Avaya Port Matrix:

Avaya Aura®
Presence Services 8.1.2

Issue 1.0
March 06, 2020

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.

1. Presence Services Components

Data flows and their sockets are owned and directed by an application. Here a server running on RHEL 7.5 has many applications, such as JBoss, PostgreSQL, SIP A/S, ASM, etc. 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 Presence Services are listed as follows.

Component	Interface	Description
Presence Services	Eth0 / Eth1	Avaya Snap-in (i.e. Java Enterprise application) running within Avaya Breeze’s Websphere Application Server

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 1. Ports for Presence Services

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Avaya Equinox	Ephemeral	Presence Services	443	TCP/HTTPS	No	Open	Multimedia Messaging service for clients
Zang	Ephemeral	Presence Services	443	TCP/HTTPS	No	Open	Messaging incoming from Zang.io
Zang	443	Presence Services	Ephemeral	TCP/HTTPS	No	Open	Messaging outgoing to Zang.io
Presence Services	Ephemeral	Session Manager	5062	TCP/SIP	No	Open	SIP connection to SM
Session Manager	Ephemeral	Presence Services	5061	TCP/SIP	No	Open	SIP Connection for SM
Presence Services	Ephemeral	Session Manager	5063	TCP/SIP	Yes	Closed	SIP Connection to SM for Microsoft Federation Relay.
Session Manager	Ephemeral	Presence Services	5063	TLS/SIP	Yes	Closed	OPTIONS ping for SM Entity Link for MS Federation Relay. Port opened when Microsoft Internal Federation is enabled.
Microsoft Front End	Ephemeral	Presence Services	5063	TLS/SIP	Yes	Closed	SIP Connection for Microsoft RTC Federation Relay. Port opened when Microsoft Internal Federation is enabled.
Presence Services	Ephemeral	Microsoft Front End	5061	TLS/SIP	Yes	Closed	SIP Connection to Microsoft Front End
Endpoint	Ephemeral	Presence Services	5222 (C)	TCP/XMPP	No	Open	XMPP Client connection to PS

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
XMPP Server	Ephemeral	Presence Services	5269 (C)	TCP/XMPP	No	Open	XMPP Federated Server-to-Server incoming connection
Presence Services	Ephemeral	XMPP Server	5269 (C)	TCP/XMPP	No	Open	XMPP Federated Server-to-Server outgoing connection
Local Presence Services SDK	Ephemeral	Presence Services	7000	TCP/RMI	No	Open	Gigaspaces Lookup Service bound to management IP
Local Presence Services SDK	Ephemeral	Presence Services	7001-7199	TCP/RMI	No	Open	Gigaspaces communication bound to management IP
Presence Services	Ephemeral	IBM Domino Server	80	TCP	No	Open	Domino Collector
Presence Services	Ephemeral	Microsoft Exchange Server	443	TCP/HTTPS	No	Open	Exchange Collector
Presence Services	Ephemeral	AES	450	TCP	Yes	Open	AES Collector JTAPI connection to AES
Presence Services	Ephemeral	AES	1050-1065, 1066-1081	TCP/TLS	Yes	Closed	AES Collector outbound connections to AES
Presence Services	Ephemeral	Websphere	2809	TCP/JMX	No	Open	Operational metrics collection bound to management IP
Presence Services	Ephemeral	Presence Services	7000	TCP/RMI	No	Open	Gigaspaces Lookup Service bound to management IP
Presence Services	Ephemeral	Presence Services	7001-7199	TCP/RMI	No	Open	Gigaspaces communication bound to management IP
Presence Services	Ephemeral	Presence Services	18443	TCP/HTTPS	No	Open	Cluster-to-cluster REST services
Presence Services	Ephemeral	Presence Services	18444	TCP/HTTPS	No	Open	Cluster-to-cluster Websocket communications
Amazon Web Services (AWS)	Ephemeral	Presence Services	18445	TCP/HTTPS	No	Open	AWS Application Load balancer health check

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Presence Services	Ephemeral	Push-Notification Provider Proxy	443	TCP/HTTPS	Yes	Open	The proxy port of the Push Notification provider (configurable). E.g. Avaya Push Notification Provider (APNP) accepts incoming connections on port 443
Presence Services	Ephemeral	LDAP Server	Depends on Enterprise	TCP/LDAPS	Yes	Open	LDAP port for the Enterprise, depending on their configuration (e.g. 389 is default unsecure, 636 secure, 3268 unsecure global catalog, 3269 secure global catalog, etc.)
Presence Services	Ephemeral	Globalrelay.com	25 or 587	TCP/SMTP	Yes	Open	SMTP connect port to GlobalRelay.com for external archiving. 587 is secure (STARTTLS). Port usage is negotiated by Avaya customer and Global Relay

