Avaya Solution & Interoperability Test Lab

Application Notes for Configuring a SonicWALL VPN with an Avaya IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe the steps for configuring SonicWALL's VPN to support an Avaya IP Telephony infrastructure consisting of a Main site with Avaya Communication Manager, and two branch sites. During compliance testing, H.323 telephone calls traversing the VPN tunnel were successfully established and maintained while competing non-VoIP traffic queued according to bandwidth reservation defined in the SonicWALL devices. In addition, non-VoIP network traffic using Network Address Translation (NAT) outside of the VPN tunnel was successfully demonstrated. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested solution comprised of Avaya Communication Manager, Avaya IP Telephones, and SonicWALL Unified Threat Management (UTM) devices. The SonicWALL UTM devices tested were the SonicWALL PRO 4060 and TZ 170.

The sample configuration simulates an enterprise with a Main Site, Branch Site A, and Branch Site B. The Main Site and Branch Site A are connected via a 768Kbps PPP WAN link. An Avaya S8300 Media Server at the Main Site is responsible for supporting Avaya IP telephones at the Main Site and Branch Site A. A SonicWALL UTM device is installed at these two sites between the WAN router and the local IP networks. Although the SonicWALL UTM device is capable of functioning as a firewall, that was not the focus of the compliance testing. A single VPN tunnel was established between the SonicWALL PRO 4060 at the Main Site and the TZ 170 at the Branch Site A. The SonicWALL UTM devices were configured to automatically recognize RTP traffic flow negotiated by the H.323 protocol and provide guaranteed bandwidth for the call. Guaranteed bandwidth for two simultaneous Avaya VoIP telephone calls was configured in the SonicWALL UTM devices.

Branch Site B simulated a PC only user site with no Avaya VoIP requirement. This site was used to demonstrate and verify that SonicWALL Network Address Translation does not interfere with Avaya VoIP traffic traversing the VPN tunnel between the Main Site and Branch Site A.

1.1. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All Avaya IP telephones are registered with Avaya Communication Manager in the Main Site. A 768K PPP link simulating a WAN link connects the Main Site and Branch Site A while the SonicWALL UTM establishes the VPN tunnel over this link. A separate 10Mbps link simulating a WAN link connects the Main Site and Branch Site B. All data traffic destined to Branch Site B is NAT to the SonicWALL PRO 4060 WAN interface IP address.

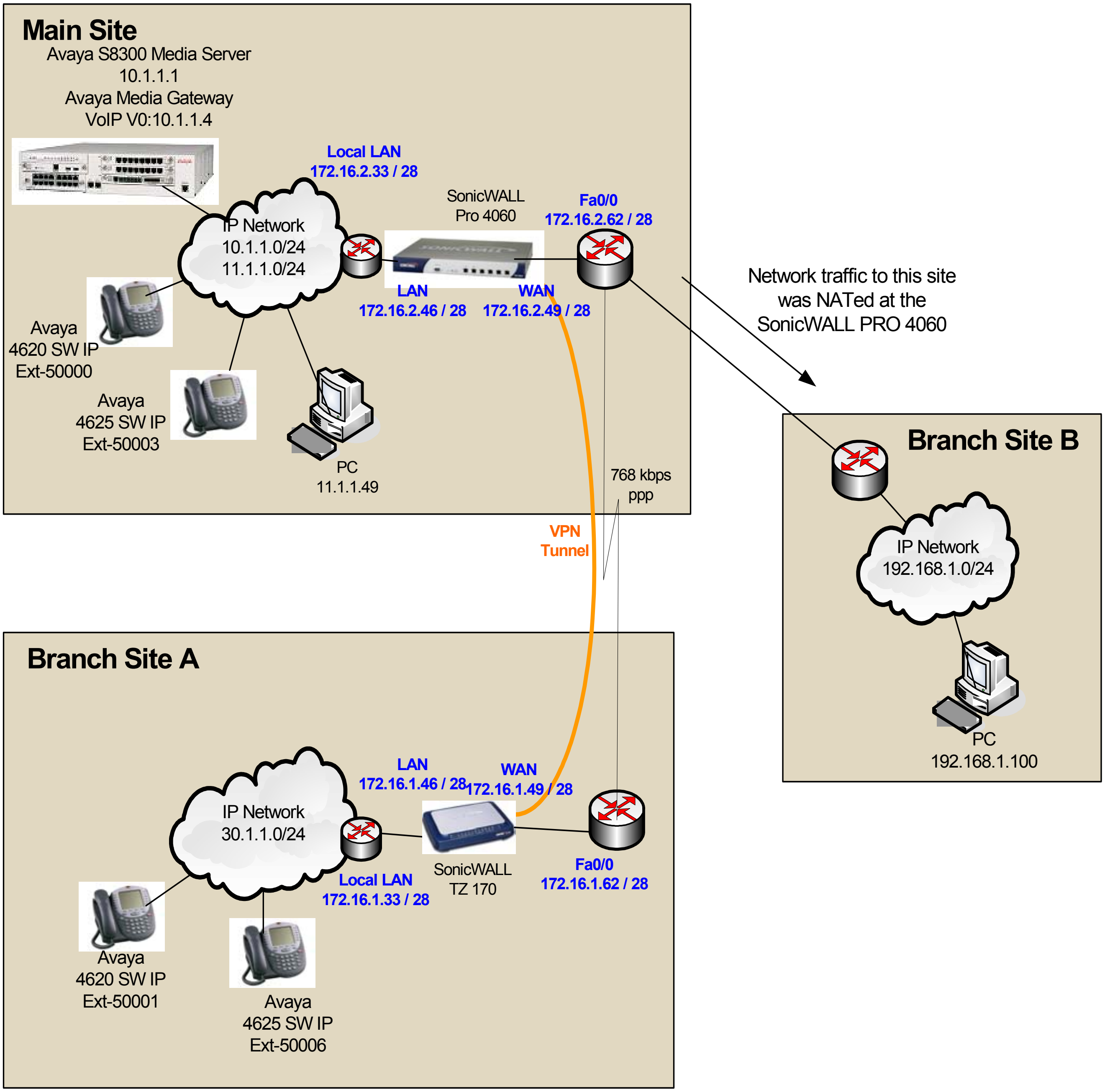


Figure 1: Sample Network Configuration

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya S8300 Media Server with G700 Media Gateway	Avaya Communication Manager 3.0.1 (R0.13x.00.0.346.0)
Avaya 4620SW IP Telephones (H.323)	2.2.3
Avaya 4625SW IP Telephones (H.323)	2.5
SonicWALL Pro4060	SonicOS Enhanced 3.2.0.0-20e
SonicWALL TZ170	SonicOS Enhanced 3.2.0.0-20e

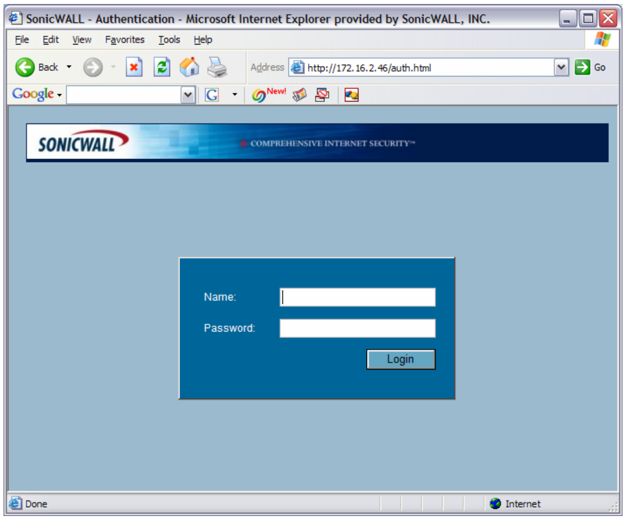
3. SonicWALL Unified Threat Management

The SonicWALL Unified Threat Management (UTM) devices SonicWALL PRO 4060 and TZ 170, were used to establish a VPN tunnel between the Main Site and Branch site A and provide Network Address Translation between the Main Site and Branch Site B. The following steps outline the configuration for SonicWALL Unified Threat Management devices and the VPN tunnel.

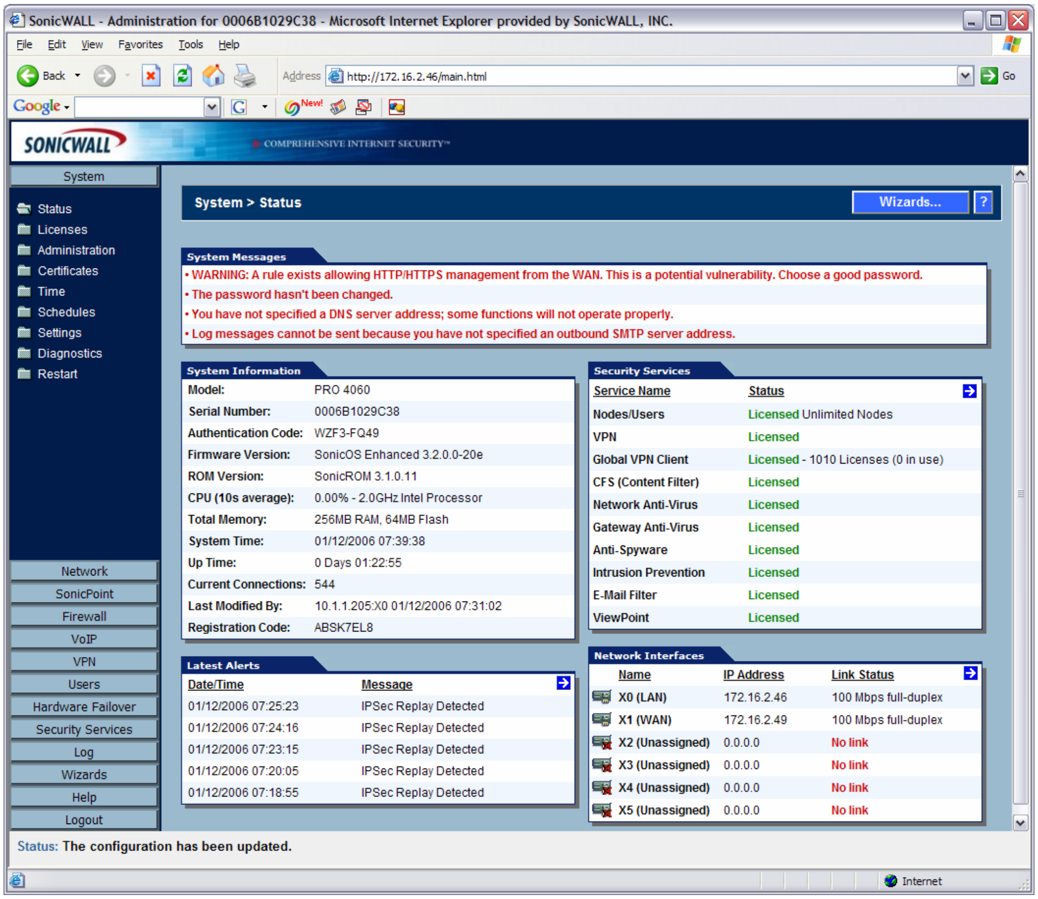
The steps in this section depict the screen displays for the SonicWALL PRO 4060 at the Main Site. Repeat these steps for the SonicWALL TZ 170 at Branch Site A with the appropriate IP address information.

3.1. General SonicWALL UTM Configuration

This section presents the SonicWALL VPN tunnel configuration.

Step	Description
1.	Enter the IP address of the SonicWALL PRO 4060 into the Web Browser. Enter the appropriate **Name** and **Password** to log into the system. 

SonicWALL - Authentication - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back
Address http://172.16.2.46/auth.html
Go
Google
SONICWALL
COMPREHENSIVE INTERNET SECURITY
Name:
Password:
Login
Done
Internet

Step	Description
2.	The **System>Status** screen is displayed after successfully logging on. Click on the **Network** tab on the left to expand it. 

