Avaya Solution & Interoperability Test Lab

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

## Abstract

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

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

# 1. Introduction

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

## 1.1. Interoperability Compliance Testing

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

The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call park, call pick-up, bridged call appearances, voicemail, 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. For compliance testing, the voice and data traffic were separated onto different VLANs.

## 2.1. Corporate Headquarters

The Corporate Headquarters consisted of one SonicWall NSA E5500, one router, one Avaya Aura™ Communication Manager Branch, two Avaya IP Telephones, one PC on DataVlan1 and a corporate DHCP/TFTP/HTTP server. The Corporate Headquarters provided a DHCP/File server for assigning IP network parameters and to download settings to the Avaya IP telephones. All Avaya IP telephones register to the Corporate Headquarters Avaya Aura™ Communication Manager Branch.

## 2.2. Remote Site A

Remote Site A consists of one SonicWall NSA 240, one router, two Avaya IP Telephones and one PC on DataVlan2. The Avaya IP telephones register to company headquarters Avaya Aura™ Communication Manager Branch.

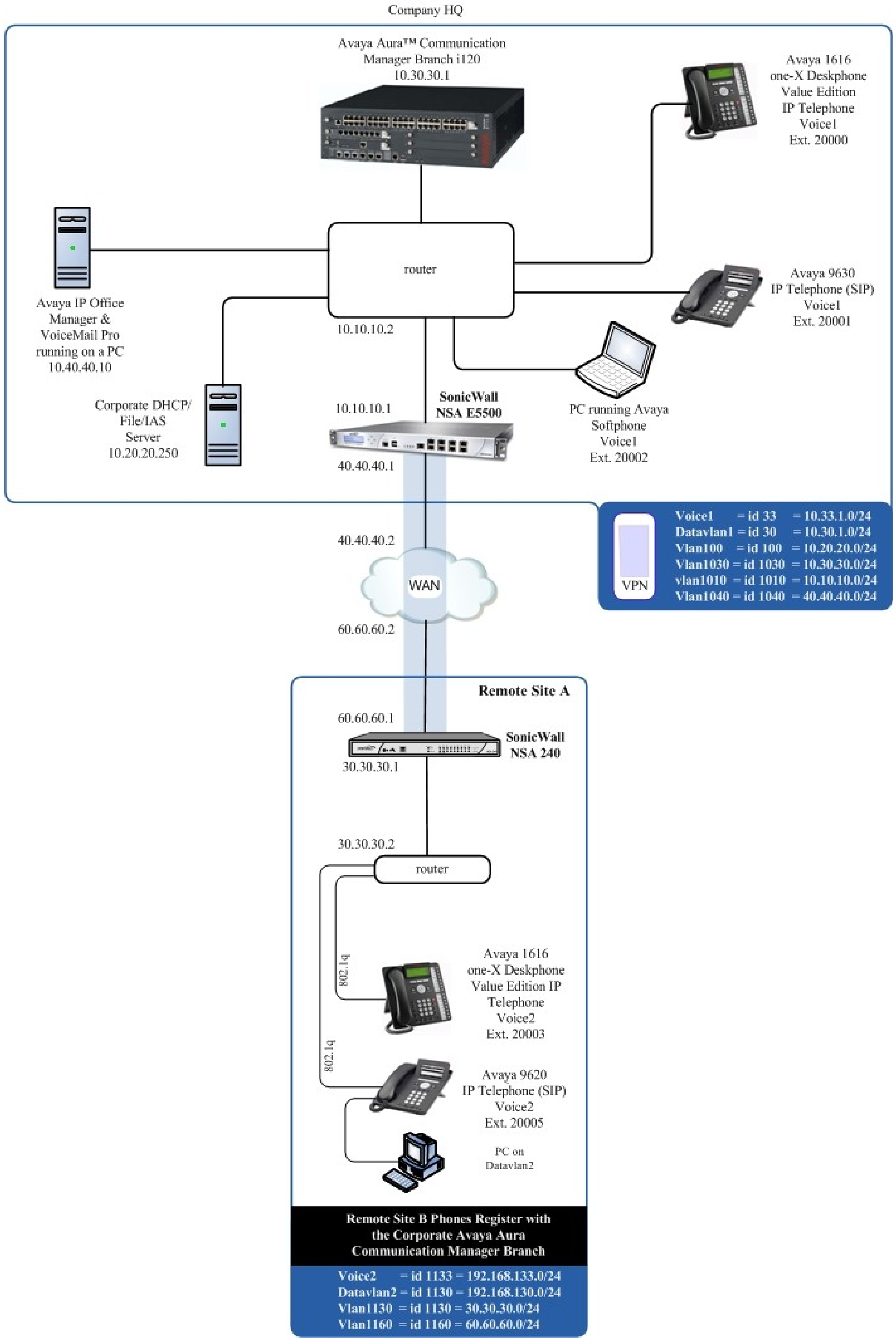

Company HQ
Avaya Aura™ Communication Manager Branch i120
10.30.30.1
Avaya 1616 one-X Deskphone Value Edition IP Telephone Voice1 Ext. 20000
router
Avaya 9630 IP Telephone (SIP) Voice1 Ext. 20001
Avaya IP Office Manager & VoiceMail Pro running on a PC
10.40.40.10
10.10.10.2
Corporate DHCP/ File/IAS Server
10.20.20.250
10.10.10.1
SonicWall NSA E5500
40.40.40.1
PC running Avaya Softphone Voice1 Ext. 20002
VPN
Voice1 = id 33 = 10.33.1.0/24
Datavlan1 = id 30 = 10.30.1.0/24
Vlan100 = id 100 = 10.20.20.0/24
Vlan1030 = id 1030 = 10.30.30.0/24
vlan1010 = id 1010 = 10.10.10.0/24
Vlan1040 = id 1040 = 40.40.40.0/24
40.40.40.2
WAN
60.60.60.2
Remote Site A
60.60.60.1
SonicWall NSA 240
30.30.30.1
30.30.30.2
router
802.1q
802.1q
Avaya 1616 one-X Deskphone Value Edition IP Telephone Voice2 Ext. 20003
Avaya 9620 IP Telephone (SIP) Voice2 Ext. 20005
PC on Datavlan2
Remote Site B Phones Register with the Corporate Avaya Aura Communication Manager Branch
Voice2 = id 1133 = 192.168.133.0/24
Datavlan2 = id 1130 = 192.168.130.0/24
Vlan1130 = id 1130 = 30.30.30.0/24
Vlan1160 = id 1160 = 60.60.60.0/24

**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 Aura™ Communication Manager Branch (i120) | 2.0.0_28.01 |
| **Avaya Telephony Sets** | |
| Avaya 1600 Series IP Telephones | Avaya one-X Deskphone Value 1.2 |
| Avaya 9600 Series IP Telephones | Avaya one-X Deskphone SIP 2.0.0 |
| **SonicWALL Products** | |
| SonicWall NSA E5500 | 5.2.0.1-21o |
| SonicWall NSA 240 | 5.2.0.1-21o |
| **MS Products** | |
| PC | Microsoft Windows 2003 Server (Running Avaya Aura™ Communication Manager Branch Manager and Avaya Aura™ Communication Manager Branch Phone Manager Pro) and (File/DHCP Service) |

# 4. Avaya Aura™ Communication Manager Branch Configuration

Communication Manager Branch is administered via a web interface. In the sample network the Communication Manager Branch was assigned the IP address 10.30.30.1 and the URL http://10.30.30.1 was used to access the administration interface. For information on how to access and setup a factory default system, refer to **Section 9, Reference** [**1**].

## 4.1. Configure QoS

IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. QoS is now utilized to prioritize VoIP traffic and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. Communication Manager Branch and Avaya IP telephones support both 802.1p and DiffServ.

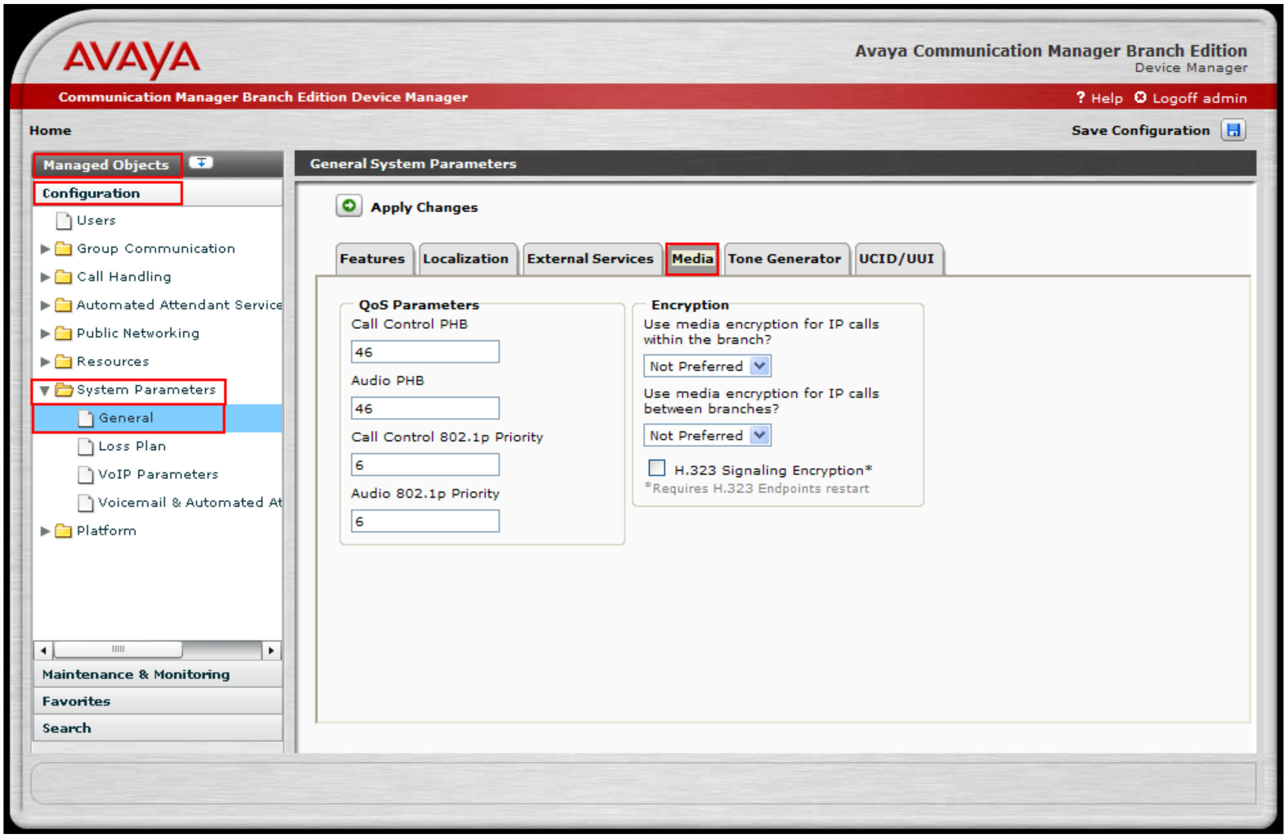
The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP Telephones via Communication Manager Branch. Avaya SIP IP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server. For more information on QoS settings please refer to **Section 9, Reference** [**1**].

**Description**

Navigate to the **General System Parameters** window, from **Manage Objects**, click **Configuration→ System Parameters → General → Media.** Set the following **QoS Parameters:**

- **Call Control PHB Value** to **46**
- **Audio PHB Value** to **46**
- **Call Control 802.1p Priority** to **6**
- **Audio 802.1p Priority** to **6**

Click **Apply Changes** and then click **Save Configuration**.



QoS Parameters

Call Control PHB: 46

Audio PHB: 46

Call Control 802.1p Priority: 6

Audio 802.1p Priority: 6

Encryption

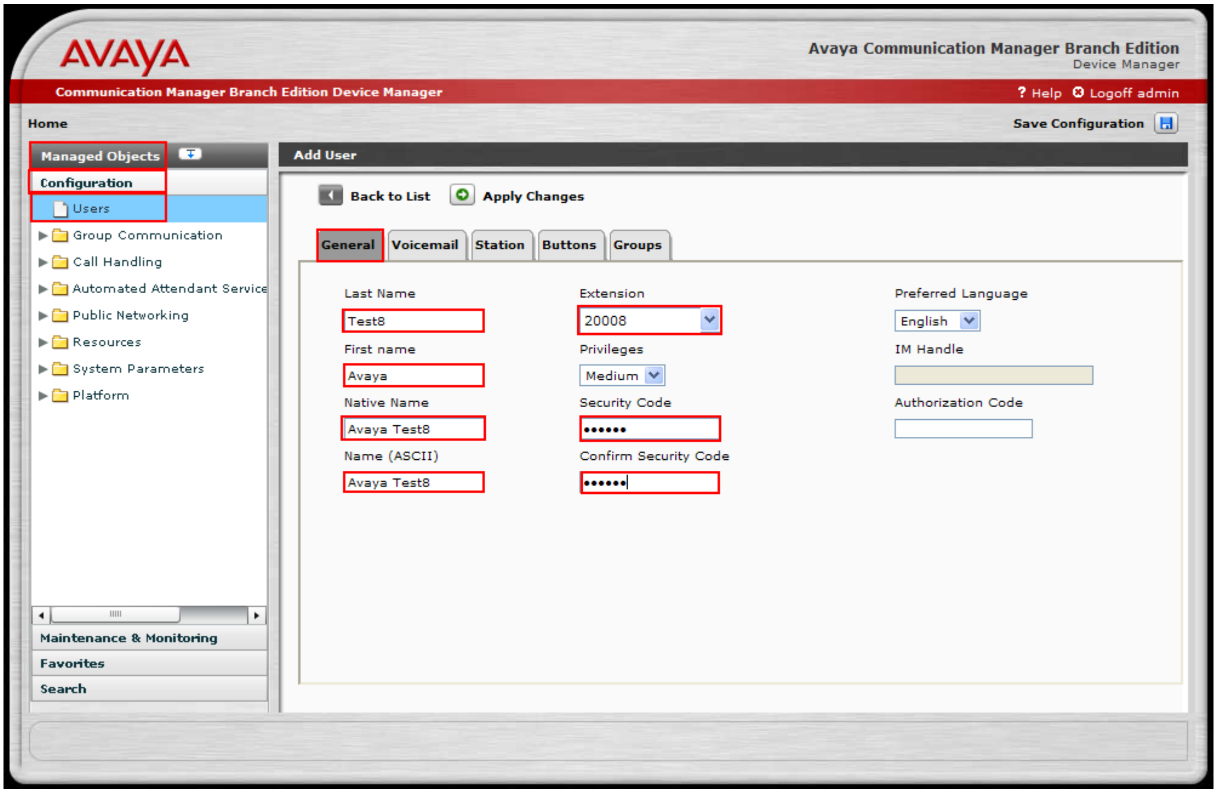
Use media encryption for IP calls within the branch? Not Preferred

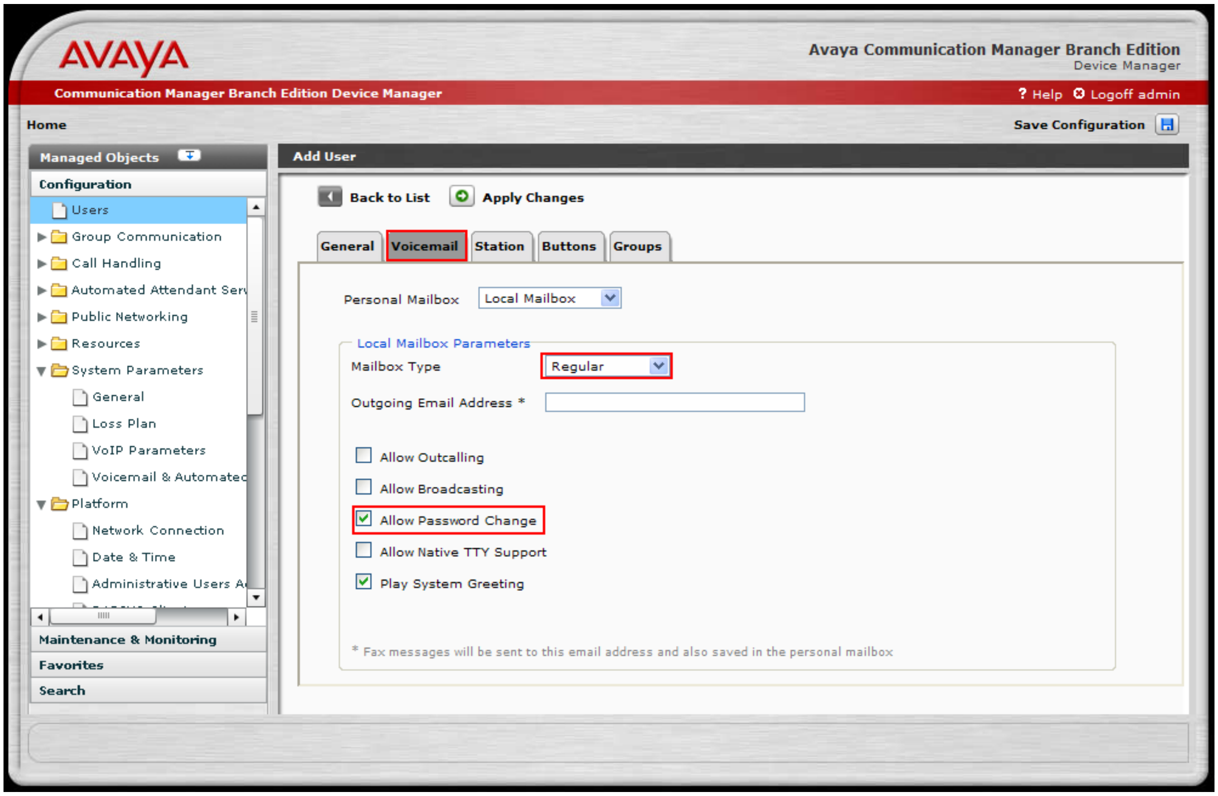
Use media encryption for IP calls between branches? Not Preferred

