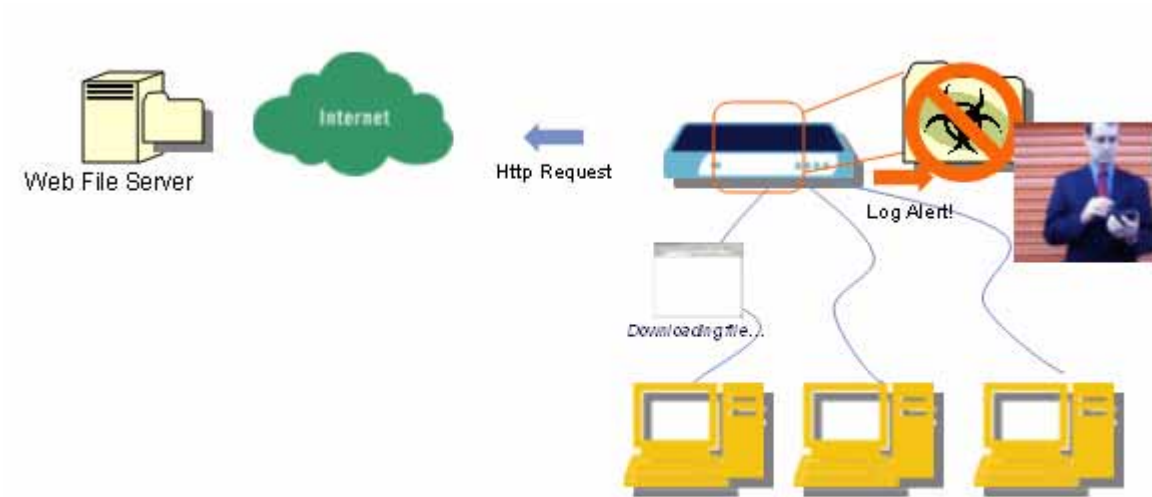
Internal Network Protection

- 1 Internal user contracts a virus and releases it internally.
- 2 All files are scanned at the gateway before being received by other network users.
- 3 If virus is found, file is discarded.
- 4 Virus is logged and alert is sent to administrator.



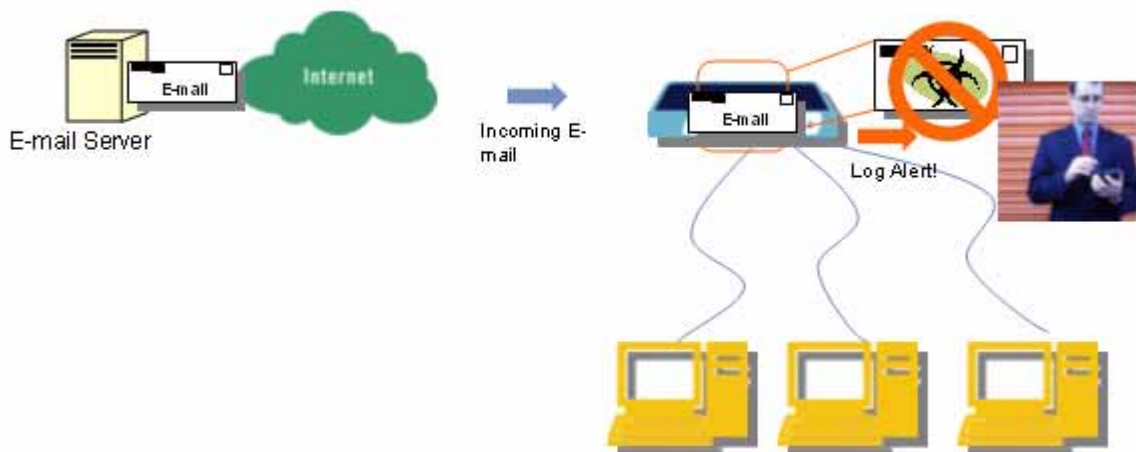
HTTP File Downloads

- 1 Client makes a request to download a file from the Web.
- 2 File is downloaded through the Internet.
- 3 File is analysed the SonicWALL GAV engine for malicious code and viruses
- 4 If virus found, file discarded.
- 5 Virus is logged and alert sent to administrator.



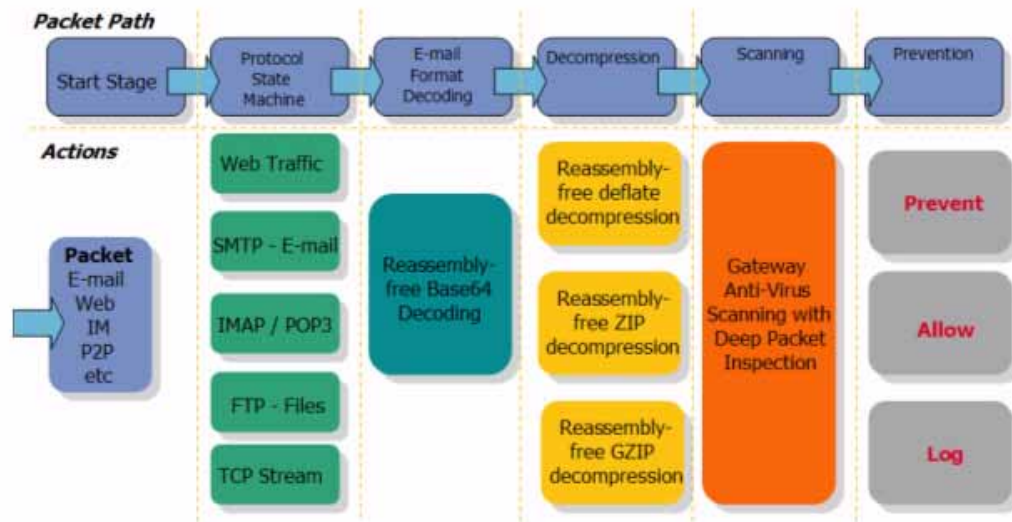
Server Protection

- 1 Outside user sends an incoming e-mail.
- 2 E-mail is analysed the SonicWALL GAV engine for malicious code and viruses before received by e-mail server.
- 3 If virus found, threat prevented.
- 4 E-mail is returned to sender, virus is logged, and alert sent to administrator.



SonicWALL GAV Architecture

SonicWALL GAV is based on SonicWALL's high performance DPIv2.0 engine (Deep Packet Inspection version 2.0) engine, which performs all scanning directly on the SonicWALL security appliance. SonicWALL GAV includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses and malware. The SonicWALL GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because SonicWALL's GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding and ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Reassembly free virus scanning functionality of the SonicWALL GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.



Building on SonicWALL's reassembly-free architecture, GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. SonicWALL GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. SonicWALL GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Anti-Spyware** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface.

Because SonicWALL Gateway Anti-Virus is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the Security Services > Intrusion Prevention page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need the following:

- **SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license.** You need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).
- **mySonicWALL.com account.** Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form from your SonicWALL security appliance management interface. Your mySonicWALL.com account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser.
- **Registered SonicWALL security appliance with active Internet connection.** Registering your SonicWALL security appliance is a simple procedure done directly from the management interface.
- **SonicOS Standard 3.1 or SonicOS Enhanced 3.1.** Your SonicWALL security appliance must be running SonicOS Standard 3.1 or SonicOS Enhanced 3.1 for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.



Tip: If your SonicWALL security appliance is connected to the Internet and registered at mySonicWALL.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.



Note: Administrator Guides for SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service are available on the SonicWALL documentation Web site: <http://www.sonicwall.com/support/documentation.html>

Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL security appliance management interface.



Note: If you already have a mysonicWALL.com account, go to [“Registering Your SonicWALL Security Appliance” on page 522](#).

- 1 Log into the SonicWALL security appliance management interface.
- 2 If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- 3 On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered**. Click here to **Register** your SonicWALL.



- 4 In the mySonicWALL.com Login page, click the [here](#) link in **If you do not have a mySonicWALL account, please click here to create one**.



- 5 In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (*) are required fields.



Note: Remember your username and password to access your mySonicWALL.com account.

- 6 Click **Submit** after completing the **MySonicWALL Account** form.
- 7 When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.

Congratulations. Your mySonicWALL.com account is activated.

Now you need to log into mySonicWALL.com to register your SonicWALL security appliance.



Note: mySonicWALL.com registration information is not sold or shared with any other company.

Registering Your SonicWALL Security Appliance

- 1 Log into the SonicWALL security appliance management interface.
 - 2 If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
 - 3 On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **mySonicWALL.com Login** page is displayed.
 - 4 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
 - 5 The next several pages inform you about the free trials available to you for SonicWALL's Security Services:
 - ♦ **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
 - ♦ **Network Anti Virus** - Provides desktop and server anti-virus protection with software running on each computer.
 - ♦ **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
 - ♦ **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
 - ♦ **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.
- Click **Continue** on each page.



Note: Clicking on the **Continue** button does not activate the **FREE TRIAL** versions of these SonicWALL Security Services.

- 6 At the top of the **Product Survey** page, Enter a "friendly name" for your SonicWALL content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
- 7 Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
- 8 Click **Submit**.
- 9 When the mySonicWALL.com server has finished processing your registration, a page is displayed informing you that the SonicWALL security appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License

Because SonicWALL Anti-Spyware is part of SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your SonicWALL security appliance.

If you do not have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you have an Activation Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- 1 On the **Security Services > Gateway Anti-Virus** page, click the **SonicWALL Gateway Anti-Virus Subscription** link. The **mySonicWALL.com Login** page is displayed.
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears.
- 3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- 4 Type in the Activation Key in the **New License Key** field and click **Submit**. SonicWALL Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Antivirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Free Trial		Renew		07 Apr 2005
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

You can apply the following activation keys:

ANTI SPYWARE 1 YR BUNDLE ASMUYZF8
 SNWL GAV 1 YR BUNDLE (PSP/GAV BUNDLE) GAMUYZF8

- 5 Click on the Anti-Spyware link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- 6 Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.
- 7 Click on the SonicWALL Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- 8 Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

Congratulations! You have activated the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on mySonicWALL.com, the activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

Activating FREE TRIALS

You can try FREE TRIAL versions of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, or SonicWALL Intrusion Prevention Service, perform these steps:

- 1 Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- 3 Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

Setting Up SonicWALL Gateway Anti-Virus Protection

Activating the SonicWALL Gateway Anti-Virus license on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Gateway Anti-Virus to begin protecting your network, you need to perform the following steps:

- 1 Enable SonicWALL Gateway Anti-Virus
- 2 Apply SonicWALL Gateway Anti-Virus Protection to Zones



Note: For complete instructions on setting up SonicWALL Gateway Anti-Virus, refer to the *SonicWALL Gateway Anti-Virus Administrator's Guide* available on the SonicWALL documentation Web site <<http://www.sonicwall.com/support/documentation.html>>.

The **Security Services > Gateway Anti-Virus** page provides the settings for configuring SonicWALL GAV on your SonicWALL security appliance.

Protocols	HTTP	FTP	IMAP	SMTP	POP3	TCP Stream
Enable Inbound Inspection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enable Outbound Inspection				<input checked="" type="checkbox"/>		
Protocol Settings	Settings	Settings	Settings	Settings	Settings	

[Configure Gateway AV Settings](#)

Enabling SonicWALL GAV

You must select **Enable Gateway Anti-Virus** check box in the **Gateway Anti-Virus Global Settings** section to enable SonicWALL GAV on your SonicWALL security appliance. If your SonicWALL security appliance is running SonicOS Enhanced 3.0, you must specify the Zones you want SonicWALL GAV protection on the **Network > Zones** page.



Note: Refer to [“Applying SonicWALL GAV Protection on Zones” on page 526](#) for instructions on applying SonicWALL GAV protection to zones.


Applying SonicWALL GAV Protection on Zones

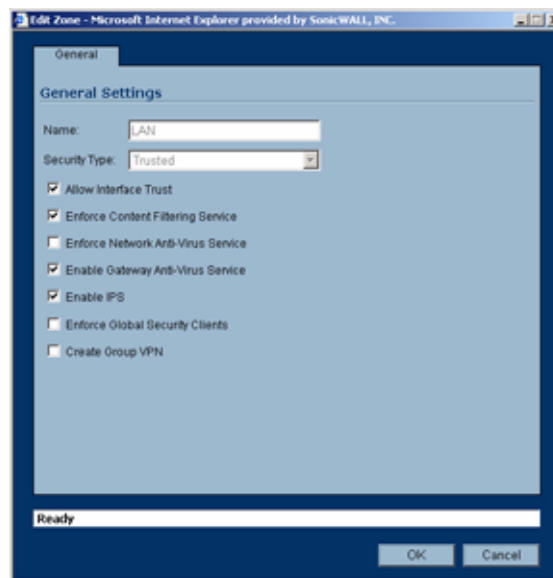
If your SonicWALL security appliance is running SonicOS Enhanced 3.0, you can enforce SonicWALL GAV not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL GAV on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic.

- 1 In the SonicWALL security appliance management interface, select **Network > Zones** or from the **Gateway Anti-Virus Status** section, on the **Security Services > Gateway Anti-Virus** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.



Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	IPS
LAN	Trusted	X0, X3V100	✓	✓	✓	✓	✓
WAN	Untrusted	X1				✓	✓
DMZ	Public	N/A	✓	✓			
VPN	Encrypted	N/A					
MULTICAST	Untrusted	N/A					
WLAN	Wireless	X4					
Accounting	Trusted	X3V20	✓	✓	✓	✓	✓

- 2 In the **Configure** column in the **Zone Settings** table, click the edit icon . The **Edit Zone** window is displayed.



Edit Zone - Microsoft Internet Explorer provided by SonicWALL, INC.

General

General Settings

Name: LAN

Security Type: Trusted

Allow Interface Trust

Enforce Content Filtering Service

Enforce Network Anti-Virus Service

Enable Gateway Anti-Virus Service

Enable IPS

Enforce Global Security Clients

Create Group VPN

Ready

OK Cancel

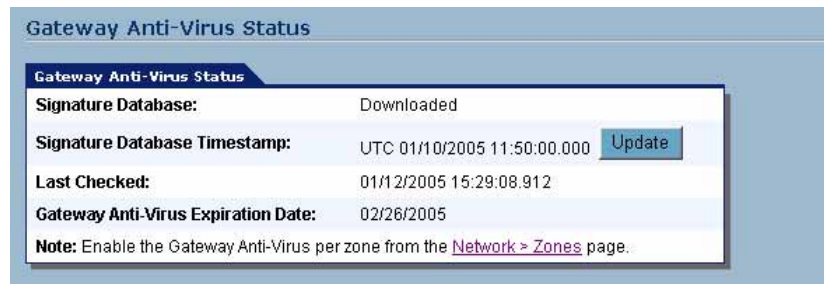
- 3 Click the **Enable Gateway Anti-Virus Service** checkbox. A checkmark appears. To disable Gateway Anti-Virus Service, uncheck the box.
- 4 Click **OK**.



Note: You also enable SonicWALL GAV protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

Viewing SonicWALL GAV Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the SonicWALL signature servers were last checked for the most current database version. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.



The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp** displays the last update to the SonicWALL GAV signature database, not the last update to your SonicWALL security appliance.
- **Last Checked** indicates the last time the SonicWALL security appliance checked the signature database for updates. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the SonicWALL GAV service expires. If your SonicWALL GAV subscription expires, the SonicWALL IPS inspection is stopped and the SonicWALL GAV configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your SonicWALL GAV license to the previously configured state.

If your SonicWALL security appliance you are running SonicOS Standard 3.0 and no interfaces are specified in the **Gateway Anti-Virus Global Settings** section, the message: **Warning: No interfaces have Gateway Anti-Virus enabled** is displayed in the **Gateway Anti-Virus Status** section. You must check the **Enable Gateway Anti-Virus on Interface** and specify the interface(s) you want to apply anti-virus scanning.

If your SonicWALL security appliance you are using SonicOS Enhanced 3.0, the **Gateway Anti-Virus Status** section displays **Note: Enable the Gateway Anti-Virus per zone from the [Network > Zones](#) page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying SonicWALL GAV on Zones.



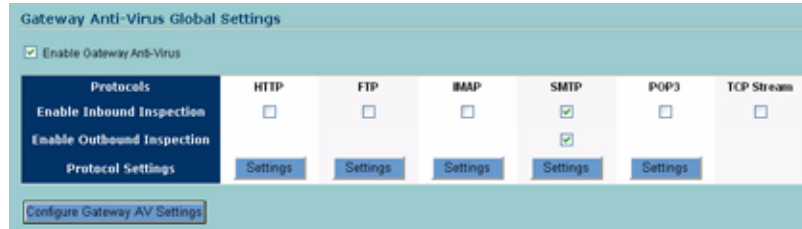
Note: Refer to [“Applying SonicWALL GAV Protection on Zones”](#) on page 526 for instructions on applying SonicWALL GAV protection to zones.

Updating SonicWALL GAV Signatures

By default, the SonicWALL security appliance running SonicWALL GAV automatically checks the SonicWALL signature servers once an hour. There is no need for an administrator to constantly check for new signature updates. You can also manually update your SonicWALL GAV database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

SonicWALL GAV signature updates are secured. The SonicWALL security appliance must first authenticate itself with a pre-shared secret, created during the SonicWALL Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

Specifying Protocol Filtering



Application-level awareness of the type of protocol that is transporting the violation allows SonicWALL GAV to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

By default, SonicWALL GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP** and **POP3** traffic. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

Enabling Inbound Inspection

Within the context of SonicWALL GAV, the **Enable Inbound Inspection** protocol traffic handling refers to the following:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted Zone destined to any Zone.
- Non-SMTP traffic from a Public Zone destined to an Untrusted Zone.
- SMTP traffic initiating from a non-Trusted Zone destined to a Trusted, Wireless, Encrypted, or Public Zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted Zone destined to a Trusted, Wireless, or Encrypted Zone.

The **Enable Inbound Inspection** protocol traffic handling represented as a table:

SMTP Traffic					
From \ To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓	✗	✗
Encrypted	✓	✓	✓	✗	✗
Wireless	✓	✓	✓	✗	✗
Public	✓	✓	✓	✓	✓
Untrusted	✓	✓	✓	✓	✓

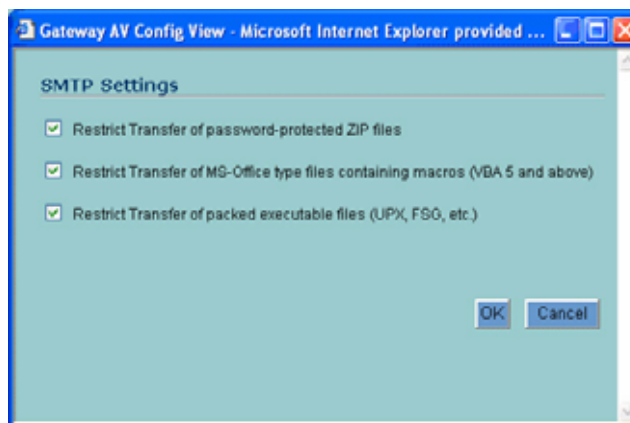
All Other Traffic					
From \ To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓	✓	✓
Encrypted	✓	✓	✓	✓	✓
Wireless	✓	✓	✓	✓	✓
Public	○	○	○	○	✓
Untrusted	○	○	○	○	○

Enabling Outbound SMTP Inspection

The **Enable Outbound Inspection** feature is available for SMTP traffic, such as for a mail server that might be hosted on the DMZ. Enabling outbound inspection for SMTP scans mail that is delivered to the internally hosted SMTP server for viruses.

Restricting File Transfers

For each protocol you can restrict the transfer of files with specific attributes by clicking on the **Settings** button under the protocol in the **Gateway Anti-Virus Global Settings** section.



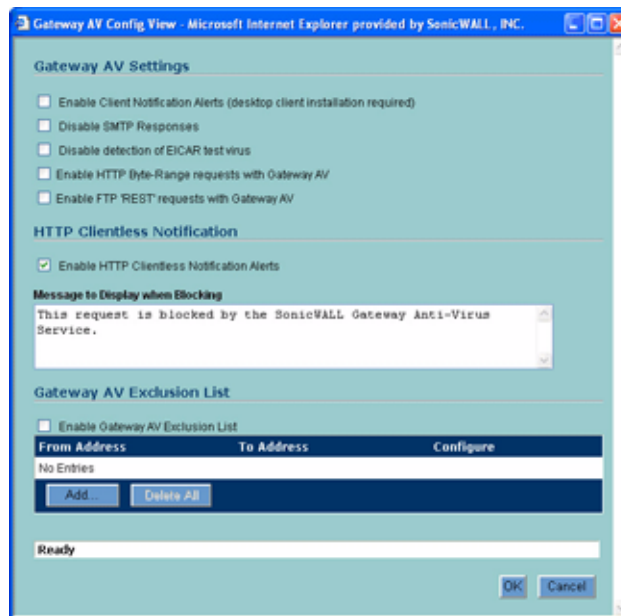
These restrict transfer settings include:

- **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (e.g. HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.

- Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities which compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. SonicWALL Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. additional formats are dynamically added along with SonicWALL GAV signature updates.

Configuring Gateway AV Settings

Clicking the **Configure Gateway AV Settings** button at the bottom of the **Gateway Anti-Virus Global Settings** section displays the **Gateway AV Config View** window, which allows you to configure client notification alerts and create a SonicWALL GAV exclusion list.



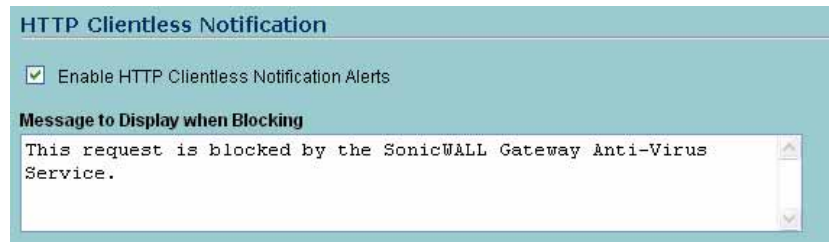
Configuring Client Alerts

If you want clients on your network to receive notifications on their desktop when a HTTP file download is blocked by GAV, check the **Enable Client Notification Alerts (desktop client installation is required)** box. You must install the client software included on the Resource CD for your SonicWALL security appliance for the client to receive these notifications from SonicWALL GAV.

If you want to suppress the sending of e-mail messages (SMTP) to clients from SonicWALL GAV when a virus is detected in an e-mail or attachment, check the **Disable SMTP Responses** box.

Configuring HTTP Clientless Notification

The HTTP Clientless Notification feature notifies users when GAV detects an incoming threat from an HTTP server. To configure this feature, check the **Enable HTTP Clientless Notification Alerts** box and enter a message in the **Message to Display when Blocking** field, as shown below.



HTTP Clientless Notification

Enable HTTP Clientless Notification Alerts

Message to Display when Blocking

This request is blocked by the SonicWALL Gateway Anti-Virus Service.

With this option disabled, when GAV detects an incoming threat from an HTTP server, GAV blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that GAV detected a threat from the HTTP server.

Tip! The HTTP Clientless Notification feature is also available for SonicWALL Anti-Spyware.

Optionally, you can configure the timeout for the HTTP Clientless Notification on the **Security Services > Summary** page under the **Security Services Summary** heading.



Security Services Settings

Synchronize Synchronize licenses with mySonicWALL.com:

Reduce Anti-Virus and E-Mail Filter traffic for ISDN connections

HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware (sec) 300

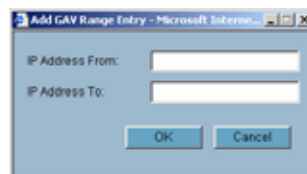
Configuring a SonicWALL GAV Exclusion List

Any IP addresses listed in the exclusion list bypass virus scanning on their traffic. The **Gateway AV Exclusion List** section provides the ability to define a range of IP addresses whose traffic will be excluded from SonicWALL GAV scanning.

Alert! Use caution when specifying exclusions to SonicWALL GAV protection.

To add an IP address range for exclusion, perform these steps:

- 1 Click the **Enable Gateway AV Exclusion List** checkbox to enable the exclusion list.
- 2 Click the **Add** button. The **Add GAV Range Entry** window is displayed.