System Messages

- WARNING: A rule exists allowing HTTP/HTTPS management from the WAN. This is a potential vulnerability. Choose a good password.
- The password hasn't been changed.
- You have not specified a DNS server address; some functions will not operate properly.
- Log messages cannot be sent because you have not specified an outbound SMTP server address.

System Information

Model:	PRO 4060
Serial Number:	0006B1029C38
Authentication Code:	WZF3-FQ49
Firmware Version:	SonicOS Enhanced 3.2.0.0-20e
ROM Version:	SonicROM 3.1.0.11
CPU (10s average):	0.00% - 2.0GHz Intel Processor
Total Memory:	256MB RAM, 64MB Flash
System Time:	01/12/2006 07:39:38
Up Time:	0 Days 01:22:55
Current Connections:	544
Last Modified By:	10.1.1.205:X0 01/12/2006 07:31:02
Registration Code:	ABSK7EL8

Security Services

Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 1010 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

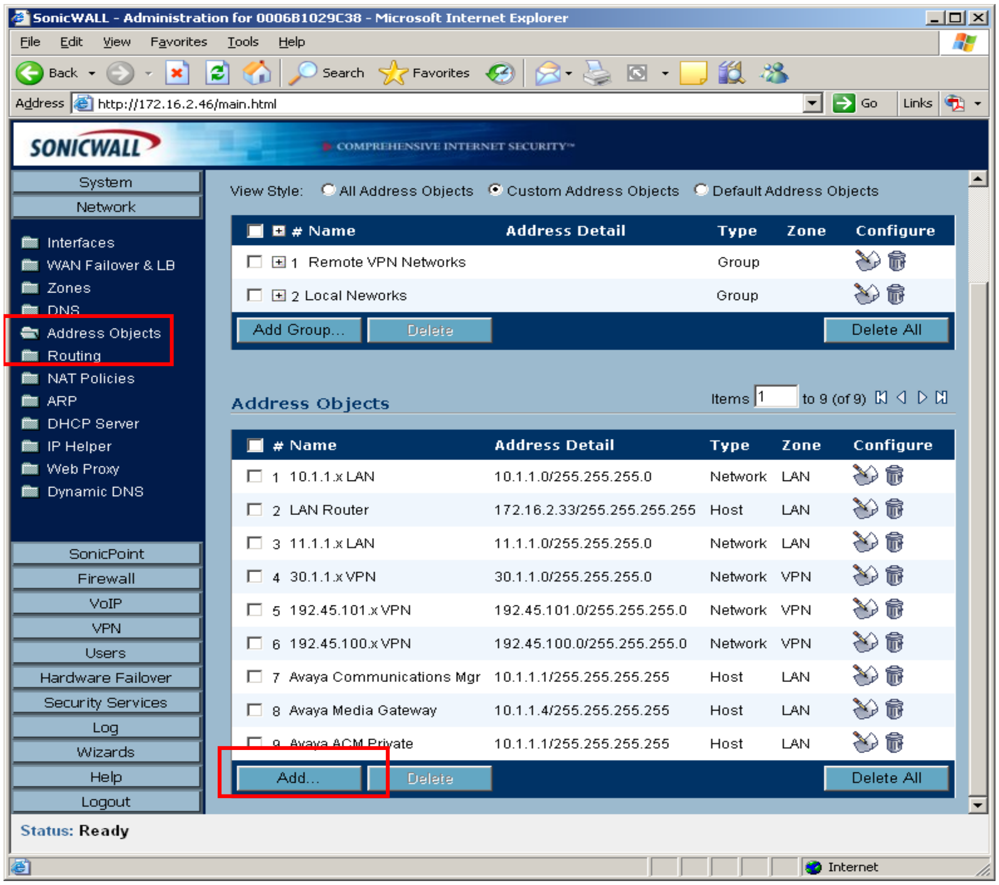
Latest Alerts

Date/Time	Message
01/12/2006 07:25:23	IPSec Replay Detected
01/12/2006 07:24:16	IPSec Replay Detected
01/12/2006 07:23:15	IPSec Replay Detected
01/12/2006 07:20:05	IPSec Replay Detected
01/12/2006 07:18:55	IPSec Replay Detected

Network Interfaces

Name	IP Address	Link Status
X0 (LAN)	172.16.2.46	100 Mbps full-duplex
X1 (WAN)	172.16.2.49	100 Mbps full-duplex
X2 (Unassigned)	0.0.0.0	No link
X3 (Unassigned)	0.0.0.0	No link
X4 (Unassigned)	0.0.0.0	No link
X5 (Unassigned)	0.0.0.0	No link

Status: The configuration has been updated.

Step	Description
3.	Under the expanded **Network** tab on the left, select **Address Objects**. Click the **Add** button in the **Address Objects** panel to display the **Add Address Objects** pop-up window. 

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

# Name	Address Detail	Type	Zone	Configure
1 Remote VPN Networks		Group		
2 Local Neworks		Group		

Add Group... Delete Delete All

Address Objects

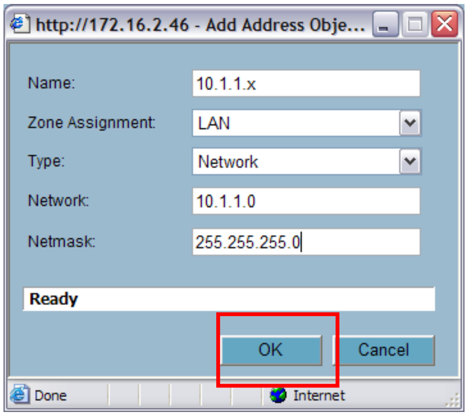
Items 1 to 9 (of 9)

#	Name	Address Detail	Type	Zone	Configure
1	10.1.1.x LAN	10.1.1.0/255.255.255.0	Network	LAN	
2	LAN Router	172.16.2.33/255.255.255.255	Host	LAN	
3	11.1.1.x LAN	11.1.1.0/255.255.255.0	Network	LAN	
4	30.1.1.x VPN	30.1.1.0/255.255.255.0	Network	VPN	
5	192.45.101.x VPN	192.45.101.0/255.255.255.0	Network	VPN	
6	192.45.100.x VPN	192.45.100.0/255.255.255.0	Network	VPN	
7	Avaya Communications Mgr	10.1.1.1/255.255.255.255	Host	LAN	
8	Avaya Media Gateway	10.1.1.4/255.255.255.255	Host	LAN	
9	Avaya ACM Private	10.1.1.1/255.255.255.255	Host	LAN	

Add... Delete Delete All

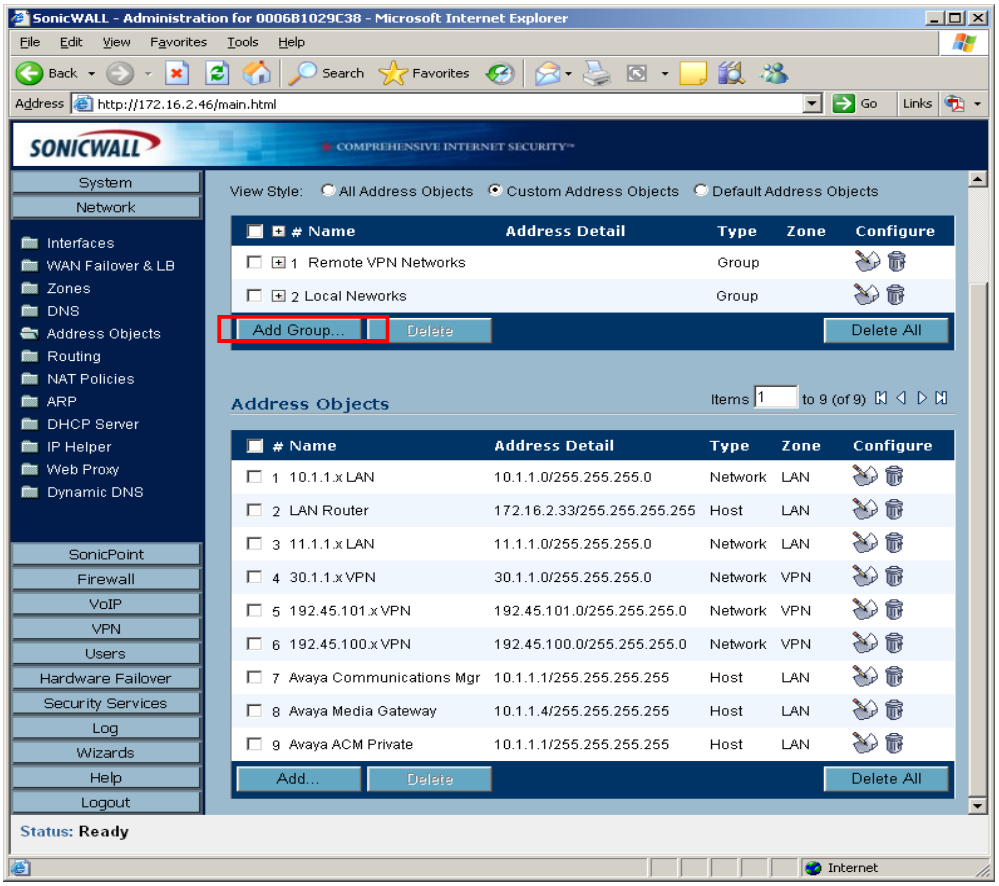
Status: Ready

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>4.</b></td><td>
Define all the IP networks that will be traversing the VPN tunnel. Click <b>OK</b> to save after entering the information. There are three IP networks and two hosts in the sample configuration that need to be defined. The IP Networks and host information are as follows:
<table>
<tr><th>Name:</th><th>Zone Assignment</th><th>Type</th><th>Network</th><th>Netmask</th></tr>
<tr><td>10.1.1.x</td><td>LAN</td><td>Network</td><td>10.1.1.0</td><td>255.255.255.0</td></tr>
<tr><td>11.1.1.x</td><td>LAN</td><td>Network</td><td>11.1.1.0</td><td>255.255.255.0</td></tr>
<tr><td>30.1.1.x</td><td>VPN</td><td>Network</td><td>30.1.1.0</td><td>255.255.255.0</td></tr>
<tr><td>LAN Router</td><td>LAN</td><td>Host</td><td>172.16.2.33</td><td>N/A</td></tr>
<tr><td>Avaya Media Gateway</td><td>LAN</td><td>Host</td><td>10.1.1.4</td><td>N/A</td></tr>
</table>
Repeat step 3 and 4 until all the IP networks and hosts above are defined.



http://172.16.2.46 - Add Address Obje...
Name: 10.1.1.x
Zone Assignment: LAN
Type: Network
Network: 10.1.1.0
Netmask: 255.255.255.0
Ready

</td></tr>
</table>

Step	Description
5.	Define the group where the **Address Objects** belong. In the sample configuration, there were two groups. The **Local Networks** was composed of all the locally connected IP networks, and the **Remote VPN Networks** was composed of all the IP networks on the other end of the VPN tunnel. Click **Add Group** to display the **Add Address Object Group** pop-up windows. 

