



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring a SonicWALL VPN solution with an Avaya IP Telephony Infrastructure using Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services in a Converged VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe the steps for configuring a SonicWALL VPN solution with an Avaya IP Telephony Infrastructure using Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services consisting of a Corporate Headquarters with three remote sites.

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 Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging, Avaya IA 770 INTUITY AUDIX 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 UTM 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 Modular Messaging and Avaya IA770 INTUITY AUDIX, 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 5 are registered with Communication Manager in the Main Site and extension numbers beginning with the number 4 are registered with the Remote Site B Communication Manager. 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 Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, SES, Avaya Modular Messaging, Avaya IA 770 INTUITY AUDIX, one Avaya 2410 Digital Telephone, one Avaya 9630 IP Telephone running Avaya one-X Deskphone Edition on VLAN Voice1, one Avaya 9640 IP Telephone running Avaya one-X Deskphone SIP on VLAN Voice1 and one Corporate DHCP/File server. The Corporate Headquarters provided a DHCP/File server for assigning IP network parameters and to download settings to the Avaya IP telephones.

2.2. Remote Site A

Remote Site A consisted of one SonicWall NSA 240, one router, one Avaya 9650 IP Telephone running Avaya one-X Deskphone Edition, one Avaya 9620 IP Telephone running Avaya one-X Deskphone SIP, and a PC on data network. The Avaya IP telephones register to headquarters Communication Manager.

2.3. Remote Site B

Remote Site B consisted of one SonicWall NSA 240, one router, Communication Manager running on an Avaya S8300 Server with an Avaya G700 Media Gateway, one Avaya 2410 Digital Telephone, one Avaya 9640G IP Telephone running Avaya one-X Deskphone Edition, one Avaya 9630 IP Telephone running Avaya one-X Deskphone Edition, and a PC on data network. The Avaya IP telephones register to the Remote Site B Communication Manager. An H.323 trunk was configured between Communication Managers at the Corporate Headquarters and Remote Site B to allow direct dialing between the sites.

2.4. Remote Site C

Remote Site C consisted of one SonicWall NSA 240, one router, one Avaya G700 Media Gateway, and two Avaya 2410 Digital Telephones. The Remote Site C Avaya Media Gateway registers to the headquarters Communication Manager. While the Avaya 2410 Digital Telephones are directly connected to the Remote Site C Avaya Media gateway, they are administered on the headquarters Communication Manager.

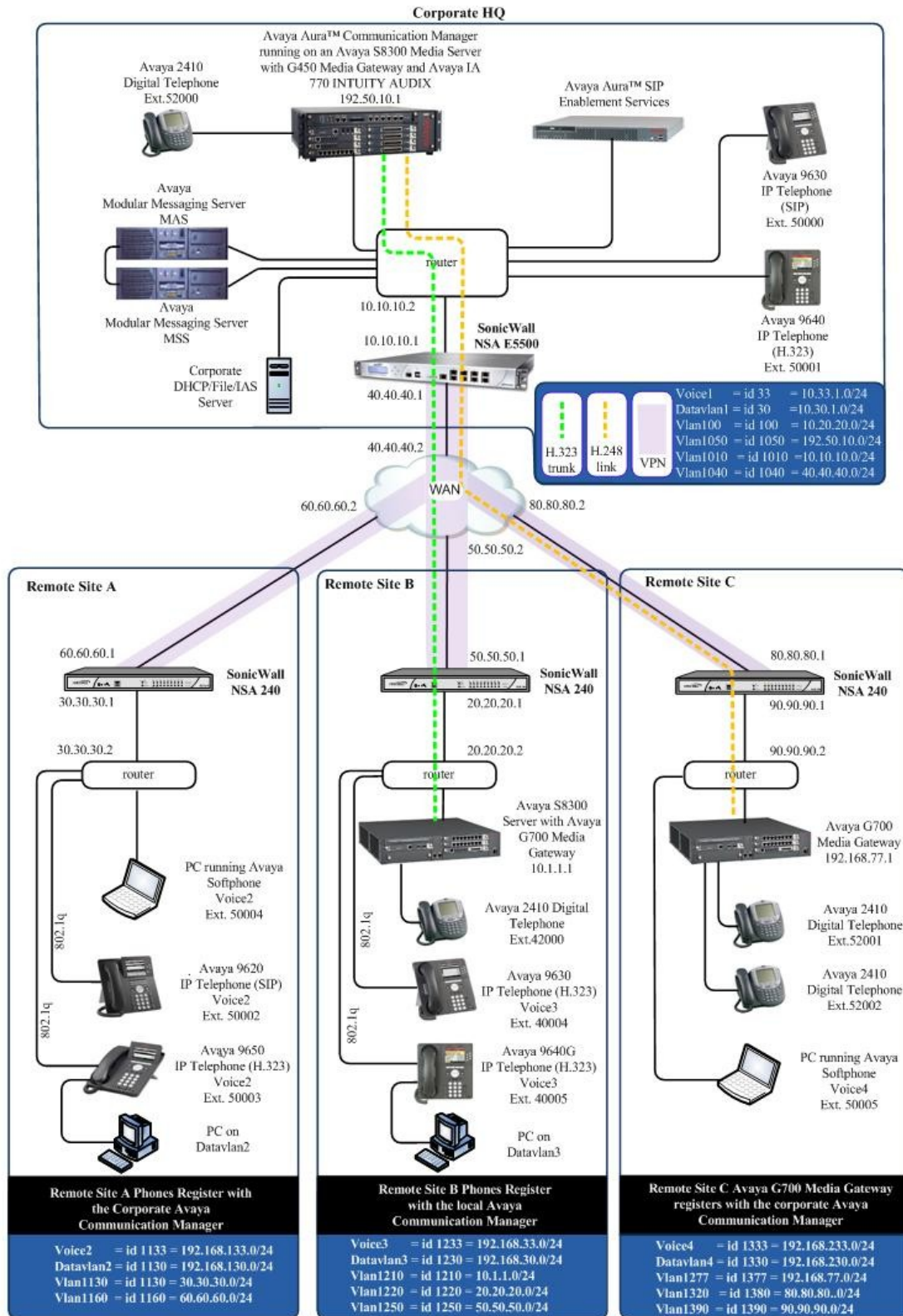


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300 Server running Avaya Aura™ Communication Manager	Avaya Aura™ Communication Manager 5.2
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module Avaya IA 770 INTUITY AUDIX	28.22.0 HW9 5.2
Avaya G700 Media Gateway (Remote Site B) MGP MM712 DCP Media Module	28.22.0 HW9
Avaya G700 Media Gateway (Remote Site C) MM712 DCP Media Module	HW9
Avaya SIP Enablement Services (SES)	
Avaya Aura™ SIP Enabled Services (SES) Server	5.2
Avaya Messaging (Voice Mail) Products	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.0
Avaya Modular Messaging - Message Storage Server (MSS)	5.0
Avaya IA 770 INTUITY AUDIX	5.1
Avaya Telephony Sets	
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 3.0
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.0.0
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	
Microsoft Windows 2003 Server	File/DHCP Service

4. Configure Avaya Aura™ Communication Manager

This section shows the steps used to configure Avaya Aura™ Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, refer to [1].


Use the **change ip-network-region 1** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/q PARAMETERS settings configured in Communication Manager.

The Differentiated Services Code Point (DSCP) value of 48 will be used for both PHB values. DSCP 48 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **46** and the **Audio PHB Value** to **46**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

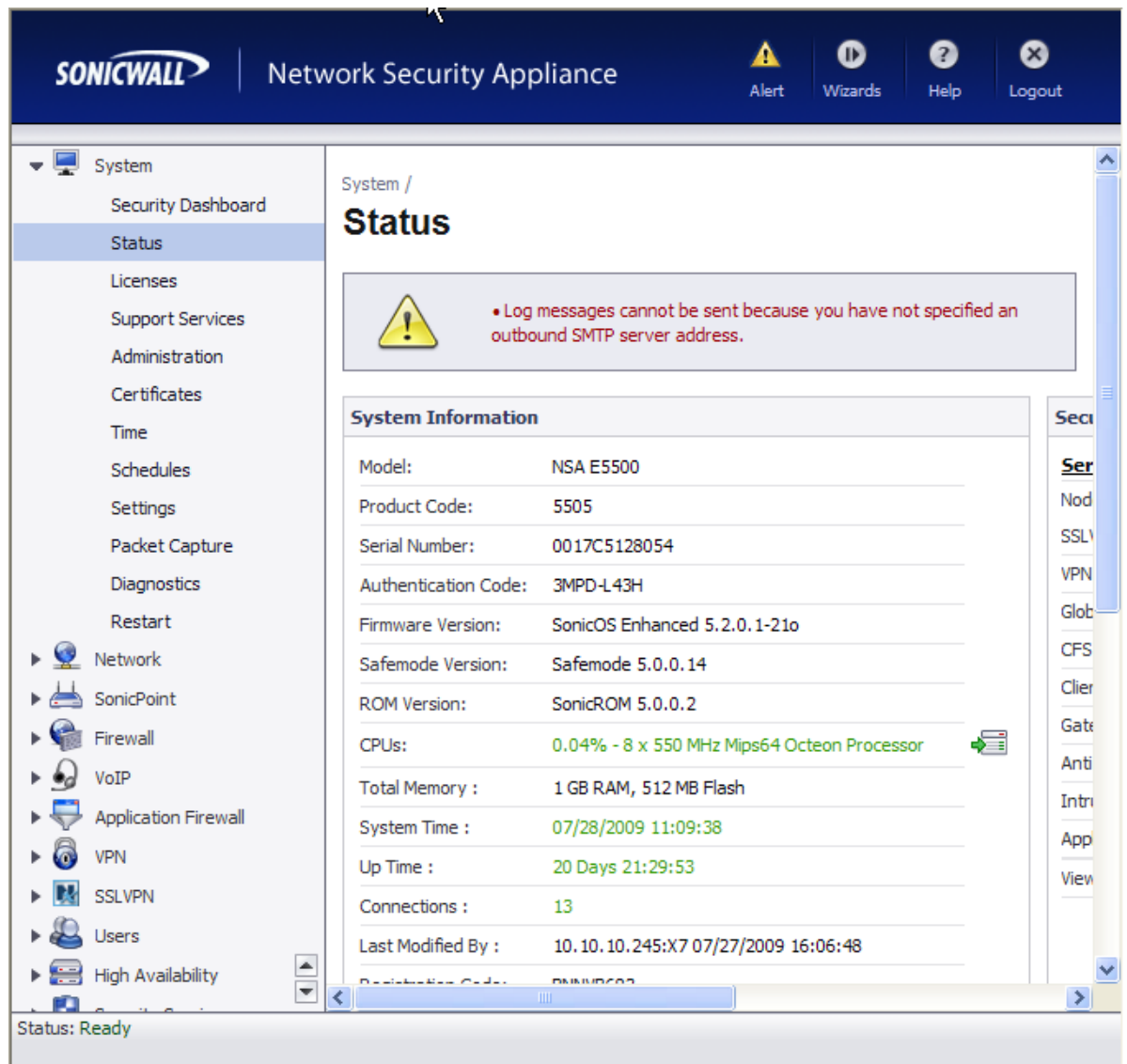
```
change ip-network-region 1                                     Page 1 of 19
                                                                IP NETWORK REGION
    Region: 1
    Location:          Authoritative Domain: devcon.com
    Name:
    MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
        Codec Set: 1      Inter-region IP-IP Direct Audio: yes
        UDP Port Min: 2048      IP Audio Hairpinning? y
        UDP Port Max: 3027
    DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? y
Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46      Use Default Server Parameters? y
        Video PHB Value: 26
    802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 IP ENDPOINTS      RSVP Enabled? n
        H.323 Link Bounce Recovery? y
        Idle Traffic Interval (sec): 20
        Keep-Alive Interval (sec): 5
        Keep-Alive Count: 5
```

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. 