Add GAV Range Entry - Microsoft Internet Explorer

IP Address From:

IP Address To:

OK Cancel

- 3 Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**. Your IP address range appears in the **Gateway AV Exclusion List** table. Click the edit icon in the **Configure** column to change an entry or click the trashcan icon to delete an entry.
- 4 Click **OK** to exit the **Gateway AV Config View** window.

Viewing SonicWALL GAV Signatures

The **Gateway Anti-Virus Signatures** section allows you to view the contents of the SonicWALL GAV signature database. All the entries displayed in the **Gateway Anti-Virus Signatures** table are from the SonicWALL GAV signature database downloaded to your SonicWALL security appliance.

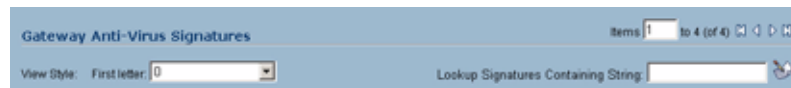


#	Name
1	0.0 (VGEN)
2	0190 (Dialer)
3	0190-dialer.com (Dialer)
4	0190-dialer.com 2 (Dialer)
5	1 (Itoned)
6	1005.0 (VGEN)
7	102 (BAT.MF)
8	116 (BAT.MF)
9	1168.512 (VGEN)
10	1168.512 (VGEN)
11	117.0 (VGEN)
12	1178.512 (VGEN)
13	118.32 (VGEN)
14	119.256 (VGEN)
15	1193.3 (VGEN)
16	12001.726 (VGEN)
17	12049.512 (VGEN)



Note: Signature entries in the database change over time in response to new threats.

Displaying Signatures

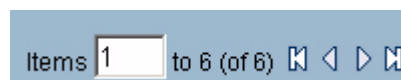


You can display the signatures in a variety of views using the **View Style** menu.

- **Use Search String** - Allows you to display signatures containing a specified string entered in the Lookup Signatures **Containing String** field.
- **All Signatures** - Displays all the signatures in the table, 50 to a page.
- **0 - 9** - Displays signature names beginning with the number you select from the menu.
- **A-Z** - Displays signature names beginning with the letter you select from menu.


Navigating the Gateway Anti-Virus Signatures Table

The SonicWALL GAV signatures are displayed fifty to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. If you're displaying the first page of a signature table, the entry might be **Items 1 to 50 (of 58)**. Use the navigation buttons to navigate the table.



Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the edit (Notepad) icon.

Lookup Signatures Containing String: 

The signatures that match the specified string are displayed in the **Gateway Anti-Virus Signatures** table.

Activating Intrusion Prevention Service

SonicWALL's Unified Threat Management Solution

SonicWALL Intrusion Prevention Service is included in SonicWALL's unified threat management solution that integrates Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service into an intelligent, real-time network security solution. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers unified threat management directly on the SonicWALL security appliance gateway.

Utilizing a configurable, high-performance deep packet inspection architecture, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service secures the network from the core to the perimeter against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans, and software vulnerabilities, such as buffer overflows, as well as peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code. Because new threats emerge daily and are often unpredictable, the deep packet inspection architecture is constantly updated to deliver the highest protection against an ever-changing threat landscape.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service inspects e-mail, Web traffic, file transfers, a multitude of stream-based protocols, as well as instant messaging and peer-to-peer applications. Because files containing malicious code, viruses and worms can be compressed and therefore inaccessible to conventional solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis. Supported compression formats include ZIP, Deflate and GZIP. As an added layer of security, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection not only against external threats, but also against those originating inside the network.

Unlike other threat management solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service has the capacity to analyze files of any size in real-time without the need to add expensive hardware drive or extra memory. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes a pro-active alerting mechanism that notifies network administrators when a new threat is discovered. Granular policy tools and an intuitive user interface enable administrators to configure a custom set of detection or prevention policies tailored to their specific network environment. Network administrator's can create global policies between security

zones and group attacks by priority, simplifying deployment and management across a distributed network.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Features

- **Integrated Deep Packet Inspection Technology** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service features a configurable, high-performance Deep Packet Inspection architecture that uses parallel searching algorithms up through the application layer to deliver complete application layer, Web and e-mail attack prevention. Parallel processing reduces the impact on the processor and maximizes available memory for exceptional performance on SonicWALL appliances.
- **Spyware Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service prevents malicious spyware from infecting networks by blocking spyware installations at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- **Real-Time AV Gateway Scanning** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent file-based virus and malicious code prevention by scanning in real-time for decompressed and compressed files containing viruses, Trojans, worms and other Internet threats over the corporate network.
- **Powerful Intrusion Prevention** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers complete protection from a comprehensive array of network-based application layer threats by scanning packet payloads for worms, Trojans, software vulnerabilities such as buffer overflows, peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.
- **Scalability and Performance** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes a per packet scanning engine, allowing the SonicWALL unified threat management solution to handle unlimited file size and virtually unlimited concurrent downloads.
- **Day Zero Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service ensures fast time-to-protection by employing a dynamically updated database of signatures created by a combination of SonicWALL's SonicAlert Team and third-party sources.
- **Extensive Signature List** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes an extensive database of thousands of attack and vulnerability signatures written to detect and prevent intrusions, viruses, spyware, worms, Trojans, application exploits, and malicious applications.
- **Distributed Enforcement Architecture** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes a distributed enforcement architecture to deliver automated signature updates, providing real-time protection from emerging threats and lowering total cost of ownership.
- **Inter-zone Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection against malicious code and other threats originating from the Internet or from internal sources. Administrators have the ability to enforce intrusion prevention and anti-virus scanning not only between each network zone and the Internet, but also between internal network zones for added security (Requires SonicOS Enhanced).
- **Advanced File Decompression Technology** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses, Trojans, worms and malware. Supported compression formats include: ZIP, Deflate and GZIP.
- **File-Based Scanning Protocol Support** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers protection for high threat viruses and malware by inspecting the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NETBIOS, instant messaging and peer-to-peer applications, and dozens of

- other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Application Control** - SonicWALL GAV/IPS provides the ability to prevent instant messaging and peer-to-peer file sharing programs from operating through the firewall, closing a potential back door that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
 - **Simplified Deployment and Management** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service allows network administrators to create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.
 - **Granular Management** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides an intuitive user interface and granular policy tools, allowing network administrators to configure a custom set of detection or prevention policies for their specific network environment and reduce the number of false policies while identifying immediate threats.
 - **Logging and Reporting** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service offers comprehensive logging of all intrusion attempts with the ability to filter logs based on priority level, enabling administrators to highlight high priority attacks. Granular reporting based on attack source, destination and type of intrusion is available through SonicWALL ViewPoint and Global Management System.

SonicWALL Intrusion Prevention Service Overview

SonicWALL Intrusion Prevention Service (SonicWALL IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWALL IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWALL IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWALL's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

SonicWALL Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a SonicWALL Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWALL Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWALL's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

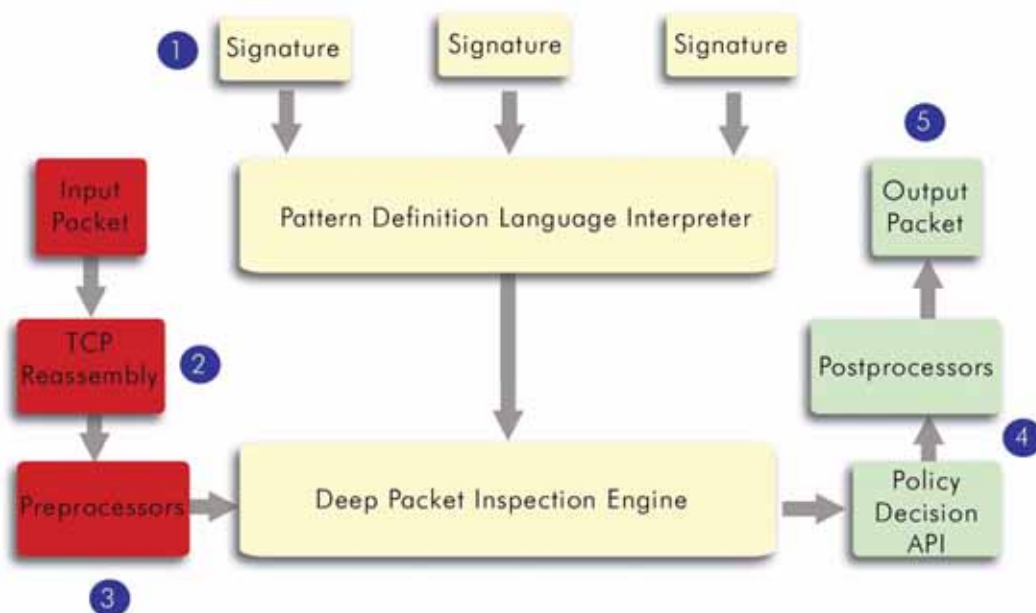
How SonicWALL's Deep Packet Inspection Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

The following steps describe how the SonicWALL Deep Packet Inspection Architecture works:

- 1 Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
- 2 TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
- 3 Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
- 4 Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
- 5 SonicWALL's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

SonicWALL DEEP PACKET INSPECTION ARCHITECTURE



SonicWALL IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.
- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.

- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Snort** - an open source network intrusion detection system. SonicWALL IPS includes open-source Snort signatures, as well as signatures from other signature databases, and SonicWALL created signatures. SonicWALL does not use the Snort engine.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Anti-Spyware** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface.

Because SonicWALL Intrusion Prevention Service is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need the following:

- **SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license.** You need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).
- **mySonicWALL.com account.** Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form from your SonicWALL security appliance management interface. Your mySonicWALL.com account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser.
- **Registered SonicWALL security appliance with active Internet connection.** Registering your SonicWALL security appliance is a simple procedure done directly from the management interface.
- **SonicOS Standard 3.1 or SonicOS Enhanced 3.1.** Your SonicWALL security appliance must be running SonicOS Standard 3.1 or SonicOS Enhanced 3.1 newer for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.



Tip: If your SonicWALL security appliance is connected to the Internet and registered at mySonicWALL.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.



Note: Administrator Guides for SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service are available on the SonicWALL documentation Web site: <http://www.sonicwall.com/support/documentation.html>

Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL security appliance management interface.



Note: If you already have a mysonicWALL.com account, go to “[Registering Your SonicWALL Security Appliance](#)” on page 540.

- 1 Log into the SonicWALL security appliance management interface.
- 2 If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- 3 On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL.**



- 4 In the mySonicWALL.com Login page, click the [here](#) link in **If you do not have a mySonicWALL account, please click here to create one.**



- 5 In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (*) are required fields.



Note: Remember your username and password to access your mySonicWALL.com account.

- 6 Click **Submit** after completing the **MySonicWALL Account** form.
- 7 When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.

Congratulations. Your mySonicWALL.com account is activated.

Now you need to log into mySonicWALL.com to register your SonicWALL security appliance.



Note: mySonicWALL.com registration information is not sold or shared with any other company.

Registering Your SonicWALL Security Appliance

- 1 Log into the SonicWALL security appliance management interface.
- 2 If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- 3 On the **System > Status** page, in the **Security Services** section, click the **Register** link. The mySonicWALL.com Login page is displayed.

- 4 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
- 5 The next several pages inform you about the free trials available to you for SonicWALL's Security Services:
 - ♦ **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
 - ♦ **Network Anti Virus** - Provides desktop and server anti-virus protection with software running on each computer.
 - ♦ **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
 - ♦ **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
 - ♦ **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.

Click **Continue** on each page.



Note: Clicking on the **Continue** button does not activate the **FREE TRIAL** versions of these SonicWALL Security Services.

- 6 At the top of the **Product Survey** page, Enter a "friendly name" for your SonicWALL content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
- 7 Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
- 8 Click **Submit**.
- 9 When the mySonicWALL.com server has finished processing your registration, a page is displayed informing you that the SonicWALL security appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

Activating FREE TRIALS

You can try FREE TRIAL versions of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, or SonicWALL Intrusion Prevention Service, perform these steps:

1. Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License

Because SonicWALL Intrusion Prevention Service is part of SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your SonicWALL security appliance.

If you do not have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you have an Activation Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- 1 On the **Security Services > Intrusion Prevention** page, click the **SonicWALL Intrusion Prevention Service Subscription** link. The **mySonicWALL.com Login** page is displayed.
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears.
- 3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- 4 Type in the Activation Key in the **New License Key** field and click **Submit**. SonicWALL Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Antivirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Free Trial		Renew		07 Apr 2005
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

You can apply the following activation keys:

ANTI SPYWARE 1 YR BUNDLE ASMUYZF8
 SNWL GAV 1 YR BUNDLE (PSIGAV BUNDLE) GAMUYZF8

- 5 Click on the Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- 6 Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.
- 7 Click on the SonicWALL Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- 8 Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

Congratulations! You have activated the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on mySonicWALL.com, the activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

Setting Up SonicWALL Intrusion Prevention Service Protection

Activating the SonicWALL Intrusion Prevention Service license on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Intrusion Prevention Service to begin protecting your network, you need to perform the following steps:

- 1 Enable SonicWALL Intrusion Prevention Service
- 2 Specify the Priority attack Groups
- 3 Apply SonicWALL Intrusion Prevention Service Protection to Zones



Note: For complete instructions on setting up SonicWALL Intrusion Prevention Service, refer to the *SonicWALL Intrusion Prevention Service Administrator's Guide* available on the SonicWALL documentation Web site <<http://www.sonicwall.com/support/documentation.html>>.

Selecting **Security Services > Intrusion Prevention** displays the configuration settings for SonicWALL IPS on your SonicWALL security appliance.

The **Intrusion Prevention Service** page is divided into three sections:

- **IPS Status** - displays status information on the state of the signature database, your SonicWALL IPS license, and other information.
- **IPS Global Settings** - provides the key settings for enabling SonicWALL IPS on your SonicWALL security appliance, specifying global SonicWALL IPS protection based on three classes of attacks, and other configuration options.
- **IPS Policies** - allows you to view SonicWALL IPS signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack.

After activating your Intrusion Prevention Service license, you must enable and configure SonicWALL IPS on the SonicWALL management interface to before intrusion prevention policies are applied to your network traffic.

Enabling SonicWALL IPS

SonicWALL IPS must be globally enabled on your SonicWALL security appliance by checking the **Enable IPS** check box in the **IPS Global Settings** section. A checkmark in the **Enable IPS** check box turns on the service on your SonicWALL security appliance.



Alert: Checking the **Enable IPS** check box does not automatically start SonicWALL IPS protection. You must also in the **IPS Global Settings** section. You must specify a **Prevent All** action in the **Signature Groups** table to activate intrusion prevention on the SonicWALL security appliance, and specify the interface or zones you want to protect.

Specifying Global Attack Level Protection

SonicWALL IPS allows you to globally manage your network protection against attacks by simply selecting the class of attacks: **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**. Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and

Medium Priority Attacks in the **Signature Groups** table, and then clicking **Apply** protects your network against the most dangerous and disruptive attacks. For more detailed information on configuring global signature groups, refer to “Configuring Global Signature Groups” in the *SonicWALL Intrusion Prevention Service Administrator’s Guide* available on the SonicWALL Resource CD or at www.sonicwall.com/support/documentation.html




Alert: Leaving the **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks** signature groups with no **Prevent All** action checked means no intrusion prevention is occurring on the SonicWALL security appliance.

Applying SonicWALL IPS Protection on Zones

If your SonicWALL security appliance is running SonicOS Enhanced 3.0 or higher, you apply SonicWALL IPS to Zones on the **Network > Zones** page to enforce SonicWALL IPS not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL IPS on the LAN zone enforces SonicWALL IPS on all incoming and outgoing LAN traffic.

In the **IPS Status** section of the **Security Services>Intrusion Prevention Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply SonicWALL IPS to a zone listed on the **Network > Zones** page.

To enable SonicWALL on a zone, perform these steps:

- 1 In the SonicWALL security appliance management interface, select **Network > Zones** or from the **IPS Status** section, on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.
- 2 In the **Configure** column in the **Zone Settings** table, click the edit icon  for the zone you want to apply SonicWALL IPS. The **Edit Zone** window is displayed.
- 3 Click the **Enable IPS** checkbox. A checkmark appears. To disable SonicWALL IPS, uncheck the box.
- 4 Click **OK**.

You also enable SonicWALL IPS protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

Activating Anti-Spyware Service

SonicWALL's Unified Threat Management Solution

SonicWALL Anti-Spyware Service is included in SonicWALL's unified threat management solution that integrates Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service into an intelligent, real-time network security solution. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers unified threat management directly on the SonicWALL security appliance gateway.

Utilizing a configurable, high-performance deep packet inspection architecture, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service secures the network from the core to the perimeter against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans, and software vulnerabilities, such as buffer overflows, as well as peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code. Because new threats emerge daily and are often unpredictable, the deep packet inspection architecture is constantly updated to deliver the highest protection against an ever-changing threat landscape.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service inspects e-mail, Web traffic, file transfers, a multitude of stream-based protocols, as well as instant messaging and peer-to-peer applications. Because files containing malicious code, viruses and worms can be compressed and therefore inaccessible to conventional solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis. Supported compression formats include ZIP, Deflate and GZIP. As an added layer of security, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection not only against external threats, but also against those originating inside the network.

Unlike other threat management solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service has the capacity to analyze files of any size in real-time without the need to add expensive hardware drive or extra memory. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes a pro-active alerting mechanism that notifies network administrators when a new threat is discovered. Granular policy tools and an intuitive user interface enable administrators to configure a custom set of detection or prevention policies tailored to their specific network environment. Network administrators can create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Features

- **Integrated Deep Packet Inspection Technology** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service features a configurable, high-performance Deep Packet Inspection architecture that uses parallel searching algorithms up through the application layer to deliver complete application layer, Web and e-mail attack prevention. Parallel processing reduces the impact on the processor and maximizes available memory for exceptional performance on SonicWALL appliances.
- **Spyware Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service prevents malicious spyware from infecting networks by blocking spyware installations at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- **Real-Time AV Gateway Scanning** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent file-based virus and malicious code prevention by scanning in real-time for decompressed and compressed files containing viruses, Trojans, worms and other Internet threats over the corporate network.
- **Powerful Intrusion Prevention** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers complete protection from a comprehensive array of network-based application layer threats by scanning packet payloads for worms, Trojans, software vulnerabilities such as buffer overflows, peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.
- **Scalability and Performance** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes a per packet scanning engine, allowing the SonicWALL unified threat management solution to handle unlimited file size and virtually unlimited concurrent downloads.
- **Day Zero Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service ensures fast time-to-protection by employing a dynamically updated database of signatures created by a combination of SonicWALL's SonicAlert Team and third-party sources.
- **Extensive Signature List** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes an extensive database of thousands of attack and vulnerability signatures written to detect and prevent intrusions, viruses, spyware, worms, Trojans, application exploits, and malicious applications.
- **Distributed Enforcement Architecture** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service utilizes a distributed enforcement architecture to deliver automated signature updates, providing real-time protection from emerging threats and lowering total cost of ownership.
- **Inter-zone Protection** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides application layer attack protection against malicious code and other threats originating from the Internet or from internal sources. Administrators have the ability to enforce intrusion prevention and anti-virus scanning not only between each network zone and the Internet, but also between internal network zones for added security (Requires SonicOS Enhanced).
- **Advanced File Decompression Technology** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses, Trojans, worms and malware. Supported compression formats include: ZIP, Deflate and GZIP.
- **File-Based Scanning Protocol Support** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers protection for high threat viruses and malware by inspecting the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NETBIOS, instant messaging and peer-to-peer applications, and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Application Control** - SonicWALL GAV/Anti-Spyware/IPS provides the ability to prevent instant messaging and peer-to-peer file sharing programs from operating through the firewall, closing a

- potential back door that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Simplified Deployment and Management** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service allows network administrators to create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.
 - **Granular Management** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service provides an intuitive user interface and granular policy tools, allowing network administrators to configure a custom set of detection or prevention policies for their specific network environment and reduce the number of false policies while identifying immediate threats.
 - **Logging and Reporting** - SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service offers comprehensive logging of all intrusion attempts with the ability to filter logs based on priority level, enabling administrators to highlight high priority attacks. Granular reporting based on attack source, destination and type of intrusion is available through SonicWALL ViewPoint and Global Management System.

SonicWALL Anti-Spyware Service Overview

SonicWALL Anti-Spyware is part of the SonicWALL Gateway Anti-Virus, Anti-Virus and Intrusion Prevention Service solution that provides comprehensive, real-time protection against viruses, worms, Trojans, spyware, and software vulnerabilities.

The SonicWALL Anti-Spyware Service protects networks from intrusive spyware by cutting off spyware installations and delivery at the gateway and denying previously installed spyware from communicating collected information outbound. SonicWALL Anti-Spyware works with other anti-spyware program, such as programs that remove existing spyware applications from hosts. You are encouraged to use or install host-based anti-spyware software as an added measure of defense against spyware.

SonicWALL Anti-Spyware analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware. If spyware has been installed on a LAN workstation prior to the SonicWALL Anti-Spyware solution install, the service will examine outbound traffic for streams originating at spyware infected clients and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the SonicWALL security appliance identifies that traffic and resets the connection.

The SonicWALL Anti-Spyware Service provides the following protection:

- Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- Scans and logs spyware threats that are transmitted through the network and alerts administrators when new spyware is detected and/or blocked.
- Stops existing spyware programs from communicating in the background with hackers and servers on the Internet, preventing the transfer of confidential information.
- Provides granular control over networked applications by enabling administrators to selectively permit or deny the installation of spyware programs.
- Prevents e-mailed spyware threats by scanning and then blocking infected e-mails transmitted either through SMTP, IMAP or Web-based e-mail.



Note: Refer to the SonicWALL Anti-Spyware Administrator's Guide on the SonicWALL Web site <<http://www.sonicwall.com/support/documentation.html>> for complete product documentation. SonicWALL Deep Packet Inspection

SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Anti-Spyware** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface.

Because SonicWALL Intrusion Prevention Service is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need the following:

- **SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license.** You need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).
- **mySonicWALL.com account.** Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form from your SonicWALL security appliance management interface. Your mySonicWALL.com account is also accessible at <<https://www.mysonicwall.com>> from any Internet connection with a Web browser.
- **Registered SonicWALL security appliance with active Internet connection.** Registering your SonicWALL security appliance is a simple procedure done directly from the management interface.
- **SonicOS Standard 3.1 or SonicOS Enhanced 3.1.** Your SonicWALL security appliance must be running SonicOS Standard 3.1 or SonicOS Enhanced 3.1 newer for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.



Tip: If your SonicWALL security appliance is connected to the Internet and registered at mySonicWALL.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.



Note: Administrator Guides for SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service are available on the SonicWALL documentation Web site: <<http://www.sonicwall.com/support/documentation.html>>

Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL security appliance management interface.



Note: If you already have a mysonicWALL.com account, go to "[Registering Your SonicWALL Security Appliance](#)" on page 549.

- 1 Log into the SonicWALL security appliance management interface.
- 2 If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- 3 On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL.**



- 4 In the **mySonicWALL.com Login** page, click the **here** link in **If you do not have a mySonicWALL account, please click here to create one.**



- 5 In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (*) are required fields.



Note: Remember your username and password to access your mySonicWALL.com account.

- 6 Click **Submit** after completing the **MySonicWALL Account** form.
- 7 When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.

Congratulations. Your mySonicWALL.com account is activated.

Now you need to log into mySonicWALL.com to register your SonicWALL security appliance.



Note: mySonicWALL.com registration information is not sold or shared with any other company.

Registering Your SonicWALL Security Appliance

- 1 Log into the SonicWALL security appliance management interface.
- 2 If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- 3 On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **mySonicWALL.com Login** page is displayed.
- 4 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
- 5 The next several pages inform you about the free trials available to you for SonicWALL's Security Services:
 - ♦ **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
 - ♦ **Network Anti Virus** - Provides desktop and server anti-virus protection with software running on each computer.

- ◆ **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
- ◆ **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
- ◆ **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.

Click **Continue** on each page.



Note: Clicking on the **Continue** button does not activate the **FREE TRIAL** versions of these SonicWALL Security Services.

- 6 At the top of the **Product Survey** page, Enter a “friendly name” for your SonicWALL content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
- 7 Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
- 8 Click **Submit**.
- 9 When the mySonicWALL.com server has finished processing your registration, a page is displayed informing you that the SonicWALL security appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

Activating FREE TRIALS

You can try **FREE TRIAL** versions of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the **FREE TRIAL** link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a **FREE TRIAL** of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, or SonicWALL Intrusion Prevention Service, perform these steps:

1. Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

Activating the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service License

Because SonicWALL Intrusion Prevention Service is part of SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your SonicWALL security appliance.