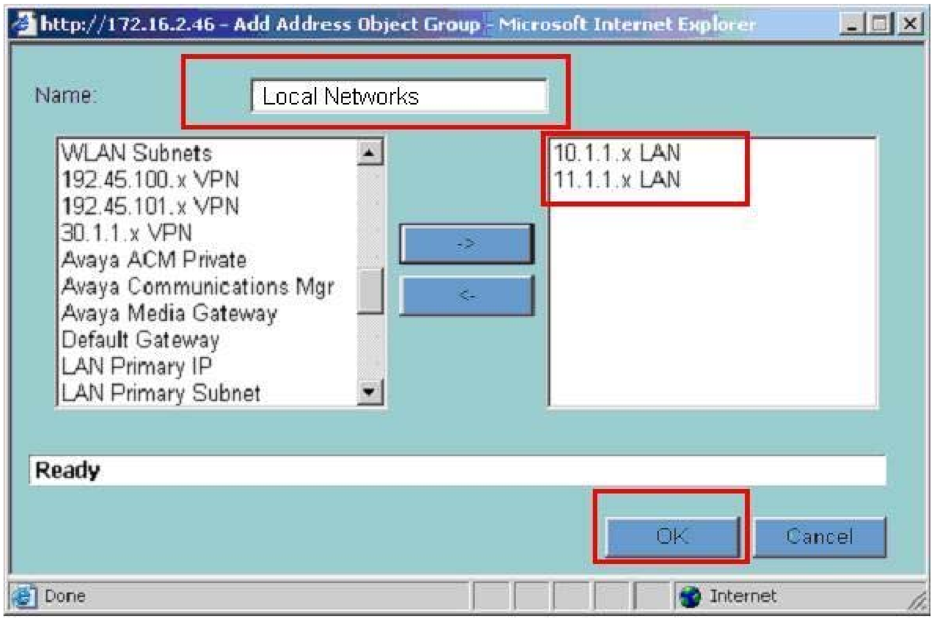
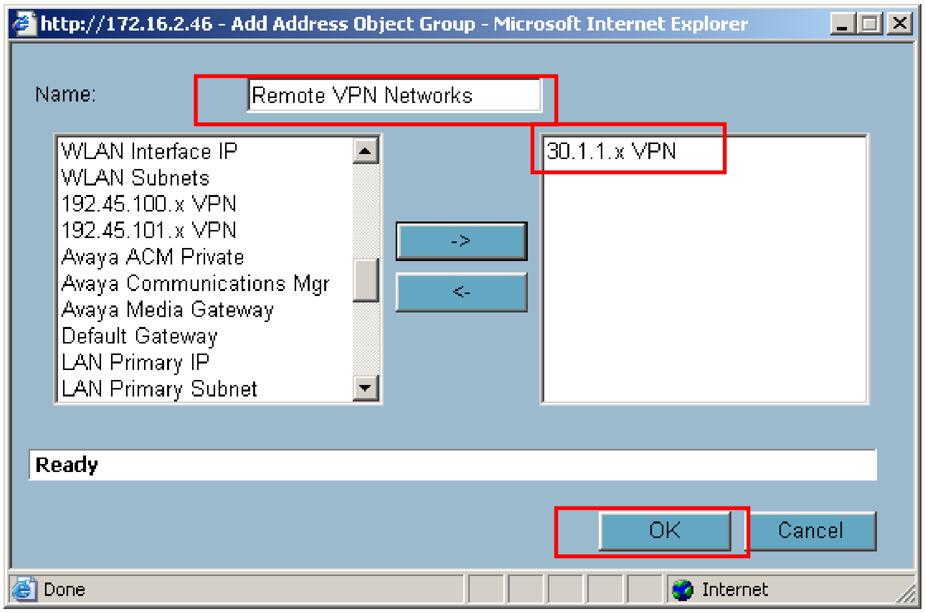
View Style: ○ All Address Objects ● Custom Address Objects ○ Default Address Objects

#	Name	Address Detail	Type	Zone	Configure
1	Remote VPN Networks		Group		
2	Local Neworks		Group		

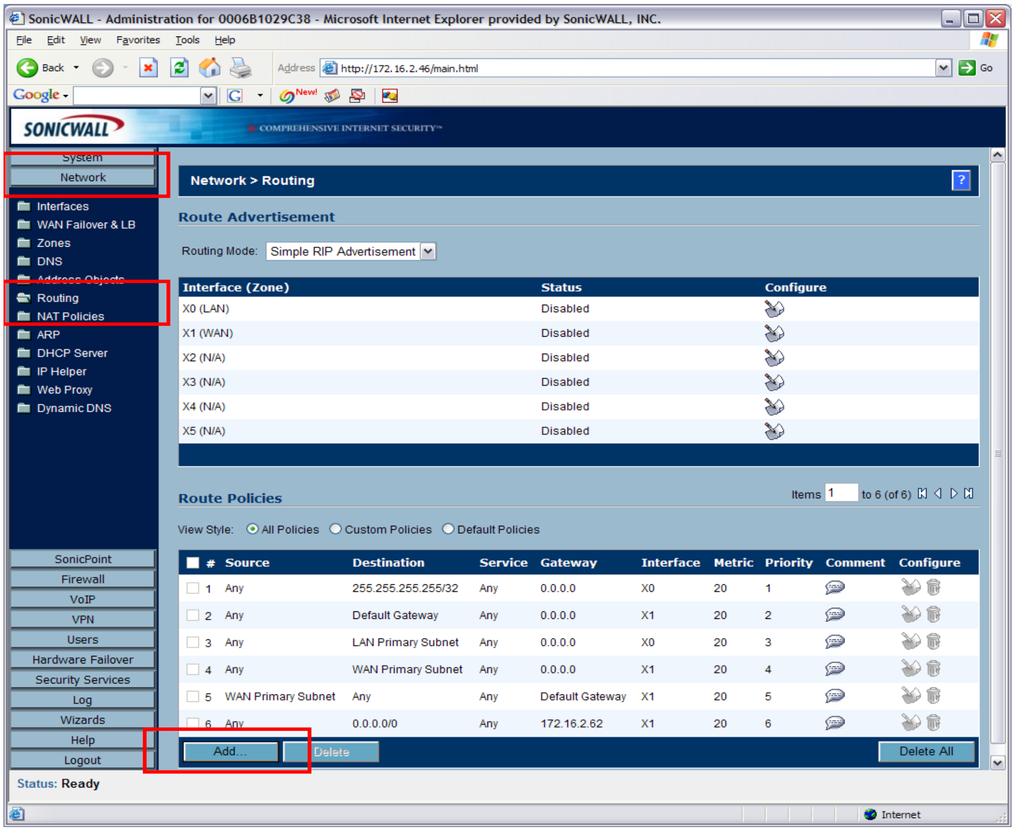
Address Objects

Items 1 to 9 (of 9)

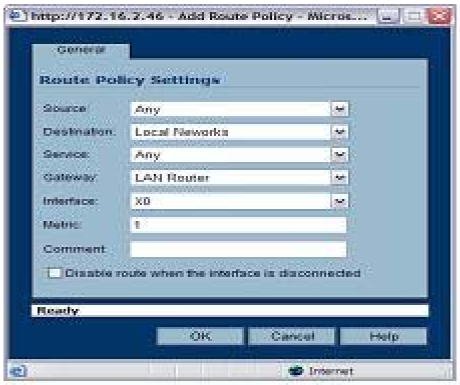
#	Name	Address Detail	Type	Zone	Configure
1	10.1.1.x LAN	10.1.1.0/255.255.255.0	Network	LAN	
2	LAN Router	172.16.2.33/255.255.255.255	Host	LAN	
3	11.1.1.x LAN	11.1.1.0/255.255.255.0	Network	LAN	
4	30.1.1.x VPN	30.1.1.0/255.255.255.0	Network	VPN	
5	192.45.101.x VPN	192.45.101.0/255.255.255.0	Network	VPN	
6	192.45.100.x VPN	192.45.100.0/255.255.255.0	Network	VPN	
7	Avaya Communications Mgr	10.1.1.1/255.255.255.255	Host	LAN	
8	Avaya Media Gateway	10.1.1.4/255.255.255.255	Host	LAN	
9	Avaya ACM Private	10.1.1.1/255.255.255.255	Host	LAN	

Step	Description
6.	At the **Add Address Object Group** window, enter the name for the network group. The sample configuration used the name **Local Networks**. Highlight the desired networks to be included in this group on the left, then click **->** to move the highlighted objects to the right. Click **OK** to complete.  http://172.16.2.46 - Add Address Object Group - Microsoft Internet Explorer Name: Local Networks 10.1.1.x LAN 11.1.1.x LAN Ready WLAN Subnets 192.45.100.x VPN 192.45.101.x VPN 30.1.1.x VPN Avaya ACM Private Avaya Communications Mgr Avaya Media Gateway Default Gateway LAN Primary IP LAN Primary Subnet -> <- OK Cancel Done Internet
7.	Repeat Step 5 for the **Remote VPN Networks**. Click **OK** to complete.  http://172.16.2.46 - Add Address Object Group - Microsoft Internet Explorer Name: Remote VPN Networks 30.1.1.x VPN Ready WLAN Interface IP WLAN Subnets 192.45.100.x VPN 192.45.101.x VPN Avaya ACM Private Avaya Communications Mgr Avaya Media Gateway Default Gateway LAN Primary IP LAN Primary Subnet -> <- OK Cancel Done Internet

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>8.</b></td><td>
<p>Define the routing configuration of the SonicWALL PRO 4060 by clicking on <b>Routing</b> under the <b>Network</b> tab on the left. Click <b>Add</b> under the <b>Route Policies</b> panel to display the <b>Add Route Policy</b> pop-up windows.</p>

