Avaya Port Matrix:

Avaya Aura®
Experience Portal
7.0/7.0.1/7.1

Issue 5
March 16, 2016
ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE INFORMATION PROVIDED HEREIN WILL ELIMINATE SECURITY THREATS TO CUSTOMERS’ SYSTEMS. AVAYA INC., ITS RELATED COMPANIES, DIRECTORS, EMPLOYEES, REPRESENTATIVES, SUPPLIERS OR AGENTS MAY NOT, UNDER ANY CIRCUMSTANCES BE HELD LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THE INFORMATION PROVIDED HEREIN. THIS INCLUDES, BUT IS NOT LIMITED TO, THE LOSS OF DATA OR LOSS OF PROFIT, EVEN IF AVAYA WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF THESE TERMS.

© 2016 Avaya Inc. All Rights Reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.
1. Avaya Aura Experience Portal Components

Data flows and their sockets are owned and directed by an application. Here a server running on RHEL 6.7 has many applications, such as Apache Web server, Tomcat, PostgreSQL, and SNMP Agent. For all applications, sockets are created on the network interfaces on the server. For the purposes of firewall configuration, these sockets are sourced from the server, so the firewall (iptables service) should be running on the same server. Application components in the Avaya Aura Experience Portal are listed as follows.

<table>
<thead>
<tr>
<th>Component</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experience Portal Manager (EPM)</td>
<td>Eth0 (public IP)</td>
<td>A component of Experience Portal. Each Experience Portal system must include exactly one Primary EPM server. Each system may, optionally, include multiple Auxiliary EPM servers. Avaya Aura® Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.</td>
</tr>
<tr>
<td>Media Processing Platform (MPP)</td>
<td>Eth0 (public IP)</td>
<td>A component of Experience Portal. A Media Processing Platform (MPP) server is a server machine running the Avaya Aura Experience Portal MPP software. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.</td>
</tr>
</tbody>
</table>
| Experience Portal Multi-Media Server | Eth0 (public IP) | A component of Experience Portal. The Experience Portal Multi-Media Server is co-resident with the EPM and provides the following services:  
- Email Service: An Experience Portal feature which provides e-mail capabilities.  
- SMS Service: An Experience Portal feature which provides SMS capabilities. |
2. Port Usage Tables

2.1 Port Usage Table Heading Definitions

**Source System**: System name or type that initiates connection requests.

**Source Port**: This is the default layer-4 port number of the connection source. Valid values include: 0 – 65535. A “(C)” next to the port number means that the port number is configurable.

**Destination System**: System name or type that receives connection requests.

**Destination Port**: This is the default layer-4 port number to which the connection request is sent. Valid values include: 0 – 65535. A “(C)” next to the port number means that the port number is configurable.

**Network/Application Protocol**: This is the name associated with the layer-4 protocol and layers-5-7 application.

**Optionally Enabled / Disabled**: This field indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid values include: Yes or No

- “No” means the default port state cannot be changed (e.g. enable or disabled).
- “Yes” means the default port state can be changed and that the port can either be enabled or disabled.

**Default Port State**: A port is either open, closed or filtered.

- Open ports will respond to queries
- Closed ports may or may not respond to queries and are only listed when they can be optionally enabled.
- Filtered ports can be open or closed. Filtered UDP ports will not respond to queries. Filtered TCP will respond to queries, but will not allow connectivity.

**Description**: Connection details. Add a reference to refer to the Notes section after each table for specifics on any of the row data, if necessary.
### 2.2 Port Tables

Below are the tables which document the port usage for this product.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network/Application Protocol</th>
<th>Optional Enabled/Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Client</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>TCP/SSH</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>EPM</td>
<td>Ephemeral</td>
<td>Remote Server</td>
<td>TCP, UDP/RPC</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>MPP</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>UDP/NTP</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>SNMP Monitor</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>UDP/SNMP</td>
<td>Yes</td>
<td>Closed</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>TCP/HTTP, HTTPS</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>App Server</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>TCP/HTTP</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>EPM Web Admin</td>
<td>Ephemeral</td>
<td>SNMP Agent</td>
<td>TCP</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>Reporting tool</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>TCP/PGSQL</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>Apache Server</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>TCP/AJP</td>
<td>No</td>
<td>Open</td>
</tr>
<tr>
<td>Apache Server</td>
<td>Ephemeral</td>
<td>EPM Multi-Media Server</td>
<td>TCP/AJP</td>
<td>Yes</td>
<td>Open</td>
</tr>
</tbody>
</table>

