



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring a SonicWALL VPN solution with an Avaya IP Telephony Infrastructure using Avaya IP Office in a Converged VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe the configuration of a Multi-Site Voice over IP (VoIP) and data network solution using SonicWALL UTM Firewalls with an Avaya Telephony Infrastructure using Avaya IP Office. Emphasis was placed on verifying the prioritization of VoIP traffic and voice quality in a Multi-Site converged VoIP and Data network scenario.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration of a Voice over IP (VoIP) solution using SonicWALL UTM Firewalls appliances with an Avaya Telephony Infrastructure consisting of Avaya IP Office, Avaya VoiceMail Pro and Avaya IP telephones. Compliance testing emphasis was placed on validating that VoIP traffic and voice features, e.g., voicemail, conferencing, worked properly through the SonicWALL firewall VPNs.

1.1. Interoperability Compliance Testing

The interoperability compliance test covered feature functionality, serviceability, and performance testing. The emphasis in the compliance test was placed on validating that VoIP traffic and voice features, e.g., voicemail, conferencing, worked properly through the SonicWALL UTM Firewalls.

The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call park, call pick-up, bridged call appearances, voicemail using Avaya VoiceMail Pro, Message Waiting Indicator (MWI), and hold and return from hold.

Serviceability testing was conducted to verify the ability of the Avaya/SonicWALL VoIP solution to recover from adverse conditions, such as power cycling network devices and disconnecting cables between the LAN interfaces. In all cases, the ability to recover after the network normalized from failures was verified.

1.2. Support

Technical Support: <http://www.sonicwall.com/us/Support.html>

2. Reference Configuration

The configuration in **Figure 1** shows a converged VoIP and data network with multiple remote sites. The extension numbers beginning with the number 30 are registered with Avaya IP Office in the Company Headquarters and extension numbers beginning with the number 31 are registered with the Remote Site B Avaya IP Office. For compliance testing, the voice and data traffic were separated onto different VLANs.

2.1. Corporate Headquarters

The Corporate Headquarters consisted of one SonicWall NSA E5500, one router, one Avaya IP Office IP500, two Avaya IP Telephones, one Avaya digital phone, one PC on Datavlan1 running Avaya IP Office Manager and Avaya IP Office Phone Manager Pro and a corporate DHCP/TFTP/HTTP server. The Corporate Headquarters provided a DHCP/File server for assigning IP network parameters and to download settings to the Avaya IP telephones. The Avaya IP telephones register to the Corporate Headquarters Avaya IP Office. An IP Line with small community network (SCN) was enabled to allow for direct dialing between the Corporate Headquarters and Remote Site A to Remote Site B.

2.2. Remote Site A

Remote Site A consisted of one SonicWall NSA 240, one router, two Avaya IP Telephones, one PC on Datavlan2 and one laptop on Datavlan2 running Avaya PhoneManager Softphone. The Avaya IP telephones register to company headquarters Avaya IP Office IP500.

2.3. Remote Site B

Remote Site B consisted of one SonicWall NSA 240, one router, one Avaya IP Office IP406V2, one Avaya 2410 Digital Telephone, two Avaya IP Telephones, one PC on Datavlan3 and one laptop on Datavlan3 running Avaya PhoneManager Softphone. The Avaya IP telephones register to the Remote Site B Avaya IP Office. An IP Line with small community network (SCN) was enabled to allow for direct dialing between the Corporate Headquarters and Remote Site A to Remote Site B.

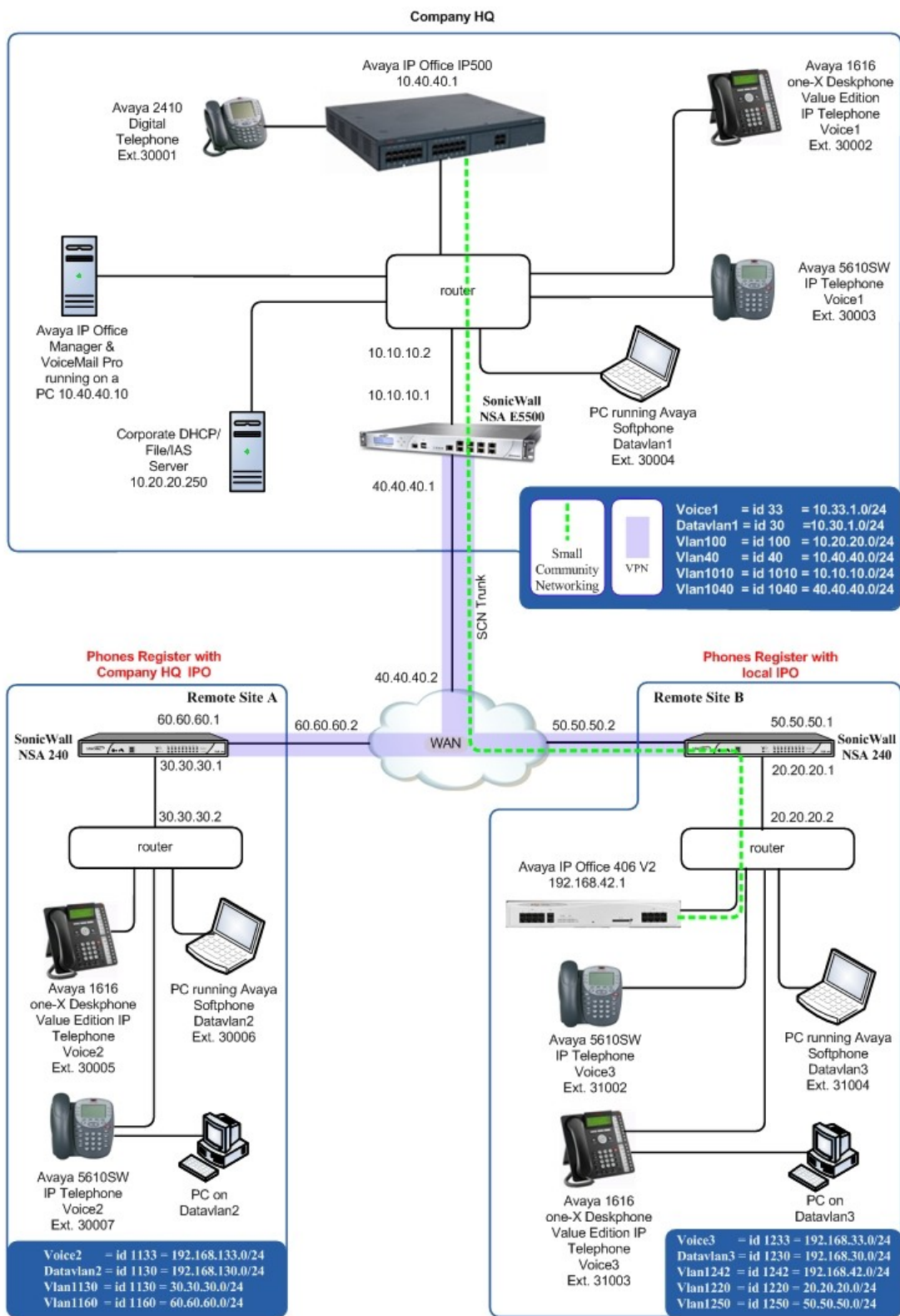


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
Avaya IP Office IP500	4.2 (17)
Avaya IP Office IP406V2	4.2 (17)
Avaya IP Office Manager (running on HP Proliant Server)	6.2 (17)
Avaya Messaging (Voice Mail) Products	
Avaya VoiceMail Pro (running on HP Proliant Server)	4.2 (30)
Avaya Telephony Sets	
Avaya 1600 Series IP Telephones	Avaya one-X Deskphone Value Edition 1.020
Avaya 5600 Series IP Telephones	8.016
Avaya 2410 Digital Telephone	5.0
SonicWALL Products	
SonicWall NSA E5500	5.2.0.1-21o
SonicWall NSA 240	5.2.0.1-21o
MS Products	
PC	Microsoft Windows 2003 Server (Running Avaya IP Office Manager and Avaya IP Office Phone Manager Pro and file/DHCP Services

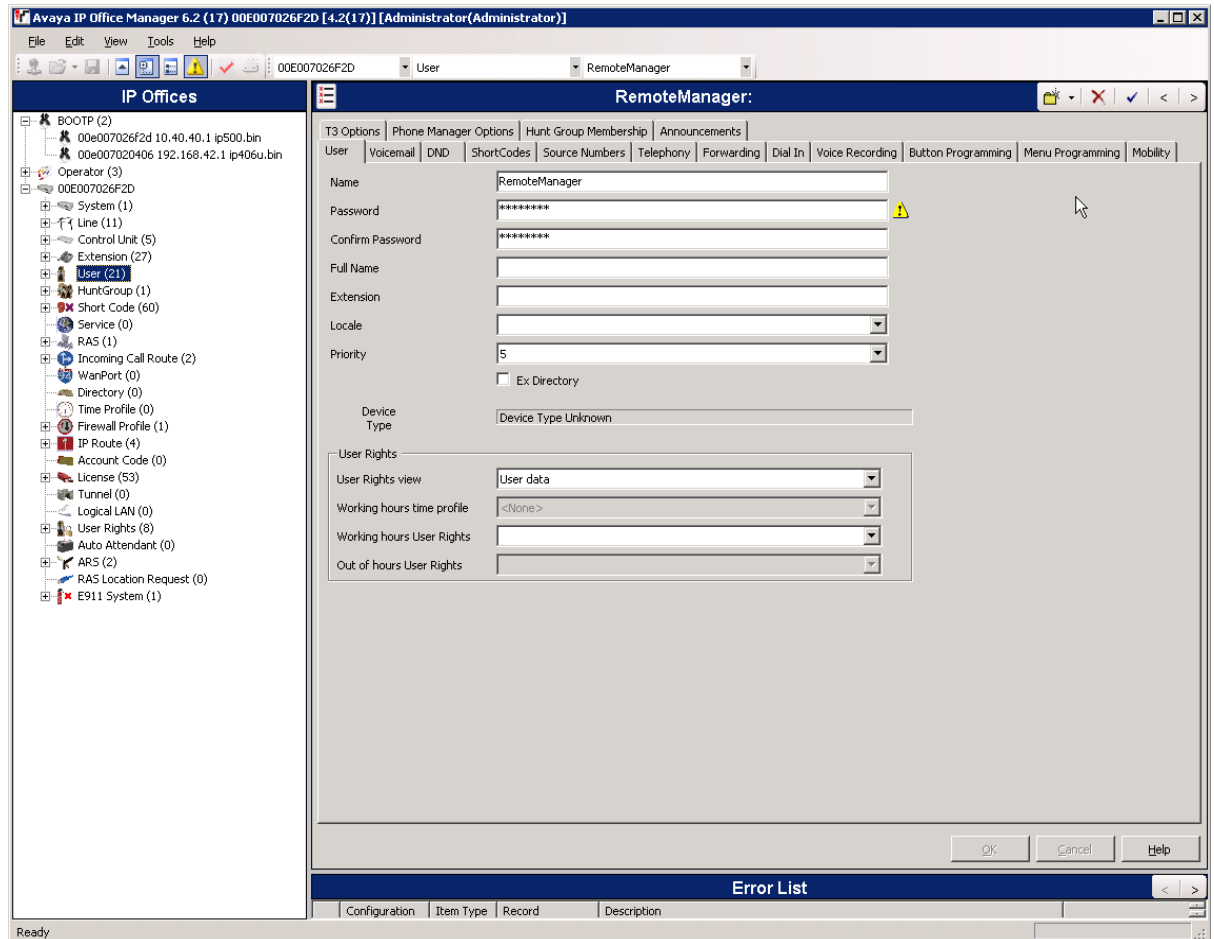
4. Avaya IP Office

This section was included to verify that Avaya IP Office was configured correctly. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage, extensions, and voice mail, please refer to the Avaya IP Office product documentation in **Section 9 [1]**.

4.1. Configure & Verify Avaya IP Office Settings

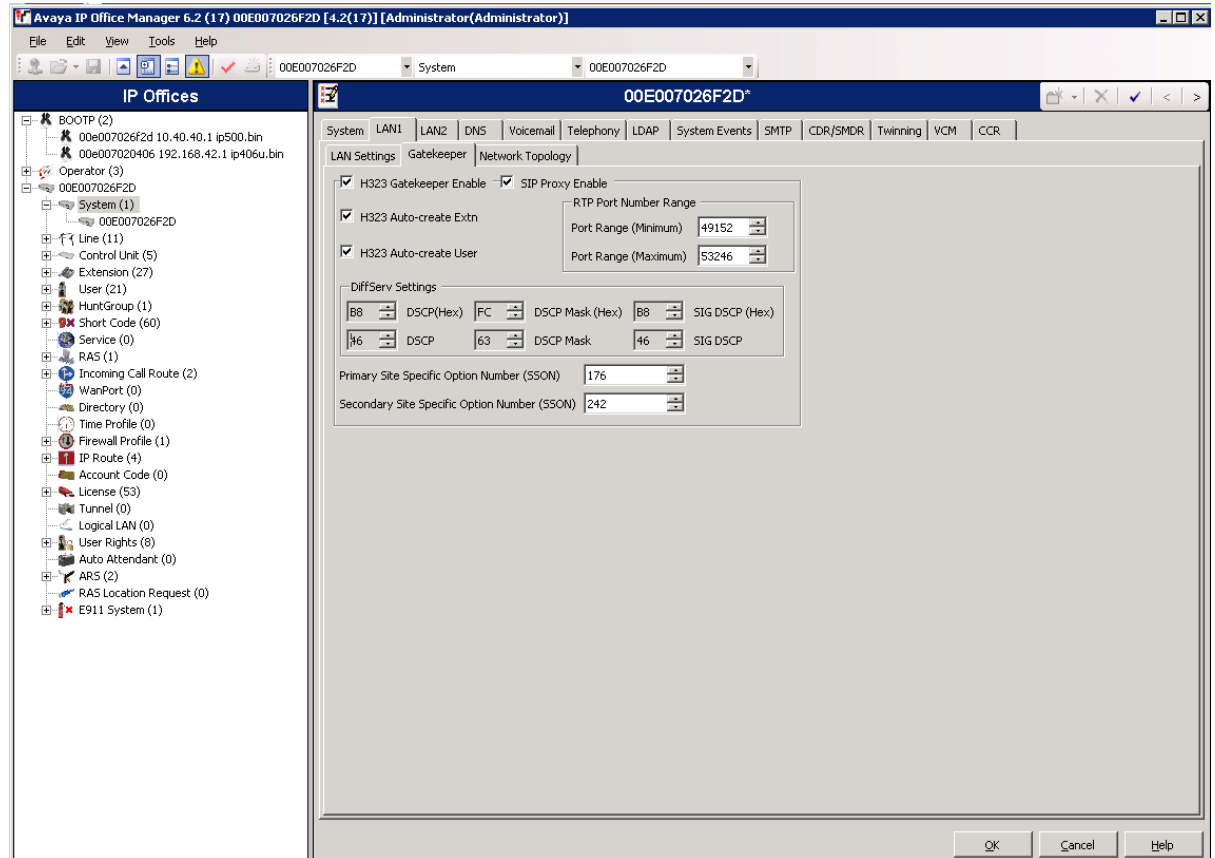
Step	Description
1.	Avaya IP Office is configured via the Avaya IP Office Manager program. Log into the Avaya IP Office Manager PC and select Start → Programs → IP Office → Manager to launch the Avaya IP Office Manager application. Select File → Open to search for IP Offices in the network. Click on the appropriate Avaya IP Office. Click OK to continue. Log into the Avaya IP Office Manager application using the appropriate credentials.