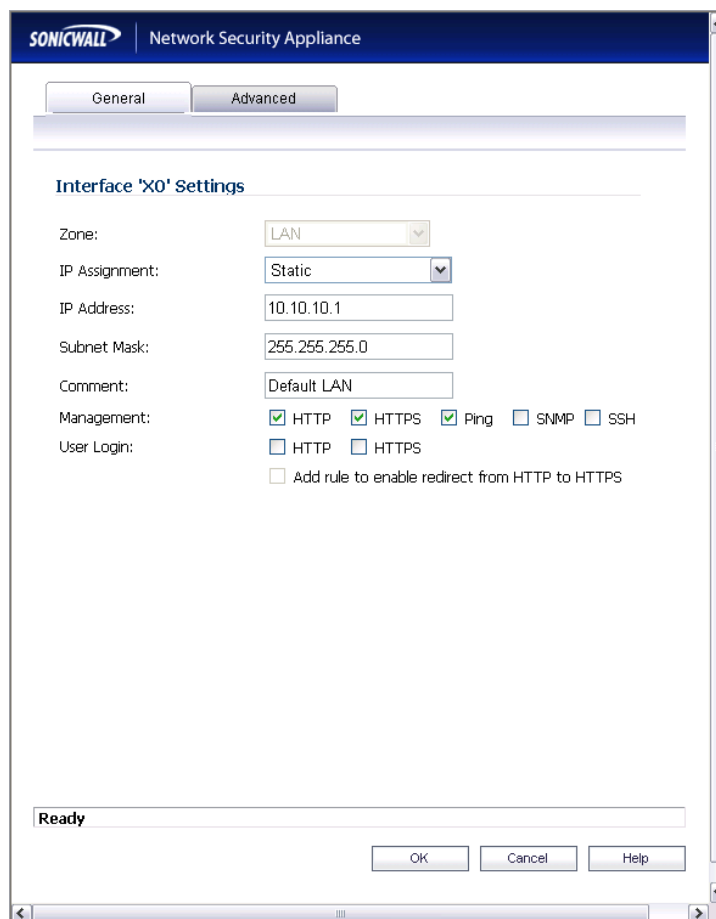
- 5.1.2. The main SonicWall NSA E5500 window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **System**.



5.2. Configure Interfaces:

5.2.1.

From the **Network → Interfaces**, click on the **Configure icon** “” 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.



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

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

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

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

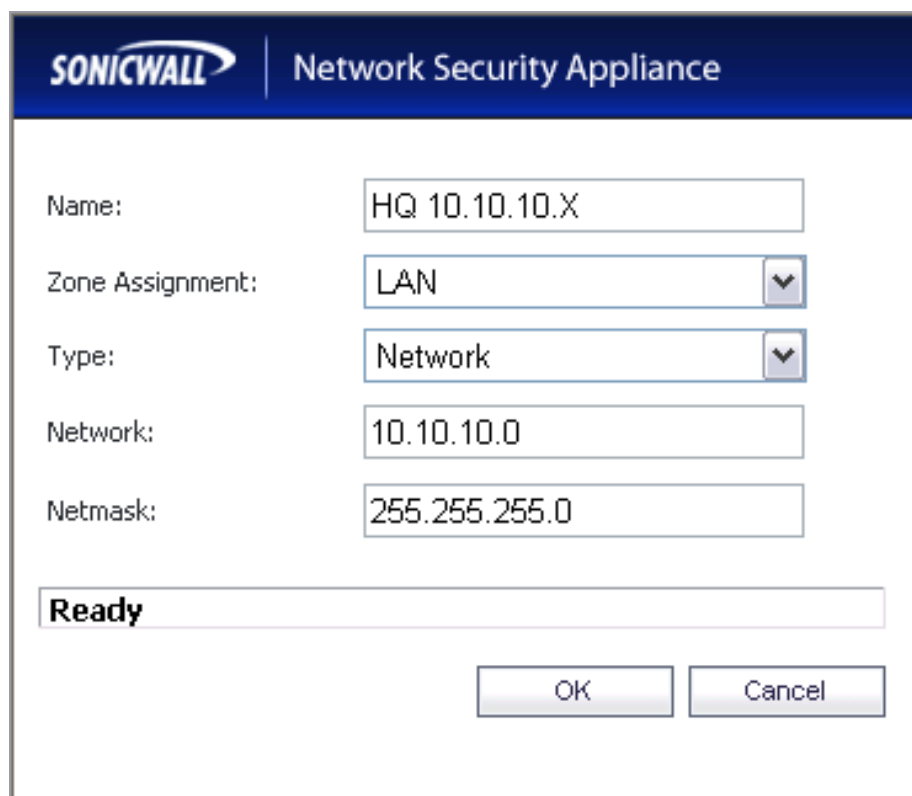
The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, SonicPoint, Firewall, VoIP, Application Firewall, VPN, SSLVPN, Users, High Availability, Security Services, and Log. The main content area is titled 'Network / Interfaces' and features an 'Accept' button. Below this is the 'Interface Settings' table, which lists interfaces X0 through X7 with their respective zones, IP addresses, subnet masks, IP assignments, and status. A 'Add Interface...' button is located below the table. At the bottom of the main content area is the 'Interface Traffic Statistics' table, which provides a summary of traffic statistics for each interface. The status at the bottom left of the interface is 'Ready'.

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	WAN	12.176.170.236	255.255.255.224	Static	100 Mbps full-duplex		

Traffic Statistics	X0	X1	X2	X3	X4	X5	X6	X7
Rx Unicast Packets	2494526	572328	0	0	0	0	0	56504
Rx Broadcast Packets	594589	594591	0	0	0	0	0	1353750
Rx Bytes	426003947	185727346	0	0	0	0	0	123819202
Tx Unicast Packets	1432492	883492	0	0	0	0	0	57463
Tx Broadcast Packets	1477	1891	0	0	0	0	0	150
Tx Bytes	469243654	137139734	0	0	0	0	0	39077954

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.

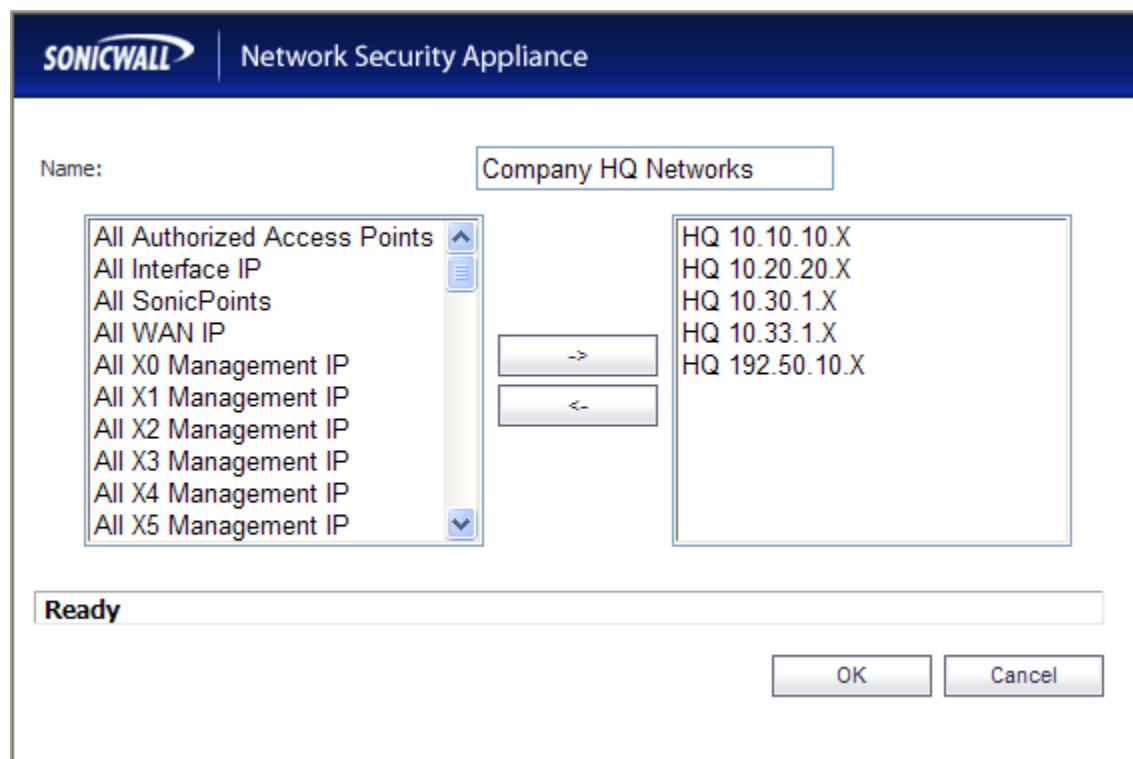
5.3.3. Once all of the Address Objects have been created, the following summary screen is displayed.