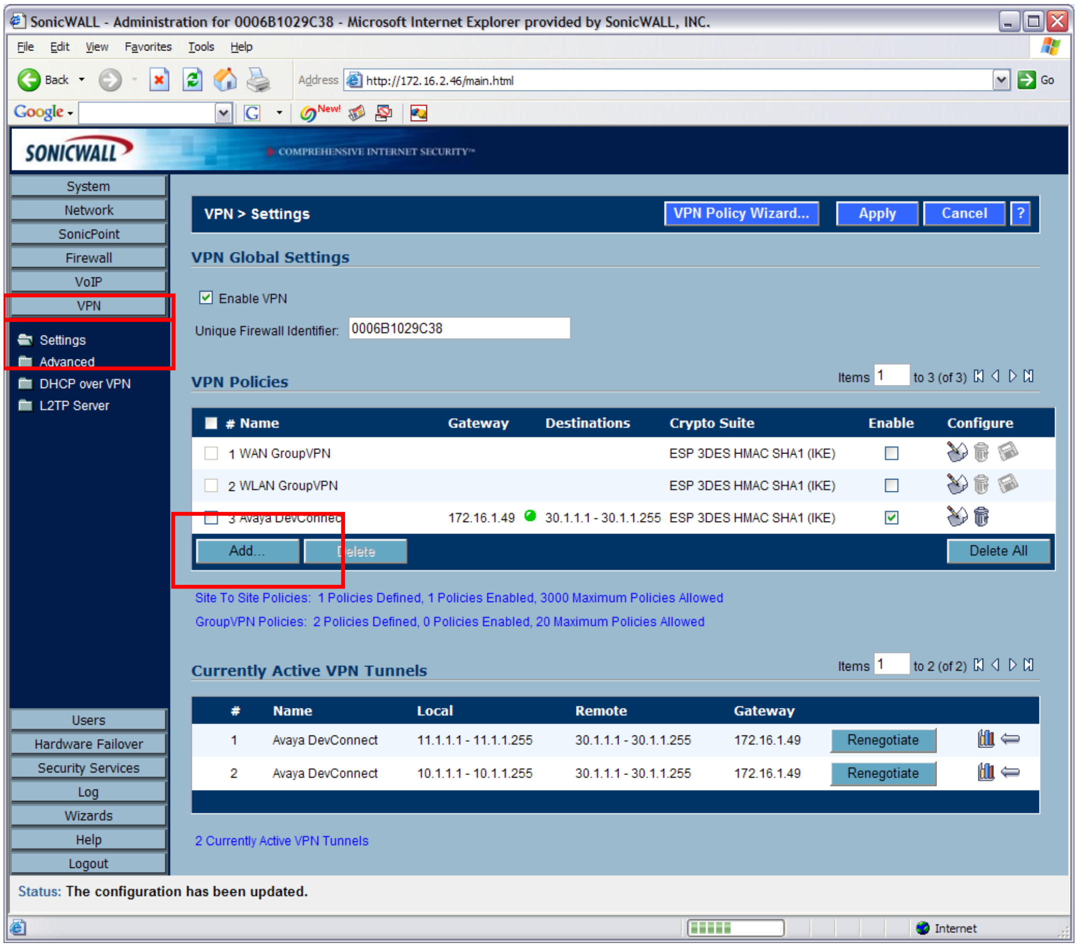


<p><b>Network > Routing</b></p>
<p><b>Route Advertisement</b></p>
<p>Routing Mode: Simple RIP Advertisement</p>
<table>
<tr><th>Interface (Zone)</th><th>Status</th><th>Configure</th></tr>
<tr><td>X0 (LAN)</td><td>Disabled</td><td></td></tr>
<tr><td>X1 (WAN)</td><td>Disabled</td><td></td></tr>
<tr><td>X2 (N/A)</td><td>Disabled</td><td></td></tr>
<tr><td>X3 (N/A)</td><td>Disabled</td><td></td></tr>
<tr><td>X4 (N/A)</td><td>Disabled</td><td></td></tr>
<tr><td>X5 (N/A)</td><td>Disabled</td><td></td></tr>
</table>
<p><b>Route Policies</b> Items 1 to 6 (of 6)</p>
<p>View Style: ● All Policies ○ Custom Policies ○ Default Policies</p>
<table>
<tr><th>☐</th><th>#</th><th>Source</th><th>Destination</th><th>Service</th><th>Gateway</th><th>Interface</th><th>Metric</th><th>Priority</th><th>Comment</th><th>Configure</th></tr>
<tr><td>☐</td><td>1</td><td>Any</td><td>255.255.255.255/32</td><td>Any</td><td>0.0.0.0</td><td>X0</td><td>20</td><td>1</td><td></td><td></td></tr>
<tr><td>☐</td><td>2</td><td>Any</td><td>Default Gateway</td><td>Any</td><td>0.0.0.0</td><td>X1</td><td>20</td><td>2</td><td></td><td></td></tr>
<tr><td>☐</td><td>3</td><td>Any</td><td>LAN Primary Subnet</td><td>Any</td><td>0.0.0.0</td><td>X0</td><td>20</td><td>3</td><td></td><td></td></tr>
<tr><td>☐</td><td>4</td><td>Any</td><td>WAN Primary Subnet</td><td>Any</td><td>0.0.0.0</td><td>X1</td><td>20</td><td>4</td><td></td><td></td></tr>
<tr><td>☐</td><td>5</td><td>WAN Primary Subnet</td><td>Any</td><td>Any</td><td>Default Gateway</td><td>X1</td><td>20</td><td>5</td><td></td><td></td></tr>
<tr><td>☐</td><td>6</td><td>Any</td><td>0.0.0.0/0</td><td>Any</td><td>172.16.2.62</td><td>X1</td><td>20</td><td>6</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td><b>9.</b></td><td>
<p>Define a route policy as shown:</p>
<p>Traffic from <b><i>Any</i></b> source destined to the <b><i>Local Networks</i></b> for <b><i>Any</i></b> service use <b><i>LAN Router</i></b> gateway reachable from interface X0 with a metric of <b><i>1</i></b>.</p>
<p><b><i>Local Networks</i></b> and <b><i>LAN Router</i></b> were defined in step 6 and 4 above respectively.</p>



<p><b>Route Policy Settings</b></p>
<p>Source: Any
Destination: Local Neworks
Service: Any
Gateway: LAN Router
Interface: X0
Metric: 1
Comment:
☐ Disable route when the interface is disconnected</p>
<p>Ready</p>
</td></tr>
</table>

3.2. Configure the VPN tunnel for the SonicWALL UTM devices

Step	Description
1.	Begin configuration of the VPN tunnel by clicking on **Settings** under the **VPN** tab on the left. Click **Add** under the VPN policies panel to display the **Security Policy** pop-up window. 

VPN > Settings

VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0006B1029C38

VPN Policies

Items 1 to 3 (of 3)

☐ # Name	Gateway	Destinations	Crypto Suite	Enable	Configure
☐ 1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
☐ 2 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
☐ 3 Avaya DevConnec	172.16.1.49 ●	30.1.1.1 - 30.1.1.255	ESP 3DES HMAC SHA1 (IKE)	☑	

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 3000 Maximum Policies Allowed

GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 20 Maximum Policies Allowed

Currently Active VPN Tunnels

Items 1 to 2 (of 2)

#	Name	Local	Remote	Gateway	
1	Avaya DevConnect	11.1.1.1 - 11.1.1.255	30.1.1.1 - 30.1.1.255	172.16.1.49	Renegotiate
2	Avaya DevConnect	10.1.1.1 - 10.1.1.255	30.1.1.1 - 30.1.1.255	172.16.1.49	Renegotiate

2 Currently Active VPN Tunnels

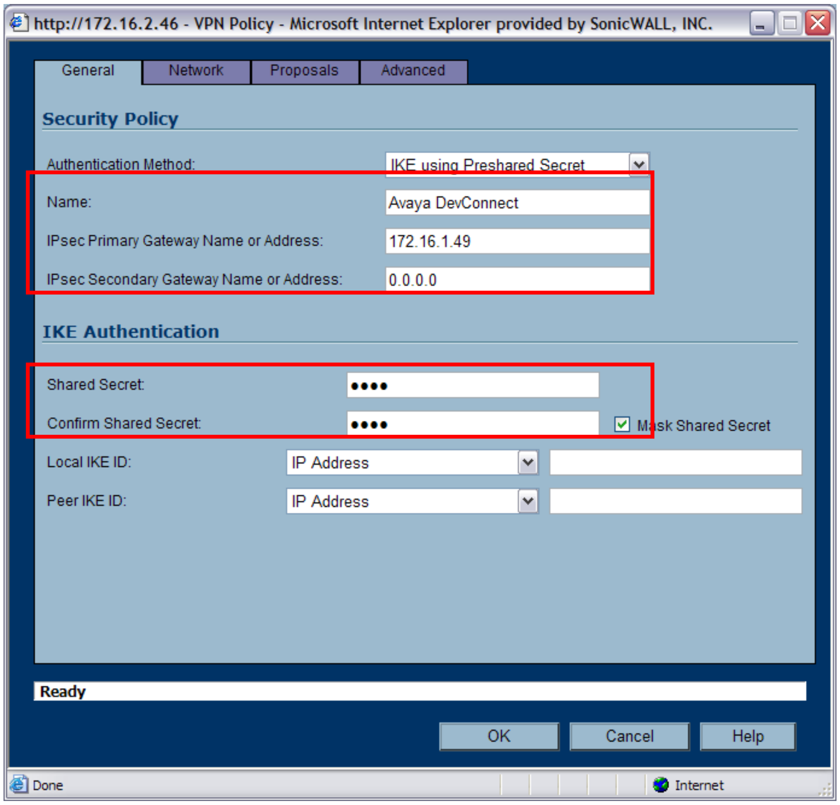
Status: **The configuration has been updated.**

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>2.</b></td><td>

In the General tab of the **Security Policy** pop-up window, enter the following information for the VPN tunnel.

Name: *Avaya DevConnect* (a descriptive name for the VPN tunnel)
IPsec Primary Gateway Name or Address:
172.16.1.49 (the IP address of the remote SonicWALL's WAN interface)
IPsec Secondary Gateway Name or Address:
0.0.0.0
Shared Secret: *1234* (a secret string that will be entered into both SonicWALL devices)

Click on the **Network** tab after entering the above information.



http://172.16.2.46 - VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.

Security Policy

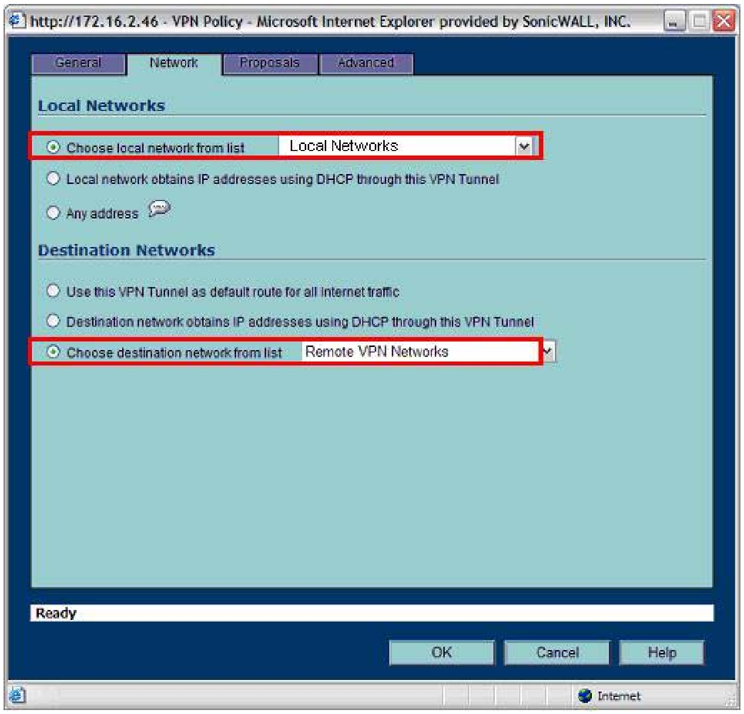
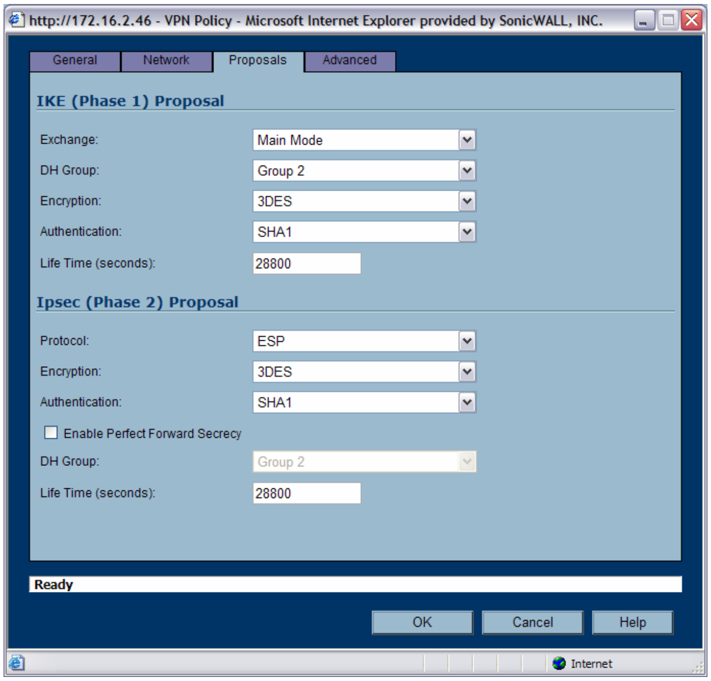
Authentication Method: IKE using Preshared Secret
Name: Avaya DevConnect
IPsec Primary Gateway Name or Address: 172.16.1.49
IPsec Secondary Gateway Name or Address: 0.0.0.0

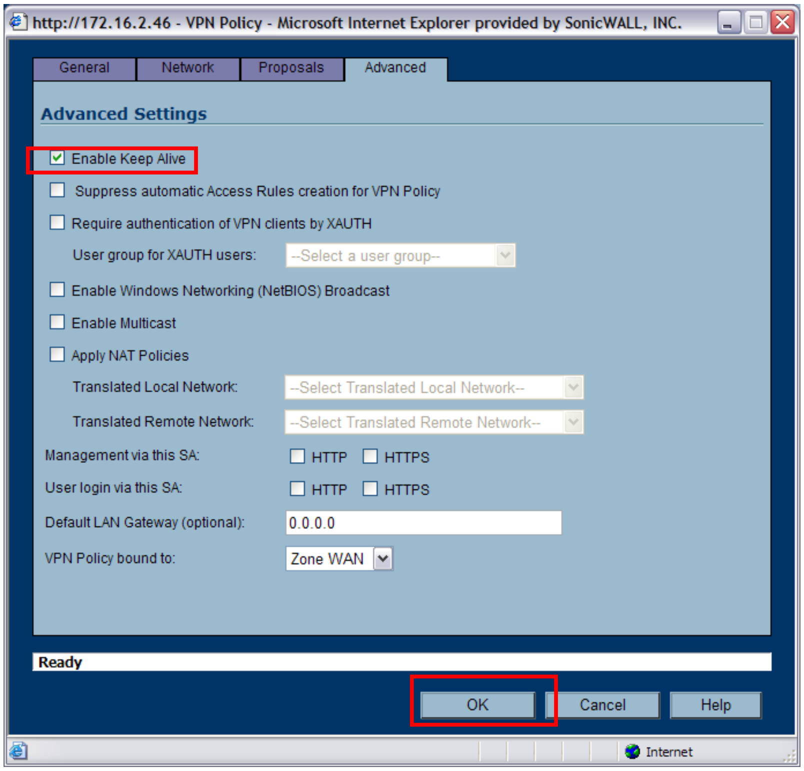
IKE Authentication

Shared Secret: ••••
Confirm Shared Secret: •••• ☑ Mask Shared Secret
Local IKE ID: IP Address
Peer IKE ID: IP Address