**Table 1. Ports for Experience Portal Manager (EPM) Interface (eth0)**

*This port is used for the Apache Server forward requests to EPM main Tomcat Server. (See Note 1)*

*This port is used for the Apache Server forward requests to EPM Multi-Media Tomcat Server. (See Note 1)*

Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy.
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>System</th>
<th>Port (Configurable Range)</th>
<th>Port (Configurable Range)</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled ?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browser/Master WebLM</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>8080, 8443</td>
<td>TCP/HTTP, HTPS</td>
<td>No</td>
<td>Open</td>
<td>WebLM Licensing Management</td>
<td></td>
</tr>
<tr>
<td>EPM OMS</td>
<td>MPP</td>
<td>9443</td>
<td>TCP/HTTPS</td>
<td>No</td>
<td>Open</td>
<td>Configuration and Status Polling of MPP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPM</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>10000</td>
<td>TCP/Proprietary</td>
<td>No</td>
<td>Open</td>
<td>The Avaya Service Locator service is used to support the logging and alarming Web Services used by the Experience Portal system. It is only configured to run on the EPM. (See Note 1)</td>
<td></td>
</tr>
<tr>
<td>EPM</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>11443</td>
<td>TCP/HTTPS</td>
<td>No</td>
<td>Open</td>
<td>Communication between the Primary EPM and the Auxiliary EPM</td>
<td></td>
</tr>
<tr>
<td>EPM</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>31050, 50200</td>
<td>TCP/Proprietary</td>
<td>No</td>
<td>Open</td>
<td>These two ports are used for inter-process communication between the services running on the EPM. (See Note 1)</td>
<td></td>
</tr>
<tr>
<td>EPM</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>61613, 61616</td>
<td>TCP</td>
<td>No</td>
<td>Open</td>
<td>Message broker; Apache ActiveMQ service implements message broker which supports Java Message Service (JMS) 1.1 API. (See Note 1)</td>
<td></td>
</tr>
<tr>
<td>Web Browser, EPM, MPP</td>
<td>Ephemeral</td>
<td>Co-resident Tomcat Application Server</td>
<td>7009, 7080, 7443</td>
<td>TCP/HTTP, HTTPS</td>
<td>Yes</td>
<td>Closed</td>
<td>Co-resident Tomcat Application Server (See Note 2)</td>
<td></td>
</tr>
</tbody>
</table>

Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy.

March 2016 
Avaya Port Matrix: Avaya Aura® Experience Portal 7.0/7.0.1/7.1

Comments? Infodev@avaya.com
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optional Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMX local clients</td>
<td>Ephemeral</td>
<td>ActiveMQ, EPM, EPM Multi-Media Tomcat Server, Co-Resident Application Server</td>
<td>40000-65535</td>
<td>TCP/RMI</td>
<td>No</td>
</tr>
<tr>
<td>EPM Multi-Media Tomcat Server</td>
<td>Ephemeral</td>
<td>External Email Server</td>
<td>25, 465, 587</td>
<td>TCP/SMTP, TCP/SMTPS(TLS), TCP/SMTP(TLSTLS)</td>
<td>No</td>
</tr>
<tr>
<td>EPM Multi-Media Tomcat Server</td>
<td>Ephemeral</td>
<td>External Email Server</td>
<td>143, 993, 143</td>
<td>TCP/IMAP, TCP/IMAPS(TLS), TCP/IMAP(STLSTLS)</td>
<td>No</td>
</tr>
<tr>
<td>EPM Multi-Media Tomcat Server</td>
<td>Ephemeral</td>
<td>External Email Server</td>
<td>110, 995, 110</td>
<td>TCP/POP3, TCP/POP3S(TLS), TCP/POP3(STLSTLS)</td>
<td>No</td>
</tr>
<tr>
<td>EPM Multi-Media Tomcat Server</td>
<td>Ephemeral</td>
<td>SMS Gateway</td>
<td>2775</td>
<td>TCP/SMPP</td>
<td>No</td>
</tr>
<tr>
<td>EPM Multi-Media Tomcat Server</td>
<td>Ephemeral</td>
<td>SMS Gateway</td>
<td>80, 443</td>
<td>TCP/HTTP, HTTPS</td>
<td>Yes</td>
</tr>
</tbody>
</table>

JMX RMI Connection ports They are allocated dynamically and set to a random port number. It is used to export JMX RMI connection objects for data.