#	Name	Address Detail	Type	Zone	Configure	Comments
1	50.50.50.X	50.50.50.0/255.255.255.0	Network	WAN		
2	60.60.60.X	60.60.60.0/255.255.255.0	Network	WAN		
3	80.80.80.X	80.80.80.0/255.255.255.0	Network	WAN		
4	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	LAN		
5	HQ 10.20.20.X	10.20.20.0/255.255.255.0	Network	LAN		
6	HQ 10.30.1.X	10.30.1.0/255.255.255.0	Network	LAN		
7	HQ 10.33.1.X	10.33.1.0/255.255.255.0	Network	LAN		
8	HQ 192.50.10.X	192.50.10.0/255.255.255.0	Network	LAN		
9	HQ Router 10.10.10.2	10.10.10.2/255.255.255.255	Host	LAN		
10	Site A 192.168.130.X	192.168.130.0/255.255.255.0	Network	VPN		
11	Site A 192.168.133.X	192.168.133.0/255.255.255.0	Network	VPN		
12	Site A 30.30.30.X	30.30.30.0/255.255.255.0	Network	VPN		
13	Site B 10.1.1.X	10.1.1.0/255.255.255.0	Network	VPN		
14	Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	VPN		
15	Site B 192.168.33.X	192.168.33.0/255.255.255.0	Network	VPN		
16	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	VPN		
17	Site C 192.168.230.X	192.168.230.0/255.255.255.0	Network	VPN		
18	Site C 192.168.233.X	192.168.233.0/255.255.255.0	Network	VPN		
19	Site C 192.168.77.X	192.168.77.0/255.255.255.0	Network	VPN		
20	Site C 90.90.90.X	90.90.90.0/255.255.255.0	Network	VPN		

Status: **Ready**

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.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, Services, and SonicPoint. The 'Address Objects' link is highlighted. The main content area shows a table of Address Object Groups. At the top of the table are buttons for 'Add Group...', 'Delete', and 'Delete All'. The table has columns for Name, Address Detail, Type, Zone, Configure, and Comments. There are four groups listed: 'Company HQ Networks', 'Remote Site A Networks', 'Remote Site B Networks', and 'Remote Site C Networks'. Each group contains several individual network objects with their respective IP addresses and zones.

#	Name	Address Detail	Type	Zone	Configure	Comments
1	Company HQ Networks		Group			
	HQ 192.50.10.X	192.50.10.0/255.255.255.0	Network	LAN		
	HQ 10.20.20.X	10.20.20.0/255.255.255.0	Network	LAN		
	HQ 10.33.1.X	10.33.1.0/255.255.255.0	Network	LAN		
	HQ 10.30.1.X	10.30.1.0/255.255.255.0	Network	LAN		
	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	LAN		
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	VPN		
	Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	VPN		
	Site B 10.1.1.X	10.1.1.0/255.255.255.0	Network	VPN		
	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	VPN		
4	Remote Site C Networks		Group			
	Site C 192.168.233.X	192.168.233.0/255.255.255.0	Network	VPN		
	Site C 192.168.230.X	192.168.230.0/255.255.255.0	Network	VPN		
	Site C 192.168.77.X	192.168.77.0/255.255.255.0	Network	VPN		
	Site C 90.90.90.X	90.90.90.0/255.255.255.0	Network	VPN		

Status: Ready

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 a 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 10.20.20.X
- Service: Any
- Gateway: HQ Router 10.10.10.2
- Interface: X0
- 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.

SONICWALL Network Security Appliance

Alert Wizards Help Logout

System
Network
Interfaces
WAN Failover & 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

Route Policies Items 1 to 17 (of 17)

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

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
<input type="checkbox"/> 1	Any	0.0.0.0/0	Any	40.40.40.2	X1	20	17		
<input type="checkbox"/> 2	Any	10.10.10.245/32	Any	0.0.0.0	X7	20	4		
<input type="checkbox"/> 3	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	2		
<input checked="" type="checkbox"/> 4	Any	50.50.50.X	Any	Default Gateway	X1	1	7		
<input checked="" type="checkbox"/> 5	Any	60.60.60.X	Any	Default Gateway	X1	1	6		
<input checked="" type="checkbox"/> 6	Any	80.80.80.X	Any	Default Gateway	X1	1	12		
<input type="checkbox"/> 7	X7 Subnet	Any	Any	Secondary Default Gateway	X7	20	15		
<input type="checkbox"/> 8	X1 Subnet	Any	Any	Default Gateway	X1	20	16		
<input type="checkbox"/> 9	Any	Default Gateway	Any	0.0.0.0	X1	20	1		
<input checked="" type="checkbox"/> 10	Any	HQ 10.20.20.X	Any	HQ Router 10.10.10.2	X0	1	8		
<input checked="" type="checkbox"/> 11	Any	HQ 10.30.1.X	Any	HQ Router 10.10.10.2	X0	1	10		
<input checked="" type="checkbox"/> 12	Any	HQ 10.33.1.X	Any	HQ Router 10.10.10.2	X0	1	9		
<input checked="" type="checkbox"/> 13	Any	HQ 192.50.10.X	Any	HQ Router 10.10.10.2	X0	1	11		
<input type="checkbox"/> 14	Any	Secondary Default Gateway	Any	0.0.0.0	X7	20	3		
<input type="checkbox"/> 15	Any	X0 Subnet	Any	0.0.0.0	X0	20	14		
<input type="checkbox"/> 16	Any	X1 Subnet	Any	0.0.0.0	X1	20	13		
<input type="checkbox"/> 17	Any	X7 Subnet	Any	0.0.0.0	X7	20	5		

Add... Delete Delete All

Status: Ready

5.6. Configure VoIP settings.

- 5.6.1.** 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 options: System, Network, SonicPoint, Firewall, VoIP, Settings, Call Status, Application Firewall, VPN, SSLVPN, Users, High Availability, Security Services, and Log. The 'VoIP / Settings' page is displayed. At the top, there is a green 'Accept' button and a grey 'Cancel' button. The settings are organized into sections: 'General Settings' with a checkbox for 'Enable consistent NAT'; 'SIP Settings' with checkboxes for 'Enable SIP Transformations', 'Permit non-SIP packets on signaling port', and 'Enable SIP Back-to-Back User Agent (B2BUA) support', along with 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); and 'H.323 Settings' with a checked checkbox for 'Enable H.323 Transformations', checkboxes for 'Only accept incoming calls from Gatekeeper' and 'Enable LDAP SLS Support', an input field for 'H.323 Signaling/Media inactivity time out (seconds):' (300), and an input field for 'Default WAN/EMC Gatekeeper IP Address:' (0.0.0.0). The status bar at the bottom indicates '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 5.4.1) for the remote site. Click **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 the 'Network' section. The 'Advanced Settings' section contains the following options:

- ☒ 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

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

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.

SONICWALL Network Security Appliance

Alert Wizards Help Logout

System
Network
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: 0017C5128054

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 5 (of 5)

VPN Policies

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
<input type="checkbox"/> 1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input type="checkbox"/> 3	HQ_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"/>	
<input type="checkbox"/> 4	HQ_To_SiteB	50.50.50.1	192.168.33.0 - 192.168.33.255 192.168.30.0 - 192.168.30.255 10.1.1.0 - 10.1.1.255 20.20.20.0 - 20.20.20.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
<input type="checkbox"/> 5	HQ_To_SiteC	80.80.80.1	192.168.233.0 - 192.168.233.255 192.168.230.0 - 192.168.230.255 192.168.77.0 - 192.168.77.255 90.90.90.0 - 90.90.90.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Add... Delete Delete All

Site To Site Policies: 3 Policies Defined, 3 Policies Enabled, 4000 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed


Status: Ready

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**.

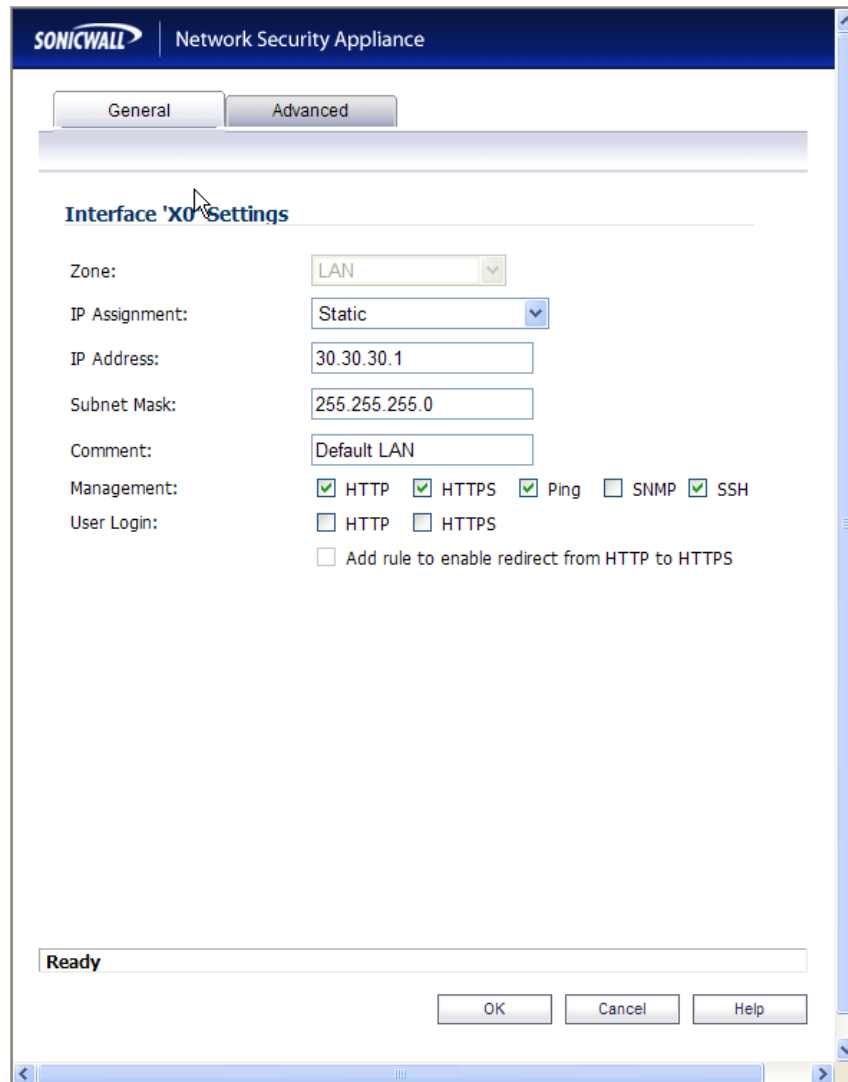
The screenshot displays the SonicWall NSA 240 web interface. The top navigation bar includes the SonicWall logo, the text "Network Security Appliance", and buttons for Register, Wizards, Help, and Logout. The left sidebar shows a Configuration Tree with the "System" category expanded, listing options like Security Dashboard, Status, Licenses, Support Services, Administration, Certificates, Time, Schedules, Settings, Packet Capture, Diagnostics, Restart, 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 features a warning icon and 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 this is a "System Information" table with the following data:

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:	0.01% - 2 x 500 MHz Mips64 Octeon Processor
Total Memory :	256 MB RAM, 32 MB Flash
System Time :	07/28/2009 17:24:46
Up Time :	33 Days 07:58:06
Connections :	13
Last Modified By :	10.10.10.245:X1 07/27/2009 19:19:12
Registration Code:	70071870

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

5.10. Configure Interfaces:

- 5.10.1** From the **Network → Interfaces**, click on the **Configure** icon “” 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.



