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.

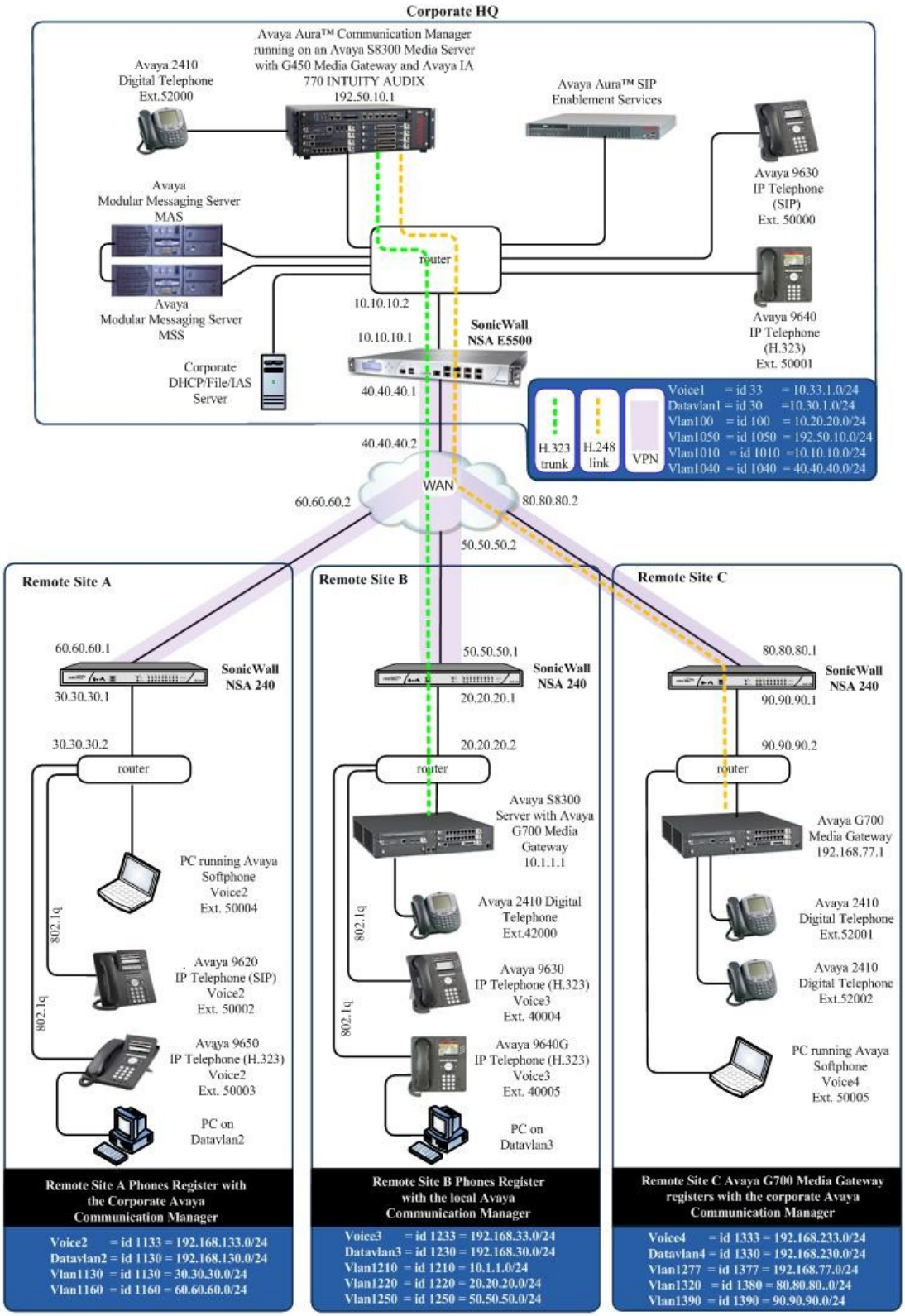


Figure 1: Sample Network Configuration

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

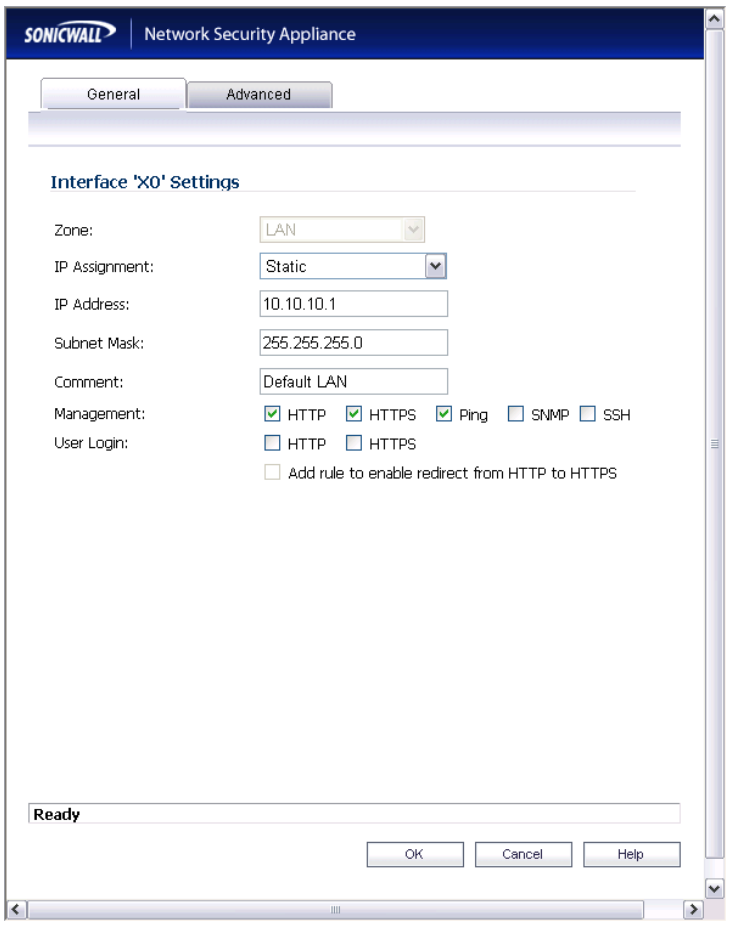
5.1. Configure SonicWall NSA E5500 (Corporate Headquarters)

Step	Description
5.1.1.	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]. Log into the NSA 5500. 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. 

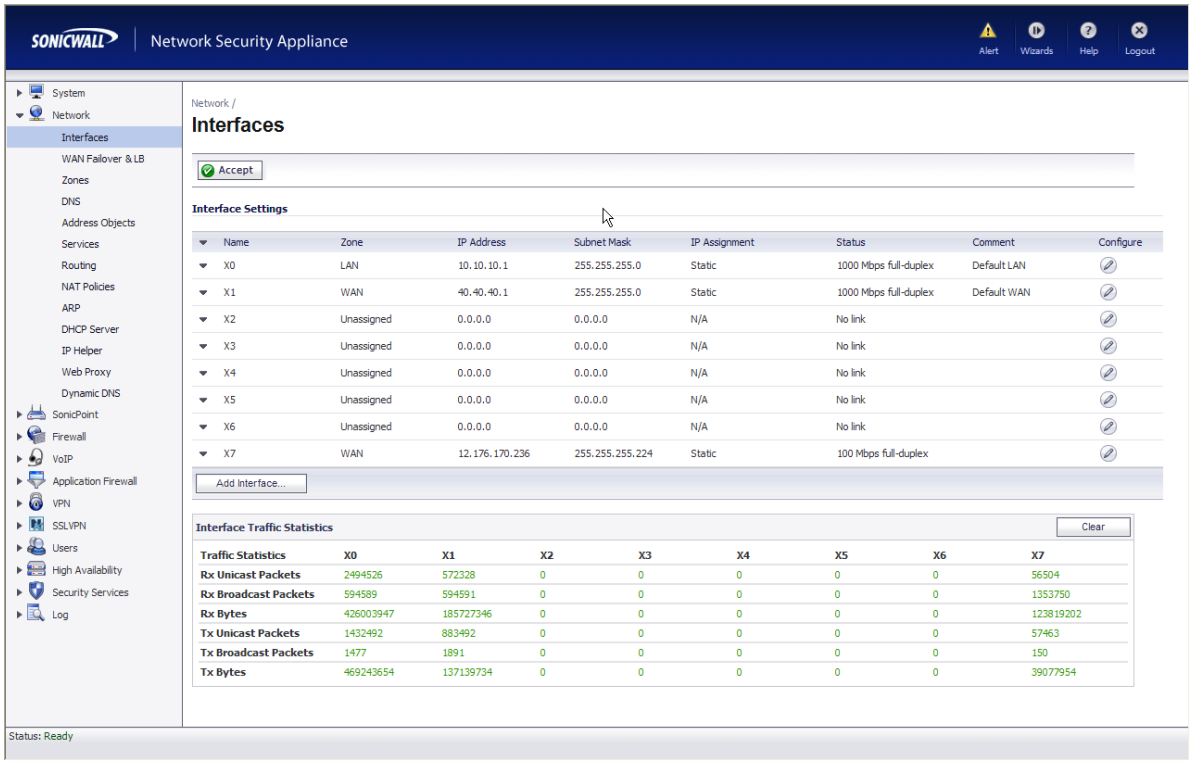
5.1.2. The main SonicWall NSA E5500 window appears. The following steps refer to the Configuration Tree which is in the left pane of the window and under the heading **System**.

5.2. Configure Interfaces:

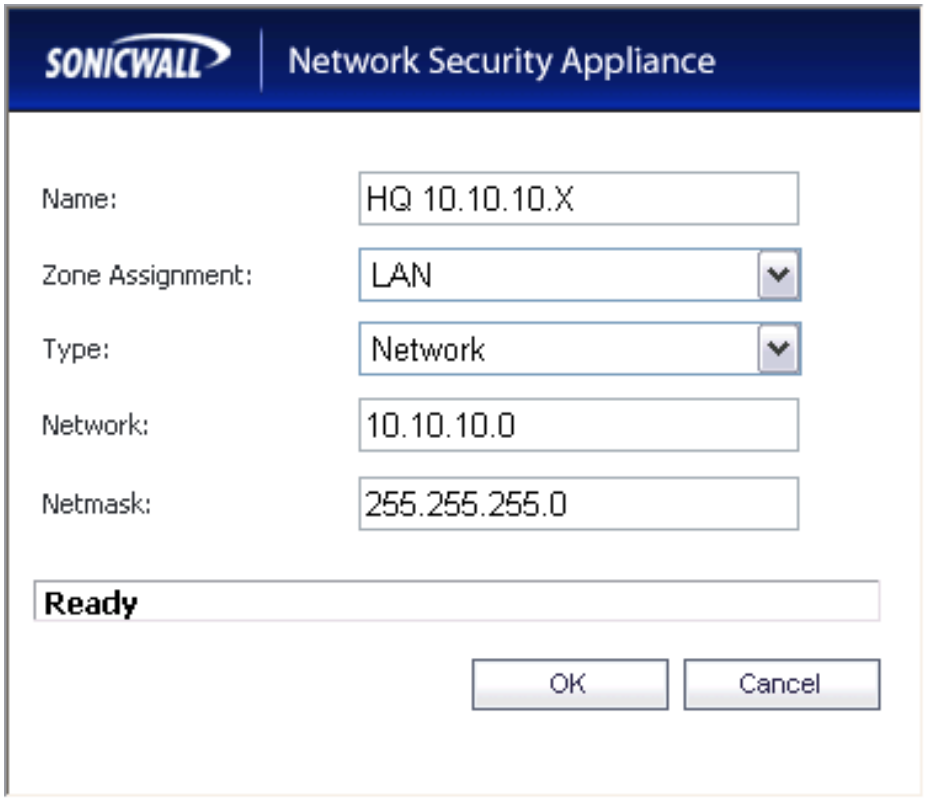
5.2.1. From the **Network → Interfaces,** click on the **Configure icon** " " for **X0** (LAN) and enter the following information for: **IP Assignmen**t, I**P Addres**s and **Subnet Mask** according to network structure to be used, Click **OK** to continue.



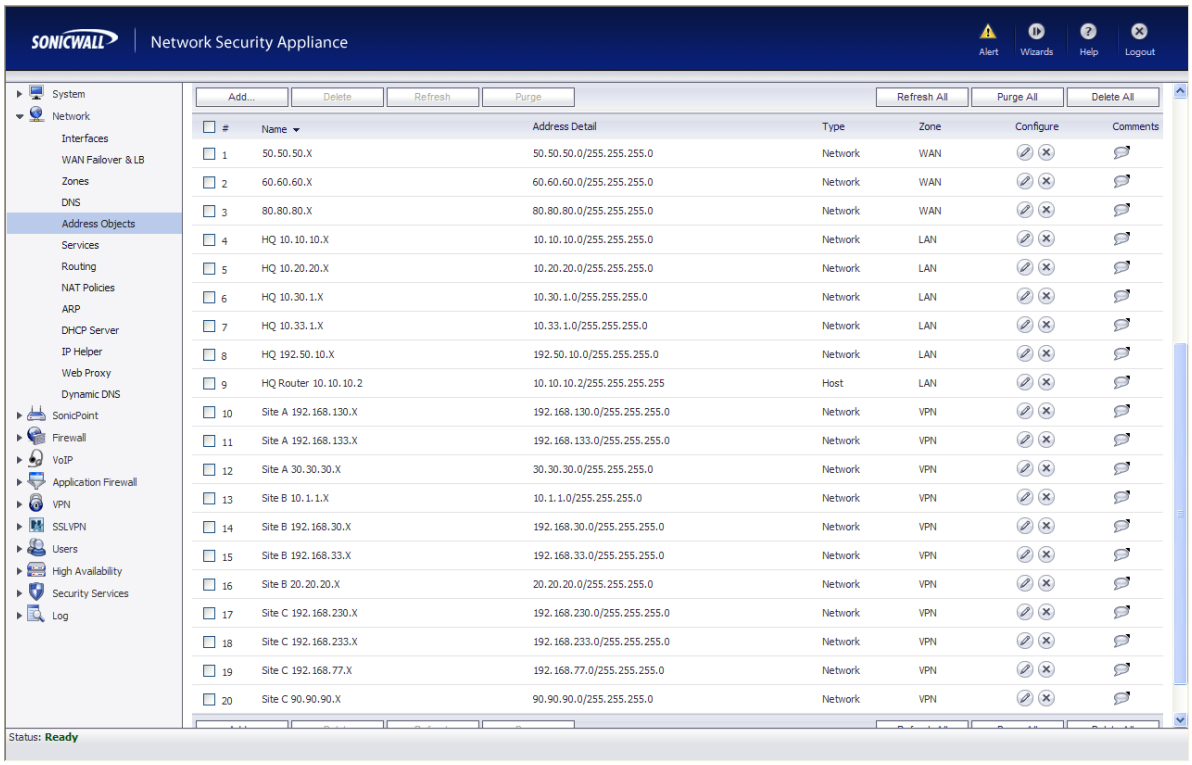
5.2.2.	Repeat for the **X1** (WAN) interface.
5.2.3.	Once configuration on the interfaces is completed, the following summary is presented.



5.3. Define networks

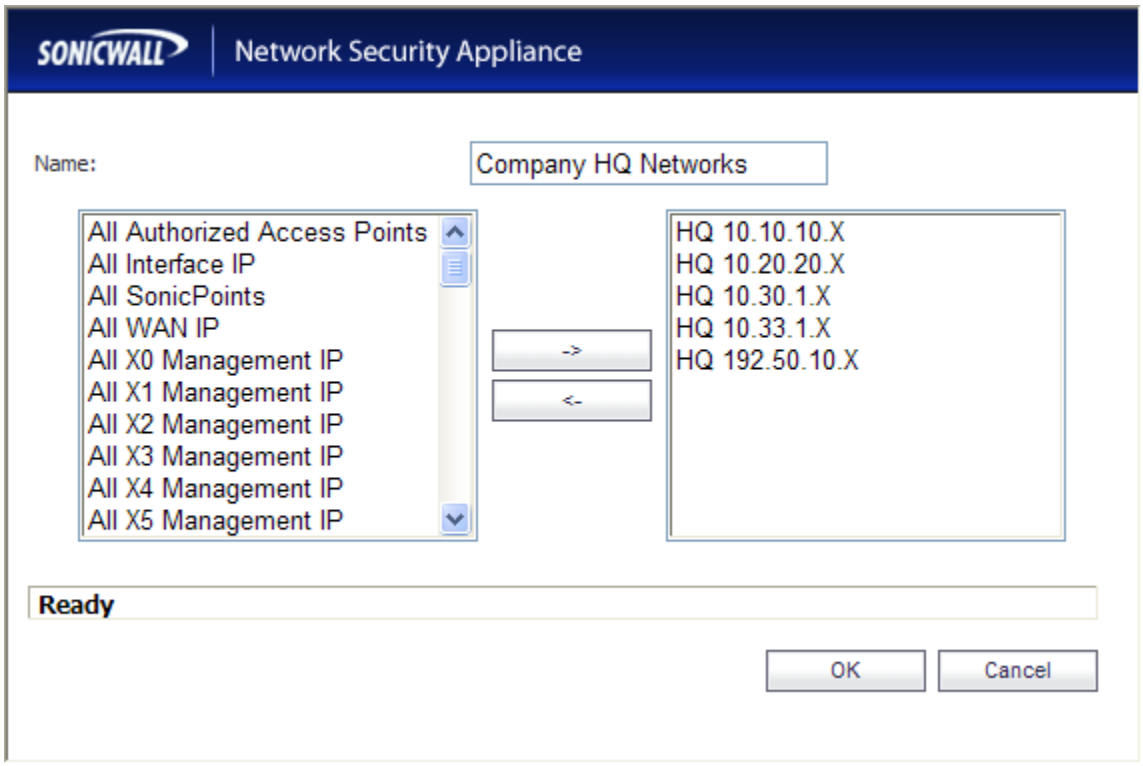
5.3.1.	Create Address Objects for each of the networks within the deployment sites. From the **Network → Address Objects,** click on the **Add** button and enter the following information for: **Name**, **Zone Assignment**, **Network**, and **Netmask** for each subnet in the topology. Click **OK** to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

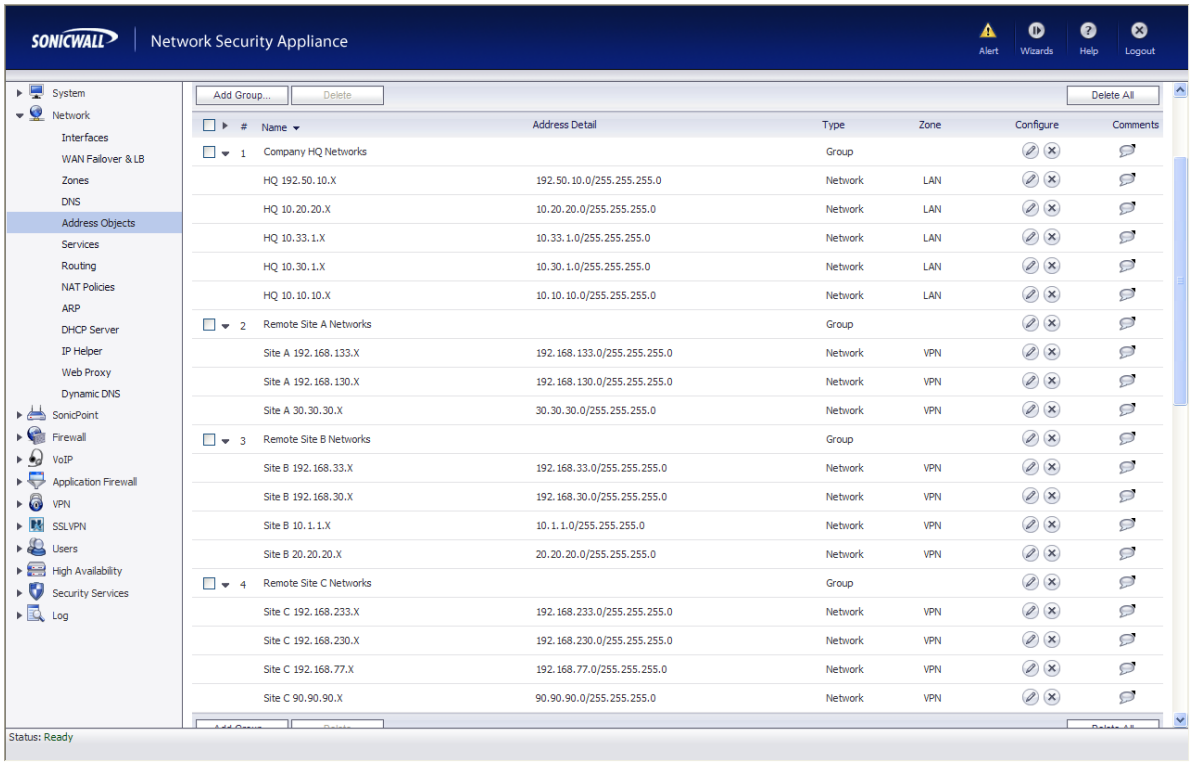


#	Name	Address Detail	Type	Zone	Configure	Comments
1	50.50.50.X	50.50.50.0/255.255.255.0	Network	WAN		
2	60.60.60.X	60.60.60.0/255.255.255.0	Network	WAN		
3	80.80.80.X	80.80.80.0/255.255.255.0	Network	WAN		
4	HQ 10.10.10.X	10.10.10.0/255.255.255.0	Network	LAN		
5	HQ 10.20.20.X	10.20.20.0/255.255.255.0	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		

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**.