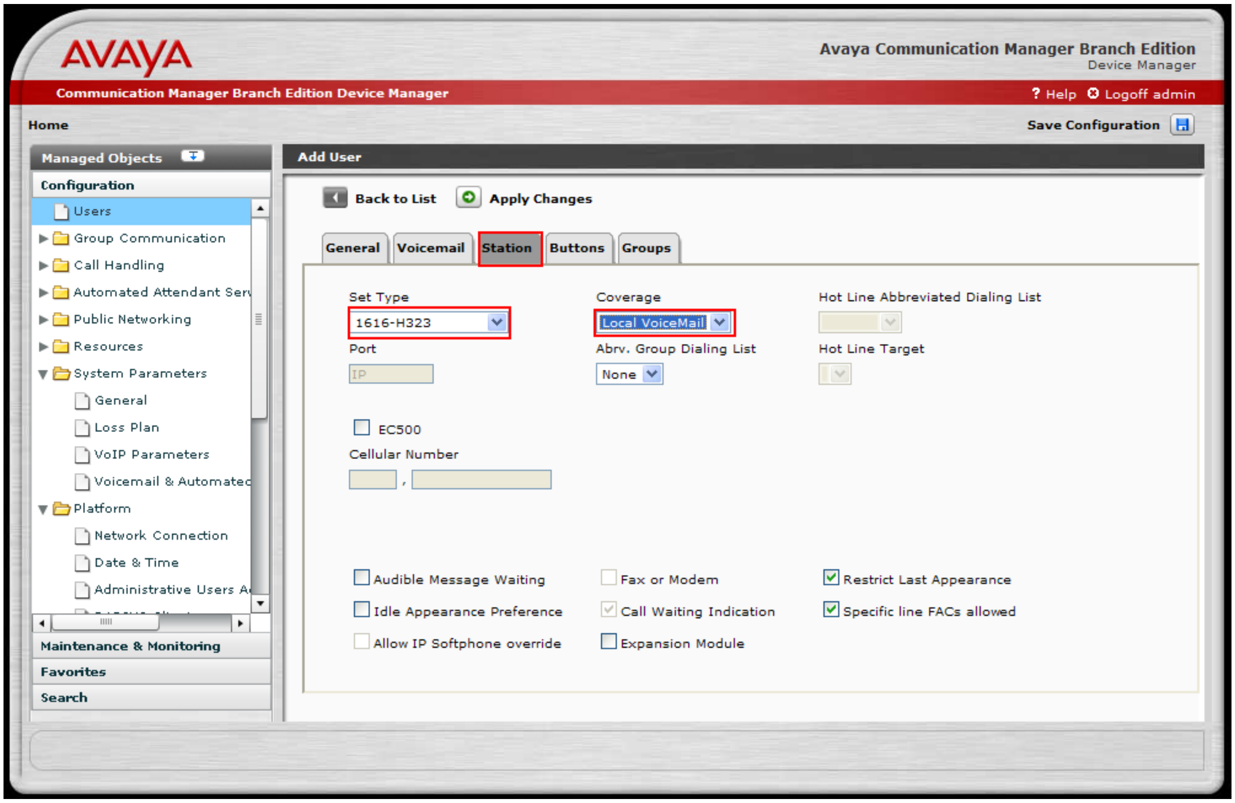
□ H.323 Signaling Encryption*

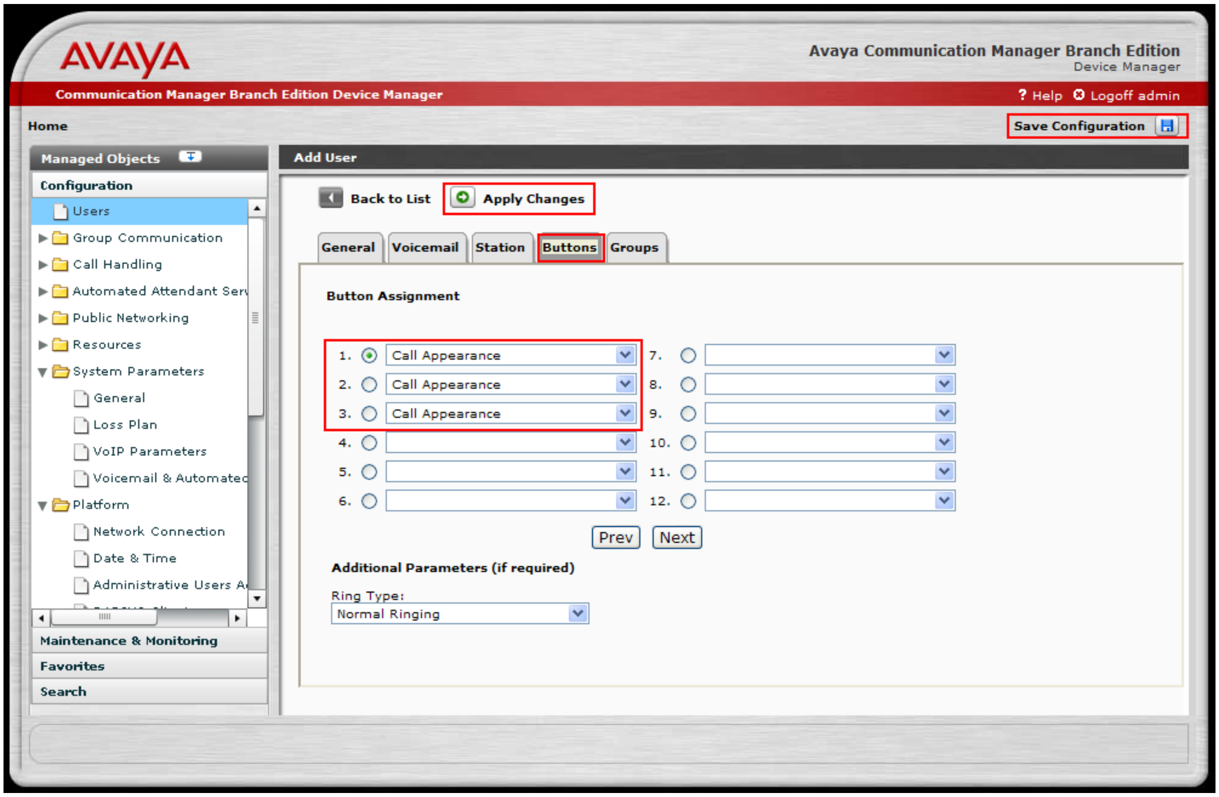
*Requires H.323 Endpoints restart

## 4.2. Configure Station

| Step | Description |
|---|---|
| 1. | Navigate to the **Add User** window, from **Manage Objects**, **click Configuration→Users → Add New User**. Enter the values displayed below and then click **Apply Changes**. **Last Name**, **First name** and **Native Name** can be any descriptive text that identifies this user. **Name (ASCII)** may be populated with the same information that is entered in **Native Name**. Enter the **Security Code** and **Confirm Security Code** information. Use the drop-down list for **Extension** and select any available extension. The remaining parameters were left at the default values. Select the **Voicemail tab** to continue.<br><br> AVAYA<br>Avaya Communication Manager Branch Edition<br>Device Manager<br>Communication Manager Branch Edition Device Manager<br>? Help<br>Logoff admin<br>Home<br>Save Configuration<br>Managed Objects<br>Configuration<br>Users<br>Group Communication<br>Call Handling<br>Automated Attendant Service<br>Public Networking<br>Resources<br>System Parameters<br>Platform<br>Maintenance & Monitoring<br>Favorites<br>Search<br>Add User<br>Back to List<br>Apply Changes<br>General<br>Voicemail<br>Station<br>Buttons<br>Groups<br>Last Name: Test8<br>First name: Avaya<br>Native Name: Avaya Test8<br>Name (ASCII): Avaya Test8<br>Extension: 20008<br>Privileges: Medium<br>Security Code: ••••••<br>Confirm Security Code: ••••••<br>Preferred Language: English<br>IM Handle:<br>Authorization Code: |

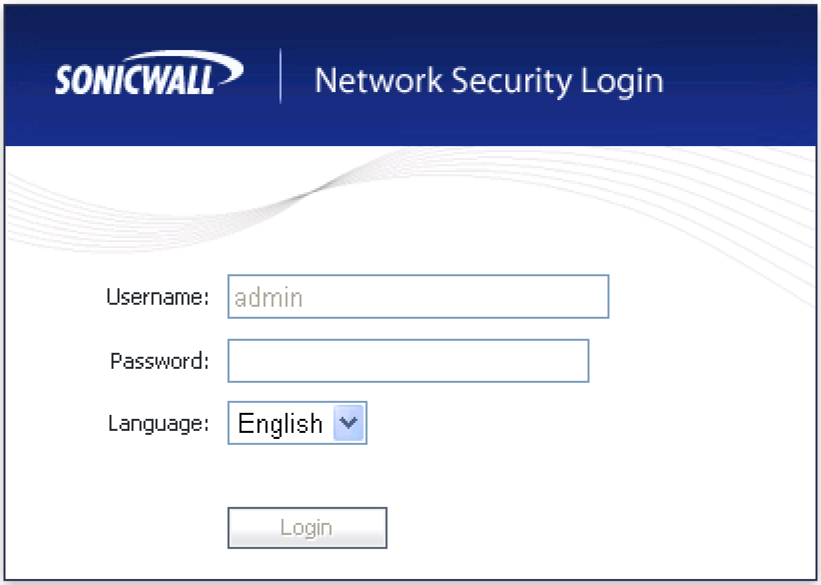
| Step | Description |
|---|---|
| 2. | Check the **Allow Password Change** check box. Use the drop-down list for **Mailbox Type** to select **Regular.** Press the **Station** tab to continue.<br><br> AVAYA<br>Avaya Communication Manager Branch Edition<br>Device Manager<br>Communication Manager Branch Edition Device Manager<br>? Help Logoff admin<br>Home<br>Save Configuration<br>Managed Objects<br>Configuration<br>Users<br>Group Communication<br>Call Handling<br>Automated Attendant Serv<br>Public Networking<br>Resources<br>System Parameters<br>General<br>Loss Plan<br>VoIP Parameters<br>Voicemail & Automated<br>Platform<br>Network Connection<br>Date & Time<br>Administrative Users A<br>Maintenance & Monitoring<br>Favorites<br>Search<br>Add User<br>Back to List<br>Apply Changes<br>General<br>Voicemail<br>Station<br>Buttons<br>Groups<br>Personal Mailbox: Local Mailbox<br>Local Mailbox Parameters<br>Mailbox Type: Regular<br>Outgoing Email Address *<br>☐ Allow Outcalling<br>☐ Allow Broadcasting<br>☑ Allow Password Change<br>☐ Allow Native TTY Support<br>☑ Play System Greeting<br>* Fax messages will be sent to this email address and also saved in the personal mailbox |

| Step | Description |
|---|---|
| 3. | Use the drop-down list for **Set Type** to select **1616-H323** and use the drop-down list for **Coverage** to select **Local VoiceMail**. The remaining parameters were left at the default values. Press the **Buttons** tab to continue.<br><br> AVAYA<br>Avaya Communication Manager Branch Edition<br>Device Manager<br>Communication Manager Branch Edition Device Manager<br>? Help<br>Logoff admin<br>Home<br>Save Configuration<br>Managed Objects<br>Configuration<br>Users<br>Group Communication<br>Call Handling<br>Automated Attendant Serv<br>Public Networking<br>Resources<br>System Parameters<br>General<br>Loss Plan<br>VoIP Parameters<br>Voicemail & Automated<br>Platform<br>Network Connection<br>Date & Time<br>Administrative Users A<br>Maintenance & Monitoring<br>Favorites<br>Search<br>Add User<br>Back to List<br>Apply Changes<br>General<br>Voicemail<br>Station<br>Buttons<br>Groups<br>Set Type: 1616-H323<br>Coverage: Local VoiceMail<br>Hot Line Abbreviated Dialing List<br>Port: IP<br>Abrv. Group Dialing List: None<br>Hot Line Target<br>☐ EC500<br>Cellular Number<br>☐ Audible Message Waiting<br>☐ Fax or Modem<br>☑ Restrict Last Appearance<br>☐ Idle Appearance Preference<br>☑ Call Waiting Indication<br>☑ Specific line FACs allowed<br>☐ Allow IP Softphone override<br>☐ Expansion Module |

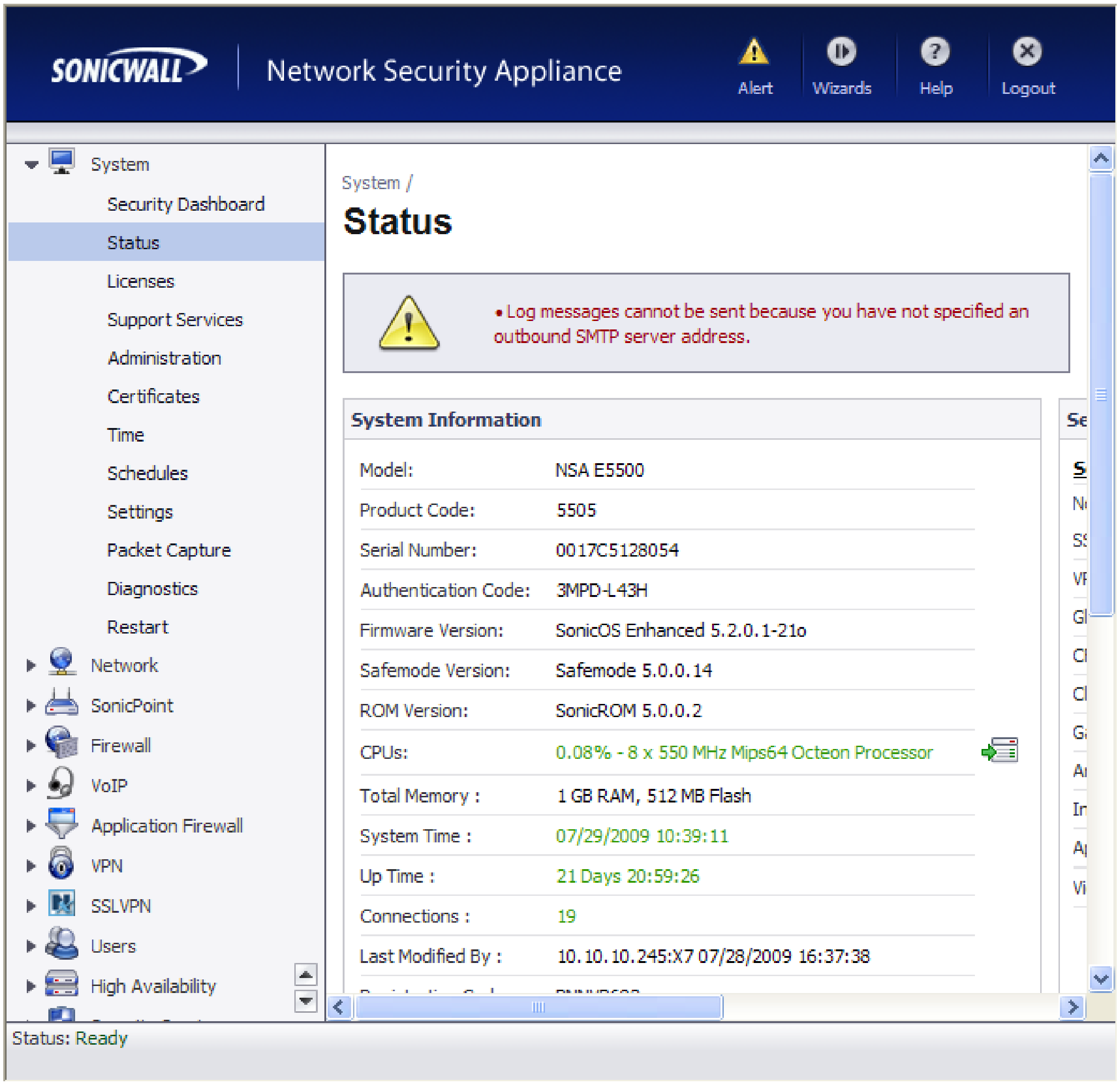
| Step | Description |
|---|---|
| 4. | Use the drop list for **Button Assignment 1 – 3** and select **Call Appearance**. The remaining parameters were left at the default values. Click **Apply Changes** and then click **Save Configuration**.<br>Note the user may receive a message indicating the system is busy if **Save Configuration** is clicked immediately after **Apply Changes**. If that occurs, simply click **Save Configuration** after one or two minutes.<br><br> AVAYA<br>Avaya Communication Manager Branch Edition<br>Device Manager<br>Communication Manager Branch Edition Device Manager<br>? Help<br>Logoff admin<br>Home<br>Save Configuration<br>Managed Objects<br>Configuration<br>Users<br>Group Communication<br>Call Handling<br>Automated Attendant Serv<br>Public Networking<br>Resources<br>System Parameters<br>General<br>Loss Plan<br>VoIP Parameters<br>Voicemail & Automated<br>Platform<br>Network Connection<br>Date & Time<br>Administrative Users A<br>Maintenance & Monitoring<br>Favorites<br>Search<br>Add User<br>Back to List<br>Apply Changes<br>General<br>Voicemail<br>Station<br>Buttons<br>Groups<br>Prev<br>Next<br>Button Assignment<br>1. ● Call Appearance<br>2. ○ Call Appearance<br>3. ○ Call Appearance<br>4. ○<br>5. ○<br>6. ○<br>7. ○<br>8. ○<br>9. ○<br>10. ○<br>11. ○<br>12. ○<br>Additional Parameters (if required)<br>Ring Type: Normal Ringing |
| 5. | Repeat Steps 1 thru 4 for each Avaya IP Telephone. |

# 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].**<br>Log into the NSA 5500.<br>1. Connect the LAN port of the computer being used to the X0 (LAN) port on the SonicWall NSA E5500.<br>2. Start the **Management Tool** as follows: Start your web browser and enter **http://192.168.168.168** Press Enter.<br>3. Log in to the SonicWall NSA E5500 using default credentials which can be obtained from the SonicWALL documentation.<br><br>Network Security Login<br>Username: admin<br>Password:<br>Language: English<br> |

**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**.



System /

Status

• Log messages cannot be sent because you have not specified an outbound SMTP server address.