The screenshot shows the SonicWall Network Security Appliance configuration window for Interface X0 Settings. The window has a title bar with the SonicWall logo and "Network Security Appliance". Below the title bar are two tabs: "General" and "Advanced". The "General" tab is selected. The main content area is titled "Interface 'X0' Settings". It contains the following fields and options:

- Zone: A dropdown menu set to "LAN".
- IP Assignment: A dropdown menu set to "Static".
- IP Address: A text box containing "30.30.30.1".
- Subnet Mask: A text box containing "255.255.255.0".
- Comment: A text box containing "Default LAN".
- Management: A section with checkboxes for HTTP, HTTPS, Ping, SNMP, and SSH. All are checked.
- User Login: A section with checkboxes for HTTP and HTTPS. Both are unchecked.
- Below the checkboxes is an unchecked checkbox labeled "Add rule to enable redirect from HTTP to HTTPS".

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

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

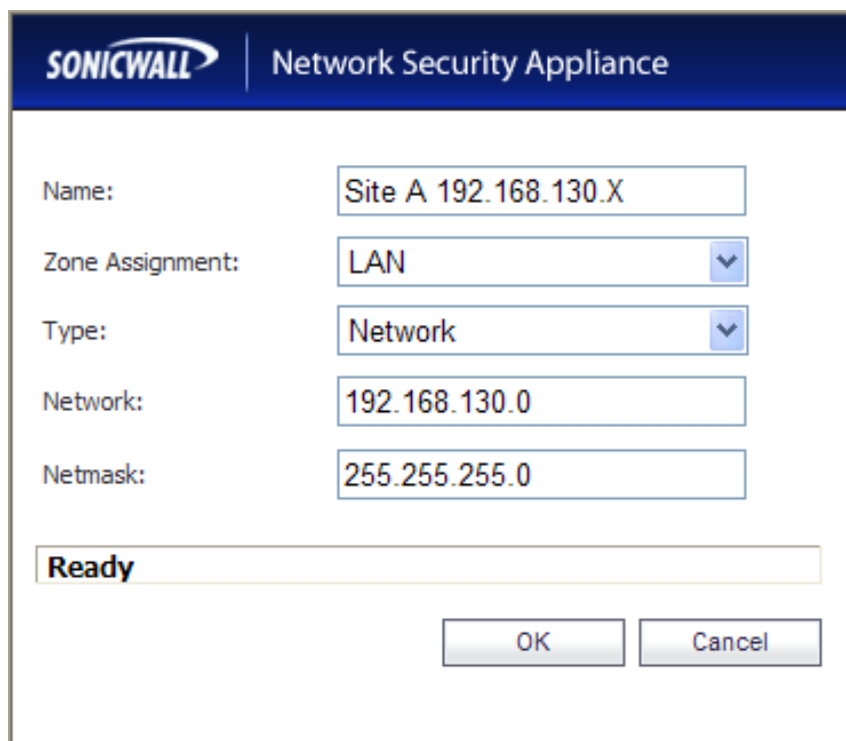
Traffic Statistics	X0	X1	X2	X3	X4	X5	X6	X7	X8	M0
Rx Unicast Packets	459478	812987	0	0	0	0	0	0	0	0
Rx Broadcast Packets	1213764	1535843	0	0	0	0	0	0	0	0
Rx Bytes	236219015	362737541	0	0	0	0	0	0	0	0
Tx Unicast Packets	186313	738922	0	0	0	0	0	0	0	0
Tx Broadcast Packets	2902	4664	0	0	0	0	0	0	0	0
Tx Bytes	27255376	219408134	0	0	0	0	0	0	0	0

Clear

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' with the value 'Site A 192.168.130.X', 'Zone Assignment' with a dropdown menu showing 'LAN', 'Type' with a dropdown menu showing 'Network', 'Network' with the value '192.168.130.0', and 'Netmask' with the value '255.255.255.0'. At the bottom, 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.

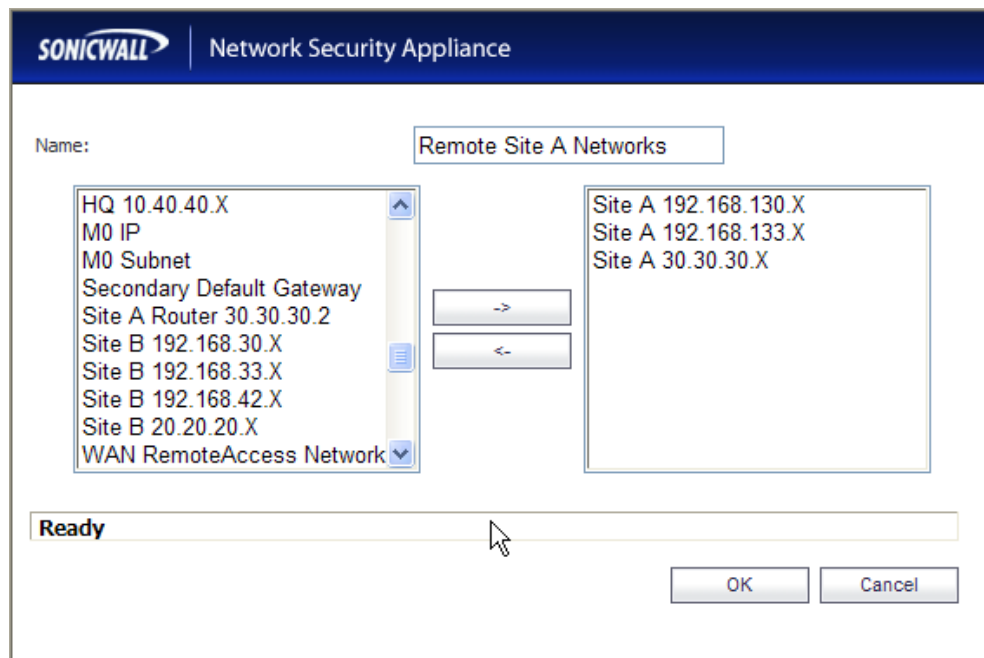
5.11.3 Once all of the Address Objects have been created, the following summary screen is displayed.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, 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, and Log. The main content area is titled 'Remote Site A Networks' and shows a summary of 'Address Objects'. At the top, there are buttons for 'Add Group...', 'Delete', and 'Delete All'. Below this, a table lists 12 address objects. The table has columns for '#', 'Name', 'Address Detail', 'Type', 'Zone', 'Configure', and 'Comments'. The objects are numbered 1 through 12. Objects 1-5 are HQ networks, 6-8 are Site A networks, 9 is Site A Router, 10 is Site B network, 11 is Site B network, and 12 is Site B network. The status bar 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 192.50.10.X	192.50.10.0/255.255.255.0	Network	VPN		
6	Site A 192.168.130.X	192.168.130.0/255.255.255.0	Network	LAN		
7	Site A 192.168.133.X	192.168.133.0/255.255.255.0	Network	LAN		
8	Site A 30.30.30.X	30.30.30.0/255.255.255.0	Network	LAN		
9	Site A Router 30.30.30.2	30.30.30.2/255.255.255.255	Host	LAN		
10	Site B 10.1.1.X	10.1.1.0/255.255.255.0	Network	VPN		
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		

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.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, and Address Objects. The main content area is titled "Address Groups" and shows a summary of configured address object groups. The interface includes a "View Style" selector (All Address Objects, Custom Address Objects, Default Address Objects) and a "Go to Address Objects" link. A table lists the address groups, including "Company HQ Networks", "Remote Site A Networks", and "Remote Site B Networks", with columns for Name, Address Detail, Type, Zone, and Actions (Configure, Delete, Comments). The table shows three groups: "Company HQ Networks" (5 objects), "Remote Site A Networks" (3 objects), and "Remote Site B Networks" (3 objects). Each group is expanded to show its constituent address objects. The bottom of the page shows a status message: "Status: The configuration has been updated." and a "Go to Address Groups" link.

#	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 192.50.10.X	192.50.10.0/255.255.255.0	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 192.168.130.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 10.1.1.X	10.1.1.0/255.255.255.0	Network	VPN		

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 a 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 A 192.168.133.X (dropdown)
- Service: Any (dropdown)
- Gateway: Site A Router 30.30.30.2 (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'.

- 5.13.2** 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: 'Route Policies' and a table of routes.

Route Policies

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

Items 1 to 8 (of 8)

#	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 A 192.168.133.X	Any	Site A Router 30.30.30.2	X0	1	3		
4	Any	Site A 192.168.130.X	Any	Site A Router 30.30.30.2	X0	1	4		
5	Any	X0 Subnet	Any	0.0.0.0	X0	20	5		
6	Any	X1 Subnet	Any	0.0.0.0	X1	20	6		
7	X1 Subnet	Any	Any	Default Gateway	X1	20	7		
8	Any	0.0.0.0/0	Any	60.60.60.2	X1	20	8		

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 like 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 'Enable consistent NAT' checkbox; 'SIP Settings' with checkboxes for 'Enable SIP Transformations', 'Permit non-SIP packets on signaling port', and 'Enable SIP Back-to-Back User Agent (B2BUA) support', along with 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); and 'H.323 Settings' with a checked 'Enable H.323 Transformations' checkbox, checkboxes for 'Only accept incoming calls from Gatekeeper' and 'Enable LDAP ILS Support', an input field for 'H.323 Signaling/Media inactivity time out (seconds)' (300), and an input field for 'Default WAN/DMZ Gatekeeper IP Address' (0.0.0.0). The status bar at the bottom indicates '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 **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 '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.

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 5.4.1) for the remote site. Click **Advanced** tab to continue.

The screenshot displays the SonicWall Network Security Appliance configuration window, specifically the 'Network' tab. The window has a dark blue header with the SonicWall logo and the text 'Network Security Appliance'. Below the header are four tabs: 'General', 'Network' (which is active), 'Proposals', and 'Advanced'. The main content area is divided into two 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 'Remote Site A 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 '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

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
<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 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 - 10.20.20.255 192.50.10.0 - 192.50.10.255 10.10.10.0 - 10.10.10.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
<input 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 10.1.1.0 - 10.1.1.255	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 24 (of 24)


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**.

