Application Notes for Configuring a Virtual Private Network (VPN) for Avaya IP Office using the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance - Issue 1.0

Abstract

These Application Notes detail the steps for configuring a Virtual Private Network (VPN) between three sites using the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance to support Avaya IP Office.

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

As IP communications continue to evolve and workers become more distributed, providing solutions that deliver security, ensure quality of service (QoS) and allow users to access corporate IP communication services remotely becomes increasingly important. The Edgewater Networks EdgeMarc 4500 VoIP Virtual Private Network (VPN) Appliance provides a secure VPN solution for branch offices and remote users.

The Edgewater Networks EdgeMarc 4500 VPN Appliance provides a secure VPN and QoS solution for branch offices and remote users. Additionally, the EdgeMarc 4500 VoIP VPN Appliance provides Mean Opinion Score (MOS) call quality metrics for each call made offering management and troubleshooting capabilities.

1.1. Network Diagram

The network diagram shown in Figure 1 illustrates the testing environment used for compliance testing. The network contains three sites (headquarters, branch and remote) connected together via a VPN provided by Edgewater Networks EdgeMarc 4500 VoIP VPN Appliances. The network is comprised of two Avaya IP Office systems, four Avaya 5600 Series IP Telephones, two Avaya 2420 Digital Telephones and three Edgewater Networks EdgeMarc 4500 VoIP VPN Appliances. Three power-over Ethernet (PoE) switches are also present in the network. All of the IP telephones within the network are provisioned statically using the keypad present on the telephones. One computer, in the headquarters, runs the Avaya IP Office Manager and Avaya IP Office Voice Mail Pro software applications. The same computer also runs a Syslog server where MOS scores for completed calls are directed.
2. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya IP Office</td>
<td>4.1.9</td>
</tr>
<tr>
<td>Avaya IP Office Manager</td>
<td>6.1.9</td>
</tr>
<tr>
<td>Avaya IP Office Voice Mail Pro</td>
<td>4.1</td>
</tr>
<tr>
<td>Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance</td>
<td>7.9.3</td>
</tr>
<tr>
<td>Avaya 5600 Series IP Telephone</td>
<td>2.3 (H.323)</td>
</tr>
<tr>
<td>Avaya 2420 Digital Telephone</td>
<td>N/A</td>
</tr>
</tbody>
</table>
3. Avaya IP Office Configuration

Avaya IP Office is administered using the Avaya IP Office Manager Windows application. The application can be accessed by navigating to **StartÆProgramsÆIP OfficeÆManager**. Appropriate logon credentials are required to gain access to the application. For information on installation and administration of Avaya IP Office software applications refer to **References [1,2]**. The following steps are for the Avaya IP Office in Site A. The appropriate steps will have to be repeated for the Avaya IP Office in Site B.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the <strong>LAN1</strong> tab by clicking under the Avaya IP Office’s MAC address under <strong>System</strong> within the navigation panel on the left side of the <strong>Avaya IP Office Manager</strong> window. Then click <strong>LAN1</strong>. Enter the information displayed below and then click <strong>OK</strong>. The <strong>OK</strong> button is found on the bottom left Avaya IP Office Manager application. Configure the <strong>IP Address</strong> and <strong>IP Mask</strong> per <strong>Figure 1</strong>. Configure <strong>DHCP Mode</strong> to “Disabled”. When changing tabs on Avaya IP Office Manager, the operator may be asked to save configuration changes. Confirm and save the configuration changes if prompted.</td>
</tr>
</tbody>
</table>

![Avaya IP Office Manager](image)

**Figure 1**: Avaya IP Office Manager interface showing LAN1 configuration.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Navigate to the <strong>Gatekeeper</strong> tab by clicking <strong>Gatekeeper</strong>. Check the <strong>H323 Auto-create User</strong> check box. This feature allows Avaya IP Office to dynamically create <strong>Users</strong> and <strong>Extensions</strong> when a telephone registers. Make note of the <strong>RTP Port Number Range</strong> information. This information will need to be configured on each EdgeMarc 4500 VoIP VPN Appliance in <strong>Section 4, Step 7.</strong></td>
</tr>
</tbody>
</table>

![Gatekeeper Tab](image)

| 3. | Navigate to the **Voicemail** tab by clicking **Voicemail**. Enter the information displayed below and then click **OK**. Use the drop-down list for **Voicemail Type** to select “Voicemail Lite/Pro”. **Voicemail IP Address** is the IP address assigned to the computer running Avaya IP Office Voice Mail Pro, see **Figure 1.** |