If you do not have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you have an Activation Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- 1 On the **Security Services > Intrusion Prevention** page, click the **SonicWALL Intrusion Prevention Service Subscription** link. The **mySonicWALL.com Login** page is displayed.
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears.
- 3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- 4 Type in the Activation Key in the **New License Key** field and click **Submit**. SonicWALL Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Antivirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Free Trial		Renew		07 Apr 2005
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

You can apply the following activation keys:

ANTI SPYWARE 1 YR BUNDLE ASMUYZF8
SNWL GAV 1 YR BUNDLE (PS/GAV BUNDLE) GAMUYZF8

- 5 Click on the Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- 6 Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

Congratulations! You have activated the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on mySonicWALL.com, the activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

Setting Up SonicWALL Anti-Spyware Service Protection

After activating SonicWALL Anti-Spyware, the **Security Services > Anti-Spyware** page displays the configuration settings for managing the service on your SonicWALL security appliance.


Refer to the **SonicWALL Anti-Spyware Administrator's Guide** on the SonicWALL Web site <<http://www.sonicwall.com/support/documentation.html>> for complete configuration instructions.

Applying SonicWALL Anti-Spyware Protection on Zones

If your SonicWALL security appliance is running SonicOS Enhanced 3.1 or higher, you can apply SonicWALL Anti-Spyware to Zones on the **Network > Zones** page to enforce SonicWALL Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL Anti-Spyware on the LAN zone enforces SonicWALL Anti-Spyware on all incoming and outgoing LAN traffic.

In the **Anti-Spyware Status** section of the **Security Services > Anti-Spyware Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply SonicWALL Anti-Spyware to a zone listed on the **Network > Zones** page.

To enable SonicWALL on a zone, perform these steps:

- 1 In the SonicWALL security appliance management interface, select **Network > Zones** or from the **Anti-Spyware Status** section, on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.
- 2 In the **Configure** column in the **Zone Settings** table, click the edit icon  for the zone you want to apply SonicWALL Anti-Spyware. The **Edit Zone** window is displayed.
- 3 Click the **Enable Anti-Spyware** checkbox. A checkmark appears. To disable SonicWALL Anti-Spyware, uncheck the box.
- 4 Click **OK**.

You can also enable SonicWALL Anti-Spyware protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

Configuring SonicWALL Real-Time Blacklist

SMTP Real-Time Black List Filtering

SMTP Real-time Black List (RBL) is a mechanism for publishing the IP addresses of SMTP servers from which or through which spammers operate. There are a number of organizations that compile this information both for free <<http://www.spamhaus.org>>, and for profit <<http://www.mail-abuse.com>>. A well maintained list of RBL services and their efficacy can be found at <<http://www.sdsc.edu/~jeff/spam/cbc.html>>.



Note: SMTP RBL is an aggressive spam filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The SonicOS implementation of SMTP RBL filtering provides a number of fine tuning mechanisms to help ensure filtering accuracy.

RBL list providers publish their lists via DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from 127.0.0.2 to 127.0.0.9 indicates some type of undesirability:

Blocked Response Codes
127.0.0.2 - Open Relay
127.0.0.3 - Dialup Spam Source
127.0.0.4 - Spam Source
127.0.0.5 - Smart Host
127.0.0.6 - Spamware Site
127.0.0.7 - Bad List Server
127.0.0.8 - Insecure Script
127.0.0.9 - Open Proxy Server

For example, an SMTP server with IP address 1.2.3.4 has been blacklisted by RBL list provider sbl-xbl.spamhaus.org, then a DNS query to 4.3.2.1.sbl-xbl.spamhaus.org will provide a 127.0.0.4 response, indicating that the server is a known source of spam, and the connection will be dropped.



Note: Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation, unbeknownst to the hosts operator. These zombie machines rarely attempt to retry failed delivery attempts, as would be the behavior of a legitimate SMTP server. As such, once the delivery attempt is thwarted by the SonicWALL RBL filter, no subsequent delivery attempts for that same piece of spam will be made.

Security Services > RBL Filter

When **Enable Real-time Black List Blocking** is enabled on the **Security Services > RBL Filter** page, inbound connections from hosts on the WAN, or outbound connections to hosts on the WAN are checked against each enabled RBL service with a DNS request to the DNS servers configured under **RBL DNS Servers**.



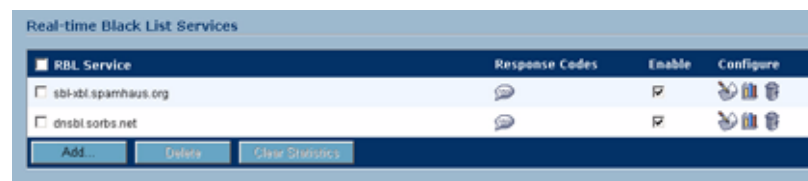
The RBL DNS Servers menu allows you to specify the DNS servers. You can choose **Inherit Settings from WAN Zone** or **Specify DNS Servers Manually**. If you select **Specify DNS Servers Manually**, enter the DNS server addresses in the **DNS Server** fields.

The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server will be filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache and a DNS request must be made. In this case the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection will be dropped.

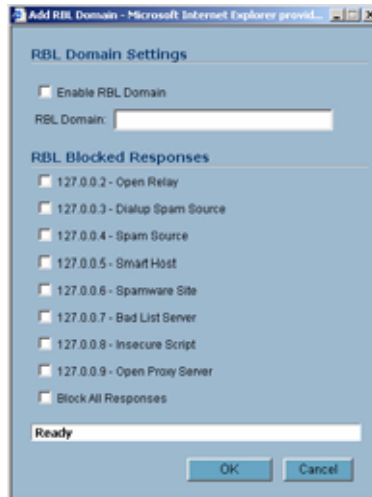
Adding RBL Services

You can add additional RBL services the **Real-time Black List Services** section.



To add an RBL services, click the **Add** button. In the **Add RBL Domain** window, you specify the RBL domain to be queried, enable it for use, and specify its expected response codes. Most RBL services

list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.



Statistics are maintained for each RBL Service in the **RBL Service** table, and can be viewed with a mouse-over of the (statistics) icon to the right on the service entry.

User-Defined SMTP Server Lists

The **User Defined SMTP Server Lists** section allows for Address Objects to be used to construct a white-list (explicit allow) or black-list (explicit deny) of SMTP servers. Entries in this list will bypass the RBL querying procedure. For example, to ensure that you always receive SMTP connections from a partner site's SMTP server, create an Address Object for the server you added using the **Add** button, click the edit icon in the **Configure** column of the **RBL User White List** row, and add the **Address Object**. The table will be updated, and that server will always be allowed to make SMTP exchanges.

The **System > Diagnostics** page also provides a **Real-time Black List Lookup** feature that allows for SMTP IP addresses (or RBL services, or DNS servers) to be specifically tested.

For a list of known spam sources to use in testing, refer to <http://www.spamhaus.org/sbl/latest.lasso>

Configuring SonicWALL Global Security Client

Security Services > Global Security Client

The SonicWALL Global Security Client combines gateway enforcement, central management, configuration flexibility and software deployment to deliver comprehensive desktop security for remote/mobile workers and corporate networks. It offers administrators the capability to manage a mobile/remote user's online access, based on corporate policies, to ensure optimal security of the network and maximize network resources. Instant messaging, high-risk Web sites and network file access can all be allowed or disallowed as security and productivity concerns dictate. Different remote/mobile users can be organized into adaptable groups with differing policies at a granular level.

SonicWALL Global Security Client delivers a low-maintenance solution to allow network administrators to secure mobile users. Residing on the remote user's system, the Global Security Client automatically communicates with an organization's SonicWALL gateway back at the office when an individual logs in to the network. Prior to allowing network access, the gateway administrator automatically updates the Global Security Client with the latest security policies and software updates. No prompting or intervention is necessary by the administrator or the remote user - it's completely seamless and transparent.

Global Security Client protection includes the SonicWALL Distributed Security Client and the SonicWALL Global VPN Client Enterprise combined with centrally managed security policies via the SonicWALL Internet Security Appliance and SonicWALL's industry-leading Distributed Enforcement Architecture (DEA).

The SonicWALL Global Security Client combines gateway enforcement, central management, configuration flexibility and software deployment to deliver comprehensive desktop security for remote/mobile workers and corporate networks. It offers administrators the capability to manage a mobile/remote user's online access, based on corporate policies, to ensure optimal security of the network and maximize network resources. Instant messaging, high-risk Web sites and network file access can all be allowed or disallowed as security and productivity concerns dictate. Different remote/mobile users can be organized into adaptable groups with differing policies at a granular level.

SonicWALL Global Security Client delivers a low-maintenance solution to allow network administrators to secure mobile users. Residing on the remote user's system, the Global Security Client automatically communicates with an organization's SonicWALL gateway back at the office when an individual logs in to the network. Prior to allowing network access, the gateway administrator automatically updates the Global Security Client with the latest security policies and software updates.

No prompting or intervention is necessary by the administrator or the remote user - it's completely seamless and transparent.

Global Security Client protection includes the SonicWALL Distributed Security Client and the SonicWALL Global VPN Client Enterprise combined with centrally managed security policies via the SonicWALL Internet Security Appliance and SonicWALL's industry-leading Distributed Enforcement Architecture (DEA).



For complete SonicWALL Global Security Client documentation, see the SonicWALL Global Security Client Administrator's Guide available at <http://www.sonicwall.com/services/documentation.html>.

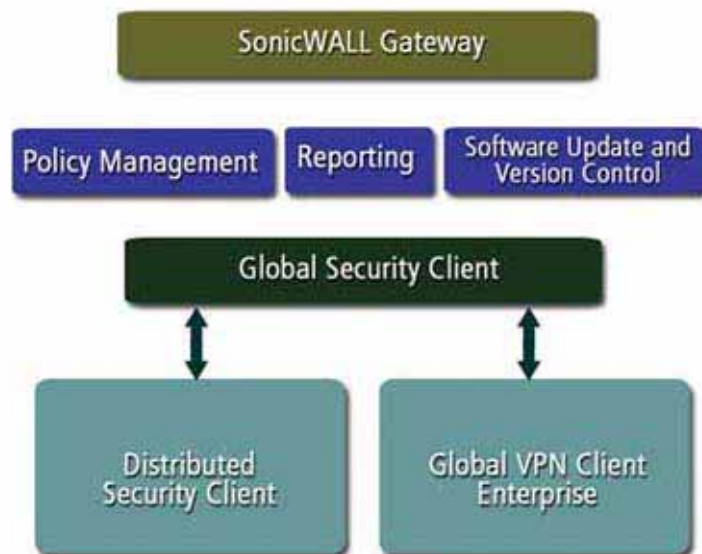
Global Security Client Features

- **Multi-Pronged Protection** - extends the boundaries of security by protecting the corporate network and remote/mobile workers from malicious attacks that occur over the Internet.
- **Enhanced Application Security** - provides an additional layer of security by protecting organizations against legal liabilities that occur when employees accidentally or intentionally run applications from the Internet that have been designated as "untrusted" by the network administrator.
- **Policy Management** - enables network administrator's to create, distribute and manage global security policies for remote and mobile users from a central location. Once a new policy is created, it is seamlessly distributed to every system on the network with no end-user interaction required. Configuration options include specifying the minimum application version, policy levels and behavior for clients not in compliance.
- **Gateway Enforcement** - enforces security policies at the gateway to ensure the end-user's system is in compliance before being granted access to the network. Users without the Global Security Client installed on their systems must contact their administrator.
- **Scalable Architecture** - features a unique client/gateway enforcement architecture that delivers comprehensive security, scaling from the individual telecommuters and mobile users up to larger, more diverse deployments with a worldwide mobile workforce.
- **Low Total Cost of Ownership** - addresses the needs of organizations looking to deploy comprehensive desktop security to remote/mobile workers and corporate networks while delivering a lower total cost of ownership through automated policy enforcement and software distribution at the gateway.
- **Easy-to-Use Local Interface** - includes an intuitive user interface that seamlessly integrates multiple applications and presents the administrator with a status page and optional configuration functionality, offering enhanced ease of use.
- **Application Reporting** - includes application reporting to provide network administrators with data on the status of the application, as well as the ability to monitor for unusual activities and perform troubleshooting.
- **Multi-Pronged Protection** - extends the boundaries of security by protecting the corporate network and remote/mobile workers from malicious attacks that occur over the Internet.
- **Enhanced Application Security** - provides an additional layer of security by protecting organizations against legal liabilities that occur when employees accidentally or intentionally run applications from the Internet that have been designated as "untrusted" by the network administrator.
- **Policy Management** - enables network administrator's to create, distribute and manage global security policies for remote and mobile users from a central location. Once a new policy is created, it is seamlessly distributed to every system on the network with no end-user interaction required. Configuration options include specifying the minimum application version, policy levels and behavior for clients not in compliance.

- **Gateway Enforcement** - enforces security policies at the gateway to ensure the end-user's system is in compliance before being granted access to the network. Users without the Global Security Client installed on their systems must contact their administrator.
- **Scalable Architecture** - features a unique client/gateway enforcement architecture that delivers comprehensive security, scaling from the individual telecommuters and mobile users up to larger, more diverse deployments with a worldwide mobile workforce.
- **Low Total Cost of Ownership** - addresses the needs of organizations looking to deploy comprehensive desktop security to remote/mobile workers and corporate networks while delivering a lower total cost of ownership through automated policy enforcement and software distribution at the gateway.
- **Easy-to-Use Local Interface** - includes an intuitive user interface that seamlessly integrates multiple applications and presents the administrator with a status page and optional configuration functionality, offering enhanced ease of use.
- **Application Reporting** - includes application reporting to provide network administrators with data on the status of the application, as well as the ability to monitor for unusual activities and perform troubleshooting.

How SonicWALL Global Security Client Works

The security administrator logs into the SonicWALL gateway to create security policies for all Global Security Clients using the intuitive Policy Editor interface. The Policy Editor allows the security administrator to create, edit, and deploy security policies that are automatically enforced by the SonicWALL gateway. When a remote user logs into the corporate network using the Global VPN Client Enterprise, the SonicWALL gateway seamlessly updates the user's security policy for the Distributed Security Client to ensure the client is in full compliance with corporate security policies while establishing a secure VPN connection via the Global VPN Client Enterprise.



SonicWALL's Distributed Enforcement Architecture (DEA) technology enables the policy enforcement capabilities that provide the framework for the Global Security Client's complete security solution for all remote and network desktops. SonicWALL's DEA technology enables the automatic installation of new software components, changes the configuration of different components, verifies version information, forces updates of components, informs the user which components do not meet the policy requirements, and provides user authentication for policy enforcement.

Global Security Client Licensing

The SonicWALL Global Security Client allows you to install the Global VPN Client Enterprise and Distributed Security Client. SonicWALL Global VPN Client Enterprise is licensed on a per connection basis. That means a 5 pack of Global Security Client gives the customer 5 concurrent Global VPN Client Enterprise connections on the SonicWALL. SonicWALL Distributed Security Client licensing is licensed on a per client basis. A 5 pack of Global Security Client allows you to install Distributed Security Client on 5 computers. The Distributed Security Client license is for subscription.

If you do not have SonicWALL Global Security Client activated on your SonicWALL, you must purchase Global Security Client from a SonicWALL reseller or your mySonicWALL.com account (limited to customers in the USA and Canada only).

Activating Global Security Client Licenses on Your SonicWALL

If you have the Activation Key for your SonicWALL Global Security Client and a mySonicWALL.com account, use the following steps to activate the Global Security Client from the SonicWALL Internet Security Appliance management interface.

1. In the **System > Licenses** page of the SonicWALL Management Interface, click the [click here](#) in **To Activate, Upgrade, or Renew services** [click here](#) in the Manage Security Services Online.
2. In the **mySonicWALL Login** page, enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System > Licenses** page appears.



Each Activation Key activates both the Global VPN Client Enterprise and Distributed Security Client licenses. You enter the Activation Key for the Distributed Security Client and the Global VPN Client Enterprise license is automatically added.

3. Click **Upgrade** in the **Manage Service** column for **Distributed Security Client** in the **Manage Services Online** table.
4. Type the Activation Key in the **New License Key** field for each Global Security Client (Distributed Security Client and Global VPN Client Enterprise).
5. Click **Submit**. Your Global Security Clients are activated. The number of Global VPN Client Enterprise and Distributed Security Client licenses appear in the **Count** column of the **Manage Services Online** table on the **System > Licenses** page. The expiration date for the Distributed Security Client is displayed in the Expiration column.

Configuring Security Policies for Global Security Clients

The **Security Services > Global Security Client** page provides the settings for configuring the security policies for Global Security Clients.

Security Services > Global Security Client Apply Cancel ?

Global Security Client Policy

Current policy version number being enforced is 0

View/Edit your current OSC policy Edit Policy

Global Security Client Enforcement

Enforce Global Security Client Policy on a zone in [Network > Zones](#)

Policy excluded IP ranges

Range type:

From Address	To Address	Configure
No Entries		

Add... Delete All

PART
13

Log

Managing Log Events

Log > View

The SonicWALL security appliance maintains an Event log for tracking potential security threats. This log can be viewed in the **Log > View** page, or it can be automatically sent to an e-mail address for convenience and archiving. The log is displayed in a table and can be sorted by column.

The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.

The screenshot shows the 'Log > View' interface. At the top right are buttons for 'Refresh', 'Clear Log', and 'E-Mail Log'. Below is the 'Log View Settings' section with filters for Priority (All), Category (All Categories), Source (All Interfaces), and Destination (All Interfaces). The filter logic is 'Priority && Category && Source && Destination'. There are buttons for 'Apply Filters', 'Reset Filters', and 'Export Log'. Below the settings is the 'Log View' table, which is currently showing items 51 to 100 of 587. The table has columns for #, Time, Priority, Category, Message, Source, Destination, Notes, and Rule.

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
51	02/09/2006 13:36:22.832	Debug	Network Access	HTTP method detected; examining stream for host header	192.168.168.65, 1560, X0 (admin)	66.94.234.72, 80, X1	TCP HTTP	
52	02/09/2006 13:36:07.576	Alert	Intrusion Prevention	Possible port scan dropped	204.127.205.10, 80, X1	68.35.78.194, 6729, X1	TCP scanned port list, 6716, 6716, 6716, 6716	
53	02/09/2006 13:35:59.560	Notice	Network Access	TCP connection dropped	63.169.44.100, 80, X1	192.168.168.65, 1544, X0	TCP Port: 1544	
54	02/09/2006 13:34:52.176	Notice	Network Access	UDP packet dropped	65.51.65.221, 20143, X1	68.35.78.194, 1026, X1	UDP Port: 1026	
55	02/09/2006 13:34:11.560	Notice	Network Access	TCP connection dropped	64.191.192.115, 80, X1	192.168.168.65, 1531, X0	TCP Port: 1531	
56	02/09/2006 13:29:47.176	Alert	Intrusion Prevention	IPS Detection Alert SQL/MSQL/Multimedia Download_SID_1912, Priority: Low	66.250.188.141, 80, X1	192.168.168.65, 1490, X0		

Log View Table

The log is displayed in a table and is sortable by column. The log table columns include:

- **Time** - the date and time of the event.
- **Priority** - the level of priority associated with your log event.
Syslog uses eight categories to characterize messages – in descending order of severity, the categories include:
 - ◆ Emergency
 - ◆ Alert
 - ◆ Critical
 - ◆ Error
 - ◆ Warning
 - ◆ Notice
 - ◆ Informational
 - ◆ Debug

Specify a priority level on a SonicWALL security appliance on the **Log > Categories** page to log messages for that priority level, plus all messages tagged with a higher severity. For example, select 'error' as the priority level to log all messages tagged as 'error,' as well as any messages tagged with 'critical,' 'alert,' and 'emergency.' Select 'debug' to log all messages.



Cross Reference: Refer to *Log Event Messages* section for more information on your specific log event.

- **Category** - the type of traffic, such as *Network Access* or *Authenticated Access*.
- **Message** - provides description of the event.
- **Source** - displays source network and IP address.
- **Destination** - displays the destination network and IP address.
- **Notes** - provides additional information about the event.
- **Rule** - notes Network Access Rule affected by event.

Navigating and Sorting Log View Table Entries

The **Log View** table provides easy pagination for viewing large numbers of log events. You can navigate these log events by using the navigation control bar located at the top right of the **Log View** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Refresh

To update log messages, clicking the **Refresh** button near the top right corner of the page.

Clear Log

To delete the contents of the log, click the **Clear Log** button near the top right corner of the page.

Export Log

To export the contents of the log to a defined destination, click the **Export Log** button below the filter table. You can export log content to two formats:

- **Plain text format**--Used in log and alert e-mail.
- **Comma-separated value (CSV) format**--Used for importing into Excel or other presentation development applications.

E-mail Log

If you have configured the SonicWALL security appliance to e-mail log files, clicking **E-mail Log** near the top right corner of the page sends the current log files to the e-mail address specified in the **Log > Automation > E-mail** section.



Note: The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately sent via e-mail, either to an e-mail address or to an e-mail pager. For sending alerts, you must enter your e-mail address and server information in the **Log > Automation** page.

Filtering Log Records Viewed

You can filter the results to display only event logs matching certain criteria. You can filter by **Priority**, **Category**, **Destination (IP or Interface)**, and **Destination (IP or Interface)**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	<input type="text"/> X1	<input type="checkbox"/>
Destination (IP, Interface):	<input type="text"/> X0	<input type="checkbox"/>
Filter Logic: Priority && Category && Source && Destination		
<input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/>		<input type="button" value="Export Log"/>

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you select an interface for **Source** and for **Destination**, the search string will look for connections matching:

Source interface AND Destination interface

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**.

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	<input type="text"/> X1	<input checked="" type="checkbox"/>
Destination (IP, Interface):	<input type="text"/> X0	<input checked="" type="checkbox"/>
Filter Logic: (Source Destination) && Priority && Category		
<input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/>		<input type="button" value="Export Log"/>

For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

(Source IP OR Destination IP) AND Protocol

Click **Apply Filter** to apply the filter immediately to the **Active Connections** table. Click **Reset** to clear the filter and display the unfiltered results again.

The following example filters for log events resulting from traffic from the WAN to the LAN:

Log View Settings

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	WAN	<input type="checkbox"/>
Destination (IP, Interface):	LAN	<input type="checkbox"/>

Filter Logic: Priority && Category && Source && Destination

Buttons: Apply Filters, Reset Filters, Export Log

Log View Items 1 to 2 (of 2)

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	02/15/2008 14:30:29.720	Alert	Intrusion Prevention	IP spoof dropped	192.168.168.195, 88, WAN	255.255.255.255, 87, LAN	MAC address: 00:0b:db:5a:a1a7	
2	02/15/2008 10:00:02.304	Alert	Intrusion Prevention	IP spoof dropped	192.168.168.20, 88, WAN	255.255.255.255, 87, LAN	MAC address: 00:0b:db:0c:ab16	

Log Event Messages

For a complete reference guide of log event messages, refer to the *SonicWALL Log Event Reference Guide* located at http://www.sonicwall.com/support/SonicOS_FW_documentation.html.

Configuring Log Categories

Log > Categories

This chapter provides configuration tasks to enable you to categorize and customize the logging functions on your SonicWALL security appliance for troubleshooting and diagnostics.



Note: You can extend your SonicWALL security appliance log reporting capabilities by using SonicWALL ViewPoint. ViewPoint is a web-based graphical reporting tool for detailed and comprehensive reports. For more information on the SonicWALL ViewPoint reporting tool, refer to www.sonicwall.com.

The screenshot shows the SonicWALL web interface for configuring log categories. The left sidebar contains navigation options: System, Network, Modem, Wireless, SonicPoint, Firewall, VoIP, VPN, Users, Security Services, Log, View, Categories, Syslog, Automation, Name Resolution, Reports, ViewPoint, Wizards, Help, and Logout. The main content area is titled "Log > Categories" and includes a "Refresh" button, "Apply" button, and "Cancel" button. Below the title, there are configuration options for "Log Severity/Priority": Logging Level (set to Debug) and Alert Level (set to Alert). There are also fields for "Log Redundancy Filter (seconds)" (set to 60) and "Alert Redundancy Filter (seconds)" (set to 300). Under "Log Categories", there is a "View Style" dropdown set to "All Categories". A table lists various log categories with their descriptions and checkboxes for Log, Alerts, and Syslog, along with an "Event Count" column.