Outbound email connection between EPM Multi-Media Email processor and external email server.

Inbound email connection between EPM Multi-Media Email processor and external email server.

Inbound email connection between EPM Multi-Media Email processor and external email server.

SMP connection between EPM Multi-Media SMS processor and external SMS Gateway.

HTTP, HTTPS connection between EPM Multi-Media SMS processor and external SMS Gateway.
NOTES:
1. Port(s) need not be exposed to outside access.
2. The co-resident application server is an optional component on the EPM.

Table 2. Ports for Experience Portal Media Processing Platform (MPP) Interface (eth0)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Port (Configurable Range)</td>
<td>System</td>
<td>Port (Configurable Range)</td>
<td>TCP/SSH</td>
<td>Yes</td>
</tr>
<tr>
<td>SSH Client</td>
<td>Ephemeral</td>
<td>MPP</td>
<td>22</td>
<td>TCP/SSH</td>
<td>Yes</td>
</tr>
<tr>
<td>MPP</td>
<td>Ephemeral</td>
<td>EPM</td>
<td>123</td>
<td>UDP/NTP</td>
<td>No</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Ephemeral</td>
<td>MPP</td>
<td>80, 443</td>
<td>TCP/HTTP, HTTPS</td>
<td>No</td>
</tr>
<tr>
<td>MPP VXXML/CCXML Browser</td>
<td>Ephemeral</td>
<td>App Server</td>
<td>80, 443</td>
<td>TCP/HTTP, HTTPS</td>
<td>No</td>
</tr>
<tr>
<td>MPP ASR/TTS module</td>
<td>Ephemeral</td>
<td>IBM/Loquendo ASR/TTS Speech Server</td>
<td>554</td>
<td>TCP/MRCP V1, RTSP</td>
<td>No</td>
</tr>
<tr>
<td>MPP ASR/TTS module</td>
<td>Ephemeral</td>
<td>Nuance Speech Server</td>
<td>4900</td>
<td>TCP/MRCP V1, RTSP</td>
<td>No</td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Network / Application Protocol</td>
<td>Optional Enabled / Disabled</td>
<td>Default Port State</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MPP ASR/TTS module</td>
<td>Ephemeral Nuance Speech Server</td>
<td>TCP/TLS MRCP V2</td>
<td>Yes</td>
<td>Closed</td>
<td>Control for ASR and TTS RTP streams</td>
</tr>
<tr>
<td>MPP H.323 Telephony module</td>
<td>Ephemeral Media Gateway</td>
<td>UDP,TCP/H.32 3</td>
<td>No</td>
<td>Open</td>
<td>H.323 Stations login and call control</td>
</tr>
<tr>
<td>MPP SIP Telephony Module</td>
<td>Ephemeral SIP Proxy Server</td>
<td>TCP/SIP</td>
<td>No</td>
<td>Open</td>
<td>SIP Call control</td>
</tr>
<tr>
<td>App Server</td>
<td>Ephemeral MPP</td>
<td>TCP/HTTPS</td>
<td>Yes</td>
<td>Open</td>
<td>“basichttp” events for HTTP IO Processing</td>
</tr>
<tr>
<td>Media Gateway 1024-65535i</td>
<td>MPP Telephony module</td>
<td>UDP/RTP</td>
<td>No</td>
<td>Closed</td>
<td>RTP data for H.323 and SIP calls</td>
</tr>
<tr>
<td>Media Gateway 1024-65535</td>
<td>MPP Telephony module</td>
<td>TCP</td>
<td>No</td>
<td>Closed</td>
<td>Call signaling data for H.323 and SIP calls</td>
</tr>
<tr>
<td>ASR/TTS Server 1024-65535</td>
<td>MPP ASR/TTS module</td>
<td>TCP/MRCP</td>
<td>No</td>
<td>Closed</td>
<td>Speech data to ASR/TTS Server</td>
</tr>
<tr>
<td>Media Gateway 1024-65535</td>
<td>MPP Telephony module</td>
<td>UDP</td>
<td>No</td>
<td>Closed</td>
<td>H.225 RAS signaling for H.323 stations</td>
</tr>
</tbody>
</table>
2.3 Port Table Changes

