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

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:

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software/Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avaya PBX Products</strong></td>
<td></td>
</tr>
<tr>
<td>Avaya S8300 Server running Avaya Aura™</td>
<td>Avaya Aura™ Communication Manager 5.2</td>
</tr>
<tr>
<td>Communication Manager</td>
<td></td>
</tr>
<tr>
<td>Avaya G450 Media Gateway (Corporate Site)</td>
<td>28.22.0</td>
</tr>
<tr>
<td>MGP</td>
<td>HW9</td>
</tr>
<tr>
<td>MM712 DCP Media Module</td>
<td></td>
</tr>
<tr>
<td>Avaya IA 770 INTUITY AUDIX</td>
<td>5.2</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway (Remote Site B)</td>
<td>28.22.0</td>
</tr>
<tr>
<td>MGP</td>
<td>HW9</td>
</tr>
<tr>
<td>MM712 DCP Media Module</td>
<td></td>
</tr>
<tr>
<td>Avaya G700 Media Gateway (Remote Site C)</td>
<td>HW9</td>
</tr>
<tr>
<td>MM712 DCP Media Module</td>
<td></td>
</tr>
<tr>
<td><strong>Avaya SIP Enablement Services (SES)</strong></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura™ SIP Enabled Services (SES) Server</td>
<td>5.2</td>
</tr>
<tr>
<td><strong>Avaya Messaging (Voice Mail) Products</strong></td>
<td></td>
</tr>
<tr>
<td>Avaya Modular Messaging - Messaging Application</td>
<td>5.0</td>
</tr>
<tr>
<td>Server (MAS)</td>
<td></td>
</tr>
<tr>
<td>Avaya Modular Messaging - Message Storage Server</td>
<td>5.0</td>
</tr>
<tr>
<td>(MSS)</td>
<td></td>
</tr>
<tr>
<td>Avaya IA 770 INTUITY AUDIX</td>
<td>5.1</td>
</tr>
<tr>
<td><strong>Avaya Telephony Sets</strong></td>
<td></td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephones</td>
<td>Avaya one-X Deskphone Edition 3.0</td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephones</td>
<td>Avaya one-X Deskphone SIP 2.0.0</td>
</tr>
<tr>
<td>Avaya 2410 Digital Telephone</td>
<td>5.0</td>
</tr>
<tr>
<td><strong>SonicWALL Products</strong></td>
<td></td>
</tr>
<tr>
<td>SonicWall NSA E5500</td>
<td>5.2.0.1-21o</td>
</tr>
<tr>
<td>SonicWall NSA 240</td>
<td>5.2.0.1-21o</td>
</tr>
<tr>
<td><strong>MS Products</strong></td>
<td>File/DHCP Service</td>
</tr>
<tr>
<td>Microsoft Windows 2003 Server</td>
<td></td>
</tr>
</tbody>
</table>
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` 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.

<table>
<thead>
<tr>
<th>change ip-network-region 1</th>
<th>Page 1 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region: 1</td>
<td></td>
</tr>
<tr>
<td>Location:</td>
<td>Authoritative Domain: devcon.com</td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>MEDIA PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Codec Set: 1</td>
<td></td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
<td></td>
</tr>
<tr>
<td>UDP Port Max: 3027</td>
<td></td>
</tr>
<tr>
<td>DIFFSERV/TOS PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Call Control PHB Value: 46</td>
<td></td>
</tr>
<tr>
<td>Audio PHB Value: 46</td>
<td></td>
</tr>
<tr>
<td>Video PHB Value: 26</td>
<td></td>
</tr>
<tr>
<td>802.1P/Q PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Call Control 802.1p Priority: 6</td>
<td></td>
</tr>
<tr>
<td>Audio 802.1p Priority: 6</td>
<td></td>
</tr>
<tr>
<td>Video 802.1p Priority: 5</td>
<td></td>
</tr>
<tr>
<td>H.323 IP ENDPOINTS</td>
<td></td>
</tr>
<tr>
<td>H.323 Link Bounce Recovery? y</td>
<td></td>
</tr>
<tr>
<td>Idle Traffic Interval (sec): 20</td>
<td></td>
</tr>
<tr>
<td>Keep-Alive Interval (sec): 5</td>
<td></td>
</tr>
<tr>
<td>Keep-Alive Count: 5</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RTCP REPORTING ENABLED</th>
<th>RTCP MONITOR SERVER PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Control</td>
<td>Audio</td>
</tr>
<tr>
<td>Report Enabled? y</td>
<td>Use Default Server Parameters? y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AUDIO RESOURCE RESERVATION PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSVP Enabled? n</td>
</tr>
</tbody>
</table>
5. Configure SonicWALL UTM Firewalls

5.1. Configure SonicWall NSA E5500 (Corporate Headquarters)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.
3. Log in to the SonicWall NSA E5500 using default credentials which can be obtained from the SonicWALL documentation.

![Network Security Login](image)
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**.