Category	Description	Log	Alerts	Syslog	Event Count
BO2.11b Management	Legacy category	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	190
Attacks	Legacy category	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
Authenticated Access	Administrator, user, and guest account activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
BOOTP	BOOTP activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
Blocked Java Etc	Legacy category	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
Blocked Web Sites	Legacy category	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
Crypto Test	Crypto algorithm and hardware testing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
DNS	Dynamic DNS activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
DNS Client	DNS Client activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Log Priority

This section provides information on configuring the level of priority log messages are captured and corresponding alert messages are sent through e-mail for notification.

Logging Level

The **Logging Level** control filters events by priority. Events of equal or greater priority are passed, and events of lower priority are dropped. The **Logging Level** menu includes the following priority scale items from highest to lowest priority:

- **Emergency** (highest priority)
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug** (lowest priority)

Alert Level

The **Alert Level** control determines how E-mail Alerts are sent. An event of equal or greater priority causes an E-mail alert to be issued. Lower priority events do not cause an alert to be sent. Events are pre-filtered by the **Logging Level** control, so if the **Logging Level** control is set to a higher priority than that of the **Alert Level** control, only alerts at the **Logging Level** or higher are sent. Alert levels include:

- **None** (disables e-mail alerts)
- **Emergency** (highest priority)
- **Alert**
- **Critical**
- **Error** (lowest priority)

Log Redundancy Filter

The **Log Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the SonicWALL log. Various attacks are often rapidly repeated, which can quickly fill up a log if each attack is logged. The Log Redundancy Filter has a default setting of 60 seconds.

Alert Redundancy Filter

The **Alert Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the SonicWALL log before an alert is issued. The Alert Redundancy Filter has a default setting of 900 seconds.

Log Categories

SonicWALL security appliances provide automatic attack protection against well known exploits. The majority of these *legacy attacks* were identified by telltale IP or TCP/UDP characteristics, and recognition was limited to a set of fixed layer 3 and layer 4 values. As the breadth and sophistication of attacks evolved, it's become essential to dig deeper into the traffic, and to develop the sort of adaptability that could keep pace with the new threats.

All SonicWALL security appliances, even those running SonicWALL IPS, continue to recognize these legacy port and protocol types of attacks. The current behavior on all SonicWALL security appliances devices is to automatically and holistically prevent these legacy attacks, meaning that it is not possible to disable prevention of these attacks either individually or globally.

SonicWALL security appliances now include an expanded list of attack categories that can be logged.

The **View Style** menu provides the following three log category views:

- **All Categories** - Displays both **Legacy Categories** and **Expanded Categories**.
- **Legacy Categories** - Displays log categories carried over from earlier SonicWALL log event categories.
- **Expanded Categories** - Displays the expanded listing of categories that includes the older Legacy Categories log events rearranged into the new structure.

Table 61.1 describes both the Legacy and Extended log categories.

Table 61.1 Log Categories

Log Type	Category	Description
802.11b Management	Legacy	Logs WLAN IEEE 802.11b connections.
Advanced Routing	Expanded	Logs messages related to RIPv2 and OSPF routing events.
Attacks	Legacy	Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing
Authenticated Access	Expanded	Logs administrator, user, and guest account activity
Blocked Java, etc.	Legacy	Logs Java, ActiveX, and Cookies blocked by the SonicWALL security appliance.
Blocked Web Sites	Legacy	Logs Web sites or newsgroups blocked by the Content Filter List or by customized filtering.
BOOTP	Expanded	Logs BOOTP activity
Crypto Test	Expanded	Logs crypto algorithm and hardware testing
DDNS	Expanded	Logs Dynamic DNS activity
Denied LAN IP	Legacy	Logs all LAN IP addresses denied by the SonicWALL security appliance.
DHCP Client	Expanded	Logs DHCP client protocol activity
DHCP Relay	Expanded	Logs DHCP central and remote gateway activity
Dropped ICMP	Legacy	Logs blocked incoming ICMP packets.
Dropped TCP	Legacy	Logs blocked incoming TCP connections.
Dropped UDP	Legacy	Logs blocked incoming UDP packets.
Firewall Event	Extended	Logs internal firewall activity
Firewall Hardware	Extended	Logs firewall hardware error events
Firewall Logging	Extended	Logs general events and errors
Firewall Rule	Extended	Logs firewall rule modifications
GMS	Extended	Logs GMS status event
High Availability	Extended	Logs High Availability activity
IPcomp	Extended	Logs IP compression activity
Intrusion Prevention	Extended	Logs intrusion prevention related activity
L2TP Client	Extended	Logs L2TP client activity
L2TP Server	Extended	Logs L2TP server activity
Multicast	Extended	Logs multicast IGMP activity
Network	Extended	Logs network ARP, fragmentation, and MTU activity

Table 61.1 Log Categories

Log Type	Category	Description
Network Access	Extended	Logs network and firewall protocol access activity
Network Debug	Legacy	Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. Network Debug information is intended for experienced network administrators.
Network Traffic	Expanded	Logs network traffic reporting events
PPP	Extended	Logs generic PPP activity
PPP Dial-Up	Extended	Logs PPP dial-up activity
PPPoE	Extended	Logs PPPoE activity
PPTP	Extended	Logs PPTP activity
RBL	Extended	Logs real-time black list activity
RIP	Extended	Logs RIP activity
Remote Authentication	Extended	Logs RADIUS and LDAP server activity
Security Services	Extended	Logs security services activity
SonicPoint	Extended	Logs SonicPoint activity
System Errors	Legacy	Logs problems with DNS or e-mail.
System Maintenance	Legacy	Logs general system activity, such as system activations.
User Activity	Legacy	Logs successful and unsuccessful log in attempts.
VOIP	Extended	Logs VoIP H.323/RAS, H.323/H.225, and H.323/H.245 activity
VPN	Extended	Logs VPN activity
VPN Client	Extended	Logs VPN client activity
VPN IKE	Extended	Logs VPN IKE activity
VPN IPsec	Extended	Logs VPN IPsec activity
VPN PKI	Extended	Logs VPN PKI activity
VPN Tunnel Status	Legacy	Logs status information on VPN tunnels.
WAN Failover	Extended	Logs WAN failover activity
Wireless	Extended	Logs wireless activity
Wlan IDS	Extended	Logs WLAN IDS activity

Managing Log Categories

The **Log Categories** table displays log category information organized into the following columns:

- **Category** - Displays log category name.
- **Description** - Provides description of the log category activity type.
- **Log** - Provides checkbox for enabling/disabling the display of the log events in on the **Log > View** page.
- **Alerts** - Provides checkbox for enabling/disabling the sending of alerts for the category.
- **Syslog** - Provides checkbox for enabling/disabling the capture of the log events into the SonicWALL security appliance Syslog.
- **Event Count** - Displays the number of events for that category. Clicking the **Refresh** button updates these numbers.

You can sort the log categories in the **Log Categories** table by clicking on the column header. For example, clicking on the **Category** header sorts the log categories in descending order from the default ascending order. An up or down arrow to the left of the column name indicates whether the column is assorted in ascending or descending order.

You can enable or disable **Log**, **Alerts**, and **Syslog** on a category by category basis by clicking on the check box for the category in the table. You can enable or disable **Log**, **Alerts**, and **Syslog** for all categories by clicking the checkbox on the column header.

Configuring Syslog Settings

Log > Syslog

In addition to the standard event log, the SonicWALL security appliance can send a detailed log to an external Syslog server. The SonicWALL Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL Syslog support requires an external server running a Syslog daemon on UDP Port 514. Syslog Analyzers such as SonicWALL ViewPoint or WebTrends Firewall Suite can be used to sort, analyze, and graph the Syslog data. Messages from the SonicWALL security appliance are then sent to the server(s). Up to three Syslog server IP addresses can be added.

The screenshot displays the SonicWALL Syslog Settings configuration page. The left sidebar contains a navigation menu with options like System, Network, SonicPoint, Firewall, VoIP, VPN, Users, Hardware Failover, Security Services, Log, View, Categories, Syslog, Automation, Name Resolution, Reports, ViewPoint, Wizards, Help, and Logout. The main content area is titled "Log > Syslog" and includes "Refresh", "Apply", "Cancel", and "?" buttons. Below this is the "Syslog Settings" section with the following fields:

- Syslog Facility: Local Use 0 (dropdown)
- Override Syslog Settings with ViewPoint Settings
- Syslog Event Redundancy Filter (seconds): 60 (text input)
- Syslog Format: Default (dropdown)
- Enable Event Rate Limiting
- Maximum Events Per Second: 10000 (text input)
- Enable Data Rate Limiting
- Maximum Bytes Per Second: 10000000 (text input)

The "Syslog Servers" section contains a table with the following data:

Server Name	Server Port	Configure
192.168.168.10	514	

Buttons for "Add..." and "Delete All" are located below the table. The status bar at the bottom indicates "Status: Ready".

Syslog Settings

Syslog Facility

- **Syslog Facility** - Allows you to select the facilities and severities of the messages based on the syslog protocol.



Cross Reference: See RCF 3164 - The BSD Syslog Protocol for more information.

- **Override Syslog Settings with ViewPoint Settings** - Check this box to override Syslog settings, if you're using SonicWALL ViewPoint for your reporting solution.



Cross Reference: For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>.

- ♦ **Syslog Event Redundancy (seconds)** - This setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Event Redundancy Rate** field, they are not written to Syslog as unique events. Instead, the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred. The **Syslog Event Redundancy** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.
- ♦ **Syslog Format** - You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select **WebTrends**, however, you must have WebTrends software installed on your system.



Alert: If the SonicWALL security appliance is managed by SonicWALL GMS, the Syslog Server fields cannot be configured by the administrator of the SonicWALL security appliance.

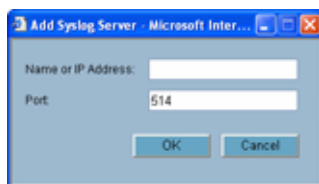
- **Enable Event Rate Limiting** - This control allows you to enable rate limiting of events to prevent the internal or external logging mechanism from being overwhelmed by log events.
- **Enable Data Rate Limiting** - This control allows you to enable rate limiting of data to prevent the internal or external logging mechanism from being overwhelmed by log events.

Syslog Servers

Adding a Syslog Server

To add syslog servers to the SonicWALL security appliance

- 1 Click **Add**. The **Add Syslog Server** window is displayed.



- 2 Type the Syslog server name or IP address in the **Name or IP Address** field. Messages from the SonicWALL security appliance are then sent to the servers.
- 3 If your syslog is not using the default port of **514**, type the port number in the **Port Number** field.
- 4 Click **OK**.
- 5 Click **Apply** to save all **Syslog Server** settings.

Configuring Log Automation

Log > Automation

The **Log > Automation** page includes settings for configuring the SonicWALL to send log files using e-mail and configuring mail server settings.

The screenshot shows the SonicWALL administration interface. The left sidebar contains a navigation menu with the following items: System, Network, Wireless, Firewall, VPN, Users, Hardware Failover, Security Services, Log, View, Categories, Syslog, Automation, Reports, ViewPoint, Wizards, Help, and Logout. The main content area is titled "Log > Automation" and includes "Apply", "Cancel", and "?" buttons. It is divided into two sections: "E-mail Log Automation" and "Mail Server Settings".

E-mail Log Automation

Send Log to E-mail Address:

Send Alerts to E-mail Address:

Send Log every at : (24-Hour Format)

Mail Server Settings

Mail Server (name or IP address):

From E-mail Address:

Authentication Method:

Status: Ready

E-mail Log Automation

- **Send Log to E-mail address** - enter your e-mail address (username@mydomain.com) in this field to receive the event log via e-mail. Once sent, the log is cleared from the SonicWALL memory. If this field is left blank, the log is not e-mailed.
- **Send Alerts to E-mail address** - enter your e-mail address (username@mydomain.com) in the **Send alerts to** field to be immediately e-mailed when attacks or system errors occur. Type a standard e-mail address or an e-mail paging service. If this field is left blank, e-mail alert messages are not sent.
- **Send Log** - determines the frequency of sending log files. The options are **When Full**, **Weekly**, or **Daily**. If the **Weekly** or **Daily** option is selected, then select the day of the week the log is sent in the **every** menu and in the **At** field, the time of day in 24-hour format in the

Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the from e-mail address, and authentication method.

- **Mail Server (name or IP address)** - Enter the IP address or FQDN of the e-mail server used to send your log e-mails in this field.
- **From E-mail Address** - Enter the E-mail address you want to display in the From field of the message.
- **Authentication Method** - You can use the default None item or select **POP Before SMTP**.

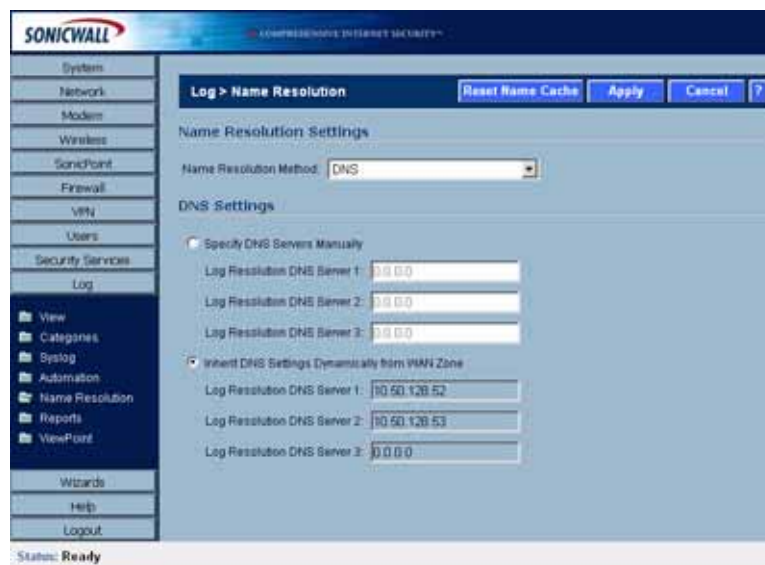


Alert: *If the **Mail Server (name or IP address)** is left blank, log and alert messages are not e-mailed.*

Configuring Name Resolution

Log > Name Resolution

The **Log > Name Resolution** page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.



The security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking **Reset Name Cache** in the top of the **Log > Name Resolution** page.

Selecting Name Resolution Settings

The security appliance can use DNS, NetBios, or both to resolve IP addresses and server names.

In the **Name Resolution Method** list, select:

- **None:** The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- **DNS:** The security appliance will use the DNS server you specify to resolve addresses and names.

- **NetBios:** The security appliance will use NetBios to resolve addresses and names. If you select NetBios, no further configuration is necessary.
- **DNS then NetBios:** The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBios.

Specifying the DNS Server

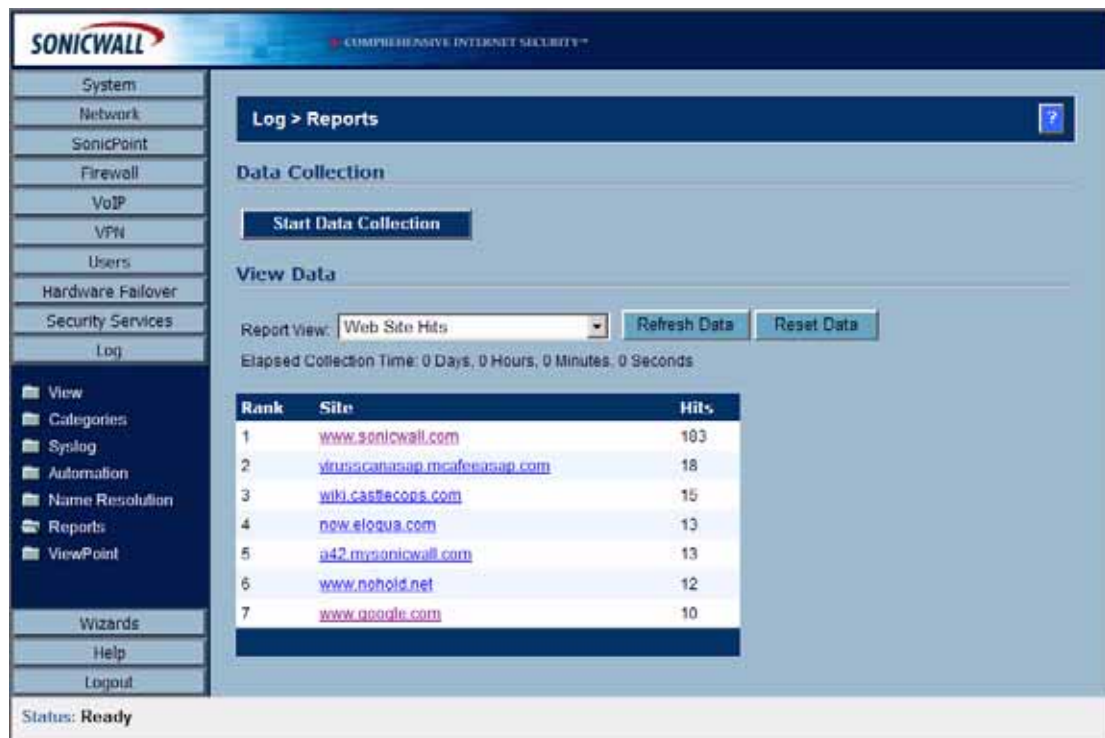
You can choose to specify DNS servers, or to use the same servers as the WAN zone.

- 1 Select **Specify DNS Servers Manually** or **Inherit DNS Settings Dynamically from WAN Zone**. The second choice is selected by default.
- 2 If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
- 3 Click **Apply** in the top right corner of the **Log > Name Resolution** page to make your changes take effect.

Generating Log Reports

Log > Reports

The SonicWALL security appliance can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. You can generate these reports from the **Log > Reports** page.



The screenshot shows the SonicWALL ViewPoint web interface. The left sidebar contains a navigation menu with options like System, Network, SonicPoint, Firewall, VoIP, VPN, Users, Hardware Failover, Security Services, Log, View, Categories, Synlog, Automation, Name Resolution, Reports, ViewPoint, Wizards, Help, and Logout. The main content area is titled "Log > Reports" and includes a "Data Collection" section with a "Start Data Collection" button. Below that is a "View Data" section with a "Report View" dropdown set to "Web Site Hits", "Refresh Data", and "Reset Data" buttons. The "Elapsed Collection Time" is shown as 0 Days, 0 Hours, 0 Minutes, 0 Seconds. A table displays the top 7 most frequently accessed web sites:

Rank	Site	Hits
1	www.sonicwall.com	103
2	viruscanasap.mcafeeasap.com	18
3	wiki.castsecops.com	15
4	now.elogua.com	13
5	a42.mysonicwall.com	13
6	www.nohold.net	12
7	www.google.com	10

The status bar at the bottom indicates "Status: Ready".



Note: SonicWALL ViewPoint provides a comprehensive Web-based reporting solution for SonicWALL security appliances. For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>

Data Collection

The **Reports** window includes the following functions and commands:

- **Start Data Collection**

Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.

- **Reset Data**

Click **Reset Data** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the SonicWALL security appliance is restarted.

View Data

Select the desired report from the **Report to view** menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below. Click **Refresh Data** to update the report. The length of time analyzed by the report is displayed in the **Current Sample Period**.

Web Site Hits

Selecting **Web Site Hits** from the **Report to view** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites. For information on blocking inappropriate Web sites, see [Chapter 53, Configuring SonicWALL Content Filtering Service](#).

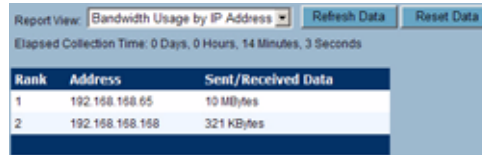
Click on the name of a Web site to open that site in a new window.



Rank	Site	Hits
1	www.sonicwall.com	827
2	www.mailtofilter.com	65
3	a42.mysonicwall.com	56
4	sonicwall.mediaroom.com	42
5	nzw.eloqua.com	34
6	www.sonicwall.de	19
7	virusscan.asp.mcafeeasap.com	18
8	pho.hitbox.com	16
9	www.nshold.net	15
10	wifi.castlecoops.com	15
11	www.google.com	10
12	www.lasalogic.com	5
13	loc1.hitprocessor.com	4
14	a42.sonicwall.com	3
15	stats.hitbox.com	2

Bandwidth Usage by IP Address

Selecting **Bandwidth Usage by IP Address** from the **Report to view** menu displays a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

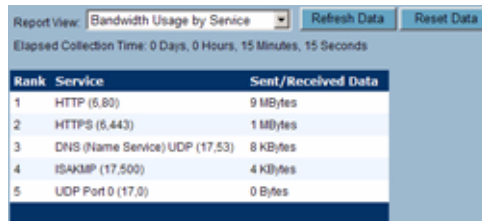


Rank	Address	Sent/Received Data
1	192.168.168.65	10 MBytes
2	192.168.168.168	321 KBytes

Bandwidth Usage by Service

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

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.



Rank	Service	Sent/Received Data
1	HTTP (6.80)	9 MBytes
2	HTTPS (6.643)	1 MBytes
3	DNS (Name Service) UDP (17.53)	8 KBytes
4	ISAKMP (17.500)	4 KBytes
5	UDP Port 0 (17.0)	0 Bytes

Activating SonicWALL ViewPoint

Log > ViewPoint

SonicWALL ViewPoint is a Web-based graphical reporting tool that provides unprecedented security awareness and control over your network environment through detailed and comprehensive reports of your security and network activities. ViewPoint's broad reporting capabilities allow administrators to easily monitor network access and Internet usage, enhance security, assess risks, understand more about employee Internet use and productivity, and anticipate future bandwidth needs.

ViewPoint creates dynamic, real-time and historical network summaries, providing a flexible, comprehensive view of network events and activities. Reports are based on syslog data streams received from each SonicWALL appliance through LAN, Wireless LAN, WAN or VPN connections. With ViewPoint, your organization can generate individual or aggregate reports about virtually any aspect of appliance activity, including individual user or group usage patterns, events on specific appliances or groups of appliances, types and times of attacks, resource consumption and constraints, and more.



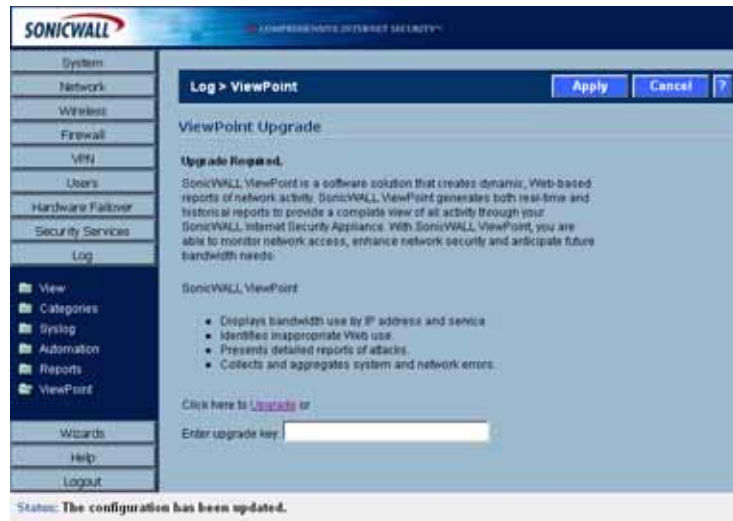
Cross Reference: For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>.



Cross Reference: For complete SonicWALL ViewPoint documentation, go to the SonicWALL documentation Web site at <http://www.sonicwall.com/services/documentation.html>.

Activating ViewPoint

The **Log > ViewPoint** page allows you to activate the ViewPoint license directly from the SonicWALL Management Interface using two methods.



If you received a license activation key, enter the activation key in the Enter upgrade key field, and click **Apply**.



Alert: You must have a [mySonicWALL.com](https://www.mysonicwall.com) account and your SonicWALL security appliance must be registered to activate SonicWALL ViewPoint for your SonicWALL security appliance.