Ready

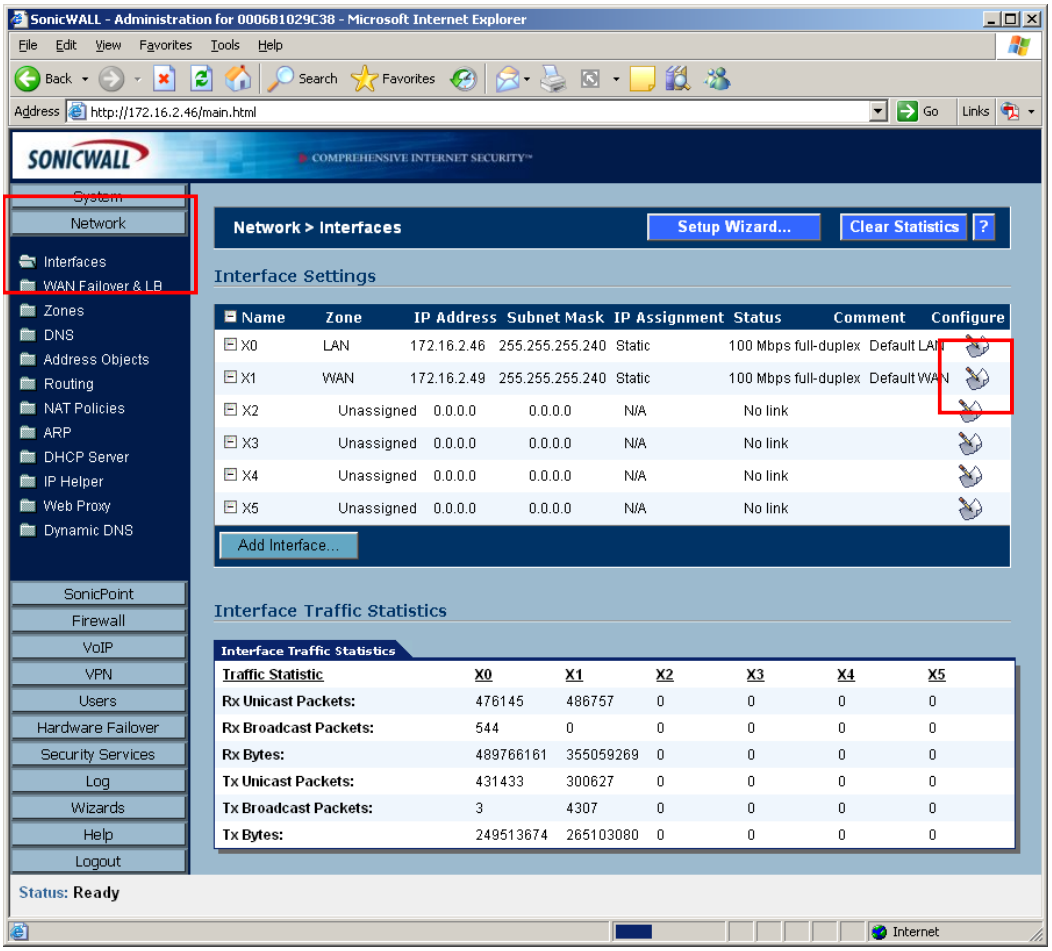
</td></tr>
</table>

Step	Description
3.	Under the Network tab, select **Local Networks** and **Remote VPN Networks** as defined in Section 3.1 step 6 and 7 respectively. Click on the **Proposals** tab.  http://172.16.2.46 - VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC. General Network Proposals Advanced Ready OK Cancel Help Internet **Local Networks** ● Choose local network from list: Local Networks ○ Local network obtains IP addresses using DHCP through this VPN Tunnel ○ 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: Remote VPN Networks
4.	All the fields in the **Proposal** tab were left at the default value in the sample configuration. Click on the **Advanced** tab to continue.  http://172.16.2.46 - VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC. General Network Proposals Advanced Ready OK Cancel Help Internet **IKE (Phase 1) Proposal** Exchange: Main Mode 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 2 Life Time (seconds): 28800

Step	Description
5.	Under the **Advanced** tab, **Enable Keep Alive** by clicking the check box on the left. Click **OK** to complete.  http://172.16.2.46 - VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC. General Network Proposals Advanced Advanced Settings ☑ Enable Keep Alive ☐ Suppress automatic Access Rules creation for VPN Policy ☐ Require authentication of VPN clients by XAUTH User group for XAUTH users: --Select a user group-- ☐ Enable Windows Networking (NetBIOS) Broadcast ☐ Enable Multicast ☐ Apply NAT Policies Translated Local Network: --Select Translated Local Network-- Translated Remote Network: --Select Translated Remote Network-- Management via this SA: ☐ HTTP ☐ HTTPS User login via this SA: ☐ HTTP ☐ HTTPS Default LAN Gateway (optional): 0.0.0.0 VPN Policy bound to: Zone WAN Ready

3.3. Configure the Firewall Access Rules and Bandwidth Reservation for the SonicWALL VPN Tunnel.

This section defines the necessary Firewall Access Rules and Bandwidth Reservation for VoIP traffic for the VPN Tunnel.

Step	Description
1.	Begin by defining the Bandwidth for the WAN interface by selecting **Interfaces** under the **Network** tab on the left. Click on the icon on the right for the WAN Zone under the Interface Settings panel. 

Network > Interfaces

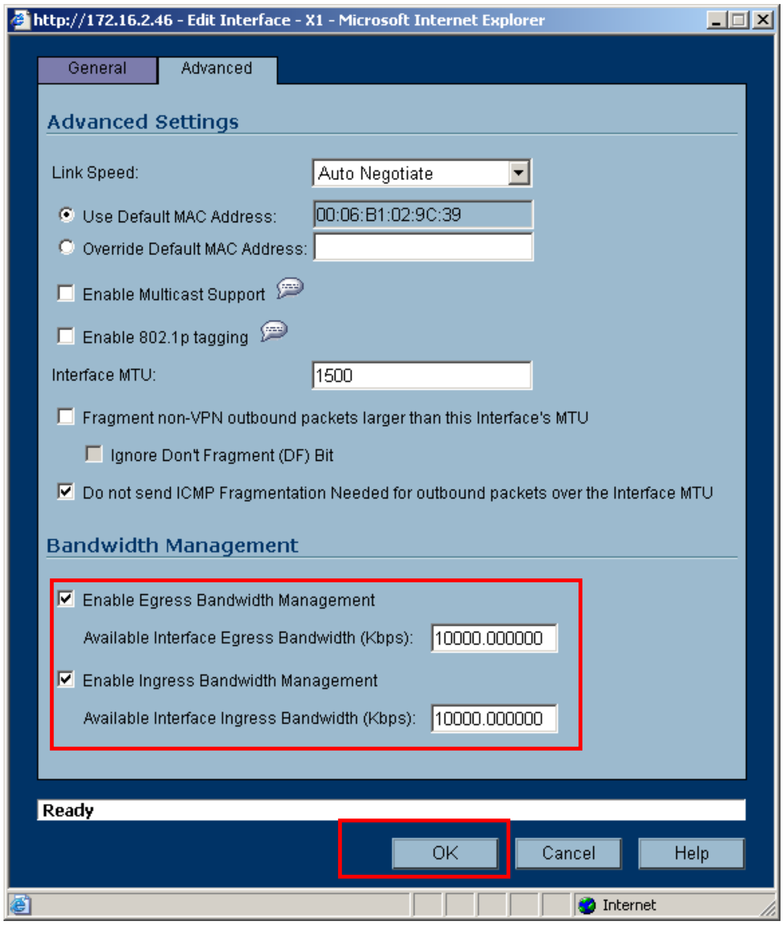
Interface Settings

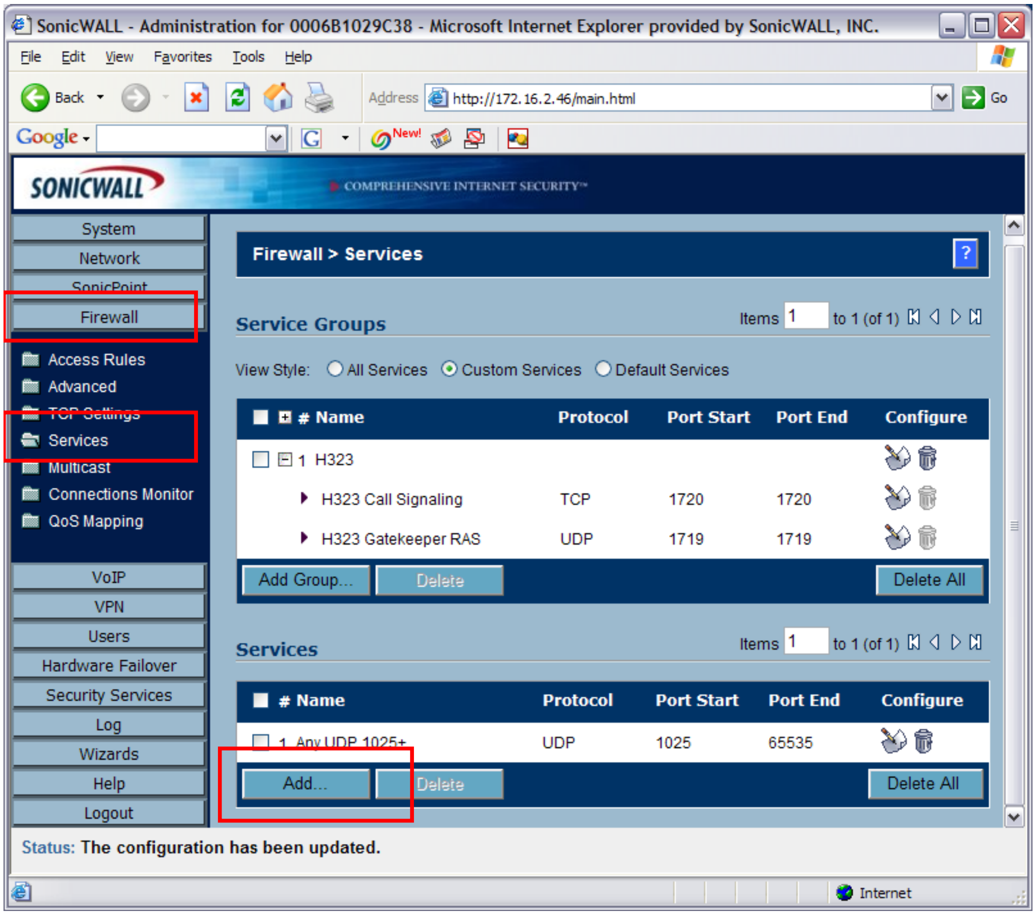
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	172.16.2.46	255.255.255.240	Static	100 Mbps full-duplex	Default LAN	
X1	WAN	172.16.2.49	255.255.255.240	Static	100 Mbps full-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	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:	476145	486757	0	0	0	0
Rx Broadcast Packets:	544	0	0	0	0	0
Rx Bytes:	489766161	355059269	0	0	0	0
Tx Unicast Packets:	431433	300627	0	0	0	0
Tx Broadcast Packets:	3	4307	0	0	0	0
Tx Bytes:	249513674	265103080	0	0	0	0

Status: Ready

Step	Description
2.	From the **Edit Interface** pop-up window, select the **Advanced** tab. Enable bandwidth management by checking the **Enable Egress Bandwidth Management** and **Enable Ingress Bandwidth Management** check box. Enter the appropriate Egress and Ingress Bandwidth in kbps. The sample configuration was configured with 10,000 kbps as shown below. This number will be used as the basis for calculating Bandwidth Reservation. Click **OK** to complete.  http://172.16.2.46 - Edit Interface - X1 - Microsoft Internet Explorer General Advanced Advanced Settings Link Speed: Auto Negotiate ● Use Default MAC Address: 00:06:B1:02:9C:39 ○ Override Default MAC Address: ☐ Enable Multicast Support ☐ Enable 802.1p tagging Interface MTU: 1500 ☐ Fragment non-VPN outbound packets larger than this Interface's MTU ☐ Ignore Don't Fragment (DF) Bit ☑ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU Bandwidth Management ☑ Enable Egress Bandwidth Management Available Interface Egress Bandwidth (Kbps): 10000.000000 ☑ Enable Ingress Bandwidth Management Available Interface Ingress Bandwidth (Kbps): 10000.000000 Ready OK Cancel Help Internet

Step	Description
3.	Now define the Firewall services by selecting **Services** under the **Firewall** tab on the left. Click on **Add** under **Services** panel to display the **Add Service** pop-up window. 