![Voicemail Tab](image)
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>By default, Avaya IP Office assigns extensions starting with 200. In the sample configuration, two Avaya IP Office systems are connected via a H.323 trunk using the Voice Networking feature. The Voice Networking feature allows the Avaya IP Office in Site A to communicate with the other Avaya IP Office in Site B. Therefore, it is required that there is a unique extension plan at each site. To accomplish this, use the <strong>Extension Renumber</strong> feature by clicking <strong>Tools</strong> and then clicking <strong>Extension Renumber</strong>. In the sample configuration, the headquarters site was configured for five digit extensions starting with “3” and the Site B was configured for five digit extensions starting with “5”. Enter the information below, appropriate to the site being configured, and then click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
5. Navigate to the **IP Route** tab by clicking **IP Route** within the navigation panel on the left side of Avaya IP Office Manager. Enter the information displayed below and then click **OK**. **IP Address** and **IP Mask** are both “0.0.0.0”, indicating a default route. **Gateway IP Address** is the IP address assigned to the LAN interface on the EdgeMarc 4500 VoIP VPN Appliance within the specific site being configured. Use the drop-down list for **Destination** and select “LAN1”.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Navigate to the <strong>IP Route</strong> tab by clicking <strong>IP Route</strong> within the navigation panel on the left side of Avaya IP Office Manager. Enter the information displayed below and then click <strong>OK</strong>. <strong>IP Address</strong> and <strong>IP Mask</strong> are both “0.0.0.0”, indicating a default route. <strong>Gateway IP Address</strong> is the IP address assigned to the LAN interface on the EdgeMarc 4500 VoIP VPN Appliance within the specific site being configured. Use the drop-down list for <strong>Destination</strong> and select “LAN1”.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>6.</td>
<td>Create a new <strong>IP Line</strong> by right clicking on <strong>Line</strong>, select <strong>New</strong> and then select <strong>IP Line</strong>. Enter the information displayed below and then click <strong>OK</strong>. <strong>Line Number</strong> will be auto-populated with the next available value. <strong>Incoming Group ID</strong> and <strong>Outgoing Group ID</strong> can be any numeric value and were set to “9” in the sample configuration.</td>
</tr>
</tbody>
</table>

![Image of IP Line configuration](image1)

| 7.   | Navigate to the **VoIP Settings** tab by clicking **VoIP Settings**. Enter the information displayed below, click **OK** and then click the save configuration icon. **Gateway IP Address** is the IP address of the Avaya IP Office on the far end of the H.323 trunk. Check the **Voice Networking** check box. |

![Image of VoIP Settings configuration](image2)
4. Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance Configuration

The initial configuration of the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance is performed via a web interface. By default, the EdgeMarc 4500 VoIP VPN Appliance will be assigned an IP address of 192.168.1.1, subnet mask of 255.255.255.0. Operators will need to configure a computer to reside in this IP network in order to access the web interface. The following URL was used to access the web interface of the EdgeMarc 4500 VoIP VPN Appliance, http://192.168.1.1. A login is required to access the web interface, for complete details on how to access the web interface of the EdgeMarc 4500 VoIP VPN Appliance refer to References [3,4].
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The initial login screen displays some basic system information such as software version, hostname, MAC address and other details. Click <strong>license key</strong>.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>2.</td>
<td>The <strong>License</strong> web page indicates the number of licensed calls the system is configured to support. A user with administrative privileges will need to ensure that their system has the appropriate license capacity to support the number of calls expected to traverse the VPN.</td>
</tr>
</tbody>
</table>

![License web page](image-url)

- **Platform Type:** EdgeMarc
- **Licensed Calls:** 8
- **SIP Support:** off
- **MGCP Support:** off
- **SIP Survivability:** off
- **MGCP Survivability:** off
- **H.323 Support:** off
- **LCS Support:** off
- **T1 Support:** on
- **Num T1 Ports:** 1
- **RTP range MOS scoring:** on
3. Navigate to the **DHCP Server** web page by clicking **DHCP Server** within the navigation panel on the left side of the web page. Enter the information displayed below and then click **Submit**. Ensure the **Enable DHCP Server** checkbox is not checked.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Navigate to the <strong>Firewall</strong> web page by clicking <strong>Firewall</strong> within the navigation panel on the left side of the web page. Enter the information displayed below and then click <strong>Submit</strong>. Check the <strong>Enable Firewall for WAN</strong> check box. The remaining check boxes enable the access types from the WAN interface on the EdgeMarc 4500 VoIP VPN Appliance. In the sample configuration, HTTP and SSH were allowed from the WAN interface. For complete information on the security recommendations for the EdgeMarc 4500 VoIP VPN Appliance, refer to <strong>Reference [2]</strong>.</td>
</tr>
</tbody>
</table>