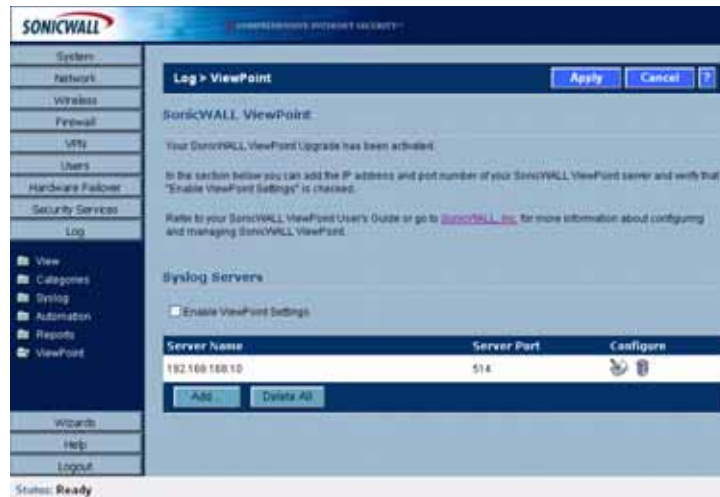
- 1 Click the **Upgrade** link in **Click here to Upgrade** on the **Log > ViewPoint** page. The **mySonicWALL.com Login** page is displayed.



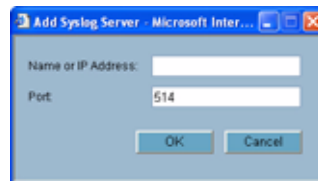
- 2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.
- 3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**.
- 4 If you activated SonicWALL ViewPoint at mySonicWALL.com, the SonicWALL ViewPoint activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL.

Enabling ViewPoint Settings

Once you have installed the SonicWALL ViewPoint software, you can point the SonicWALL security appliance to the server running ViewPoint.



- 1 Check the **Enable ViewPoint Settings** checkbox in the **Syslog Servers** section of the **Log > ViewPoint** page.
- 2 Click the **Add** button. The **Add Syslog Server** window is displayed.



- 3 Enter the IP address or FQDN of the SonicWALL ViewPoint server in the **Name or IP Address** field.
- 4 Enter the port number for the SonicWALL ViewPoint server traffic in the **Port** field or use the default port number.
- 5 Click **Apply**.



Note: The **Override Syslog Settings with ViewPoint Settings** control on the **Log > Syslog** page is automatically checked when you enable ViewPoint from the **Log > ViewPoint** page. The IP address or FQDN you entered in the **Add Syslog Server** window is also displayed on the **Log > Syslog** page as well as in the **Syslog Servers** table on the **Log > ViewPoint** page.

Clicking the Edit icon displays the **Add Syslog Server** window for editing the ViewPoint server information. Clicking the Delete (Trashcan) icon, deletes the ViewPoint syslog server entry.

PART
14

Wizards

Configuring Internet Connectivity Using the Setup Wizard

Internet Connectivity Using the Setup Wizard

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



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

Using the Setup Wizard

The Setup Wizard

The Setup Wizard helps you configure the following settings:

- Wireless deployment scenario (TZ 170 Wireless and TZ 170 SP Wireless)
- Modem settings (TZ 170 SP and TZ 170 SP Wireless)
- WAN networking mode and WAN network configuration (All SonicWALL security appliances)
- LAN network configuration
- WLAN network configuration (TZ 170 Wireless and TZ 170 SP Wireless)
- WiFiSec secure wireless connectivity settings (TZ 170 Wireless and TZ 170 SP Wireless)
- Wireless Guest Services (TZ 170 Wireless and TZ 170 SP Wireless)

The **Setup Wizard** screens change depending on the choices you make. For example, if you choose Guest Internet Gateway, The **Setup Wizard** will display the screens for Modem, WAN, WLAN, and Wireless Guest Services setup. It will not display the screens for LAN and WiFiSec setup, because they do not apply in a Guest Internet Gateway deployment.

Wireless Deployment Scenarios

If you are setting up a TZ 170 Wireless and TZ 170 SP Wireless, the **Setup Wizard** provides the following four wireless deployment scenarios:

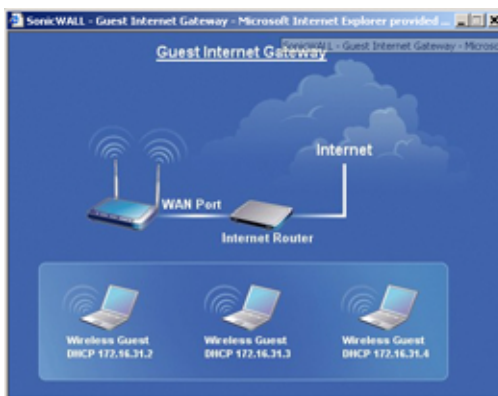
Office Gateway - Provides secure access for wired and wireless users on your network.



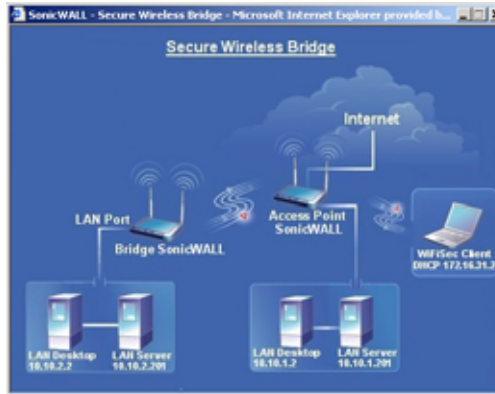
Secure Access Point - Add secure wireless access to an existing wireless network.



Guest Internet Gateway - Provide guests controlled wireless access to the Internet only.



Secure Wireless Bridge - Operate in wireless bridge mode to securely bridge two networks with WiFiSec.



Configuring a Static IP Address with NAT Enabled

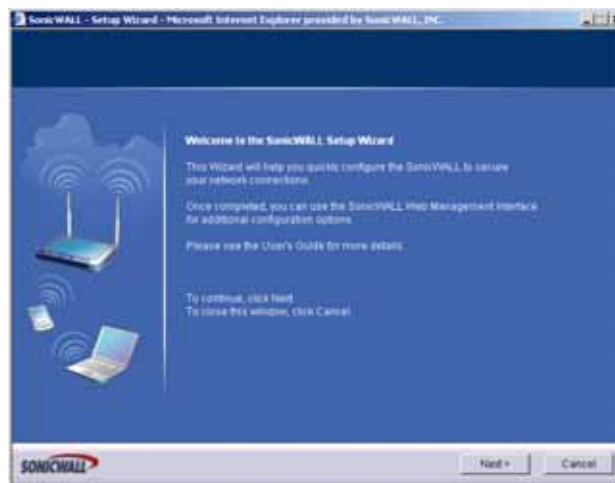
Using NAT to set up your SonicWALL eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough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

Start the 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 meet these criteria.

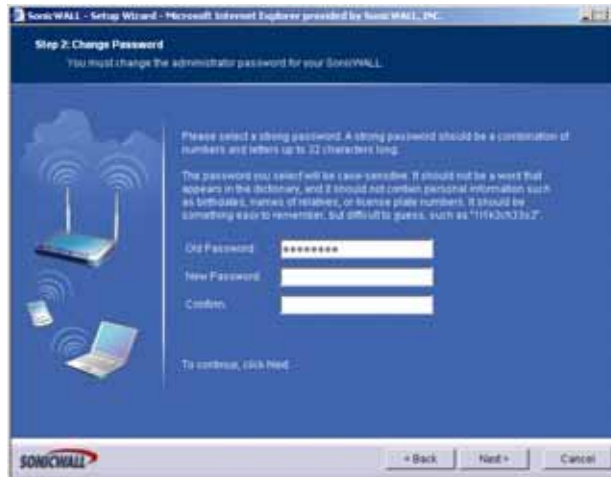
- 1 Click the **Setup Wizard** button on the **Network > Settings** page. Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Select the Wireless Deployment Scenario



- 2 For the TZ 170 Wireless and TZ 170 SP Wireless, select the Wireless Deployment Scenario and click **Next**.

Step 2: Change Password

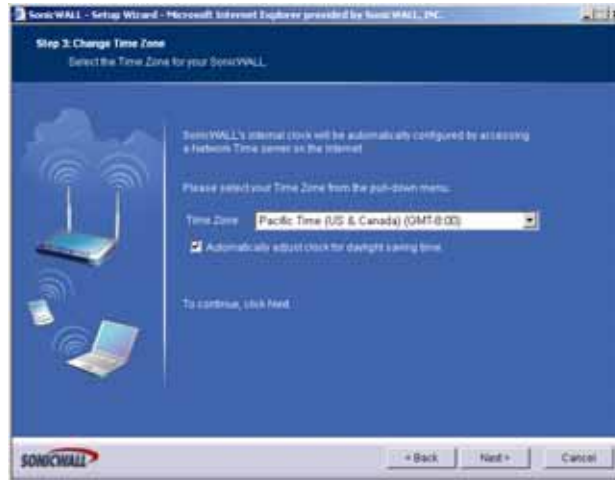


- 3 To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.



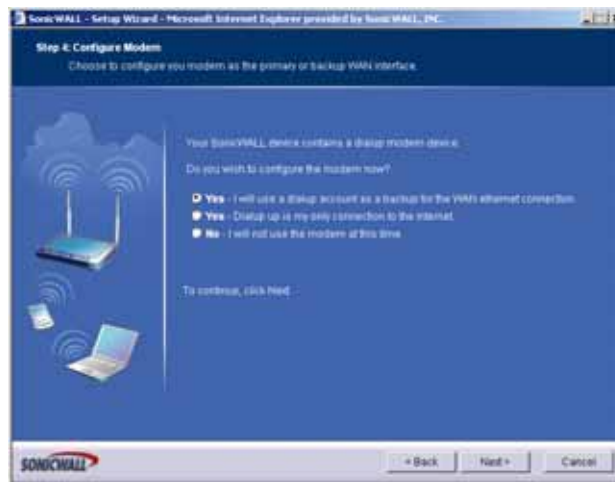
Tip: It is very important to choose a password which cannot be easily guessed by others.

Step 3: Change Time Zone



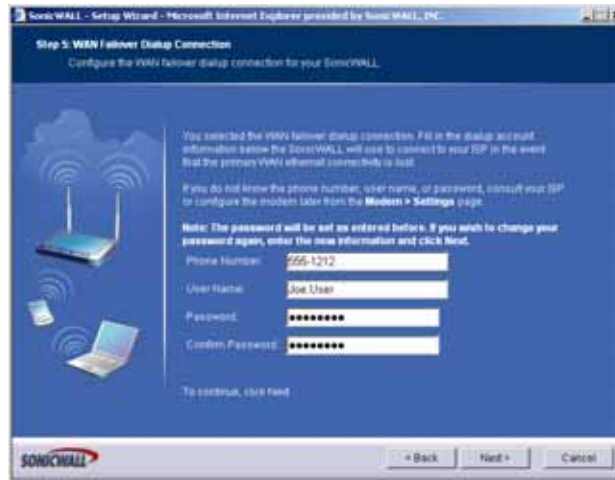
- 4 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 4: Configure the Modem



- 5 If you are setting up a SonicWALL TZ 170 SP or TZ 170 SP Wireless, select how you will use the modem. You can choose to use the modem:
- ◆ As a backup to your WAN
 - ◆ As your primary internet connection. **Note:** If you choose to use the modem as your primary connection, the Setup Wizard will not ask you to configure the WAN interface.
 - ◆ Not use the modem
- 6 Click **Next**.

7 If you chose to use the modem, enter the Dial-up Connection information



8 Enter the dial-up **Phone Number**, **User Name**, and **Password**. Click **Next**.

Step 5: WAN Network Mode



9 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.

10 Choose **Static IP** and click **Next**.

Step 6: WAN Network Mode: NAT Enabled

- 11 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 7: LAN Settings

- 12 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 8: LAN DHCP Settings



- 13 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.

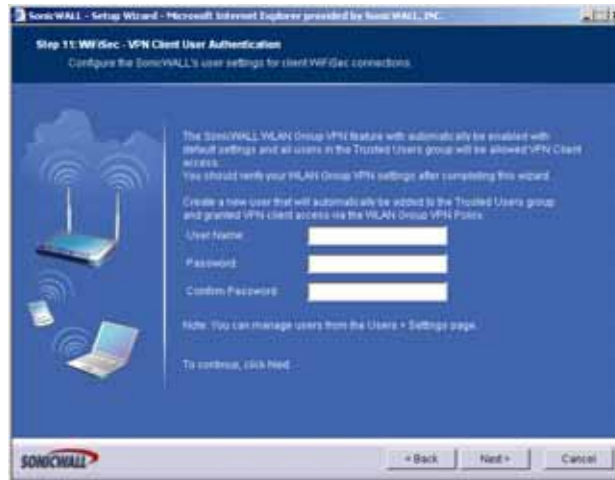
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

Step 9: WLAN 802.11b/g Settings



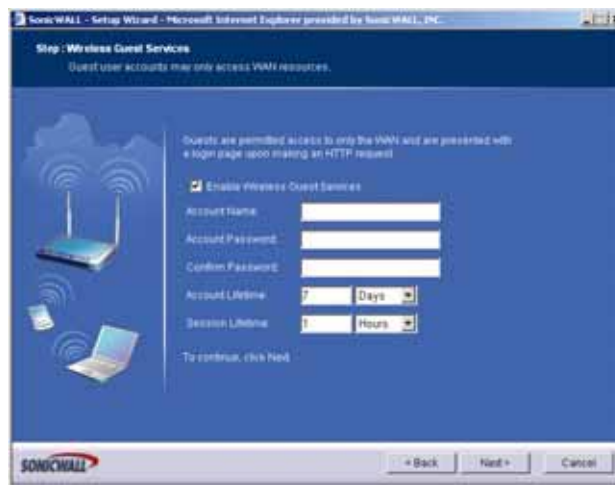
- 14 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, configure the radio settings for the security appliance. Click **Next**.

Step 10: WiFiSec - VPN Client User Authentication



- 15 Enter a first user for the WLAN GroupVPN policy. Use this username and password when you first connect wirelessly to the TZ 170 Wireless or TZ 170 SP Wireless. Click **Next**.

Step 11: Wireless Guest Services



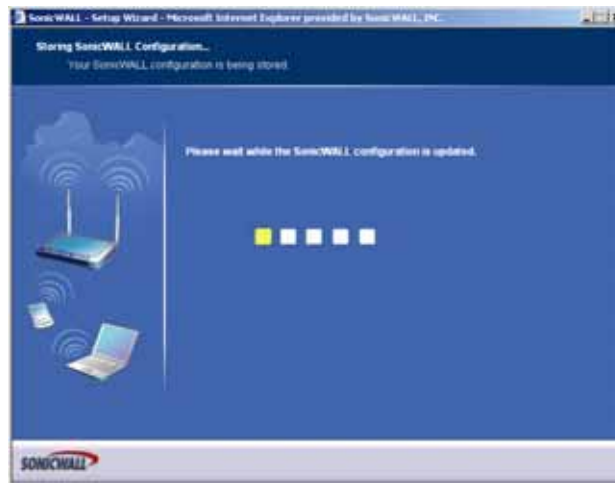
- 16 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, select whether you want to enable Guest Services, and configure an initial guest account. Click **Next**.

Step 12: SonicWALL Configuration Summary



- 17 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

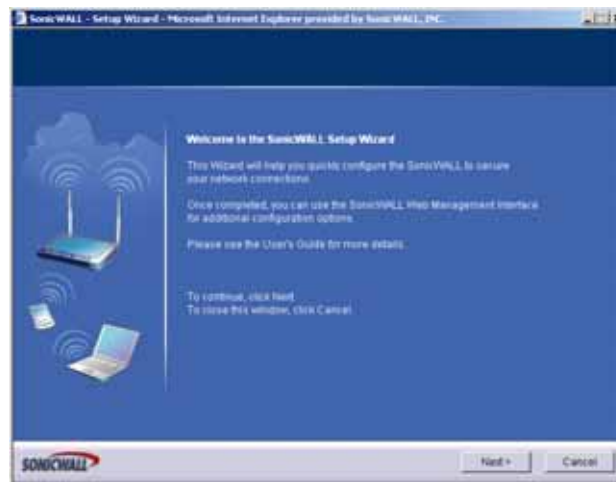


- 18 The SonicWALL stores the network settings.
- 19 Click **Close** to return to the SonicWALL Management Interface.

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.



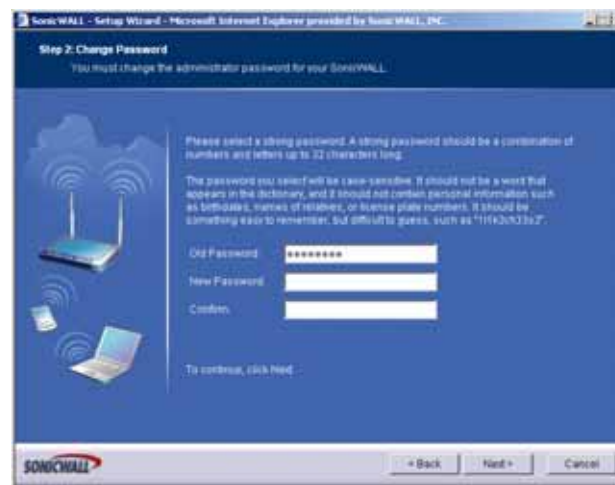
- 2 Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Select the Wireless Deployment Scenario



- 3 For the TZ 170 Wireless and TZ 170 SP Wireless, select the Wireless Deployment Scenario and click **Next**.

Step 2: Change Password

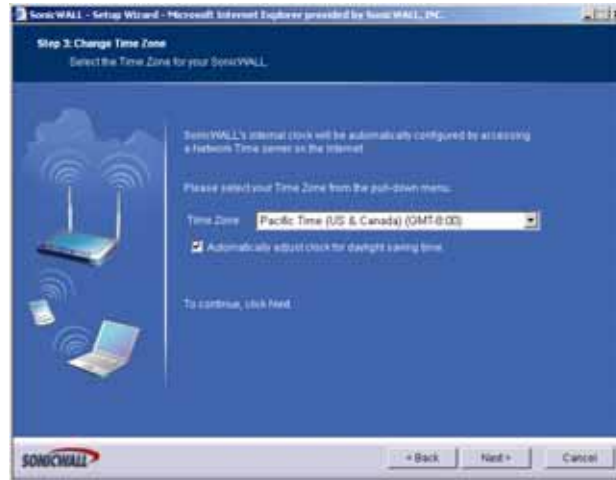


- 4 To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.



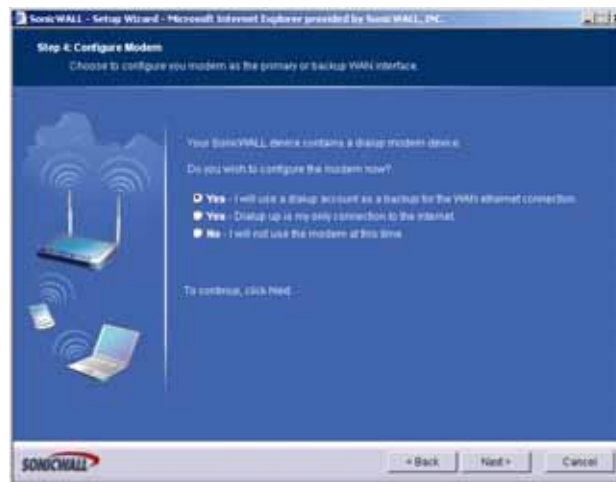
Tip: *It is very important to choose a password which cannot be easily guessed by others.*

Step 3: Change Time Zone



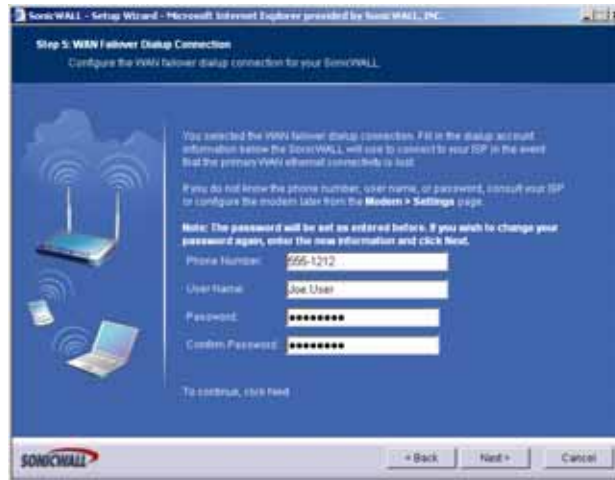
- 5 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 4: Configure the Modem



- 6 If you are setting up a SonicWALL TZ 170 SP or TZ 170 SP Wireless, select how you will use the modem. You can choose to use the modem:
- ◆ As a backup to your WAN
 - ◆ As your primary internet connection. **Note:** If you choose to use the modem as your primary connection, the Setup Wizard will not ask you to configure the WAN interface.
 - ◆ Not use the modem
- 7 Click **Next**.

8 If you chose to use the modem, enter the Dial-up Connection information



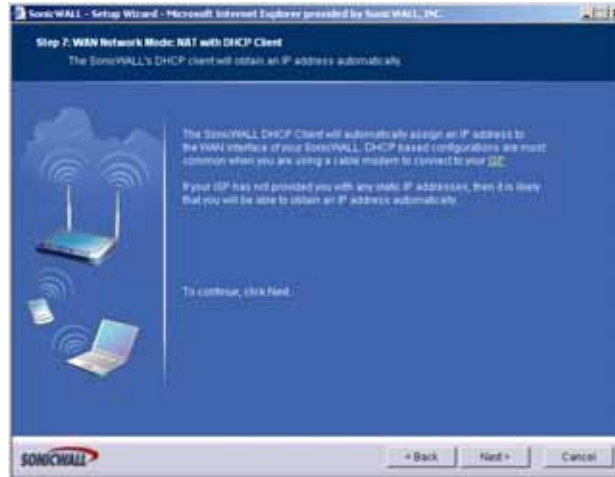
9 Enter the dial-up **Phone Number**, **User Name**, and **Password**. Click **Next**.

Step 5: WAN Network Mode



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

Step 6: WAN Network Mode: NAT with DHCP Client



- 11 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 7: LAN Settings



- 12 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 8: DHCP Settings



- 13 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.

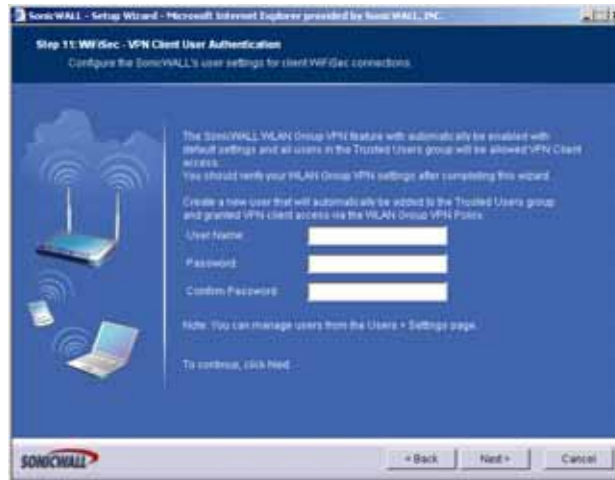
If **Enable DHCP Server** is not selected, the DHCP Server is disabled. Click **Next** to continue.

Step 9: WLAN 802.11b/g Settings



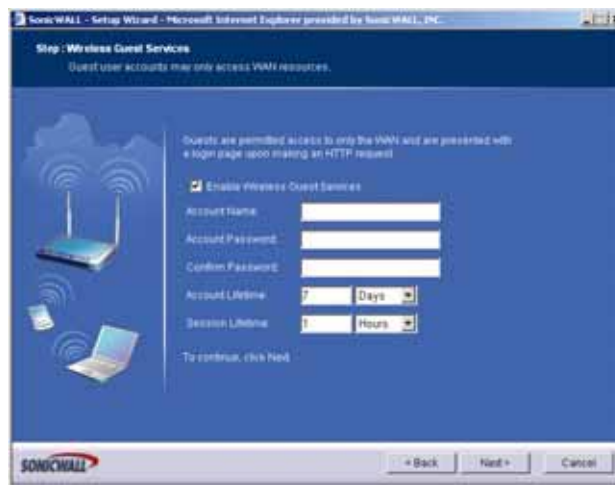
- 14 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, configure the radio settings for the security appliance. Click **Next**.