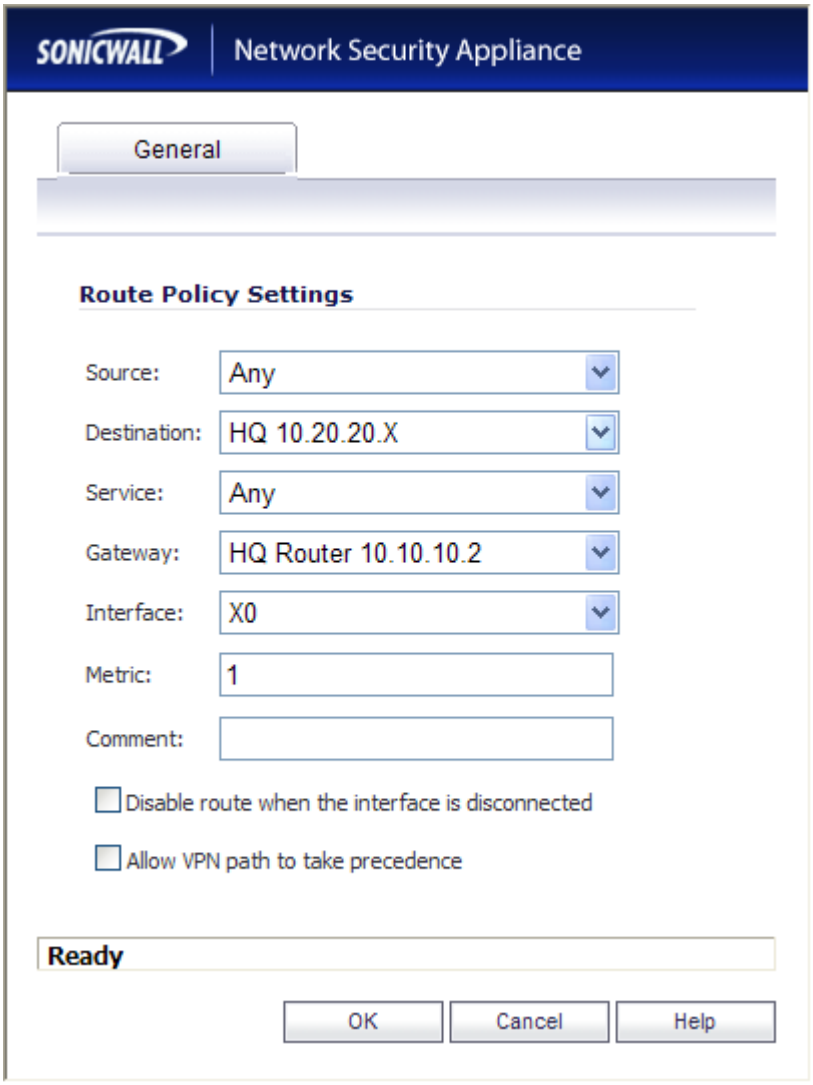
5.4.3. Once completed, the following Address Object Group summary is displayed.



5.5. Define routes for 'local' networks.

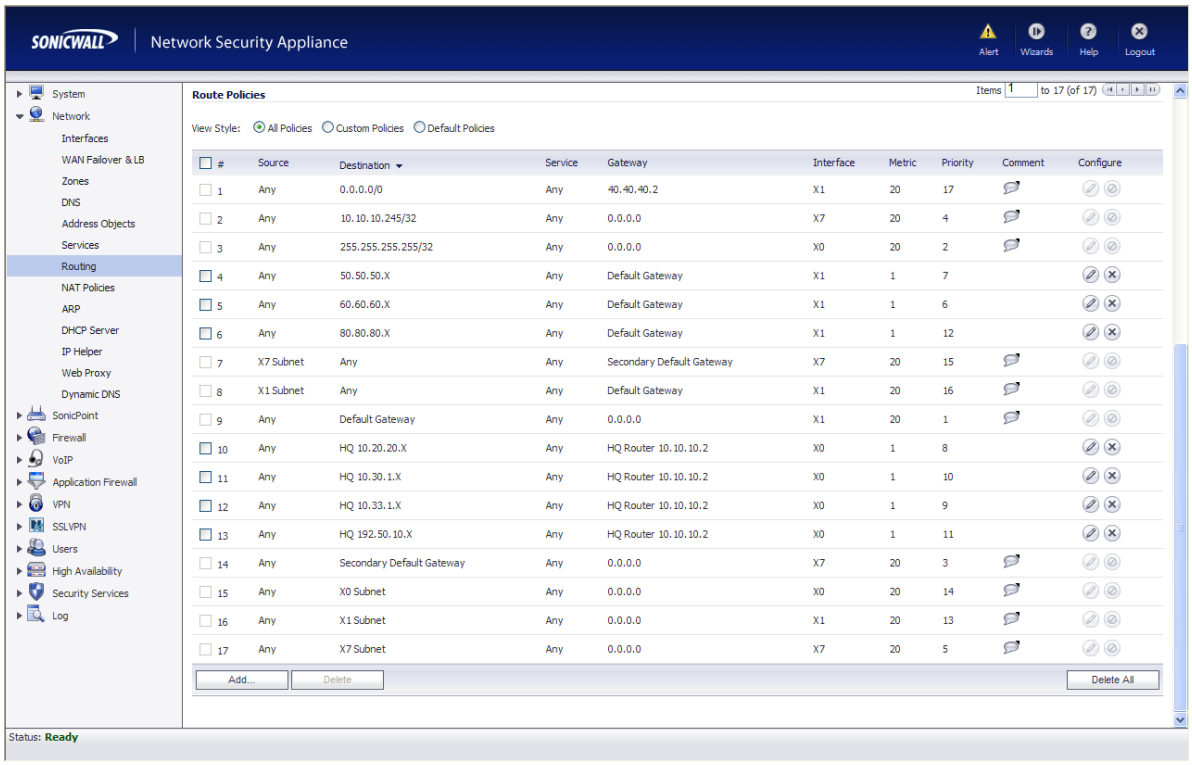
Configure the routing information for all the LAN subnets not directly connected to the Corporate Headquarters SonicWALL NSA E5500.

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.



5.5.2. Repeat for each LAN subnet.

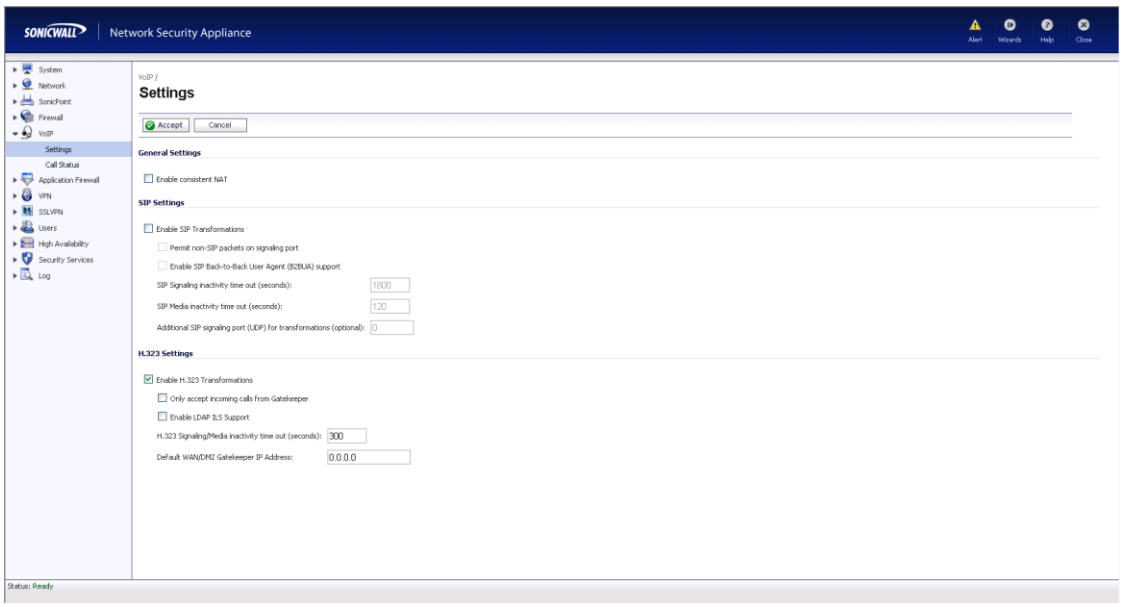
5.5.3. Once all of the LAN subnet routes have been added, the following routing summary is displayed.



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

5.6. Configure VoIP settings.

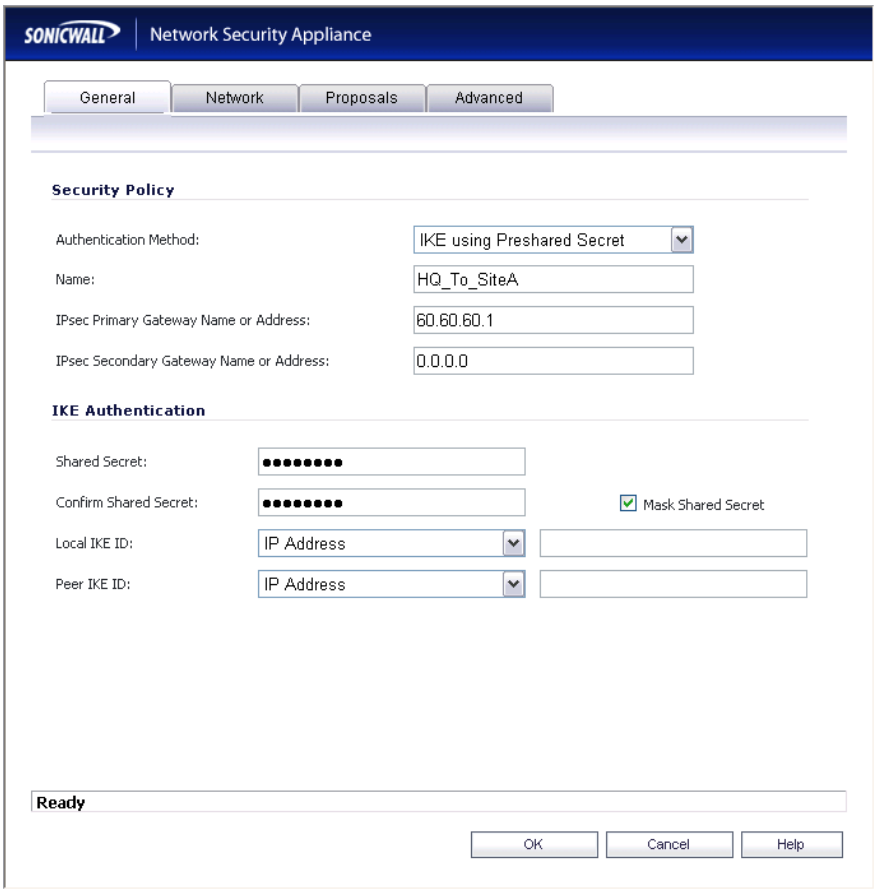
5.6.1. From the **VoIP → Settings,** click on the **Enable H.323 Transformations** checkbox. Click **Accept** to continue.



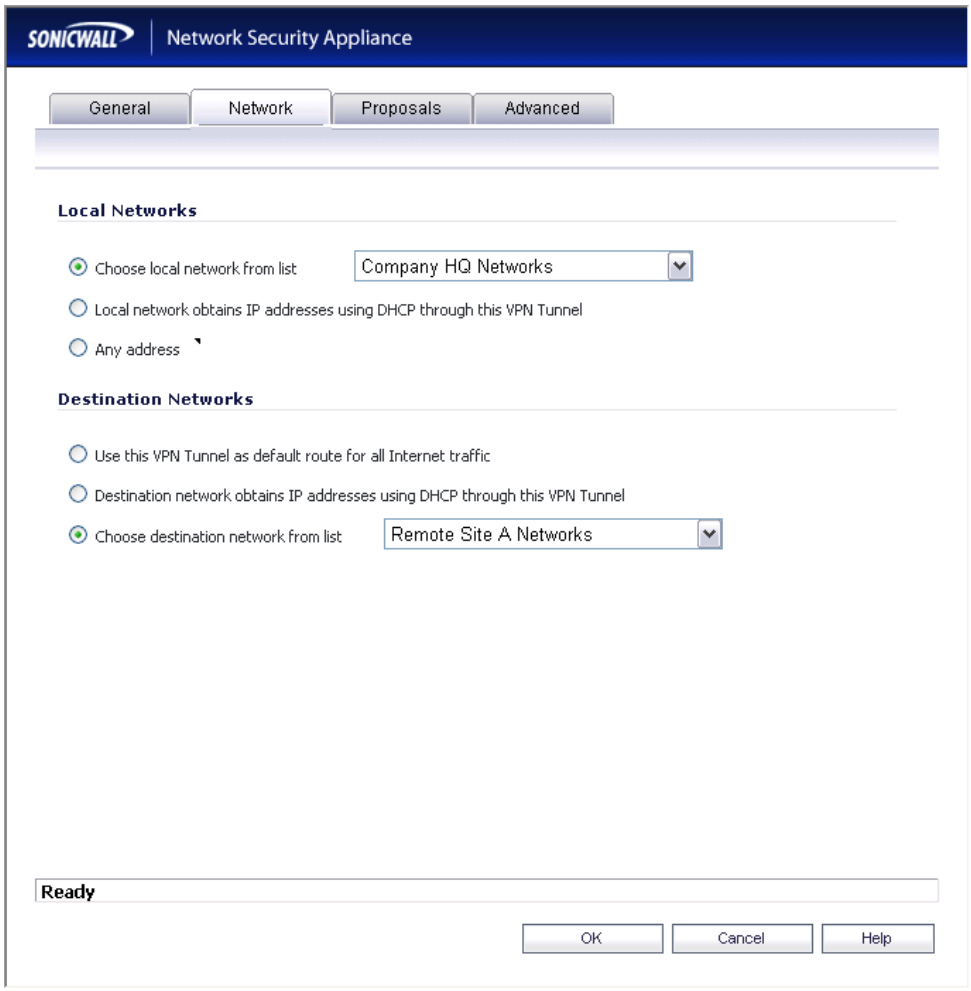
5.7. Create VPN policies

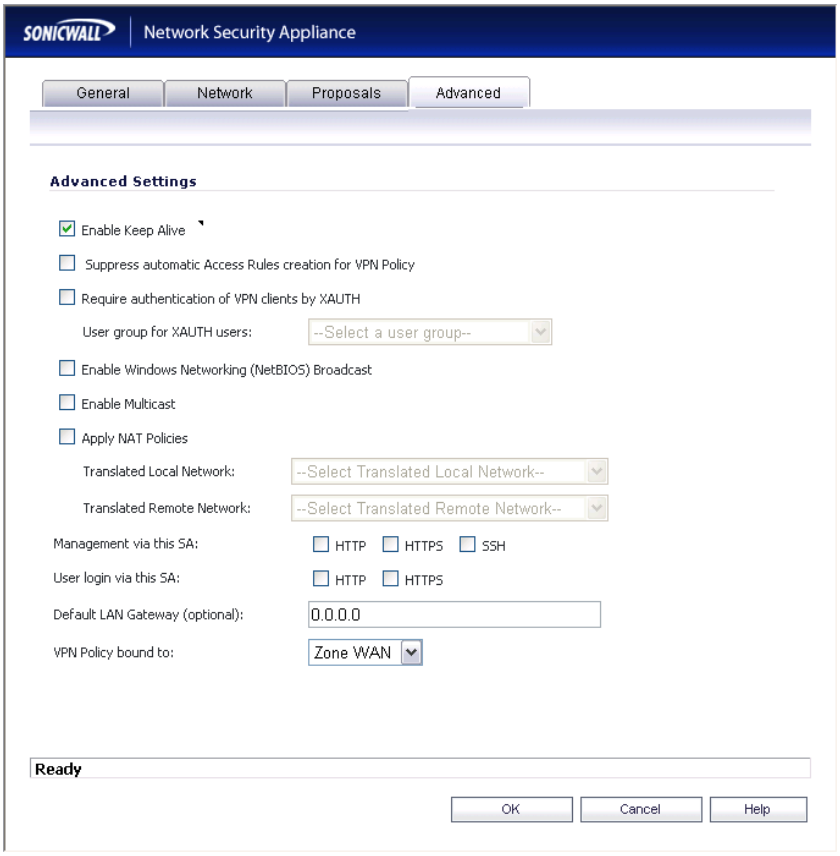
For each site within the network structure, create a VPN policy to allow secure communication between SonicWALL appliances.

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.

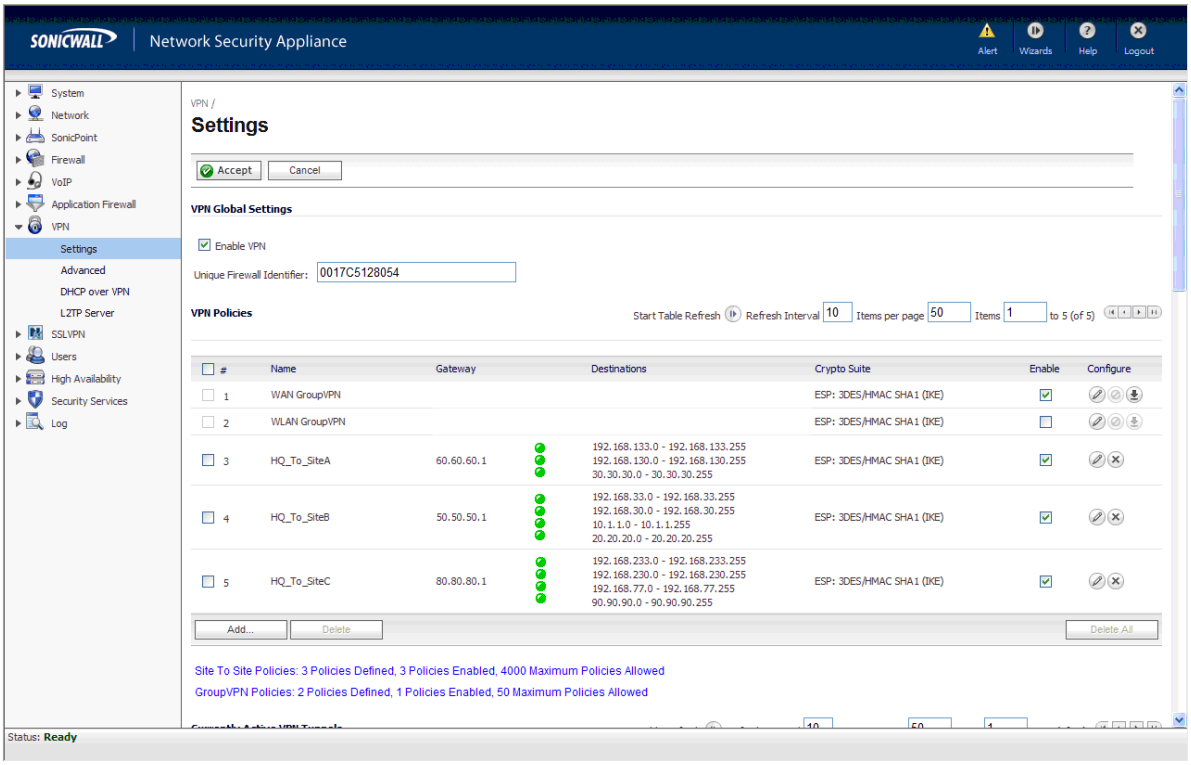


5.7.2.	Specify subnets accessible over the VPN tunnel. Within the **Choose local network from list** pull down, select the Address Object Group (created in Step **5.4.1**) for this site. Within the **Choose remote network from list** scroll list, select the Address Object Group (created in Step **5.4.1**)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



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. 
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.