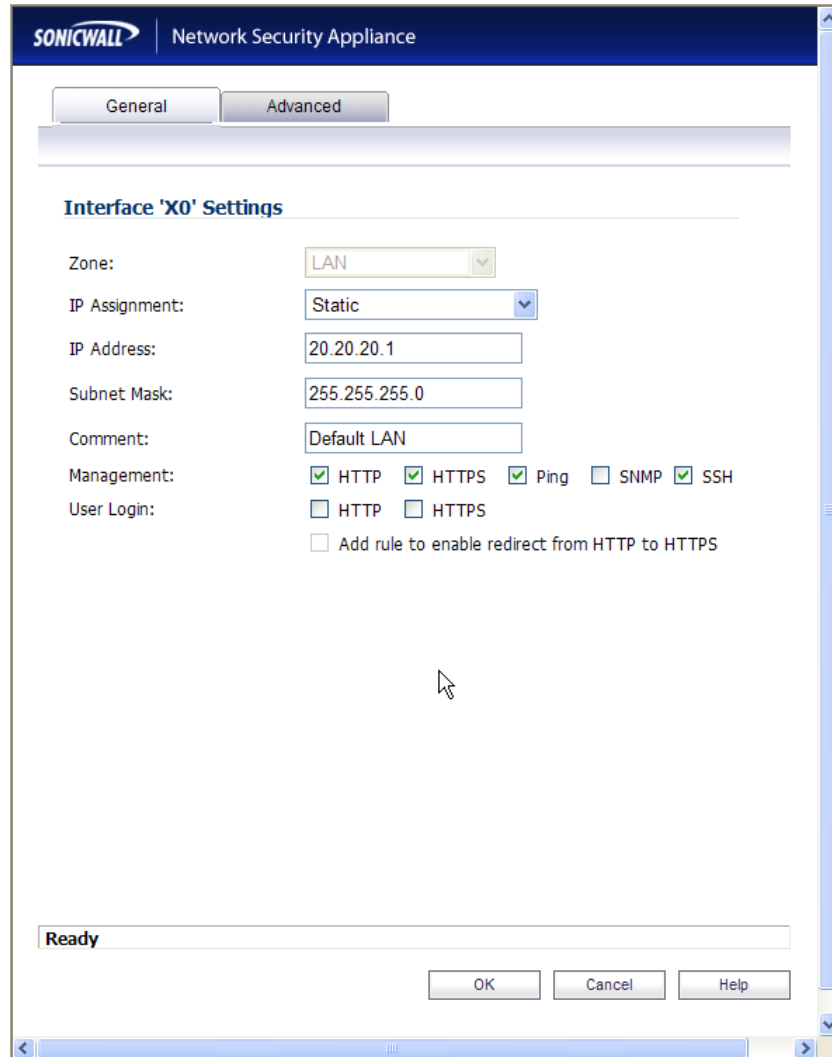
The screenshot displays the SonicWall NSA 240 web interface. The top navigation bar includes the SonicWall logo, the text "Network Security Appliance", and buttons for Register, Wizards, Help, and Logout. The left sidebar shows a Configuration Tree with the "System" category expanded, listing options like Security Dashboard, Status, Licenses, Support Services, Administration, Certificates, Time, Schedules, Settings, Packet Capture, Diagnostics, Restart, 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 features a warning icon and 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 this is a "System Information" table with the following data:

System Information	
Model:	NSA 240
Product Code:	6900
Serial Number:	0017C52BE3F5
Authentication Code:	QGPK-TK7Z
Firmware Version:	SonicOS Enhanced 5.2.0.1-21o
Safemode Version:	Safemode 5.0.1.11
ROM Version:	SonicROM 5.0.2.12
CPU:	0.26% - 2 x 500 MHz Mips64 Octeon Processor
Total Memory :	256 MB RAM, 32 MB Flash
System Time :	07/28/2009 17:56:03
Up Time :	33 Days 08:28:18
Connections :	10
Last Modified By :	10.10.10.245:X1 07/27/2009 19:36:56
Registration Code:	57C30X4M1

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

5.18. Configure Interfaces:

- 5.18.1** From the **Network → Interfaces**, click on the **Configure** icon “” 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.



SONICWALL | Network Security Appliance

General Advanced

Interface 'X0' Settings

Zone:

IP Assignment:

IP Address:

Subnet Mask:

Comment:

Management: ☒ HTTP ☒ HTTPS ☒ Ping ☐ SNMP ☒ SSH

User Login: ☐ HTTP ☐ HTTPS

☐ Add rule to enable redirect from HTTP to HTTPS

Ready

OK Cancel Help

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

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

The screenshot shows the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, and various services. The main content area is titled 'Interfaces' and shows a table of interface settings. Below the table is a section for 'Interface Traffic Statistics'.

Interface Settings

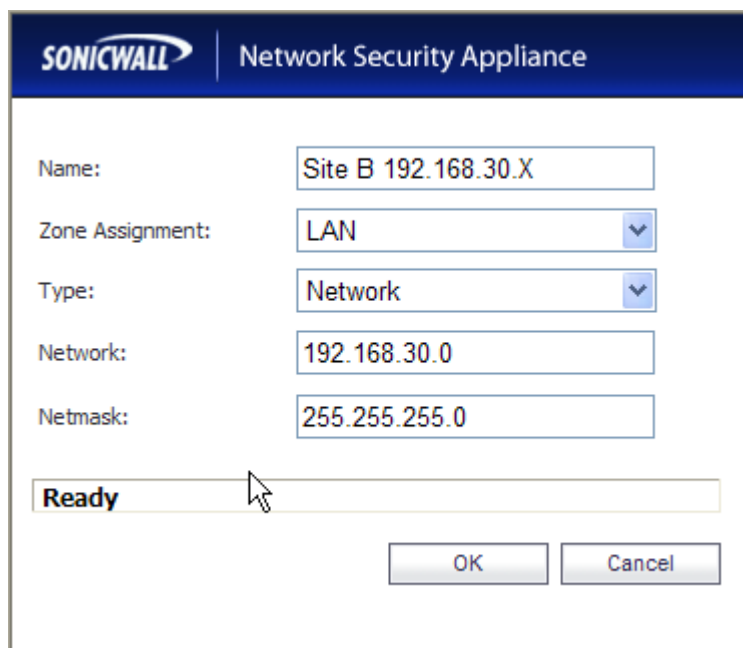
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	20.20.20.1	255.255.255.0	Static	1000 Mbps full-duplex	Default LAN	
X1	WAN	50.50.50.1	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No 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	286859	480593	0	0	0	0	0	0	0	0
Rx Broadcast Packets	1536829	1294025	0	0	0	0	0	0	0	0
Rx Bytes	226000919	248607076	0	0	0	0	0	0	0	0
Tx Unicast Packets	18151	444502	0	0	0	0	0	0	0	0
Tx Broadcast Packets	1323	3585	0	0	0	0	0	0	0	0

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.

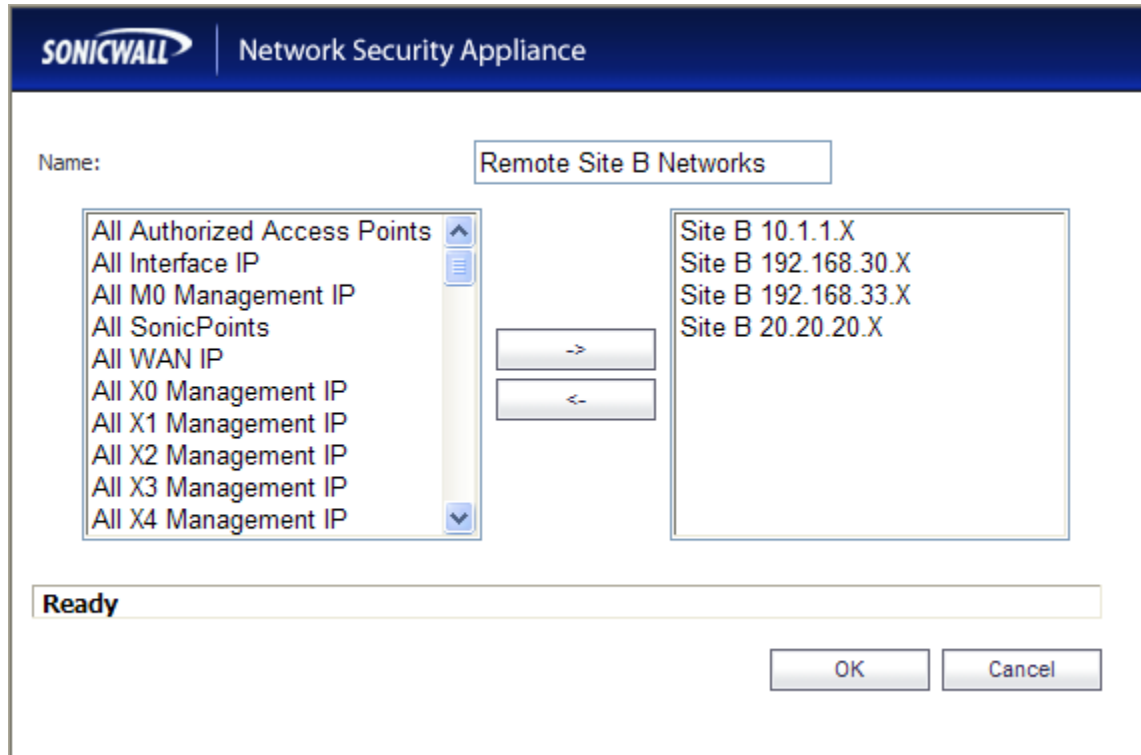
5.19.3 Once all of the Address Objects have been created, the following summary screen is displayed.

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 such as HQ 10.10.10.X, HQ 10.20.20.X, HQ 10.30.1.X, HQ 10.33.1.X, HQ 192.50.10.X, Site A 192.168.130.X, Site A 192.168.133.X, Site A 30.30.30.X, Site B 10.1.1.X, Site B 192.168.30.X, Site B 192.168.33.X, Site B 20.20.20.X, and Site B Router 20.20.20.2. The interface also includes buttons for Add, Delete, Refresh, Purge, Refresh All, Purge All, and Delete All. The status bar at the bottom indicates 'Status: Ready'.

#	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 192.50.10.X	192.50.10.0/255.255.255.0	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 10.1.1.X	10.1.1.0/255.255.255.0	Network	LAN		
10	Site B 192.168.30.X	192.168.30.0/255.255.255.0	Network	LAN		
11	Site B 192.168.33.X	192.168.33.0/255.255.255.0	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.

The screenshot shows the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, 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, and Log. The main content area is titled "Address Objects" and includes a sub-section "Address Groups". It features a "View Style" selector (All Address Objects, Custom Address Objects, Default Address Objects) and a "Go to Address Objects" link. A table lists the address object groups and their details:

#	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 192.50.10.X	192.50.10.0/255.255.255.0	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 10.1.1.X	10.1.1.0/255.255.255.0	Network	LAN		
	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	LAN		

The status at the bottom left is "Status: Ready".