Step 10: WiFiSec - VPN Client User Authentication



- 15 Enter a first user for the WLAN GroupVPN policy. Use this username and password when you first connect wirelessly to the TZ 170 Wireless or TZ 170 SP Wireless. Click **Next**.

Step 11: Wireless Guest Services



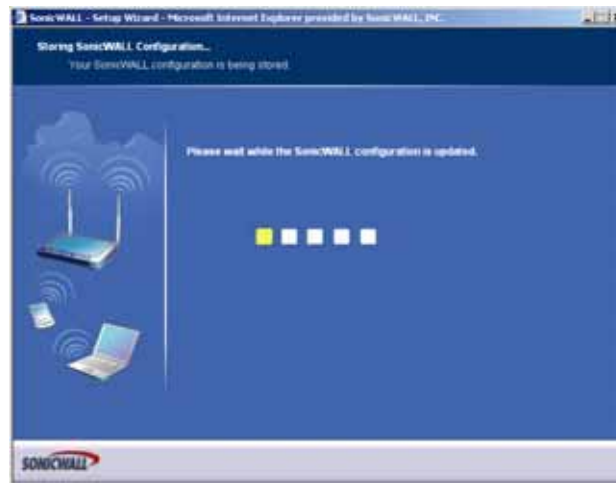
- 16 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, select whether you want to enable Guest Services, and configure an initial guest account. Click **Next**.

Step 12: SonicWALL Configuration Summary



- 17 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



- 18 The SonicWALL stores the network settings.
- 19 Click **Close** to return to the SonicWALL Management Interface.

✓ **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.



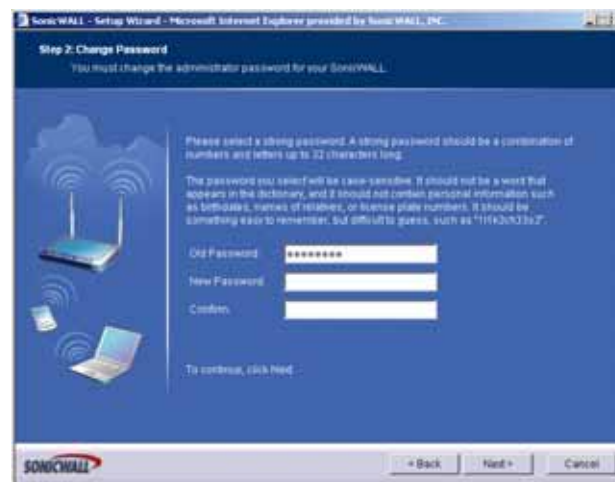
- 2 Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Select the Wireless Deployment Scenario



- 3 For the TZ 170 Wireless and TZ 170 SP Wireless, select the Wireless Deployment Scenario and click **Next**.

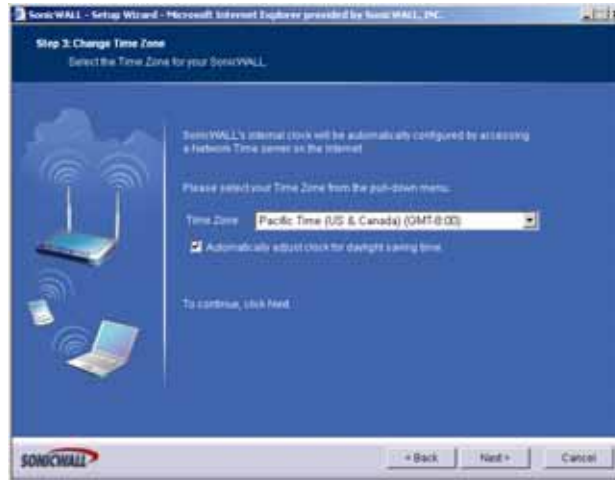
Step 2: Change Password



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

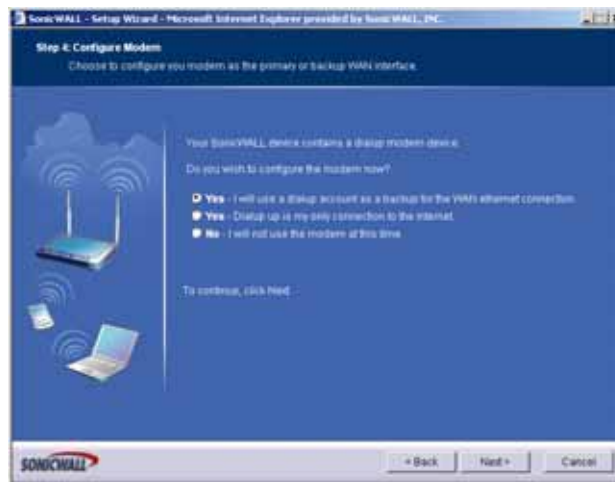
✓ **Tip:** *It is very important to choose a password which cannot be easily guessed by others.*

Step 3: Change Time Zone



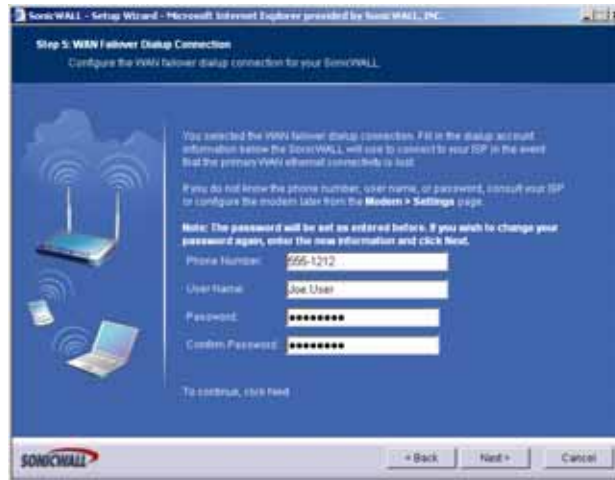
- 5 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 4: Configure the Modem



- 6 If you are setting up a SonicWALL TZ 170 SP or TZ 170 SP Wireless, select how you will use the modem. You can choose to use the modem:
- ◆ As a backup to your WAN
 - ◆ As your primary internet connection. **Note:** If you choose to use the modem as your primary connection, the Setup Wizard will not ask you to configure the WAN interface.
 - ◆ Not use the modem
- 7 Click **Next**.

8 If you chose to use the modem, enter the Dial-up Connection information



9 Enter the dial-up **Phone Number**, **User Name**, and **Password**. Click **Next**.

Step 5: WAN Network Mode



10 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 6: WAN Network Mode: NAT with PPPoE Client



- 11 Select whether to use a dynamic or static IP address, and enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.

Step 7: LAN Settings



- 12 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**.

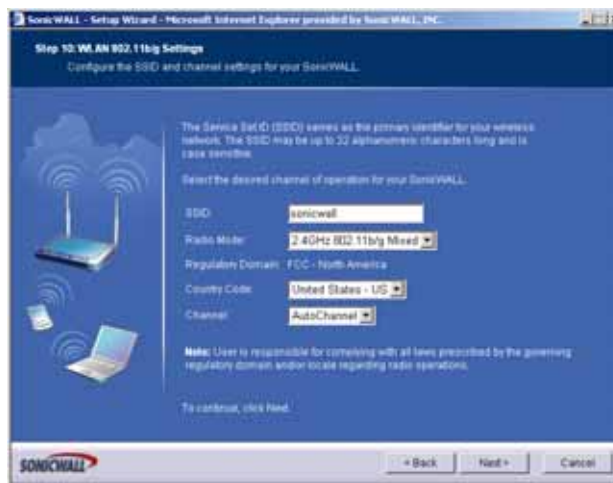
Step 8: DHCP Server



- 13 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.

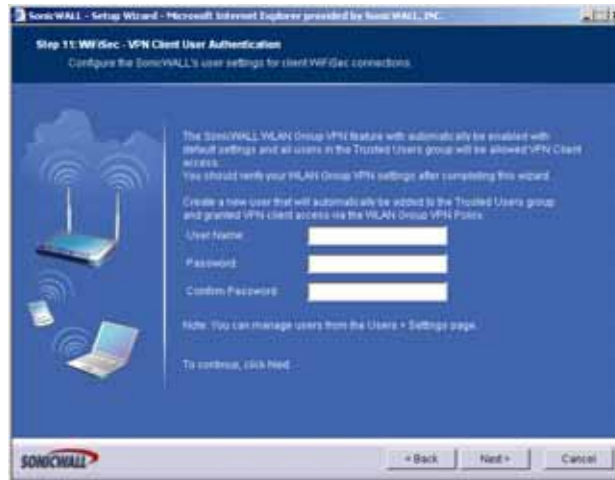
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

Step 9: WLAN 802.11b/g Settings



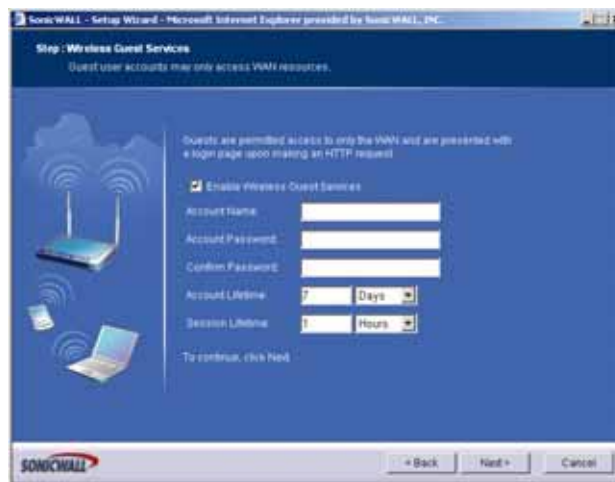
- 14 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, configure the radio settings for the security appliance. Click **Next**.

Step 10: WiFiSec - VPN Client User Authentication



- 15 Enter a first user for the WLAN GroupVPN policy. Use this username and password when you first connect wirelessly to the TZ 170 Wireless or TZ 170 SP Wireless. Click **Next**.

Step 11: Wireless Guest Services



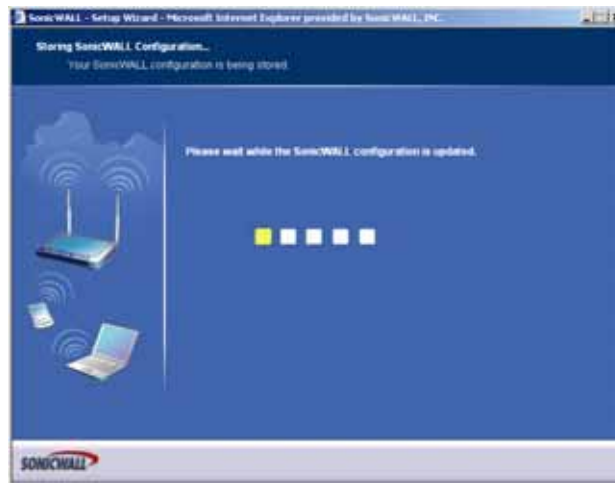
- 16 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, select whether you want to enable Guest Services, and configure an initial guest account. Click **Next**.

Step 12: SonicWALL Configuration Summary



- 17 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



- 18 The SonicWALL stores the network settings.
- 19 Click **Close** to return to the SonicWALL Management Interface.

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.



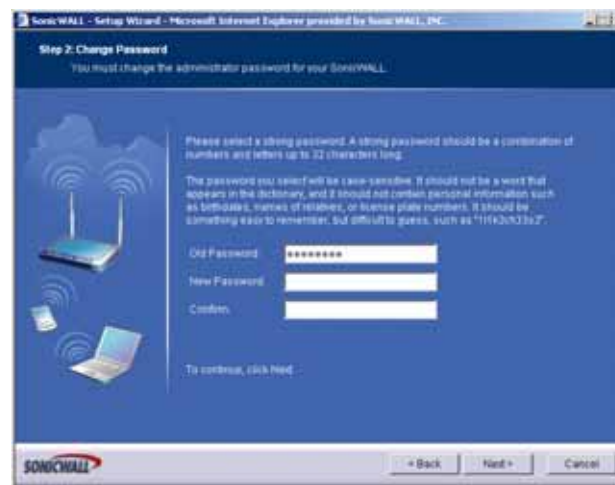
- 2 Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Select the Wireless Deployment Scenario



- 3 For the TZ 170 Wireless and TZ 170 SP Wireless, select the Wireless Deployment Scenario and click **Next**.

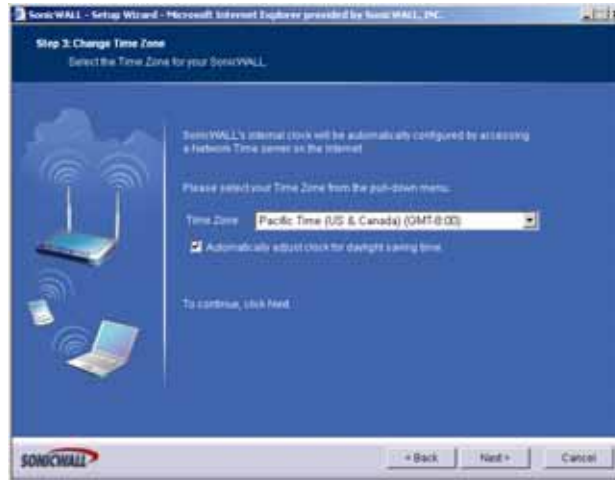
Step 2: Change Password



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

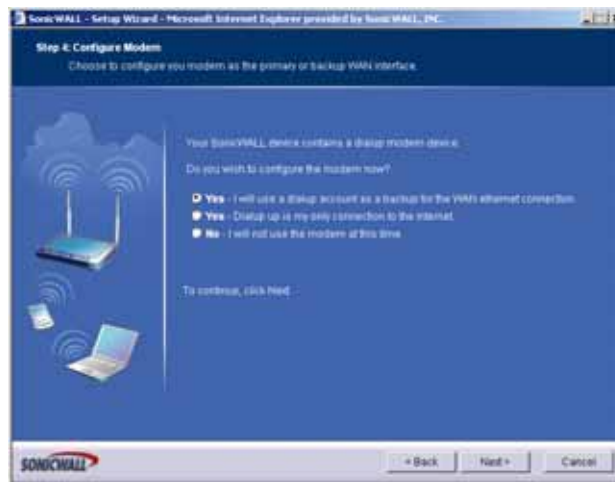
✓ **Tip:** *It is very important to choose a password which cannot be easily guessed by others.*

Step 3: Change Time Zone



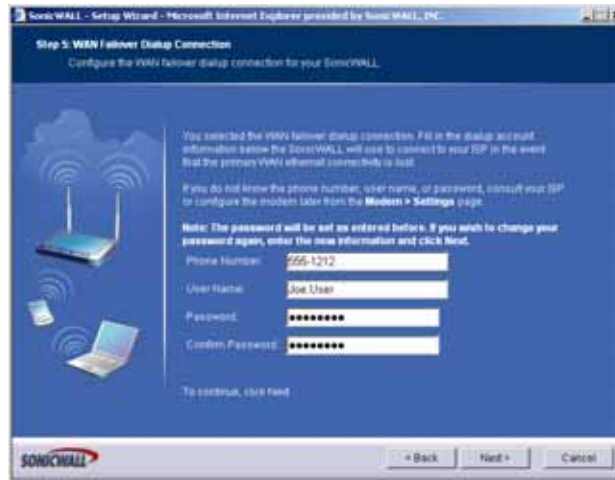
- 5 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 4: Configure the Modem



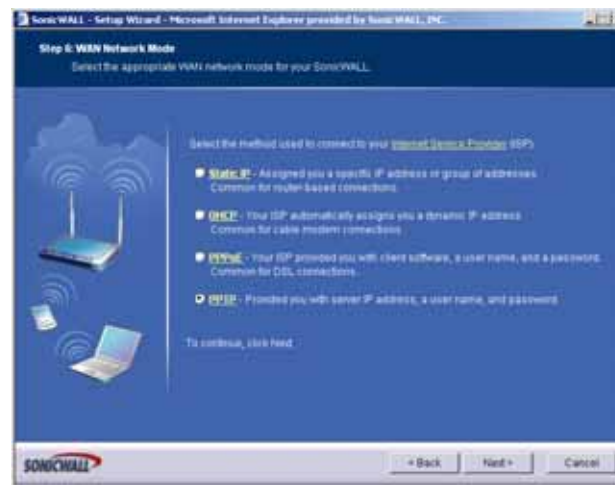
- 6 If you are setting up a SonicWALL TZ 170 SP or TZ 170 SP Wireless, select how you will use the modem. You can choose to use the modem:
- ◆ As a backup to your WAN
 - ◆ As your primary internet connection. **Note:** If you choose to use the modem as your primary connection, the Setup Wizard will not ask you to configure the WAN interface.
 - ◆ Not use the modem
- 7 Click **Next**.

8 If you chose to use the modem, enter the Dial-up Connection information



9 Enter the dial-up **Phone Number**, **User Name**, and **Password**. Click **Next**.

Step 5: WAN Network Mode



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

Step 6: WAN Network Mode: NAT with PPTP Client

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

Step 7: LAN Settings

- 12 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**.

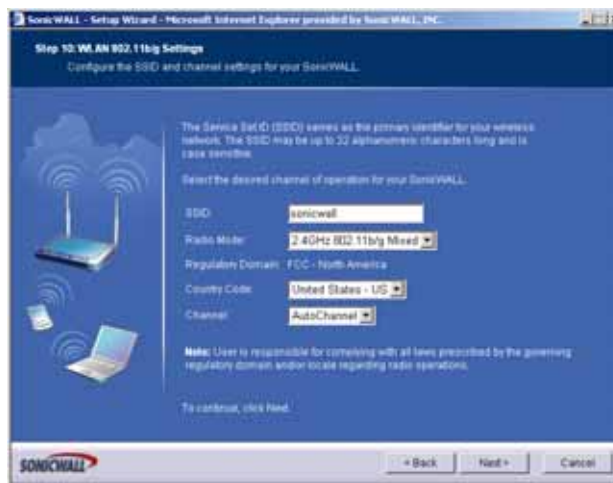
Step 8: DHCP Server



- 13 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.

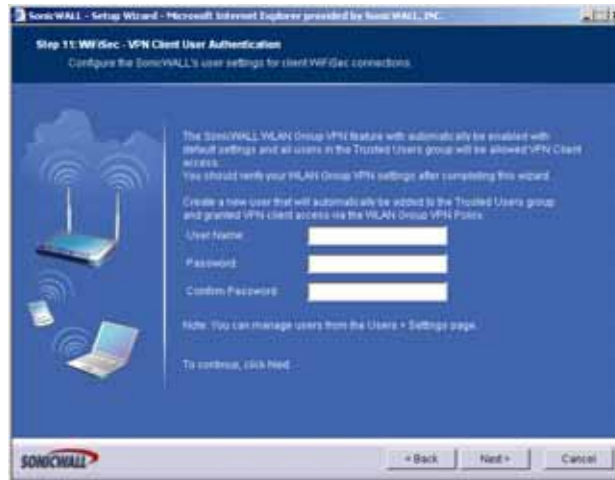
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

Step 9: WLAN 802.11b/g Settings



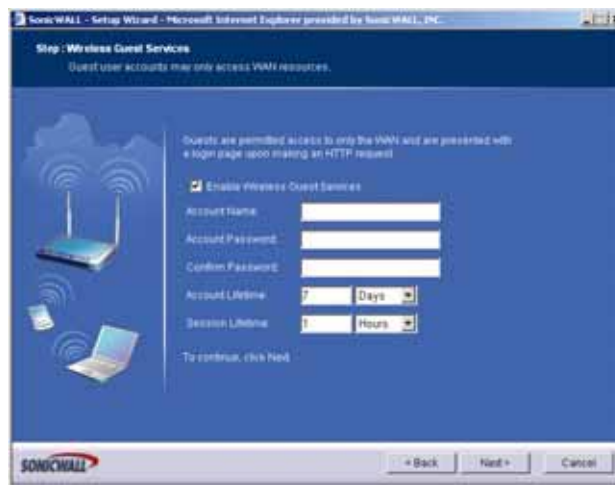
- 14 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, configure the radio settings for the security appliance. Click **Next**.

Step 10: WiFiSec - VPN Client User Authentication



- 15 Enter a first user for the WLAN GroupVPN policy. Use this username and password when you first connect wirelessly to the TZ 170 Wireless or TZ 170 SP Wireless. Click **Next**.

Step 11: Wireless Guest Services



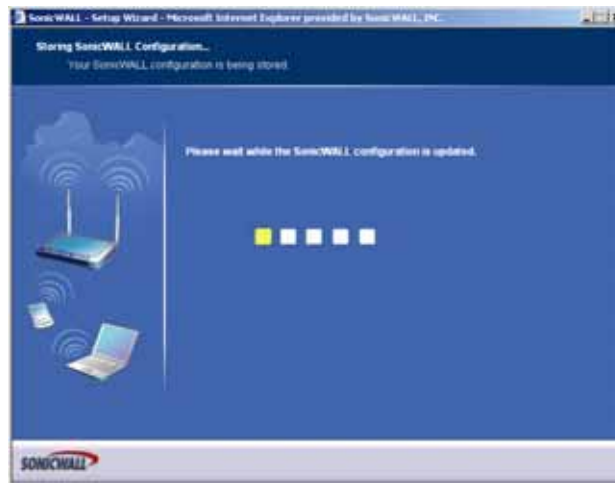
- 16 If you are setting up a TZ 170 Wireless or TZ 170 SP Wireless, select whether you want to enable Guest Services, and configure an initial guest account. Click **Next**.

Step 12: SonicWALL Configuration Summary



- 17 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

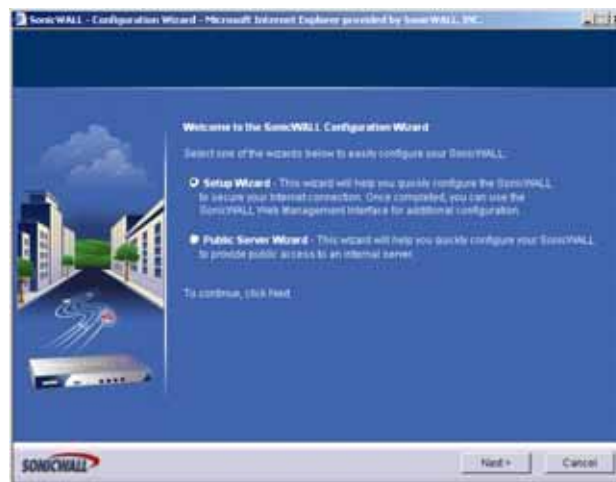


- 18 The SonicWALL stores the network settings.
- 19 Click **Close** to return to the SonicWALL Management Interface.

Configuring a Public Server with the Wizard

Create a Server with the Public Server Wizard

- 1 Start the wizard: In the navigator, click **Wizards**.



- 2 Select **Public Server Wizard** and click **Next**.



- 3 Select the type of server from the **Server Type** list. Depending on the type you select, the available services change. Check the box for the services you are enabling on this server. Click **Next**



- 4 Enter the name of the server.
- 5 Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to zone where you want to put this server. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs.
- 6 Click **Next**.



- 7 Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

8 Click **Next**.

9 The Summary page displays a summary of all the configuration you have performed in the wizard. It should show:



- Server Address Objects

The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the wizard binds the address object to the DMZ zone. It gives the object a name of the name you specified for the server plus “_private”. If you specify an IP in the range of another zone, it will bind the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the wizard will bind the address object to the LAN zone.

Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another address, the server will create an object for that address bound to the WAN zone and assign the new address object a name of the name you specified for the server plus “_public”.

- Server Service Group Object

The wizard creates a service group object for the services used by the new server. Because the server in the example is a web server, the service group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.

- Server NAT Policies

The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (10.0.93.43), the NAT policy will translate its address to 172.22.2.44.

The wizard also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

- Server Access Rules

The wizard creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.

- 10 Click **Apply** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your SonicWALL.



✓ **Tip:** The new IP address used to access the new server, internally and externally is displayed in the **URL** field of the **Congratulations** window.



- 11 Click **Close** to close the wizard.