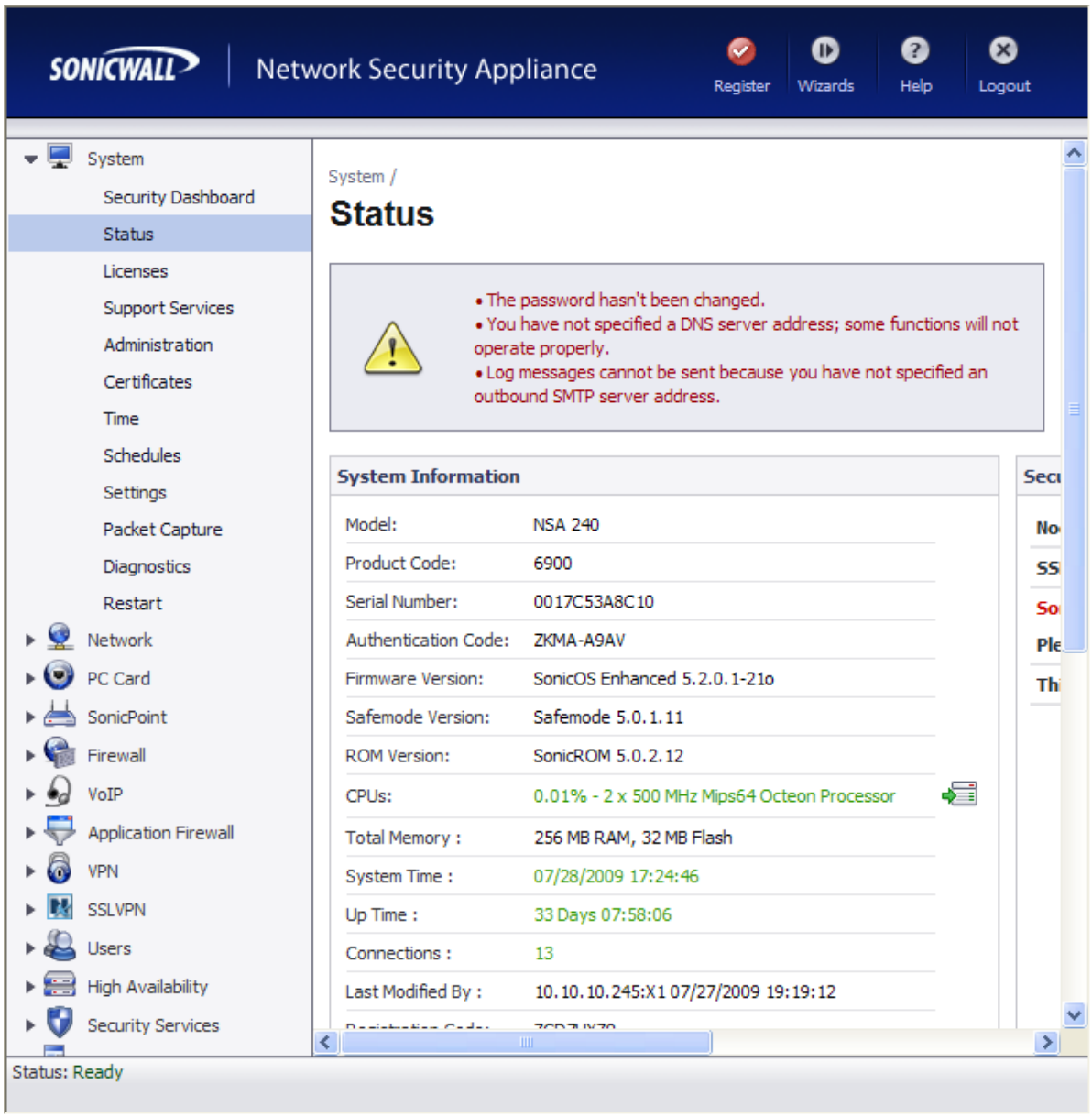
5.8. Save settings

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)

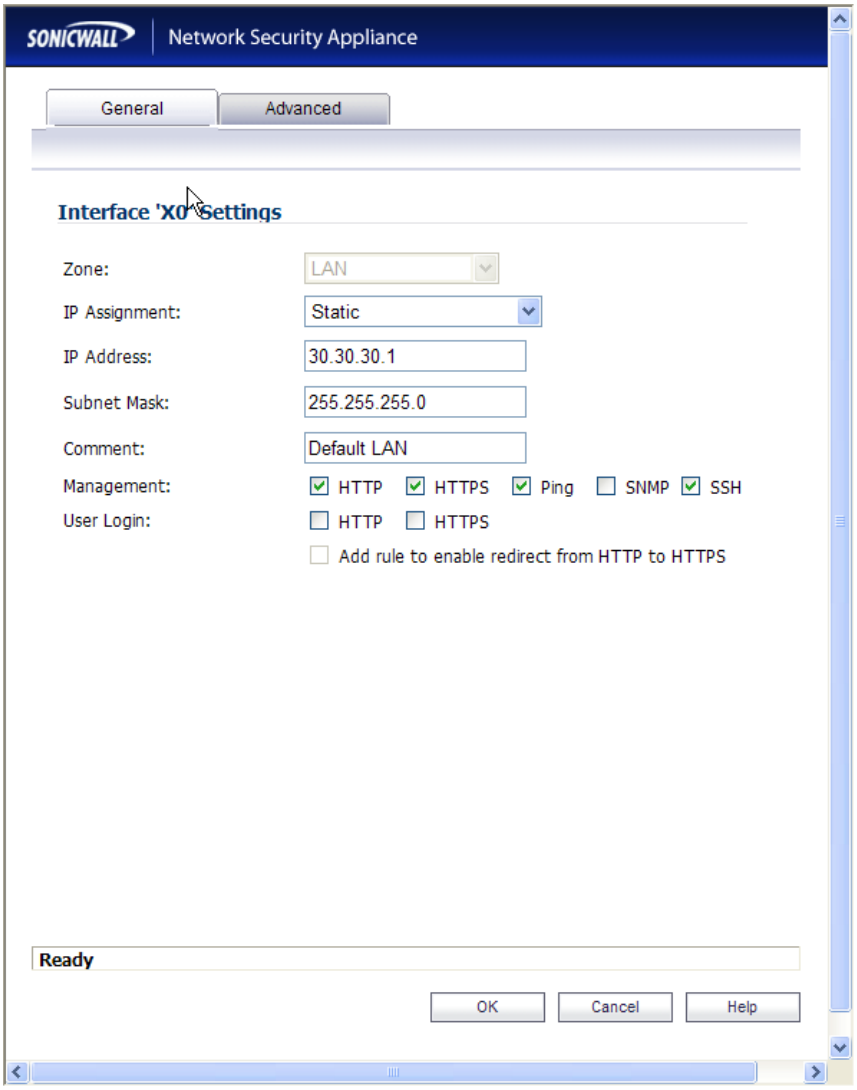
Step	Description
5.9.1.	Configure the SonicWall NSA 240 at Remote Site A using the built-in web-based **Management Tool.** Access this tool by establishing a web browser connection to the SonicWall NSA 240. Refer to Section 9 [6]. Log into the SonicWall NSA 240. 1. Connect the LAN port of the computer 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**.

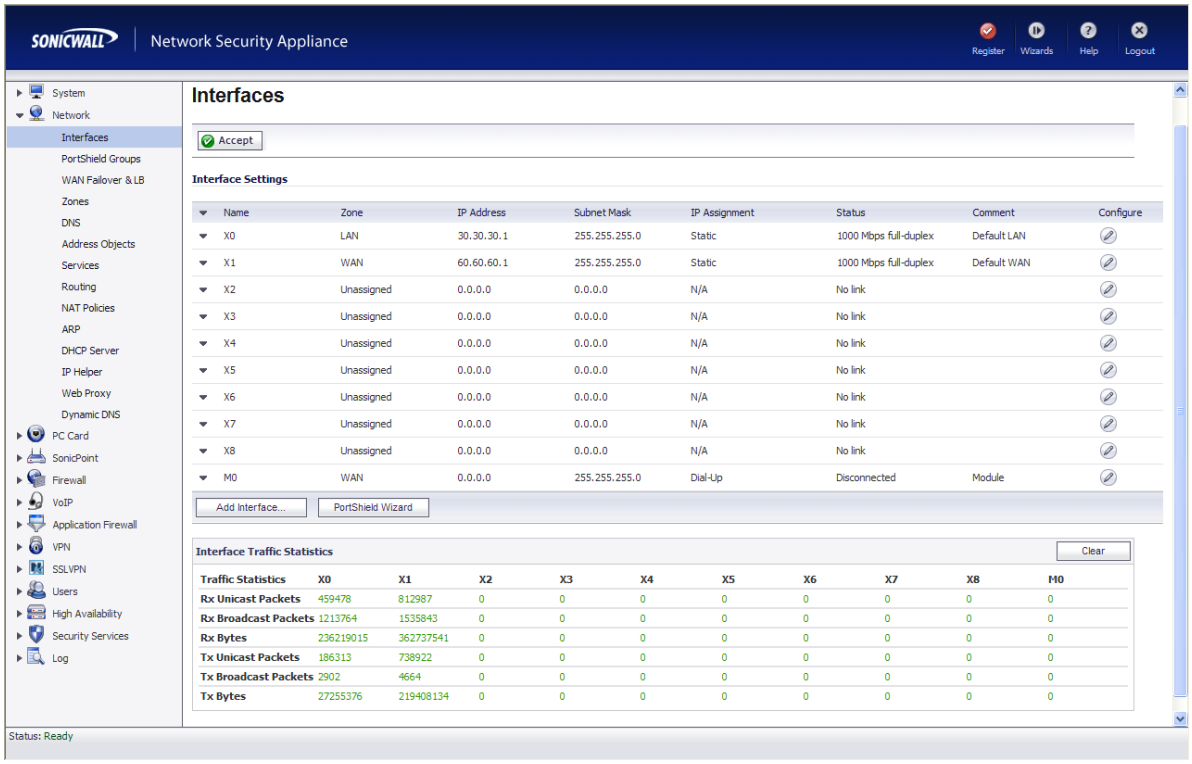


5.10. Configure Interfaces:

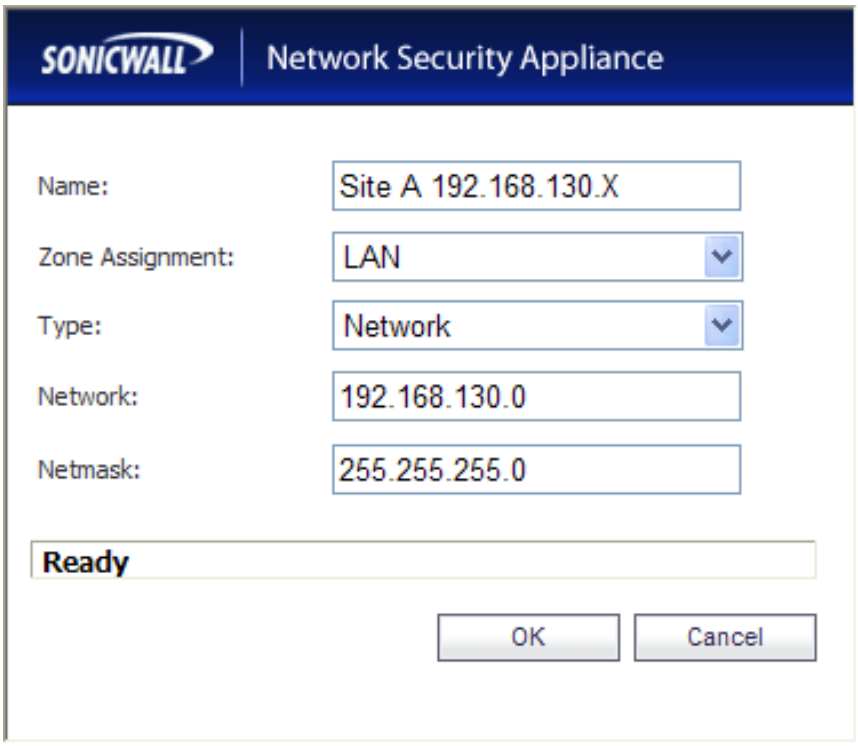
5.10.1 From the **Network → Interfaces,** click on the **Configure icon** " " for **X0** (LAN) and enter the following information for: **IP Assignment**, **IP Address** and **Subnet Mask** according to network structure to be used, Click **OK** to continue.



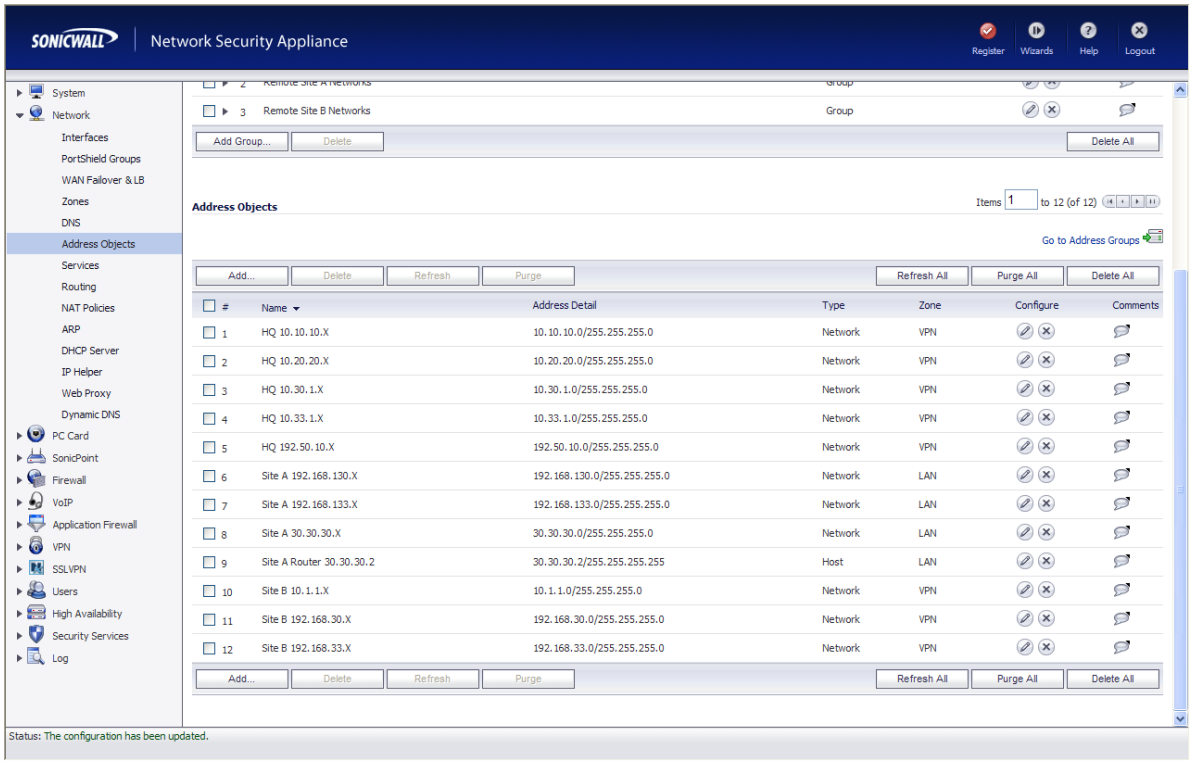
5.10.2	Repeat for the **X1** (WAN) interface.
5.10.3	Once configuration on the interfaces is completed, the following summary is presented.



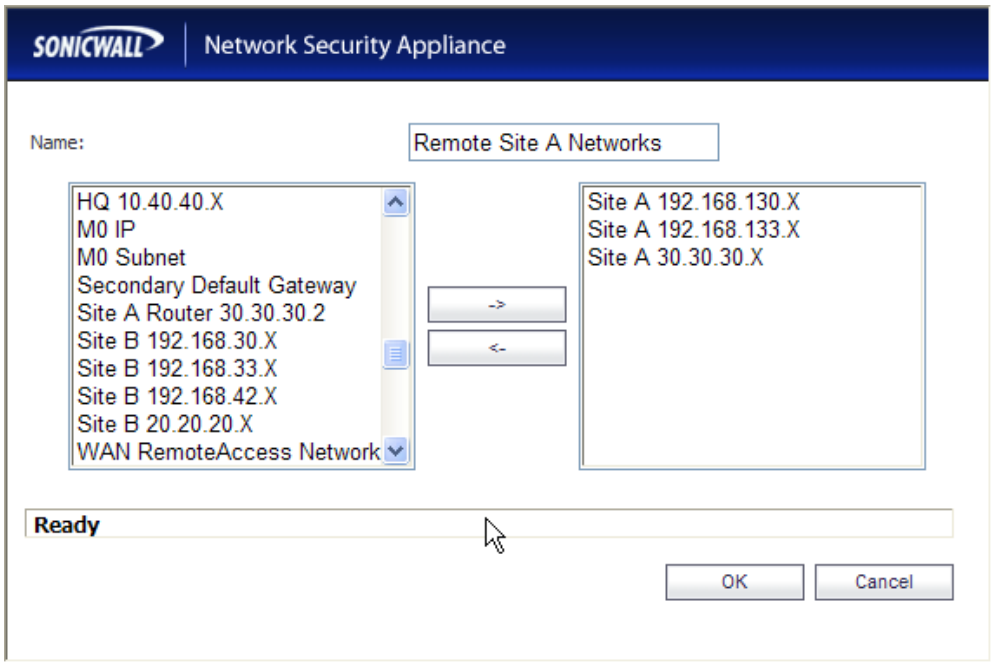
5.11. Define networks

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. 
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.

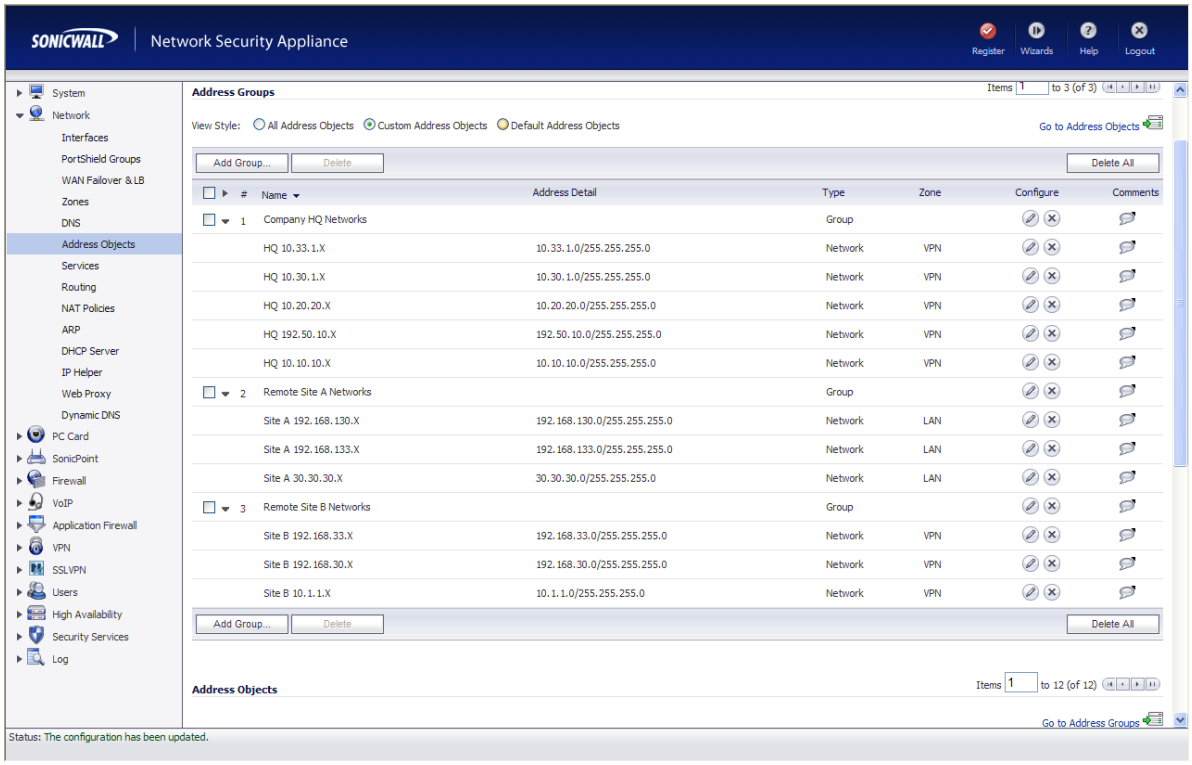
5.11.3 Once all of the Address Objects have been created, the following summary screen is displayed.



