Configuring the SonicWALL TZ215 Router for NAT Traversal

Release 4.0

June 2013

© 2013 by Vertical Communications, Inc. All rights reserved.

Vertical Communications and the Vertical Communications logo and combinations thereof and Vertical ViewPoint and Wave Contact Center are trademarks of Vertical Communications, Inc. All other brand and product names are used for identification only and are the property of their respective holders.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY

Vertical Communications, Inc. makes no representation or warranties with respect to the accuracy or completeness of the content of this publication and specifically disclaims any implied warranty of merchantability or fitness for any particular purpose, and shall not be liable for any loss of profit or any other commercial damage, including but not limited to, special, incidental, or consequential.

COPYRIGHT STATEMENT

This publication contains proprietary and confidential information of Vertical Communications, Inc. The contents of this document may not be disclosed, copied or translated by third parties, in any form, or by any means known, or not now known or conceived, without prior explicit written permission from Vertical Communications, Inc.

Vertical Communications, Inc. reserves the right to revise this publication and to make changes in content without notice.

What’s new in this version

This is the initial version of *Configuring the SonicWALL TZ215 Router fro NAT Traversal*, introduced in Wave 4.0.

For details on everything that’s new in Wave 4.0, see the *Wave 4.0 Release Notes*.

Contents

Chapter 1

About Using NAT Traversal with Wave

Chapter Contents

Overview

NAT traversal is one method to enhance Wave remote phone integration.

NAT traversal establishes and maintains IP connections that traverse network address translation (NAT) gateways. NAT provides automated translation of IP addresses between different networks. For example, a company might use private IP addresses on a LAN that are represented by a single IP address on the WAN side of your router.

In order to use NAT traversal with Wave, you need to perform the following tasks:

- Enable and configure NAT traversal on your Wave Server. See Chapter 2.
- Configure your router. See Chapter 3.

Important: This guide describes how to configure the Dell™ SonicWALL™ TZ215 Network Security Appliance. While these configuration steps and settings should apply to other SonicWALL routers, testing was only performed on this specific model.

Chapter 2

Configuring NAT Traversal on the Wave Server

CHAPTER CONTENTS

This chapter describes the steps to configure NAT traversal on the Wave Server.

For complete details on how to configure Wave's IP telephony features, see Chapter 6 in the *Wave Global Administrator Guide*.

Enabling NAT traversal and specifying STUN servers

Session Traversal Utilities for NAT (STUN) is a public service that is used to aid a phone or phone system in properly routing signaling so a call is successful and audio is present. A STUN server allows NAT clients (for example computers behind a firewall) to set up phone calls to a VoIP provider hosted outside of the local Wave network.

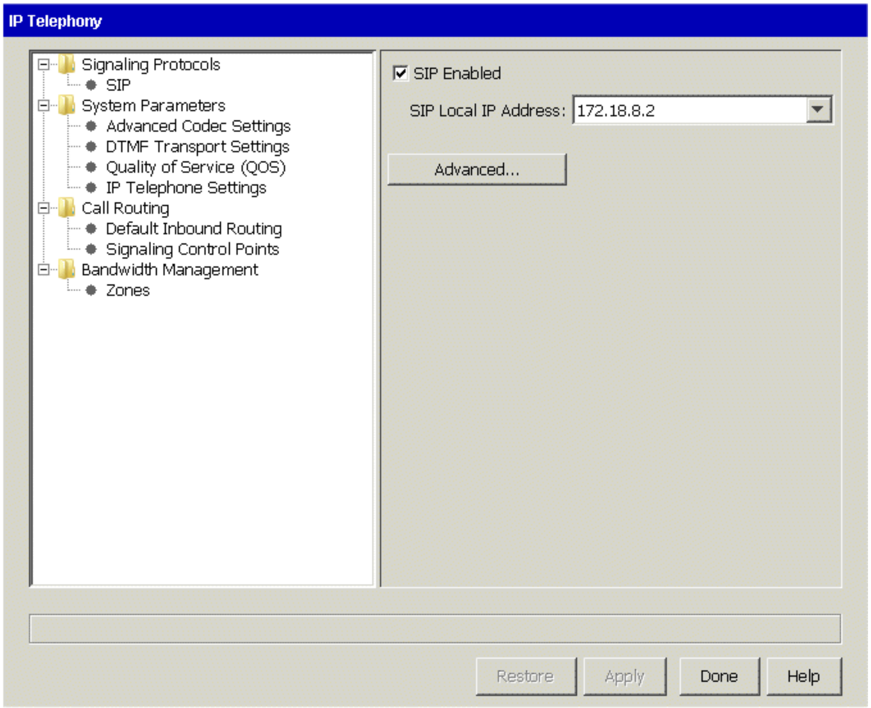
When you deploy NAT traversal, best practice is to specify more than one STUN server.

- At least one STUN server must be specified for auto discovery to work.
- Typically a minimum of two STUN servers are specified to provide some level of fault tolerance.
- You can specify up to 3 STUN Servers.

To enable NAT traversal and specify STUN servers

1. In the Global Administrator Management Console, click **IP Telephony**, located in the PBX Administration section.

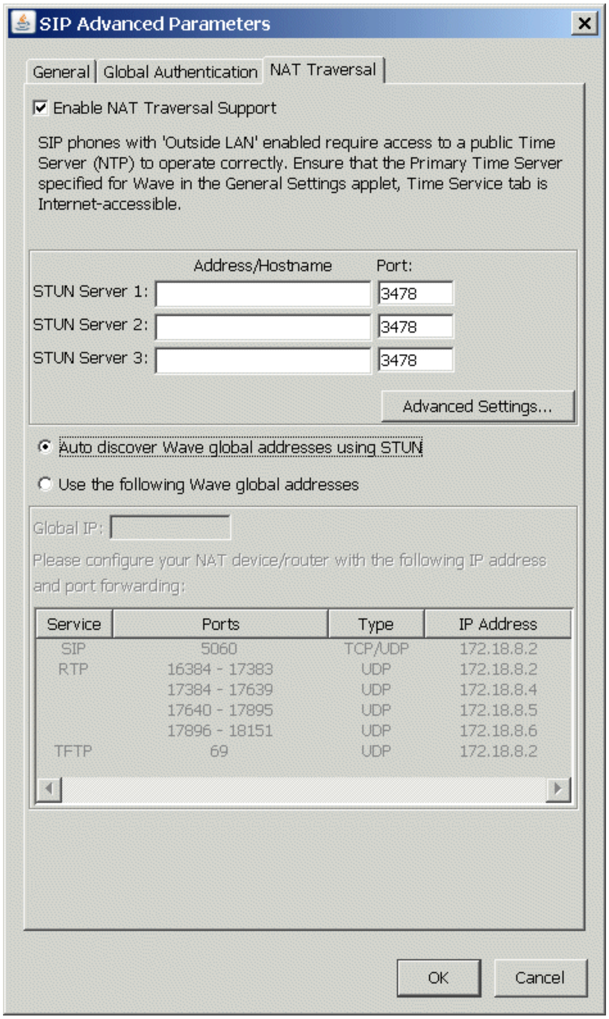
2. Click **Advanced**.



☑ SIP Enabled

SIP Local IP Address: 172.18.8.2

3. On the NAT Traversal tab, select the following options:
    - **Enable NAT Traversal Support**
    - **Auto discover Wave global addresses using STUN.**



SIP Advanced Parameters

☑ Enable NAT Traversal Support

SIP phones with 'Outside LAN' enabled require access to a public Time Server (NTP) to operate correctly. Ensure that the Primary Time Server specified for Wave in the General Settings applet, Time Service tab is Internet-accessible.