Configuring VPN Policies with the VPN Policy Wizard

Configuring GroupVPN using the VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN on the SonicWALL. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the SonicWALL Management Interface for optional advanced configuration options.

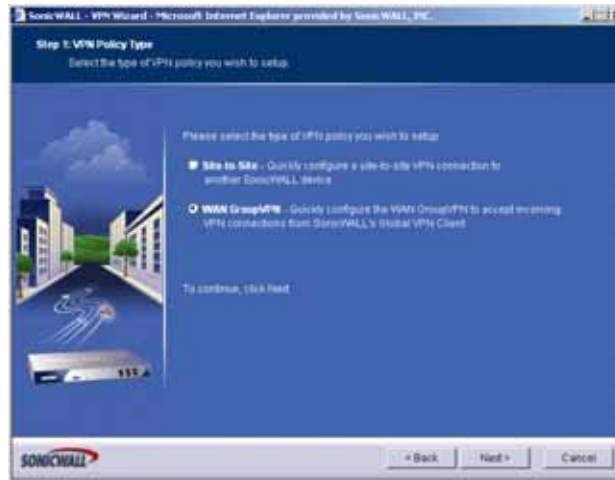
Using the VPN Policy Wizard

1. In the top right corner of the **VPN > Settings** page, click on **VPN Policy Wizard**.

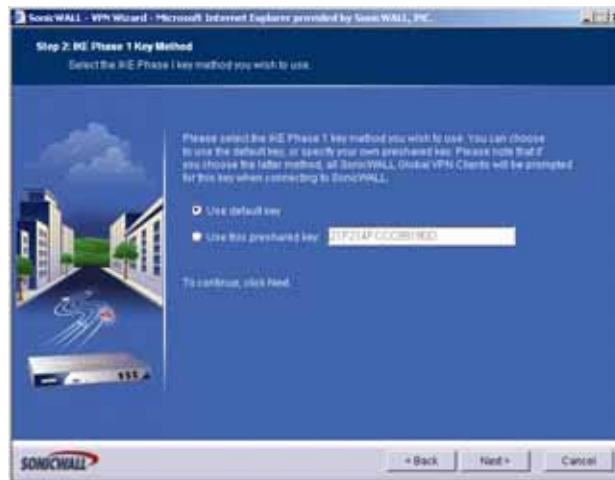


2. Click **Next**.

3. In the **VPN Policy Type** page, select **WAN GroupVPN** and click **Next**.



4. In the **IKE Phase 1 Key Method** page, you select the authentication key to use for this VPN policy:



- ♦ **Default Key:** If you choose the default key, all your Global VPN Clients and Global Security Clients will automatically use the default key generated by the SonicWALL to authenticate with the SonicWALL.
- ♦ **Use this Key:** If you choose a custom preshared key, you must distribute the key to every VPN Client because the user is prompted for this key when connecting to the SonicWALL.



Note: If you select *Use this Key*, and leave the default key as the value, you must still distribute the key to your VPN clients.

5. Click **Next**.

6. In the **IKE Security Settings** page, you select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the defaults settings.



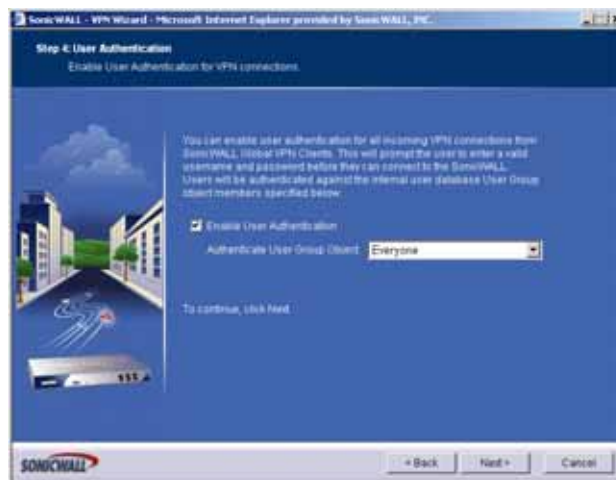
- ◆ **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.
- ◆ **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel.
- ◆ **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
- ◆ **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).



Alert: *The SonicWALL Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWALL Global VPN Client versions 2.x and higher will be able to connect.*

7. Click **Next**.

8. In the **User Authentication** page, select if you want the VPN Users to be required to authenticate with the firewall when they connect. If you select **Enable User Authentication**, you must select the user group which contains the VPN users. For this example, leave **Enable User Authentication** unchecked.





Note: If you enable user authentication, the users must be entered in the SonicWALL database for authentication. Users are entered into the SonicWALL database on the **Users > Local Users** page, and then added to groups in the **Users > Local Groups** page.

9. Click **Next**.
10. In the **Configure Virtual IP Adapter** page, select whether you want to use the SonicWALL's internal DHCP server to assign each VPN client IP address from the LAN zone's IP range. Therefore, when a user connects, it appears that the user is inside the LAN. Check the **Use Virtual IP Adapter** box and click **Next**.



11. The **Configuration Summary** page details the settings that will be pushed to the SonicWALL when you apply the configuration. Click **Apply** to create your GroupVPN.



Connecting the Global VPN Clients

Remote SonicWALL Global VPN Clients install the Global VPN Client software. Once the application is installed, they use a connection wizard to setup their VPN connection. To configure the VPN connection, the client must have the following information:

- A public IP address (or domain name) of the WAN port for your SonicWALL
- The shared secret if you selected a custom pre-shared secret in the VPN Wizard.
- The authentication username and password.

Configuring a Site-to-Site VPN using the VPN Wizard

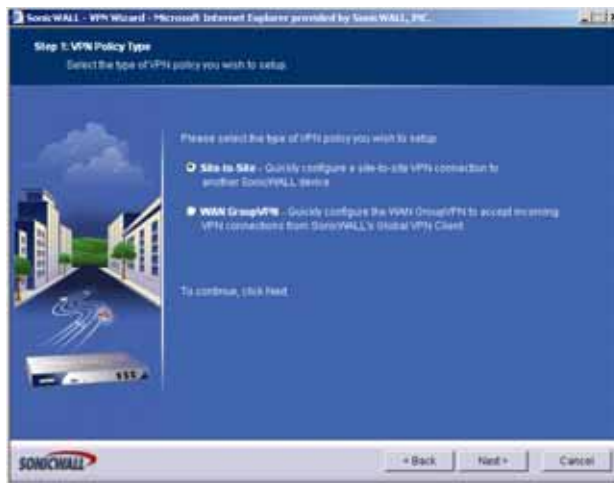
You use the **VPN Policy Wizard** to create the site-to-site VPN policy.

Using the VPN Wizard to Configure Preshared Secret

1. On the **System > Status** page, click on **Wizards**.
2. In the **Welcome to the SonicWALL Configuration Wizard** page select **VPN Wizard** and click **Next**.



3. In the **VPN Policy Type** page, select **Site-to-Site** and click **Next**.



4. In the **Create Site-to-Site Policy** page, enter the following information:

- **Policy Name:** Enter a name you can use to refer to the policy. For example, Boston Office.
- **Preshared Key:** Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default SonicWALL generated Preshared Key.
- **I know my Remote Peer IP Address (or FQDN):** If you check this option, this SonicWALL can initiate the contact with the named remote peer.

If you do not check this option, the peer must initiate contact to create a VPN tunnel. This device will use aggressive mode for IKE negotiation.

For this example, leave the option unchecked.

- **Remote Peer IP Address (or FQDN):** If you checked the option above, enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (For example, *boston.yourcompany.com*).
5. Click **Next**.
6. In the **Network Selection** page, select the local and destination resources this VPN will be connecting:

- **Local Networks:** Select the local network resources protected by this SonicWALL that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses.

If the object or group you want has not been created yet, select **Create Object** or **Create Group**. Create the new object or group in the dialog box that pops up. Then select the new object or group.

For this example, select **LAN Subnets**.

- **Destination Networks:** Select the network resources on the destination end of the VPN Tunnel. If the object or group does not exist, select **Create new Address Object** or **Create new Address Group**.

For example:

- a Select **Create new Address Group**.



- b In the **Name** field, enter "LAN Group".

- c In the list on the left, select **LAN Subnets** and click the **->** button.

- d Click **OK** to create the group and return to the Network Selection page.
 - e In the **Destination Networks** field, select the newly created group.
7. Click **Next**.
 8. In the **IKE Security Settings** page, select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the default settings.



- **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.
 - **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel
 - **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
 - **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).
9. The **Configuration Summary** page details the settings that will be pushed to the security appliance when you apply the configuration.



10. Click **Apply** to create the VPN.



Configuring Your Wireless Network with the Wireless Wizard

Using the Wireless Wizard

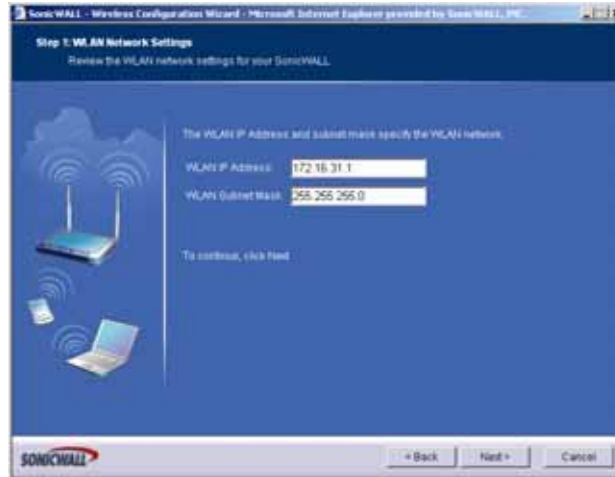
You can use the Wireless Wizard to quickly and easily set up your wireless network for your SonicWALL TZ 170 Wireless or TZ 170 SP Wireless. Log in to your security appliance, and click **Wireless** on the menu bar. Click **Wireless Wizard** to launch the wizard and begin the configuration process. Or click **Wizards**, and select **Wireless Wizard**.

Welcome to the SonicWALL Wireless Configuration Wizard



1. When the Wireless Wizard launches, the **Welcome** page is displayed. Click **Next** to continue configuration.

WLAN Network Settings



2. Use the default IP address for the WLAN or choose a different private IP address. The default value works for most networks. Click **Next** to continue.



Alert: You cannot use the same private IP address range as the range assigned to the LAN port.

WLAN 802.11b Settings



3. Type a unique identifier for the TZ 170 Wireless or TZ 170 SP Wireless in the SSID field. It can be up to 32 alphanumeric characters in length and is case-sensitive. The default value is **sonicwall**.

WLAN Security Settings



4. Choose the desired security setting for the wireless network. **WiFiSec** is the most secure and enforces IPsec over the wireless network. If you have an existing wireless network and want to use the SonicWALL security appliance, select **WEP + Stealth Mode**.

WiFiSec - VPN Client User Authentication

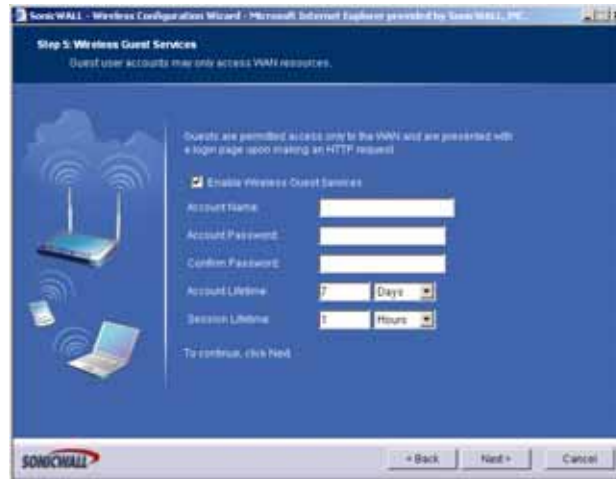


5. Create a new user with VPN Client privileges by typing a user name and password in the **User Name** and **Password** fields.



Alert: Selecting *WiFiSec* automatically enables the SonicWALL Group VPN feature and its default settings. Verify your Group VPN settings after configuring your wireless connection.

Wireless Guest Services



- The **Enable Wireless Guest Services** check box is selected by default. You can create guest wireless accounts to grant access to the WAN only.
If you enable Wireless Guest Services, type a name for the account in the **Account Name** field, and a password in the **Account Password** field.
The **Account Lifetime** is set to one hour by default, but you can configure **Minutes**, **Hours**, or **Days** to determine how long the guest account is active.
Type the value in the **Session Timeout** field. Select **Minutes**, **Hours**, or **Days**.

Wireless Configuration Summary



- Review your wireless settings for accuracy. If you want to make changes, click **Back** until the settings are displayed. Then click **Next** until you reach the **Summary** page.

Updating the Configuration



8. The security appliance is now updating the wireless configuration with your settings.

Congratulations



9. Congratulations! You have successfully completed configuration of your wireless settings. Click **Finish** to exit the Wizard.

Configuring Additional Wireless Features

The SonicWALL TZ 170 Wireless and TZ 170 SP Wireless have the following features available:

- **WiFiSec Enforcement** - an IPsec-based VPN overlay for wireless networking
- **WEP Encryption** - configure Wired Equivalent Privacy (WEP) Encryption
- **Beaconing and SSID Controls** - manage transmission of the wireless signal.
- **Wireless Client Communications** - configure wireless client settings.
- **Advanced Radio Settings** - fine-tune wireless broadcasting on the TZ 170 Wireless
- **MAC Filtering** - use MAC addresses for allowing access or blocking access to the TZ 170 Wireless.

Configuring PortShield Interfaces Using the Setup Wizard

Internet Connectivity Using the Setup Wizard

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



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

Using the PortShield Wizard

The SonicWALL PortShield Interface Wizard enables you to quickly segment and configure the integrated 25-port managed PRO 1260 switch. After you complete the configuration, the wizard creates the necessary PortShield interfaces, address objects, NAT policies, and access rules so that you can configure the switch ports within the context of these settings.

Note that the wizard configuration is essentially a starting point for PortShield interface configuration. It provides two basic tasks in PortShield interface setup:

- Partitions the ports on the device into groupings that become your PortShield interfaces.
- Automatically assigns or enables manual assignment of an IP address and a subnetwork mask to each of the partitioned port groups.

For more detailed configuration, go to the PortShield interface configuration dialog boxes in either the Interfaces or Switch Ports environments in SonicOS.

Configuring a Static IP Address with NAT Enabled

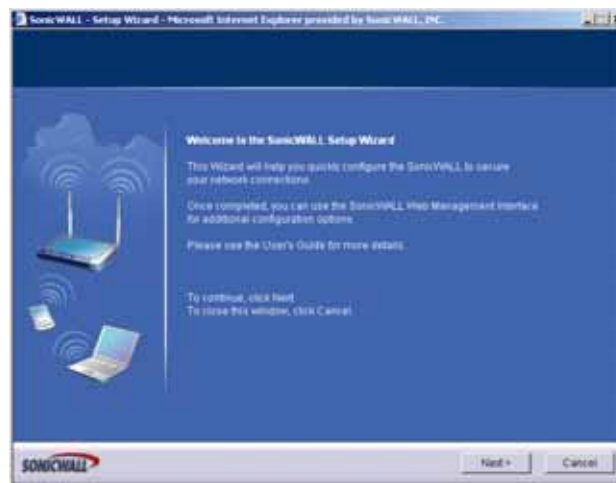
Using NAT to set up your SonicWALL eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough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

Start the 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 meet these criteria.

- 1 Log in to the device.
- 2 Click on the Network option in the left navigation bar. The management software displays the Interfaces page. If the default page is different, click on the Interfaces option in the left navigation bar.

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
LAN	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
Administration	WLAN	10.100.2.1	255.255.255.0	Static	Switch PortShield Interface		
WAN	WAN	10.0.93.35	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
OPT	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

Setup Wizard Button

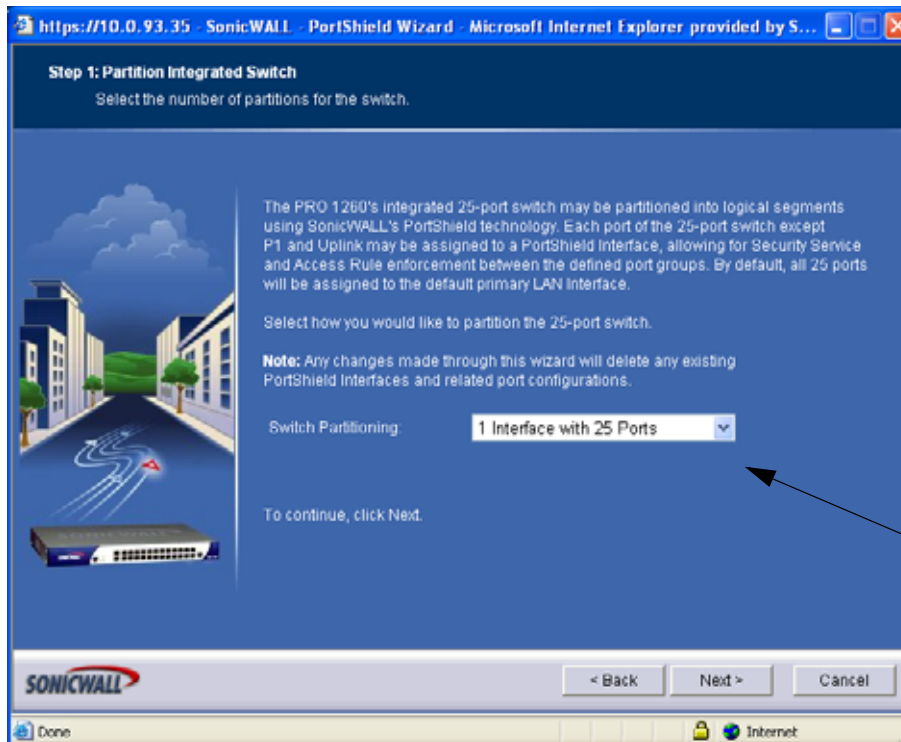
Note that you can launch the SonicWALL PRO 1260 Wizard from the following areas in SonicOS:

- ♦ the Network > Interfaces window as shown in this example.
 - ♦ the Network > Switch Ports window (button to the upper right of the device graphic of the PRO 1260)
 - ♦ the System > Status window (button in the upper right hand corner of window).
 - ♦ the Wizards window launched by clicking on the Wizards option in the navigation pane.
- 3 Click the Setup Wizard button. SonicOS displays the Partition Integrated Switch screen. This screen enables you to map a specified number of ports to an interface. It contains preset groupings of ports. SonicOS groups ports in counting order and automatically assigns them to PortShield Interfaces named by numbers also in counting order. The following table displays each grouping:

Grouping	Port Numbers
Primary LAN	1, 2, 3, 4, 5, 6
PortShield Interface 1	7, 8, 9, 10, 11, 12
PortShield Interface 2	13, 14, 15, 16, 17, 18
PortShield Interface 3	19, 20, 21, 22, 23, 24



Note: The default is 25 ports to one interface.

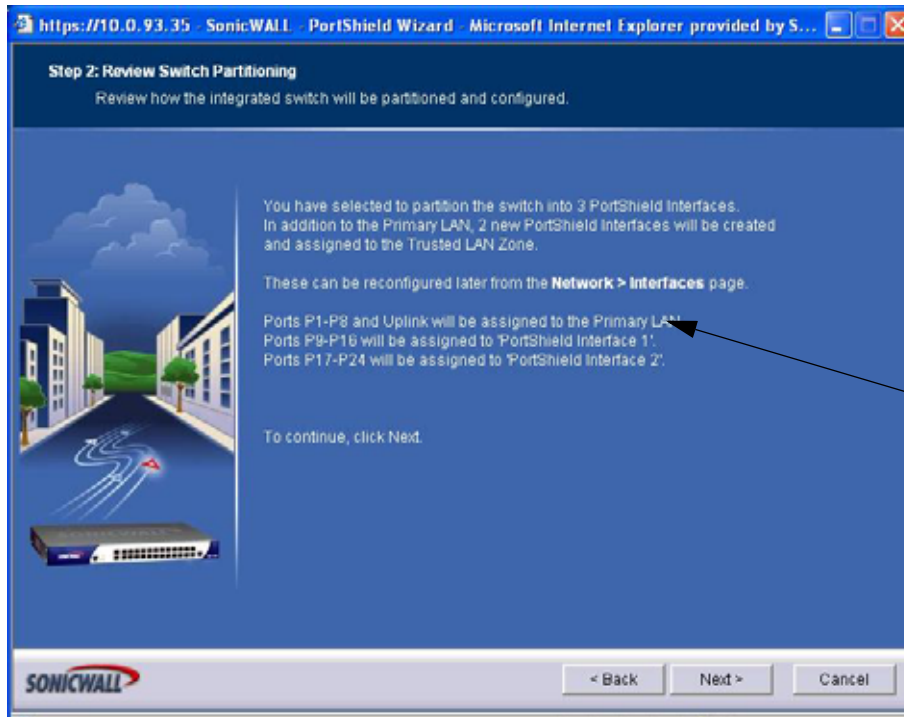


Port-Interface Mappings

- 4 Click the Switch Partitioning list box and click on switch partition option that indicates the number of ports to be mapped to a specified number of interfaces. Then click Next to continue. SonicOS displays the Review Switch Partitioning Screen that enables you to review your selections.



Note: The port breakout for each grouping will vary depending on which switch partition option you selected in the previous screen



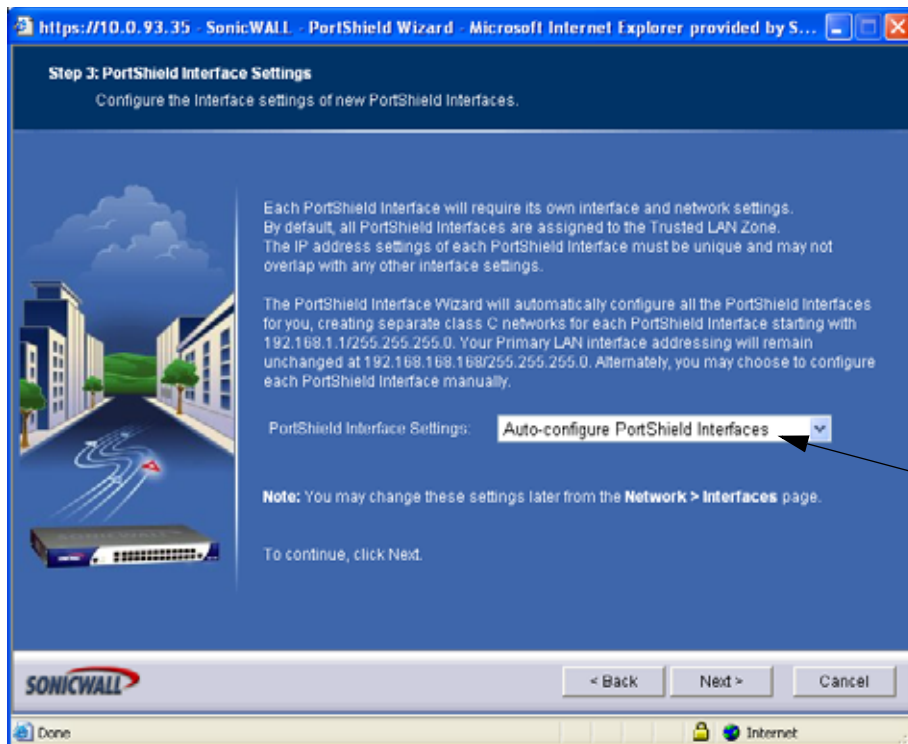
Port-Interface Review Area

5 Review the switch partitions you selected in the Partition Integrated Switch screen and make sure they are the ones you want. If you decide you would like ports grouped in a different way, you can go back to the previous screen and make another section by clicking the back button. Also, you can regroup them after you complete the wizard configuration by going to either the Interfaces or Switch Ports window.