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 a 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 B 192.168.30.X
- Service: Any
- Gateway: Site B Router 20.20.20.2
- Interface: X0
- 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'.

- 5.21.2** Repeat for each LAN subnet.

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

SONICWALL Network Security Appliance

Register Wizards Help Logout

Address Objects

Items 1 to 3 (of 3)

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 192.50.10.X	192.50.10.0/255.255.255.0	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 10.1.1.X	10.1.1.0/255.255.255.0	Network	LAN		
	Site B 20.20.20.X	20.20.20.0/255.255.255.0	Network	LAN		

Add Group... Delete

Delete All

Status: Ready

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 shows the SonicWall Network Security Appliance interface. The left sidebar contains a navigation menu with options: System, Network, PC Card, SonicPoint, Firewall, VoIP, Settings (selected), Call Status, Application Firewall, VPN, SSLVPN, Users, High Availability, Security Services, and Log. The main content area is titled 'VoIP / Settings' and features an 'Accept' button and a 'Cancel' button. Below this, the 'General Settings' section includes a checkbox for 'Enable consistent NAT'. The 'SIP Settings' section includes a checkbox for 'Enable SIP Transformations', a checkbox for 'Permit non-SIP packets on signaling port', a checkbox for 'Enable SIP Back-to-Back User Agent (B2BUA) support', and three input fields: '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 includes a checked checkbox for 'Enable H.323 Transformations', a checkbox for 'Only accept incoming calls from Gatekeeper', a checkbox for 'Enable LDAP ILS Support', an input field for 'H.323 Signaling/Media inactivity time out (seconds): 300', and an input field for '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 **Network** tab to continue.

The screenshot shows the 'Add' VPN policy configuration window on a SonicWALL Network Security Appliance. The window has a title bar with the SonicWALL logo and 'Network Security Appliance'. Below the title bar are four tabs: 'General', 'Network', 'Proposals', and 'Advanced'. The 'General' tab is selected. The 'Security Policy' section contains the following fields: 'Authentication Method' (a dropdown menu set to 'IKE using Preshared Secret'), 'Name' (a text box containing 'SiteB_To_HQ'), 'IPsec Primary Gateway Name or Address' (a text box containing '40.40.40.1'), and 'IPsec Secondary Gateway Name or Address' (a text box containing '0.0.0.0'). The 'IKE Authentication' section contains: 'Shared Secret' and 'Confirm Shared Secret' (both masked with dots), a checked checkbox for 'Mask Shared Secret', 'Local IKE ID' (a dropdown menu set to 'IP Address' and an empty text box), and 'Peer IKE ID' (a dropdown menu set to 'IP Address' and an empty text box). At the bottom, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

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 5.4.1) for the remote site. Click **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".

Local Networks

- ☒ Choose local network from list: Remote Site B 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.

5.23.3**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 interface. At the top, there are tabs for General, Network, Proposals, and Advanced. The Advanced tab is selected. Below the tabs, the title "Advanced Settings" is displayed. 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 menu 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:", the "HTTP" and "HTTPS" checkboxes are checked, and the "SSH" checkbox is unchecked. Under "User login via this SA:", the "HTTP" and "HTTPS" checkboxes are unchecked. The "Default LAN Gateway (optional)" field is set to "0.0.0.0". The "VPN Policy bound to:" dropdown menu is set to "Zone WAN". At the bottom, there is a "Ready" status bar and three buttons: "OK", "Cancel", and "Help".

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.

SONICWALL | Network Security Appliance

Register | Wizards | Help | Logout

System | Network | PC Card | SonicPoint | Firewall | VoIP | Application Firewall | **VPN**

Settings | Advanced | DHCP over VPN | LZTP Server | SSLVPN | Users | High Availability | Security Services | Log

VPN / **Settings**

Accept | Cancel

VPN Global Settings

☒ Enable VPN

Unique Firewall Identifier: 0017C52BE3F5

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 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 - 10.20.20.255 192.50.10.0 - 192.50.10.255 10.10.10.0 - 10.10.10.255	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
<input 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 29 (of 29)


Status: **Ready**

5.24. Save settings

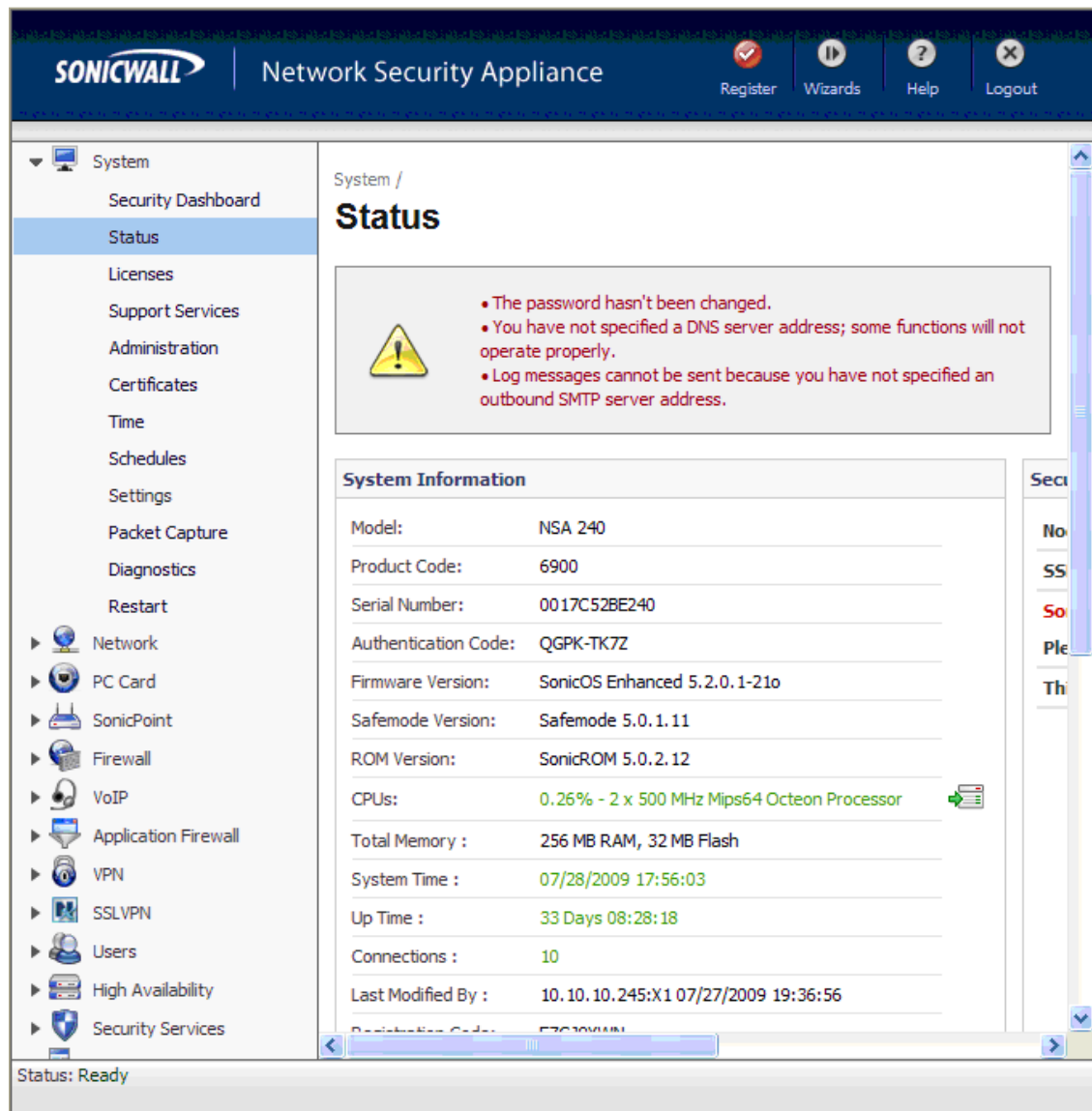
- 5.24.1** Save settings
From the **System > Settings**, click on the **Export Settings** button to save the SonicWALL appliance configuration.




5.25. Configure SonicWall NSA 240 (Remote Site C)

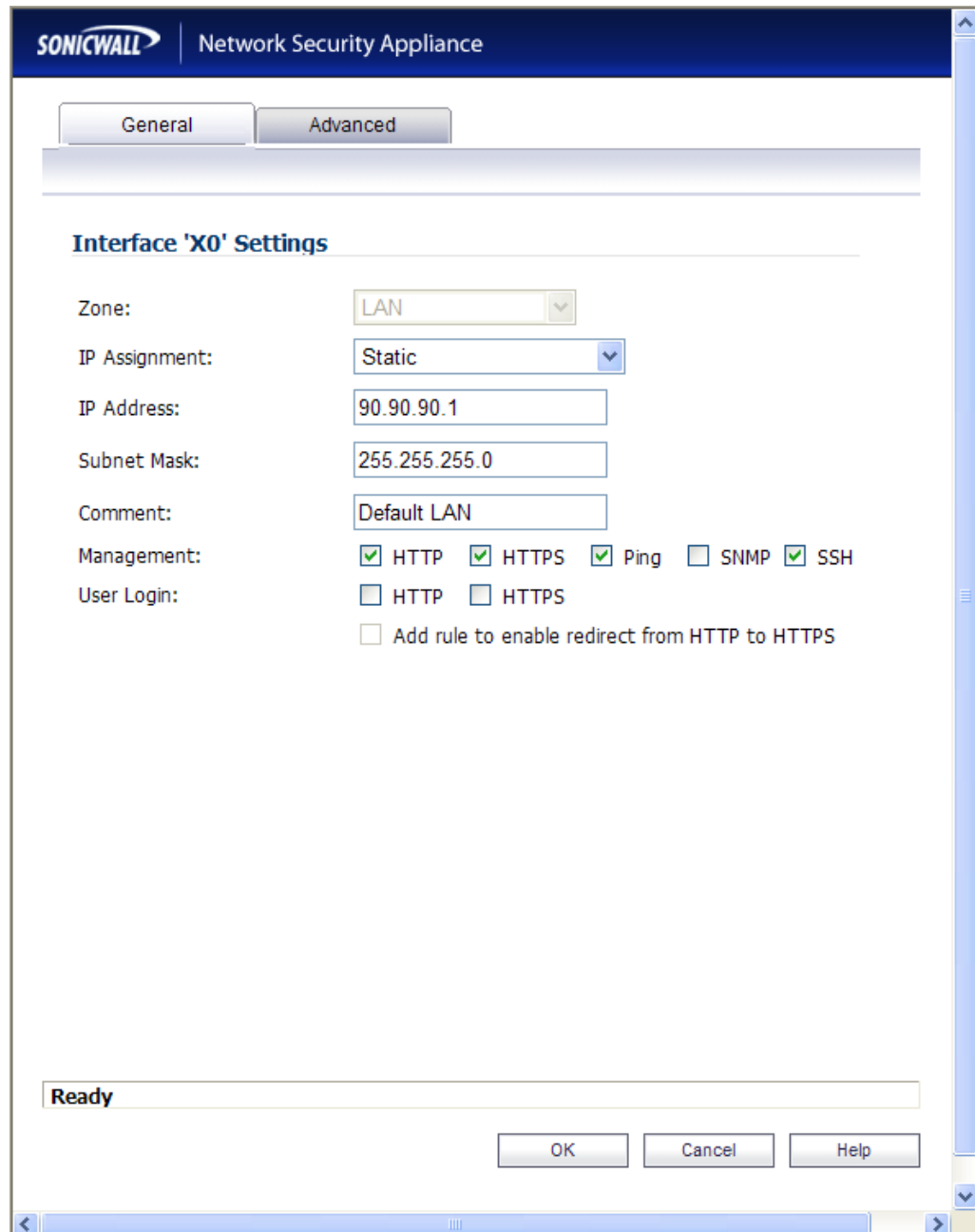
Step	Description
5.25.1	<p>Configure the SonicWall NSA 240 at Remote Site C using the built-in web-based Management Tool. Access this tool by establishing a web browser connection to the SonicWall NSA 240. Refer to Section 9 [6].</p> <p>Log into the Remote Site C SonicWall NSA 240.</p> <ol style="list-style-type: none">4. Connect the LAN port of the computer being used to the X0 (LAN) port on the SonicWall NSA 240.5. Start the Management Tool as follows: Start your web browser and enter http://192.168.168.168 Press Enter.6. Log in to the SonicWall NSA 240 using default credentials which can be obtained from the SonicWALL documentation. 