**Table 3.** Port Changes From Avaya Aura Experience Portal 7.0 to 7.0.1

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System</td>
<td>Protocol</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port (Configurable Range)</td>
<td>Port (Interface)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PORTS ADDED**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**PORTS REMOVED**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Table 3.** Port Changes From Avaya Aura Experience Portal 7.0.1 to 7.1

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System</td>
<td>Protocol</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port (Configurable Range)</td>
<td>Port (Interface)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PORTS ADDED**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**PORTS REMOVED**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Network / Application Protocol</th>
<th>Optionally Enabled / Disabled?</th>
<th>Default Port State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
3. Port Usage Diagram

Avaya Experience Portal Manager (eth0)

- HTTPS-TCP: 443
- TCP/POSGSQL: 5432
- HTTP/HTTPS-TCP: 8080, 8443

Avaya Media Processing Platform (eth0)

- HTTPS-TCP: 9443
- NTP-UDP: 123
- HTTP/HTTPS-TCP: 9444

Backup Server

- HTTPS-TCP: 9443
- HTTP/HTTPS-TCP: 10443

Application Server

- HTTPS-TCP: 9443
- HTTP/HTTPS-TCP: 7080, 7443

Email Server

- SMTP: 25
- POP3/POP3S: 110, 995

SMTP/SMTPS-TCP: 25, 465, 587

SAL Gateway

- SNMP-UDP: 162
- SSH-TCP: 22

PBX/Media Gateway

- H235-UDP/TCP
- Default 2702/2701

ASR/TTS Server

- SIP(S)/H.323
- Default 5060/5061, but configurable via SMGR/Phone

SIP Enabled Server

- RTSP/RTSP-UDP-TCP: 554

NMS

- SNMP-UDP: 161
- SSH-TCP: 22

Network Admin

- SSH-TCP: 22

SMSC Server

- SMPP-UDP: 2775

Default

- 1719/1720

HTTP/HTTPS

- TCP
- UDP

Proprietary

- TCP
- UDP

Comments? Infodev@avaya.com

Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy.
Appendix A: Overview of TCP/IP Ports

What are ports and how are they used?

TCP and UDP use ports (defined at [http://www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers)) to route traffic arriving at a particular IP device to the correct upper layer application. These ports are logical descriptors (numbers) that help devices multiplex and de-multiplex information streams. For example, your PC may have multiple applications simultaneously receiving information: email using destination TCP port 25, a browser using destination TCP port 443 and a ssh session using destination TCP port 22. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streams inside the PC. Each of the mini-streams is directed to the correct high-level application identified by the port numbers. Every IP device has incoming (Ingress) and outgoing (Egress) data streams.

Ports are used in TCP and UDP to name the ends of logical connections which carry data flows. TCP and UDP streams have an IP address and port number for both source and destination IP devices. The pairing of an IP address and a port number is called a socket. Therefore, each data stream is uniquely identified with two sockets. Source and destination sockets must be known by the source before a data stream can be sent to the destination. Some destination ports are “open” to receive data streams and are called “listening” ports. Listening ports actively wait for a source (client) to make contact with the known protocol associated with the port number. HTTPS, as an example, is assigned port number 443. When a destination IP device is contacted by a source device using port 443, the destination uses the HTTPS protocol for that data stream conversation.

Port Types

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic Ports (sometimes called Private Ports). The Well Known and Registered ports are assigned by IANA (Internet Assigned Numbers Authority) and are found here: [http://www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers).