2. From the IP Office Manager window.
The main IP Office Manager window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **IP Offices**.


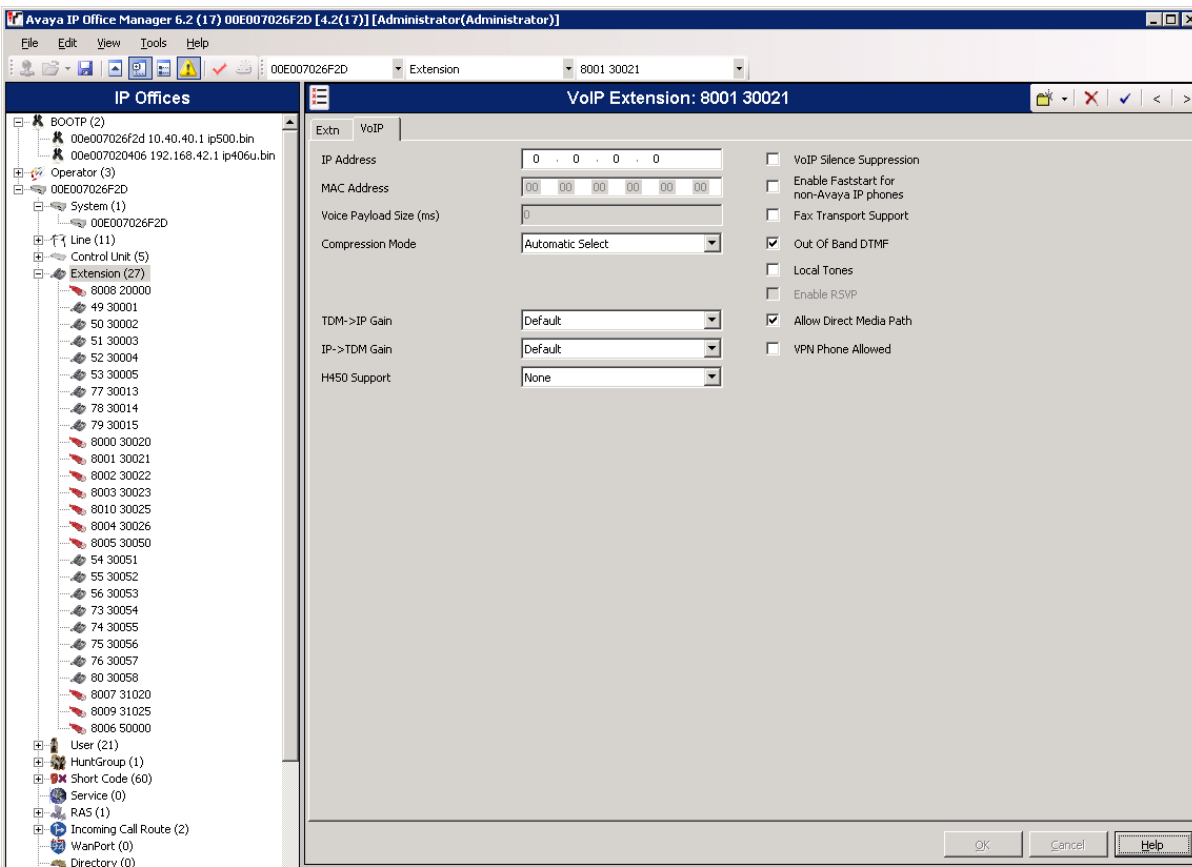


3. Verify H323 Gatekeeper information.

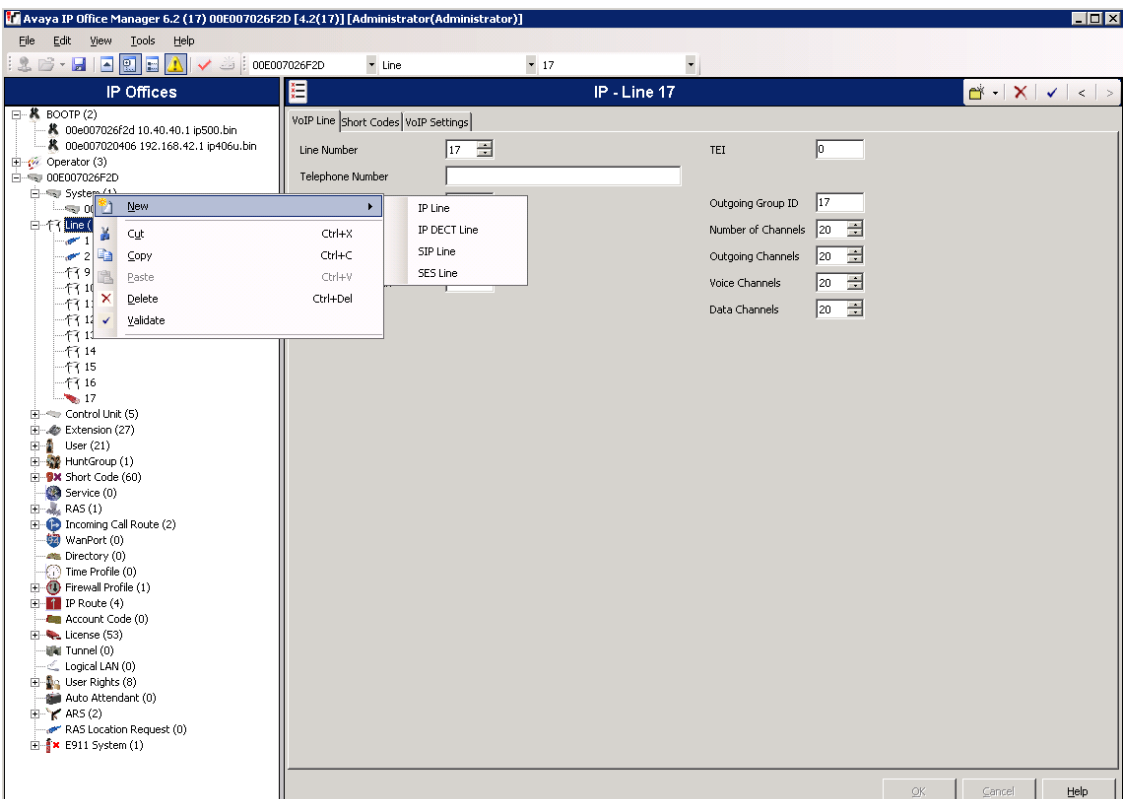
The Avaya IP Telephones will get Differentiated Services information from the Avaya IP Office. In the Manager window, go to the Configuration Tree and click **System** → **LAN1** → **Gatekeeper**. Verify that the **DiffServ Settings** for **DSCP** and **SIG DSCP** are set to **46** and **46**, respectively.



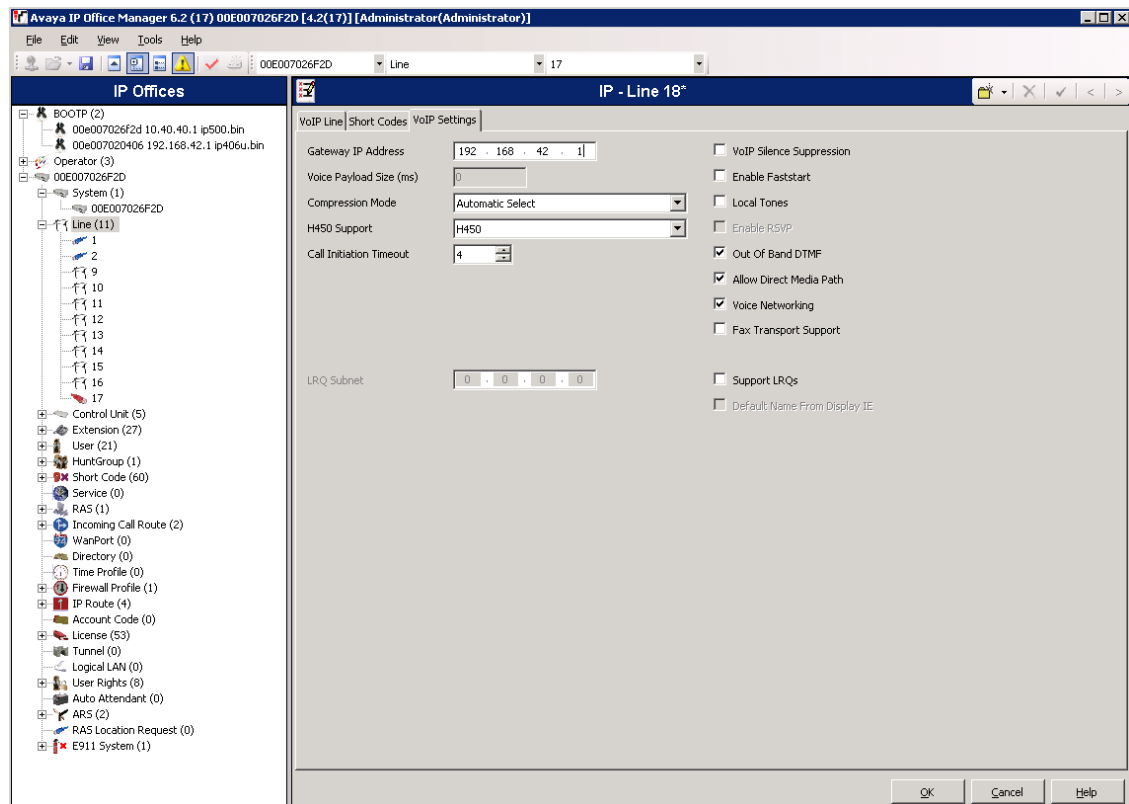
4. Disable DHCP server on Avaya IP Office. Click **System LAN1 → LAN Settings**. Set the **DHCP Mode** to **Disabled**. Click **OK** to continue.

Step	Description
5.	<p>Verify Direct Media Path.</p> <p>From the Configuration Tree, select Extension. Click on the IP telephone extension, Select the VoIP tab. Verify that Allow Direct Media Path is checked. Click OK to continue. The changes must be saved before they will take effect, click to the  icon to save the configuration.</p> 
6.	Repeat Section 4 Steps 1 thru 5 for the Remote Site B IP Office.

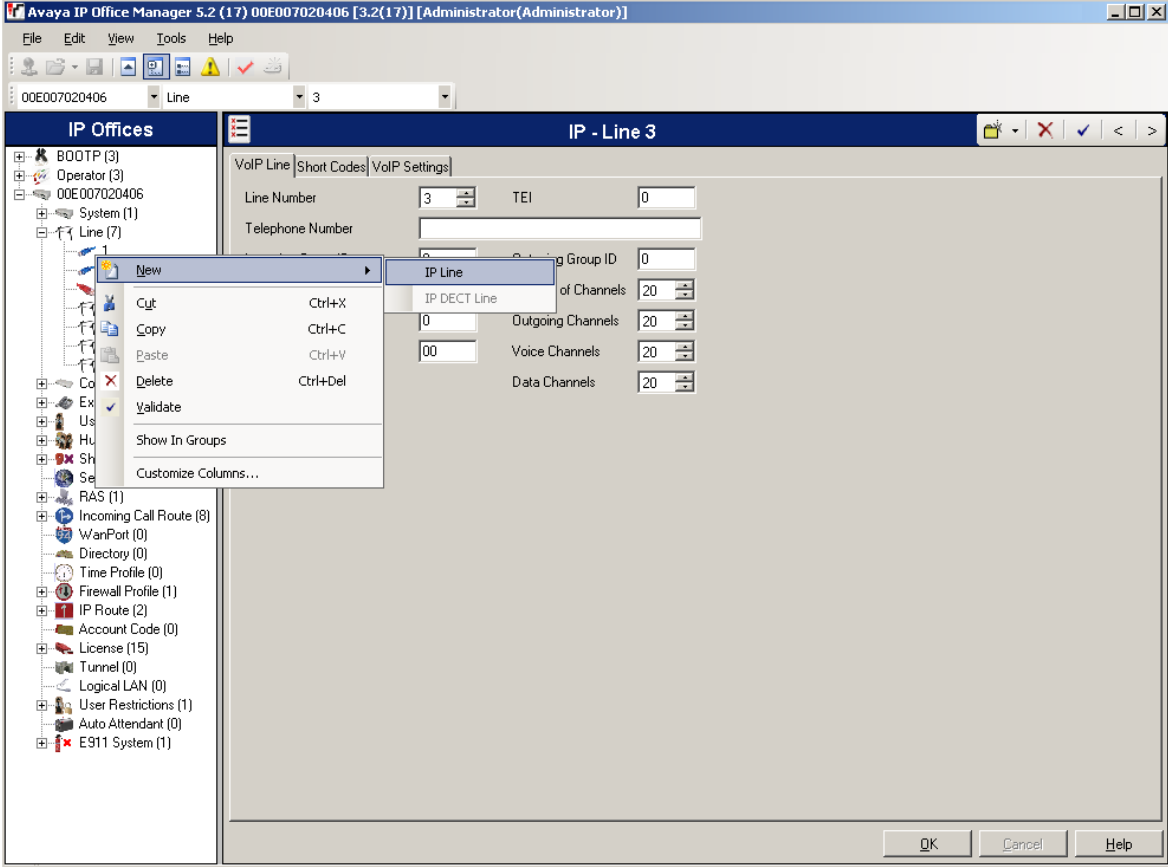
4.2. Avaya IP Office Settings Corporate Headquarters IP Office