5.25.2 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**.



5.26. Configure Interfaces:

- 5.26.1** From the **Network → Interfaces**, click on the **Configure icon** “” 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.



SONICWALL Network Security Appliance

General Advanced

Interface 'X0' Settings

Zone: LAN

IP Assignment: Static

IP Address: 90.90.90.1

Subnet Mask: 255.255.255.0

Comment: Default LAN

Management: ☒ HTTP ☒ HTTPS ☒ Ping ☐ SNMP ☒ SSH

User Login: ☐ HTTP ☐ HTTPS

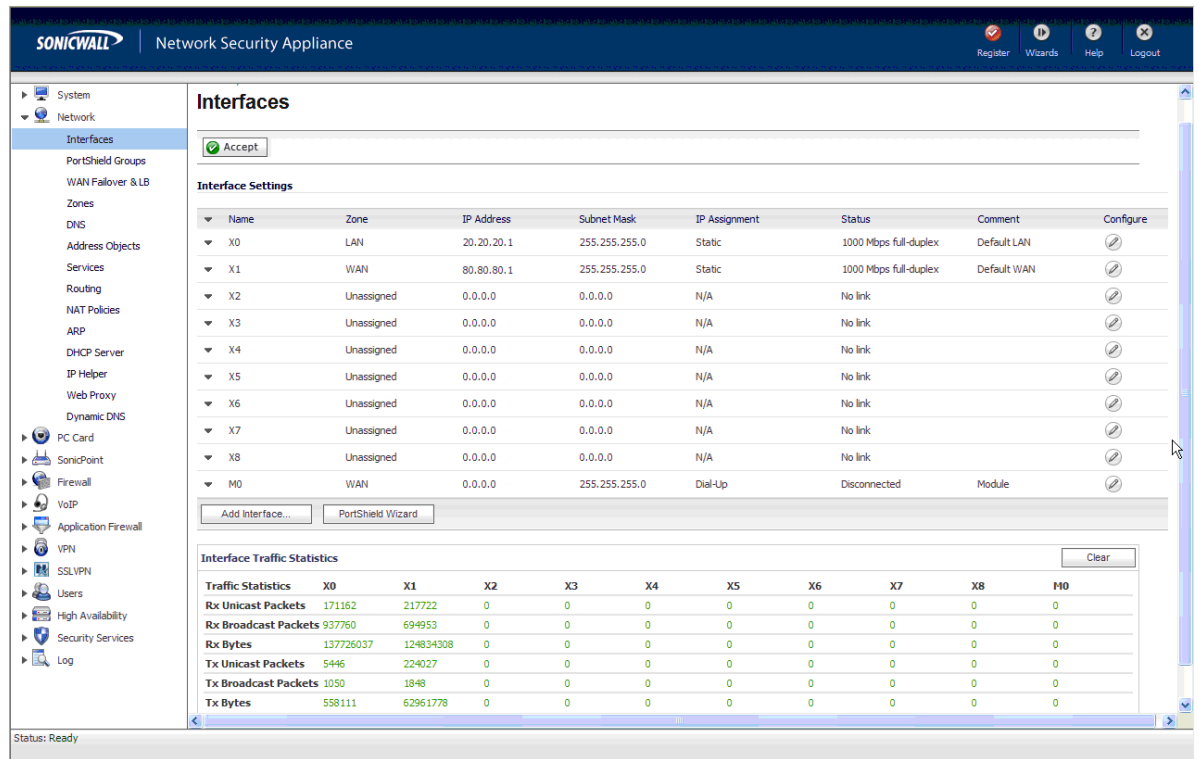
☐ Add rule to enable redirect from HTTP to HTTPS

Ready

OK Cancel Help

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

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



SonicWall Network Security Appliance

Register Wizards Help Logout

System
Network
Interfaces
PortShield Groups
WAN Failover & 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

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	Configure
X1	WAN	80.80.80.1	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	Configure
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		Configure
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		Configure
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		Configure
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		Configure
X6	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		Configure
X7	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		Configure
X8	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		Configure
M0	WAN	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	Configure

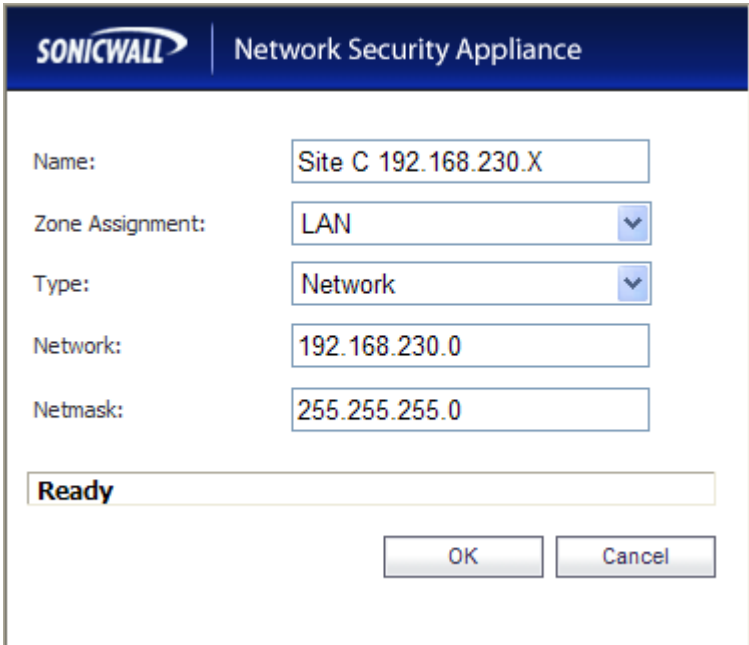
Add Interface... PortShield Wizard

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

5.27. Define networks


5.27.1	<p>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.</p>
	
5.27.2	<p>Repeat Step 5.27.1 for each subnet in the topology. Refer to Figure 1 for details of topology used for compliance testing.</p>

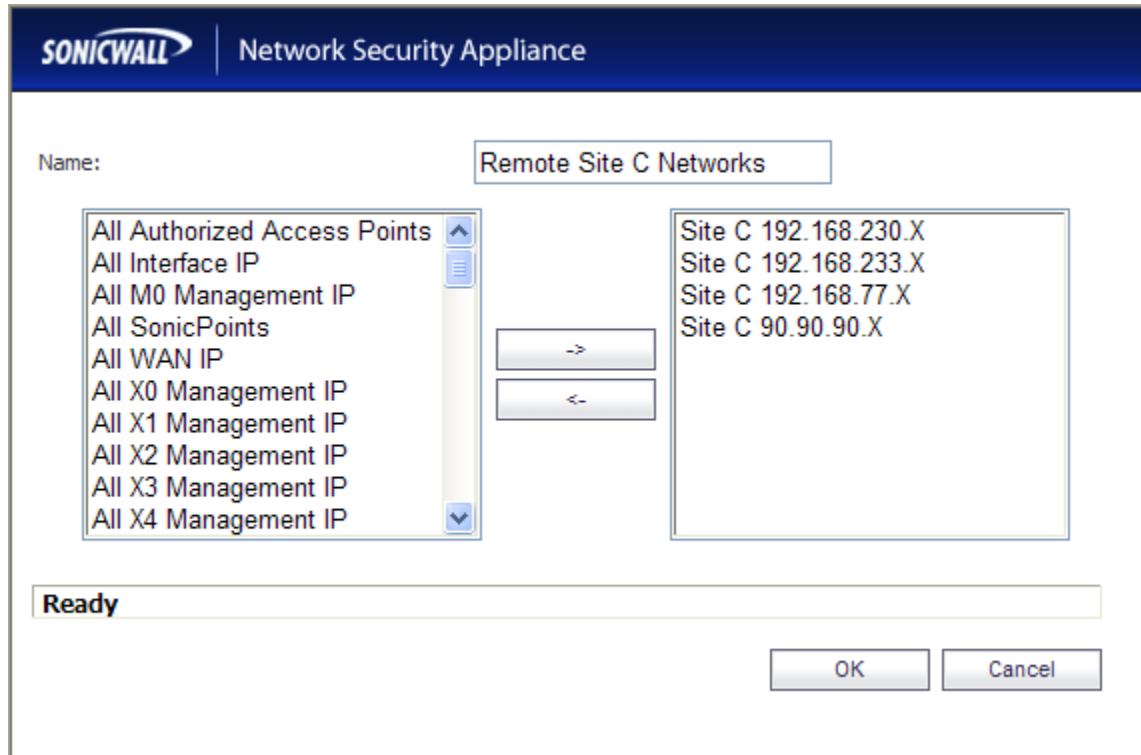
5.27.3 Once all of the Address Objects have been created, the following summary screen is displayed.