	Address/Hostname	Port:
STUN Server 1:		3478
STUN Server 2:		3478
STUN Server 3:		3478

● Auto discover Wave global addresses using STUN

○ Use the following Wave global addresses

Global IP:

Please configure your NAT device/router with the following IP address and port forwarding:

Service	Ports	Type	IP Address
SIP	5060	TCP/UDP	172.18.8.2
RTP	16384 - 17383	UDP	172.18.8.2
	17384 - 17639	UDP	172.18.8.4
	17640 - 17895	UDP	172.18.8.5
	17896 - 18151	UDP	172.18.8.6
TFTP	69	UDP	172.18.8.2

You typically do not need to change the default STUN advanced settings.

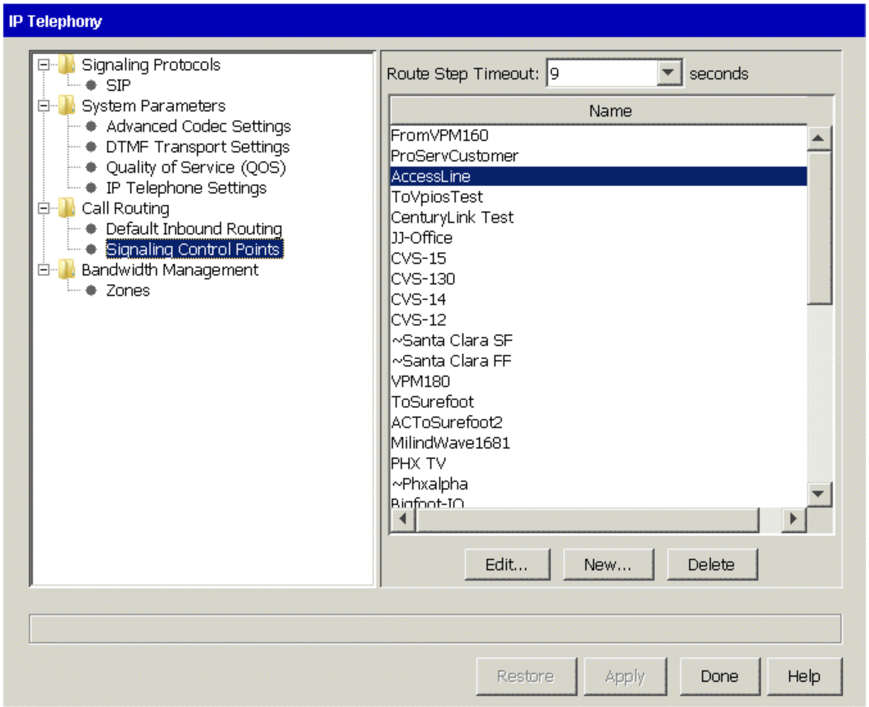
4. For **STUN Server 1**, **STUN Server 2**, and **STUN Server 3**, enter the IP address or hostname of each STUN Server you are using.

   Important: Note the table at the bottom of the SIP Advanced Parameters dialog on the previous page that lists the RTP port ranges and IP addresses used by each of the SIP endpoints on the Wave Server—the VAM and three MRM DSPs. You will use the IP address and port range information listed here when you configure your router for NAT traversal, as described in Chapter 3. In this example, the four RTP services listed are for (in top-down order) the VAM, MRMA, MRMB, and MRMC.

5. Click **OK**.

To configure the SCP

6. Expand **Call Routing** in the left pane, and then click **Signaling Control Points**.

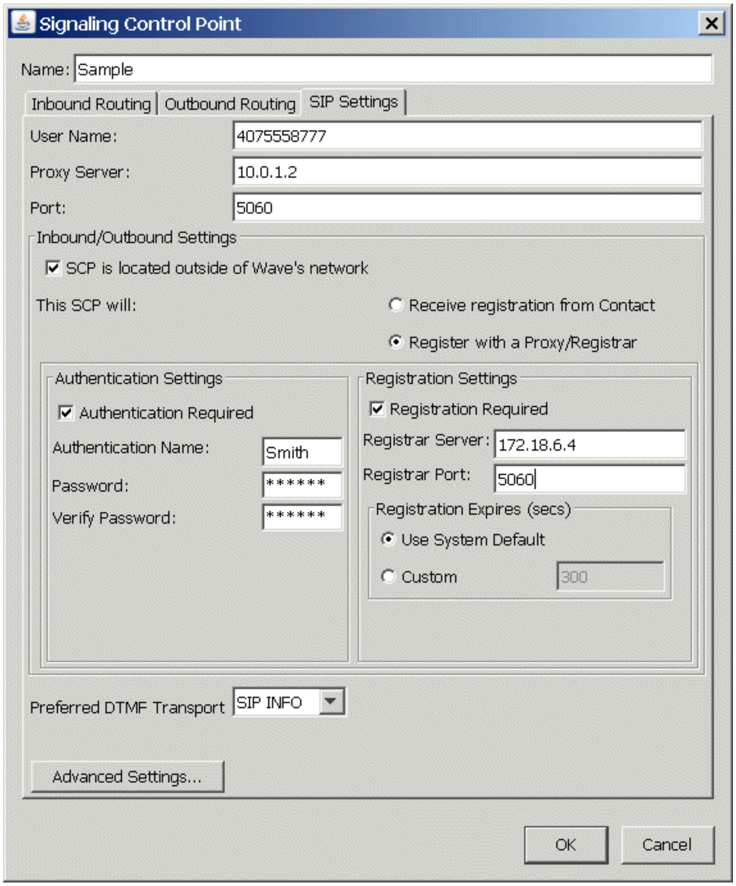


Route Step Timeout: 9 seconds

FromVPM160
ProServCustomer
AccessLine
ToVpiosTest
CenturyLink Test
JJ-Office
CVS-15
CVS-130
CVS-14
CVS-12
~Santa Clara SF
~Santa Clara FF
VPM180
ToSurefoot
ACToSurefoot2
MilindWave1681
PHX TV
~Phxalpha
Bigfoot-IO

7. Select your ITSP’s SCP and then click **Edit.**

8. Click the SIP Settings tab. In the Inbound/Outbound Settings section, select the **SCP is located outside of Wave’s network** checkbox.



Name: Sample

User Name: 4075558777

Proxy Server: 10.0.1.2

Port: 5060

Inbound/Outbound Settings

☑ SCP is located outside of Wave's network

This SCP will: ○ Receive registration from Contact ● Register with a Proxy/Registrar

Authentication Settings

☑ Authentication Required

Authentication Name: Smith

Password: ******

Verify Password: ******

Registration Settings

☑ Registration Required

Registrar Server: 172.18.6.4

Registrar Port: 5060

Registration Expires (secs)

● Use System Default

○ Custom 300

Preferred DTMF Transport SIP INFO

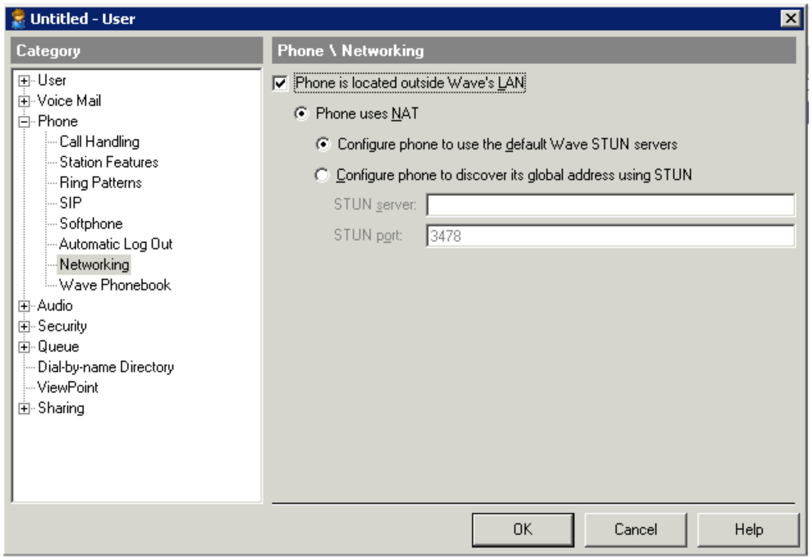
9. Click **OK**, and then exit IP Telephony.