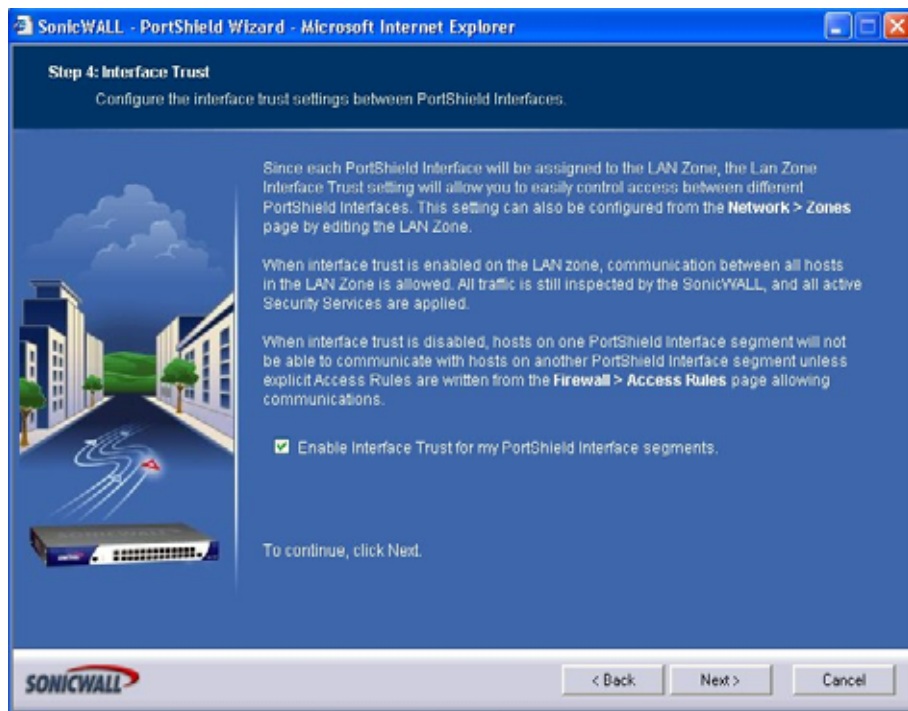
Note: Any changes you make in the wizard session for partitioning ports overwrite existing PortShield interfaces and related port configurations. Use care in assessing the switch partitions you chose before continuing.

- 6 If you are sure you want to use the switch partitions you created and to overwrite existing switch partitions, click Next. The management software displays the PortShield Interface Settings screen that enables you to select a type of configuration you want to use.

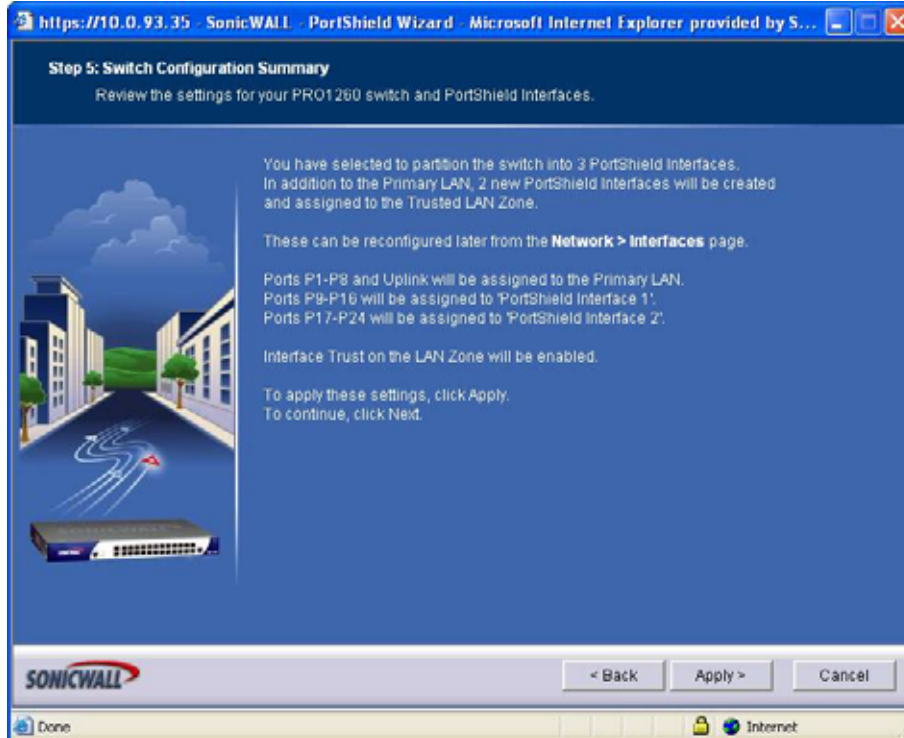


Manual-Automatic Options

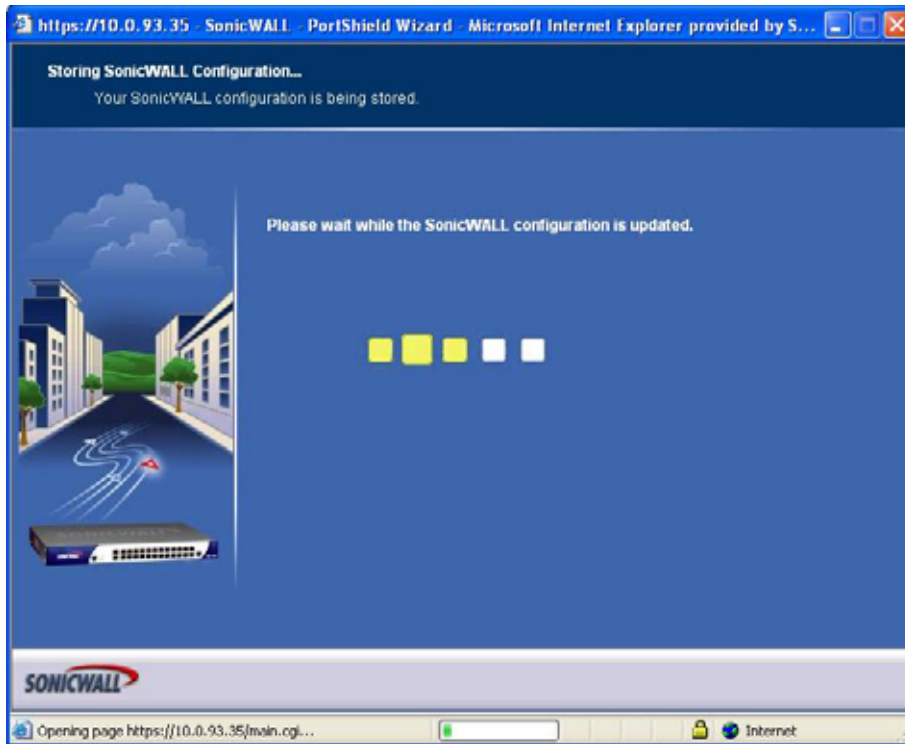
- 7 Click on the PortShield Interface Settings list box and click on a configuration type.
 - ♦ If you want the wizard to automatically configure your port-to-interface mappings, click Auto-configure PortShield Interfaces.
 - ♦ If you want to manually configure your port-to-interface mappings, click Configure PortShield Interfaces Manually.
- 8 Click Next to continue. SonicOS displays the Interface Trust dialog box that enables you to set access levels between different PortShield interfaces.



- 9 Click Next. SonicOS displays the Switch Configuration Summary screen. This screen displays the following settings you configured in the PortShield Wizard:
 - ◆ the number of PortShield interfaces you created
 - ◆ the zone type to which you mapped the PortShield interface
 - ◆ the port ranges assigned to each PortShield interface
 - ◆ the setting of the Interface Trust on the LAN zone (either enabled or disabled)



- 10 Review the settings. If you decide you want this initial PortShield configuration for your SonicWALL PRO 1260, click Apply. Wait a few moments while the SonicOS stores the configuration to flash memory on the device



- 11 If the device does not accept the configuration because of a conflict, the wizard indicates it could not create the configuration. You may want to exit and try creating another PortShield configuration with the wizard or try configuring a PortShield interface in either the Interfaces or Switch Ports window.
- 12 If the device accepts the configuration, SonicOS displays the PortShield Wizard Complete screen



- 13 To provide more settings for the PortShield interfaces you created, go to either the Interfaces or Switch Ports windows and continue your configuration there.

Index

Symbols

291, 591, 594, 595, 596, 601, 602, 603, 604, 605, 606, 609, 610, 611, 612, 613, 614, 618, 619, 620, 621, 622, 627, 631, 632, 647

Numerics

802.11a 286
802.11g 255, 286

A

acceptable use policy 464
access point status 259
access points
 SonicPoints 283
access rules
 adding 303
 advanced options 309
 bandwidth management 302
 deleting 303
 displaying traffic statistics 303
 editing 303
 enabling or disabling 303
 examples 309
 public server wizard 630
 view styles 303
 viewing 303
 zones 303
account lifetime 644
add 305
address group
 VPN policy wizard 637
address object
 VPN policy wizard 637
address objects
 about 171
 adding 133, 179
 creating groups 180
 default 173
 host 171
 MAC address 171
 network 171
 public server wizard 629
 range 171
 types 171
administration
 administrator name and password 57
 firewall name 57
 GMS management 61
 login security 58

SNMP management 59
 web management settings 58
advance access rules 311
advanced access rules
 drop source routed packets 312
 force inbound and outbound FTP data connections to use default port 20 312
 randomize IP ID 312
 RTSP transformations 312
 stealth mode 312
 support for Oracle (SQLNet) 312
 support for Windows Messenger 312
alerts 570
 redundancy filter 570
ARP 215
 ARP cache table 219
 flushing cache 220
 navigating and sorting entries 219
associated stations 259
authentication
 VPN policy wizard 633
authentication type 270
B
beaconing 273
C
certificates 65
 certificate revocation list 69
 importing 67
 signing request 69
CFS Exclusion List 503
channel 259, 262
client alerts 530
clientless notification 531
connection limiting 308
consent 505
consistent NAT 379
content filtering service 499
 activating 501
 blocked message text 503
 CFS Standard 500
custom list 503
D
deep packet inspection 519
deployment scenarios 592
 guest internet gateway 592, 648
 office gateway 592
 secure access point 592
 secure wireless bridge 593
DF bit 432
DH group 633
 VPN policy wizard 638
DHCP
 relay mode 435
 setup wizard 596
 VPN central gateway 436

- VPN remote gateway 437
- DHCP over VPN
 - leases 439
- DHCP server 221
 - current leases 227
 - dynamic ranges 223
 - static entries 225
 - VoIP settings 226
- diagnostics 83
 - active connections monitor 85
 - CPU monitor 86
 - DNS name lookup 87
 - find network path 87
 - packet trace 88
 - ping 89
 - process monitor 90
 - reverse name resolution 90
 - tech support report 84
 - trace route 91
 - web server monitor 91
- Diffie-Hellman, see DH group
- discards 260
 - bad WEP key 260
- Distributed Enforcement Architecture (DEA) 537
- DNS
 - configuring 169
 - inherit settings dynamically 170
 - specify DNS servers manually 169
 - with L2TP server 442
- DSL
 - setup wizard 601
- DTIM interval 274
- dynamic DNS 233
 - configuring 234
 - providers 234
- E**
- EAP, see extensible authentication protocol
- easy ACL 257
- Edit Zone window 544, 552
- E-mail filter 511
- encryption
 - VPN policy wizard 633, 638
- exclusion list
 - configuring 531
- extensible authentication protocol 270, 271
- F**
- failure trigger level 431
- FCS errors 260
- file transfers, restrict 529
- filter properties 503
- FIPS 81
- firmware management
 - automatic notification 78, 79
 - backup firmware image 80
 - booting firmware 79

- export settings 78
- import settings 78
- safemode 80
- updating firmware 80
- fragmentation threshold 274
- fragmented packet handling 432
- fragments 259

G

GAV

- client alerts 530
- configuring 524–533
- deep packet inspection 519
- features 514
- HTTP clientless notification 531
- HTTP file downloads 518
- inbound inspection 528
- outbound inspection 529
- overview 514–520
- protocol filtering 528
- restrict file transfers 529
- signatures 527, 532
- SMTP messages 530
- status information 527
- UUdecoding 515
- zones 526

GAV/IPS features

- application control 537, 546
- file based scanning protocol support 536, 546
- file decompression technology 536, 546
- granular management 537, 547
- inter-zone scanning 536, 546

Global Security Client

- About 557
- Activating Licenses 560
- Features 558
- How it Works 559
- Licensing 560

Global VPN Clients

- VPN policy wizard 634

groups

- adding 469
- users 467
- guest internet gateway 592, 648
- guest profiles 472
- guest services 471
 - guest profile 472
 - login status window 472
- guest status 478

H

- H.323 370
 - transforming H.323 messages 381
- hardware failover
 - before configuring 484
 - configuring 487
 - crash detection 484

- forcing transitions 488
- how it works 483
- monitoring links 489
- status 490
- synchronize settings 487
- synchronizing firmware 489
- terminology 486
- HTTP clientless notification 531
- HTTP file downloads protection 518

I

- IDS 295
 - authorizing access points 297
 - rogue access points 296
- IEEE 802.11b 255
- IEEE 802.11g 255
- IKE
 - DH group 633
 - phase 2 638
 - VPN policy wizard 638
- IKE dead peer detection 331
- inbound inspection 528
- interface
 - Ethernet settings 103
 - Internet traffic statistics 99
 - physical 96
- interfaces
 - bandwidth management 108
 - configuring LAN/DMZ/OPT interfaces 100, 101, 103
 - configuring WAN interface 106
 - settings 99
 - transparent mode 101
- internal network protection 517
- intrusion detection system, see IDS
- intrusion prevention service
 - architecture 538
 - deep packet inspection 537
 - features 514
 - terminology 538
- IP Helper 231
 - add policy 232
- ISP
 - setup wizard 601

L

- L2TP 441
 - configuring 442
- L2TP-over-IPSec 441
- LAN
 - setup wizard 597
- Layer 2 Tunneling Protocol, see L2TP
- local groups
 - adding 469
- local users 465
 - adding 466
 - editing 467

- log
 - automation 577, 579
 - e-mail alert addresses 578
 - e-mailing logs 567
 - event message priority levels 568
 - exporting 567
 - generating reports 581
 - legacy attacks 570
 - log categories 573
 - mail server settings 578
 - redundancy filter 570
 - view table 566
 - viewing events 565
- login status window 472
- logs
 - priority, configuring 569
- loopback policy 630

M

- MAC address 259
- MAC filter list 257, 275
- MAC filtering 645
- manage security services online 53
- management interface 37
 - applying changes 38
 - common icons 39
 - getting help 39
 - logging out 40
 - navigating 37
 - navigating tables 39
 - status bar 37
 - submenus 37
- mandatory filtered IP addresses 506
- MCUs 371
- modem
 - WAN failover 155
- multicast 331
 - create a new multicast object 332
 - IGMP state table 333
 - multicast state table entry timeout 332
 - reception of all multicast addresses 332
 - require IGMP membership reports for multicast data forwarding 332
 - snooping 332
- multicast frames 259
- multiple retry frames 260
- mySonicWALL.com
 - creating account 521

N

- NAT policies 201
 - comment field 204
 - creating 206
 - creating a many-to-many NAT policy 207
 - creating a many-to-one NAT policy 206
 - creating a one-to-one NAT policy for inbound traffic 208

- creating a one-to-one NAT policy for outbound traffic 207
- enable 204
- inbound interface 204
- inbound port address translation via one-to-one NAT policy 210
- inbound port address translation via WAN (X1) IP address 211
- navigating and sorting 202
- original destination 204
- original service 204
- original source 204
- settings 203
- translated destination 204
- translated service 204
- translated source 204
- NAT policy
 - loopback policy 630
 - outbound interface 204
 - public server wizard 630
 - reflective policy 204
- NAT traversal 432
- network anti-virus 507
 - activating 508
- network settings
 - setup wizard 594
- O**
- objects
 - service group 630
- office gateway 592
- open system 270
- outbound SMTP inspection 529
- P**
- phase 2
 - VPN policy wizard 638
- PPPoE
 - setup wizard 596
- PPTP
 - setup wizard 596
- preamble length 274
- pre-shared key 270
- preshared key
 - VPN policy wizard 636
- protocol filtering 528
- PSK, see pre-shared key
- public server wizard 629
 - access rules 630
 - NAT policies 630
 - server address objects 629
 - server name 628
 - server private IP address 628
 - server type 628
 - service group object 630
 - starting 627

- R**
- RADIUS
 - configuring user authentication 449
 - with L2TP server 442
 - registering SonicWALL security appliance 522
 - remote site protection 517
 - restart SonicWALL security appliance 92
 - restore default settings 274
 - restrict web features 502
 - retry limit exceeded 260
 - rogue access points 296
 - route policies 185
 - routing 183
 - metric values 185
 - policy based routing 185
 - route advertisement 184
 - route advertisement configuration 184
 - route policies table 186
 - route policy example 187
 - static routes 183
 - RTS threshold 274
- S**
- SDP 289, 380
- secure access point 592
- secure wireless bridge 593
- security services
 - licenses 52
 - managing online 495
 - manual upgrade 54
 - manual upgrade for closed environments 54
 - manually update 497
 - summary 493
- server protection 518
- service group
 - public server wizard 630
- services 325
 - adding custom services 327
 - adding custom services group 329
 - default services 326
 - supported protocols 327
- session timeout 644
- settings
 - users 448
 - VPN 395
- setup wizard
 - change password 594, 602, 610, 618
 - change time zone 595, 603, 611, 619
 - configuration summary 600, 608, 616, 624
 - DHCP mode 601
 - DHCP server 614, 622
 - DHCP settings 606
 - LAN DHCP settings
 - 598
 - LAN settings 597, 598, 605, 606, 613, 614, 621, 622

- NAT with DHCP client 605
- NAT with PPPoE 609
- NAT with PPPoE client 613
- NAT with PPTP 617
- NAT with PPTP client 621
- static IP address with NAT enabled 593, 648
- WAN Network mode 620
- WAN network mode 596, 604, 612
- shared key 270
- signal retry frames 260
- signatures 527
 - manually update 497
- signatures table 532
- SIP 371
 - media 380
 - signaling 380
 - transforming SIP messages 380
 - UDP port 381
- site-to-site VPN
 - policy name 636
 - VPN policy wizard 635
- SMTP messages, suppressing 530
- SonicPoint
 - provisioning profiles 284
 - station status 291
- SonicPoints 283
 - IDS 295
 - managing 283
- SonicWALL discovery protocol, see SDP
- SonicWALL simple provisioning protocol, see SSPP
- SonicWALL technical support xxiii
- SonicWALL ViewPoint 585
 - activating 585
 - enabling 587
- SSID 259
- SSID controls 273
- SSPP 290
- static IP
 - setup wizard 596
- status
 - security services 45
 - users 447
 - wireless 258
- syslog
 - adding server 576
 - event redundancy rate 576
 - server settings 576
- syslog server 575
- system
 - alerts 45
 - information 44
 - network interfaces 48
 - status 43

T

- This 301
- time
 - NTP settings 72
 - setting 72
- transmit power 274
- trusted domains 502

U

- unicast frame 259
- unified threat management 513
- user authentication
 - VPN policy wizard 633
- users
 - acceptable use policy 464
 - active sessions 447
 - adding 466
 - adding local groups 469
 - authentication methods 448
 - configuring RADIUS authentication 449
 - creating local groups 468
 - editing 467
 - global settings 462
 - groups 467
 - guest accounts 474
 - guest profile 472
 - guest services 471
 - guest status 478
 - local users 465
 - login status window 472
 - settings 448
 - SonicWALL authentication 466
 - status 447

- UUdecoding 515

V

- virtual IP adapter
 - VPN policy wizard 634
- VPN 395, 431
 - active L2TP sessions 443
 - active tunnels 407
 - advanced settings 431
 - DF bit 432
 - DHCP leases 439
 - DHCP over VPN 435
 - central gateway 436
 - remote gateway 437
 - DHCP relay mode 435
 - export client policy 415
 - global security client 399
 - global VPN client 399
 - GroupVPN 408
 - L2TP Server 441
 - L2TP-over-IPSec 441
 - NAT traversal 432
 - planning sheet 400
 - settings 395

- site-to-site 416
 - VPN policy window 417
 - VPN policy wizard 631
- VPN policy wizard
 - authentication 633, 638
 - configuration summary 638
 - connecting Global VPN Clients 634
 - destination networks 637
 - DH group 633, 638
 - encryption 633, 638
 - IKE phase 1 key method 632
 - IKE security settings 633, 638
 - life time 638
 - local networks 636
 - peer IP address 636
 - policy name 636
 - preshared key 636
 - site-to-site VPN 635
 - user authentication 633
 - virtual IP adapter 634
 - VPN policy type 632

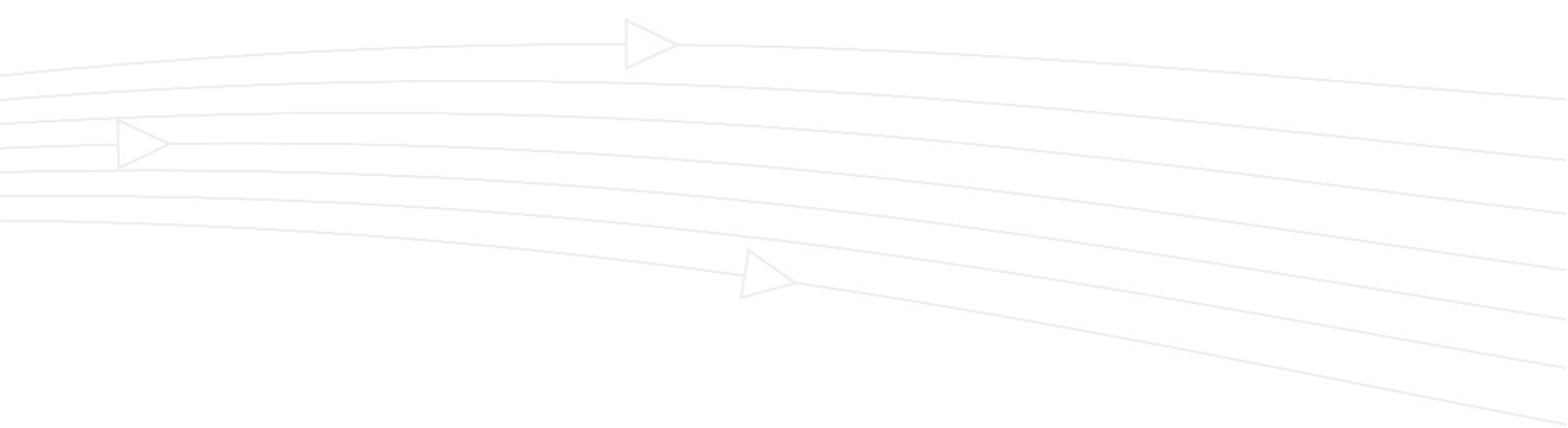
W

- WAN
 - GroupVPN 632
- WAN failover 151
 - caveats 151
 - modem 155
 - outbound load balancing methods 153
 - probe monitoring 155
 - setting up 152
 - statistics 157
- web proxy 229
 - bypass proxy servers 230
 - configuring 230
- WEP 286
- WEP encryption 645
- WEP key
 - alphanumeric 270
 - hexadecimal. 270
- WEP key mode 270
- WiFiSec 255, 259
- WiFiSec enforcement 257
- WiFiSec Protected Access 270
 - EAP 271
 - PSK 271

- wireless
 - guest internet gateway 592, 648
 - IDS 295
 - office gateway 592
 - secure access point 592
 - secure wireless bridge 593
 - SonicPoints 283
 - WPA 270
- wireless client communications 645
- wireless encryption protocol, see WEP
- wireless firmware 259
- wireless guest services 259
 - account lifetime 644
 - wizard 644
- wireless node count 257
- wireless status 258
- wireless wizard 641
- wireless zones 283
- wizard
 - setup wizard 647
- wizards
 - setup wizards 591
 - wireless wizard 641
- WLAN 259
 - IP address 259
 - settings 258
 - statistics 259
 - subnet mask 259
- WPA encryption 270
- WPA, see WiFiSec Protected Access

Z

- zone
 - SonicPoints 283
 - wireless 283
- zones 159
 - adding 164
 - allow interface trust 162, 165
 - enabling security services 162
 - GAV 526
 - how zones work 160
 - inter-zone protection 514
 - predefined 161
 - security types 162
 - zone settings table 163



SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale, CA 94089-1306

T: 408.745.9600
F: 408.745.9300

www.sonicwall.com

© 2006 SonicWALL, Inc. SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change with out notice.

P/N 232-000987-00
Rev A 03/06