Well Known Ports

Well Known Ports are those numbered from 0 through 1023.
For the purpose of providing services to unknown clients, a service listen port is defined. This port is used by the server process as its listen port. Common services often use listen ports in the well-known port range. A well-known port is normally active meaning that it is “listening” for any traffic destined for a specific application. For example, well known port 23 on a server is actively waiting for a data source to contact the server IP address using this port number to establish a Telnet session. Well known port 25 is waiting for an email session, etc. These ports are tied to a well understood application and range from 0 to 1023.

In UNIX and Linux operating systems, only root may open or close a well-known port. Well Known Ports are also commonly referred to as “privileged ports”.

Registered Ports

Registered Ports are those numbered from 1024 through 49151.
Unlike well-known ports, these ports are not restricted to the root user. Less common services register ports in this range. Avaya uses ports in this range for call control. Some, but not all, ports used by Avaya in this range include: 1719/1720 for H.323, 5060/5061 for SIP, 2944 for H.248 and others. The registered port range is 1024 – 49151. Even though a port is registered with an application name, industry often uses these ports for different applications. Conflicts can occur in an enterprise when a port with one meaning is used by two servers with different meanings.
Dynamic Ports

Dynamic Ports are those numbered from 49152 through 65535. Dynamic ports, sometimes called “private ports”, are available to use for any general purpose. This means there are no meanings associated with these ports (similar to RFC 1918 IP Address Usage). These are the safest ports to use because no application types are linked to these ports. The dynamic port range is 49152 – 65535.

Sockets

A socket is the pairing of an IP address with a port number. An example would be 192.168.5.17:3009, where 3009 is the socket number associated with the IP address. A data flow, or conversation, requires two sockets – one at the source device and one at the destination device. The data flow then has two sockets with a total of four logical elements. Each data flow must be unique. If one of the four elements is unique, the data flow is unique. The following three data flows are uniquely identified by socket number and/or IP address.

Data Flow 1: 172.16.16.14:1234 - 10.1.2.3:2345
    two different port numbers and IP addresses and is a valid and typical socket pair

Data Flow 2: 172.16.16.14.1235 - 10.1.2.3:2345
    same IP addresses and port numbers on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique

Data Flow 3: 172.16.16.14:1234 - 10.1.2.4:2345

If one IP address octet changes, or one port number changes, the data flow is unique.

Understanding Firewall Types and Policy Creation

Firewall Types

There are three basic firewall types:

- Packet Filtering
- Application Level Gateways (Proxy Servers)
- Hybrid (Stateful Inspection)
Packet Filtering is the most basic form of the firewalls. Each packet that arrives or leaves the network has its header fields examined against criterion to either drop the packet or let it through. Routers configured with Access Control Lists (ACL) use packet filtering. An example of packet filtering is preventing any source device on the Engineering subnet to telnet into any device in the Accounting subnet.

Application level gateways (ALG) act as a proxy, preventing a direct connection between the foreign device and the internal destination device. ALGs filter each individual packet rather than blindly copying bytes. ALGs can also send alerts via email, alarms or other methods and keep log files to track significant events.

Hybrid firewalls are dynamic systems, tracking each connection traversing all interfaces of the firewall and making sure they are valid. In addition to looking at headers, the content of the packet, up through the application layer, is examined. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Stateful inspection firewalls close off ports until the connection to the specific port is requested. This is an enhancement to security against port scanning.

Firewall Policies

The goals of firewall policies are to monitor, authorize and log data flows and events. They also restrict access using IP addresses, port numbers and application types and sub-types.

This paper is focused with identifying the port numbers used by Avaya products so effective firewall policies can be created without disrupting business communications or opening unnecessary access into the network.

Knowing that the source column in the following matrices is the socket initiator is key in building some types of firewall policies. Some firewalls can be configured to automatically create a return path through the firewall if the initiating source is allowed through. This option removes the need to enter two firewall rules, one for each stream direction, but can also raise security concerns.

Another feature of some firewalls is to create an umbrella policy that allows access for many independent data flows using a common higher layer attribute. Finally, many firewall policies can be avoided by placing endpoints and the servers that serve those endpoints in the same firewall zone.