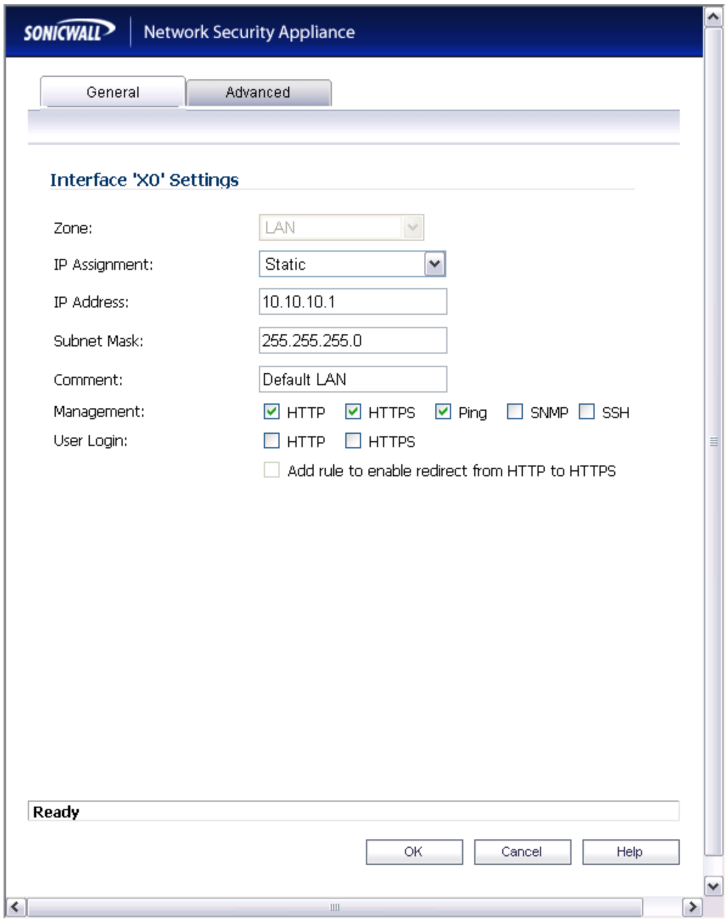
System Information

| | |
|---|---|
| Model: | NSA E5500 |
| Product Code: | 5505 |
| Serial Number: | 0017C5128054 |
| Authentication Code: | 3MPD-L43H |
| Firmware Version: | SonicOS Enhanced 5.2.0.1-21o |
| Safemode Version: | Safemode 5.0.0.14 |
| ROM Version: | SonicROM 5.0.0.2 |
| CPUs: | 0.08% - 8 x 550 MHz Mips64 Octeon Processor |
| Total Memory : | 1 GB RAM, 512 MB Flash |
| System Time : | 07/29/2009 10:39:11 |
| Up Time : | 21 Days 20:59:26 |
| Connections : | 19 |
| Last Modified By : | 10.10.10.245:X7 07/28/2009 16:37:38 |

Status: Ready

## 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, **IP Addres**s and **Subnet Mask** according to network structure to be used, Click **OK** to continue.



Interface 'X0' Settings

Zone: LAN

IP Assignment: Static

IP Address: 10.10.10.1

Subnet Mask: 255.255.255.0

Comment: Default LAN

Management: ☑ HTTP ☑ HTTPS ☑ Ping □ SNMP □ SSH

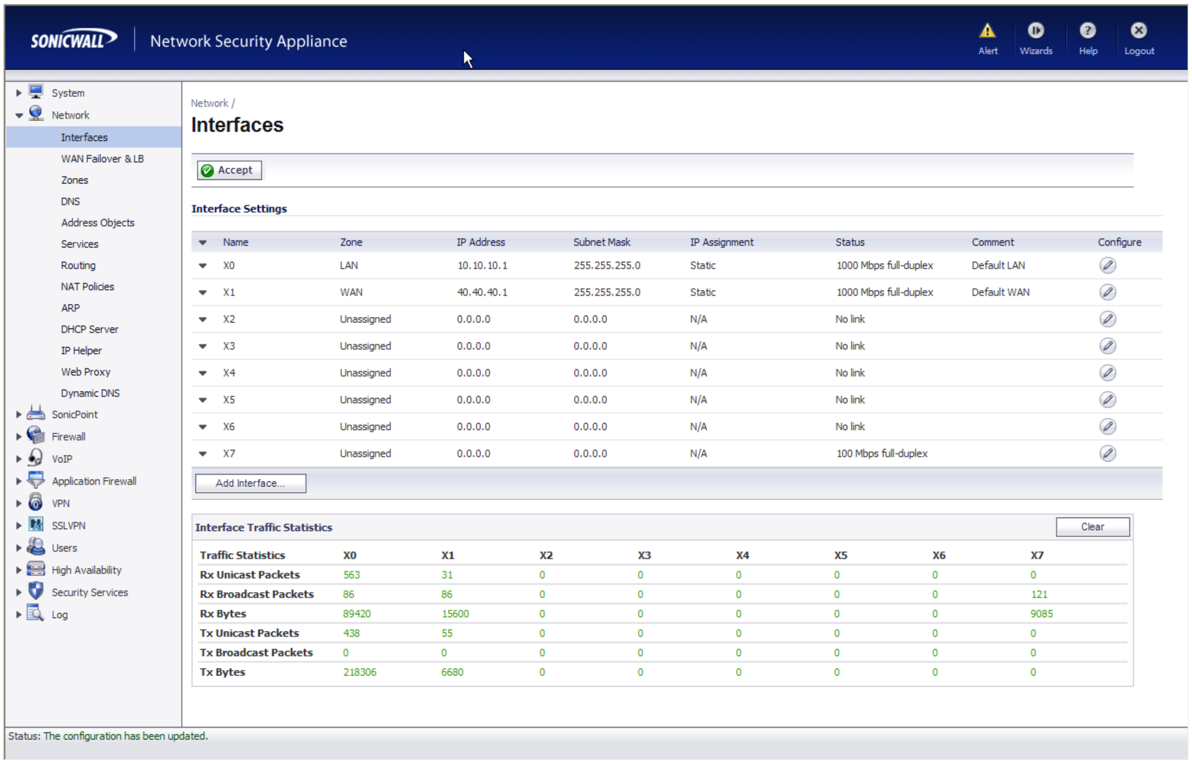
User Login: □ HTTP □ HTTPS

□ Add rule to enable redirect from HTTP to HTTPS

Ready

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

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



Interfaces

Interface Settings

| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|---|---|---|---|---|---|---|---|
| X0 | LAN | 10.10.10.1 | 255.255.255.0 | Static | 1000 Mbps full-duplex | Default LAN | |
| X1 | WAN | 40.40.40.1 | 255.255.255.0 | Static | 1000 Mbps full-duplex | Default WAN | |
| X2 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| X3 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| X4 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| X5 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| X6 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| X7 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | 100 Mbps full-duplex | | |

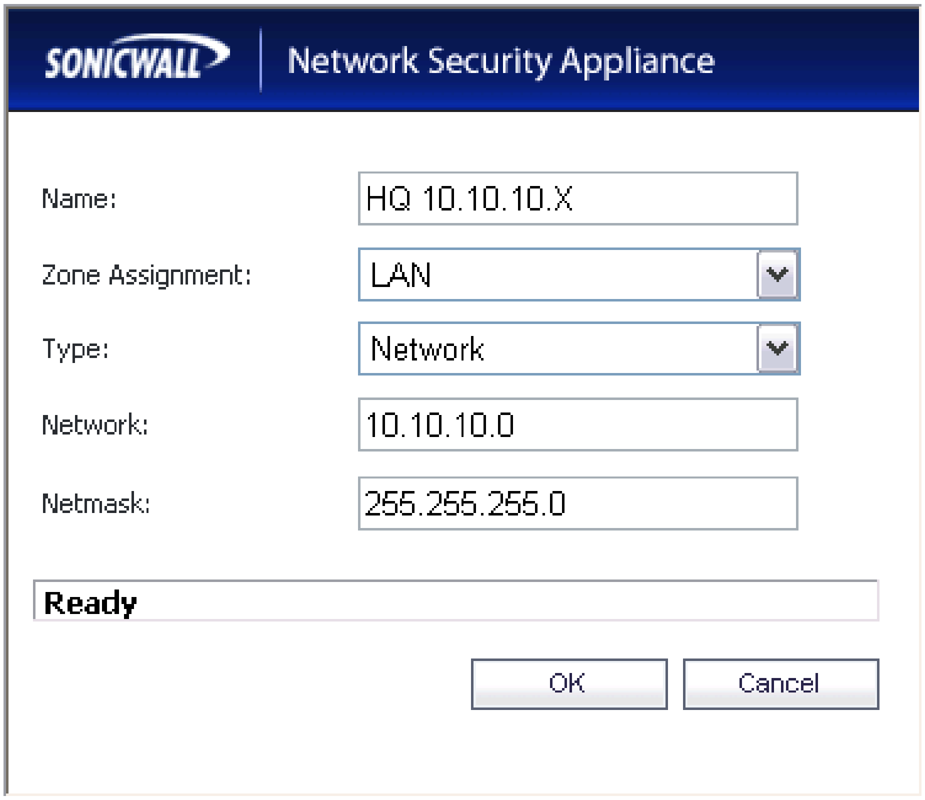
Interface Traffic Statistics

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

Status: The configuration has been updated.

## 5.3. Define networks

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



Name: HQ 10.10.10.X

Zone Assignment: LAN

Type: Network

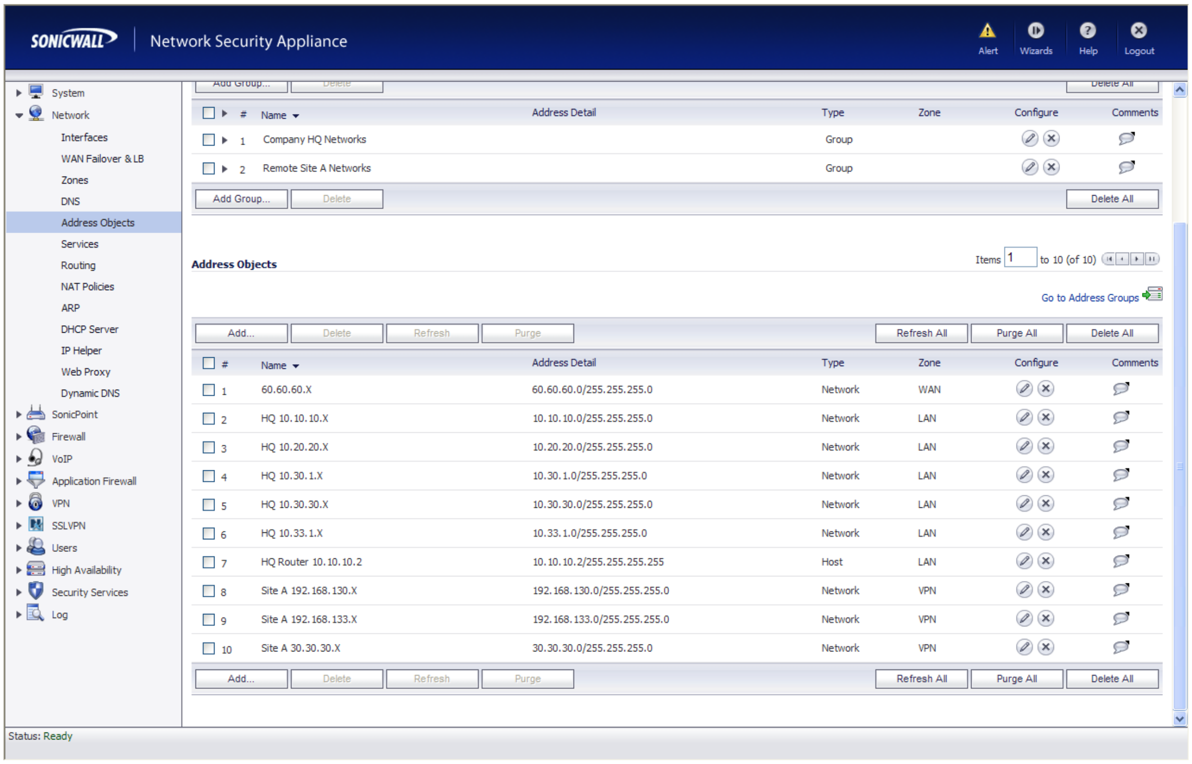
Network: 10.10.10.0

Netmask: 255.255.255.0

Ready

**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 | Company HQ Networks | | Group | | | |
| 2 | Remote Site A Networks | | Group | | | |

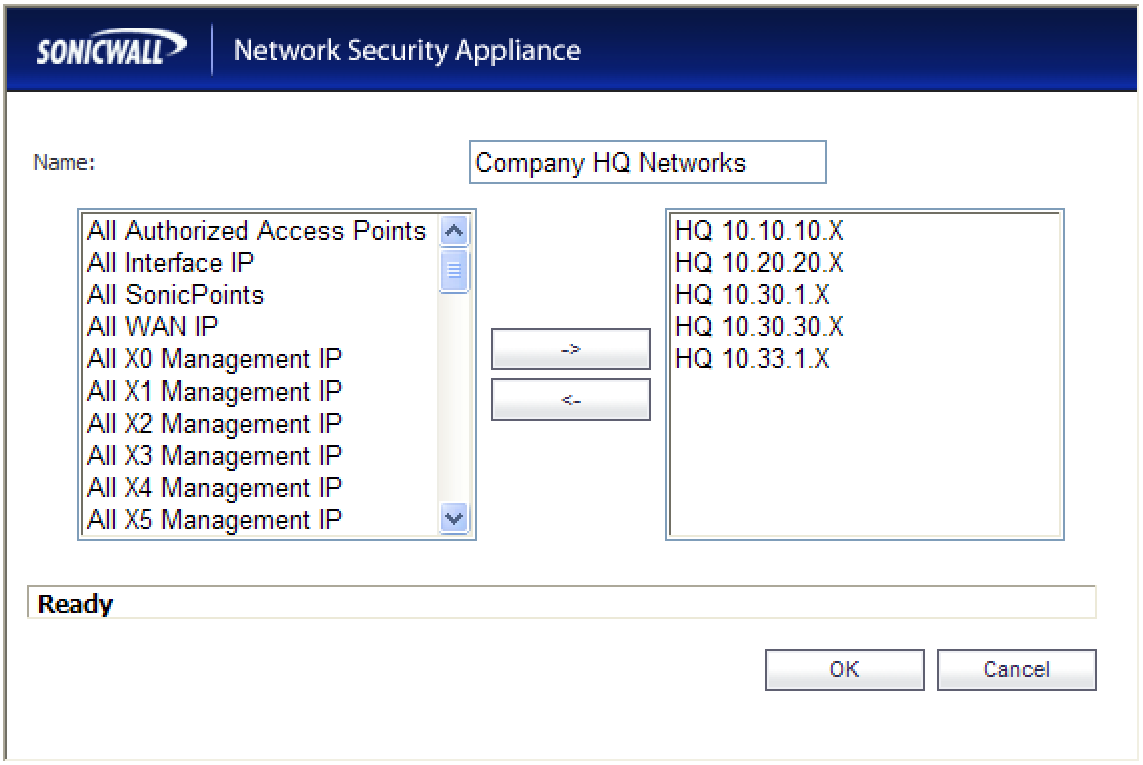
Address Objects

Items 1 to 10 (of 10)