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with categories like System, Network, and Firewall. The main content area is titled 'Address Objects' and shows a summary of 10 objects. The objects are listed in a table with columns for #, Name, Address Detail, Type, Zone, Configure, and Comments. The objects include HQ networks, Site C networks, and a Site C Router. The interface also includes buttons for 'Add...', 'Delete', 'Refresh', and 'Purge' for the objects, and 'Refresh All', 'Purge All', and 'Delete All' for the entire list. The status at the bottom left is 'Status: Ready'.

#	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 192.50.10.X	192.50.10.0/255.255.255.0	Network	VPN		
6	Site C 192.168.230.X	192.168.230.0/255.255.255.0	Network	LAN		
7	Site C 192.168.233.X	192.168.233.0/255.255.255.0	Network	LAN		
8	Site C 192.168.77.X	192.168.77.0/255.255.255.0	Network	LAN		
9	Site C 90.90.90.X	90.90.90.0/255.255.255.0	Network	LAN		
10	Site C Router 90.90.90.2	90.90.90.2/255.255.255.255	Host	LAN		

5.28. Group Address Objects based on site within topology

- 5.28.1** 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 5.27.1) and click  to add to group.



SONICWALL | Network Security Appliance

Name: Remote Site C Networks

All Authorized Access Points
All Interface IP
All M0 Management IP
All SonicPoints
All WAN IP
All X0 Management IP
All X1 Management IP
All X2 Management IP
All X3 Management IP
All X4 Management IP

Site C 192.168.230.X
Site C 192.168.233.X
Site C 192.168.77.X
Site C 90.90.90.X

Ready

OK Cancel

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

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

SONICWALL | Network Security Appliance

Register Alert 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

Network /
Address Objects

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 192.50.10.X	192.50.10.0/255.255.255.0	Network	VPN		
	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	VPN		
2	Remote Site C Networks		Group			
	Site C 192.168.233.X	192.168.233.0/255.255.255.0	Network	LAN		
	Site C 192.168.230.X	192.168.230.0/255.255.255.0	Network	LAN		
	Site C 192.168.77.X	192.168.77.0/255.255.255.0	Network	LAN		
	Site C 90.90.90.X	90.90.90.0/255.255.255.0	Network	LAN		

Add Group... Delete

Address Objects

Status: Ready

5.29. 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.

- 5.29.1** From the **Network → Routing**, click on the **Add** button and enter a 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 C 192.168.233.X
- Service: Any
- Gateway: Site C Router 90.90.90.2
- 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 are buttons for 'OK', 'Cancel', and 'Help'.

- 5.29.2** Repeat for each LAN subnet.

5.29.3 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 routes. The table has columns for #, Source, Destination, Service, Gateway, Interface, Metric, Priority, Comment, and Configure. There are 9 routes listed, including a default gateway and specific subnets. The status at the bottom is 'Ready'.

#	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	80.80.80.2	X1	20	9		

5.30. Configure VoIP settings.

5.30.1 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 options: System, Network, PC Card, SonicPoint, Firewall, VoIP, Settings (selected), Call Status, Application Firewall, VPN, SSLVPN, Users, High Availability, Security Services, and Log. The main content area is titled 'VoIP / Settings' and features an 'Accept' button with a green checkmark and a 'Cancel' button. Below this are three sections: 'General Settings' with an unchecked 'Enable consistent NAT' checkbox; 'SIP Settings' with an unchecked 'Enable SIP Transformations' checkbox, sub-options for 'Permit non-SIP packets on signaling port' and 'Enable SIP Back-to-Back User Agent (B2BUA) support', and 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'; and 'H.323 Settings' with a checked 'Enable H.323 Transformations' checkbox, sub-options for 'Only accept incoming calls from Gatekeeper' and 'Enable LDAP ILS Support', and 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 left indicates 'Status: Ready'.

5.31. Create VPN policies

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

5.31.1 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 'Security Policy' configuration window for a SonicWALL Network Security Appliance. The window has a dark blue header with the SonicWALL logo and the text 'Network Security Appliance'. Below the header are four tabs: 'General', 'Network', 'Proposals', and 'Advanced'. The 'Network' tab is selected. The main content area is titled 'Security Policy' and contains the following fields:

- Authentication Method:** A dropdown menu set to 'IKE using Preshared Secret'.
- Name:** A text box containing 'SiteC_To_HQ'.
- IPsec Primary Gateway Name or Address:** A text box containing '40.40.40.1'.
- IPsec Secondary Gateway Name or Address:** A text box containing '0.0.0.0'.

Below these fields is a section titled 'IKE Authentication' with the following fields:

- Shared Secret:** A text box with masked characters (dots).
- Confirm Shared Secret:** A text box with masked characters (dots).
- Mask Shared Secret:** A checkbox that is checked.
- Local IKE ID:** A dropdown menu set to 'IP Address' and an empty text box.
- Peer IKE ID:** A dropdown menu set to 'IP Address' and an empty text box.

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

5.31.2

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 5.4.1) for the remote site. Click **Advanced** tab to continue.

SONICWALL | Network Security Appliance

General Network Proposals **Advanced**

Local Networks

☒ Choose local network from list Remote Site C 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 ▼

Ready

OK Cancel Help

5.31.3**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 interface. At the top, there are tabs for General, Network, Proposals, and Advanced. The Advanced tab is selected. Below the tabs, the title "Advanced Settings" is displayed. The settings are as follows:

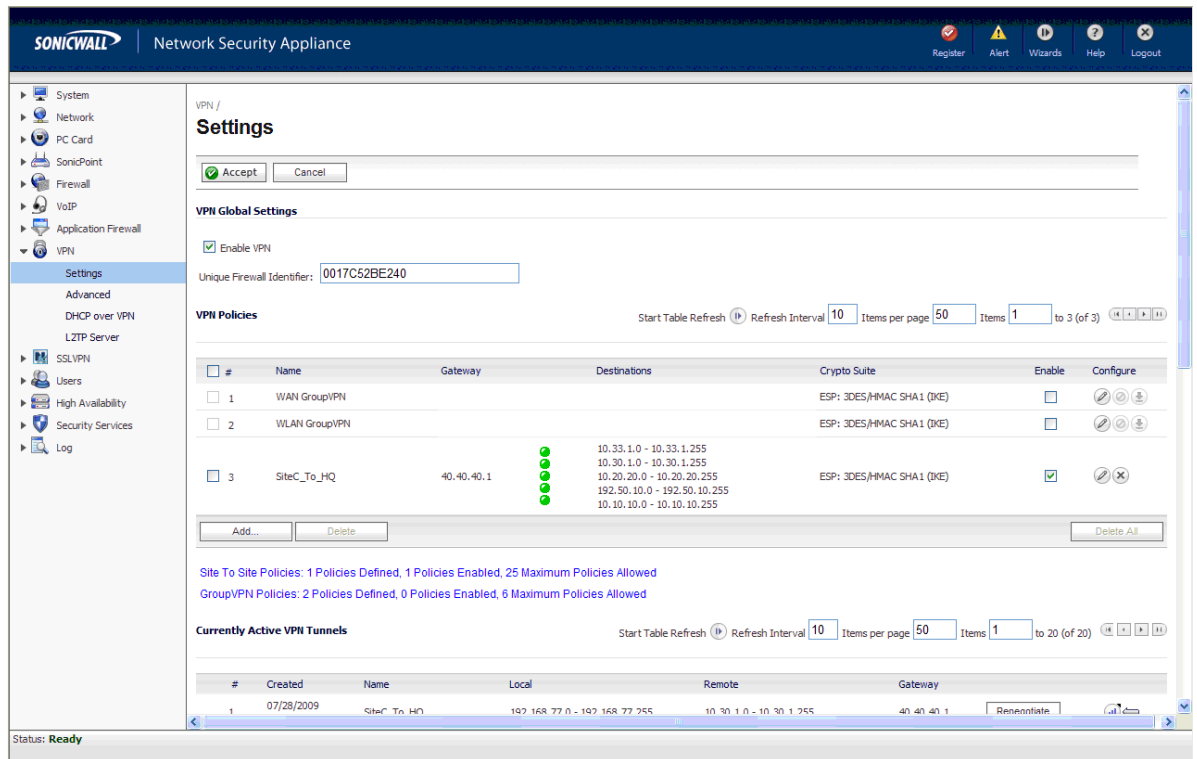
- ☒ Enable Keep Alive
- ☐ Suppress automatic Access Rules creation for VPN Policy
- ☐ Require authentication of VPN clients by XAUTH
 - User group for XAUTH users: --Select a user group--
- ☐ Enable Windows Networking (NetBIOS) Broadcast
- ☐ Enable Multicast
- ☐ Apply NAT Policies
 - Translated Local 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

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

5.31.4

Repeat Steps 5.31.1, 5.31.2 and 5.31.3 for each **VPN policy** within the network structure.

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



5.32. Save settings

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



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 Remote Site C Avaya G700 Media Gateway registers with the corporate Avaya Communication Manager.
- Verify H.323 trunk between the corporate Communication Manager and Remote Site B Communication Manager.
- Registration of Remote Site A SIP IP telephones with corporate SES.
- Registration of Remote Site A H.323 IP telephones with corporate Communication Manager.
- Inter-office calls using G.711 mu-law & G.729 codecs
- Verifying that DSCP and 802.1p Priority QoS values are not altered by the SonicWALL firewall VPNs.
- Verifying that Avaya Modular Messaging voicemail and MWI work properly.
- Verifying that Avaya IA 770 INTUITY AUDIX voicemail 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, and bridged call appearances.

6.2. Test Results

All feature functionality, serviceability, and performance test cases passed. VoIP traffic and voice features worked properly while running through the SonicWALL UTM Firewall VPNs.

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. Check that the Avaya SIP IP telephones have successfully registered with Avaya SIP Enablement Services (SES) through the SES administrative GUI.
3. 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. 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.

The following Avaya product documentation can be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura™ Communication Manager*, May 2009, Issue 5.0, Document Number 03-300509.
- [2] *Administering Avaya Aura™ SIP Enablement Services*, May 2009, Issue 2.1, Document 03-602508.
- [3] *Avaya Aura™ SIP Enablement Services (SES) Implementation Guide*, May 2009, Issue 6, Document 16-300140.
- [4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.0*, Document Number 16-300698.
- [5] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.0*, Document Number 16-601944.
- [6] *Modular Messaging, Release 5.0 with the Avaya MSS Messaging Application Server (MAS) Administration Guide*, January 2009.
- [7] *Avaya IA 770 INTUITY AUDIX Messaging Application Release 5.1 Administering. Communication Manager Servers to Work with IA 770*, June 2008.

The SonicWALL product documentation can be found at

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

10. Change History

Issue	Date	Reason
1.0	8/19/09	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.