5.12. Group Address Objects based on site within topology

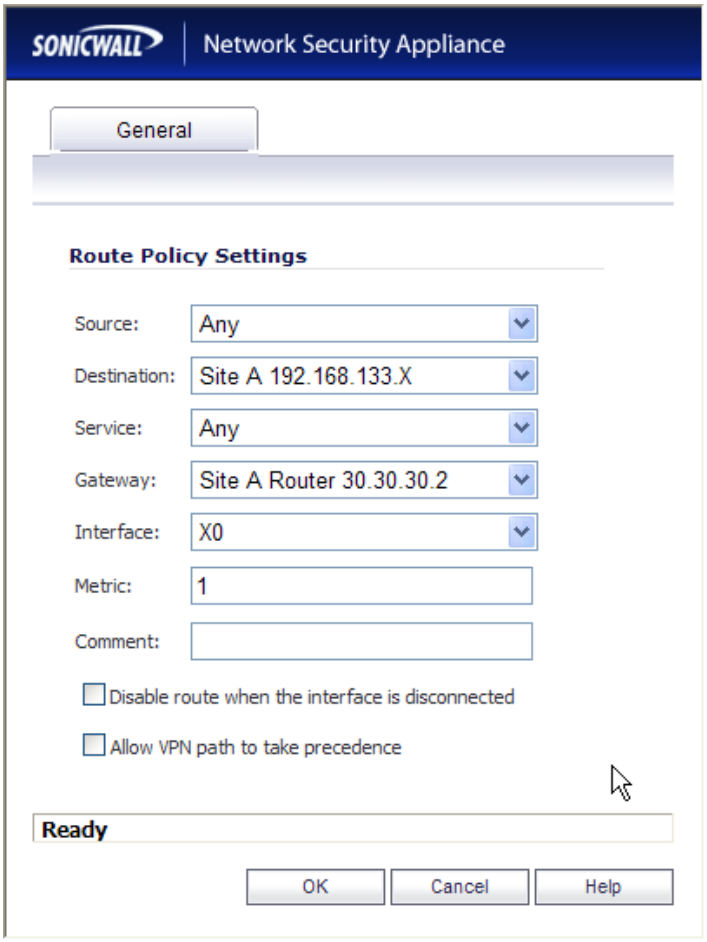
5.12.1	From the **Network → Address Objects,** click on the **Add Group** button and enter a unique name for the site and highlight all related Address Objects (created in Steps **5.11.1**) and click -> to add to group. 
5.12.2	Repeat for all sites within network structure as shown in **Figure 1**.

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

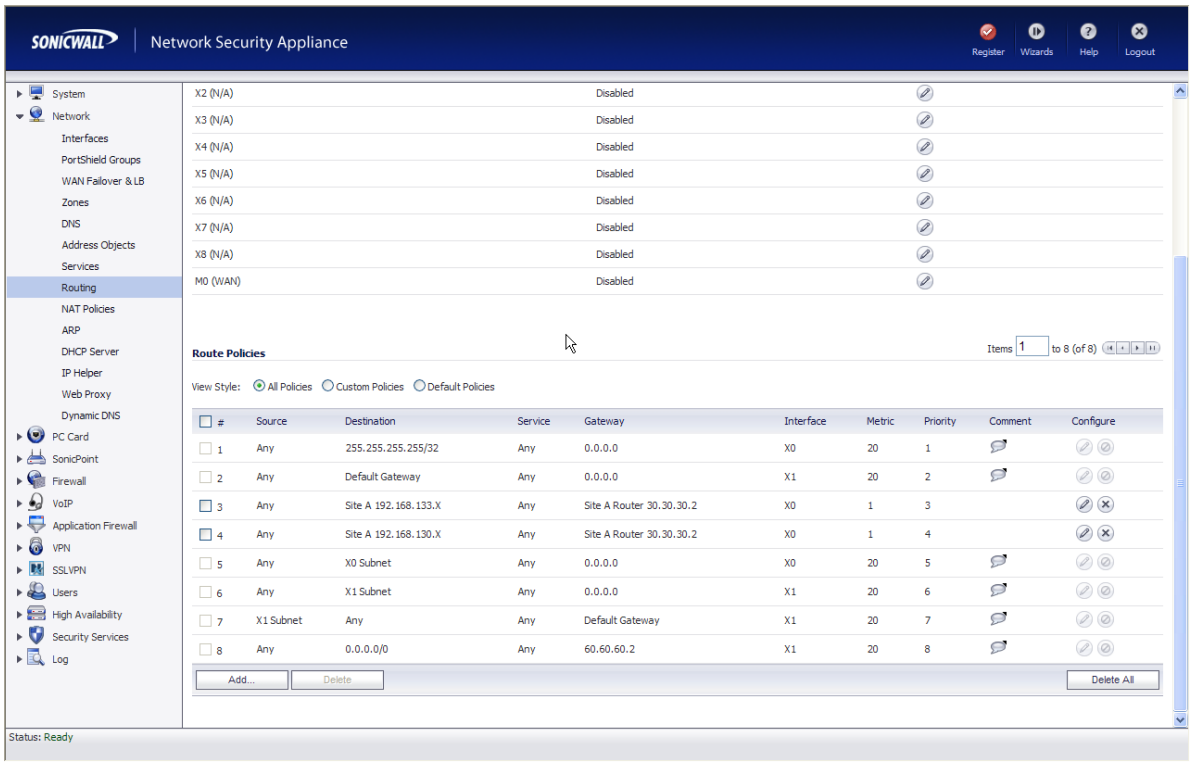


5.13. Define routes for 'local' networks.

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

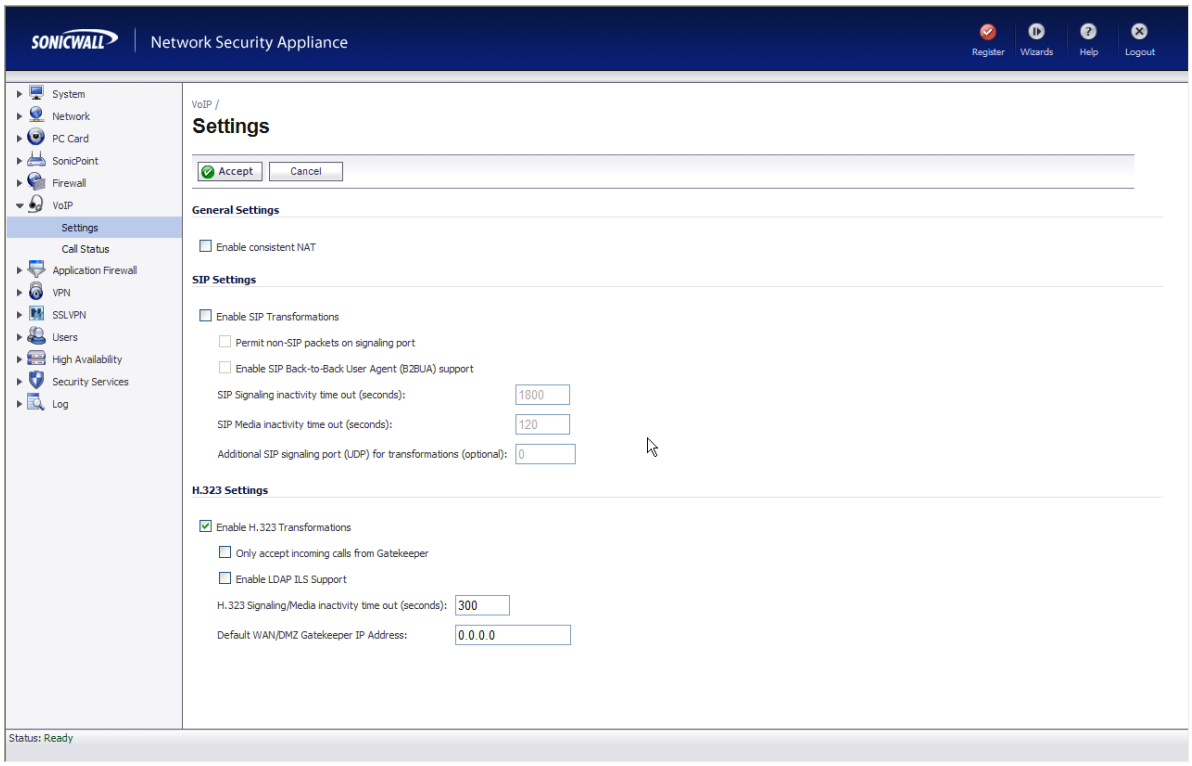
5.13.1	From the **Network → Routing,** click on the **Add** button and enter a route information (**Source**, **Destination**, **Service, Gateway**, and **Interface**) for each LAN subnet. Click **OK** to continue. 
5.13.2	Repeat for each LAN subnet.

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



5.14. Configure VoIP settings.

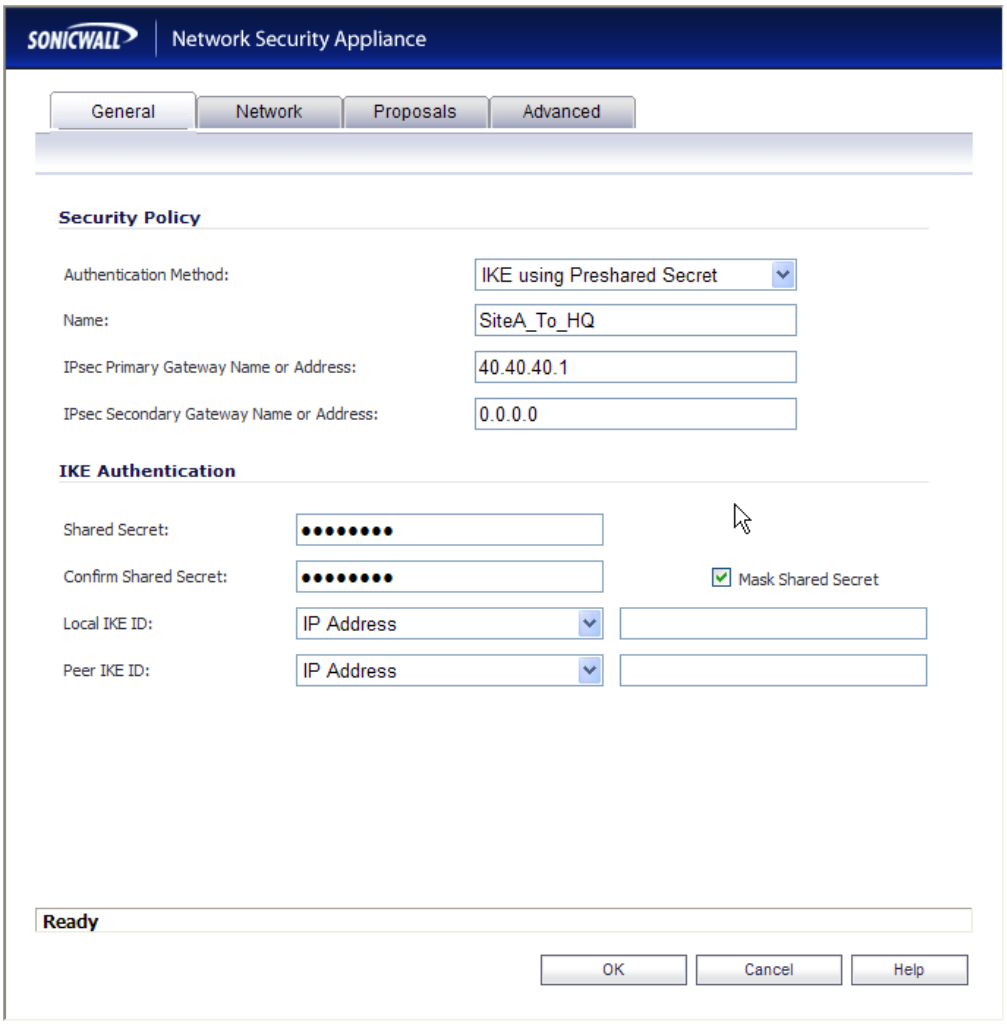
5.14.1 From the **VoIP → Settings,** click on the **Enable H.323 Transformations** checkbox. Click **Accept** to continue.



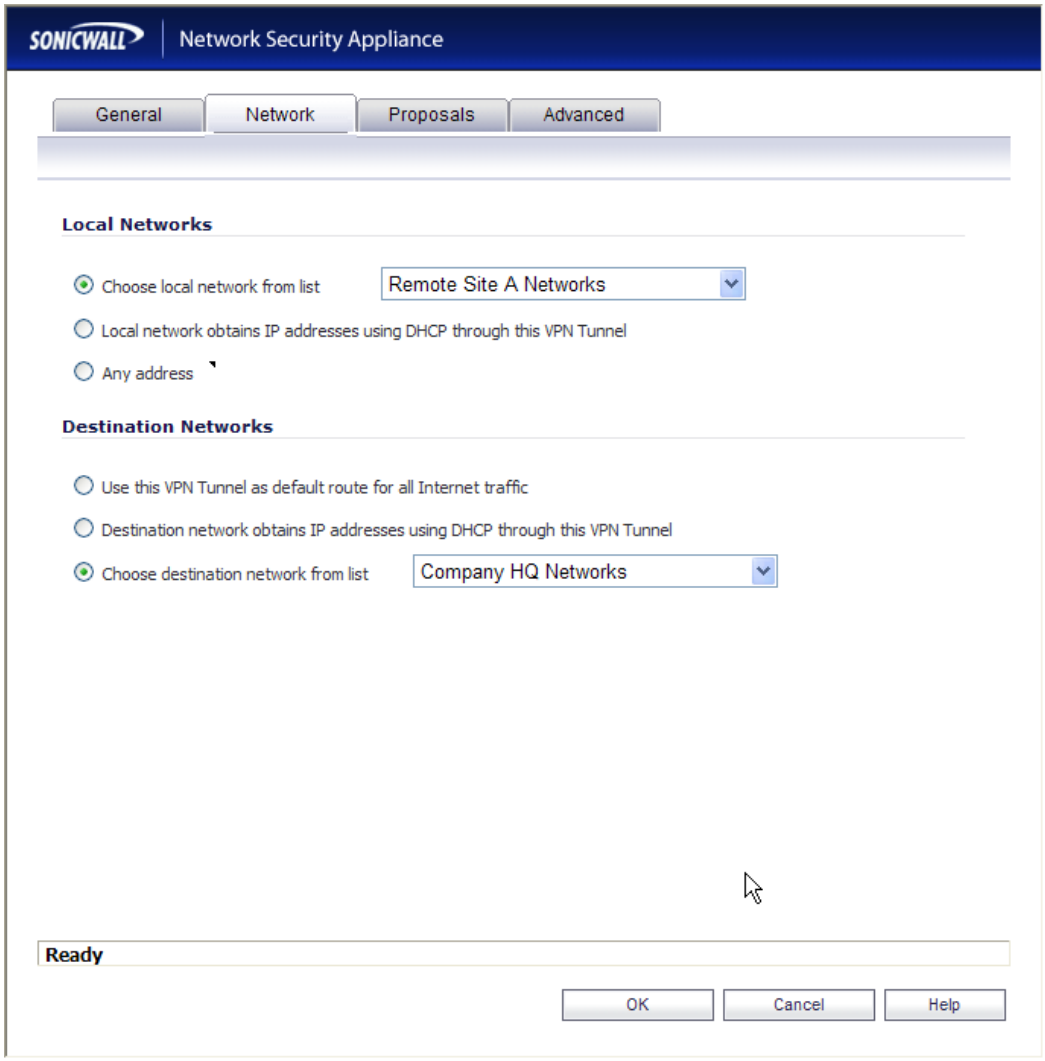
5.15. Create VPN policies

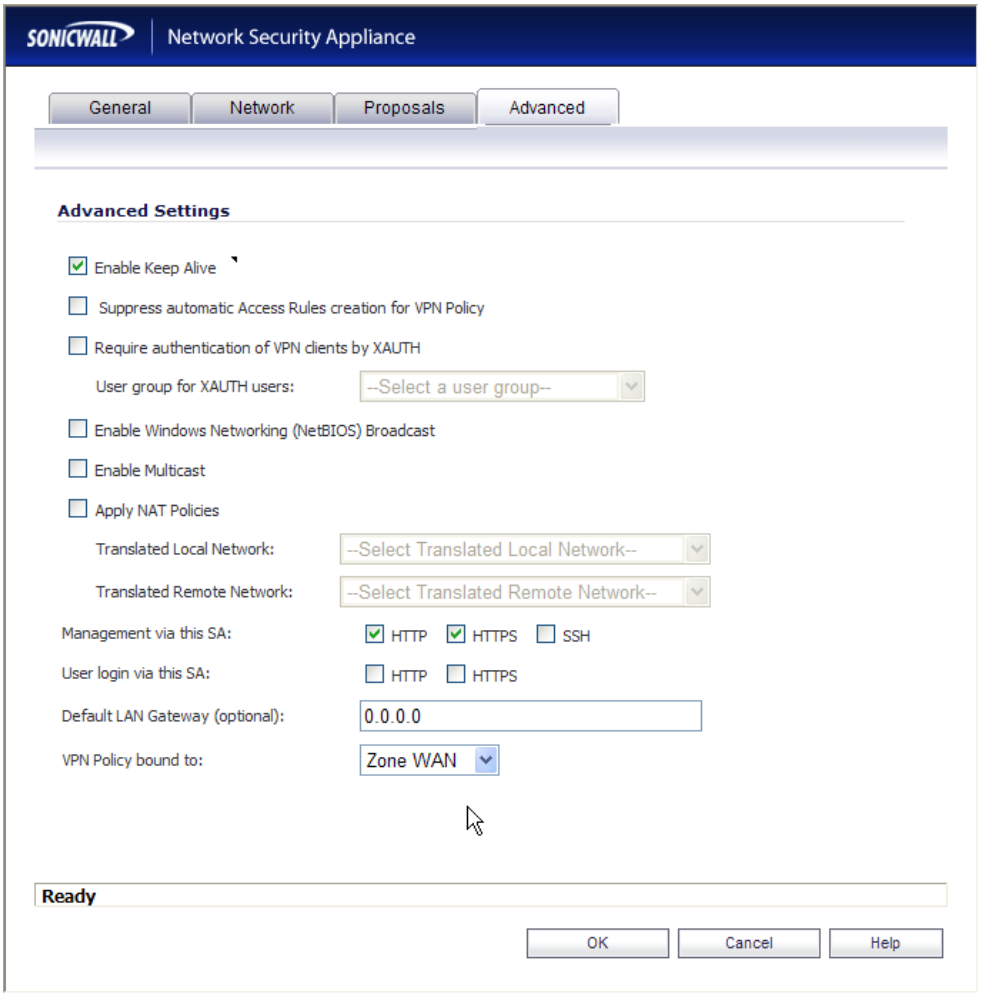
For each site within the network structure, create a VPN policy to allow secure communication between SonicWALL appliances.

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.

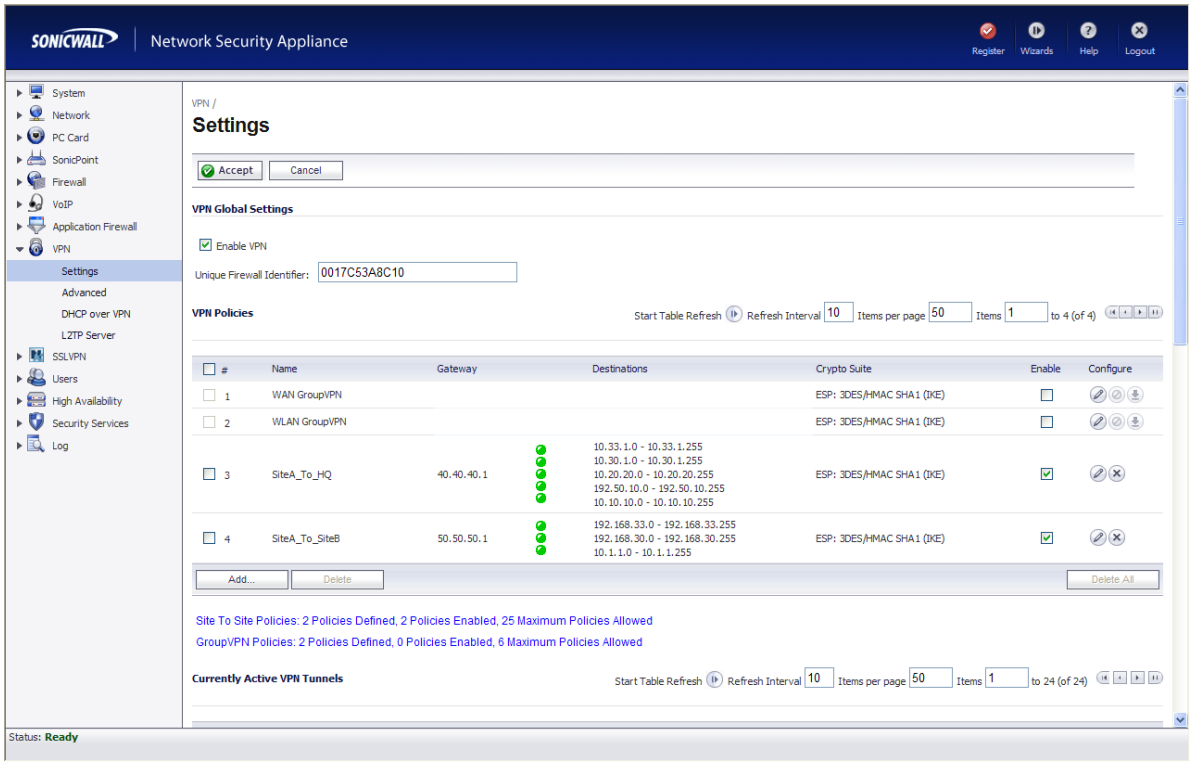


5.15.2	Specify subnets accessible over the VPN tunnel. Within the **Choose local network from list** scroll list, select the Address Object Group (created in Step **5.12.1**) for this site. Within the **Choose remote network from list** scroll list, select the Address Object Group (created in Step **5.4.1**) for the remote site. Click **Advanced** tab to continue.



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. 
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.