![Firewall Configuration Menu](image)
Step Description

5. Navigate to the Services Configuration web page by clicking System and then clicking Services Configuration within the navigation panel on the left side of the web page. Enter the information displayed below and then click Submit. The EdgeMarc 4500 VoIP VPN Appliance can provide Syslog data, which includes a MOS score for calls completed across the VPN. Check the Enable Remote System Logging and Enable MOS Scoring check boxes. Remote Syslog Hosts was set to “10.30.30.125”, which is the IP address of a Syslog server, see Figure 1. Set Hostname can be any alpha-numeric string that identifies the system. Set Hostname was set to “HQ-4500T4” in the sample configuration.
6. Navigate to the **System Time** web page by clicking **System Time** within the navigation panel on the left side of the web page. Configure the correct date/time and then click **Submit**.

![System Time configuration interface](image)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Navigate to System Time by clicking System Time within the navigation panel on the left side of the web page. Configure the correct date/time and then click Submit.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>7.</td>
<td>Navigate to the VoIP ALG web page by clicking VoIP ALG within the navigation panel on the left side of the web page. Enter the information displayed below and then click Submit. RTP range is set to the same value for RTP Port Number Range fields configured in Section 3, Step 2.</td>
</tr>
</tbody>
</table>

### VoIP ALG

ALG allows the system to recognize and register network devices.

<table>
<thead>
<tr>
<th>Configuration Menu</th>
</tr>
</thead>
</table>
| Network
| DHCP Relay
| DHCP Server
| Firewall
| NAT
| Traffic Shaper
| **VoIP ALG**
| H.323
| MGCP
| SIP
| Survivability
| PRI/Net
| Configuration
| CAS/Net
| Configuration
| PRI/Client
| Configuration
| CAS/Client
| Configuration
| VPN
| System
| Certificate
| Clients List
| Dynamic DNS
| File Download
| File Server
| Network Information
| Network Restart
| Network Test Tools
| **Proxy ARP**
| RADIUS Settings
| Reboot System
| Route
| Services Configuration
| Set Link
| System Information
| System Time
| **T1 Configuration**
| **T1 Diagnostics**
| TACACS Settings |

- **TFTP Server IP address:** 0.0.0.0

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports (e.g. when VRRP is enabled). The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

- **Use ALG Alias IP Addresses:**
  - **Enable Client List lockdown:**
  - **Allow Shared Usernames:**
  - **Use Unique Ports for Shared users:**
  - **Strip G.729 from calls:**
  - **Allow clients on WAN:**

- **Allow non-translated RTP to be MOS scored:**
  - **RTP range:** 49152-65535

### Bandwidth Settings for H.323

The maximum bandwidth to be used. The total bandwidth is counted as RTP payload plus IP header overhead, i.e. the actual link bandwidth set aside for RTP streams. The per-call bandwidth is the RTP payload bandwidth only, i.e. the value used in the client to specify the bandwidth of the call.

| Maximum total bandwidth (kbps): |
| Maximum per-call bandwidth (kbps): |
| Default audio stream bandwidth (kbps): |
| Default video stream bandwidth (kbps): |
| Current payload bandwidth: |
| Estimated current total bandwidth: |

The ALG feature is registered. View license key.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Navigate to the <strong>Traffic Shaper</strong> web page by clicking <strong>Traffic Shaper</strong> within the navigation panel on the left side of the web page. Enter the information displayed below and then click <strong>Submit</strong>. Check the <strong>Enable Traffic Shaping</strong> and <strong>Enable Priority IP Addresses</strong> check boxes. The values for <strong>WAN Downstream Bandwidth</strong> and <strong>WAN Upstream Bandwidth</strong> are applicable to the sample configuration and were set to “768”. These parameters define the link speed on the WAN interface and will need to be modified for the specific installation of the EdgeMarc 4500 VoIP VPN Appliance. Enter the IP address of each Avaya IP Office into the box found under <strong>Enable Priority IP Addresses</strong>.</td>
</tr>
</tbody>
</table>

![Traffic Shaper Configuration](image.png)
### Step Description

9. Navigate to the **Network** web page by clicking **Network** within the navigation panel on the left side of the web page. Enter the information displayed below and then click **Submit**. Ensure that **Static IP Address** is selected for the **WAN Interface Settings**. Configure the **LAN Interface Settings** and **WAN Interface Settings** fields per **Figure 1**. **Network Settings: Default Gateway** is the IP address of the gateway on the WAN interface. Note the values used here are only applicable to the sample configuration.