Service Groups Items 1 to 1 (of 1)

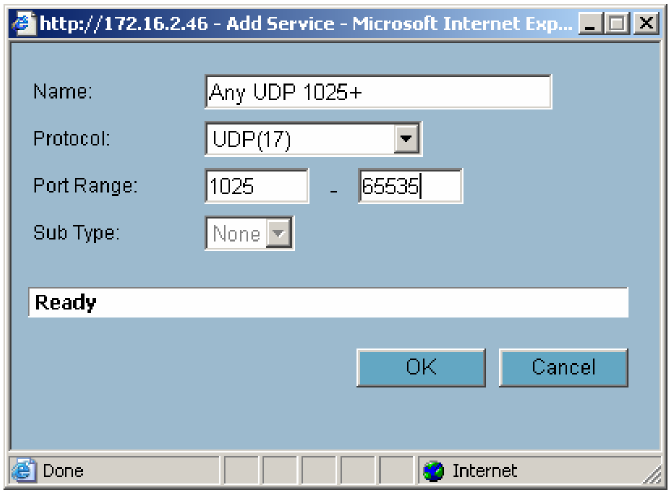
View Style: ○ All Services ● Custom Services ○ Default Services

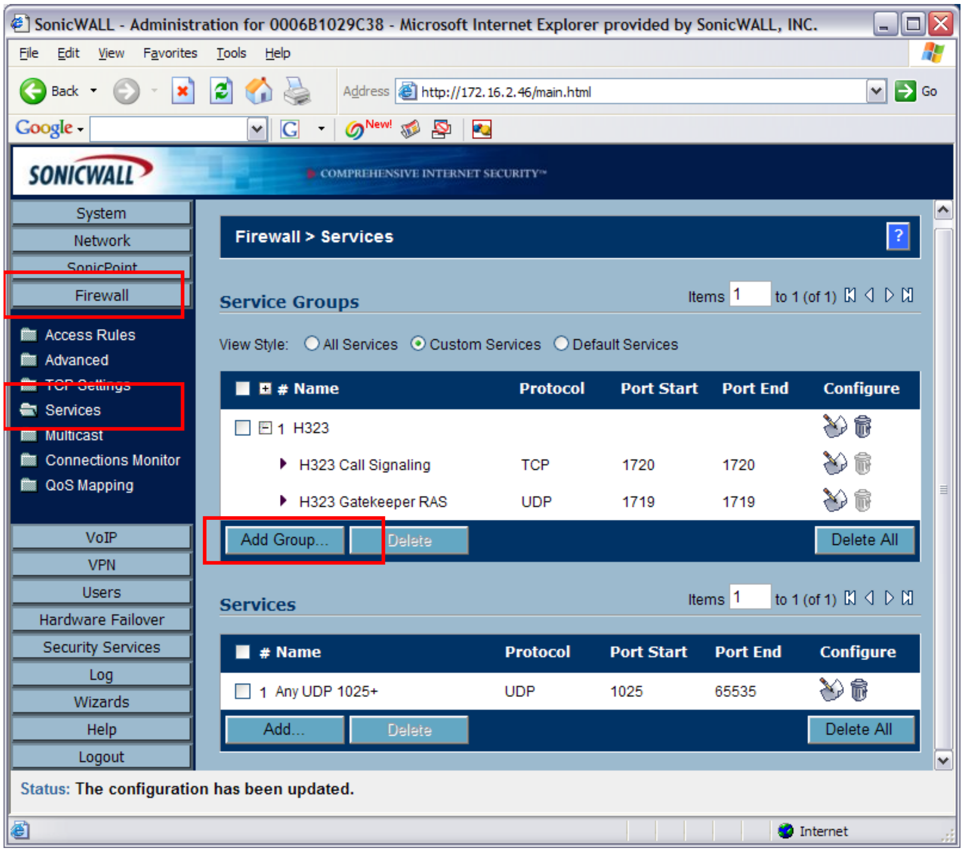
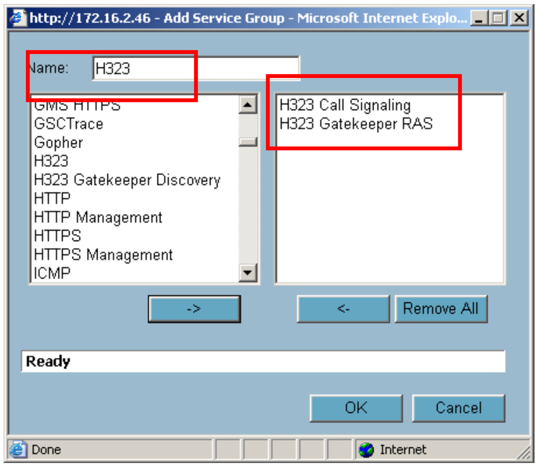
☐ ⊞ # Name	Protocol	Port Start	Port End	Configure
☐ ⊟ 1 H323				
H323 Call Signaling	TCP	1720	1720	
H323 Gatekeeper RAS	UDP	1719	1719	

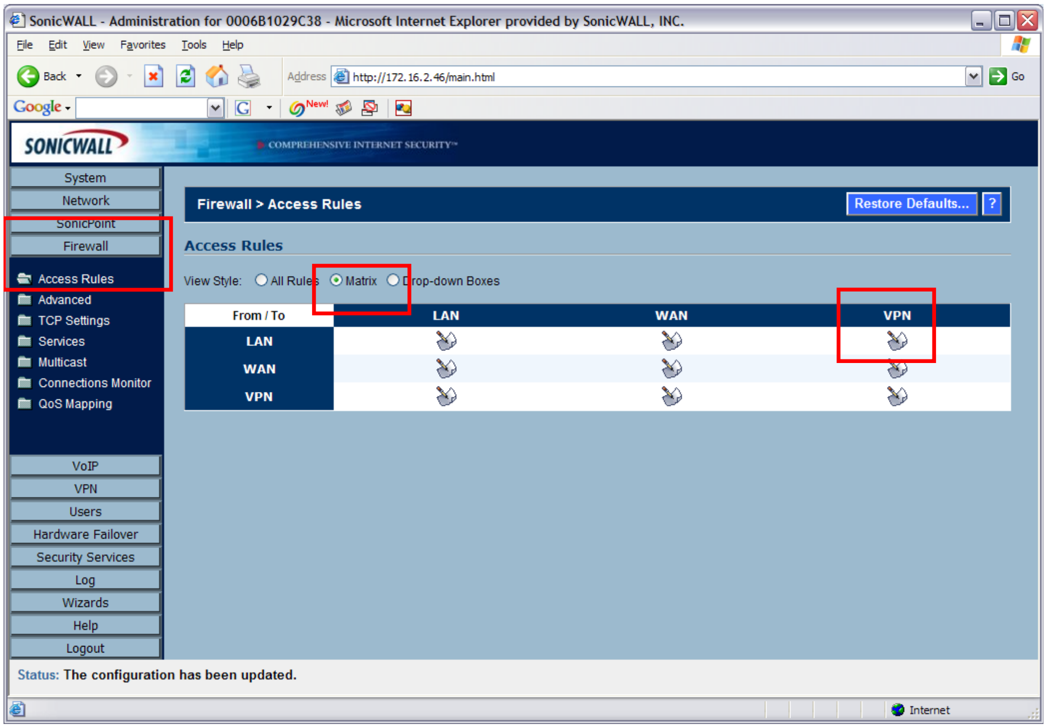
Services Items 1 to 1 (of 1)

☐ # Name	Protocol	Port Start	Port End	Configure
☐ 1 Any UDP 1025+	UDP	1025	65535	

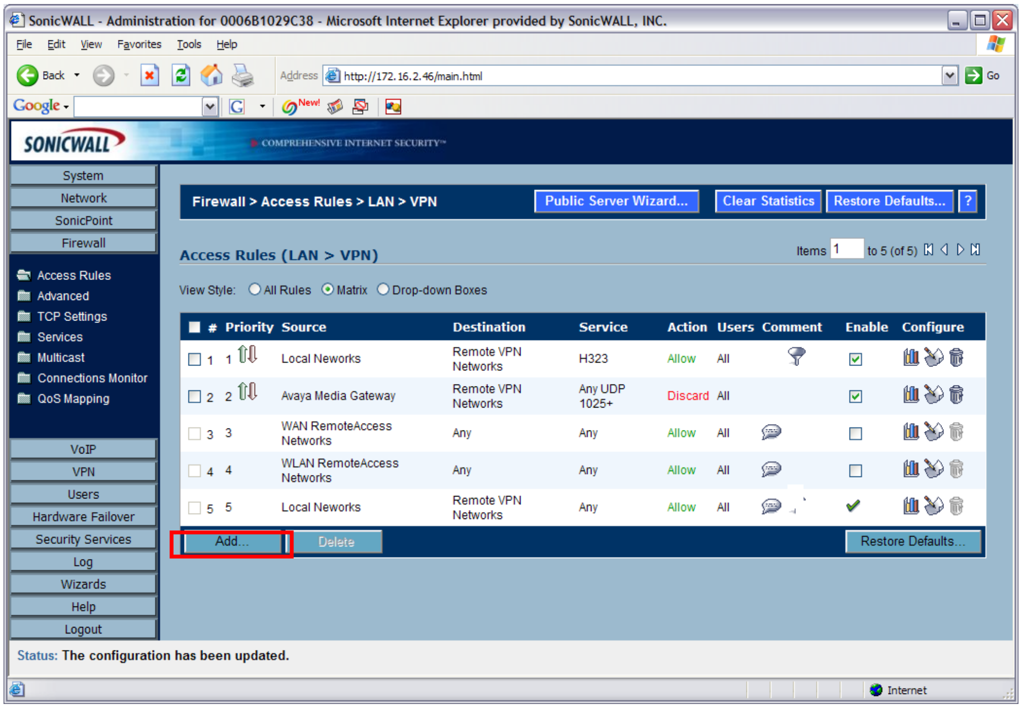
Status: The configuration has been updated.