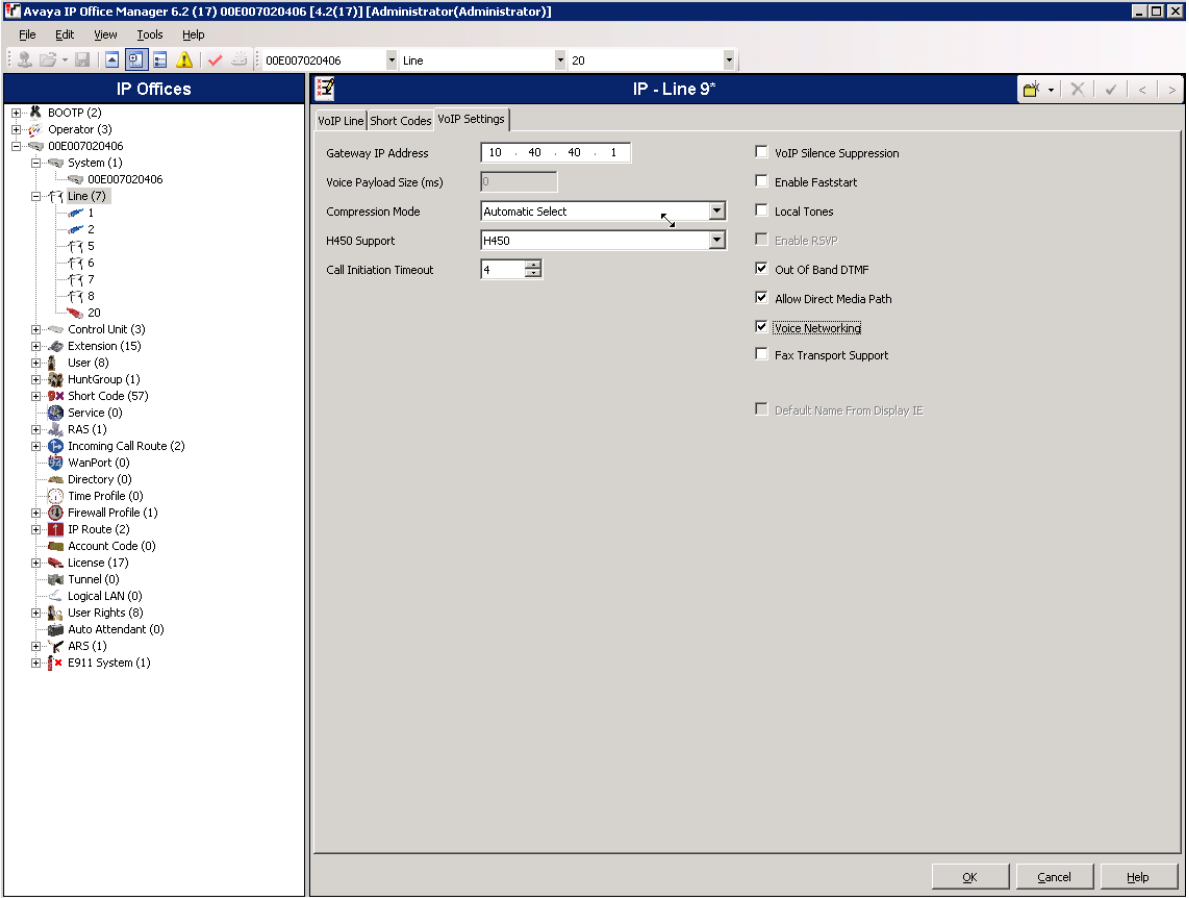
Step	Description
1.	Log into the Avaya IP Office Manager PC and select Start → Programs → IP Office → Manager . Select File → Open to search for the Campus A IP Office. Click OK to continue Log into the Avaya IP Office Manager application using the appropriate credentials.
2.	<p>Create IP trunk to Campus B's Avaya IP Office.</p> <p>From the Configuration Tree, Right mouse click Line → New → IP Line.</p> 

3. Select the **VoIP Settings** tab, assign an IP address for the **Gateway IP Address** (address of the Remote Site B IP Office) and enable **Voice Networking**.




4.3. Avaya IP Office Settings Remote Site B

Step	Description
1.	Log into the Avaya IP Office Manager PC and select Start → Programs → IP Office → Manager . Select File → Open to search for the Remote Site B IP Office. Click OK to continue. Log into the Avaya IP Office Manager application using the appropriate credentials.
2.	<p>Create IP trunk to Campus A's Avaya IP Office</p> <p>From the Configuration Tree, Right mouse click Line → New → IP Line.</p> 

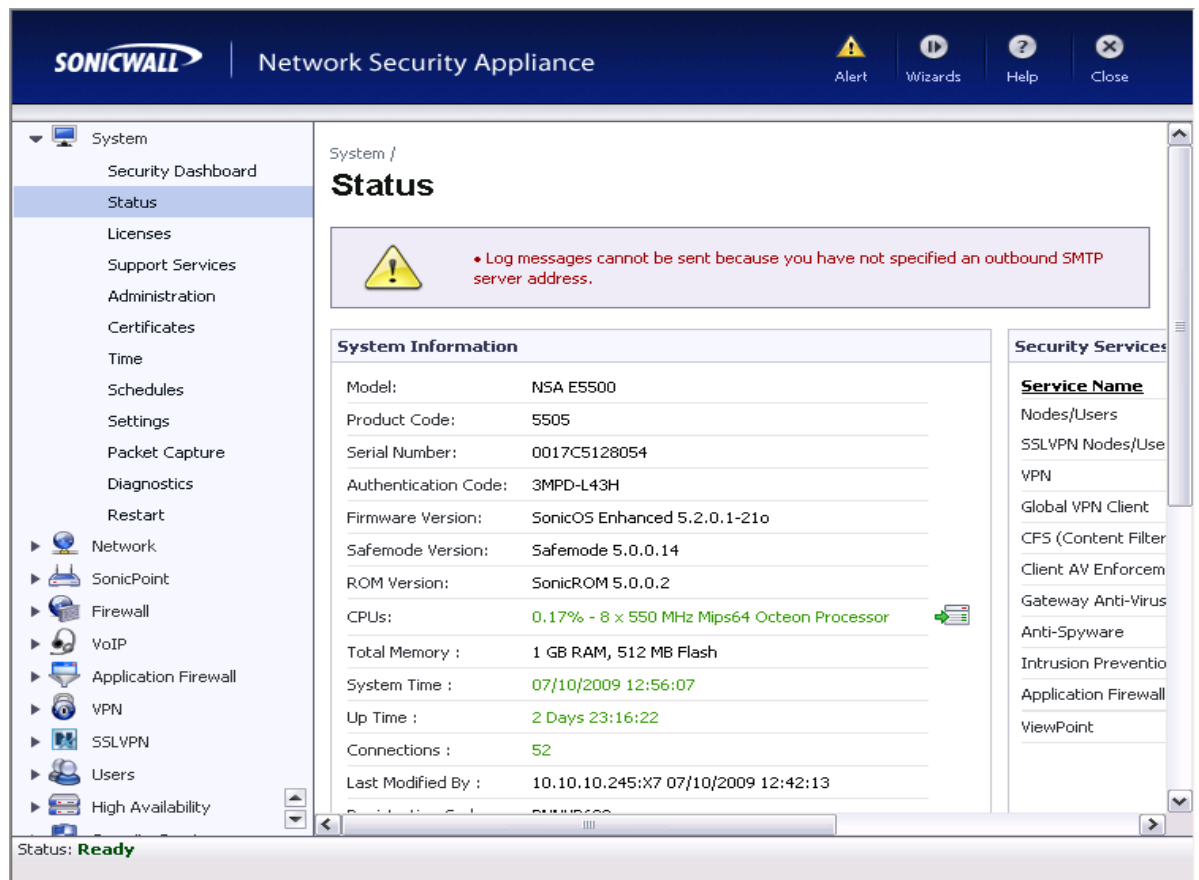
Step	Description
3.	<p>Select the VoIP Settings tab, assign an IP address for the Gateway IP Address (address of the Campus A IP Office) and enable Voice Networking.</p>  <p>The screenshot shows the Avaya IP Office Manager 6.2 (17) 00E007020406 [4.2(17)] [Administrator/Administrator] interface. The left pane displays a tree view of the IP Office configuration, including BOOTP (2), Operator (3), System (1), Line (7), Control Unit (3), Extension (15), User (8), HuntGroup (1), Short Code (57), Service (0), RAS (1), Incoming Call Route (2), WanPort (0), Directory (0), Time Profile (0), Firewall Profile (1), IP Route (2), Account Code (0), License (17), Tunnel (0), Logical LAN (0), User Rights (8), Auto Attendant (0), ARS (1), and E911 System (1). The right pane shows the 'IP - Line 9' configuration window with the 'VoIP Settings' tab selected. The settings include: Gateway IP Address (10.40.40.1), Voice Payload Size (ms) (0), Compression Mode (Automatic Select), H450 Support (H450), Call Initiation Timeout (4), and various checkboxes for VoIP features. The 'Voice Networking' checkbox is checked, and the 'Default Name From Display IE' checkbox is unchecked. The bottom of the window has OK, Cancel, and Help buttons.</p>

5. Configure SonicWALL UTM Firewalls

5.1. Configure SonicWall NSA E5500 (Corporate Headquarters)


Step	Description
5.1.1.	<p>Configure the SonicWall NSA E5500 using the built-in web-based Management Tool. Access this tool by establishing a web browser connection to the SonicWall NSA E5500. Refer to Section 9 [6].</p> <p>Log into the NSA 5500.</p> <ol style="list-style-type: none">1. Connect the LAN port of the computer being used to the X0 (LAN) port on the SonicWall NSA E5500.2. Start the Management Tool as follows: Start your web browser and enter http://192.168.168.168 Press Enter.3. Log in to the SonicWall NSA E5500 using default credentials which can be obtained from the SonicWALL documentation. 

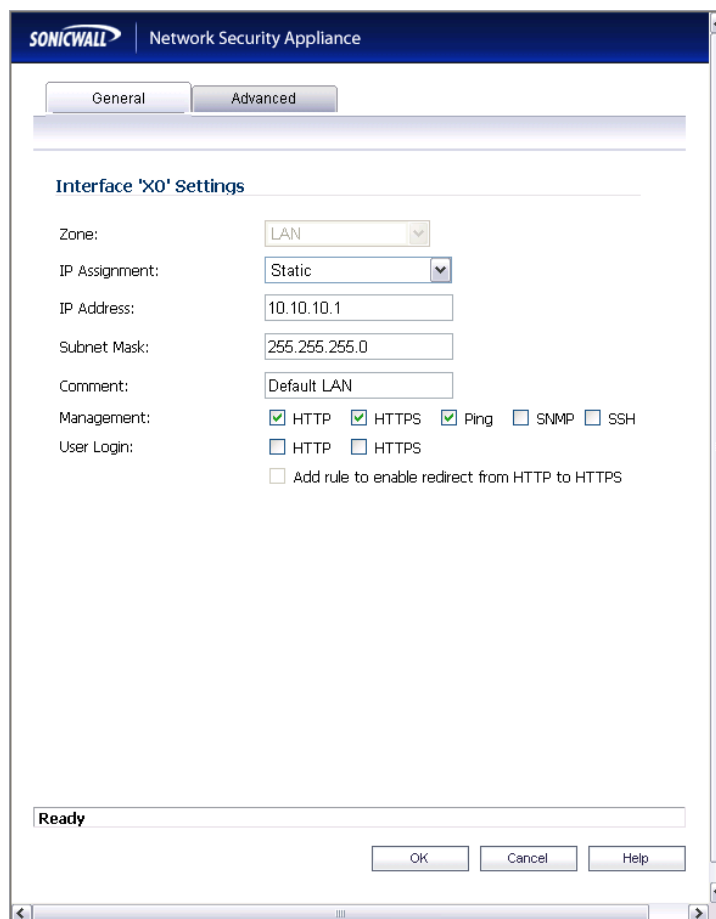
- 5.1.2. The main SonicWall NSA E5500 window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **System**.



5.2. Configure Interfaces:

5.2.1.

From the **Network → Interfaces**, click on the **Configure icon** , not shown, for **X0** (LAN) and enter the following information for: **IP Assignment**, **IP Address** and **Subnet Mask** for the network structure to be used. Click **OK** to continue.



The screenshot shows the 'Interface 'X0' Settings' dialog box in the SonicWall Network Security Appliance configuration interface. The 'General' tab is selected. The settings are as follows:

- Zone: LAN
- IP Assignment: Static
- IP Address: 10.10.10.1
- Subnet Mask: 255.255.255.0
- Comment: Default LAN
- Management: ☒ HTTP, ☒ HTTPS, ☒ Ping, ☐ SNMP, ☐ SSH
- User Login: ☐ HTTP, ☐ HTTPS
- ☐ Add rule to enable redirect from HTTP to HTTPS

The status bar at the bottom indicates 'Ready'. The dialog box has 'OK', 'Cancel', and 'Help' buttons.

5.2.2. Repeat for the **X1** (WAN) interface.

5.2.3. Once configuration on the interfaces is completed, the following summary is presented.

SONICWALL | Network Security Appliance

Alert Wizards Help Logout

System
Network
Interfaces
WAN Fallover & LB
Zones
DNS
Address Objects
Services
Routing
NAT Policies
ARP
DHCP Server
IP Helper
Web Proxy
Dynamic DNS
SonicPoint
Firewall
VoIP
Application Firewall
VPN
SSLVPN
Users
High Availability
Security Services
Log

Network /
Interfaces

Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	10.10.10.1	255.255.255.0	Static	1000 Mbps full-duplex	Default LAN	
X1	WAN	40.40.40.1	255.255.255.0	Static	1000 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		
X6	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X7	Unassigned	0.0.0.0	0.0.0.0	N/A	100 Mbps full-duplex		

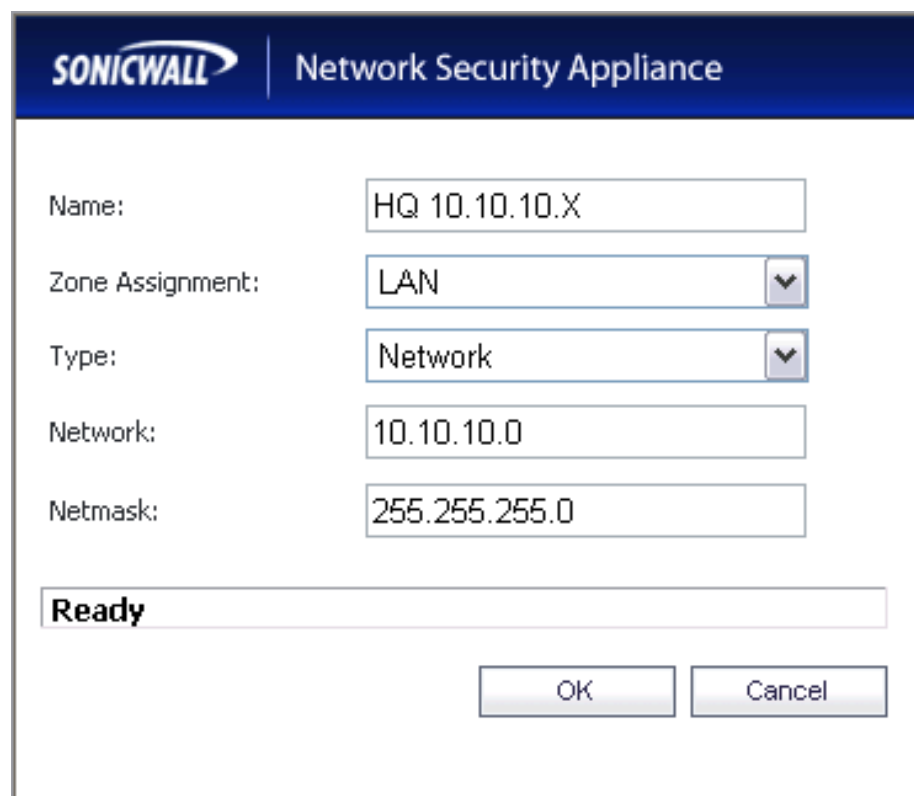
Interface Traffic Statistics

Traffic Statistics	X0	X1	X2	X3	X4	X5	X6	X7
Rx Unicast Packets	563	31	0	0	0	0	0	0
Rx Broadcast Packets	86	86	0	0	0	0	0	121
Rx Bytes	89420	15600	0	0	0	0	0	9085
Tx Unicast Packets	438	55	0	0	0	0	0	0
Tx Broadcast Packets	0	0	0	0	0	0	0	0
Tx Bytes	218306	6680	0	0	0	0	0	0

Status: The configuration has been updated.