Configuring remote users for NAT traversal

Perform the following step for each Wave user with a remote SIP phone (a SIP phone that is outside your Wave network).

1. In the Global Administrator Management Console, click **User/Group Management**, located in the PBX Administration section.

2. Edit the user, and select **Phone > Networking** in the left pane.



Untitled - User

Category

- User
- Voice Mail
- Phone
  - Call Handling
  - Station Features
  - Ring Patterns
  - SIP
  - Softphone
  - Automatic Log Out
  - Networking
  - Wave Phonebook
- Audio
- Security
- Queue
- Dial-by-name Directory
- ViewPoint
- Sharing

Phone \ Networking

☑ Phone is located outside Wave's LAN

● Phone uses NAT

● Configure phone to use the default Wave STUN servers

○ Configure phone to discover its global address using STUN

STUN server:

STUN port: 3478

3. Select the following options:
   - **Phone is located outside Wave's LAN**
   - **Phone uses NAT**

4. Select one of the following:
   - **Configure phone to use the default Wave STUN servers**. Select this option if you want this user to use the STUN servers that you specified via IP Telephony. In most cases, you should select this option.
   - **Configure phone to discover its global address using STUN**. Select this option if you want this user to use a different STUN server, then specify the STUN server's IP address or hostname.

5. Click **OK** to save the user.

Chapter 3

Configuring the SonicWALL Router for NAT Traversal

Chapter Contents

The steps described in this chapter assume that you have a generic public-WAN-to-private-LAN network configuration. If you have a special-case or more customized or complex network—for example with multiple addresses or multiple zones—you will need to resolve any configuration issues using your router's documentation or your router vendor.

This chapter does not cover every step of configuring the SonicWALL router for your environment—only the steps required to configure the router to support NAT traversal with Wave.

Perform the steps in this chapter in the order indicated.

Configuration overview

Configuring your SonicWALL router for NAT traversal with Wave consists of the following tasks. The specific components that you need to create are described in the next section.

- **Configuring VoIP settings**.
- **Creating address objects**. An address object specifies the IP address of a specific network-addressable hardware component on the Wave Server.
- **Creating service objects**. A service object defines the IP protocol and the port range used for each type of service.
- **Creating service groups**. A service group defines a group of service objects, and is used when creating access rules and NAT policies.
- **Creating an access rule**. An access rule gives permission for traffic to pass through the firewall and how.
- **Creating NAT policies**. NAT policies describe the route traffic takes—identifying how traffic from a specific port range is routed to a particular IP address on the Wave Server.

Configuration requirements

This section describes the specific components that you need to configure on your SonicWALL router to support NAT traversal with Wave.

Address object requirements

The address objects that you need to create depend on your Wave Server's hardware configuration:

- **Wave Address Object**. This address object identifies the IP address of the Wave Server.
- **MRM Address Objects**. You create an address object for each IP address on a media resource module (MRM), if one is installed. An MRM has 1-3 IP addresses, depending on the model installed:
  - An MRMA has one IP address and requires *one* address object, **MRMA**.
  - An MRMB has two IP addresses and requires *two* address objects, **MRMA** and **MRMB**.

  - An MRMC has three IP addresses and requires *three* address objects, **MRMA**, **MRMB**, and **MRMC**.

Service object requirements

The service objects that you need to create depend on your Wave Server's hardware configuration:

- **Wave Service Object**.
- **MRM Service Objects**. You create a service object for each IP address on a media resource module (MRM), if one is installed.
  - An MRMA requires *one* service object, **MRMA**.
  - An MRMB requires *two* service objects, **MRMA** and **MRMB**.
  - An MRMC requires *three* service objects, **MRMA**, **MRMB**, and **MRMC**.

Service group requirements

You need to create two service groups:

- **Wave Services Group**. This group contains the Wave Service Object that you created, as well as the default SonicWALL service objects SIP and TFTP. The Wave Service Group will be used when creating NAT policies.
- **All Wave Services Group**. This group include all of the service objects included in the Wave Service Group, as well as each MRM Service Object that you created previously. The All Wave Service Group will be used when creating access rules.

Access rule requirements

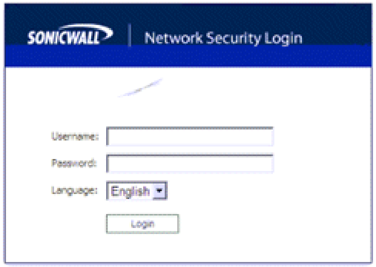
You need to create an access rule that allows *all* Wave traffic to pass through the firewall at *all* times.

NAT policy requirements

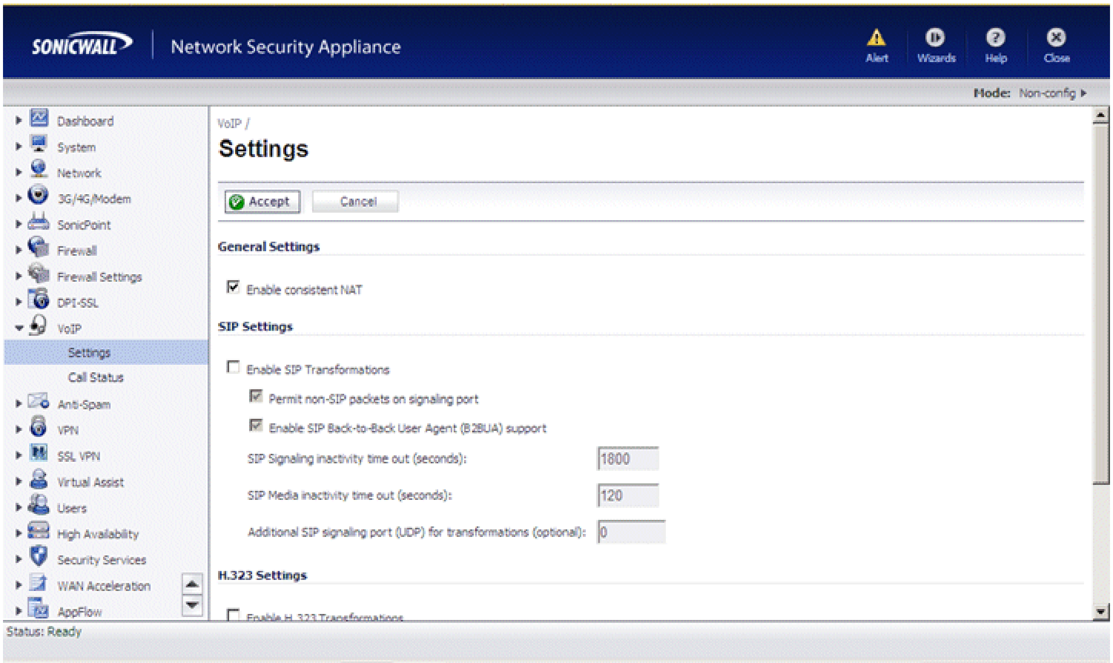
You need to create a NAT policy for the Wave Address Object and each MRM Address Object that you created previously.