---

1 The act of systematically scanning a computer’s ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.
Appendix B: Firewall Policy Recommendation for Avaya Aura Experience Portal AAEP 7.0/7.0.1/7.1 (Linux EPM and Linux MPP)

The “iptables” is a user space application program that allows customers to configure the tables provided by the Linux kernel firewall and the chains and rules it stores.

The following lists the “iptables” rules recommendation for the AAEP 7.0/7.0.1/7.1 to function correctly. You should take the following recommendation into account when configuring your Linux firewall policy in order to match your environment needs but not impacting the AAEP 7.0/7.0.1/7.1 functionality.

If you have the managed applications deployed, e.g. POM, ICR, please refer to the managed applications documentation to adjust the firewall policy.

```
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
*filter

# Default Firewall policy (to begin with)
# - Allow all outbound traffic
# - Drop all inbound and forwarding traffic
#
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

# Drop outbound IGMP packets
#
-A OUTPUT -d 224.0.0.0/255.255.255.0 -p igmp -j DROP
```

Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy.
# Allow inbound ICMP type of traffic:

# 0 - Echo Reply (for ping)
# 8 - Echo Request (for ping)
# 3 - Destination unreachable
# 4 - Source Quench
# 11 - Time exceeded (for traceroute)

-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT

# Allow outbound DNS

-A INPUT -p udp --sport 53 -j ACCEPT
-A INPUT -p tcp --sport 53 -j ACCEPT

# Allow Loopback access

-A INPUT -i lo -j ACCEPT
-A OUTPUT -o lo -j ACCEPT

# Allow Portmap service ports in order to perform EP system backup and restore

Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy.
```bash
-A INPUT -p tcp -m tcp --dport 111 -j ACCEPT
-A INPUT -p udp -m udp --dport 111 -j ACCEPT

# NOTE: Allow rpcbind ports. rpcbind ports are dynamically assigned for RPC services.
# If possible, edit /etc/sysconfig/nfs configuration file to control which ports are required RPC
# Services run on.
# Modify iptables configuration file to allow the rpc.bind and rpc.statd ports
#

# Allow NTP traffic in order to perform clock synchronization
#
-A INPUT -p udp --dport 123 -j ACCEPT

# Allow SNMP Agent traffic for the EPM to act as an SNMP agent so that a third party
# Network management software can retrieve the EP system status.
# Note: this is for EPM only. Not needed if no SNMP agent is configured.
#
# Please refer to the EP SNMP Agent Configuration to make necessary change
#
-A INPUT -p udp -m udp --dport 161 -j ACCEPT
-A INPUT -p udp -m udp --sport 161 -j ACCEPT
```
# Allow SNMP Trap traffic for the EPM to send SNMP traps
# Note: this is for EPM only. Not needed if no SNMP trap is configured.
#
# Please refer to the SNMP Trap Configuration to make necessary protocol / port change
#
-A INPUT -p tcp -m tcp --sport 162 -j ACCEPT
-A INPUT -p udp -m udp --sport 162 -j ACCEPT

# Allow inbound SSH traffic for the EPM to perform managed upgrade to the MPP
# Note: this is for EPM and MPP
#
-A INPUT -p tcp -m multiport --dports 22 -j ACCEPT
-A INPUT -p tcp -m multiport --sports 22 -j ACCEPT

# Allow inbound HTTP/HTTPS traffic for the EPM
# Note: this is for EPM only
#
-A INPUT -p tcp -m multiport --dports 80,443,11443 -j ACCEPT
-A INPUT -p tcp -m multiport --sports 80,443,11443 -j ACCEPT

# Allow inbound HTTP/HTTPS traffic for the WebLM
# Note: this is for EPM only
#
-A INPUT -p tcp -m multiport --dports 8080,8443 -j ACCEPT
-A INPUT -p tcp -m multiport --sports 8080,8443 -j ACCEPT

#
# Allow inbound HTTP/HTTPS traffic for the MPP
# Note: this is for MPP only
#
-A INPUT -p tcp -m multiport --dports 80,443,9443,10443 -j ACCEPT
-A INPUT -p tcp -m multiport --ports 80,443,9443,10443 -j ACCEPT