![SonicWall NSA E5500 window](image)

- 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:** 3MP0-L43H
- **Firmware Version:** SonicOS Enhanced 5.2.0.1-210
- **Safemode Version:** Safemode 5.0.0.14
- **ROM Version:** SonicROM 5.3.0.2
- **CPU:** 0.04% - 6 x 550 MHz MIPS64 Octeon Processor
- **Total Memory:** 1 GB RAM, 512 MB Flash
- **System Time:** 07/28/2009 11:09:38
- **Up Time:** 29 Days 22:29:53
- **Connections:** 13
- **Last Modified By:** 10.10.10.245:X7 07/27/2009 16:06:48
- **Registration Code:** BVNC000
5.2. Configure Interfaces:

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

![Network Security Appliance Interface](image)

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.

![SonicWALL Network Security Appliance](image)

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

The default name of the file will be `sonicwall-NSA_E5500-5_2_0_1-210.exp`.

[Export] [Cancel]
## 5.9. Configure SonicWall NSA 240 (Remote Site A)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |

![SonicWall Network Security Login](image_url)
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.

![Network Security Appliance](image)

**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.
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.

![SonicWALL Network Security Appliance](image)

#### 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.
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.

5.14.1 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.
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.
Once all the VPN policies have been added, the following summary is displayed.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Gateway</th>
<th>Destinations</th>
<th>Crypto Suite</th>
<th>Enable</th>
<th>Configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WLAN80211PN</td>
<td>10.10.1.1</td>
<td>10.23.3.2-10.23.3.233</td>
<td>ESP: 3DES,MAC SHA1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>WLAN80211PN</td>
<td>10.10.1.2</td>
<td>10.23.3.2-10.23.3.233</td>
<td>ESP: 3DES,MAC SHA1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3G/4G_4G</td>
<td>10.10.1.2</td>
<td>10.23.3.2-10.23.3.233</td>
<td>ESP: 3DES,MAC SHA1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3G/4G_4G</td>
<td>10.10.1.2</td>
<td>10.23.3.2-10.23.3.233</td>
<td>ESP: 3DES,MAC SHA1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 5.16. Save settings

<table>
<thead>
<tr>
<th>5.16.1</th>
<th>Save settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the <strong>System &gt; Settings</strong>, click on the <strong>Export Settings</strong> button to save the SonicWALL appliance configuration.</td>
<td></td>
</tr>
</tbody>
</table>

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

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

[Image of SonicWALL export settings]
### 5.17. Configure SonicWall NSA 240 (Remote Site B)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.17.1</strong></td>
<td>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].</td>
</tr>
</tbody>
</table>

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.
3. Log in to the SonicWall NSA 240 using default credentials which can be obtained from the SonicWALL documentation.

![Login Screen](image-url)
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.

![Configuration Tree Screen](image-url)
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.

![Address Object Configuration](image)

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.

<table>
<thead>
<tr>
<th>Address Object Group</th>
<th>Address Detail</th>
<th>Type</th>
<th>Zone</th>
<th>Config</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company HQ Networks</td>
<td>20.33.1.0/24 - 20.34.255.255.255</td>
<td>Group</td>
<td>VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HQ 10.10.1.0/24</td>
<td>20.33.1.0/24 - 20.34.255.255.255</td>
<td>Network</td>
<td>VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HQ 10.20.20.0/24</td>
<td>20.33.1.0/24 - 20.34.255.255.255</td>
<td>Network</td>
<td>VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HQ 192.168.254.0/24</td>
<td>10.33.10.0/24 - 10.34.255.255.255</td>
<td>Network</td>
<td>VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HQ 10.30.10.0/24</td>
<td>20.33.1.0/24 - 20.34.255.255.255</td>
<td>Network</td>
<td>VPN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remote Site A Networks

| Site A (10.10.1.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Group | VPN  |        |          |
| Site A (192.168.10.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Network | VPN  |        |          |
| Site A (192.168.20.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Network | VPN  |        |          |

Remote Site B Networks

| Site B (10.10.1.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Group | VPN  |        |          |
| Site B (192.168.10.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Network | VPN  |        |          |
| Site B (192.168.20.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Network | VPN  |        |          |

| Site C (10.10.1.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Group | VPN  |        |          |
| Site C (192.168.10.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Network | VPN  |        |          |
| Site C (192.168.20.0/24) | 20.33.1.0/24 - 20.34.255.255.255 | Network | VPN  |        |          |
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

<table>
<thead>
<tr>
<th>5.24.1</th>
<th>Save settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From the <strong>System &gt; Settings</strong>, click on the <strong>Export Settings</strong> button to save the SonicWALL appliance configuration.</td>
</tr>
</tbody>
</table>

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

The default name of the file will be 'sonicwall-NSA_240-5_2_0_1-21o.exp'.
### 5.25. Configure SonicWall NSA 240 (Remote Site C)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.25.1</strong></td>
<td>Configure the SonicWall NSA 240 at Remote Site C using the built-in web-based <strong>Management Tool</strong>. Access this tool by establishing a web browser connection to the SonicWall NSA 240. Refer to Section 9 [6].</td>
</tr>
</tbody>
</table>

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.
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**.

![Network Security Appliance](image)

- 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.
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.

![Network Security Appliance](image)

```
Name: Site C 192.168.230.X
Zone Assignment: LAN
Type: Network
Network: 192.168.230.0
Netmask: 255.255.255.0
```

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.
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.

![SONICWALL Network Security Appliance](image)

5.32. Save settings

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

![SONICWALL Network Security Appliance](image)
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](http://support.avaya.com).


10. Change History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>8/19/09</td>
<td>Initial issue</td>
</tr>
</tbody>
</table>