5.3. Define networks

- 5.3.1.** Create Address Objects for each of the networks within the deployment sites. From the **Network → Address Objects**, click on the **Add** button and enter the following information for: **Name**, **Zone Assignment**, **Network**, and **Netmask** for each subnet in the topology. Click **OK** to continue.



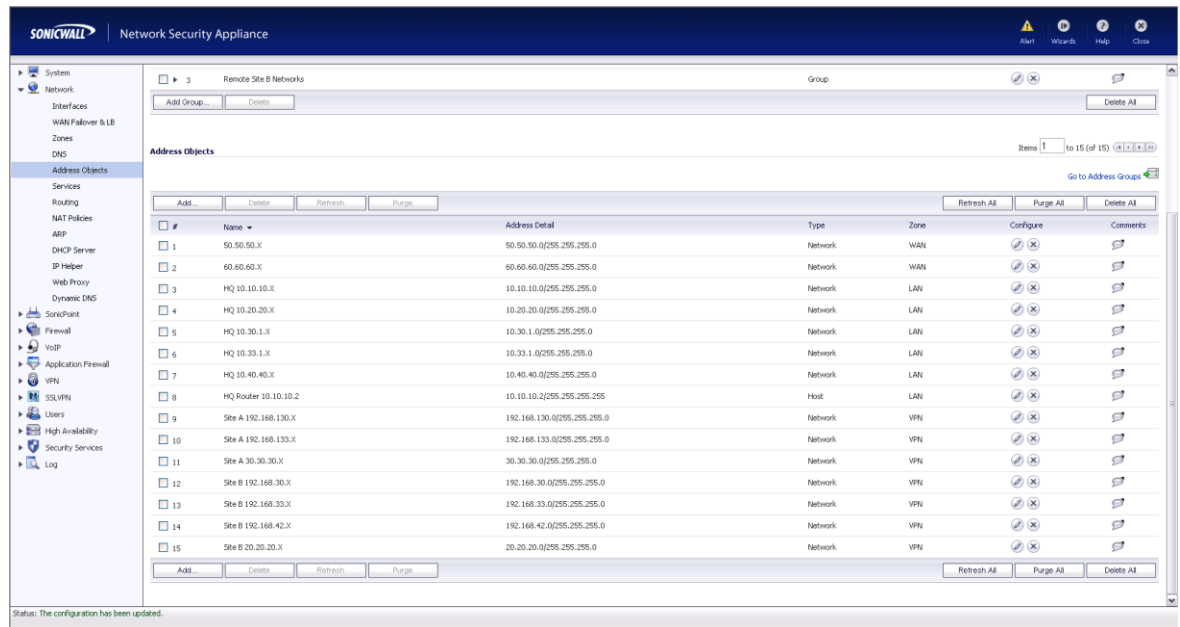
The screenshot shows the 'Add Address Object' dialog box in the SonicWall Network Security Appliance interface. The dialog has a title bar with the SonicWall logo and 'Network Security Appliance'. The fields are as follows:

Field	Value
Name:	HQ 10.10.10.X
Zone Assignment:	LAN
Type:	Network
Network:	10.10.10.0
Netmask:	255.255.255.0


At the bottom, there is a 'Ready' status bar and two buttons: 'OK' and 'Cancel'.

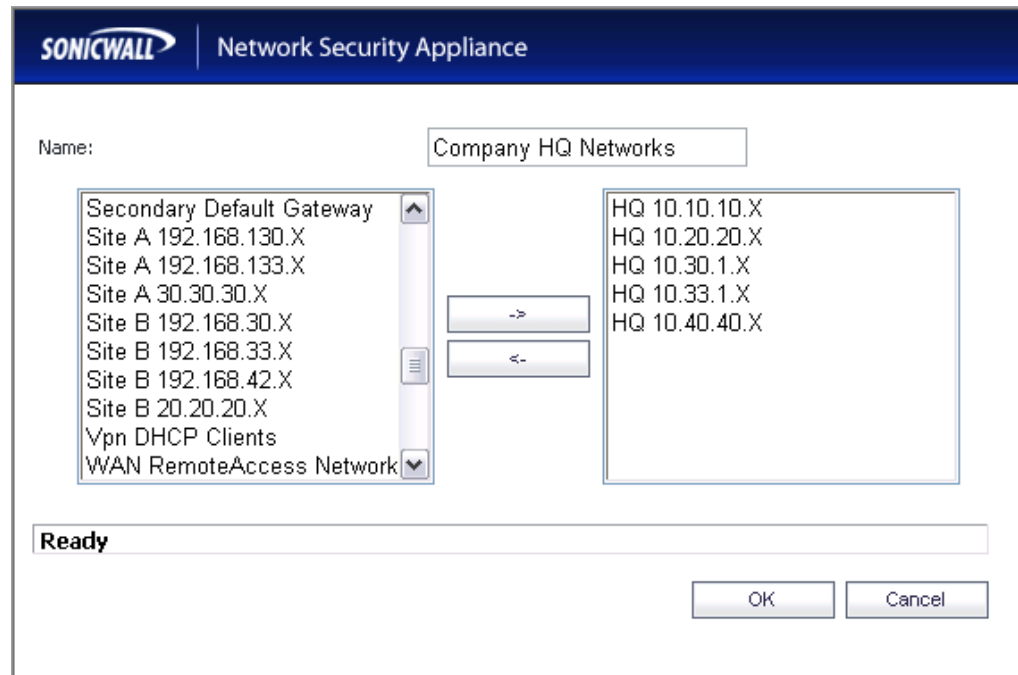
- 5.3.2.** Repeat Step 5.3.1 for each subnet in the topology. Refer to **Figure 1** for details of topology used for compliance testing.

5.3.3. Once all of the Address Objects have been created, the following summary screen is displayed.



5.4. Group Address Objects based on site within topology

- 5.4.1.** From the **Network → Address Objects**, click on the **Add Group** button and enter a unique name for the site and highlight all related Address Objects (created in **Step 5.3.1**) and click  to add to group.



- 5.4.2.** Repeat for all sites within network structure as shown in **Figure 1**.

5.4.3. Once completed, the following Address Object Group summary is displayed.

SONICWALL Network Security Appliance

Network / **Address Objects**

Address Groups Items 1 to 3 (of 3)

View Style: ☐ All Address Objects ☒ Custom Address Objects ☐ Default Address Objects [Go to Address Objects](#)

<input type="checkbox"/>	#	Name	Address Detail	Type	Zone	Configure	Comments
<input type="checkbox"/>	1	Company HQ Networks		Group		<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		HQ 10.40.40.X	10.40.40.0/255.255.255.0	Network	LAN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		HQ 10.20.20.X	10.20.20.0/255.255.255.0	Network	LAN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		HQ 10.33.1.X	10.33.1.0/255.255.255.0	Network	LAN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		HQ 10.30.1.X	10.30.1.0/255.255.255.0	Network	LAN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	LAN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
<input type="checkbox"/>	2	Remote Site A Networks		Group		<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		Site A 192.168.133.X	192.168.133.0/255.255.255.0	Network	VPN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		Site A 192.168.130.X	192.168.130.0/255.255.255.0	Network	VPN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		Site A 30.30.30.X	30.30.30.0/255.255.255.0	Network	VPN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
<input type="checkbox"/>	3	Remote Site B Networks		Group		<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		Site B 192.168.33.X	192.168.33.0/255.255.255.0	Network	VPN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	VPN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		Site B 192.168.42.X	192.168.42.0/255.255.255.0	Network	VPN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>
		Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	VPN	<input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Comment"/>

Address Objects Items 1 to 15 (of 15)

Status: The configuration has been updated.

5.5. Define routes for 'local' networks.

Configure the routing information for all the LAN subnets not directly connected to the Corporate Headquarters SonicWALL NSA E5500.

- 5.5.1.** From the **Network → Routing**, click on the **Add** button and enter route information (**Source**, **Destination**, **Service**, **Gateway**, and **Interface**) for each LAN subnet. Click **OK** to continue.

The screenshot shows the 'Route Policy Settings' dialog box in the SonicWall Network Security Appliance interface. The 'General' tab is selected. The settings are as follows:

- Source: Any
- Destination: HQ 10.40.40.X
- Service: Any
- Gateway: HQ Router 10.10.10.2
- Interface: XD
- Metric: 1
- Comment: (empty)
- ☐ Disable route when the interface is disconnected
- ☐ Allow VPN path to take precedence

At the bottom, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

- 5.5.2.** Repeat for each LAN subnet.

5.5.3. Once all of the LAN subnet routes have been added, the following routing summary is displayed.

The screenshot shows the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, and Services. The 'Routing' section is selected. The main area displays the 'Route Policies' table, which lists 16 routes. The table columns are: #, Source, Destination, Service, Gateway, Interface, Metric, Priority, Comment, and Configure. The routes include default gateways, specific subnets, and HQ routers. The status at the bottom left is 'Ready'.

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	Default Gateway	Any	0.0.0.0	X1	20	1		
2	Any	Secondary Default Gateway	Any	0.0.0.0	X7	20	2		
3	Any	10.10.10.245/32	Any	0.0.0.0	X7	20	3		
4	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	4		
5	Any	X7 Subnet	Any	0.0.0.0	X7	20	5		
6	Any	60.60.60.X	Any	Default Gateway	X1	1	6		
7	Any	50.50.50.X	Any	Default Gateway	X1	1	7		
8	Any	HQ 10.40.40.X	Any	HQ Router 10.10.10.2	X0	1	8		
9	Any	HQ 10.20.20.X	Any	HQ Router 10.10.10.2	X0	1	9		
10	Any	HQ 10.33.1.X	Any	HQ Router 10.10.10.2	X0	1	10		
11	Any	HQ 10.30.1.X	Any	HQ Router 10.10.10.2	X0	1	11		
12	Any	X1 Subnet	Any	0.0.0.0	X1	20	12		
13	Any	X0 Subnet	Any	0.0.0.0	X0	20	13		
14	X7 Subnet	Any	Any	Secondary Default Gateway	X7	20	14		
15	X1 Subnet	Any	Any	Default Gateway	X1	20	15		
16	Any	0.0.0.0/0	Any	40.40.40.2	X1	20	16		

5.6. Configure VoIP settings.

- 5.6.1.** From the VoIP → Settings, click on the **Enable H.323 Transformations** checkbox. Click **Accept** to continue.

SonicWall Network Security Appliance

VoIP / Settings

Accept Cancel

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 SLS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/EMC Gatekeeper IP Address: 0.0.0.0

Status: Ready

5.7. Create VPN policies

For each site within the network structure, create a VPN policy to allow secure communication between SonicWALL appliances.

- 5.7.1.** From the **VPN → Settings**, click the **Add** button to add a VPN policy. In this popup enter **Name**, **IPsec Primary Gateway or Address**, **Shared Secret**, and **Confirm Shared Secret**. Click **Network** tab to continue.

The screenshot shows the 'Add VPN Policy' dialog box in the SonicWall Network Security Appliance interface. The 'Network' tab is selected. The 'Security Policy' section contains the following fields: 'Authentication Method' (set to 'IKE using Preshared Secret'), 'Name' (set to 'HQ_To_SiteA'), 'IPsec Primary Gateway Name or Address' (set to '60.60.60.1'), and 'IPsec Secondary Gateway Name or Address' (set to '0.0.0.0'). The 'IKE Authentication' section contains: 'Shared Secret' and 'Confirm Shared Secret' (both masked with dots), a checked 'Mask Shared Secret' checkbox, 'Local IKE ID' (set to 'IP Address'), and 'Peer IKE ID' (set to 'IP Address'). At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

5.7.2.

Specify subnets accessible over the VPN tunnel.

Within the **Choose local network from list** pull down, select the Address Object Group (created in **Step 5.4.1**) for this site. Within the **Choose remote network from list** scroll list, select the Address Object Group (created in **Step 5.4.2**) for the remote site. Click the **Advanced** tab to continue.

The screenshot displays the SonicWall Network Security Appliance configuration interface. At the top, the SonicWall logo and 'Network Security Appliance' are visible. Below this, there are four tabs: 'General', 'Network', 'Proposals', and 'Advanced'. The 'Network' tab is currently selected. The interface is divided into two main sections: 'Local Networks' and 'Destination Networks'. In the 'Local Networks' section, there are three radio button options: 'Choose local network from list' (which is selected), 'Local network obtains IP addresses using DHCP through this VPN Tunnel', and 'Any address'. A dropdown menu next to the selected option shows 'Company HQ Networks'. In the 'Destination Networks' section, there are three radio button options: 'Use this VPN Tunnel as default route for all Internet traffic', 'Destination network obtains IP addresses using DHCP through this VPN Tunnel', and 'Choose destination network from list' (which is selected). A dropdown menu next to the selected option shows 'Remote Site A Networks'. At the bottom of the interface, there is a status bar that says 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'.