Step	Description
4.	Enter the following information for the new Firewall service. **Name:** Any UDP 1025+ (a descriptive name for the Firewall service) **Protocol:** UDP(17) **Port Range:** 1025 - 65535 This rule is designed to filter out all UDP traffic that has not been negotiated using the H.323. Click **OK** after entering all the information.  http://172.16.2.46 - Add Service - Microsoft Internet Exp... Name: Any UDP 1025+ Protocol: UDP(17) Port Range: 1025 - 65535 Sub Type: None Ready

Step	Description
5.	From the Firewall's Services display, click **Add Group** under the **Service Groups** panel to add a new Service Group.  SonicWALL - Administration for 0006B1029C38 - Microsoft Internet Explorer provided by SonicWALL, INC. Address: http://172.16.2.46/main.html Firewall > Services Service Groups — Items 1 to 1 (of 1) View Style: ○ All Services ● Custom Services ○ Default Services # Name / Protocol / Port Start / Port End / Configure 1 H323 H323 Call Signaling / TCP / 1720 / 1720 H323 Gatekeeper RAS / UDP / 1719 / 1719 Services — Items 1 to 1 (of 1) # Name / Protocol / Port Start / Port End / Configure 1 Any UDP 1025+ / UDP / 1025 / 65535 Status: The configuration has been updated.
6.	At the **Add Service Group** pop-up window, enter a name for the new Service Group. The sample network used the name ***H323***. Highlight **H323 Call Signaling** and **H323 Gatekeeper RAS** from the left, and then click **->** to move the selected Services to the right panel. Click **OK** to complete.  http://172.16.2.46 - Add Service Group - Microsoft Internet Explo... Name: H323 GMS HTTPS GSCTrace Gopher H323 H323 Gatekeeper Discovery HTTP HTTP Management HTTPS HTTPS Management ICMP H323 Call Signaling H323 Gatekeeper RAS Ready

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>**7.**</td><td>Select **Access Rules** under the **Firewall** tab on the left to configure the Firewall’s rules. Select **Matrix** to better display all the selections. There are two sides of the firewall that need to be configured. One is LAN to VPN and the other is VPN to LAN. Select the icon in the first row and third column to configure the LAN to VPN Access rule.


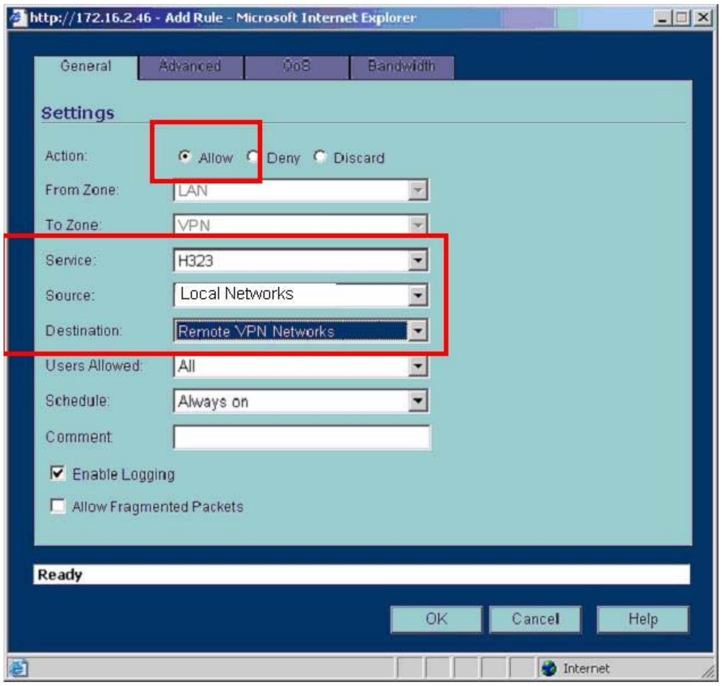
http://172.16.2.46/main.html
Firewall > Access Rules
Access Rules
View Style: ○ All Rules ● Matrix ○ Drop-down Boxes
<table>
<tr><th>From / To</th><th>LAN</th><th>WAN</th><th>VPN</th></tr>
<tr><td>LAN</td><td></td><td></td><td></td></tr>
<tr><td>WAN</td><td></td><td></td><td></td></tr>
<tr><td>VPN</td><td></td><td></td><td></td></tr>
</table>
Status: The configuration has been updated.</td></tr>
</table>

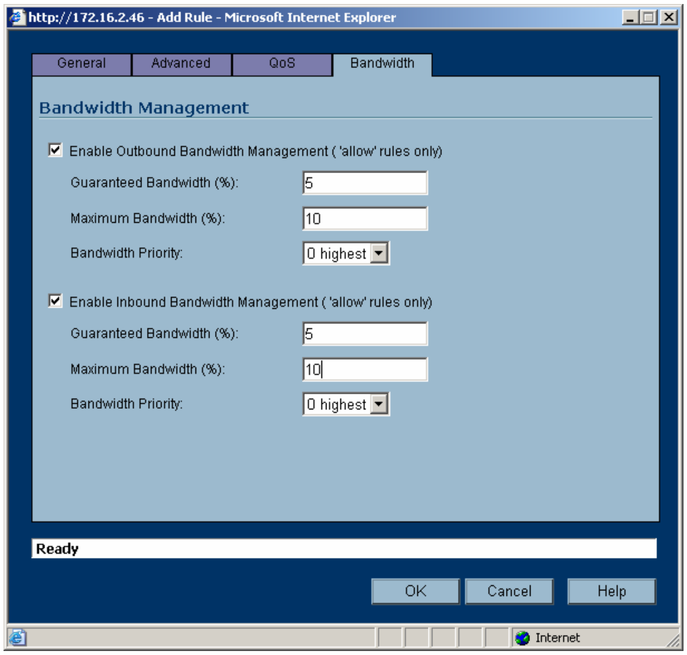
Step	Description
8.	Click on **Add** under the **Firewall > Access Rules > LAN > VPN** panel to add a new Access Rule. 

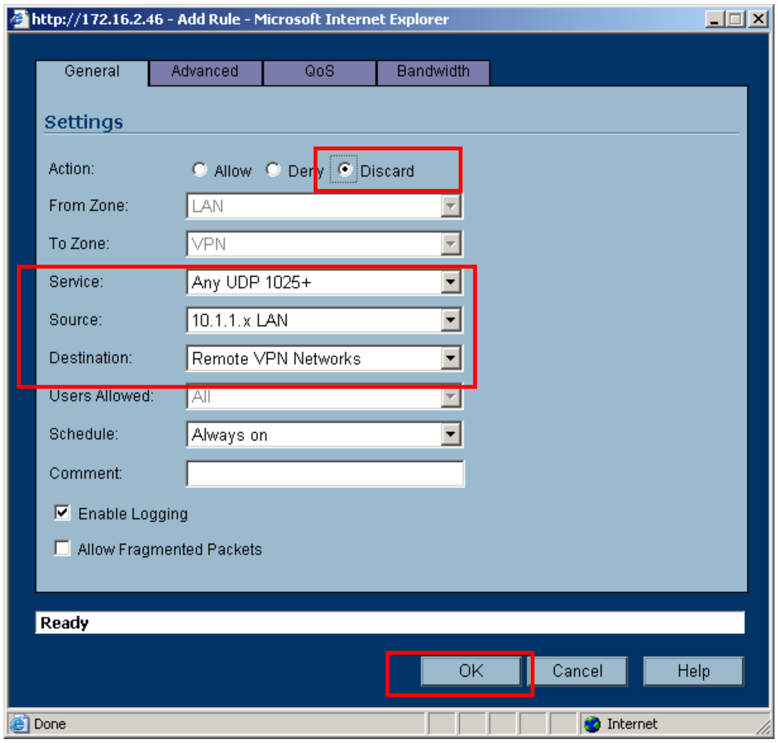
View Style: ○ All Rules ● Matrix ○ Drop-down Boxes

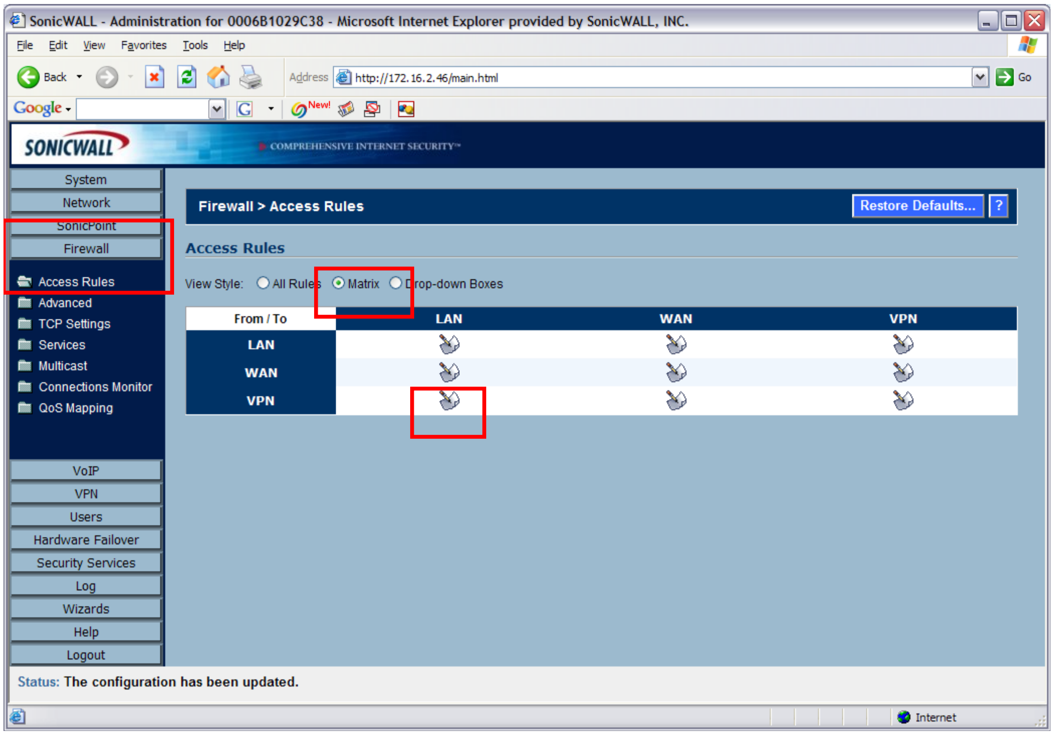
☐	#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
☐	1	1	Local Neworks	Remote VPN Networks	H323	Allow	All		☑	
☐	2	2	Avaya Media Gateway	Remote VPN Networks	Any UDP 1025+	Discard	All		☑	
☐	3	3	WAN RemoteAccess Networks	Any	Any	Allow	All		☐	
☐	4	4	WLAN RemoteAccess Networks	Any	Any	Allow	All		☐	
☐	5	5	Local Neworks	Remote VPN Networks	Any	Allow	All		✓	

Status: The configuration has been updated.