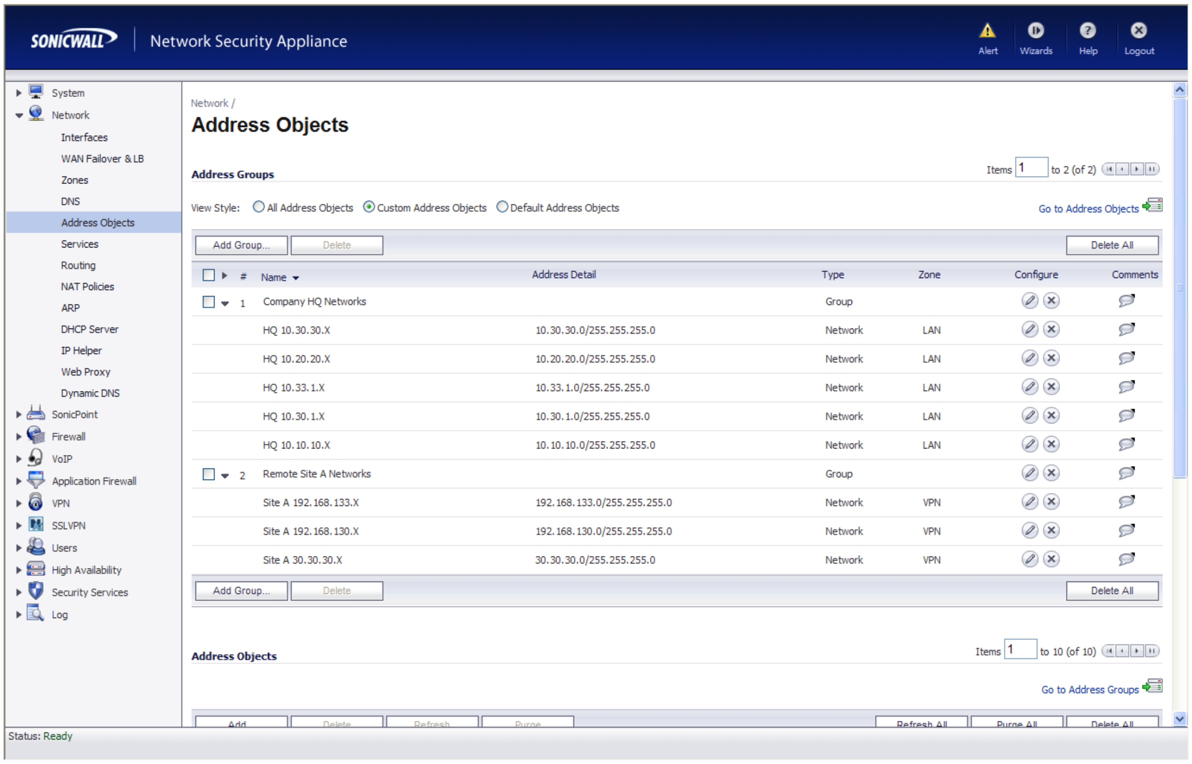
| # | Name | Address Detail | Type | Zone | Configure | Comments |
|---|---|---|---|---|---|---|
| 1 | 60.60.60.X | 60.60.60.0/255.255.255.0 | Network | WAN | | |
| 2 | HQ 10.10.10.X | 10.10.10.0/255.255.255.0 | Network | LAN | | |
| 3 | HQ 10.20.20.X | 10.20.20.0/255.255.255.0 | Network | LAN | | |
| 4 | HQ 10.30.1.X | 10.30.1.0/255.255.255.0 | Network | LAN | | |
| 5 | HQ 10.30.30.X | 10.30.30.0/255.255.255.0 | Network | LAN | | |
| 6 | HQ 10.33.1.X | 10.33.1.0/255.255.255.0 | Network | LAN | | |
| 7 | HQ Router 10.10.10.2 | 10.10.10.2/255.255.255.255 | Host | LAN | | |
| 8 | Site A 192.168.130.X | 192.168.130.0/255.255.255.0 | Network | VPN | | |
| 9 | Site A 192.168.133.X | 192.168.133.0/255.255.255.0 | Network | VPN | | |
| 10 | Site A 30.30.30.X | 30.30.30.0/255.255.255.0 | 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.<br><br> <br>Name: Company HQ Networks<br>All Authorized Access Points<br>All Interface IP<br>All SonicPoints<br>All WAN IP<br>All X0 Management IP<br>All X1 Management IP<br>All X2 Management IP<br>All X3 Management IP<br>All X4 Management IP<br>All X5 Management IP<br>HQ 10.10.10.X<br>HQ 10.20.20.X<br>HQ 10.30.1.X<br>HQ 10.30.30.X<br>HQ 10.33.1.X<br>Ready<br> |
| **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.



Network /

Address Objects

Address Groups

Items 1 to 2 (of 2)

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

Go to Address Objects

Add Group... Delete Delete All

| □ | # | Name | Address Detail | Type | Zone |
|---|---|---|---|---|---|
| □ | 1 | Company HQ Networks | | Group | |
| | | HQ 10.30.30.X | 10.30.30.0/255.255.255.0 | 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 |

Add Group... Delete Delete All

Address Objects

Items 1 to 10 (of 10)

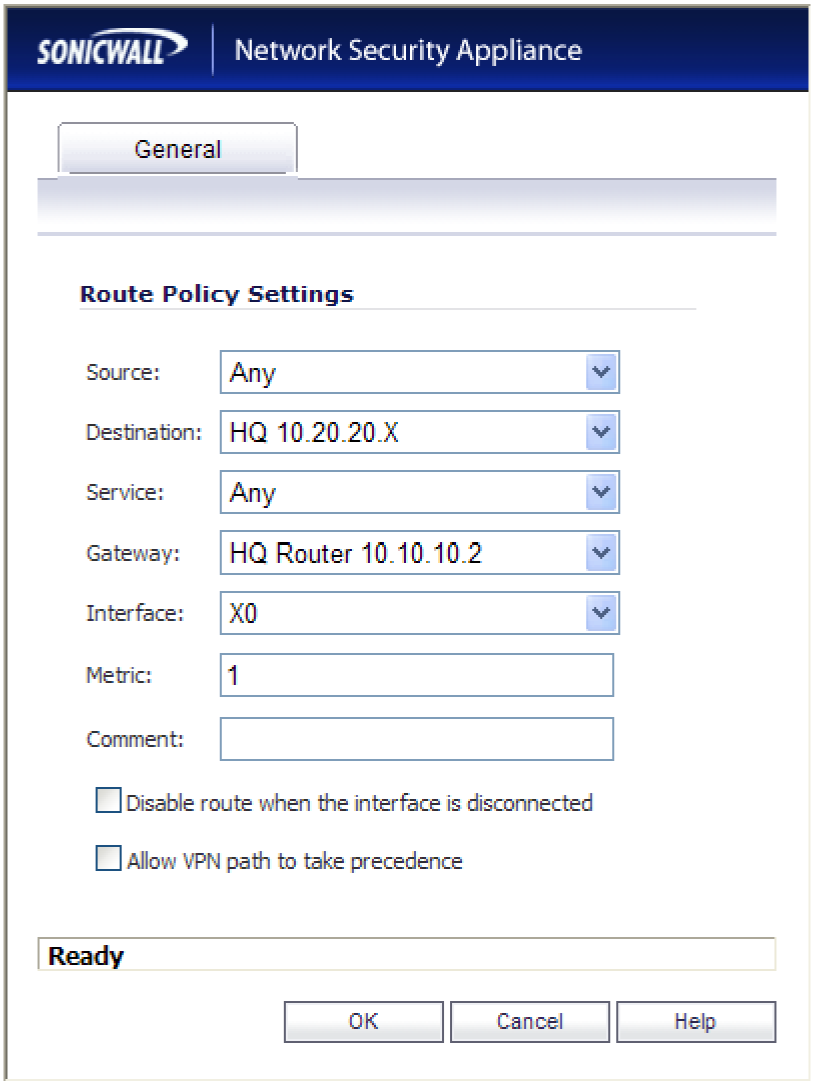
Go to Address Groups

Add Delete Refresh Purge Refresh All Purge All Delete All

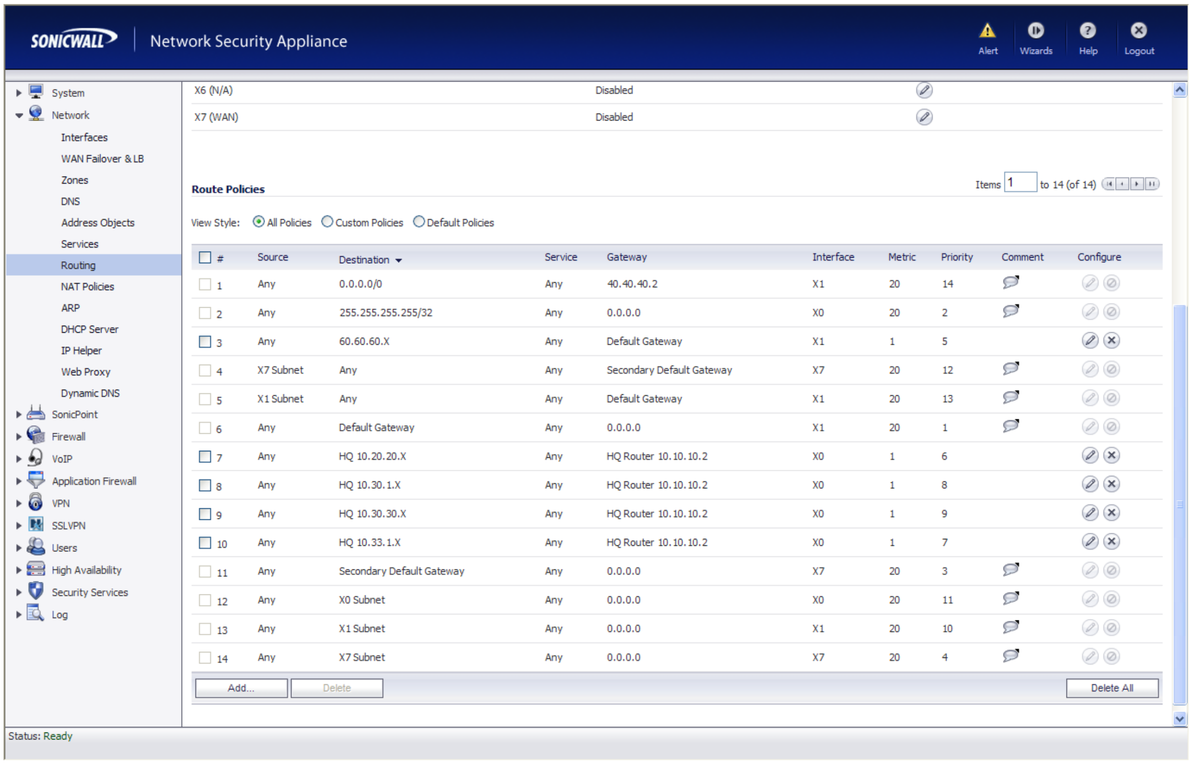
Status: Ready

## 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.<br><br> SONICWALL<br>Network Security Appliance<br>General<br>Ready<br>OK<br>Cancel<br>Help<br>**Route Policy Settings**<br>Source: Any<br>Destination: HQ 10.20.20.X<br>Service: Any<br>Gateway: HQ Router 10.10.10.2<br>Interface: X0<br>Metric: 1<br>Comment:<br>□ Disable route when the interface is disconnected<br>□ Allow VPN path to take precedence |
| **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.



| | | |
|---|---|---|
| X6 (N/A) | Disabled | |
| X7 (WAN) | Disabled | |

**Route Policies**

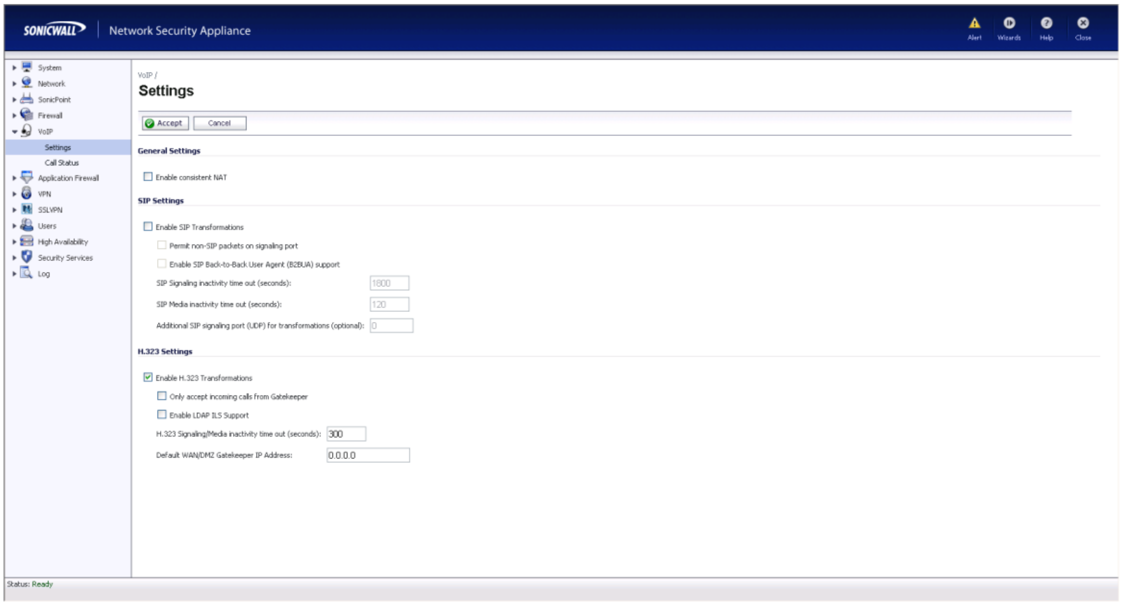
Items 1 to 14 (of 14)

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

| □ # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|---|---|---|---|---|---|---|---|---|---|
| □ 1 | Any | 0.0.0.0/0 | Any | 40.40.40.2 | X1 | 20 | 14 | | |
| □ 2 | Any | 255.255.255.255/32 | Any | 0.0.0.0 | X0 | 20 | 2 | | |
| □ 3 | Any | 60.60.60.X | Any | Default Gateway | X1 | 1 | 5 | | |
| □ 4 | X7 Subnet | Any | Any | Secondary Default Gateway | X7 | 20 | 12 | | |
| □ 5 | X1 Subnet | Any | Any | Default Gateway | X1 | 20 | 13 | | |
| □ 6 | Any | Default Gateway | Any | 0.0.0.0 | X1 | 20 | 1 | | |
| □ 7 | Any | HQ 10.20.20.X | Any | HQ Router 10.10.10.2 | X0 | 1 | 6 | | |
| □ 8 | Any | HQ 10.30.1.X | Any | HQ Router 10.10.10.2 | X0 | 1 | 8 | | |
| □ 9 | Any | HQ 10.30.30.X | Any | HQ Router 10.10.10.2 | X0 | 1 | 9 | | |
| □ 10 | Any | HQ 10.33.1.X | Any | HQ Router 10.10.10.2 | X0 | 1 | 7 | | |
| □ 11 | Any | Secondary Default Gateway | Any | 0.0.0.0 | X7 | 20 | 3 | | |
| □ 12 | Any | X0 Subnet | Any | 0.0.0.0 | X0 | 20 | 11 | | |
| □ 13 | Any | X1 Subnet | Any | 0.0.0.0 | X1 | 20 | 10 | | |
| □ 14 | Any | X7 Subnet | Any | 0.0.0.0 | X7 | 20 | 4 | | |

## 5.6. Configure VoIP settings.

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



VoIP /

Settings

General Settings

□ Enable consistent NAT

SIP Settings

□ Enable SIP Transformations

□ Permit non-SIP packets on signaling port

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

SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 120

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

H.323 Settings

☑ Enable H.323 Transformations

□ Only accept incoming calls from Gatekeeper

□ Enable LDAP ILS Support

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

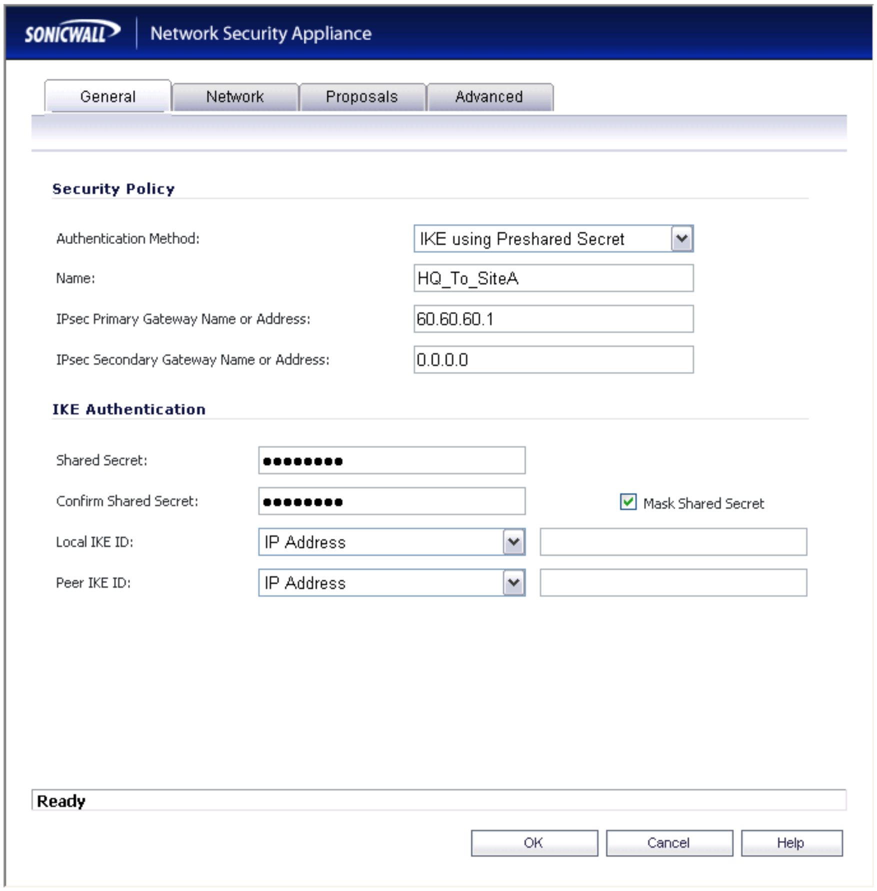
Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