#
# Allow inbound HTTP/HTTPS traffic for co-resident Tomcat Application Server
# Note: this is for EPM only
#
-A INPUT -p tcp -m multiport --dports 7080,7443 -j ACCEPT
-A INPUT -p tcp -m multiport --ports 7080,7443 -j ACCEPT

#
# Allow for PostgreSQL inbound traffic
# Note: This is for EPM only
#
-A INPUT -p tcp --dport 5432 -j ACCEPT
-A INPUT -p tcp --sport 5432 -j ACCEPT

#
# Allow ActiveMQ, Service Locator traffic. This is for internal communication
# Note: This is for EPM only
#
-A INPUT -p tcp -m multiport --dport 10000,31050,50200,61613,61616 -j ACCEPT

#
# Allow inbound unsecure Email traffic to the EPM
# Note: This is for EPM only. Not needed if no email connection is configured.
#
# Please refer to the Email Connection configuration to make necessary change

Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy.
# 25 is the default SMPT TCP port
# 143 is the default IMAP TCP port
# 110 is the default POP3 TCP port
#
-A INPUT -p tcp -m multiport --sport 25,110,143 -j ACCEPT
#
# Allow inbound secure Email traffic to the EPM
# Note: This is for EPM only. Not needed if no email connection is configured.
#
# Please refer to the Email Connection configuration to make necessary change
# 587 is the default SMTP STARTTLS port
# 143 is the default IMAP STARTTLS port
# 110 is the default POP3 STARTTLS port
-A INPUT -p tcp -m multiport --sport 587,143,110 -j ACCEPT
# 465 is the default SMTP TLS port
# 993 is the default IMAP TLS port
# 995 is the default POP3 TLS port
#
-A INPUT -p tcp -m multiport --sport 465,993,995 -j ACCEPT
#
# Allow inbound unsecure SMS traffic to the EPM
# Note: This is for EPM only. Not needed if no SMS connection is configured.
#
# Please refer to the SMS Connection configuration to make necessary change
# 2775 is the default SMPP port
#
-A INPUT -p tcp --sport 2775 -j ACCEPT
#
# Allow the LDAP server inbound traffic for the EPM to authenticate the LDAP users
# Note: This is for EPM only. Not needed if no LDAP Settings is configured.

Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy.
# Please refer to the LDAP Settings page to make necessary change
# 389 is the default LDAP server port
# 636 is the default secure LDAP server port
#
-A INPUT -p tcp -m multiport --sport 389,636 -j ACCEPT
#
# Allow the EPM to connect to the external reporting database
# Note: This is for EPM only. Not needed if no external reporting database is configured.
#
# The allowed ports could be vary depends on what type of external database is configured.
# Please refer to the Report Database Settings if EPM use external reporting database
#
#
# Allow inbound H.323 Traffic to the MPP
# Note: This is for MPP only. Not needed if no H.323 connection is configured.
#
# Please refer to the H.323 Connection configuration to make necessary change
#
-A INPUT -p tcp -m multiport --dport 1719,1720 -j ACCEPT
-A INPUT -p tcp -m multiport --sport 1719,1720 -j ACCEPT
#
# Allow inbound SIP Traffic to the MPP
# Note: This is for MPP only. Not needed if no SIP connection is configured.
#
# Please refer to the SIP Connection configuration to make necessary change
#
-A INPUT -p tcp -m multiport --dport 5060,5061 -j ACCEPT
-A INPUT -p tcp -m multiport --sport 5060,5061 -j ACCEPT
# Allow for MRCP and RTSP traffic
# Note: This is for MPP only
#
# Please refer to the Speech Server configuration to make necessary change
#
-A INPUT -p tcp --dport 4900 -j ACCEPT
-A INPUT -p tcp --sport 4900 -j ACCEPT
#
# Allow RTP, Call Signaling, RAS data for H323 and SIP
# Note: This is for MPP only
#
# Please refer to the VoIP configuration to make necessary change
#
-A INPUT -p udp --dport 11000:30999 -j ACCEPT
-A INPUT -p tcp --dport 31000:33499 -j ACCEPT
-A INPUT -p tcp --dport 34000:36499 -j ACCEPT
-A INPUT -p udp --dport 37000:39499 -j ACCEPT

COMMIT