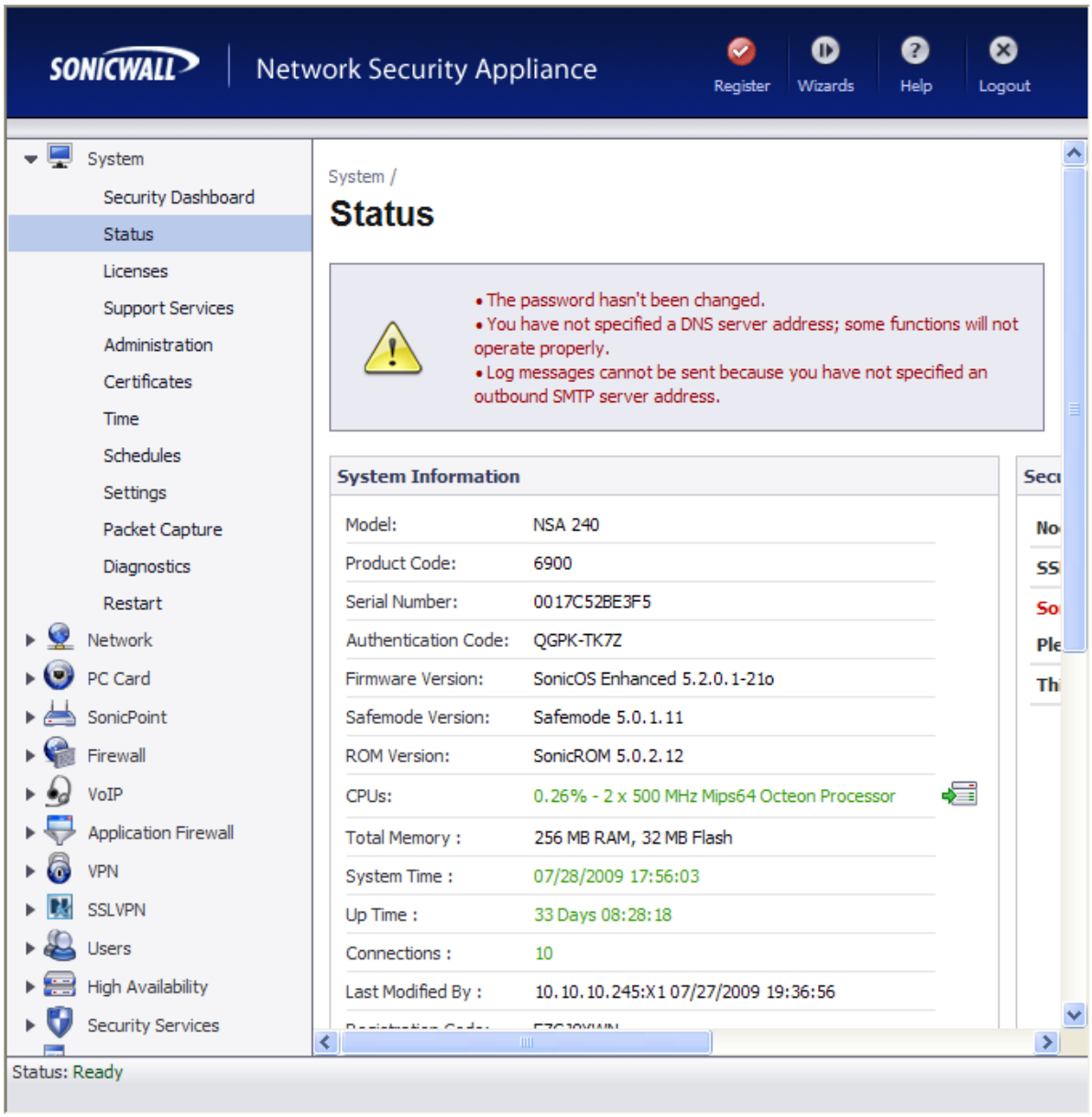
5.16. Save settings

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)

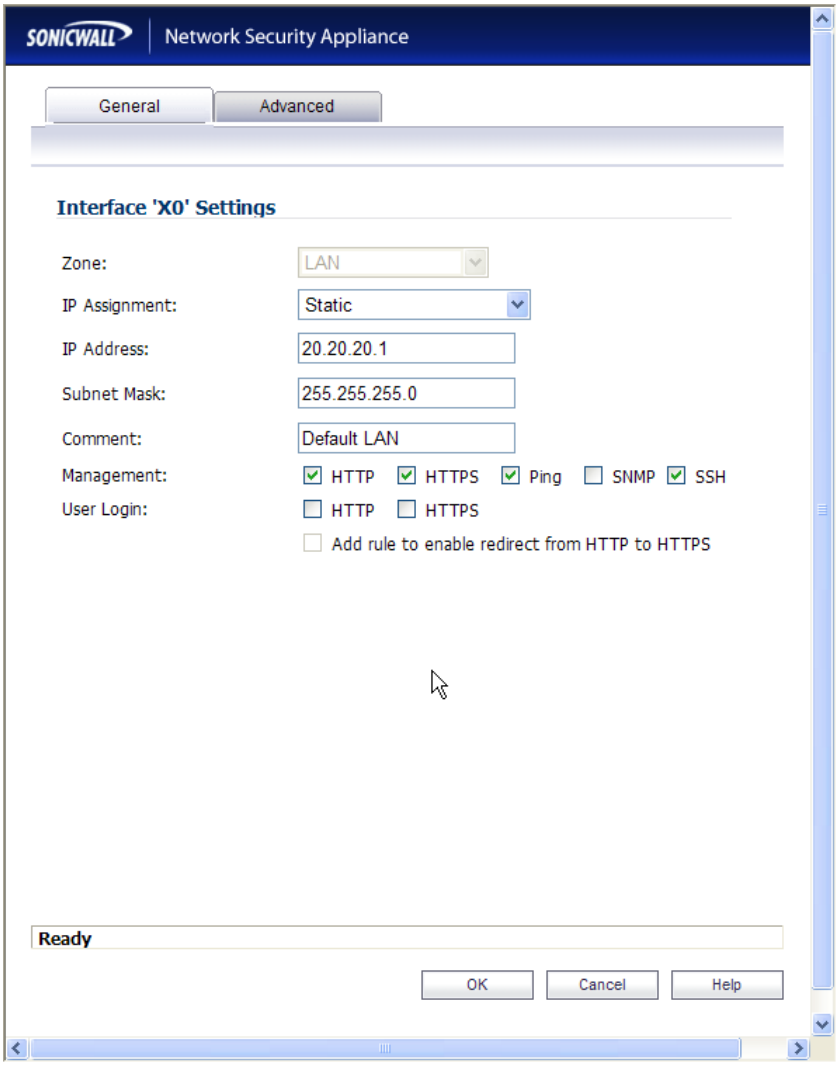
Step	Description
5.17.1	Configure the SonicWall NSA 240 at Remote Site B using the built-in web-based **Management Tool.** Access this tool by establishing a web browser connection to the SonicWall NSA 240. Refer to Section 9 [6]. Log into the Remote Site B SonicWall NSA 240. 1. Connect the LAN port 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**.

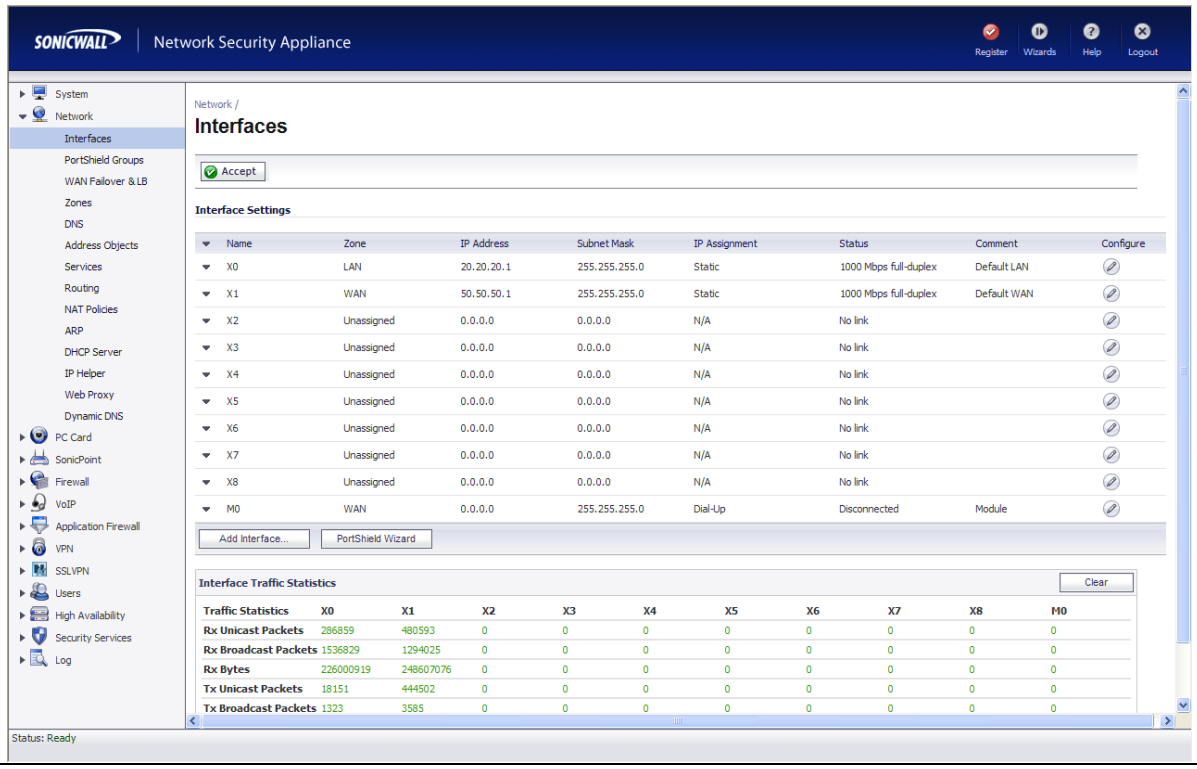


5.18. Configure Interfaces:

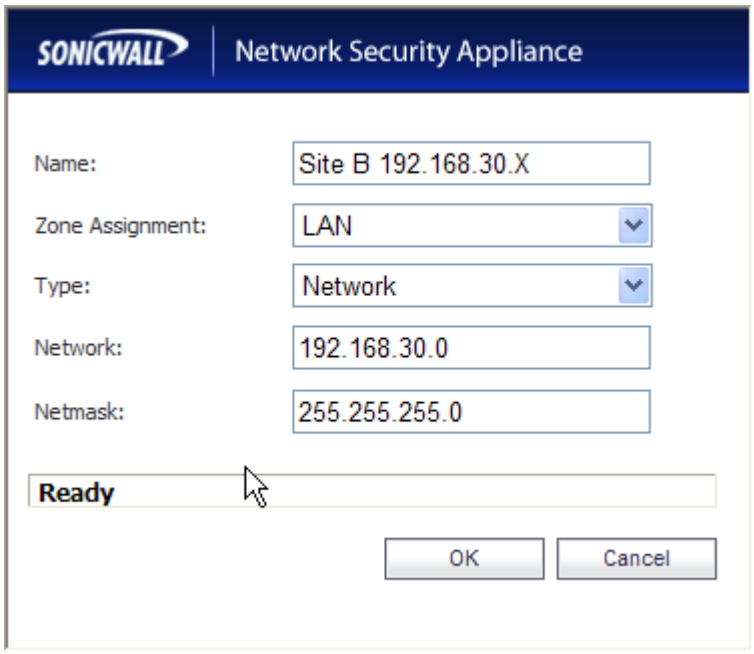
5.18.1 From the **Network → Interfaces,** click on the **Configure icon** " " for **X0** (LAN) and enter the following information for: **IP Assignment**, **IP Address** and **Subnet Mask** according to network structure to be used, Click **OK** to continue.



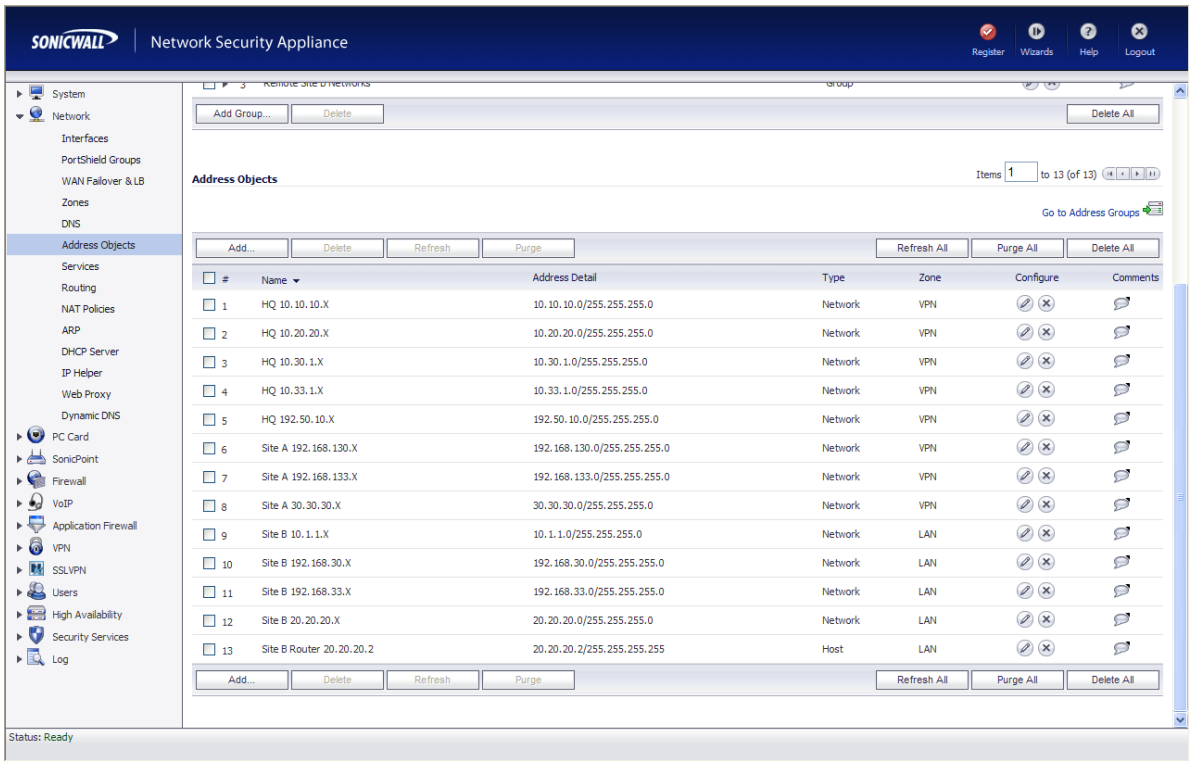
5.18.2	Repeat for the **X1** (WAN) interface.
5.18.3	Once configuration on the interfaces is completed, the following summary is presented.



5.19. Define networks

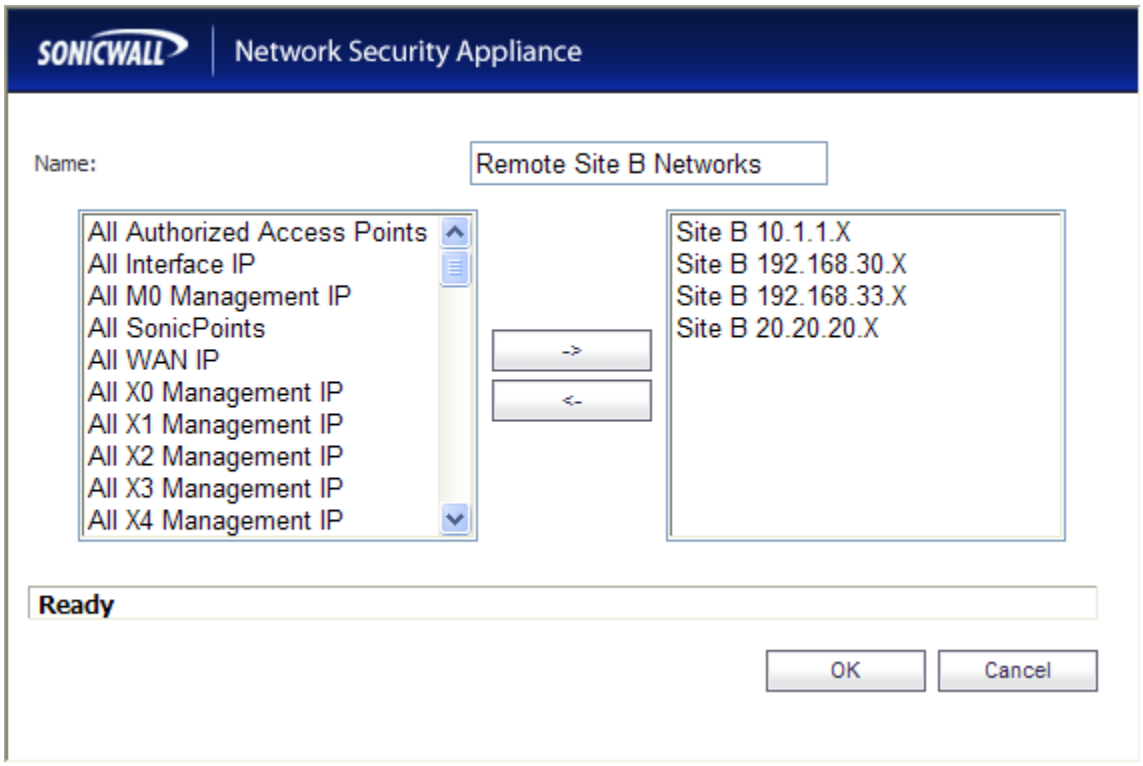
5.19.1	Create Address Objects for each of the networks within the deployment sites. From the **Network → Address Objects,** click on the **Add** button and enter the following information for: **Name**, **Zone Assignment**, **Network**, and **Netmask** for each subnet in the topology. Click **OK** to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



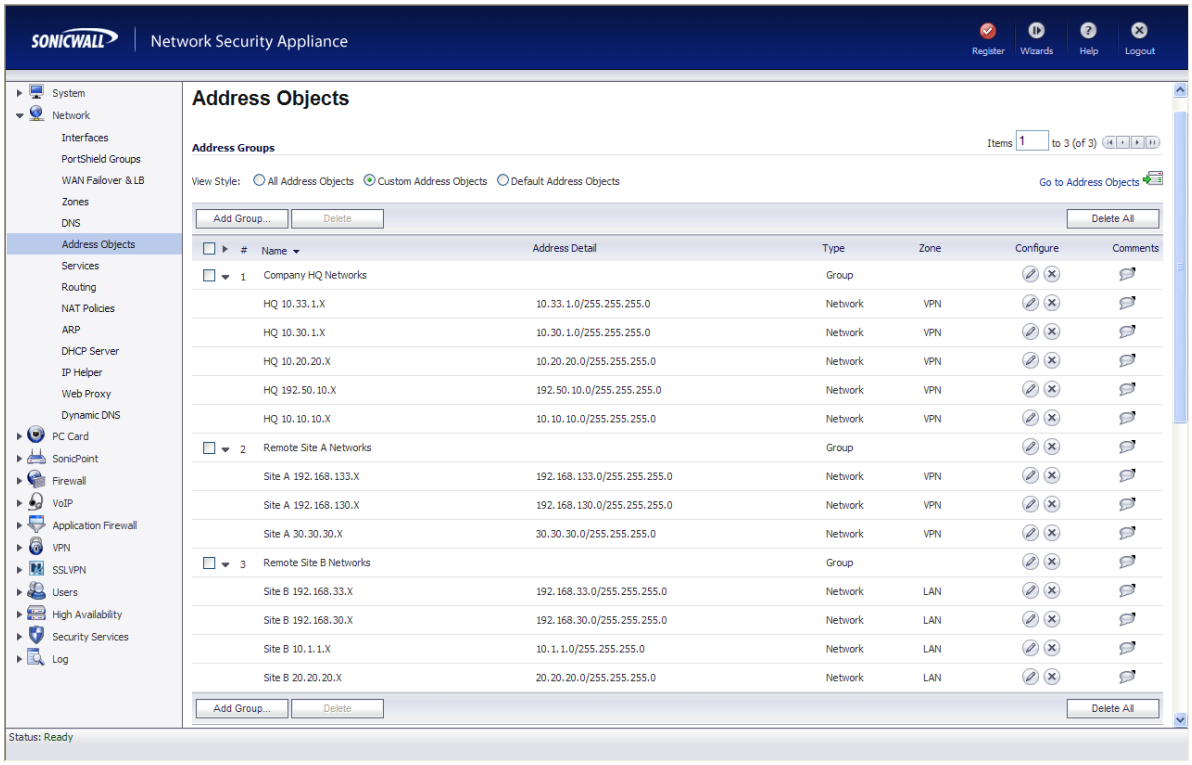
5.20. Group Address Objects based on site within topology

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.