Status: Ready

## 5.7. Create VPN policies

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

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



Security Policy

Authentication Method: IKE using Preshared Secret

Name: HQ_To_SiteA

IPsec Primary Gateway Name or Address: 60.60.60.1

IPsec Secondary Gateway Name or Address: 0.0.0.0

IKE Authentication

Shared Secret: ●●●●●●●●●

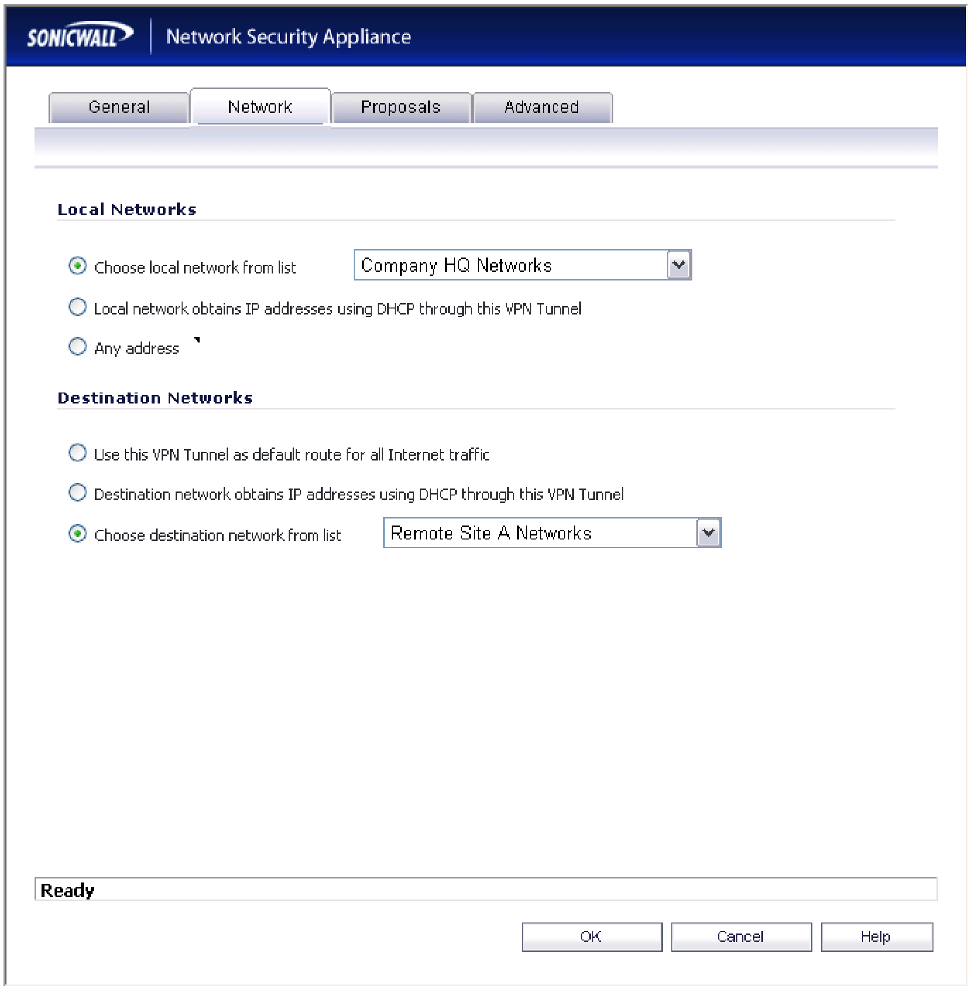
Confirm Shared Secret: ●●●●●●●●●

☑ Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

Ready

| | |
|---|---|
| **5.7.2.** | Specify subnets accessible over the VPN tunnel.<br>Within the **Choose local network from list** pull down, select the Address Object Group (created in Step **5.4.1**) for this site. Within the **Choose remote network from list** scroll list, select the Address Object Group (created in Step **5.4.2**) for the remote site. Click **Advanced** tab to continue.<br> |

**Local Networks**

● Choose local network from list: Company HQ Networks

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

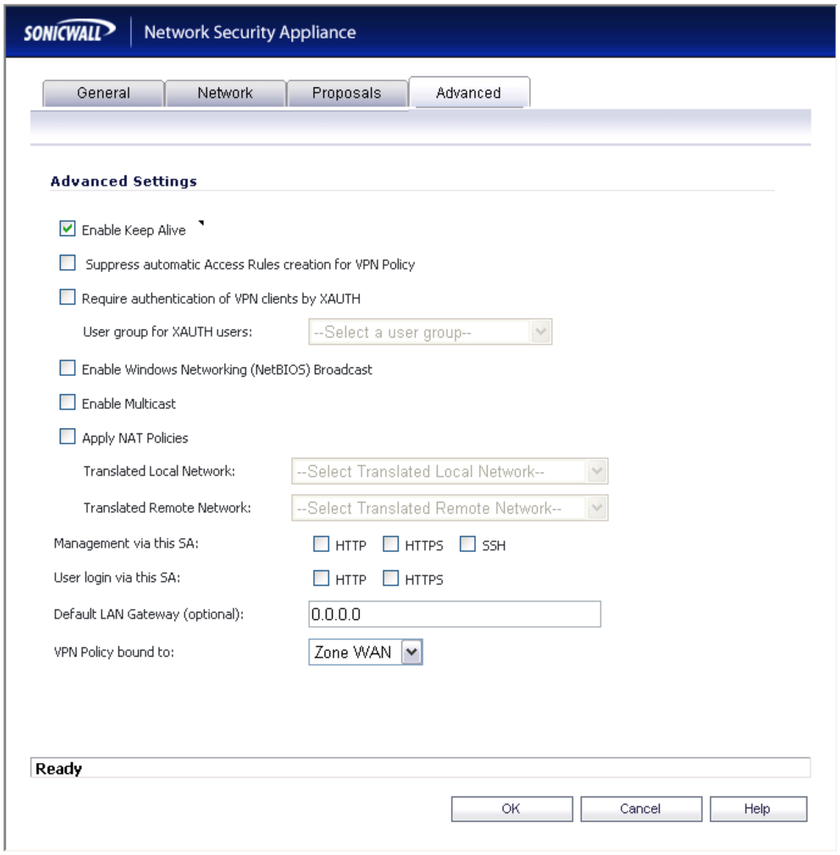
**Destination Networks**

○ Use this VPN Tunnel as default route for all Internet traffic

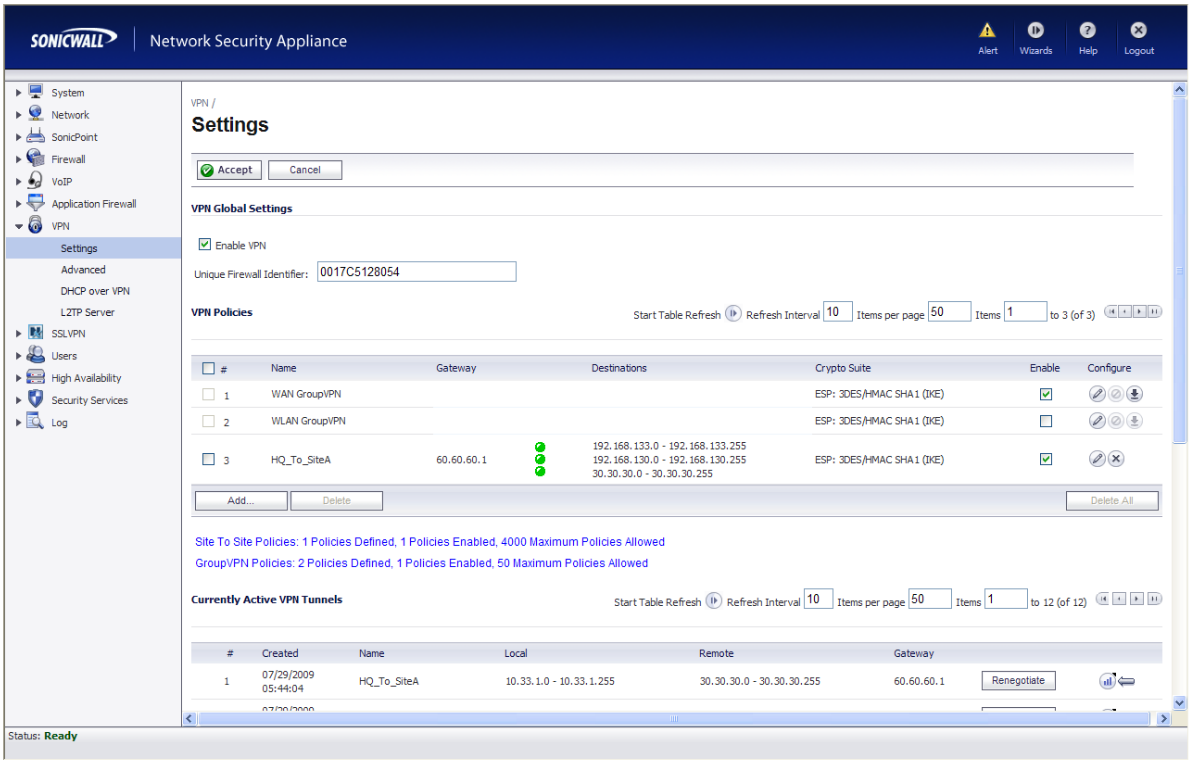
○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list: Remote Site A Networks

Ready

| | |
|---|---|
| **5.7.3.** | Enable Keep Alive for VPN tunnel<br>To avoid VPN tunnel establishment latency, click on the **Enable Keep Alive** checkbox. Click **OK** to continue.<br><br>SONICWALL Network Security Appliance<br>General Network Proposals Advanced<br>**Advanced Settings**<br>☑ Enable Keep Alive<br>□ Suppress automatic Access Rules creation for VPN Policy<br>□ Require authentication of VPN clients by XAUTH<br>User group for XAUTH users: --Select a user group--<br>□ Enable Windows Networking (NetBIOS) Broadcast<br>□ Enable Multicast<br>□ Apply NAT Policies<br>Translated Local Network: --Select Translated Local Network--<br>Translated Remote Network: --Select Translated Remote Network--<br>Management via this SA: □ HTTP □ HTTPS □ SSH<br>User login via this SA: □ HTTP □ HTTPS<br>Default LAN Gateway (optional): 0.0.0.0<br>VPN Policy bound to: Zone WAN<br>**Ready**<br>OK Cancel 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.



VPN /

Settings

**VPN Global Settings**

☑ Enable VPN

Unique Firewall Identifier: 0017C5128054

**VPN Policies**

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 3 (of 3)

| □ # | Name | Gateway | | Destinations | Crypto Suite | Enable | Configure |
|---|---|---|---|---|---|---|---|
| □ 1 | WAN GroupVPN | | | | ESP: 3DES/HMAC SHA1 (IKE) | ☑ | |
| □ 2 | WLAN GroupVPN | | | | ESP: 3DES/HMAC SHA1 (IKE) | □ | |
| □ 3 | HQ_To_SiteA | 60.60.60.1 | ●<br>●<br>● | 192.168.133.0 - 192.168.133.255<br>192.168.130.0 - 192.168.130.255<br>30.30.30.0 - 30.30.30.255 | ESP: 3DES/HMAC SHA1 (IKE) | ☑ | |

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 4000 Maximum Policies Allowed

GroupVPN Policies: 2 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed

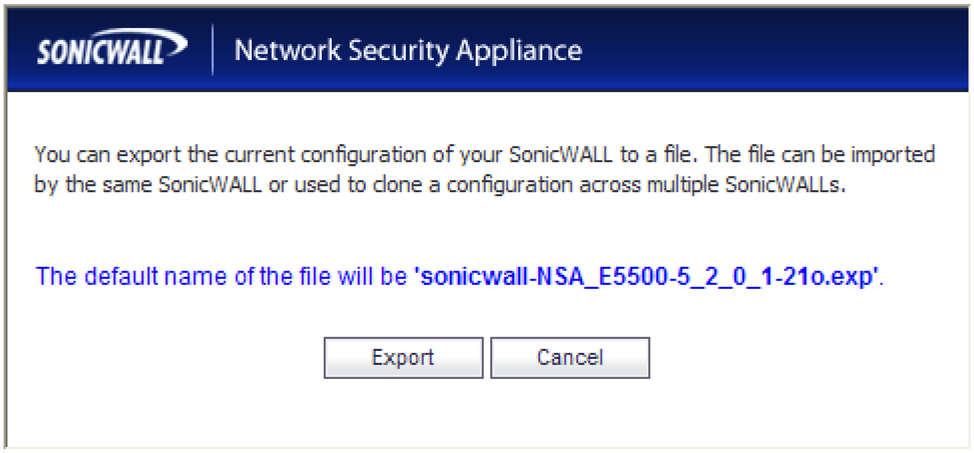
**Currently Active VPN Tunnels**

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 12 (of 12)

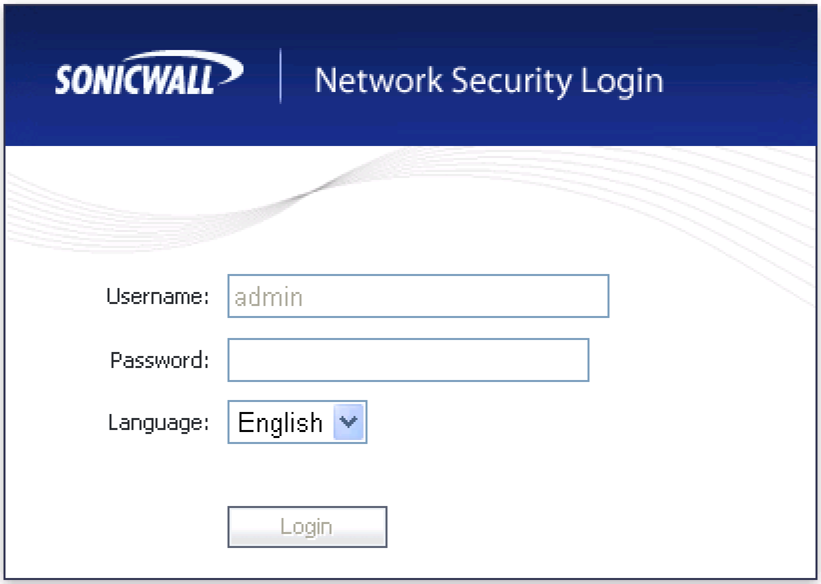
| # | Created | Name | Local | Remote | Gateway | | |
|---|---|---|---|---|---|---|---|
| 1 | 07/29/2009<br>05:44:04 | HQ_To_SiteA | 10.33.1.0 - 10.33.1.255 | 30.30.30.0 - 30.30.30.255 | 60.60.60.1 | Renegotiate | |

Status: Ready

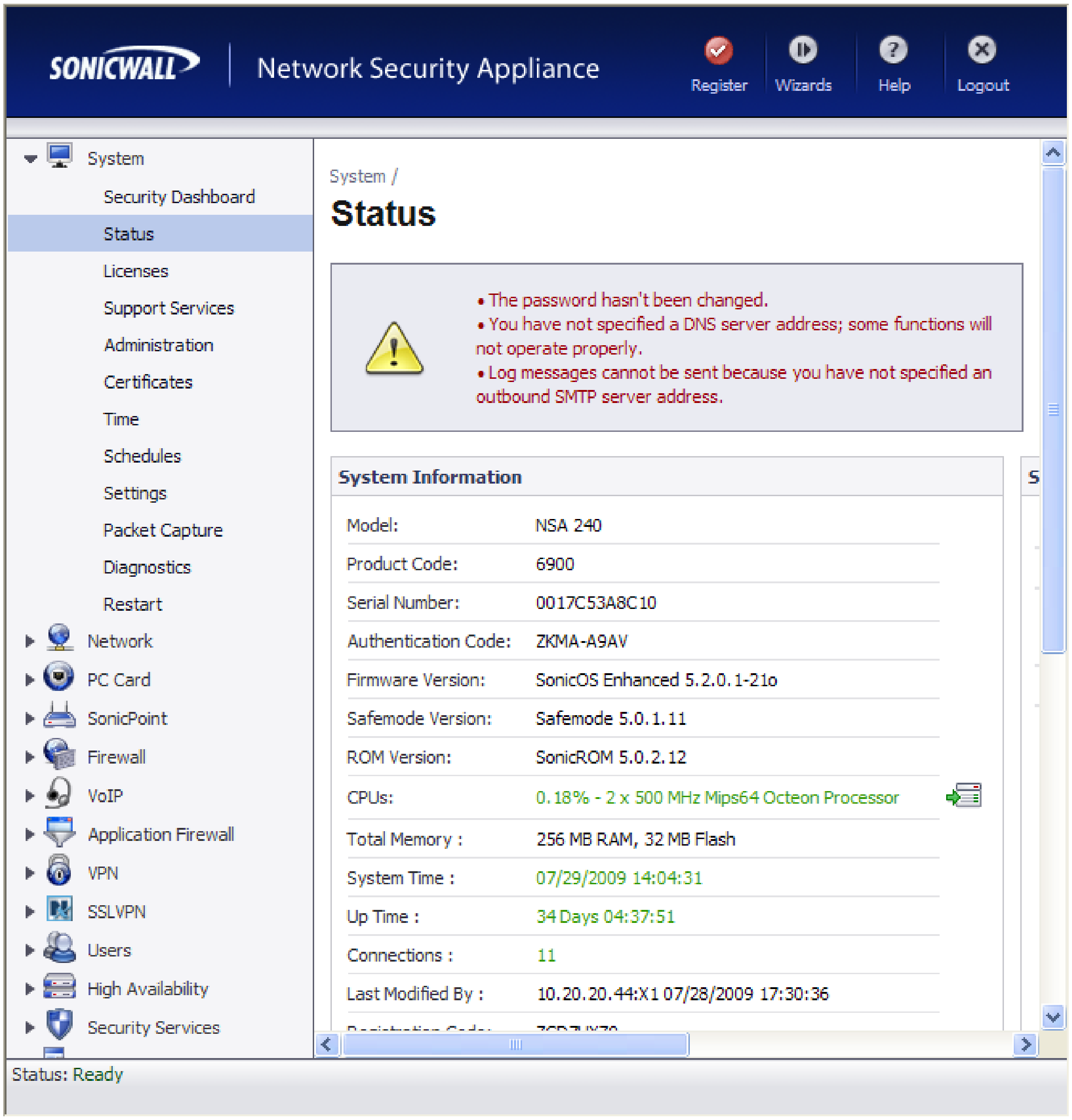
## 5.8. Save settings

| | |
|---|---|
| **5.8.1.** | From the **System** > **Settings**, click on the **Export Settings** button to save the SonicWALL appliance configuration.<br><br>SONICWALL Network Security Appliance<br>You can export the current configuration of your SonicWALL to a file. The file can be imported by the same SonicWALL or used to clone a configuration across multiple SonicWALLs.<br>The default name of the file will be **'sonicwall-NSA_E5500-5_2_0_1-21o.exp'**.<br> |