5.7.3.**Enable Keep Alive for VPN tunnel**

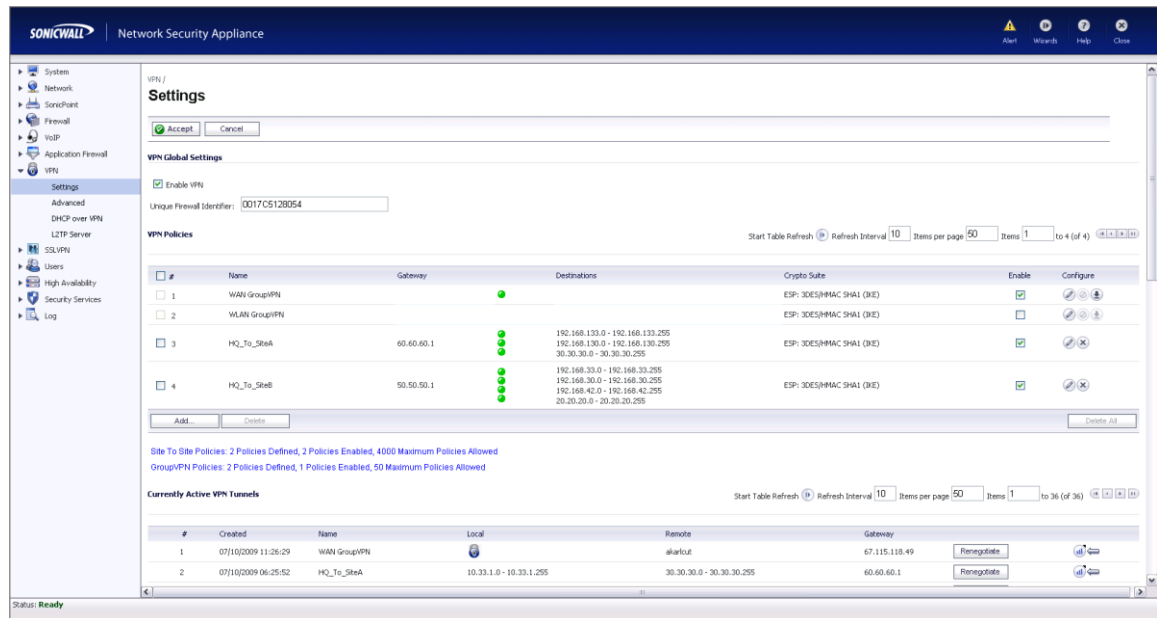
To avoid VPN tunnel establishment latency, click on the **Enable Keep Alive** checkbox. Click **OK** to continue.

The screenshot shows the SonicWall Network Security Appliance configuration interface. The 'Advanced' tab is selected. Under 'Advanced Settings', the 'Enable Keep Alive' checkbox is checked. Other options include 'Suppress automatic Access Rules creation for VPN Policy', 'Require authentication of VPN clients by XAUTH' (with a dropdown for 'User group for XAUTH users'), 'Enable Windows Networking (NetBIOS) Broadcast', 'Enable Multicast', and 'Apply NAT Policies' (with dropdowns for 'Translated Local Network' and 'Translated Remote Network'). Management and login protocols (HTTP, HTTPS, SSH) are also configurable. The 'Default LAN Gateway (optional)' is set to '0.0.0.0' and the 'VPN Policy bound to' is set to 'Zone WAN'. A status bar at the bottom shows 'Ready'.

5.7.4.

Repeat Steps 5.7.1, 5.7.2 and 5.7.3 for each **VPN policy** within the network structure.

5.7.5. Once all the **VPN policies** have been added, the following summary is displayed.




5.8. Save settings

5.8.1. From the **System > Settings**, click on the **Export Settings** button to save the SonicWALL appliance configuration.



5.9. Configure SonicWall NSA 240 (Remote Site A)

Step	Description
5.9.1.	<p>Configure the SonicWall NSA 240 at Remote Site A using the built-in web-based Management Tool. Access this tool by establishing a web browser connection to the SonicWall NSA 240. Refer to Section 9 [6].</p> <p>Log into the SonicWall NSA 240.</p> <ol style="list-style-type: none">1. Connect the LAN port of the computer being used to the X0 (LAN) port on the SonicWall NSA 240.2. Start the Management Tool as follows: Start your web browser and enter http://192.168.168.168 Press Enter.3. Log in to the SonicWall NSA 240 using default credentials which can be obtained from the SonicWALL documentation. 


- 5.9.2.** The main SonicWall NSA 240 window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **System**.

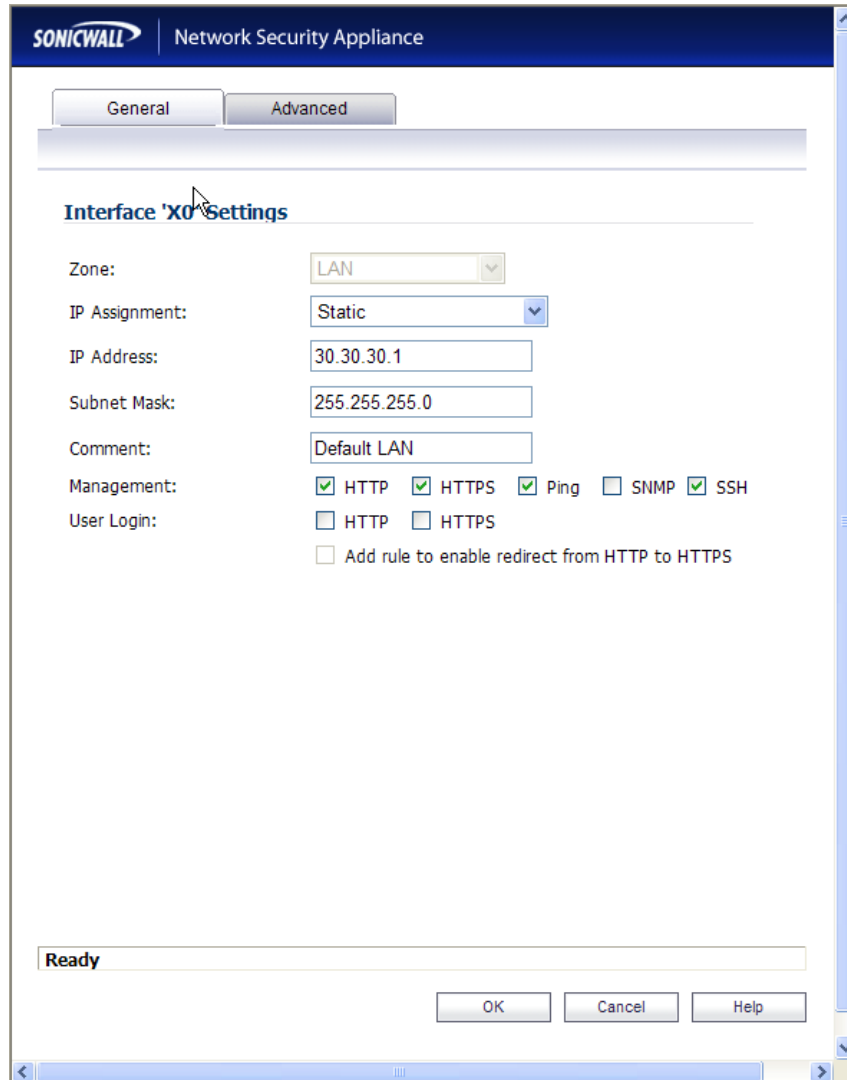
The screenshot displays the SonicWall NSA 240 web interface. The top header features the SonicWall logo and the text "Network Security Appliance". Navigation links include "Register", "Wizards", "Help", and "Logout". The left sidebar shows a "System" menu with options like "Security Dashboard", "Status", "Licenses", "Support Services", "Administration", "Certificates", "Time", "Schedules", "Settings", "Packet Capture", "Diagnostics", and "Restart". Below these are expandable sections for "Network", "PC Card", "SonicPoint", "Firewall", "VoIP", "Application Firewall", "VPN", "SSLVPN", "Users", "High Availability", and "Security Services". The main content area is titled "System / Status" and contains a warning box with three red bullet points: "The password hasn't been changed.", "You have not specified a DNS server address; some functions will not operate properly.", and "Log messages cannot be sent because you have not specified an outbound SMTP server address." Below the warning is a "System Information" table.

System Information	
Model:	NSA 240
Product Code:	6900
Serial Number:	0017C53A8C10
Authentication Code:	ZKMA-A9AV
Firmware Version:	SonicOS Enhanced 5.2.0.1-21o
Safemode Version:	Safemode 5.0.1.11
ROM Version:	SonicROM 5.0.2.12
CPU:	0.10% - 2 x 500 MHz Mips64 Oction Processor
Total Memory :	256 MB RAM, 32 MB Flash
System Time :	07/15/2009 16:52:45
Up Time :	20 Days 07:26:05
Connections :	35
Last Modified By :	10.20.20.77:X1 07/10/2009 15:02:51

At the bottom left of the interface, the status is indicated as "Status: Ready".

5.10. Configure Interfaces:

- 5.10.1** From the **Network → Interfaces**, click on the **Configure icon** , Not shown, for **X0** (LAN) and enter the following information for: **IP Assignment**, **IP Address** and **Subnet Mask** according to network structure to be used, Click **OK** to continue.



5.10.2 Repeat for the **X1** (WAN) interface.

5.10.3 Once configuration on the interfaces is completed, the following summary is presented.

SonicWall Network Security Appliance

Register Wizards Help Logout

Interfaces

Accept

Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	30.30.30.1	255.255.255.0	Static	1000 Mbps full-duplex	Default LAN	
X1	WAN	60.60.60.1	255.255.255.0	Static	1000 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		
X6	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X7	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X8	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
M0	WAN	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	

Add Interface... PortShield Wizard

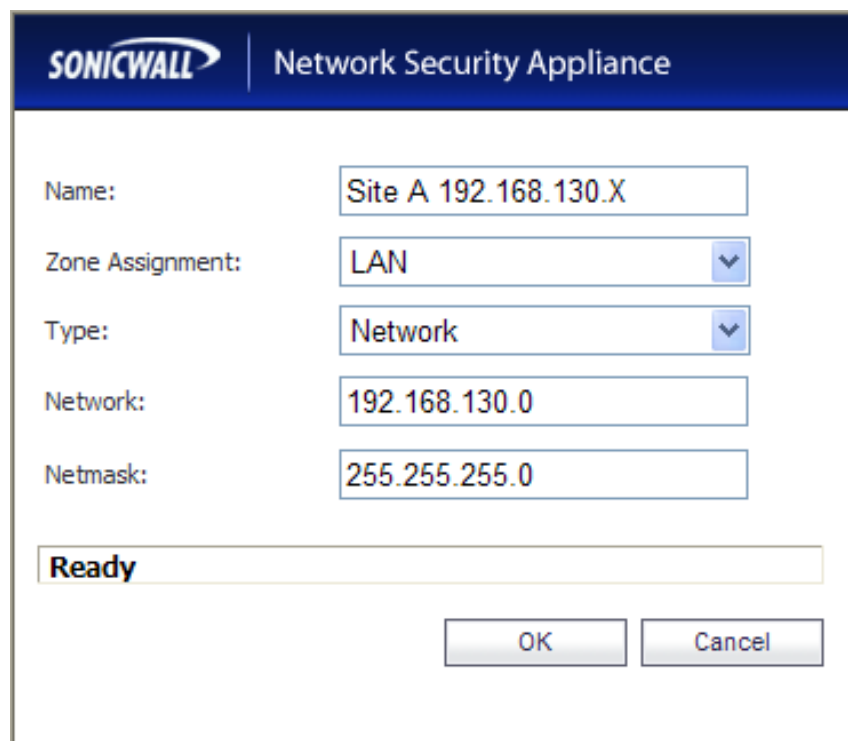
Interface Traffic Statistics

Traffic Statistics	X0	X1	X2	X3	X4	X5	X6	X7	X8	M0
Rx Unicast Packets	368952	494576	0	0	0	0	0	0	0	0
Rx Broadcast Packets	613829	935926	0	0	0	0	0	0	0	0
Rx Bytes	147526648	219215495	0	0	0	0	0	0	0	0
Tx Unicast Packets	108619	458358	0	0	0	0	0	0	0	0
Tx Broadcast Packets	1136	2804	0	0	0	0	0	0	0	0
Tx Bytes	10539209	164457678	0	0	0	0	0	0	0	0

Status: Ready

5.11. Define networks

- 5.11.1** Create Address Objects for each of the networks within the deployment sites. From the **Network → Address Objects**, click on the **Add** button and enter the following information for: **Name**, **Zone Assignment**, **Network**, and **Netmask** for each subnet in the topology. Click **OK** to continue.



The screenshot shows the 'Add Address Object' dialog box in the SonicWall Network Security Appliance interface. The dialog has a blue header with the SonicWall logo and the text 'Network Security Appliance'. Below the header, there are five input fields: 'Name' (containing 'Site A 192.168.130.X'), 'Zone Assignment' (a dropdown menu showing 'LAN'), 'Type' (a dropdown menu showing 'Network'), 'Network' (containing '192.168.130.0'), and 'Netmask' (containing '255.255.255.0'). At the bottom of the dialog, there is a 'Ready' status bar and two buttons: 'OK' and 'Cancel'.


- 5.11.2** Repeat Step **5.11.1** for each subnet in the topology. Refer to **Figure 1** for details of topology used for compliance testing.

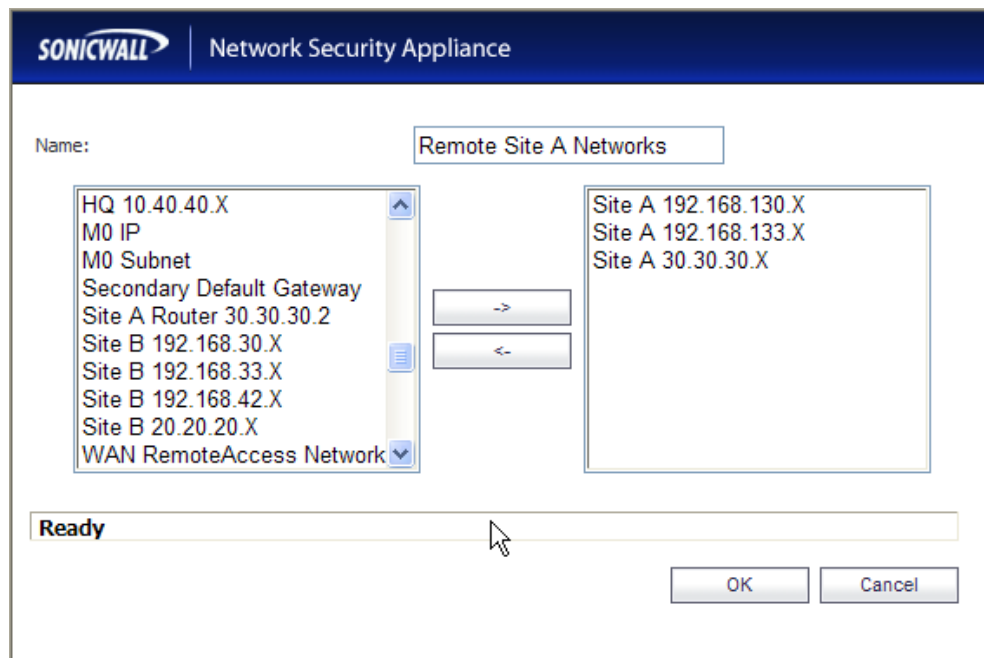
5.11.3 Once all of the Address Objects have been created, the following summary screen is displayed.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, Services, Routing, NAT Policies, ARP, DHCP Server, IP Helper, Web Proxy, Dynamic DNS, PC Card, SonicPoint, Firewall, VoIP, Application Firewall, VPN, SSLVPN, Users, High Availability, Security Services, and Log. The main content area is titled "Address Objects" and shows a list of 14 objects. Each object has a checkbox, a number, a name, an address detail, a type, a zone, and configuration options (Configure, Delete, Comments). The objects are numbered 1 through 14. The interface also includes buttons for "Add...", "Delete", "Refresh", "Purge", "Refresh All", "Purge All", and "Delete All". A status message at the bottom indicates "Status: The configuration has been updated."