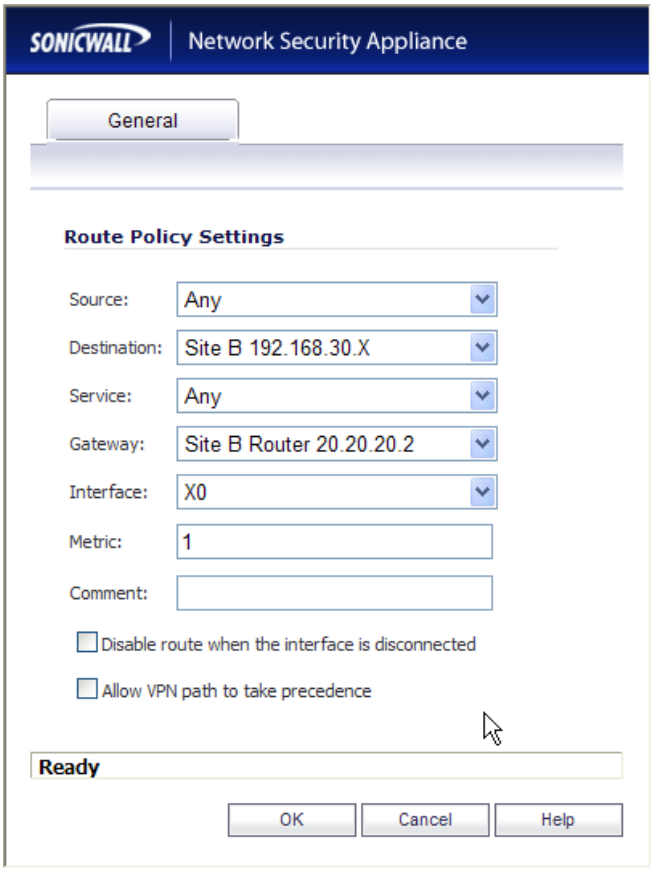
5.20.2 Repeat for all sites within network structure as shown in **Figure 1**.

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

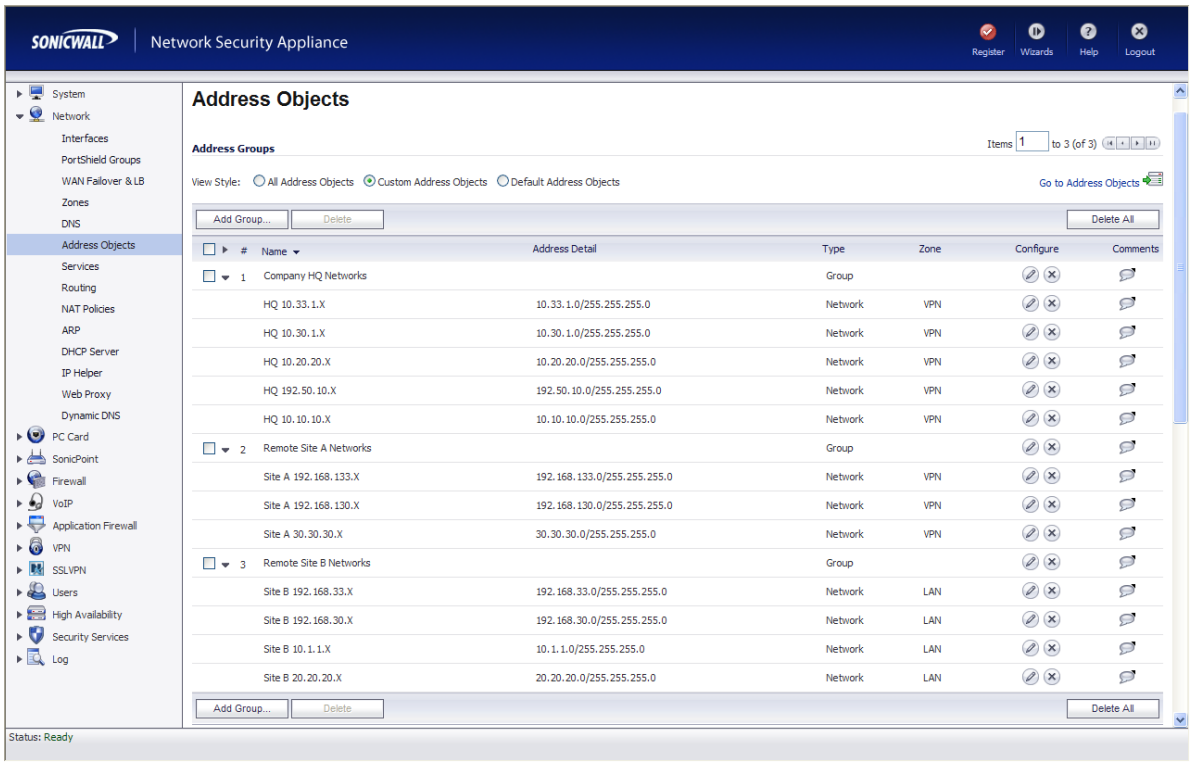


5.21. Define routes for 'local' networks.

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

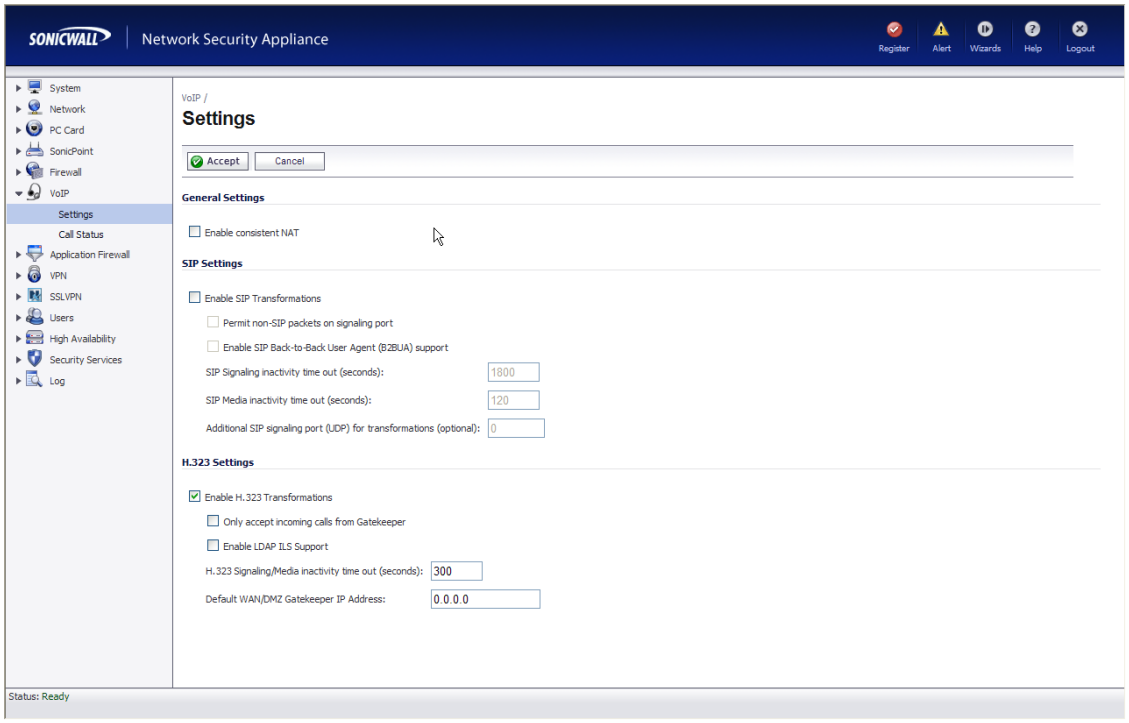
5.21.1	From the **Network → Routing,** click on the **Add** button and enter a route information (**Source**, **Destination**, **Service, Gateway**, and **Interface**) for each LAN subnet. Click **OK** to continue. 
5.21.2	Repeat for each LAN subnet.

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



5.22. Configure VoIP settings.

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

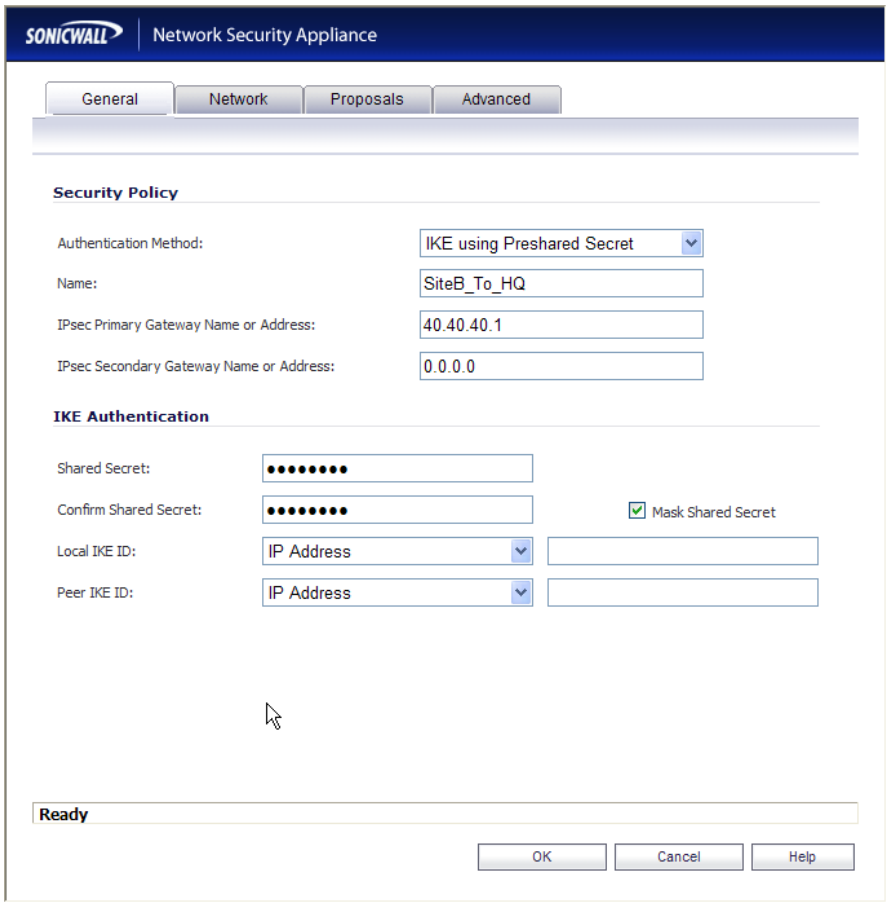


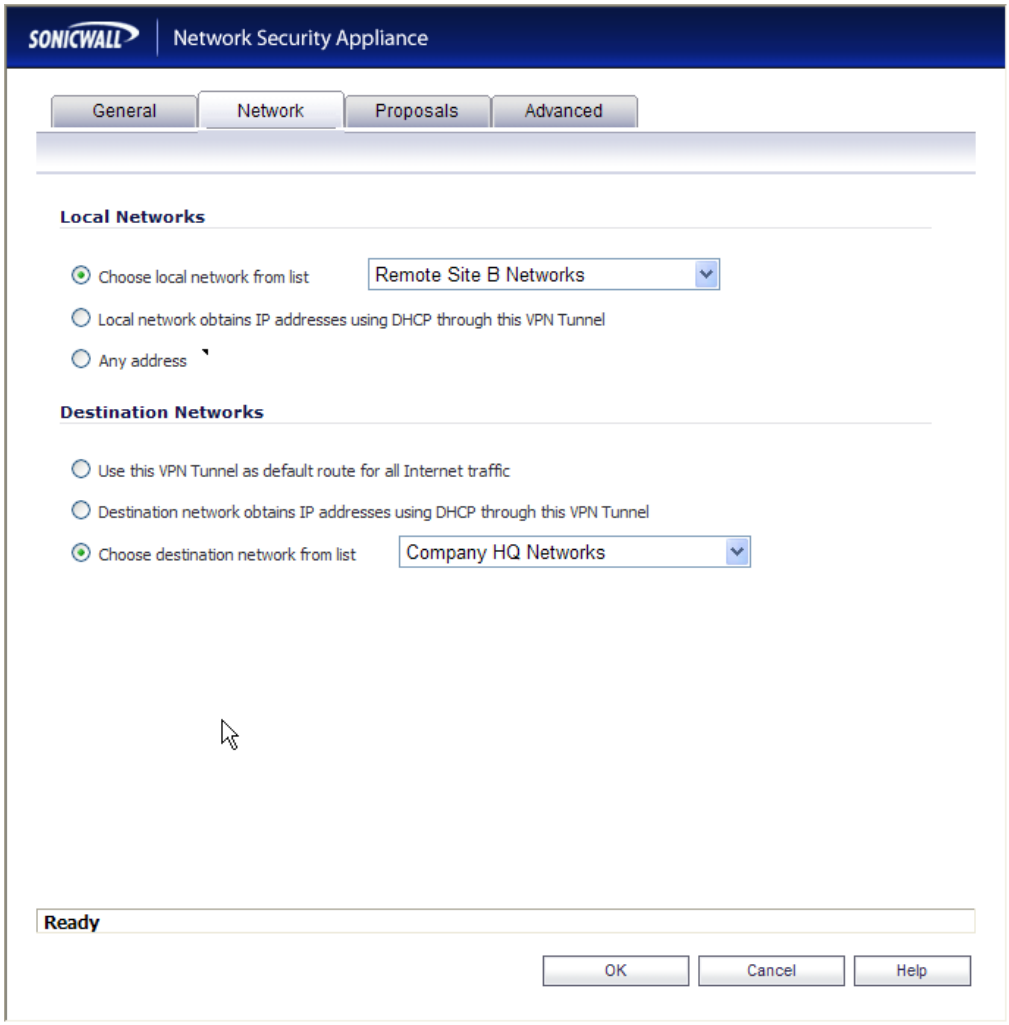
5.23. Create VPN policies

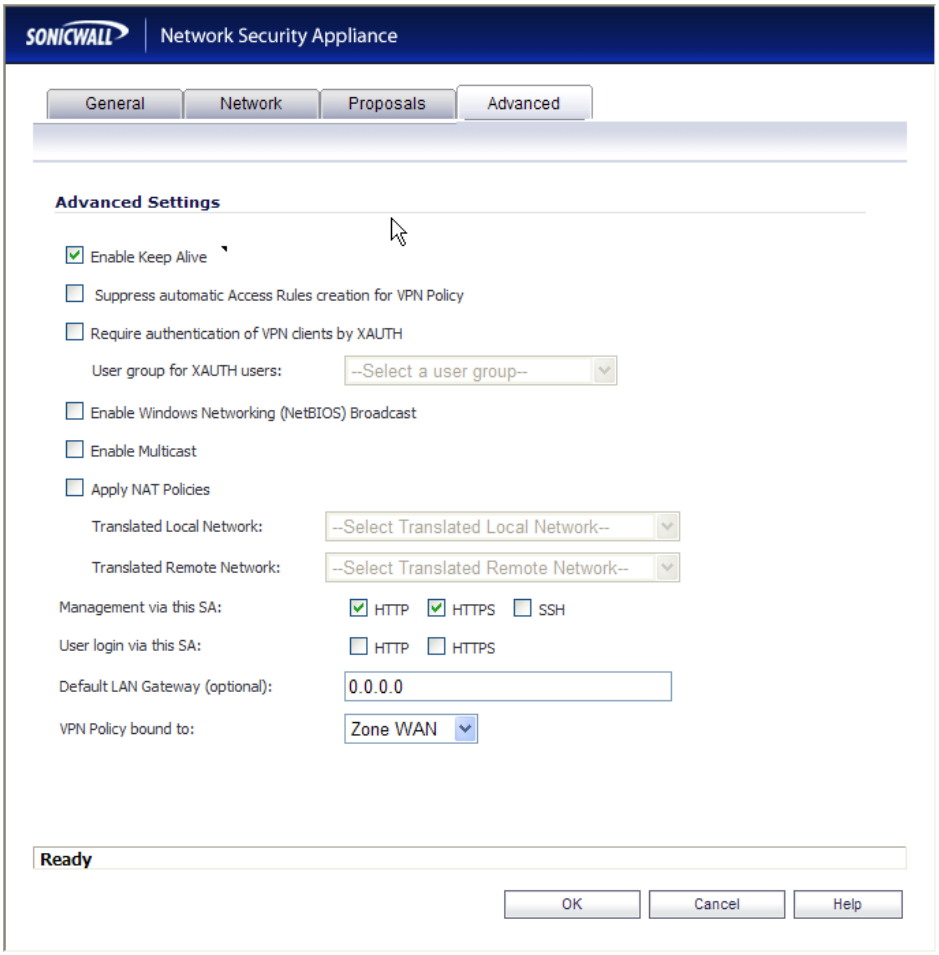
For each site within the network structure, create a VPN policy to allow secure communication between SonicWALL appliances.

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**.

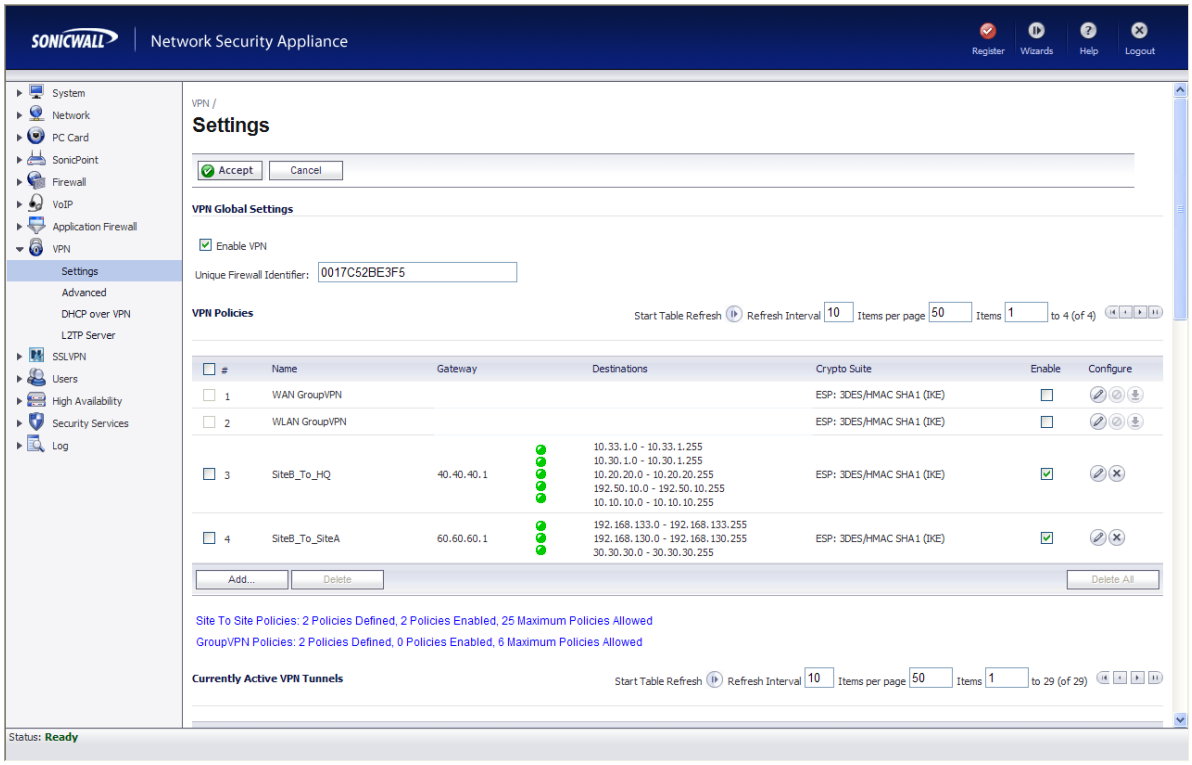
Click **Network** tab to continue.



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. 

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. 
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.