## 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].**<br>Log into the SonicWall NSA 240.<br>1. Connect the LAN port of the computer being used to the X0 (LAN) port on the SonicWall NSA 240.<br>2. Start the **Management Tool** as follows: Start your web browser and enter **http://192.168.168.168** Press Enter.<br>3. Log in to the SonicWall NSA 240 using default credentials which can be obtained from the SonicWALL documentation.<br><br>Username: admin<br>Password:<br>Language: English<br> |

**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**.



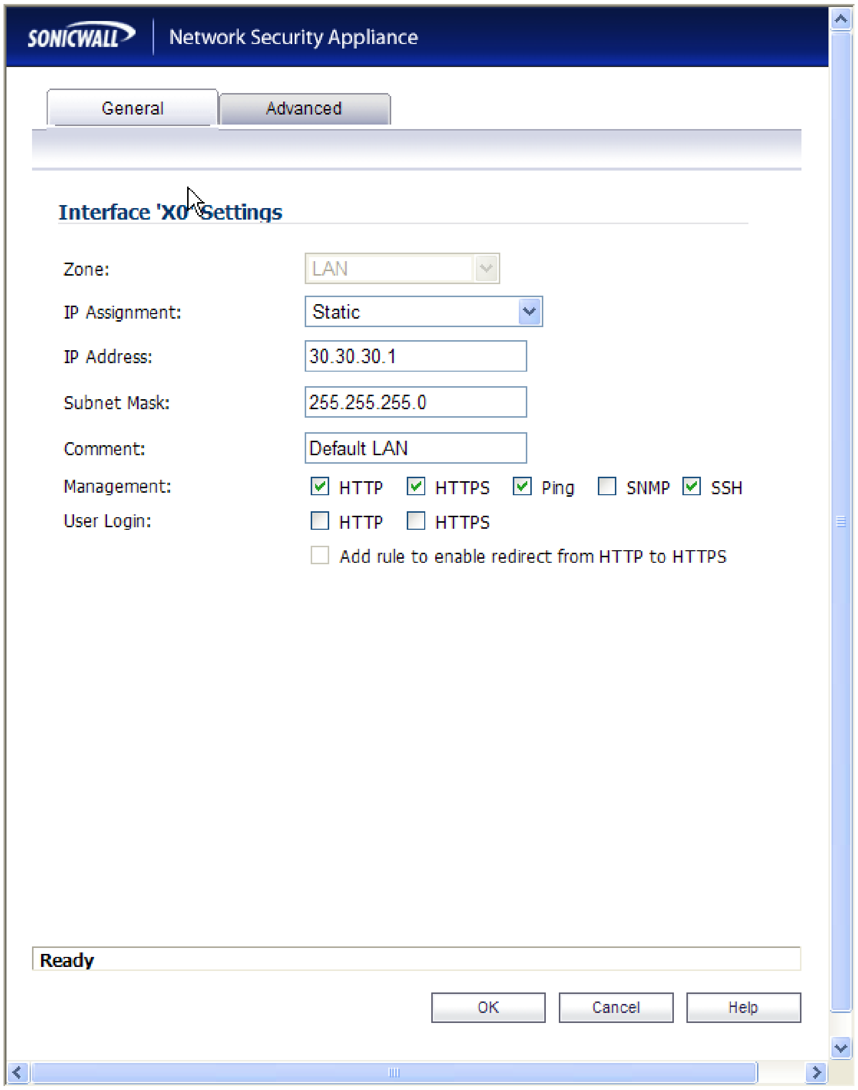
- The password hasn't been changed.
- You have not specified a DNS server address; some functions will not operate properly.
- Log messages cannot be sent because you have not specified an outbound SMTP server address.

**System Information**

| | |
|---|---|
| Model: | 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 |
| CPUs: | 0.18% - 2 x 500 MHz Mips64 Octeon Processor |
| Total Memory : | 256 MB RAM, 32 MB Flash |
| System Time : | 07/29/2009 14:04:31 |
| Up Time : | 34 Days 04:37:51 |
| Connections : | 11 |
| Last Modified By : | 10.20.20.44:X1 07/28/2009 17:30:36 |

## 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.



Interface 'X0' Settings

Zone: LAN

IP Assignment: Static

IP Address: 30.30.30.1

Subnet Mask: 255.255.255.0

Comment: Default LAN

Management: ☑ HTTP ☑ HTTPS ☑ Ping □ SNMP ☑ SSH

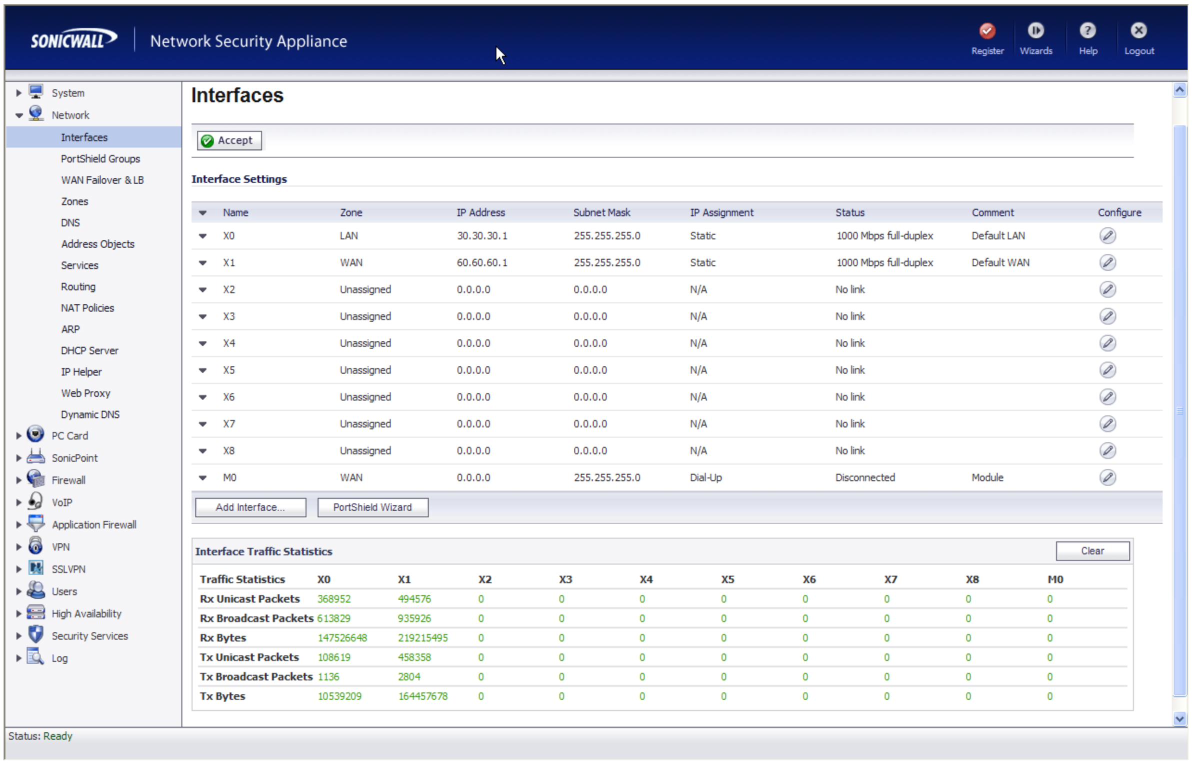
User Login: □ HTTP □ HTTPS

□ Add rule to enable redirect from HTTP to HTTPS

Ready

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

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



Interfaces

Interface Settings

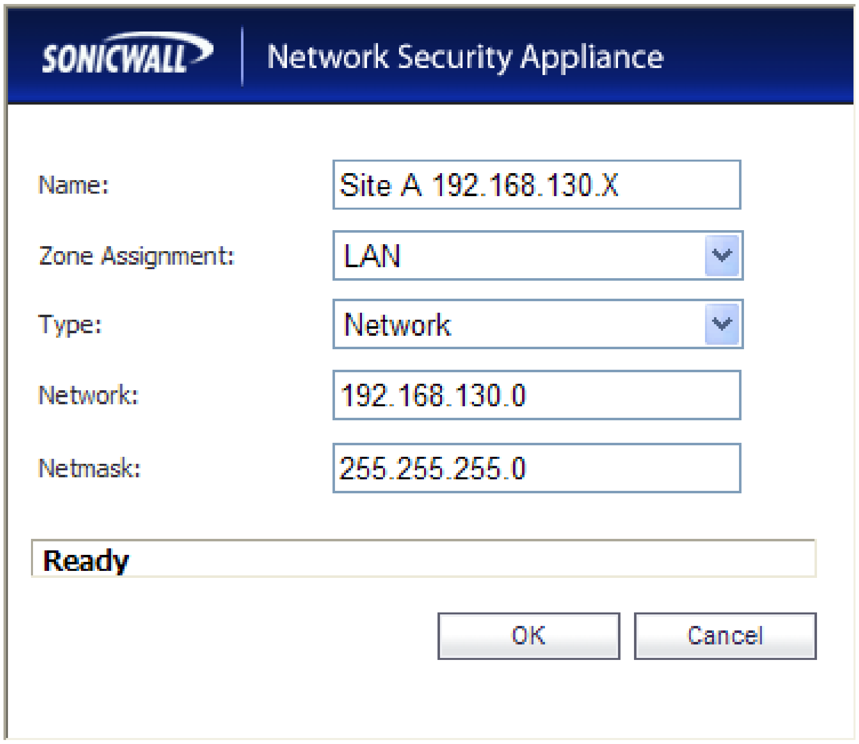
| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|---|---|---|---|---|---|---|---|
| X0 | LAN | 30.30.30.1 | 255.255.255.0 | Static | 1000 Mbps full-duplex | Default LAN | |
| X1 | WAN | 60.60.60.1 | 255.255.255.0 | Static | 1000 Mbps full-duplex | Default WAN | |
| 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 | |

Interface Traffic Statistics

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

## 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.



Name: Site A 192.168.130.X

Zone Assignment: LAN

Type: Network

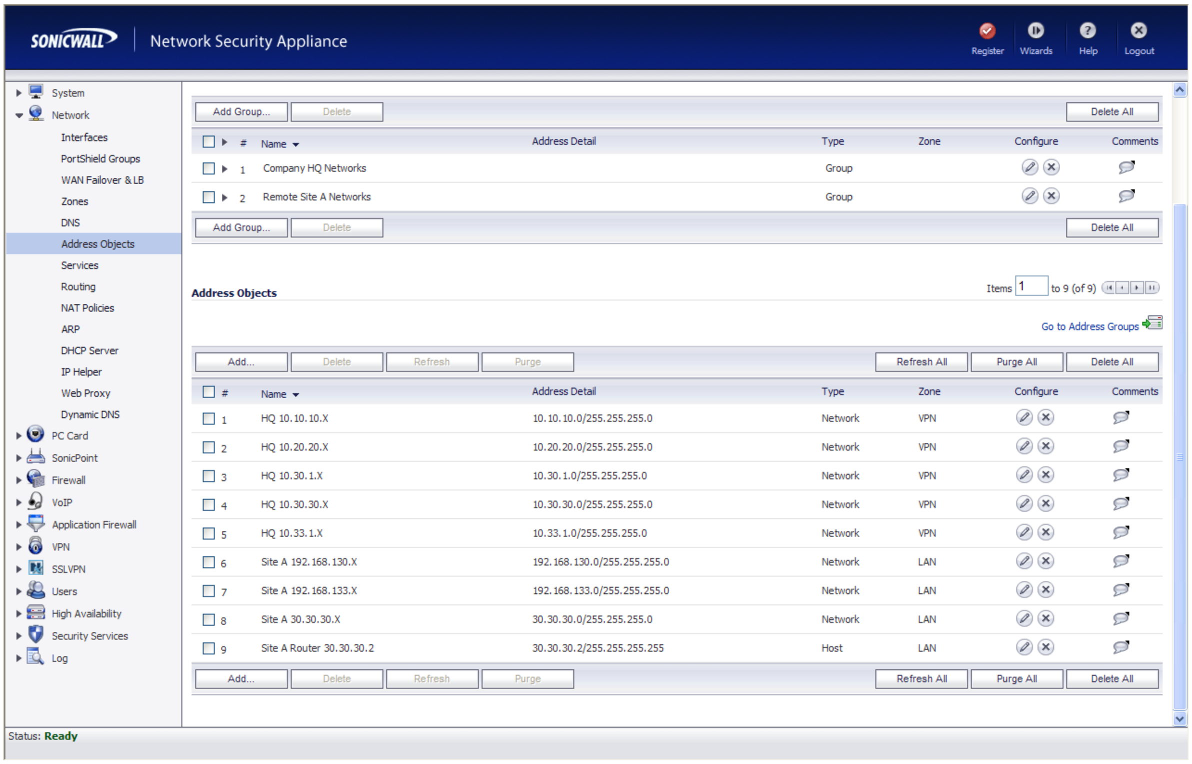
Network: 192.168.130.0

Netmask: 255.255.255.0

Ready

**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.



| □ | # | Name | Address Detail | Type | Zone | Configure | Comments |
|---|---|---|---|---|---|---|---|
| □ | 1 | Company HQ Networks | | Group | | | |
| □ | 2 | Remote Site A Networks | | Group | | | |

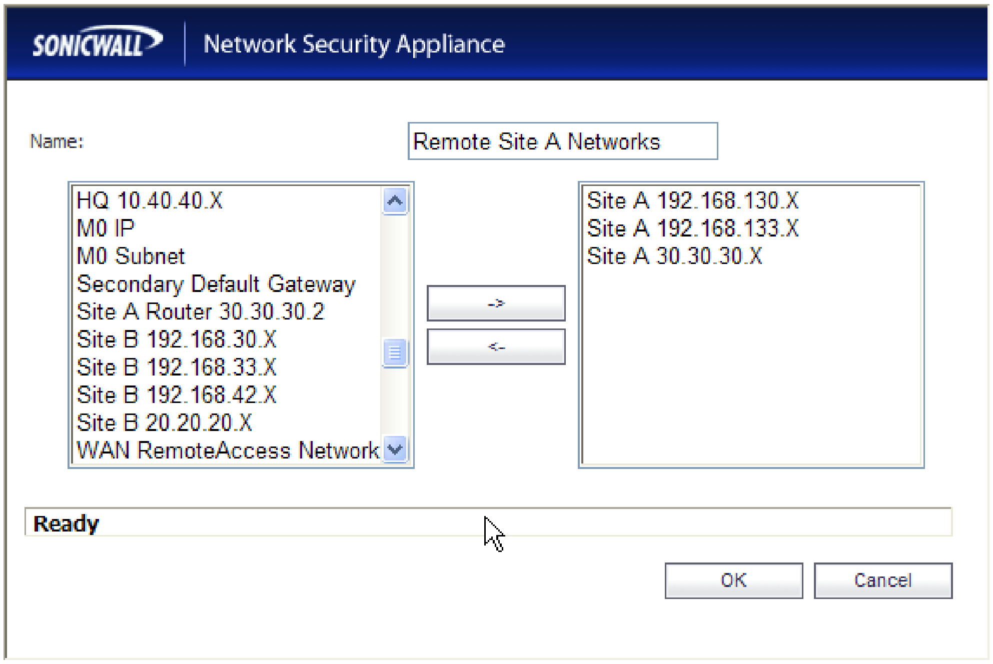
**Address Objects**

Items 1 to 9 (of 9)