Configuring VoIP settings

1 Login in to your SonicWALL router:



2 Choose **VoIP > Settings** in the navigation pane:



General Settings

☑ Enable consistent NAT

SIP Settings

☐ Enable SIP Transformations

☑ Permit non-SIP packets on signaling port

☑ Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 120

Additional SIP signaling port (UDP) for transformations (optional): 0

H.323 Settings

☐ Enable H.323 Transformations

3 Make the following changes:

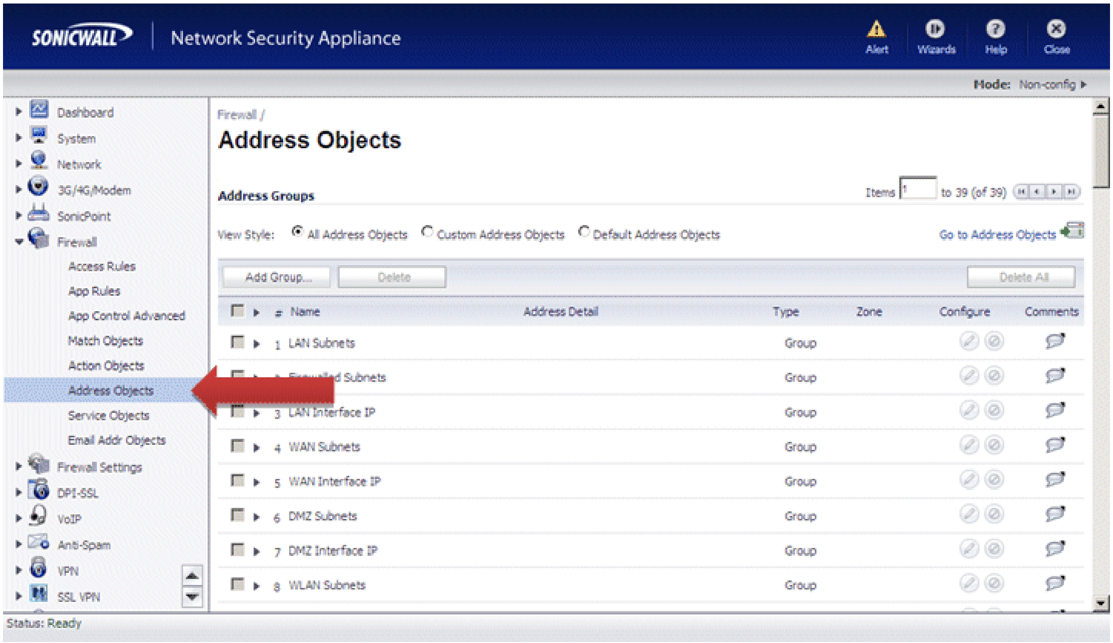
- Select the **Enable Consistent NAT** checkbox. Consistent NAT ensures that the same ports are used on each request. This is required to allow VoIP audio to pass reliably.
- Deselect the **Enable SIP Transformations** checkbox. This is Sonicwall's attempted NAT traversal setting and enabling it will compete with Wave's NAT traversal efforts.
- Deselect the **Enable H.323 Transformations** checkbox. Wave does not use H.323.

4 Click **Accept** to apply your changes.

Creating address objects

See “Configuration overview” on page 3-2 for details on the specific address objects you need to create.

1 Choose **Firewall > Address Objects** in the navigation pane:



Address Objects

Address Groups

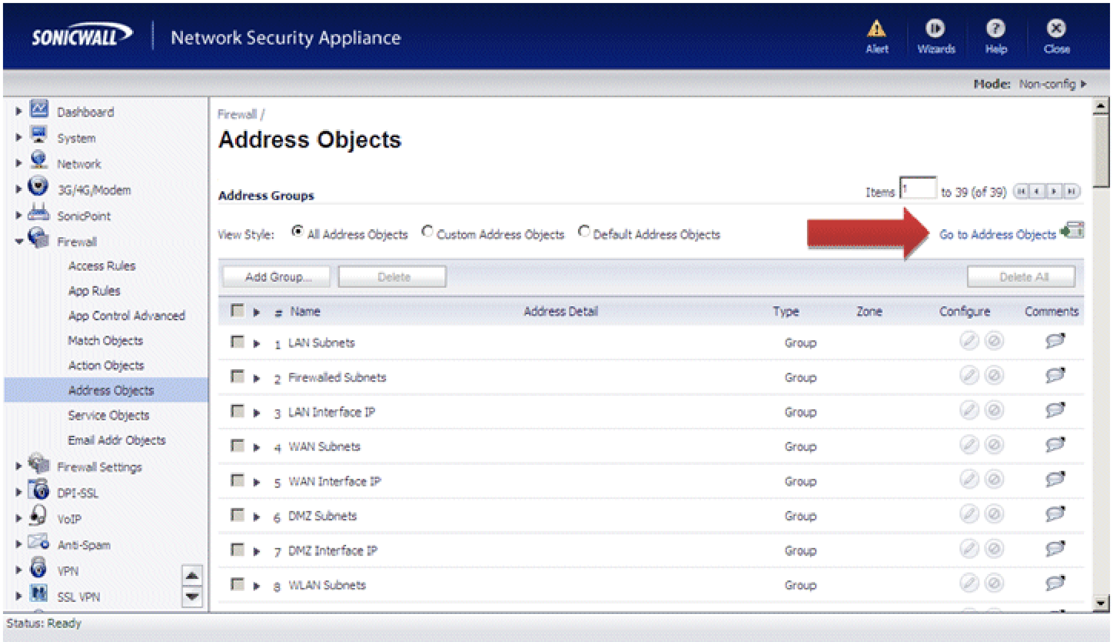
Items 1 to 39 (of 39)

View Style: ● All Address Objects ○ Custom Address Objects ○ Default Address Objects

#	Name	Address Detail	Type	Zone	Configure	Comments
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			

The screen that opens shows address groups, which are *collections* of address objects.

2 To create a new address object, click **Go to Address Objects**.



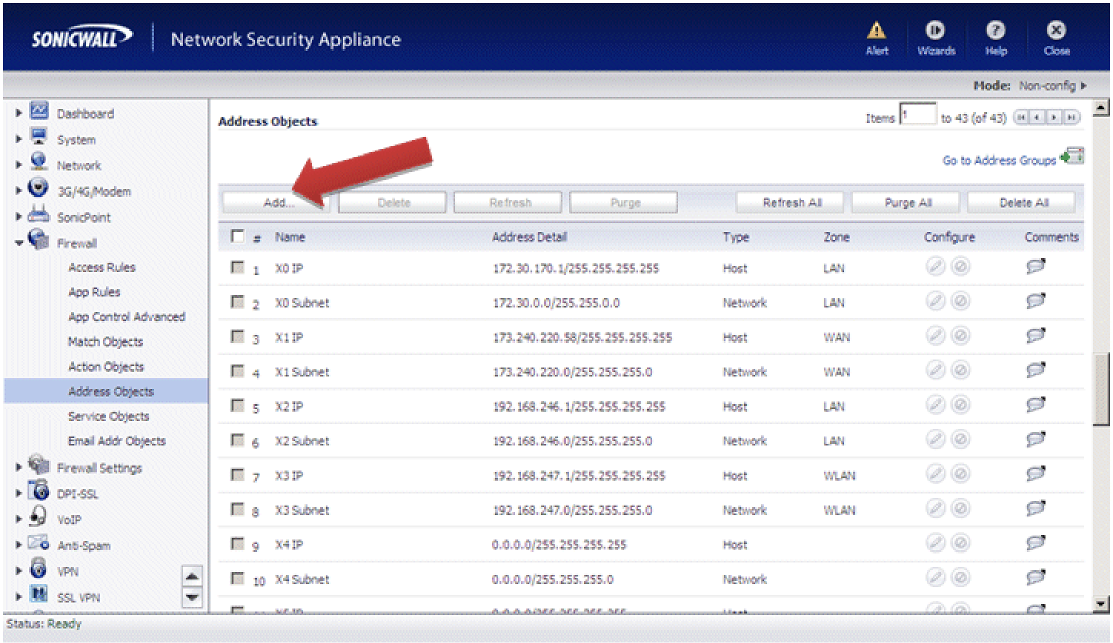
Address Objects

Address Groups

View Style: ● All Address Objects ○ Custom Address Objects ○ Default Address Objects