#	Name	Address Detail	Type	Zone	Configure	Comments
1	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	VPN		
2	HQ 10.20.20.X	10.20.20.0/255.255.255.0	Network	VPN		
3	HQ 10.30.1.X	10.30.1.0/255.255.255.0	Network	VPN		
4	HQ 10.30.30.X	10.30.30.0/255.255.255.0	Network	VPN		
5	HQ 10.33.1.X	10.33.1.0/255.255.255.0	Network	VPN		
6	HQ 10.40.40.X	10.40.40.0/255.255.255.0	Network	VPN		
7	Site A 192.168.130.X	192.168.130.0/255.255.255.0	Network	LAN		
8	Site A 192.168.133.X	192.168.133.0/255.255.255.0	Network	LAN		
9	Site A 30.30.30.X	30.30.30.0/255.255.255.0	Network	LAN		
10	Site A Router 30.30.30.2	30.30.30.2/255.255.255.255	Host	LAN		
11	Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	VPN		
12	Site B 192.168.33.X	192.168.33.0/255.255.255.0	Network	VPN		
13	Site B 192.168.42.X	192.168.42.0/255.255.255.0	Network	VPN		
14	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	VPN		

5.12. Group Address Objects based on site within topology

- 5.12.1** From the **Network → Address Objects**, click on the **Add Group** button and enter a unique name for the site and highlight all related Address Objects (created in **Steps 5.11.1**) and click  to add to group.



- 5.12.2** Repeat for all sites within network structure as shown in **Figure 1**.

5.12.3 Once completed, the following Address Object Group summary is displayed.

SonicWall Network Security Appliance

Register Wizards Help Logout

System
Network
Interfaces
PortShield Groups
WAN Fallover & LB
Zones
DNS
Address Objects
Services
Routing
NAT Policies
ARP
DHCP Server
IP Helper
Web Proxy
Dynamic DNS
PC Card
SonicPoint
Firewall
VoIP
Application Firewall
VPN
SSLVPN
Users
High Availability
Security Services
Log

Address Groups

View Style: ☐ All Address Objects ☒ Custom Address Objects ☐ Default Address Objects

Go to Address Objects

Add Group... Delete

#	Name	Address Detail	Type	Zone	Configure	Comments
1	Company HQ Networks		Group			
	HQ 10.33.1.X	10.33.1.0/255.255.255.0	Network	VPN		
	HQ 10.30.1.X	10.30.1.0/255.255.255.0	Network	VPN		
	HQ 10.20.20.X	10.20.20.0/255.255.255.0	Network	VPN		
	HQ 10.40.40.X	10.40.40.0/255.255.255.0	Network	VPN		
	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	VPN		
	HQ 10.30.30.X	10.30.30.0/255.255.255.0	Network	VPN		
2	Remote Site A Networks		Group			
	Site A 192.168.130.X	192.168.130.0/255.255.255.0	Network	LAN		
	Site A 192.168.133.X	192.168.133.0/255.255.255.0	Network	LAN		
	Site A 30.30.30.X	30.30.30.0/255.255.255.0	Network	LAN		
3	Remote Site B Networks		Group			
	Site B 192.168.33.X	192.168.33.0/255.255.255.0	Network	VPN		
	Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	VPN		
	Site B 192.168.42.X	192.168.42.0/255.255.255.0	Network	VPN		
	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	VPN		

Add Group... Delete

Delete All

Status: The configuration has been updated.

5.13. Define routes for 'local' networks.

Configure the routing information for all the LAN subnets not directly connected to the Remote Site A SonicWALL NSA 240.

- 5.13.1** From the **Network → Routing**, click on the **Add** button and enter route information. (**Source**, **Destination**, **Service**, **Gateway**, and **Interface**) for each LAN subnet. Click **OK** to continue.



The screenshot shows the 'Route Policy Settings' dialog box in the SonicWall Network Security Appliance interface. The 'General' tab is selected. The settings are as follows:

- Source: Any
- Destination: Site A 192.168.133.X
- Service: Any
- Gateway: Site A Router 30.30.30.2
- Interface: X0
- Metric: 1
- Comment: (empty)
- ☐ Disable route when the interface is disconnected
- ☐ Allow VPN path to take precedence

The status bar at the bottom indicates 'Ready'. At the bottom right, there are buttons for 'OK', 'Cancel', and 'Help'.

- 5.13.2** Repeat for each LAN subnet.

5.13.3 Once all of the LAN subnet routes have been added, the following routing summary is displayed.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar shows the navigation menu with 'Routing' selected. The main content area is divided into two sections: 'Routing' and 'Route Policies'.

Routing Summary:

Interface	Status	Action
X2 (N/A)	Disabled	[Edit]
X3 (N/A)	Disabled	[Edit]
X4 (N/A)	Disabled	[Edit]
X5 (N/A)	Disabled	[Edit]
X6 (N/A)	Disabled	[Edit]
X7 (N/A)	Disabled	[Edit]
X8 (N/A)	Disabled	[Edit]
M0 (WAN)	Disabled	[Edit]

Route Policies:

View Style: ☒ All Policies ☐ Custom Policies ☐ Default Policies

Items 1 to 8 (of 8) [Navigation icons]

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
<input type="checkbox"/> 1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1	[Edit]	[Edit] [Delete]
<input type="checkbox"/> 2	Any	Default Gateway	Any	0.0.0.0	X1	20	2	[Edit]	[Edit] [Delete]
<input checked="" type="checkbox"/> 3	Any	Site A 192.168.133.X	Any	Site A Router 30.30.30.2	X0	1	3		[Edit] [Delete]
<input checked="" type="checkbox"/> 4	Any	Site A 192.168.130.X	Any	Site A Router 30.30.30.2	X0	1	4		[Edit] [Delete]
<input type="checkbox"/> 5	Any	X0 Subnet	Any	0.0.0.0	X0	20	5	[Edit]	[Edit] [Delete]
<input type="checkbox"/> 6	Any	X1 Subnet	Any	0.0.0.0	X1	20	6	[Edit]	[Edit] [Delete]
<input type="checkbox"/> 7	X1 Subnet	Any	Any	Default Gateway	X1	20	7	[Edit]	[Edit] [Delete]
<input type="checkbox"/> 8	Any	0.0.0.0/0	Any	60.60.60.2	X1	20	8	[Edit]	[Edit] [Delete]

Buttons: Add..., Delete, Delete All

Status: Ready

5.14. Configure VoIP settings.

5.14.1 From the **VoIP → Settings**, click on the **Enable H.323 Transformations** checkbox. Click **Accept** to continue.

The screenshot shows the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories: System, Network, PC Card, SonicPoint, Firewall, and VoIP. Under VoIP, the 'Settings' option is selected. The main content area is titled 'VoIP / Settings' and includes an 'Accept' button. Below this, there are three sections: 'General Settings' with an unchecked 'Enable consistent NAT' checkbox; 'SIP Settings' with an unchecked 'Enable SIP Transformations' checkbox and several sub-options and time-out fields; and 'H.323 Settings' with a checked 'Enable H.323 Transformations' checkbox and other related settings. The status bar at the bottom indicates 'Status: Ready'.

SonicWall Network Security Appliance

Register Wizards Help Logout

System
Network
PC Card
SonicPoint
Firewall
VoIP

Settings
Call Status
Application Firewall
VPN
SSLVPN
Users
High Availability
Security Services
Log

VoIP / Settings

Accept Cancel

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): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

Status: Ready

5.15. Create VPN policies

For each site within the network structure, create a VPN policy to allow secure communication between SonicWALL appliances.

- 5.15.1** From the **VPN → Settings**, click the **Add** button to add a VPN policy. In this popup enter **Name**, **IPSec Primary Gateway or Address**, **Shared Secret**, and **Confirm Shared Secret**. Click the **Network** tab to continue.

The screenshot shows the 'Add VPN Policy' dialog box on a SonicWall Network Security Appliance. The 'Network' tab is selected. The 'Security Policy' section contains the following fields: 'Authentication Method' (set to 'IKE using Preshared Secret'), 'Name' (set to 'SiteA_To_HQ'), 'IPsec Primary Gateway Name or Address' (set to '40.40.40.1'), and 'IPsec Secondary Gateway Name or Address' (set to '0.0.0.0'). The 'IKE Authentication' section contains: 'Shared Secret' and 'Confirm Shared Secret' (both masked with dots), a checked 'Mask Shared Secret' checkbox, 'Local IKE ID' (set to 'IP Address'), and 'Peer IKE ID' (set to 'IP Address'). At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

SONICWALL Network Security Appliance	
Security Policy	
Authentication Method:	IKE using Preshared Secret
Name:	SiteA_To_HQ
IPsec Primary Gateway Name or Address:	40.40.40.1
IPsec Secondary Gateway Name or Address:	0.0.0.0
IKE Authentication	
Shared Secret:
Confirm Shared Secret:
	<input checked="" type="checkbox"/> Mask Shared Secret
Local IKE ID:	IP Address
Peer IKE ID:	IP Address
Ready	
OK Cancel Help	

5.15.2

Specify subnets accessible over the VPN tunnel.

Within the **Choose local network from list** scroll list, select the Address Object Group (created in **Step 5.12.1**) for this site. Within the **Choose remote network from list** scroll list, select the Address Object Group (created in **Step 5.12.2**) for the remote site. Click the **Advanced** tab to continue.

The screenshot shows the SonicWall Network Security Appliance configuration window, specifically the Network tab and the Advanced section. The window has a title bar with the SonicWall logo and the text "Network Security Appliance". Below the title bar are four tabs: General, Network, Proposals, and Advanced. The Advanced tab is selected. The main content area is divided into two sections: "Local Networks" and "Destination Networks".

Local Networks

- ☒ Choose local network from list: Remote Site A 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: Company HQ Networks

At the bottom of the window, there is a status bar that says "Ready" and three buttons: OK, Cancel, and Help.

5.15.3**Enable Keep Alive for VPN tunnel**

To avoid VPN tunnel establishment latency, click on the **Enable Keep Alive** checkbox. Click **OK** to continue.

SONICWALL | Network Security Appliance

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 ☐ SSH

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: Zone WAN

Ready

OK Cancel Help

5.15.4

Repeat Steps 5.15.1, 5.15.2 and 5.15.3 for each **VPN policy** within the network structure.

5.15.5 Once all the VPN policies have been added, the following summary is displayed.

SONICWALL | Network Security Appliance

Register Wizards Help Logout

System
Network
PC Card
SonicPoint
Firewall
VoIP
Application Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
SSLVPN
Users
High Availability
Security Services
Log

VPN /
Settings

Accept Cancel

VPN Global Settings

☒ Enable VPN

Unique Firewall Identifier: 0017C53A8C10

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 4 (of 4)

VPN Policies

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
<input type="checkbox"/> 1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input type="checkbox"/> 2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input checked="" type="checkbox"/> 3	SiteA_To_HQ	40.40.40.1	10.33.1.0 - 10.33.1.255 10.30.1.0 - 10.30.1.255 10.20.20.0 - 10.20.20.255 10.40.40.0 - 10.40.40.255 10.10.10.0 - 10.10.10.255 10.30.30.0 - 10.30.30.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 4	SiteA_To_SiteB	50.50.50.1	192.168.33.0 - 192.168.33.255 192.168.30.0 - 192.168.30.255 192.168.42.0 - 192.168.42.255 20.20.20.0 - 20.20.20.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Add... Delete Delete All

Site To Site Policies: 2 Policies Defined, 2 Policies Enabled, 25 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 6 Maximum Policies Allowed

Currently Active VPN Tunnels

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 27 (of 27)


Status: Ready

5.16. Save settings

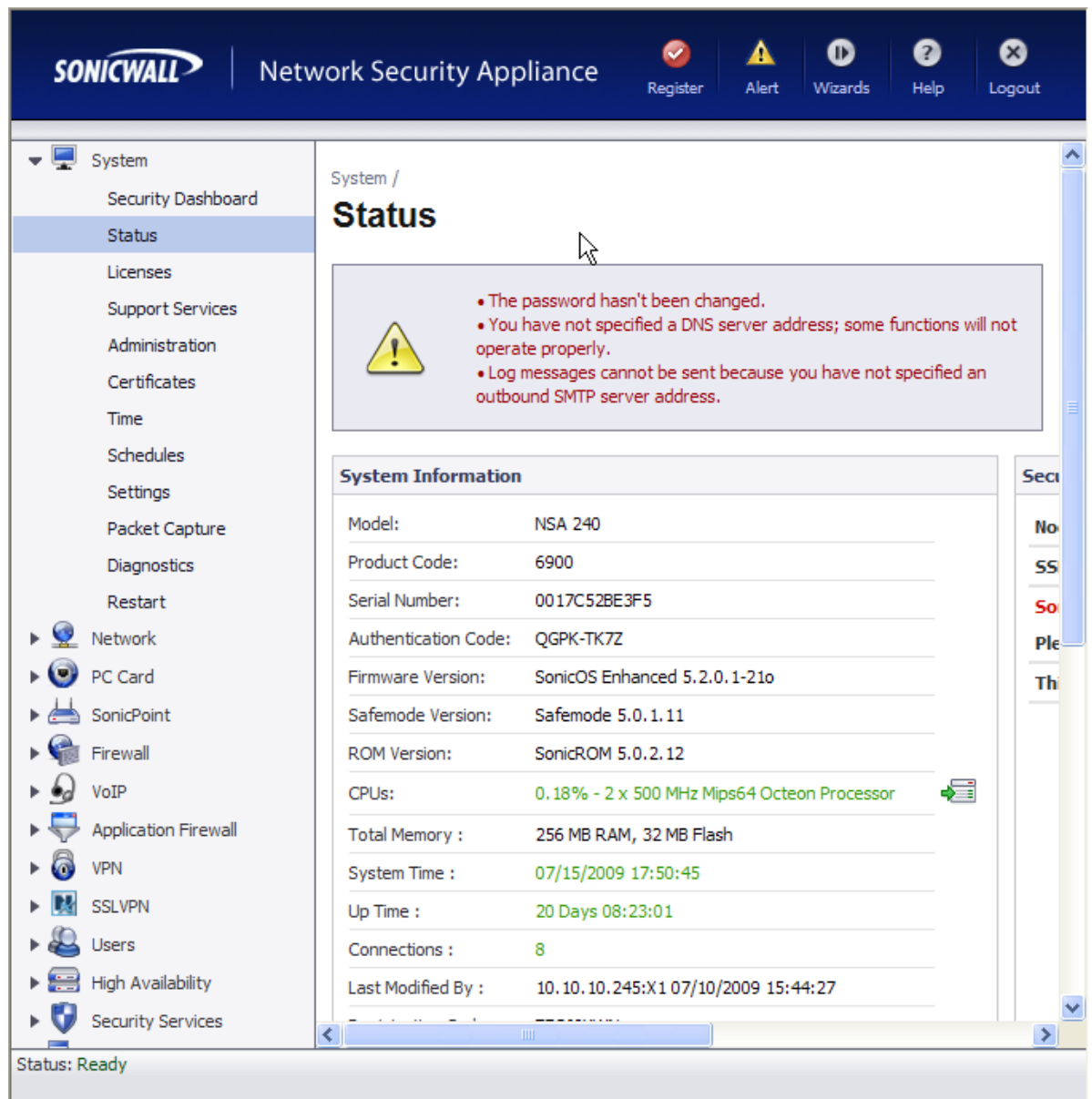
- 5.16.1** Save settings
From the **System > Settings**, click on the **Export Settings** button to save the SonicWALL appliance configuration.