![Configuration Menu](image)

---

**LAN Interface Settings:**

- **IP Address:** 10.39.30.264
- **Subnet Mask:** 255.255.255.0
- **Enable VLAN support:**

**WAN Interface Settings:**

- **IP Address:** 192.168.30.1
- **Subnet Mask:** 255.255.255.0

**Network Settings:**

- **Default Gateway:** 192.168.30.254
- **Primary DNS Server:**
- **Secondary DNS Server:**
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>Navigate to the <strong>VPN Configuration</strong> web page by clicking <strong>VPN</strong> within the navigation panel on the left side of the web page. Enter the information displayed below and then click <strong>Apply</strong>. Use the drop-down list for <strong>VPN Tunnels</strong> to select “New Tunnel”. <strong>Tunnel Name</strong> can be any descriptive text that identifies the tunnel and “HQ-to-Branch” was used for the tunnel between the headquarters and branch office sites. Check the <strong>Enable Tunnel</strong> check box. <strong>Local VPN Gateway</strong> is the IP address assigned to the <strong>WAN Interface Settings: IP Address</strong> configured in Step 9. <strong>Protected Local Network</strong> is the network of the <strong>LAN Interface Settings</strong> configured in Step 9. <strong>Remote VPN Gateway</strong> is the <strong>WAN Interface Settings: IP Address</strong> of the branch office EdgeMarc 4500 VoIP VPN Appliance. <strong>Protected Remote Network</strong> is the network of the <strong>LAN Interface Settings</strong> configured on the branch office EdgeMarc 4500 VoIP VPN Appliance. <strong>Shared Secret</strong> can be any alpha-numeric string and must match on both tunnels.</td>
</tr>
</tbody>
</table>

![VPN Configuration](image_url)
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>Repeat <strong>Step 10</strong> and create another tunnel to the other site per <strong>Figure 1</strong>, modifying the appropriate parameters.</td>
</tr>
<tr>
<td>12.</td>
<td>Repeat <strong>Steps 1 – 11</strong> for each EdgeMarc 4500 VoIP VPN Appliance in the other locations again modifying the appropriate parameters per <strong>Figure 1</strong>.</td>
</tr>
</tbody>
</table>

### 5. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying the capability of the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance support an Avaya IP Office solution comprised of three sites.

#### 5.1. General Test Approach

The general test approach was to validate proper communication across the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance when using a H.323 trunk between two Avaya IP Office systems. Additional testing verified the proper communication of a remote site, where only IP telephones were present.

#### 5.2. Test Results

The Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance passed all test cases as listed below:

- Supporting an H.323 trunk between two Avaya IP Office systems using the Voice Networking feature
- Supporting a remote site where only IP telephones were present.
- Providing priority for Avaya IP Office and IP telephones when competing data traffic was passing through the VPN.
- Providing Syslog data that contained a MOS score for completed telephones calls through the VPN.
- Allowing proper operation of telephony features such as conference calls, hold/return from hold, DTMF tone interpretation, MWI, voicemail, caller ID, multiple call appearances and supporting calls with direct media between endpoints or with media centralized through one of the Avaya IP Office systems.
6. Verification Steps
The following steps can be used to ascertain the functional status of sample network.

- Verify that the VPN tunnels between each site are established. Use the VPN Configuration web page from Section 4, Step 10 to obtain the status of the VPN tunnels. The graphic below shows the tunnel establishment process, each tunnel should show “Established”.

- Verify that each tunnel has the correct Local/Remote interfaces and networks. See Section 4, Step 10.
- Place calls from site to site and verify two-way audio.
- Verify proper DTMF tone interpretation by successfully logging into voicemail.
- Access the Syslog server log and verify the receipt of Syslog data from the Edgewater Networks EdgeMarc 4500 VoIP VPN Appliance and verify that the data contains a MOS value.

7. Support
Technical support for Edgewater Networks can be obtained through the following:

- **Phone:** 1-408-351-7255
- **Email:** support@edgewaternetworks.com
- **Web:** http://www.edgewaternetworks.com

8. Conclusion
These Application Notes detail the configuration process that builds a VPN between three sites using Edgewater Networks EdgeMarc 4500 VoIP VPN Appliances to support Avaya IP Office. These Application Notes also detail the configuration process that builds an H.323 trunk between two Avaya IP Office systems using the Voice Networking feature.
9. Additional References

The documents references below were used for additional configuration are available at http://support.avaya.com.