#	Name	Address Detail	Type	Zone	Configure	Comments
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			

3 Click **Add**:

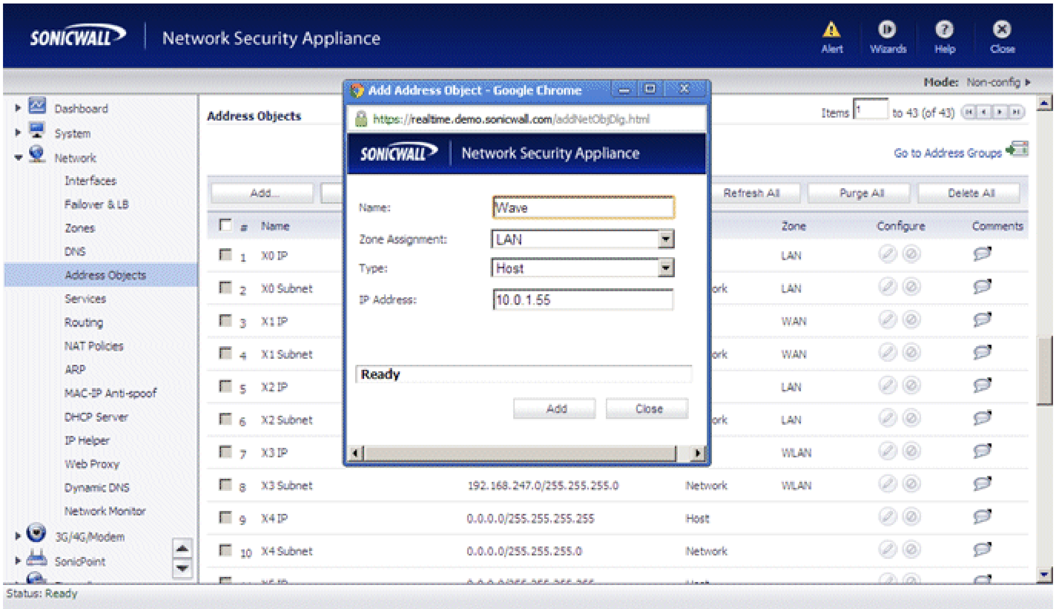


Address Objects

Items 1 to 43 (of 43)

#	Name	Address Detail	Type	Zone
1	X0 IP	172.30.170.1/255.255.255.255	Host	LAN
2	X0 Subnet	172.30.0.0/255.255.0.0	Network	LAN
3	X1 IP	173.240.220.58/255.255.255.255	Host	WAN
4	X1 Subnet	173.240.220.0/255.255.255.0	Network	WAN
5	X2 IP	192.168.246.1/255.255.255.255	Host	LAN
6	X2 Subnet	192.168.246.0/255.255.255.0	Network	LAN
7	X3 IP	192.168.247.1/255.255.255.255	Host	WLAN
8	X3 Subnet	192.168.247.0/255.255.255.0	Network	WLAN
9	X4 IP	0.0.0.0/255.255.255.255	Host	
10	X4 Subnet	0.0.0.0/255.255.255.0	Network	

4 For each new address object, enter the following information:



Name: Wave

Zone Assignment: LAN

Type: Host

IP Address: 10.0.1.55

Ready

- **Name**. Enter a meaningful name, for example “Wave”, “MRMA”, “MRMB”, or “MRMC”.
- **Zone Assignments**. Leave the default, “LAN”.
- **Type**. Leave the default, “Host”.
- **IP Address**. Enter the IP Address of the hardware component for which you are adding an address object.

  You can view the assigned IP addresses via IP Telephony in the Wave Global Administrator Management Console, as described in the Important note on page 2-4.

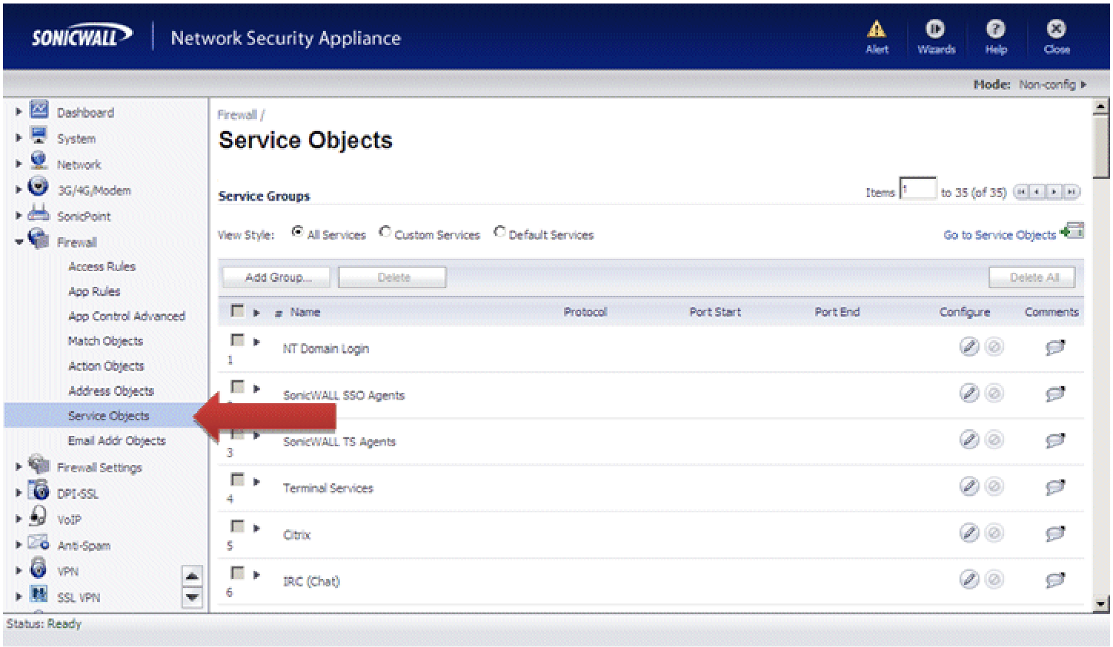
5 Click **Add** to create the new address object.

6 Repeat steps 3-6 to create the rest of the required address objects. Change the name, but keep all of the other settings the same for each address object.

Creating service objects

See “Configuration overview” on page 3-2 for details on the specific service groups you need to create.