5.17. Configure SonicWall NSA 240 (Remote Site B)


Step	Description
5.17.1	<p>Configure the SonicWall NSA 240 at Remote Site B using the built-in web-based Management Tool. Access this tool by establishing a web browser connection to the SonicWall NSA 240. Refer to Section 9 [6].</p> <p>Log into the Remote Site B SonicWall NSA 240.</p> <ol style="list-style-type: none">1. Connect the LAN port of the computer being used to the X0 (LAN) port on the SonicWall NSA 240.2. Start the Management Tool as follows: Start your web browser and enter http://192.168.168.168 Press Enter.3. Log in to the SonicWall NSA 240 using default credentials which can be obtained from the SonicWALL documentation. 

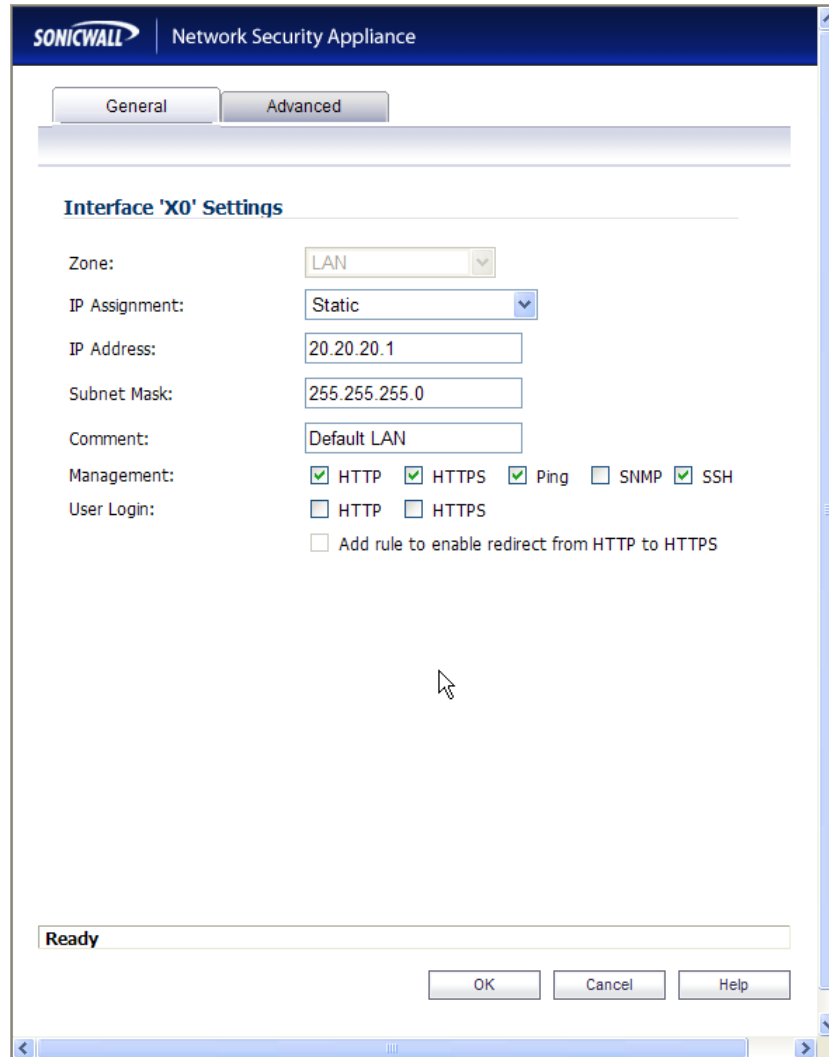
- 5.17.2** The main SonicWall NSA 240 window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **System**.



5.18. Configure Interfaces:

5.18.1

From the **Network** → **Interfaces**, click on the **Configure icon** , not shown, for **X0** (LAN) and enter the following information for: **IP Assignment**, **IP Address** and **Subnet Mask** for the network structure to be used, Click **OK** to continue.



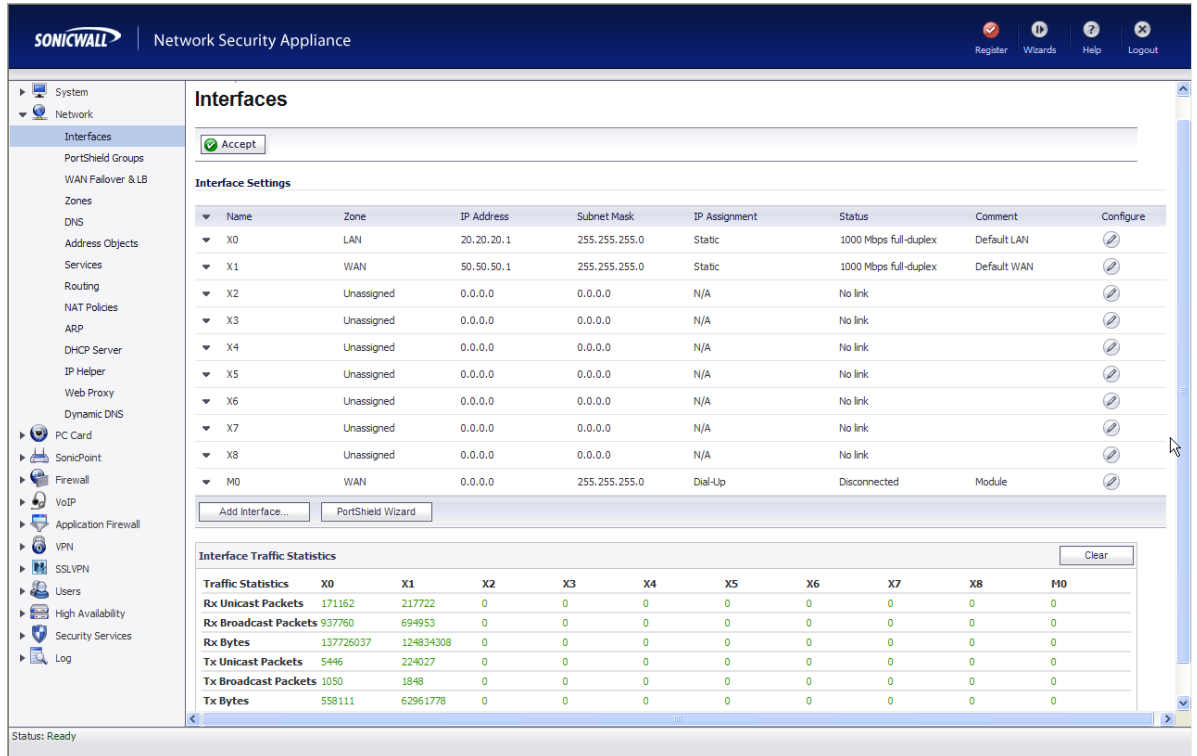
The screenshot shows the 'Interface 'X0' Settings' dialog box in the SonicWall Network Security Appliance configuration interface. The 'General' tab is selected. The settings are as follows:

- Zone: LAN
- IP Assignment: Static
- IP Address: 20.20.20.1
- Subnet Mask: 255.255.255.0
- Comment: Default LAN
- Management: ☒ HTTP, ☒ HTTPS, ☒ Ping, ☐ SNMP, ☒ SSH
- User Login: ☐ HTTP, ☐ HTTPS
- ☐ Add rule to enable redirect from HTTP to HTTPS

The status bar at the bottom indicates 'Ready'. The dialog box has 'OK', 'Cancel', and 'Help' buttons.

5.18.2 Repeat for the X1 (WAN) interface.

5.18.3 Once configuration on the interfaces is completed, the following summary is presented.



Interfaces

☒ Accept

Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	20.20.20.1	255.255.255.0	Static	1000 Mbps full-duplex	Default LAN	
X1	WAN	50.50.50.1	255.255.255.0	Static	1000 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		
X6	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X7	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X8	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
M0	WAN	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	

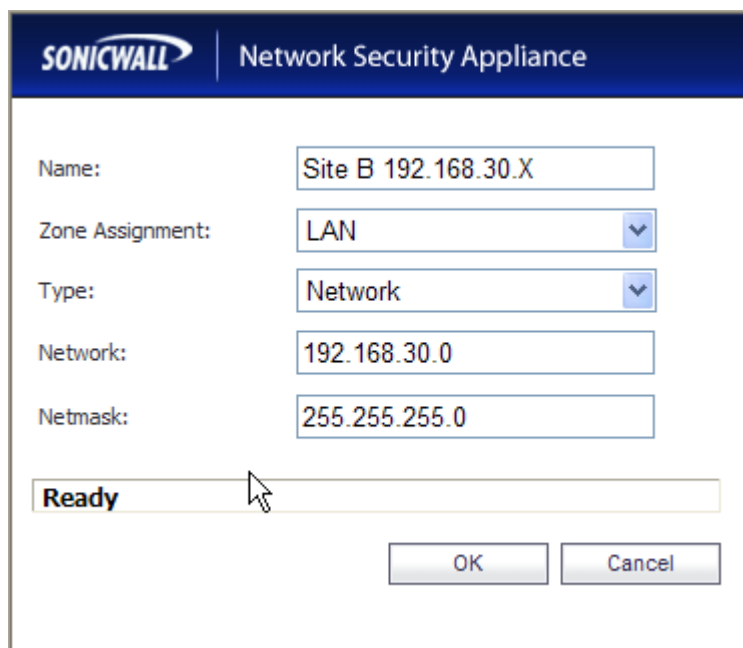
Interface Traffic Statistics

Traffic Statistics	X0	X1	X2	X3	X4	X5	X6	X7	X8	M0
Rx Unicast Packets	171162	217722	0	0	0	0	0	0	0	0
Rx Broadcast Packets	937760	694953	0	0	0	0	0	0	0	0
Rx Bytes	137726037	124834308	0	0	0	0	0	0	0	0
Tx Unicast Packets	5446	224027	0	0	0	0	0	0	0	0
Tx Broadcast Packets	1050	1848	0	0	0	0	0	0	0	0
Tx Bytes	558111	62961778	0	0	0	0	0	0	0	0

Status: Ready

5.19. Define networks

- 5.19.1** Create Address Objects for each of the networks within the deployment sites. From the **Network → Address Objects**, click on the **Add** button and enter the following information for: **Name**, **Zone Assignment**, **Network**, and **Netmask** for each subnet in the topology. Click **OK** to continue.



The screenshot shows the 'Add Address Object' dialog box in the SonicWall Network Security Appliance interface. The dialog has a blue header with the SonicWall logo and the text 'Network Security Appliance'. Below the header, there are five input fields: 'Name' (containing 'Site B 192.168.30.X'), 'Zone Assignment' (a dropdown menu showing 'LAN'), 'Type' (a dropdown menu showing 'Network'), 'Network' (containing '192.168.30.0'), and 'Netmask' (containing '255.255.255.0'). At the bottom left, there is a 'Ready' status bar with a mouse cursor pointing at it. At the bottom right, there are two buttons: 'OK' and 'Cancel'.


- 5.19.2** Repeat Step **5.19.1** for each subnet in the topology. Refer to **Figure 1** for details of topology used for compliance testing.

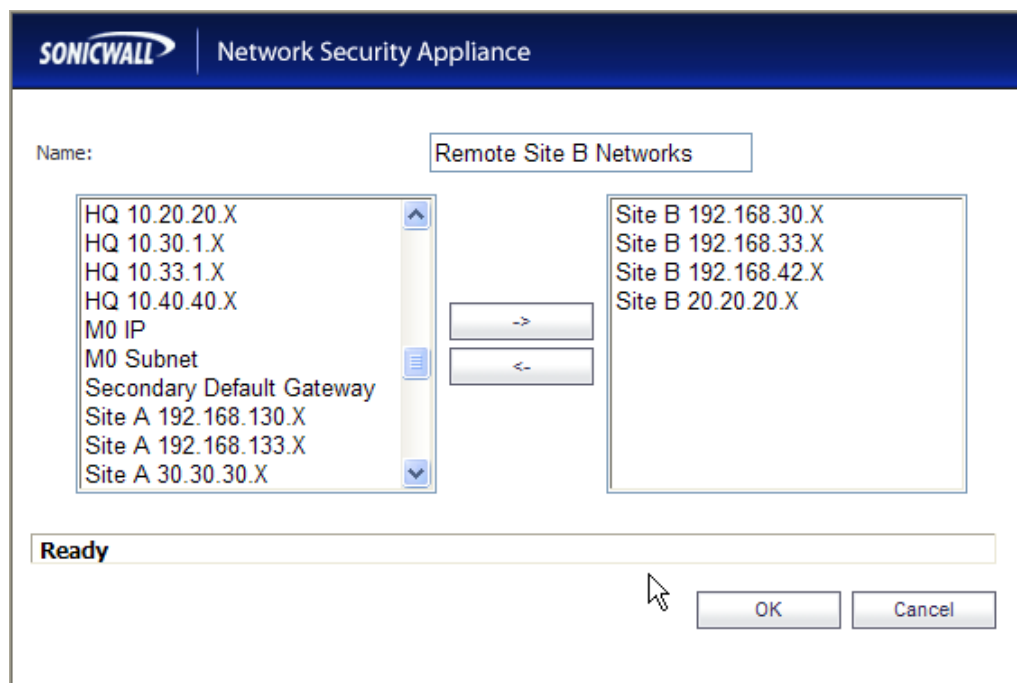
5.19.3 Once all of the Address Objects have been created, the following summary screen is displayed.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar shows the navigation menu with categories like System, Network, Services, Routing, NAT Policies, ARP, DHCP Server, IP Helper, Web Proxy, Dynamic DNS, PC Card, SonicPoint, Firewall, VoIP, Application Firewall, VPN, SSLVPN, Users, High Availability, Security Services, and Log. The main content area is titled 'Address Objects' and shows a list of 13 objects. The list includes columns for #, Name, Address Detail, Type, Zone, Configure, and Comments. The objects are numbered 1 through 13 and include details like 'HQ 10.10.10.X', 'Site A 192.168.130.X', and 'Site B Router 20.20.20.2'. The interface also features buttons for 'Add...', 'Delete', 'Refresh', 'Purge', 'Refresh All', 'Purge All', and 'Delete All'. A status message at the bottom indicates 'Status: The configuration has been updated.'