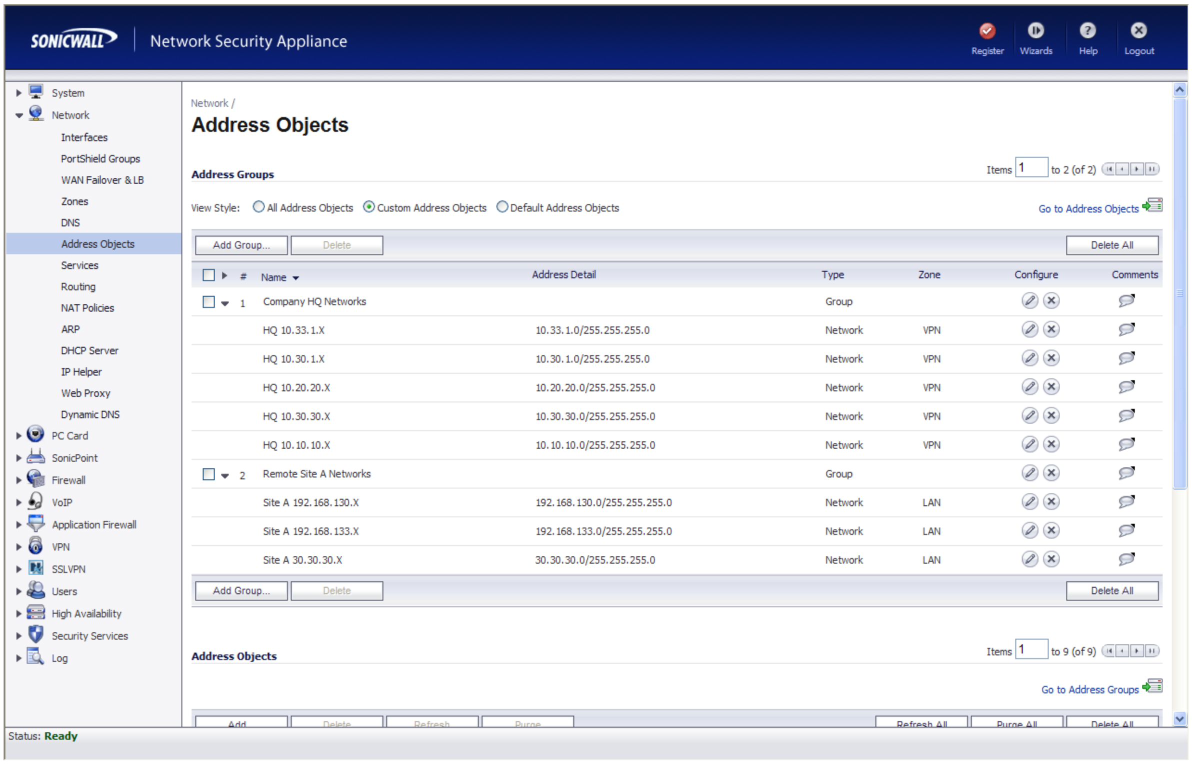
| □ | # | Name | Address Detail | Type | Zone | Configure | Comments |
|---|---|---|---|---|---|---|---|
| □ | 1 | HQ 10.10.10.X | 10.10.10.0/255.255.255.0 | Network | VPN | | |
| □ | 2 | HQ 10.20.20.X | 10.20.20.0/255.255.255.0 | Network | VPN | | |
| □ | 3 | HQ 10.30.1.X | 10.30.1.0/255.255.255.0 | Network | VPN | | |
| □ | 4 | HQ 10.30.30.X | 10.30.30.0/255.255.255.0 | Network | VPN | | |
| □ | 5 | HQ 10.33.1.X | 10.33.1.0/255.255.255.0 | Network | VPN | | |
| □ | 6 | 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 | | |

Status: Ready

## 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.<br><br> SONICWALL<br>Network Security Appliance<br>-><br><-<br>OK<br>Cancel<br>Name: Remote Site A Networks<br>HQ 10.40.40.X<br>M0 IP<br>M0 Subnet<br>Secondary Default Gateway<br>Site A Router 30.30.30.2<br>Site B 192.168.30.X<br>Site B 192.168.33.X<br>Site B 192.168.42.X<br>Site B 20.20.20.X<br>WAN RemoteAccess Network<br>Site A 192.168.130.X<br>Site A 192.168.133.X<br>Site A 30.30.30.X<br>Ready |
| **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.



Network /

Address Objects

Address Groups — Items 1 to 2 (of 2)

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

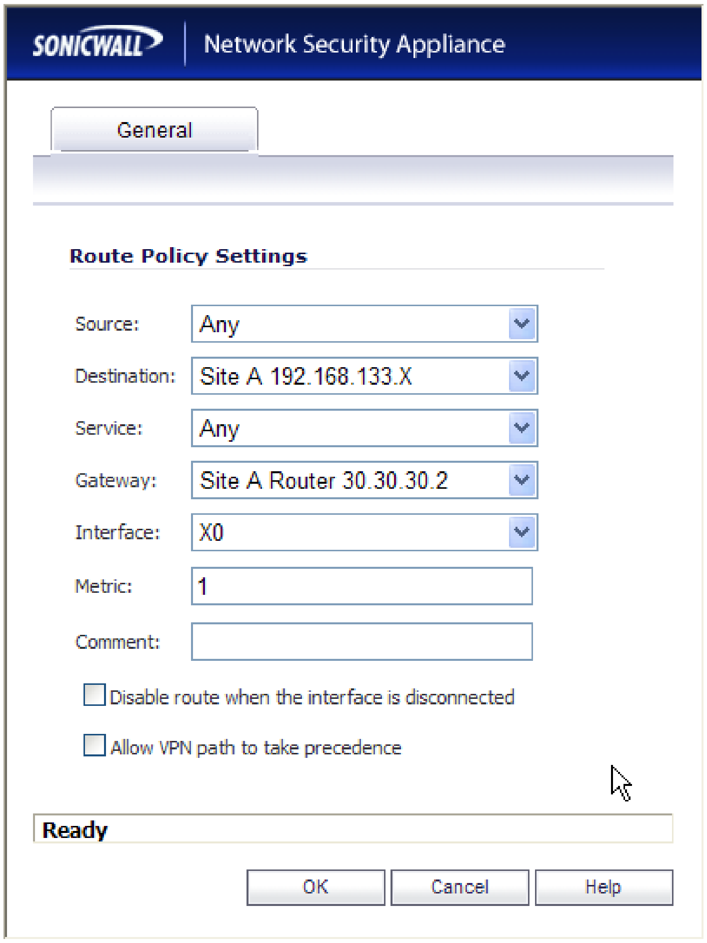
| # | Name | Address Detail | Type | Zone |
|---|---|---|---|---|
| 1 | Company HQ Networks | | Group | |
| | HQ 10.33.1.X | 10.33.1.0/255.255.255.0 | Network | VPN |
| | HQ 10.30.1.X | 10.30.1.0/255.255.255.0 | Network | VPN |
| | HQ 10.20.20.X | 10.20.20.0/255.255.255.0 | Network | VPN |
| | HQ 10.30.30.X | 10.30.30.0/255.255.255.0 | 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 |

Address Objects — Items 1 to 9 (of 9)

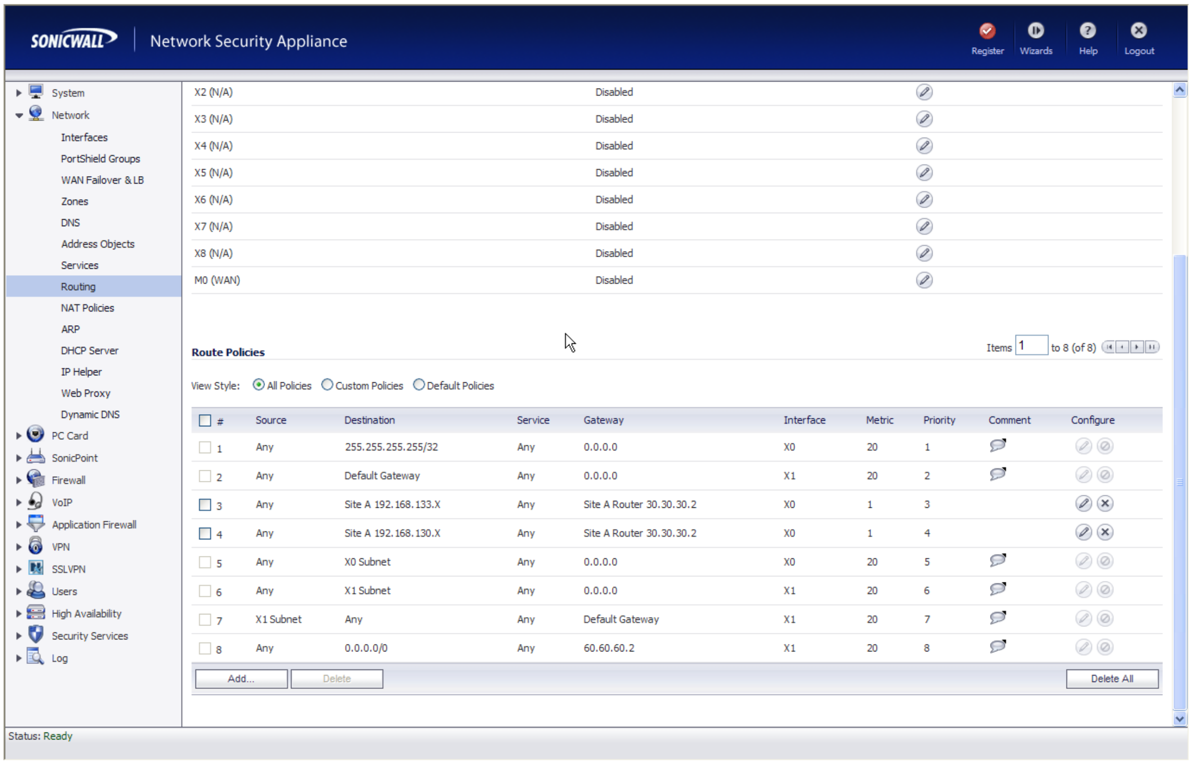
Status: Ready

## 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.<br><br> SONICWALL Network Security Appliance<br>General<br>OK<br>Cancel<br>Help<br>Route Policy Settings<br>Source: Any<br>Destination: Site A 192.168.133.X<br>Service: Any<br>Gateway: Site A Router 30.30.30.2<br>Interface: X0<br>Metric: 1<br>Comment:<br>□ Disable route when the interface is disconnected<br>□ Allow VPN path to take precedence<br>Ready |
| **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.



| | | |
|---|---|---|
| X2 (N/A) | Disabled | ✎ |
| X3 (N/A) | Disabled | ✎ |
| X4 (N/A) | Disabled | ✎ |
| X5 (N/A) | Disabled | ✎ |
| X6 (N/A) | Disabled | ✎ |
| X7 (N/A) | Disabled | ✎ |
| X8 (N/A) | Disabled | ✎ |
| M0 (WAN) | Disabled | ✎ |

**Route Policies**

Items 1 to 8 (of 8)

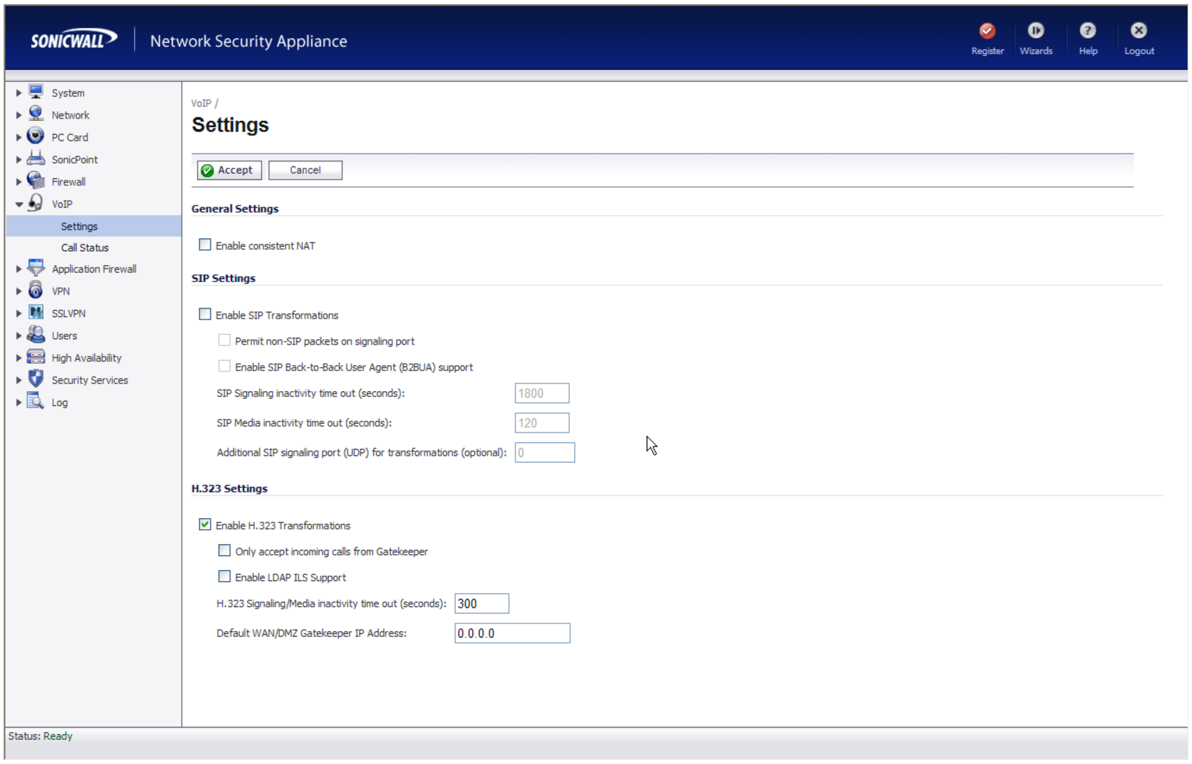
View Style: ● All Policies ○ Custom Policies ○ Default Policies

| □ # | 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 | 💬 | ✎ ⊘ |

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.



Settings

General Settings

□ Enable consistent NAT

SIP Settings

□ Enable SIP Transformations

□ Permit non-SIP packets on signaling port

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

SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 120

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

H.323 Settings

☑ Enable H.323 Transformations

□ Only accept incoming calls from Gatekeeper

□ Enable LDAP ILS Support

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

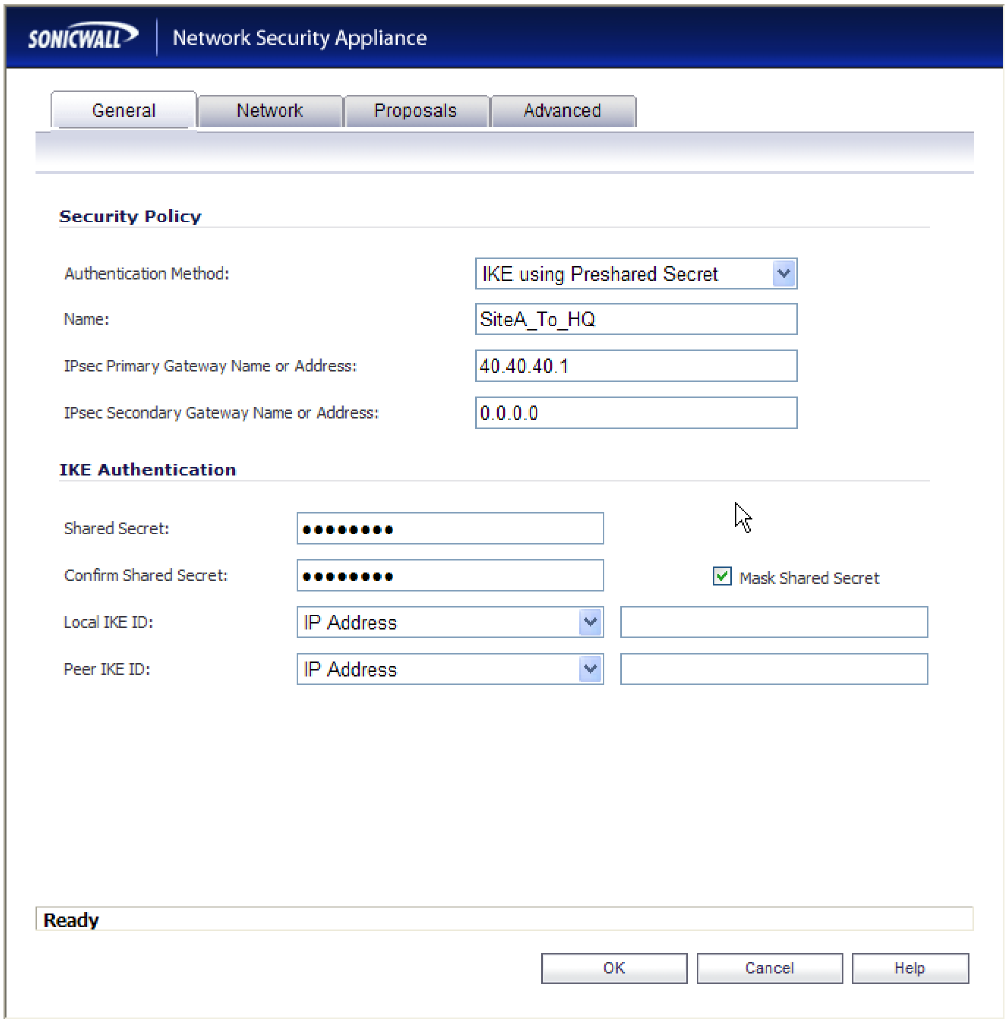
Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