1 Choose **Firewall > Service Objects** in the navigation pane:



Service Objects

Service Groups

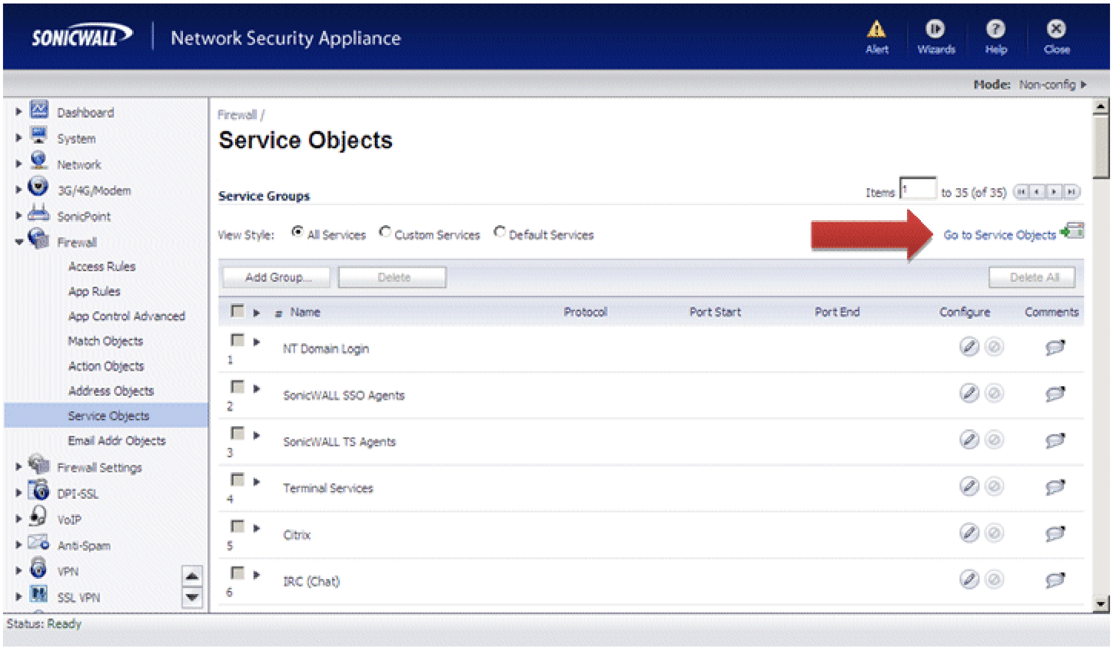
Items 1 to 35 (of 35)

View Style: ● All Services ○ Custom Services ○ Default Services

#	Name	Protocol	Port Start	Port End	Configure	Comments
1	NT Domain Login					
	SonicWALL SSO Agents					
3	SonicWALL TS Agents					
4	Terminal Services					
5	Citrix					
6	IRC (Chat)					

The screen that opens shows service groups, which are *collections* of service objects.

2 To create a new service object, click **Go to Service Objects**.



Service Objects

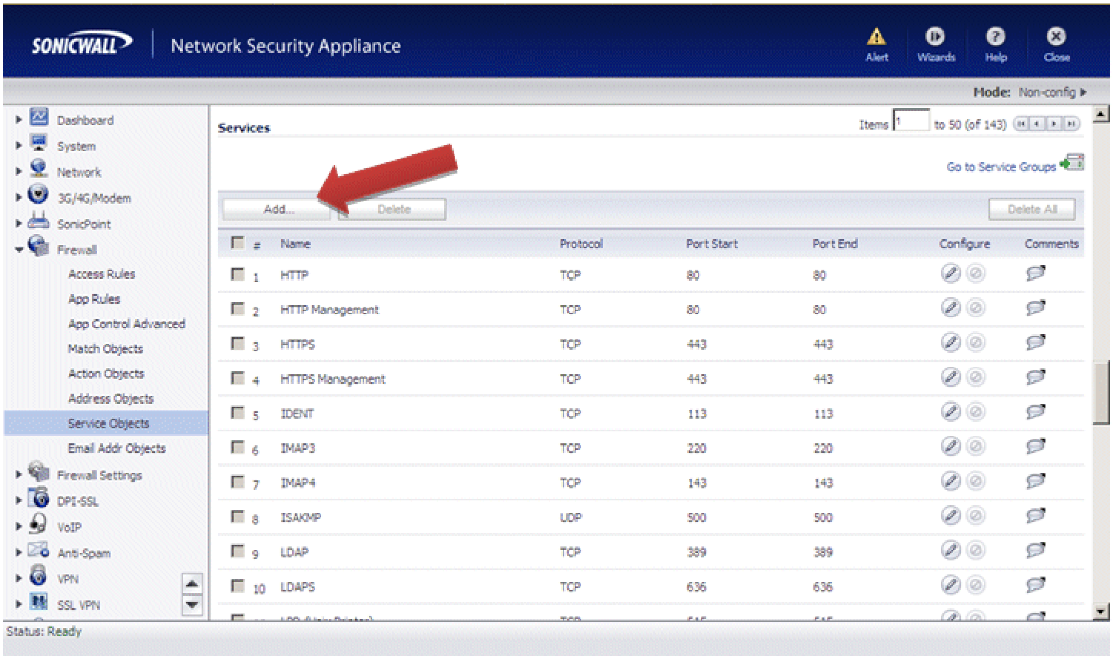
Service Groups

Items 1 to 35 (of 35)

View Style: ● All Services ○ Custom Services ○ Default Services

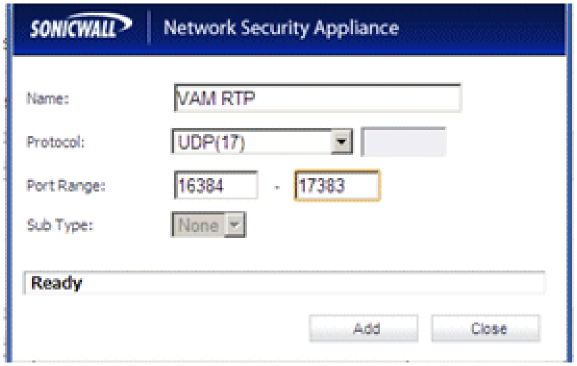
□	#	Name	Protocol	Port Start	Port End	Configure	Comments
□	1	NT Domain Login					
□	2	SonicWALL SSO Agents					
□	3	SonicWALL TS Agents					
□	4	Terminal Services					
□	5	Citrix					
□	6	IRC (Chat)					

3 Click **Add**:



□	#	Name	Protocol	Port Start	Port End	Configure	Comments
□	1	HTTP	TCP	80	80		
□	2	HTTP Management	TCP	80	80		
□	3	HTTPS	TCP	443	443		
□	4	HTTPS Management	TCP	443	443		
□	5	IDENT	TCP	113	113		
□	6	IMAP3	TCP	220	220		
□	7	IMAP4	TCP	143	143		
□	8	ISAKMP	UDP	500	500		
□	9	LDAP	TCP	389	389		
□	10	LDAPS	TCP	636	636		

4 For each new service object, enter the following information:



Name: VAM RTP

Protocol: UDP(17)

Port Range: 16384 - 17383

Sub Type: None

Ready

- **Name**. Enter a meaningful name, for example “VAM RTP”, “MRMA”, “MRMB”, or “MRMC”.
- **Protocol**. Select UDP(17).
- **Port Range**. Enter the port range to use for this service object.

  You can view the assigned port ranges via IP Telephony in the Wave Global Administrator Management Console, as described in the Important note on page 2-4.
- **Sub Type**. Not used.