#	Name	Address Detail	Type	Zone	Configure	Comments
1	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	VPN		
2	HQ 10.20.20.X	10.20.20.0/255.255.255.0	Network	VPN		
3	HQ 10.30.1.X	10.30.1.0/255.255.255.0	Network	VPN		
4	HQ 10.33.1.X	10.33.1.0/255.255.255.0	Network	VPN		
5	HQ 10.40.40.X	10.40.40.0/255.255.255.0	Network	VPN		
6	Site A 192.168.130.X	192.168.130.0/255.255.255.0	Network	VPN		
7	Site A 192.168.133.X	192.168.133.0/255.255.255.0	Network	VPN		
8	Site A 30.30.30.X	30.30.30.0/255.255.255.0	Network	VPN		
9	Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	LAN		
10	Site B 192.168.33.X	192.168.33.0/255.255.255.0	Network	LAN		
11	Site B 192.168.42.X	192.168.42.0/255.255.255.0	Network	LAN		
12	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	LAN		
13	Site B Router 20.20.20.2	20.20.20.2/255.255.255.255	Host	LAN		

5.20. Group Address Objects based on site within topology

- 5.20.1** From the **Network → Address Objects**, click on the **Add Group** button and enter a unique name for the site and highlight all related Address Objects (created in **Steps 5.19.1**) and click  to add to group.



- 5.20.2** Repeat for all sites within network structure as shown in **Figure 1**.

5.20.3 Once completed, the following Address Object Group summary is displayed.

SONICWALL | Network Security Appliance

Register Alert Wizards Help Logout

Address Objects

Address Groups Items 1 to 3 (of 3) Go to Address Objects

View Style: ☐ All Address Objects ☒ Custom Address Objects ☐ Default Address Objects

Add Group... Delete Delete All

#	Name	Address Detail	Type	Zone	Configure	Comments
1	Company HQ Networks		Group			
	HQ 10.33.1.X	10.33.1.0/255.255.255.0	Network	VPN		
	HQ 10.30.1.X	10.30.1.0/255.255.255.0	Network	VPN		
	HQ 10.20.20.X	10.20.20.0/255.255.255.0	Network	VPN		
	HQ 10.40.40.X	10.40.40.0/255.255.255.0	Network	VPN		
	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	VPN		
2	Remote Site A Networks		Group			
	Site A 192.168.133.X	192.168.133.0/255.255.255.0	Network	VPN		
	Site A 192.168.130.X	192.168.130.0/255.255.255.0	Network	VPN		
	Site A 30.30.30.X	30.30.30.0/255.255.255.0	Network	VPN		
3	Remote Site B Networks		Group			
	Site B 192.168.33.X	192.168.33.0/255.255.255.0	Network	LAN		
	Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	LAN		
	Site B 192.168.42.X	192.168.42.0/255.255.255.0	Network	LAN		
	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	LAN		

Add Group... Delete Delete All

Status: The configuration has been updated.

5.21. Define routes for 'local' networks.

Configure the routing information for all the LAN subnets not directly connected to the Remote Site B SonicWALL NSA 240.

- 5.21.1** From the **Network → Routing**, click on the **Add** button and enter route information (**Source**, **Destination**, **Service**, **Gateway**, and **Interface**) for each LAN subnet. Click **OK** to continue.

The screenshot shows the 'Route Policy Settings' dialog box in the SonicWall Network Security Appliance interface. The 'General' tab is selected. The settings are as follows:

- Source: Any (dropdown)
- Destination: Site B 192.168.30.X (dropdown)
- Service: Any (dropdown)
- Gateway: Site B Router 20.20.20.2 (dropdown)
- Interface: X0 (dropdown)
- Metric: 1 (text input)
- Comment: (empty text input)
- ☐ Disable route when the interface is disconnected
- ☐ Allow VPN path to take precedence

At the bottom, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

- 5.21.2** Repeat for each LAN subnet.

5.21.3 Once all of the LAN subnet routes have been added, the following routing summary is displayed.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar shows the navigation menu with categories like System, Network, Firewall, and VPN. The 'Routing' section is selected, showing a list of interfaces (X3 to X8 and M0) and their status (Disabled). The main content area shows the 'Route Policies' section with a table of 9 routes. The table columns are #, Source, Destination, Service, Gateway, Interface, Metric, Priority, Comment, and Configure. The routes include a default gateway (255.255.255.255/32) and several specific subnets (Site B, X0 Subnet, X1 Subnet, and 0.0.0.0/0).

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1		
2	Any	Default Gateway	Any	0.0.0.0	X1	20	2		
3	Any	Site B 192.168.30.X	Any	Site B Router 20.20.20.2	X0	1	3		
4	Any	Site B 192.168.42.X	Any	Site B Router 20.20.20.2	X0	1	4		
5	Any	Site B 192.168.33.X	Any	Site B Router 20.20.20.2	X0	1	5		
6	Any	X0 Subnet	Any	0.0.0.0	X0	20	6		
7	Any	X1 Subnet	Any	0.0.0.0	X1	20	7		
8	X1 Subnet	Any	Any	Default Gateway	X1	20	8		
9	Any	0.0.0.0/0	Any	50.50.50.2	X1	20	9		

Buttons: Add..., Delete, Delete All

5.22. Configure VoIP settings.

- 5.22.1** From the **VoIP → Settings**, click on the **Enable H.323 Transformations** checkbox. Click **Accept** to continue.

The screenshot displays the SonicWall Network Security Appliance interface. The top navigation bar includes the SonicWall logo and the title 'Network Security Appliance'. On the right, there are links for Register, Alert, Wizards, Help, and Logout. The left sidebar shows a tree view of system settings, with 'VoIP' selected and 'Settings' expanded. The main content area is titled 'VoIP / Settings' and features an 'Accept' button. Below this, the 'General Settings' section includes an unchecked 'Enable consistent NAT' checkbox. The 'SIP Settings' section has an unchecked 'Enable SIP Transformations' checkbox, with sub-options for 'Permit non-SIP packets on signaling port' and 'Enable SIP Back-to-Back User Agent (B2BUA) support'. It also includes input fields for 'SIP Signaling inactivity time out (seconds)' (1800), 'SIP Media inactivity time out (seconds)' (120), and 'Additional SIP signaling port (UDP) for transformations (optional)' (0). The 'H.323 Settings' section has the 'Enable H.323 Transformations' checkbox checked, with sub-options for 'Only accept incoming calls from Gatekeeper' and 'Enable LDAP ILS Support'. It also includes input fields for 'H.323 Signaling/Media inactivity time out (seconds)' (300) and 'Default WAN/DMZ Gatekeeper IP Address' (0.0.0.0). The status bar at the bottom indicates 'Status: Ready'.

5.23. Create VPN policies

For each site within the network structure, create a VPN policy to allow secure communication between SonicWALL appliances.

5.23.1 From the **VPN → Settings**, click the **Add** button to add a VPN policy. In this popup enter **Name**, **IPsec Primary Gateway or Address**, **Shared Secret**, and **Confirm Shared Secret**.

Click the **Network** tab to continue.

The screenshot shows the 'Add VPN Policy' dialog box in the SonicWall Network Security Appliance interface. The 'Network' tab is selected. The 'Security Policy' section contains the following fields: 'Authentication Method' (set to 'IKE using Preshared Secret'), 'Name' (set to 'SiteB_To_HQ'), 'IPsec Primary Gateway Name or Address' (set to '40.40.40.1'), and 'IPsec Secondary Gateway Name or Address' (set to '0.0.0.0'). The 'IKE Authentication' section contains: 'Shared Secret' and 'Confirm Shared Secret' (both masked with dots), a checked 'Mask Shared Secret' checkbox, 'Local IKE ID' (set to 'IP Address'), and 'Peer IKE ID' (set to 'IP Address'). At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

5.23.2

Specify subnets accessible over the VPN tunnel.

Within the **Choose local network from list** scroll list, select the Address Object Group (created in **Step 5.20.1**) for this site. Within the **Choose remote network from list** scroll list, select the Address Object Group (created in **Step 5.20.2**) for the remote site. Click the **Advanced** tab to continue.

The screenshot shows the SonicWall Network Security Appliance configuration window, specifically the **Network** tab. The window has a title bar with the SonicWall logo and the text "Network Security Appliance". Below the title bar are four tabs: **General**, **Network**, **Proposals**, and **Advanced**. The **Network** tab is selected. The main content area is divided into two sections: **Local Networks** and **Destination Networks**. In the **Local Networks** section, there are three radio buttons: "Choose local network from list" (selected), "Local network obtains IP addresses using DHCP through this VPN Tunnel", and "Any address". A dropdown menu next to the selected radio button shows "Remote Site B Networks". In the **Destination Networks** section, there are three radio buttons: "Use this VPN Tunnel as default route for all Internet traffic", "Destination network obtains IP addresses using DHCP through this VPN Tunnel", and "Choose destination network from list" (selected). A dropdown menu next to the selected radio button shows "Company HQ Networks". At the bottom of the window, there is a status bar that says "Ready" and three buttons: "OK", "Cancel", and "Help".

5.23.3

Enable Keep Alive for VPN tunnel.

To avoid VPN tunnel establishment latency, click on the **Enable Keep Alive** checkbox. Click **OK** to continue.

The screenshot shows the SonicWall Network Security Appliance configuration interface. The top navigation bar includes tabs for General, Network, Proposals, and Advanced. The 'Advanced' tab is selected, and the 'Advanced Settings' section is visible. The 'Enable Keep Alive' checkbox is checked. Other options include 'Suppress automatic Access Rules creation for VPN Policy', 'Require authentication of VPN clients by XAUTH' (with a dropdown for 'User group for XAUTH users'), 'Enable Windows Networking (NetBIOS) Broadcast', 'Enable Multicast', and 'Apply NAT Policies' (with dropdowns for 'Translated Local Network' and 'Translated Remote Network'). Under 'Management via this SA', 'HTTP' and 'HTTPS' are checked, while 'SSH' is unchecked. Under 'User login via this SA', both 'HTTP' and 'HTTPS' are unchecked. The 'Default LAN Gateway (optional)' is set to '0.0.0.0'. The 'VPN Policy bound to' is set to 'Zone WAN'. A status bar at the bottom left shows 'Ready'. At the bottom right are 'OK', 'Cancel', and 'Help' buttons.

5.23.4

Repeat Steps 5.23.1, 5.23.2 and 5.23.3 for each **VPN policy** within the network structure.

5.23.5 Once all the VPN policies have been added, the following summary is displayed.

VPN / Settings

Accept Cancel

VPN Global Settings

☒ Enable VPN

Unique Firewall Identifier: 0017C52BE3F5

VPN Policies

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 4 (of 4)

#	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 type="checkbox"/>	
3	SiteB_To_HQ	40.40.40.1	10.33.1.0 - 10.33.1.255 10.30.1.0 - 10.30.1.255 10.20.20.0 - 10.20.20.255 10.40.40.0 - 10.40.40.255 10.10.10.0 - 10.10.10.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
4	SiteB_To_SiteA	60.60.60.1	192.168.133.0 - 192.168.133.255 192.168.130.0 - 192.168.130.255 30.30.30.0 - 30.30.30.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Add... Delete Delete All

Site To Site Policies: 2 Policies Defined, 2 Policies Enabled, 25 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 6 Maximum Policies Allowed

Currently Active VPN Tunnels

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 32 (of 32)

#	Created	Name	Local	Remote	Gateway
---	---------	------	-------	--------	---------

5.24. Save settings

- 5.24.1** Save settings
From the **System > Settings**, click on the **Export Settings** button to save the SonicWALL appliance configuration.

SONICWALL | Network Security Appliance

You can export the current configuration of your SonicWALL to a file. The file can be imported by the same SonicWALL or used to clone a configuration across multiple SonicWALLs.

The default name of the file will be 'sonicwall-NSA_240-5_2_0_1-210.exp'.

Export Cancel

6. General Test Approach and Test Results

6.1. Test Approach

All feature functionality test cases were performed manually. The general test approach entailed verifying the following list through the SonicWALL firewall VPNs:

- LAN/WAN connectivity between all locations
- Registration of Avaya IP Telephones with Avaya IP Office
- Verification of the Small Community Networking trunk between the two Avaya IP Offices.
- Verifying that DSCP and 802.1p Priority QoS values are not altered by the SonicWALL firewall VPNs.
- Verifying that Avaya VoiceMail Pro and MWI work properly.
- Retrieving Voicemail messages from Remote locations.
- Features Tested: attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call park, call pick-up, bridged call appearances

6.2. Test Results

All feature functionality, serviceability, and performance test cases passed. The Multi-Site SonicWALL firewall VPN implementation yielded good voice quality and no calls were lost. The stability of the Avaya/ SonicWALL solution was successfully verified through performance and serviceability testing.

7. Verification Steps

While running through the SonicWALL firewall VPNs these verification steps can be run:

1. Check that the Avaya H.323 IP telephones have successfully registered with Avaya Communication Manager using the **list registered-station** command.
2. Place internal and external calls between the digital telephone and IP telephones at each site.

8. Conclusion

These Application Notes describe the configuration steps for integrating the SonicWALL UTM Firewalls with an Avaya telephony infrastructure using Avaya IP Office. For the configuration described in these Application Notes, VoIP traffic, voice features and Data traffic traversed the network properly through the SonicWALL firewall VPNs.

9. Additional References

The documents referenced below were used for additional support and configuration information.

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>

- [1] *Avaya IP Office 4.2 Installation Manual*, Document Number 15-601042
- [2] *Avaya IP Office 4.2 Embedded Voicemail User Guide*, Document Number 15-601067
- [3] *Avaya IP Office 4.2 Phone Manager User Guide*, Document Number 15-600988
- [4] *Avaya IP Office 4.2 Manager 6.2*, Document # 16-601443
- [5] *Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide*, Document # 16-601443

The SonicWALL product documentation can be found at

- [6] <http://www.sonicwall.com/us/support/6832.html>

10. Change History

Issue	Date	Reason
1.0	9/25/09	Initial issue

©2009 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 DevConnect Program at devconnect@avaya.com.