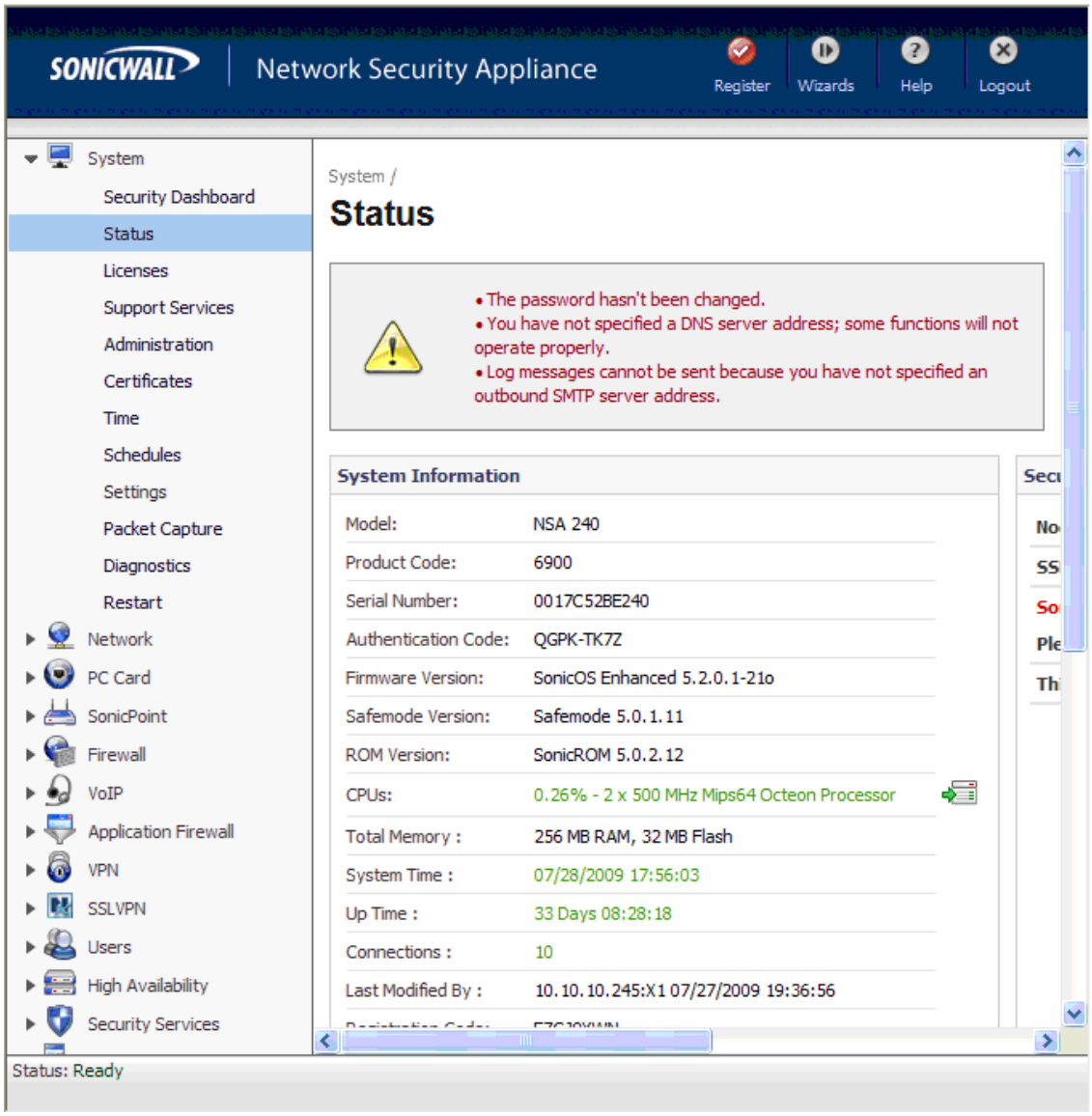
5.24. Save settings

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)

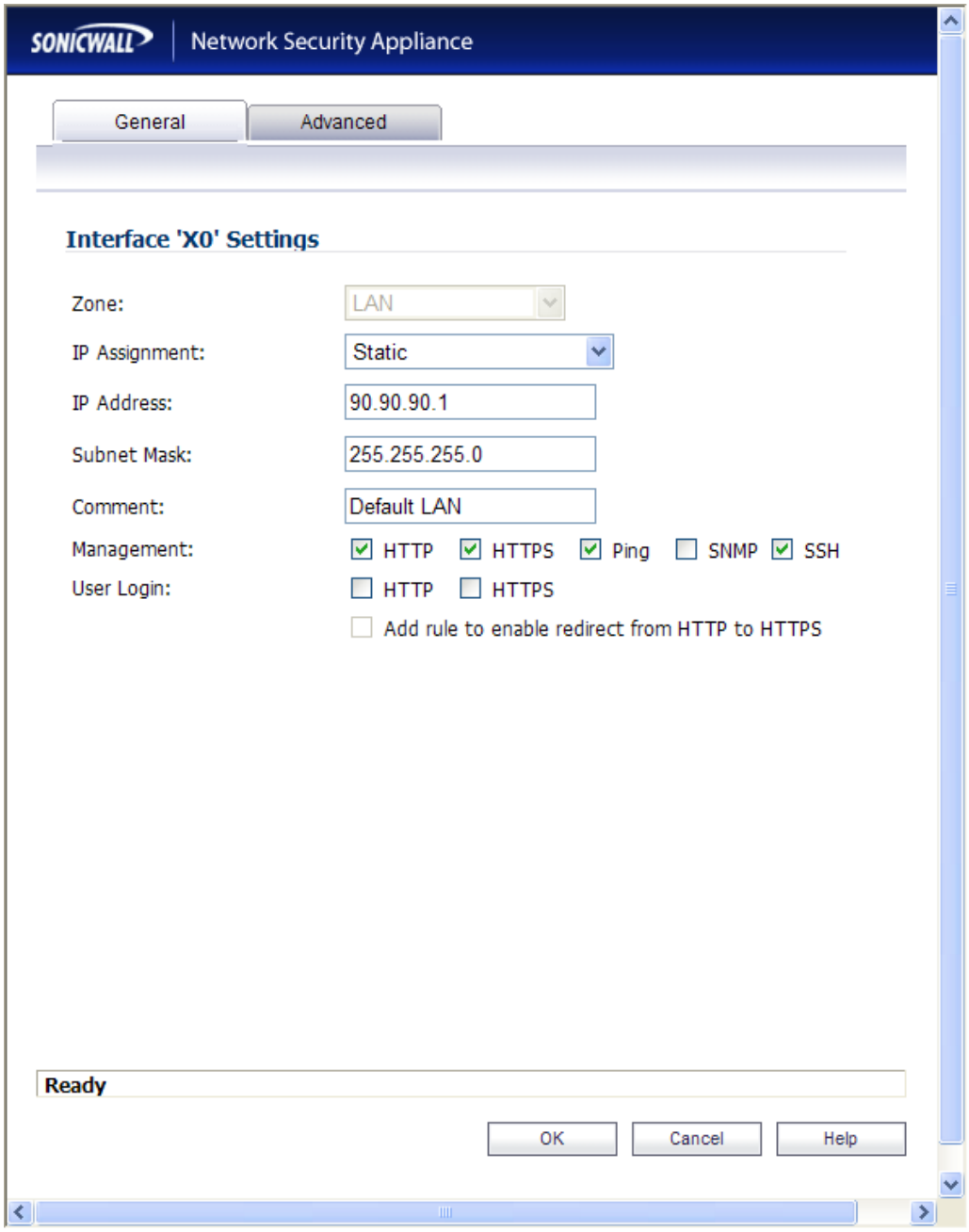
Step	Description
5.25.1	Configure the SonicWall NSA 240 at Remote Site C using the built-in web-based **Management Tool.** Access this tool by establishing a web browser connection to the SonicWall NSA 240. Refer to Section 9 [6]. Log into the Remote Site C SonicWall NSA 240. 4. Connect the LAN port 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**.

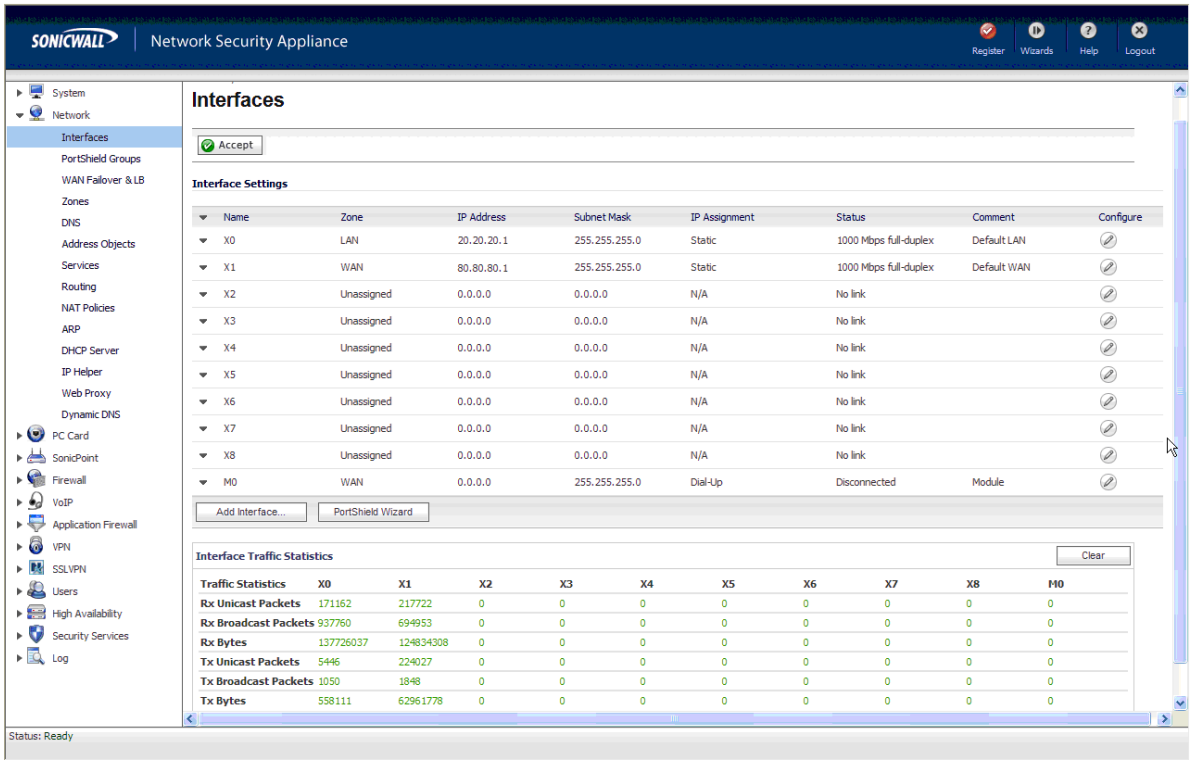


5.26. Configure Interfaces:

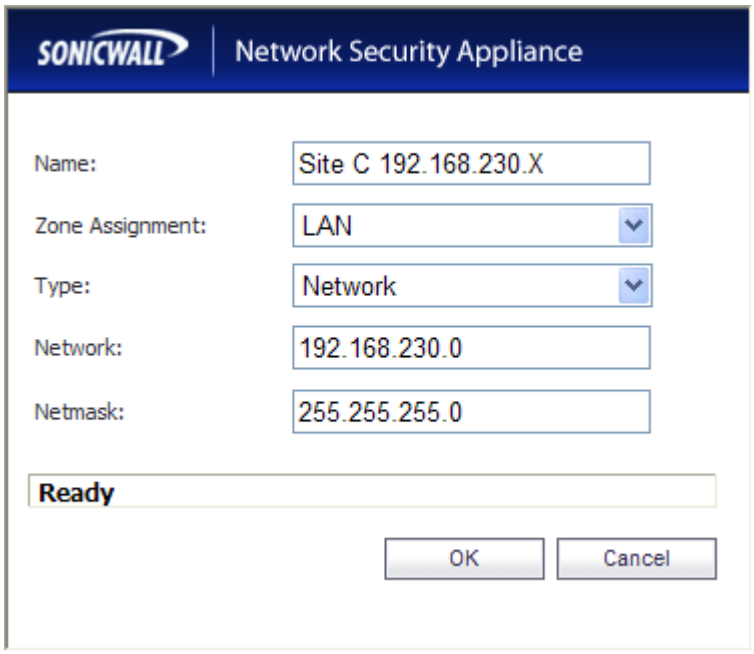
5.26.1 From the **Network → Interfaces,** click on the **Configure icon** " " for **X0** (LAN) and enter the following information for: **IP Assignment**, **IP Address** and **Subnet Mask** according to network structure to be used, Click **OK** to continue.



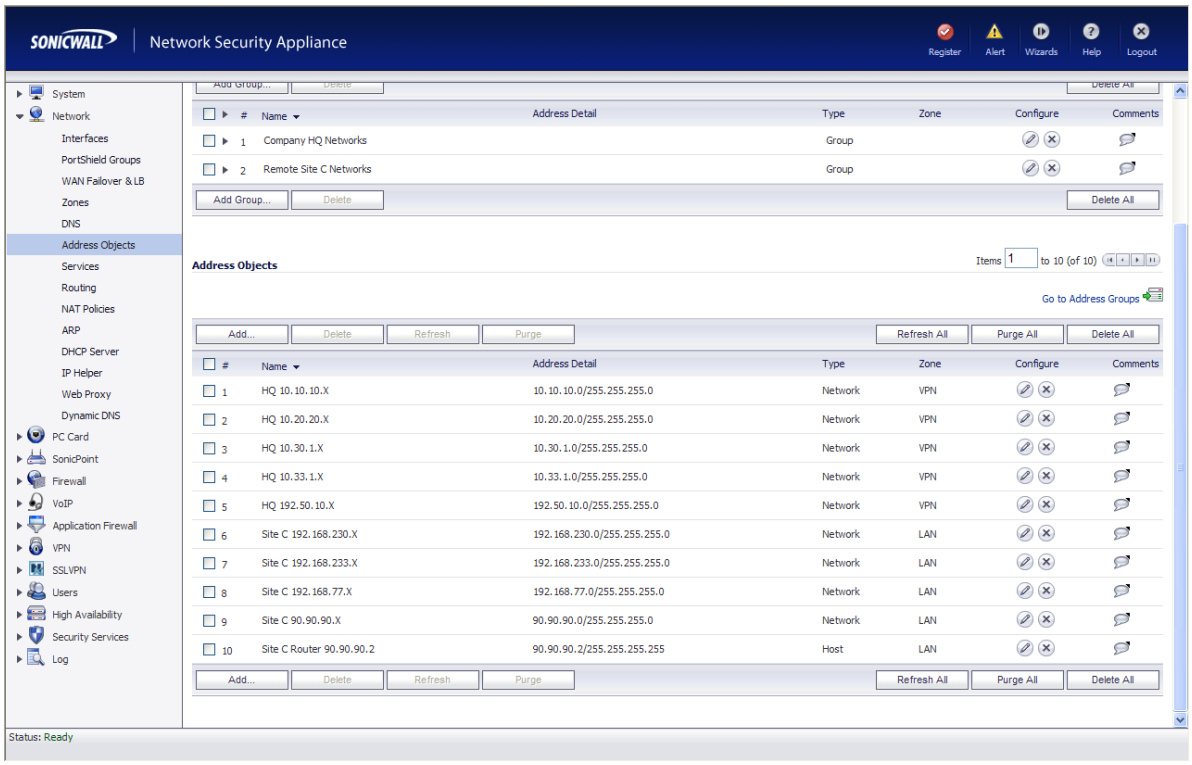
5.26.2	Repeat for the **X1** (WAN) interface.
5.26.3	Once configuration on the interfaces is completed, the following summary is presented.



5.27. Define networks

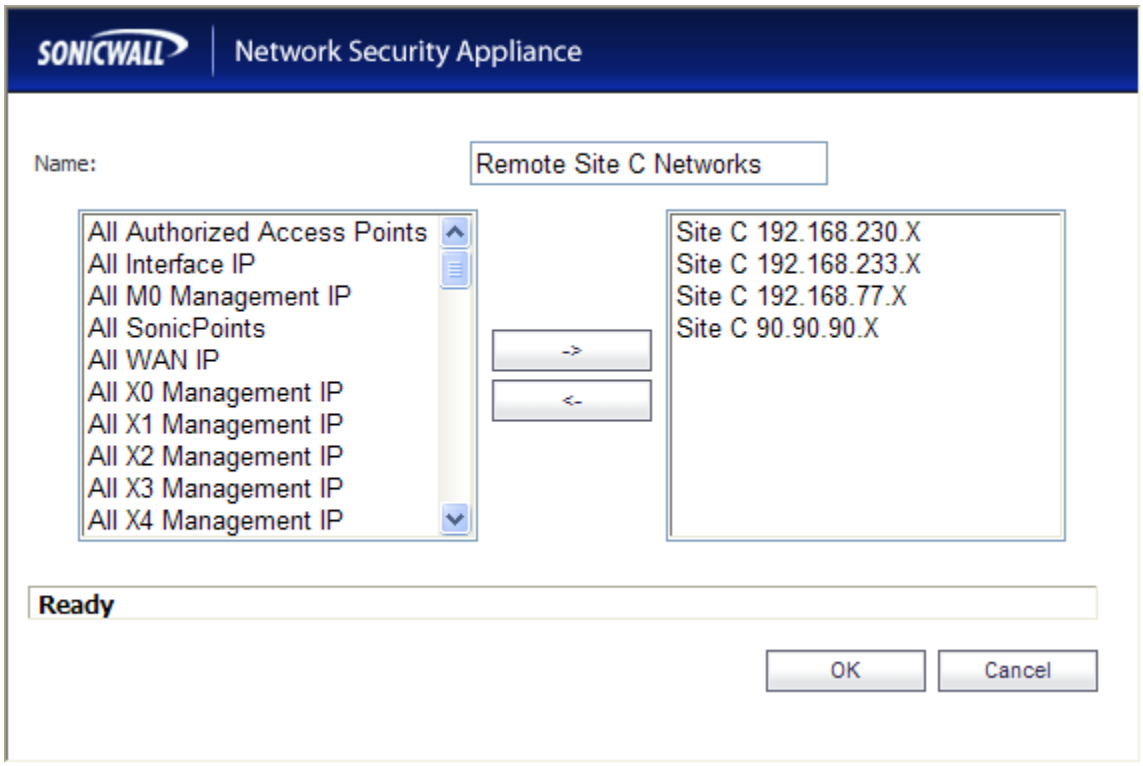
5.27.1	Create Address Objects for each of the networks within the deployment sites. From the **Network → Address Objects,** click on the **Add** button and enter the following information for: **Name**, **Zone Assignment**, **Network**, and **Netmask** for each subnet in the topology. Click **OK** to continue. 
5.27.2	Repeat Step **5.27.1** for each subnet in the topology. Refer to **Figure 1** for details of topology used for compliance testing.

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



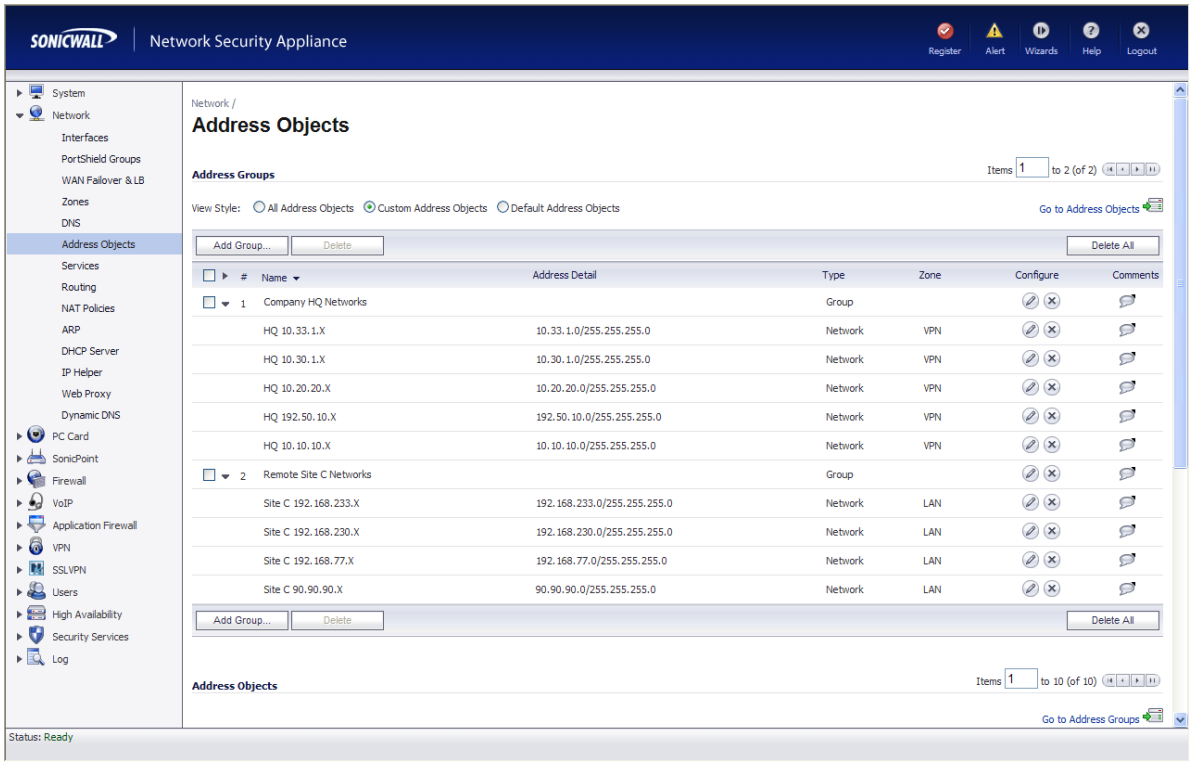
5.28. Group Address Objects based on site within topology

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.