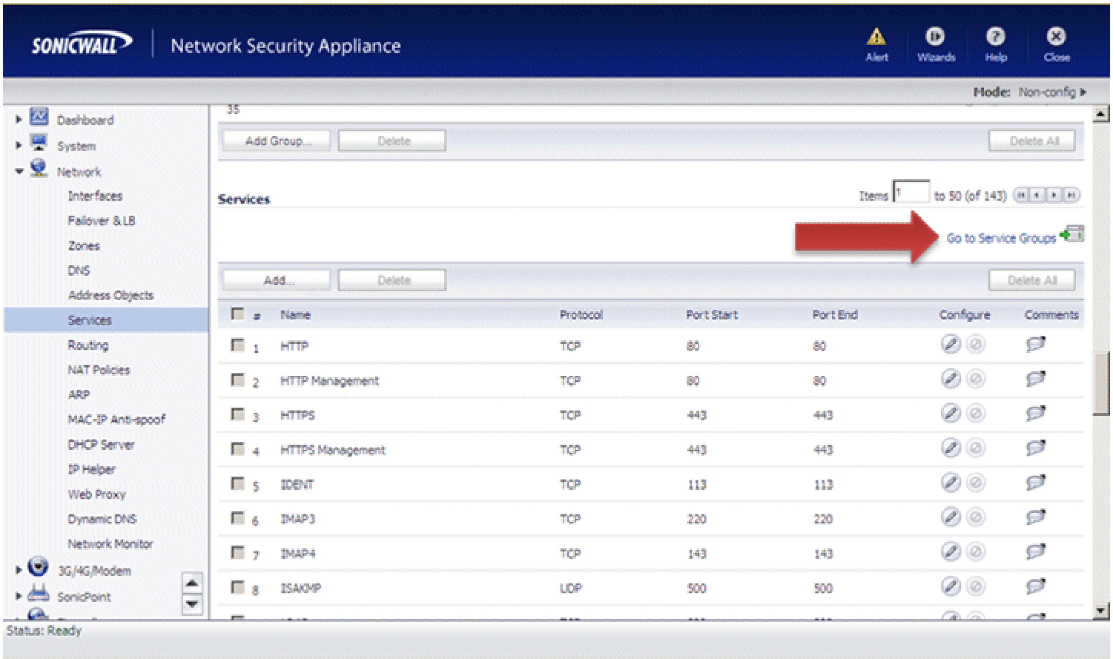
5 Click **Add** to save the new service object.

6 Repeat steps 3-5 to create the rest of the required service objects.

Creating service groups

See “Configuration overview” on page 3-2 for details on the specific service groups you need to create.

1 To create a new service group, click **Go to Service Groups**.

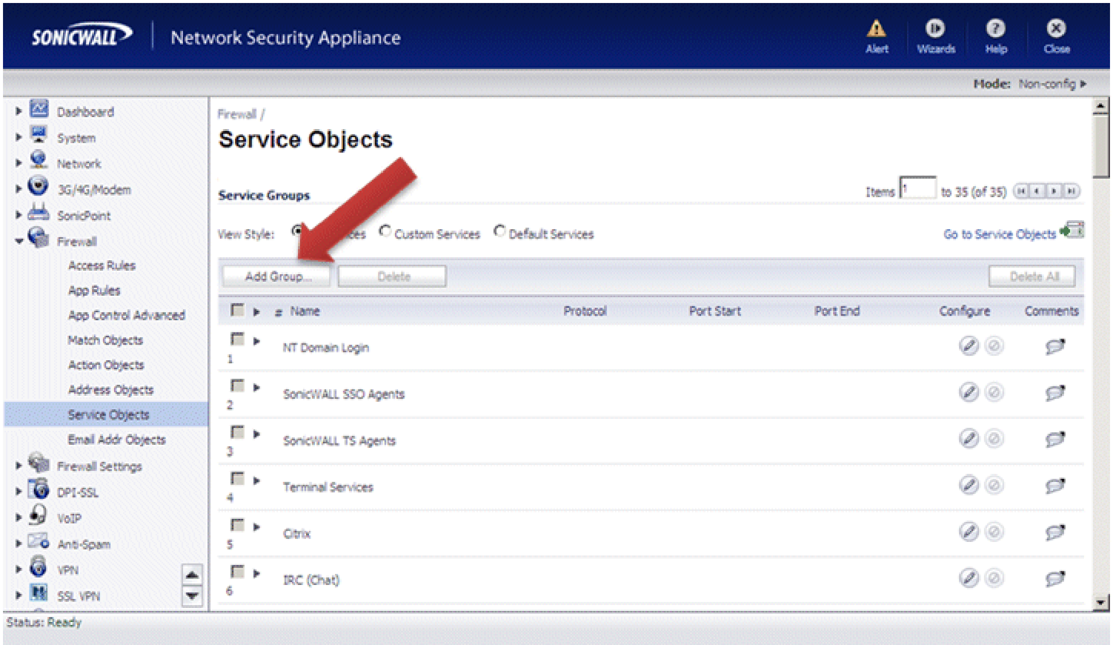


Services

#	Name	Protocol	Port Start	Port End	Configure	Comments
1	HTTP	TCP	80	80		
2	HTTP Management	TCP	80	80		
3	HTTPS	TCP	443	443		
4	HTTPS Management	TCP	443	443		
5	IDENT	TCP	113	113		
6	IMAP3	TCP	220	220		
7	IMAP4	TCP	143	143		
8	ISAKMP	UDP	500	500		

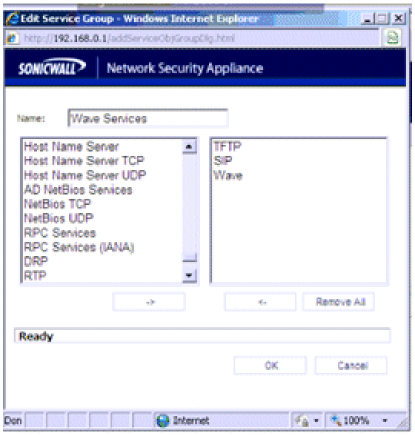
The screen that opens shows service groups, which are *collections* of service objects.

2 Click **Add Group**:



#	Name	Protocol	Port Start	Port End	Configure	Comments
1	NT Domain Login					
2	SonicWALL SSO Agents					
3	SonicWALL TS Agents					
4	Terminal Services					
5	Citrix					
6	IRC (Chat)					

3 Enter a name for the service group, and then add the Wave, TFTP, and SIP service objects:


Edit Service Group - Windows Internet Explorer
http://192.168.0.1/addServiceObjGroupDlg.html
SONICWALL
Network Security Appliance
->
<-
Remove All
OK
Cancel
Don
Internet
100%

Name: Wave Services

Host Name Server
Host Name Server TCP
Host Name Server UDP
AD NetBios Services
NetBios TCP
NetBios UDP
RPC Services
RPC Services (IANA)
DRP
RTP

TFTP
SIP
Wave

Ready

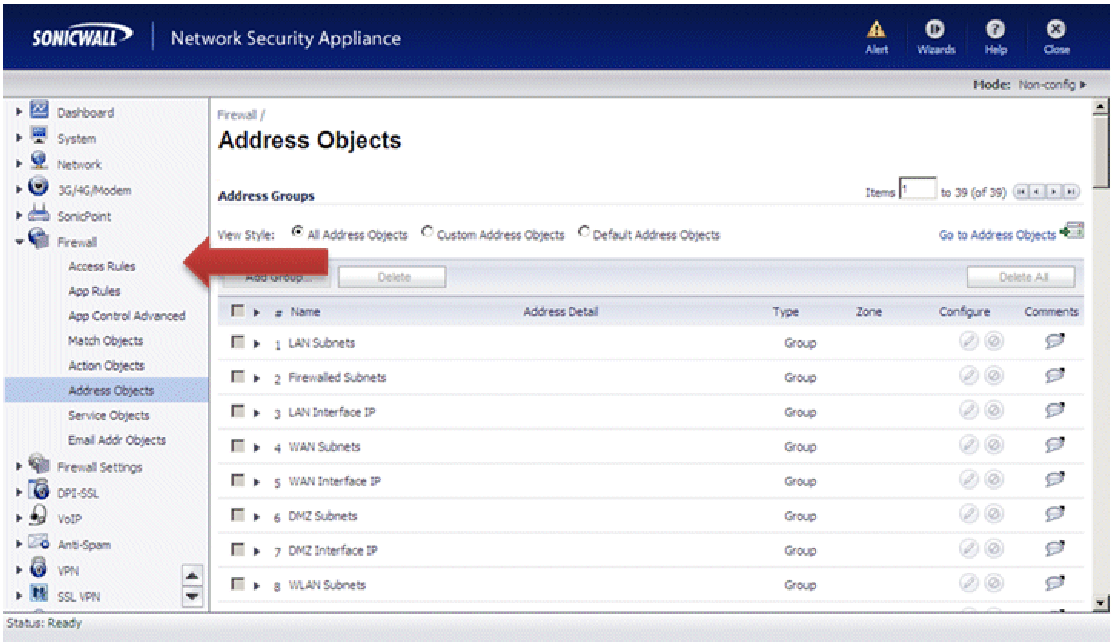
4 Click **OK** to save the new service group.