Status: Ready

## 5.15. Create VPN policies

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

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



**Security Policy**

Authentication Method: IKE using Preshared Secret

Name: SiteA_To_HQ

IPsec Primary Gateway Name or Address: 40.40.40.1

IPsec Secondary Gateway Name or Address: 0.0.0.0

**IKE Authentication**

Shared Secret: ••••••••

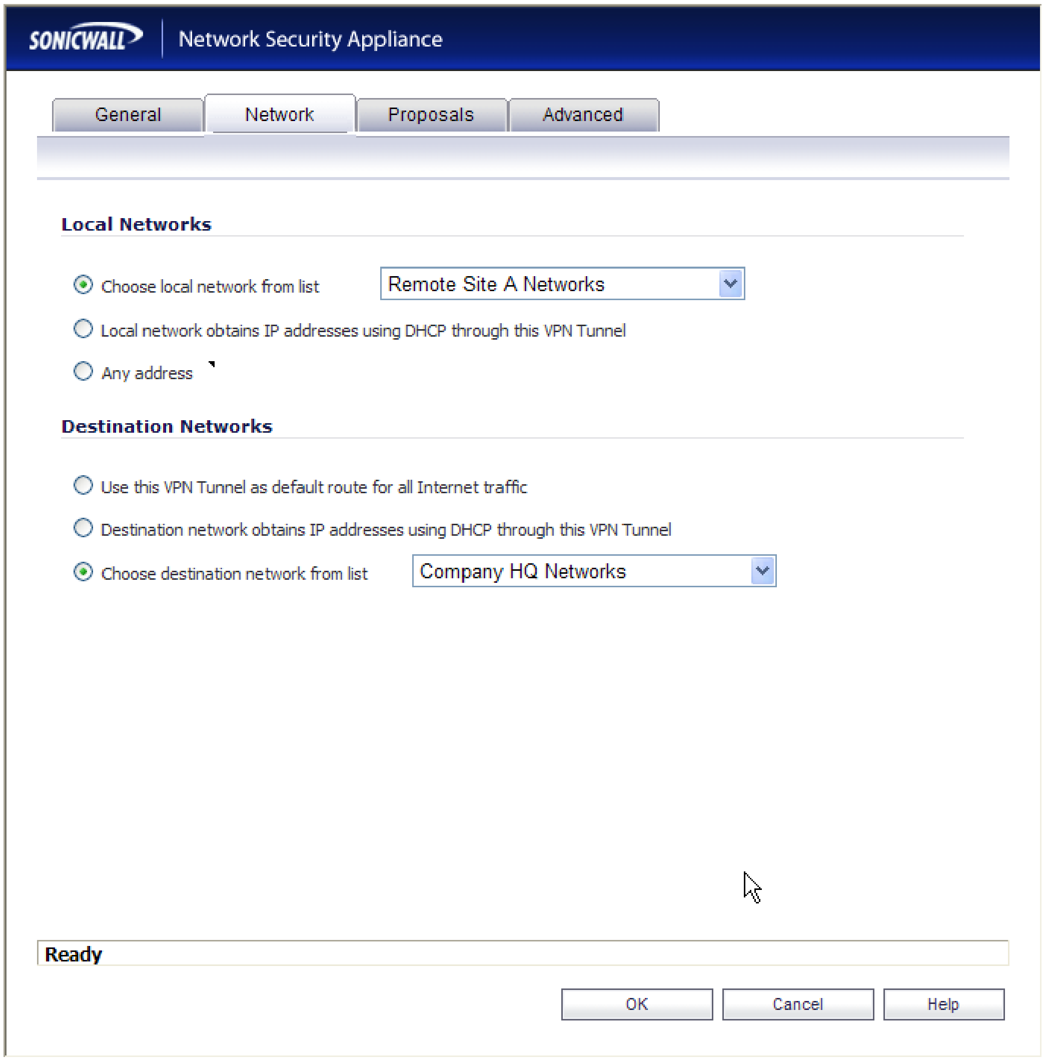
Confirm Shared Secret: ••••••••

☑ Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

**Ready**

| | |
|---|---|
| **5.15.2** | Specify subnets accessible over the VPN tunnel.<br>Within the **Choose local network from list** scroll list, select the Address Object Group (created in Step **5.12.1**) for this site. Within the **Choose remote network from list** scroll list, select the Address Object Group (created in Step **5.12.2**) for the remote site. Click **Advanced** tab to continue.<br> |

**Local Networks**

● Choose local network from list: Remote Site A Networks

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

**Destination Networks**

○ Use this VPN Tunnel as default route for all Internet traffic

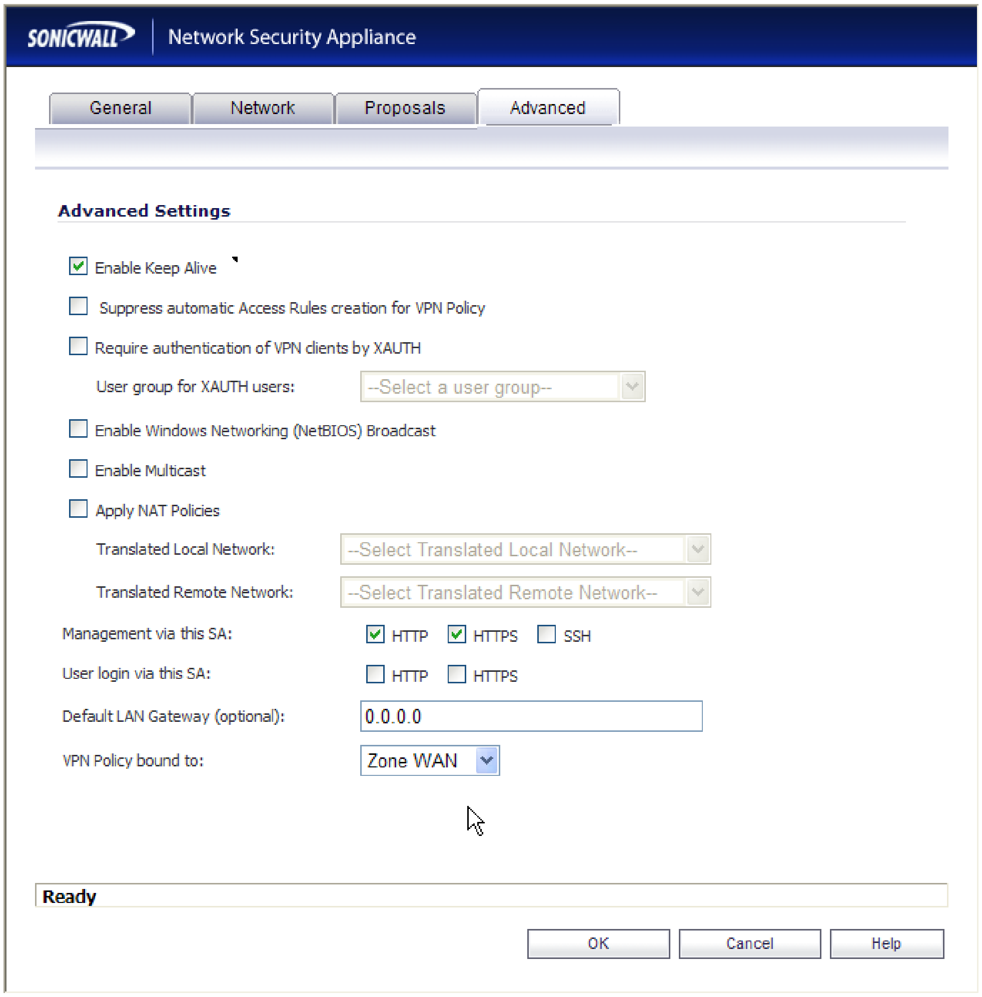
○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list: Company HQ Networks

Ready

**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.



**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

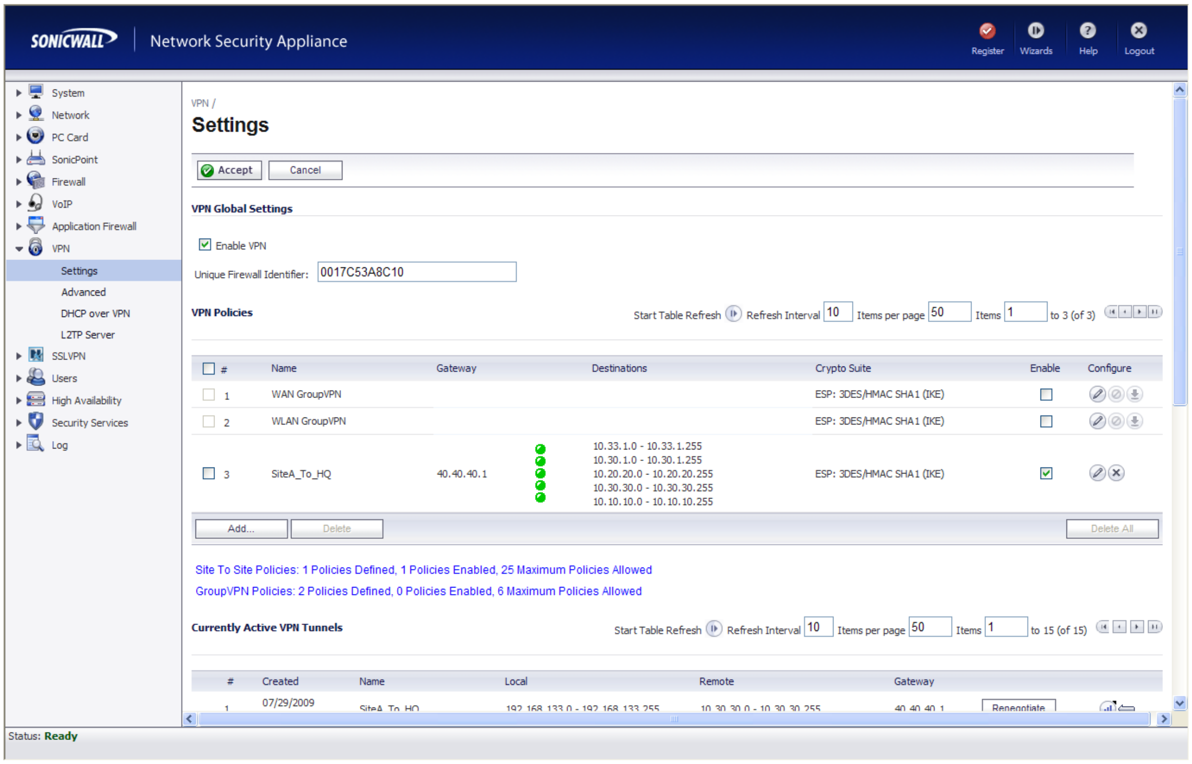
Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: Zone WAN

Ready

**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.



VPN /

Settings

VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0017C53A8C10

VPN Policies

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 3 (of 3)

| □ # | Name | Gateway | | Destinations | Crypto Suite | Enable | Configure |
|---|---|---|---|---|---|---|---|
| □ 1 | WAN GroupVPN | | | | ESP: 3DES/HMAC SHA1 (IKE) | □ | |
| □ 2 | WLAN GroupVPN | | | | ESP: 3DES/HMAC SHA1 (IKE) | □ | |
| □ 3 | SiteA_To_HQ | 40.40.40.1 | ●<br>●<br>●<br>●<br>● | 10.33.1.0 - 10.33.1.255<br>10.30.1.0 - 10.30.1.255<br>10.20.20.0 - 10.20.20.255<br>10.30.30.0 - 10.30.30.255<br>10.10.10.0 - 10.10.10.255 | ESP: 3DES/HMAC SHA1 (IKE) | ☑ | |

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 25 Maximum Policies Allowed

GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 6 Maximum Policies Allowed

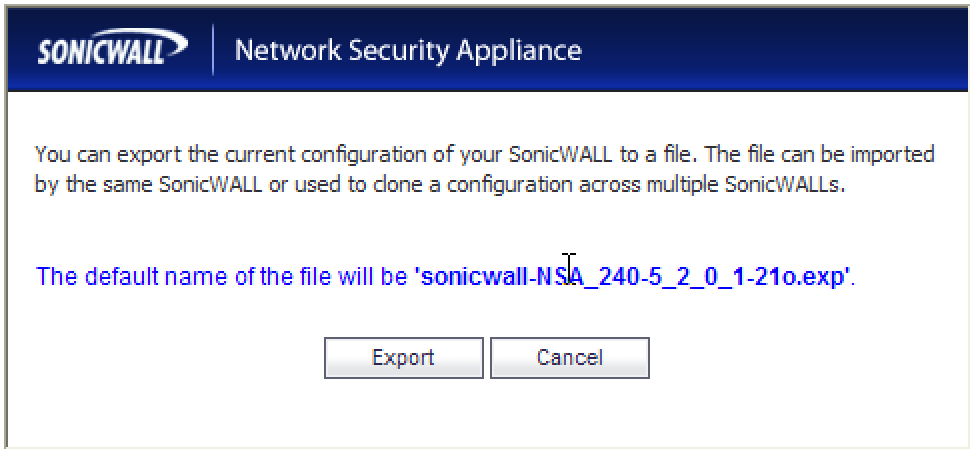
Currently Active VPN Tunnels

Start Table Refresh Refresh Interval 10 Items per page 50 Items 1 to 15 (of 15)

| # | Created | Name | Local | Remote | Gateway | | |
|---|---|---|---|---|---|---|---|
| 1 | 07/29/2009 | SiteA_To_HQ | 192.168.133.0 - 192.168.133.255 | 10.30.30.0 - 10.30.30.255 | 40.40.40.1 | Renegotiate | |

Status: Ready

## 5.16. Save settings

| | |
|---|---|
| **5.16.1** | Save settings<br>From the **System** > **Settings**, click on the **Export** button to save the SonicWALL appliance configuration.<br><br> <br>You can export the current configuration of your SonicWALL to a file. The file can be imported by the same SonicWALL or used to clone a configuration across multiple SonicWALLs.<br>The default name of the file will be 'sonicwall-NSA_240-5_2_0_1-21o.exp'.<br> |

# 6. General Test Approach and Test Results

## 6.1. Test Approach

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

- LAN/WAN connectivity between all locations
- Registration of Avaya IP Telephones with Avaya Aura Communication Manager Branch
- Verifying that DSCP and 802.1p Priority QoS values are not altered by the SonicWALL firewall VPNs.
- Verifying that Avaya 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

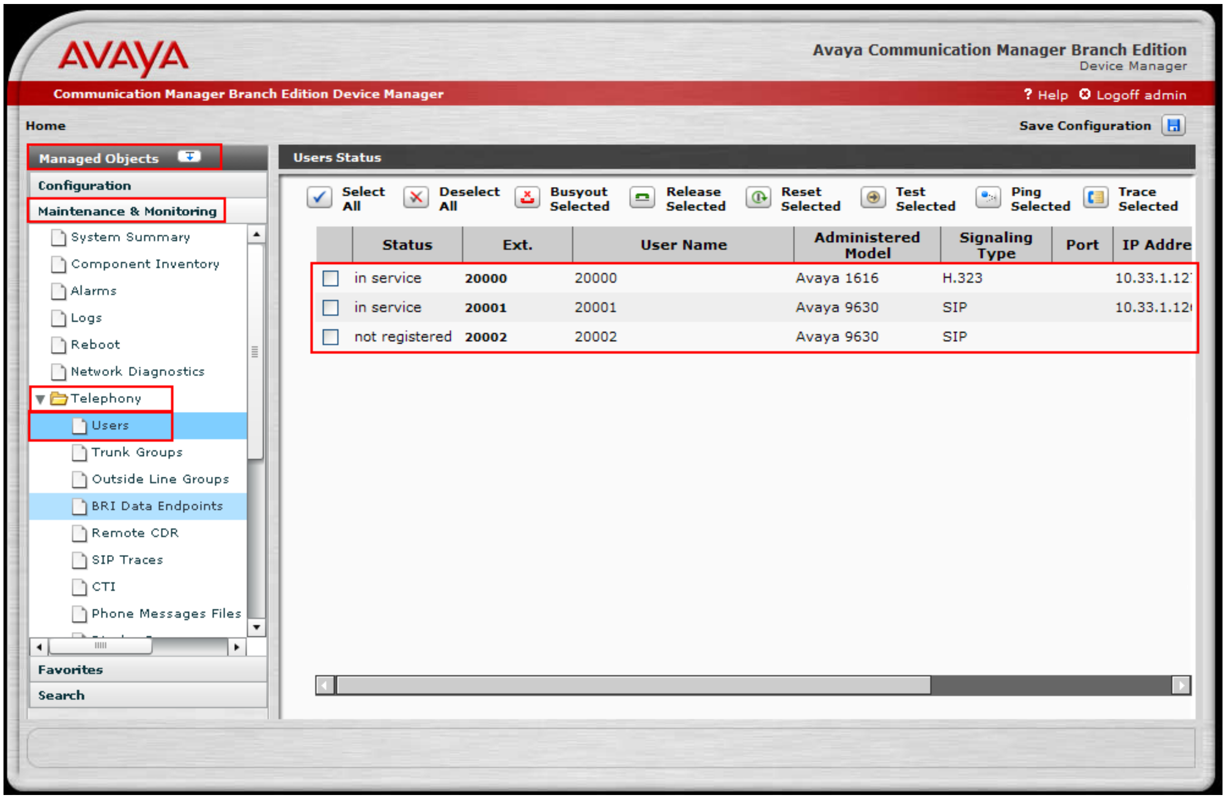
All feature functionality, serviceability, and performance test cases passed. The Multi-Site SonicWALL firewall VPN implementation yielded good voice quality and no calls were lost. The stability of the Avaya/ SonicWALL solution was successfully verified through performance and serviceability testing.

# 7. Verification Steps

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

1. Place internal and external calls between the digital telephone and IP telephones at each site.

2. Check that the Avaya IP telephones have successfully registered with Communication Manager Branch. Log into Communication Manager Branch using the appropriate credentials, under **Managed Objects,** select **Maintenance & Monitoring → Telephony → Users,** look for **in service**.



| | Status | Ext. | User Name | Administered Model | Signaling Type | Port | IP Addre |
|---|---|---|---|---|---|---|---|
| ☐ | in service | **20000** | 20000 | Avaya 1616 | H.323 | | 10.33.1.12 |
| ☐ | in service | **20001** | 20001 | Avaya 9630 | SIP | | 10.33.1.12 |
| ☐ | not registered | **20002** | 20002 | Avaya 9630 | SIP | | |

# 8. Conclusion

These Application Notes describe the configuration steps for integrating the SonicWALL UTM Firewalls with an Avaya telephony infrastructure using Avaya Aura™ Communication Manager Branch. 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] *Avaya Aura™ Communication Manager Branch i120 Installation Quick Start*, May 2009, Document Number 03-602289.

[2] *Avaya Aura™ Communication Manager Branch voice mail Quick Reference Guide.* May 2009, Document Number 03-602108

[3] *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide Release 1*, Document # 16-601443.

[4] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Installation and Maintenance Guide Release 2.0,* Document Number 16-601943.

[5] *4600 Series IP Telephone LAN Administrator Guide*, Document Number: 555-233-507.

The SonicWALL product documentation can be found at

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

# 10. Change History

| Issue | Date | Reason |
|---|---|---|
| 1.0 | 8/20/09 | Initial issue |

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.