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

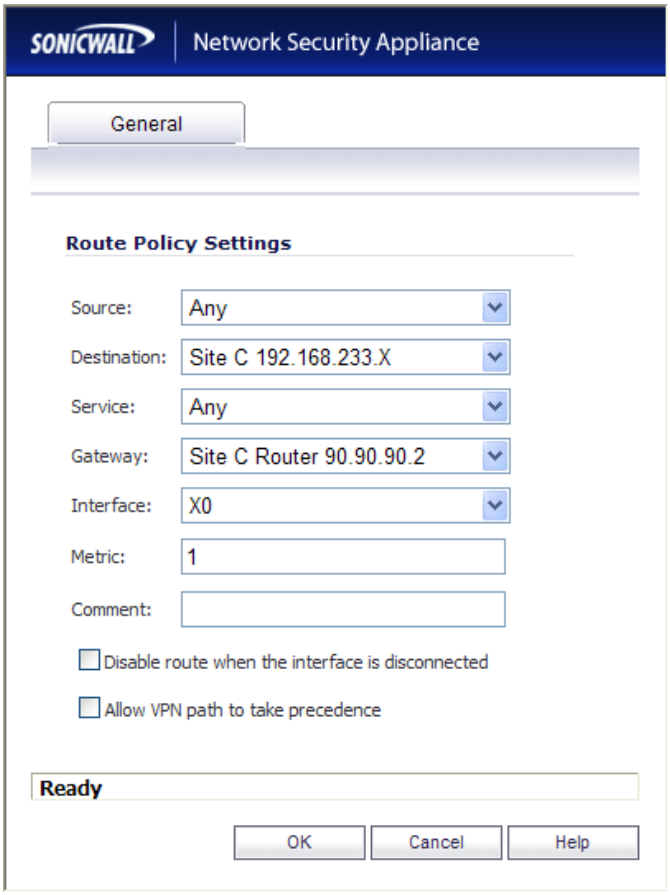
5.28.3 Once completed, the following Address Object Group summary is displayed.



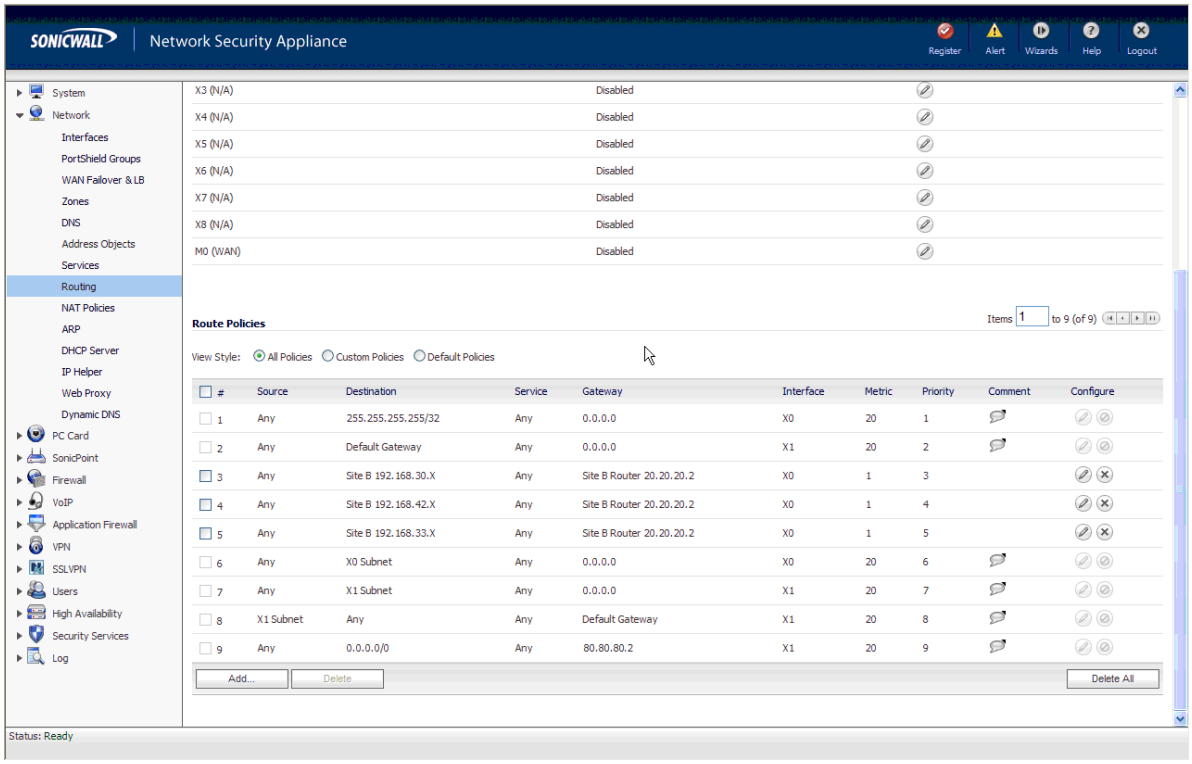
5.29. Define routes for 'local' networks.

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.
5.29.2	Repeat for each LAN subnet.

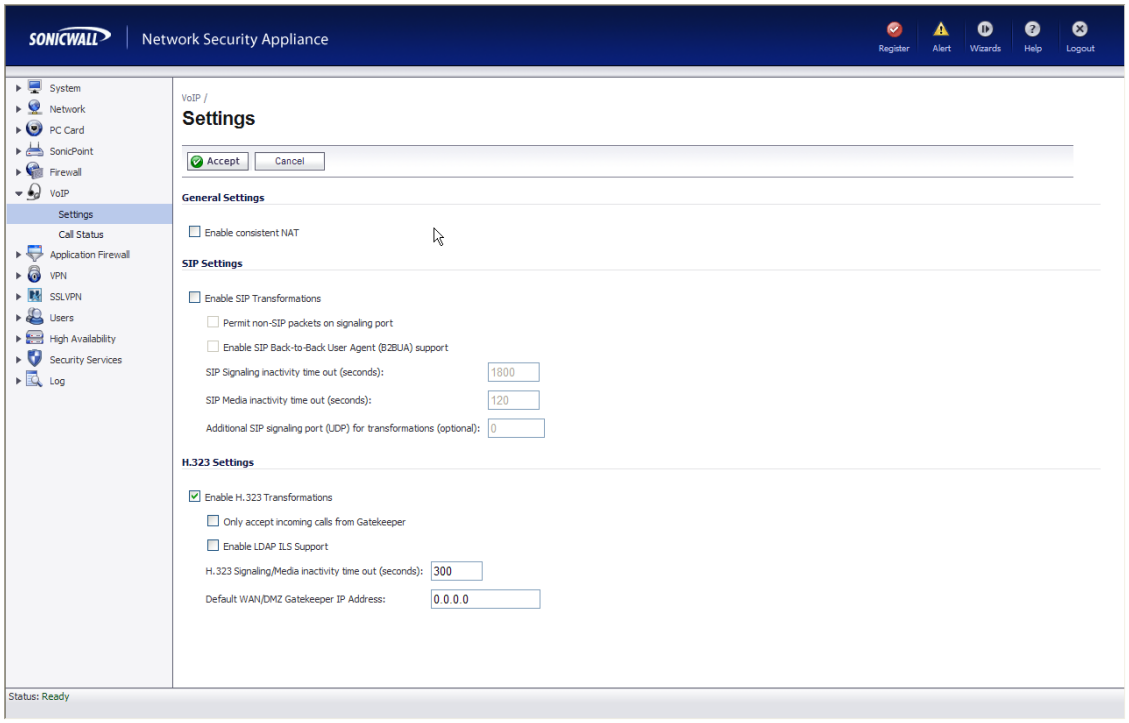


5.29.3 Once all of the LAN subnet routes have been added, the following routing summary is displayed.



5.30. Configure VoIP settings.

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

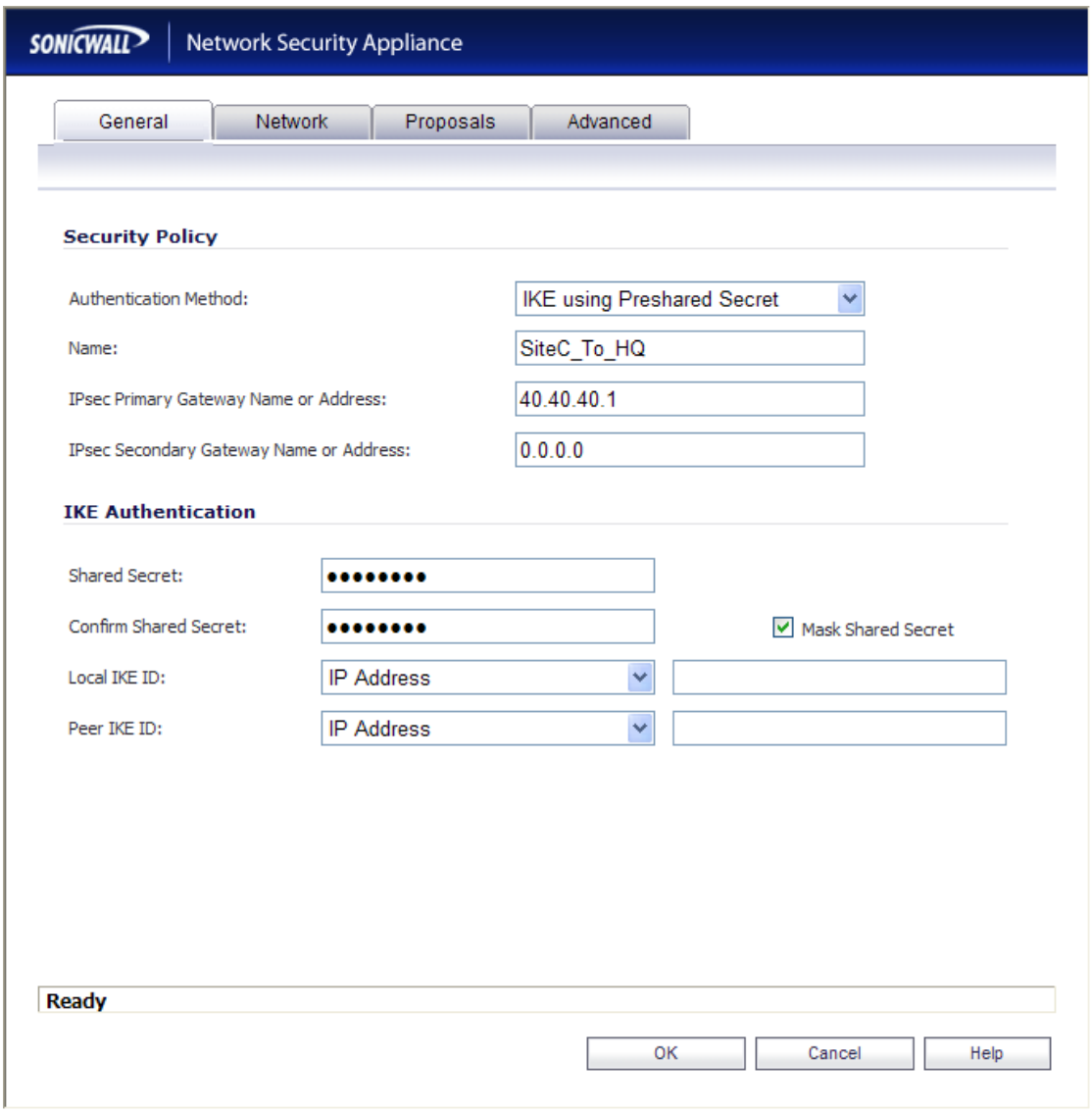


5.31. Create VPN policies

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**.

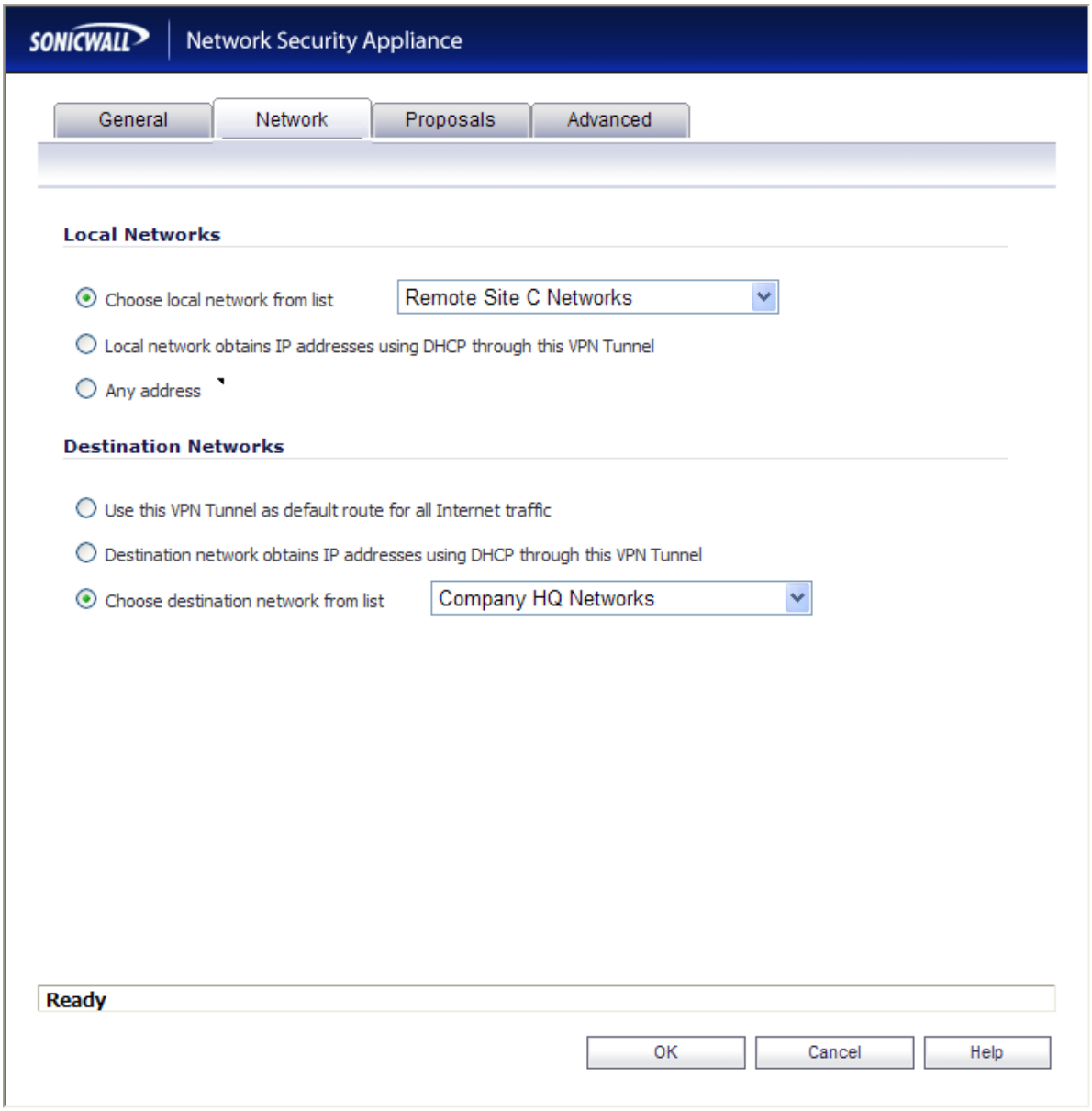
Click **Network** tab to continue.

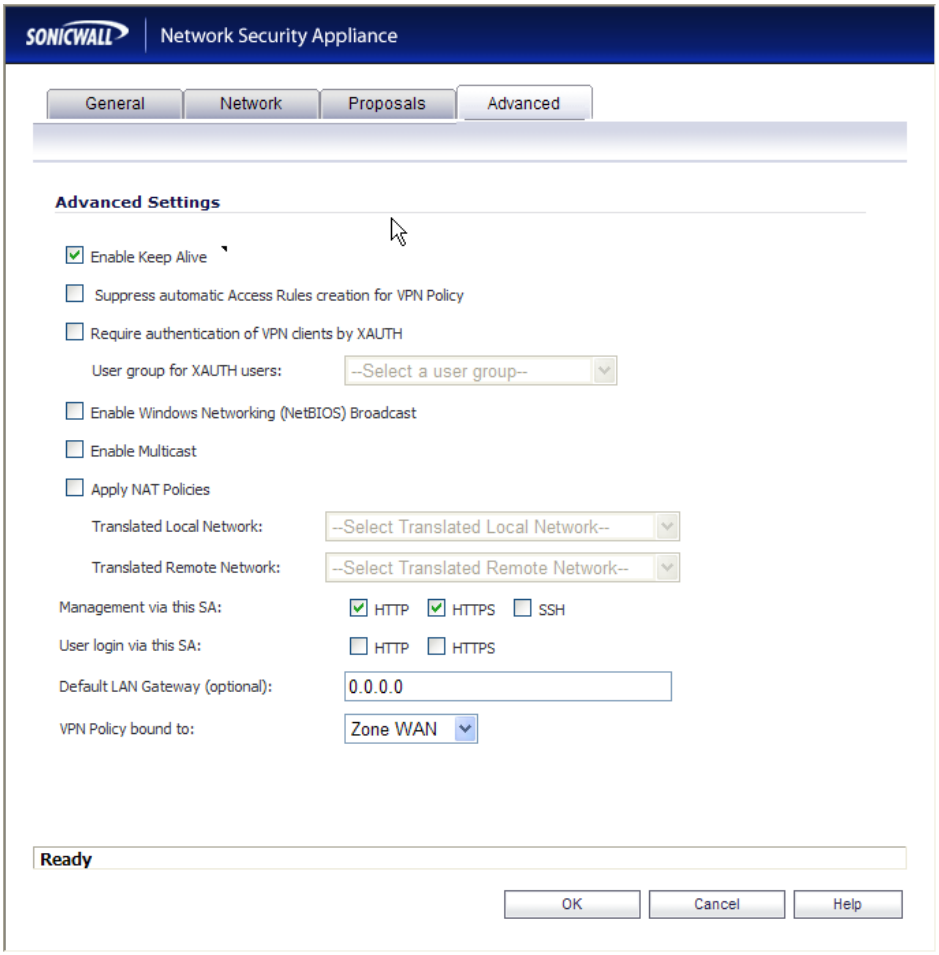


5.31.2

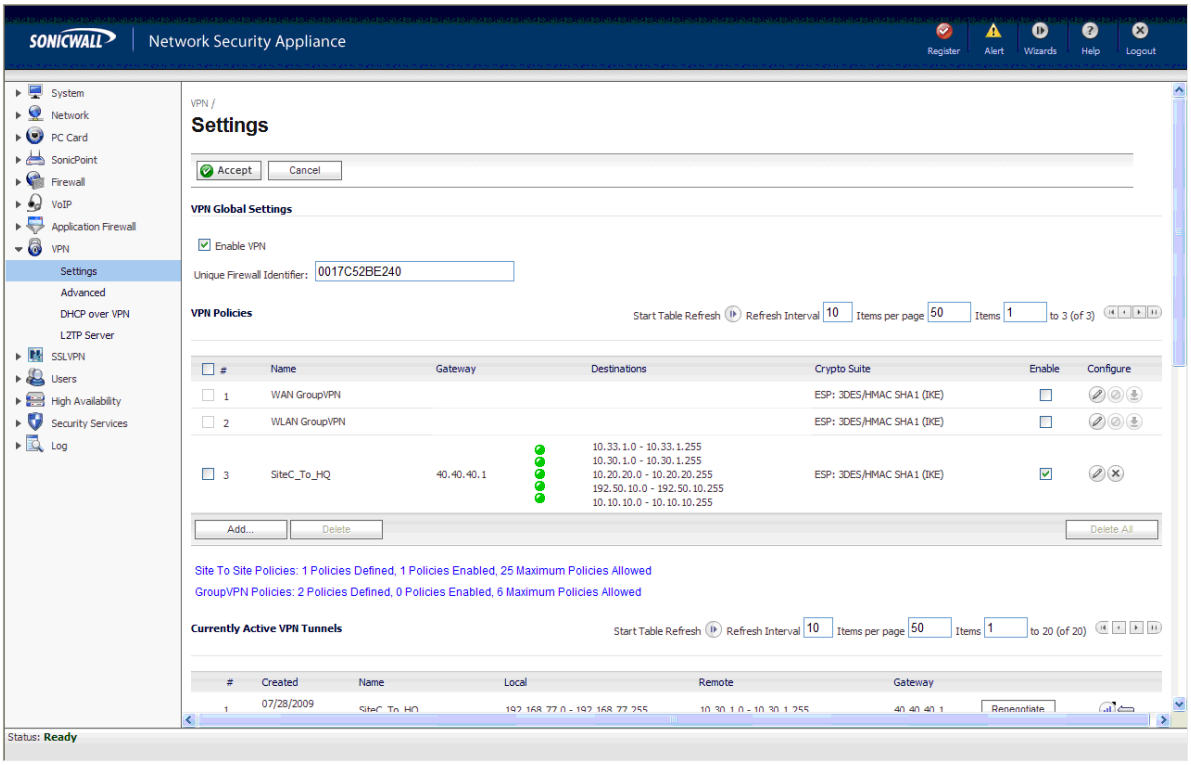
Specify subnets accessible over the VPN tunnel.

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.



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. 
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

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.