5 Repeat steps 2-4 to create another service group called All Wave Services. Add the Wave, TFTP, and SIP service objects, as well as all of the MRM service objects that you created previously.

Creating access rules

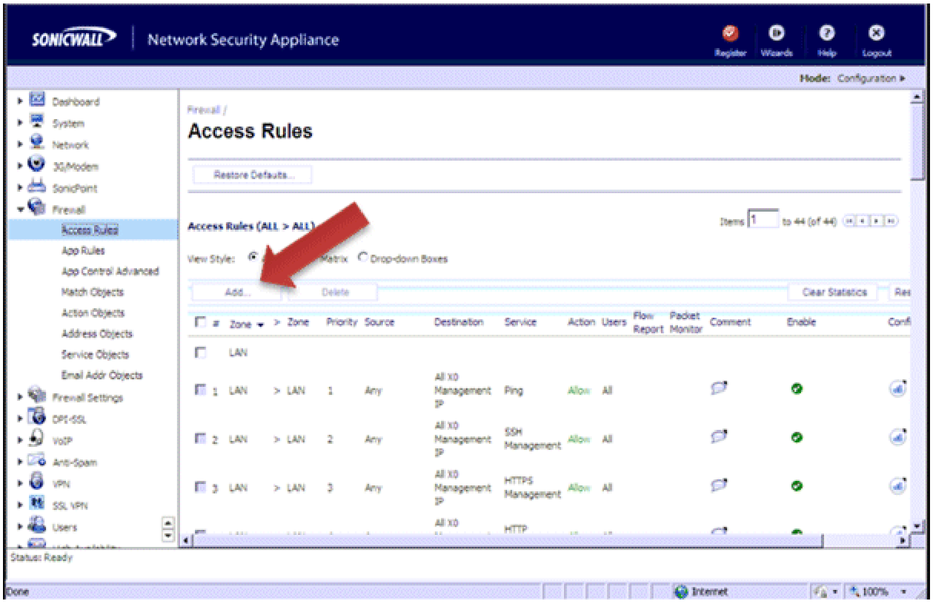
See “Configuration overview” on page 3-2 for details on the specific access rules you need to create.

1 Choose **Firewall > Access Rules** in the navigation pane:



#	Name	Address Detail	Type	Zone	Configure	Comments
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			

2 Click **Add.**



Firewall /

Access Rules

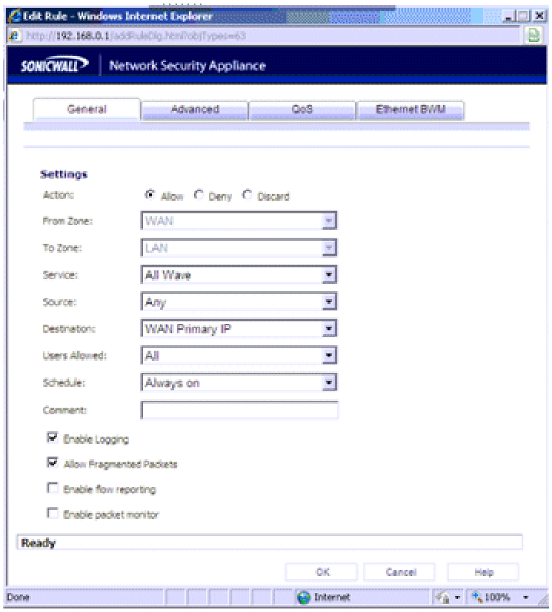
Access Rules (ALL > ALL)

Items 1 to 44 (of 44)

View Style: ● Matrix ○ Drop-down Boxes

□	#	Zone	> Zone	Priority	Source	Destination	Service	Action	Users	Flow Report	Packet Monitor	Comment	Enable	Confi
□		LAN												
□	1	LAN	> LAN	1	Any	All X0 Management IP	Ping	Allow	All				✓	
□	2	LAN	> LAN	2	Any	All X0 Management IP	SSH Management	Allow	All				✓	
□	3	LAN	> LAN	3	Any	All X0 Management IP	HTTPS Management	Allow	All				✓	
						All X0	HTTP							

3 Use the following settings for the rule:


Edit Rule - Windows Internet Explorer
http://192.168.0.1/addRuleDlg.html?objType=63
SONICWALL
Network Security Appliance
General
Advanced
QoS
Ethernet BWM
OK
Cancel
Help
Done
Internet
100%

Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: WAN

To Zone: LAN

Service: All Wave

Source: Any

Destination: WAN Primary IP

Users Allowed: All

Schedule: Always on

Comment:

☑ Enable Logging

☑ Allow Fragmented Packets

□ Enable flow reporting

□ Enable packet monitor

Ready

- **Actions**. Click **Allow.**
- **From Zone**. Select “WAN” from the drop-down list.
- **To Zone**. Select “LAN”.
- **Service**. Select “All Wave”.
- **Source**. Select “Any”.
- **Destination**. Select “WAN Primary IP”.
- **Users Allowed**. Select “All”.
- **Schedule**. Select “Always on”.

4 Click **OK** to save the new rule.

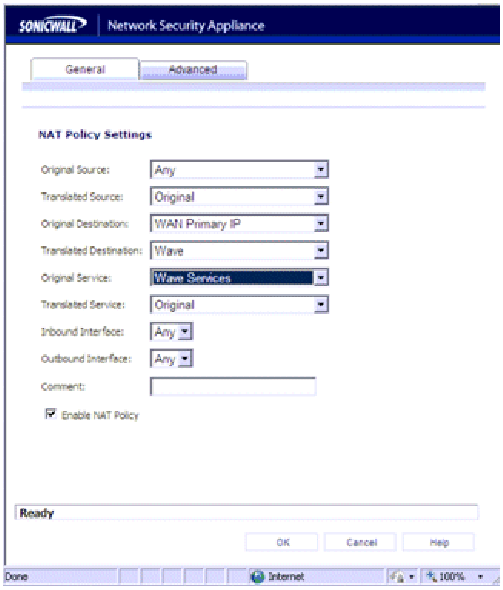
Creating NAT policies

See “Configuration overview” on page 3-2 for details on the specific NAT policies you need to create.

1 Choose **Network > NAT Policies** in the navigation pane.

2 Click **Add**.

3 Create the Wave Policy. Use the following settings for the rule:



NAT Policy Settings

Original Source: Any
Translated Source: Original
Original Destination: WAN Primary IP
Translated Destination: Wave
Original Service: Wave Services
Translated Service: Original
Inbound Interface: Any
Outbound Interface: Any
Comment:
☑ Enable NAT Policy

Ready

- **Original Source**. Select “Any” from the drop-down list.
- **Translated Source**. Select “Original”.
- **Original Destination**. Select “WAN Primary IP”.
- **Translated Destination**. Select “Wave”.
- **Original Service**. Select “Wave Services”.
- **Translated Service**. Select “Original”.
- **Inbound Interface**. Select “Any”.
- **Outbound Interface**. Select “Any”.

4 Click **OK** to save the new policy.

5 Repeat steps 2-4 to create the rest of the required NAT policies for each MRM.

- Change the name, for example “MRMA Policy”.
- For **Translated Destination**, select the appropriate MRM address object from the drop-down list.
- For **Original Service**, select the appropriate MRM service object.

Index