Step	Description
9.	Under the **General** tab of the **Add Rules** pop-up window, enter the following information: **Action:** *Allow* radio button selected **Service:** *H323* (defined in section 3.3 step 6) **Source:** *Local Networks* (defined in section 3.1 step 6) **Destination:** *Remote VPN Networks* (defined in section 3.1 step 7) Click on the **Bandwidth** tab to continue.  http://172.16.2.46 - Add Rule - Microsoft Internet Explorer General Advanced QoS Bandwidth Settings OK Cancel Help Internet Action: ● Allow ○ Deny ○ Discard From Zone: LAN To Zone: VPN Service: H323 Source: Local Networks Destination: Remote VPN Networks Users Allowed: All Schedule: Always on Comment: ☑ Enable Logging ☐ Allow Fragmented Packets Ready

Step	Description
10.	Under the **Bandwidth** tab, the bandwidth and priority are defined for the Outbound and Inbound traffic. The **H323** Access Rule in the sample network has defined the following: **Outbound Bandwidth Management** **Guaranteed Bandwidth (%):** ***5*** **Maximum Bandwidth (%):** ***10*** **Bandwidth Priority:** ***0 highest*** **Inbound Bandwidth Management** **Guaranteed Bandwidth (%):** ***5*** **Maximum Bandwidth (%):** ***10*** **Bandwidth Priority:** ***0 highest*** After entering all the information, click **OK** to complete. Note: The percentage is based on the WAN interface bandwidth defined in Section 3.3 Step 2, not the bandwidth of the VPN tunnel.  http://172.16.2.46 - Add Rule - Microsoft Internet Explorer Bandwidth Management ☑ Enable Outbound Bandwidth Management ('allow' rules only) Guaranteed Bandwidth (%): 5 Maximum Bandwidth (%): 10 Bandwidth Priority: 0 highest ☑ Enable Inbound Bandwidth Management ('allow' rules only) Guaranteed Bandwidth (%): 5 Maximum Bandwidth (%): 10 Bandwidth Priority: 0 highest Ready General Advanced QoS Bandwidth OK Cancel Help Internet

Step	Description
11.	Click **Add** again from the **Firewall > Access Rule > LAN > VPN** menu in Section 3.3 Step 6 to add another access rule. Under the General tab of the Access Rules pop-up window, enter the following information: **Action:** ***Discard*** radio button selected **Service:** ***Any UDP 1025 +*** (defined in section 3.3 step 2) **Source:** ***10.1.1.x LAN*** (defined in section 3.1 step 4) **Destination:** ***Remote VPN Networks*** (defined in section 3.1 step 7) This rule discards RTP traffic that has not been negotiated using H.323. Click on the **OK** tab to complete.  http://172.16.2.46 - Add Rule - Microsoft Internet Explorer General Advanced QoS Bandwidth Settings OK Cancel Help Done Internet Action: ○ Allow ○ Deny ● Discard From Zone: LAN To Zone: VPN Service: Any UDP 1025+ Source: 10.1.1.x LAN Destination: Remote VPN Networks Users Allowed: All Schedule: Always on Comment: ☑ Enable Logging ☐ Allow Fragmented Packets Ready
12.	After entering the “H323” and “Any UDP 1025 +” access rules, make sure the rules order is as displayed in Step 8 of this section. The “H323” must be before the “Any UDP 1025 +” Access Rule. If necessary, use the ⇅ icon to move the selected rule up or down to obtain the appropriate order.

Step	Description
13.	Now configure the VPN to LAN access Rule by selecting **Access Rules** under the **Firewall** tab on the left. Select **Matrix** to better display the selections. Select the icon in the third row and first column to configure the VPN to LAN access rule. 

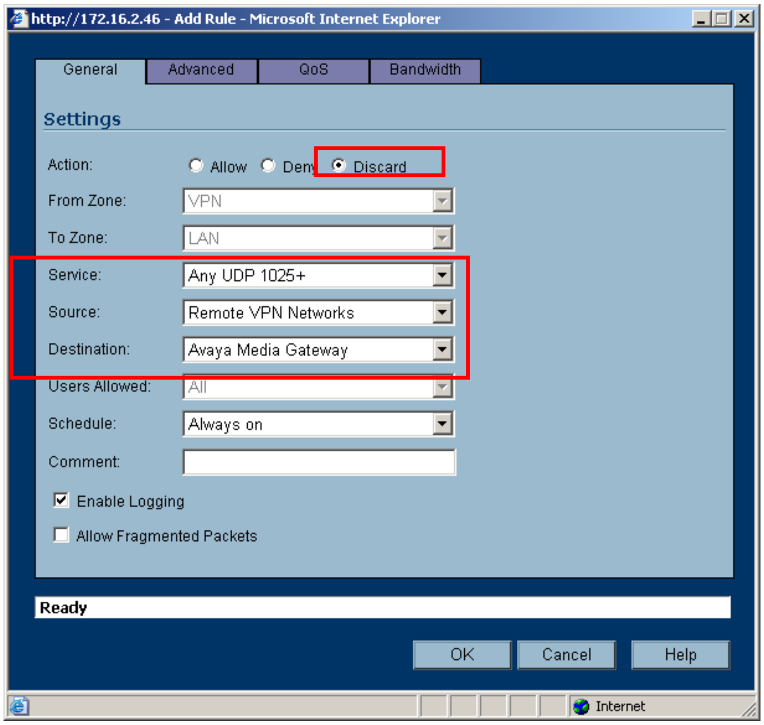
Firewall > Access Rules

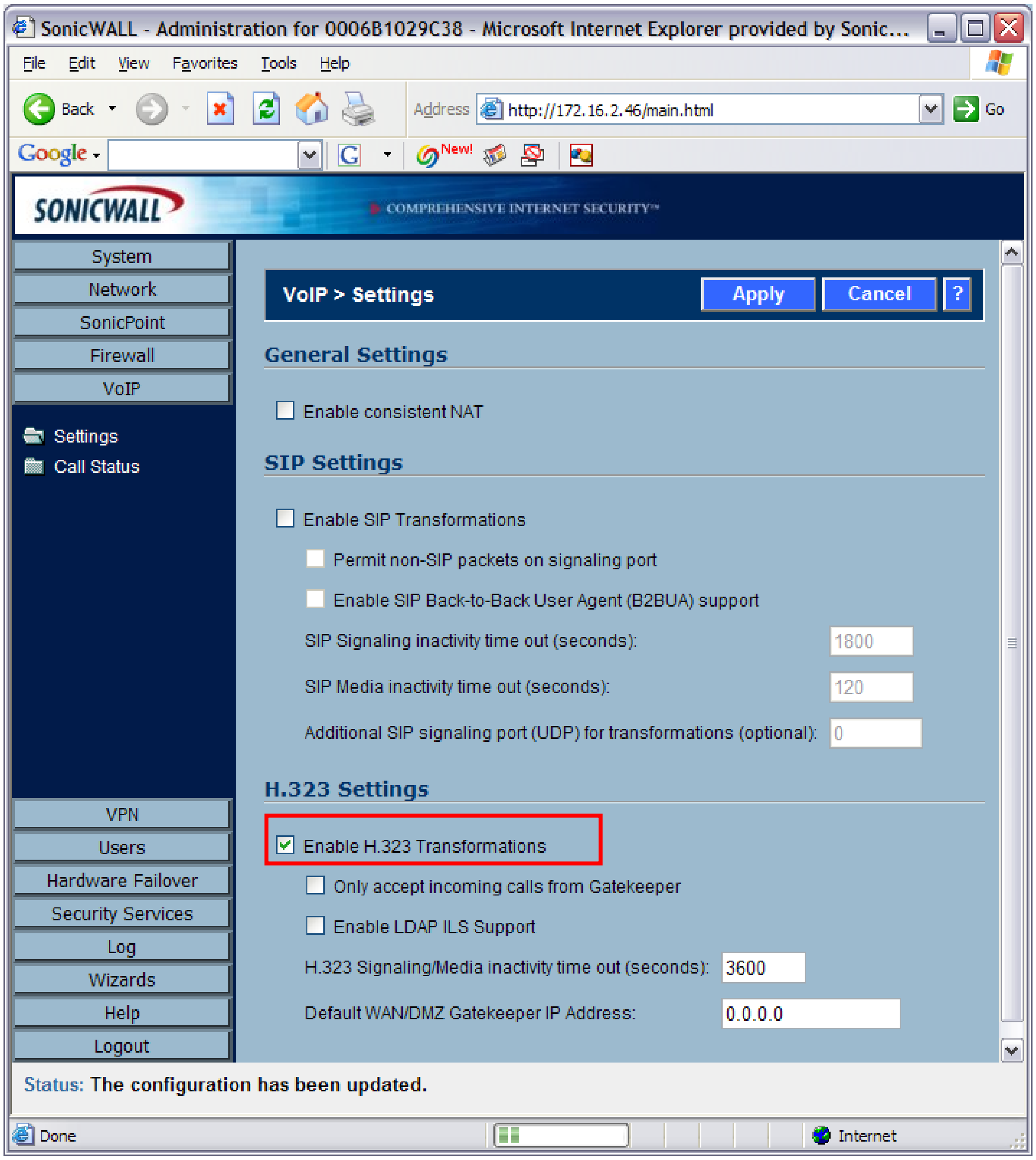
Access Rules

View Style: ○ All Rules ● Matrix ○ Drop-down Boxes

From / To	LAN	WAN	VPN
LAN	✎	✎	✎
WAN	✎	✎	✎
VPN	✎	✎	✎

Status: The configuration has been updated.

Step	Description
14.	Repeat Steps 8-13 in this Section to configure the same Access Rules for the VPN to LAN direction. Note: Make sure in Step 9 the **Source** is ***Remote VPN Networks*** and the **Destination** is ***Avaya Media Gateway*** as shown below.  http://172.16.2.46 - Add Rule - Microsoft Internet Explorer General Advanced QoS Bandwidth Settings Ready OK Cancel Help Internet Action: ○ Allow ○ Deny ● Discard From Zone: VPN To Zone: LAN Service: Any UDP 1025+ Source: Remote VPN Networks Destination: Avaya Media Gateway Users Allowed: All Schedule: Always on Comment: ☑ Enable Logging ☐ Allow Fragmented Packets

Step	Description
15.	Select **Settings** under the **VoIP** tab on the left. ***Check*** the **Enable H.323 Transformations** field. Click **Apply** to complete. 

SonicWALL - Administration for 0006B1029C38 - Microsoft Internet Explorer provided by Sonic...
File Edit View Favorites Tools Help
Back
Address http://172.16.2.46/main.html
Go
Google
New!
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
SonicPoint
Firewall
VoIP
Settings
Call Status
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Done
Internet

VoIP > Settings

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

☐ Only accept incoming calls from Gatekeeper

☐ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 3600

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

Status: The configuration has been updated.

4. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the SonicWALL PRO 4060 and TZ170 to establish a VPN tunnel that would support an infrastructure consisting of Avaya Communication Manager, and Avaya 46xx IP telephones while providing guaranteed bandwidth management for Avaya VoIP traffic.

4.1. General Test Approach

The general test approach was to verify that the Avaya IP telephones could successfully place and receive calls through the network as shown in **Figure 1** while competing with simulated non-VoIP low priority traffic. In addition, network traffic to Branch Site B was Network Address Translated to that of the IP address of the SonicWALL PRO 4060 WAN interface.

The main objectives were to verify:

- SonicWALL UTM devices can automatically allow RTP traffic streams based on H.323 signaling.
- Calls between telephones at the different locations were successfully completed and maintained with good voice quality.
- Multiple telephone calls between sites could be completed as per the desired bandwidth configured in the SonicWALL UTM devices.
- Non-VoIP traffic did not encroach upon the bandwidth reserved for the voice application.
- The solution supports G.711 and G.729 codecs.
- The solution supports DTMF.
- Preservation of Layer-3 DiffServ information.
- Network Address Translation (NAT) was implemented between the Main Site and Branch Site B.

4.2. Test Results

The objectives were successfully verified during compliance testing. Multiple telephone calls were successfully placed and received as per the bandwidth policy defined by the SonicWall UTM devices during varying levels of simulated competing traffic. Voice quality was good throughout testing regardless of traffic flow. DTMF was verified via access to the Meet-me Conference configured the Avaya Communication Manager.

5. Verification Steps

The following steps may be used to verify the configuration:

- Make sure all the SonicWALL UTM devices interfaces are reachable.
- Place and receive call from the Avaya telephones.
- From the SonicWALL UTM devices, verify the status of the VPN Link.
- From the SonicWALL UTM devices, verify the Access Rules are configured correctly by placing the mouse pointer over the bar chart icon in Step 8 Section 3.3. A pop-up window will display the packet count and byte processed by the Access Rule.

6. Support

For technical support on the SonicWALL UTM, contact SonicWALL, Inc. at http://www.sonicwall.com/support/contact.html

North America	1-888-777-1476

7. Conclusion

These Application Notes have described the administration steps required to configure the SonicWALL UTM devices to interoperate with and prioritize WAN bandwidth for Avaya IP H.323 phone traffic. During compliance testing, H.323 phone calls traversing the WAN link were successfully established and maintained while sharing the link with non-VoIP traffic.

8. Additional References

[1] *Administrator Guide for Avaya Communication Manager, Doc # 03-300509*, Issue 1, June 2005
[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005 Release 3.0
[3] *SonicOS Enhanced 3.0 Administrator's Guide*

Product documentation for Avaya products may be found at http://support.avaya.com

Product documentation for SonicWALL products may be found at http://www.sonicwall.com

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.