2.3 Port Table Changes

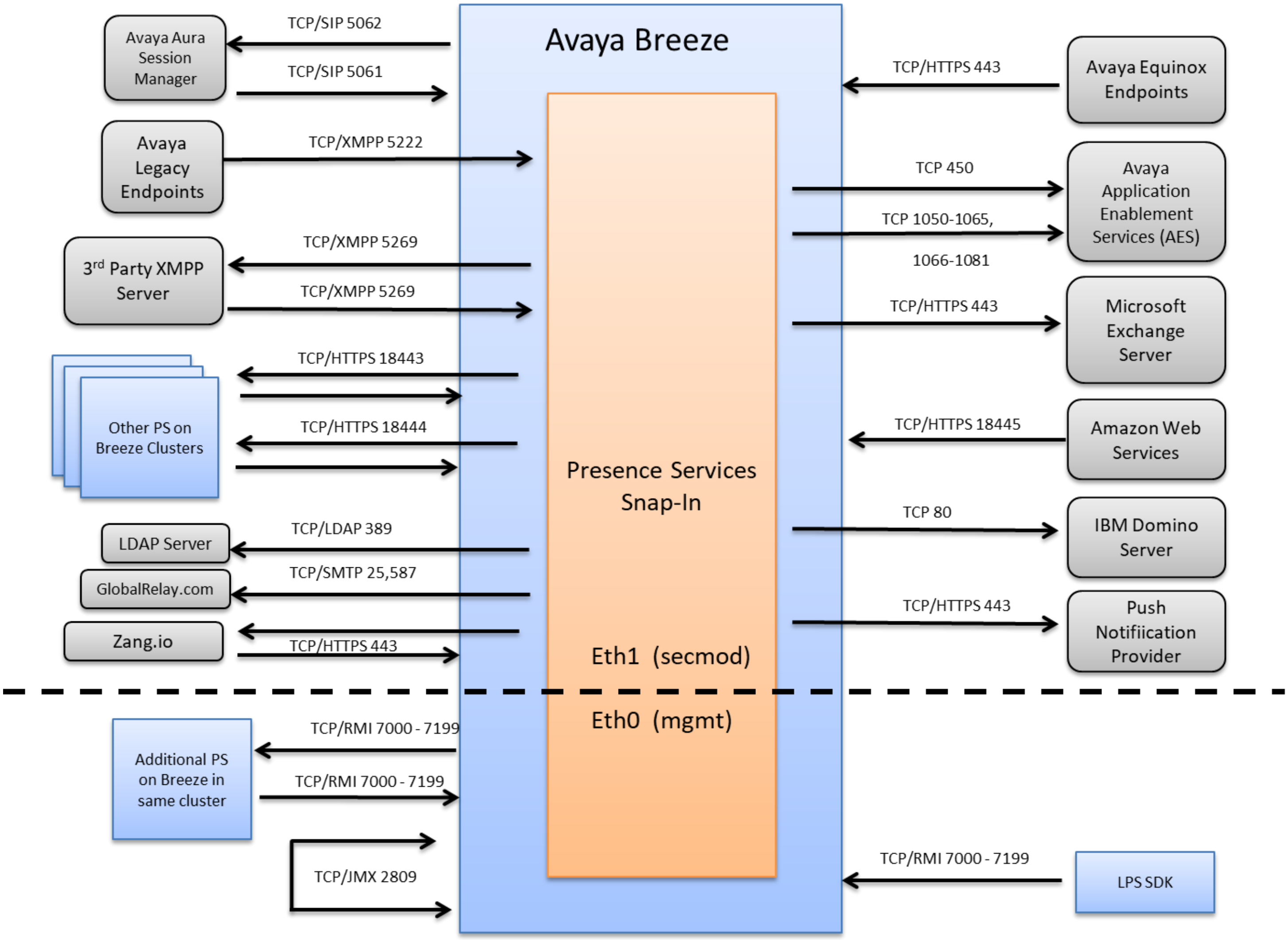
Table 3. Port Changes from Presence Services 8.1.1 to 8.1.2

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Interface)				

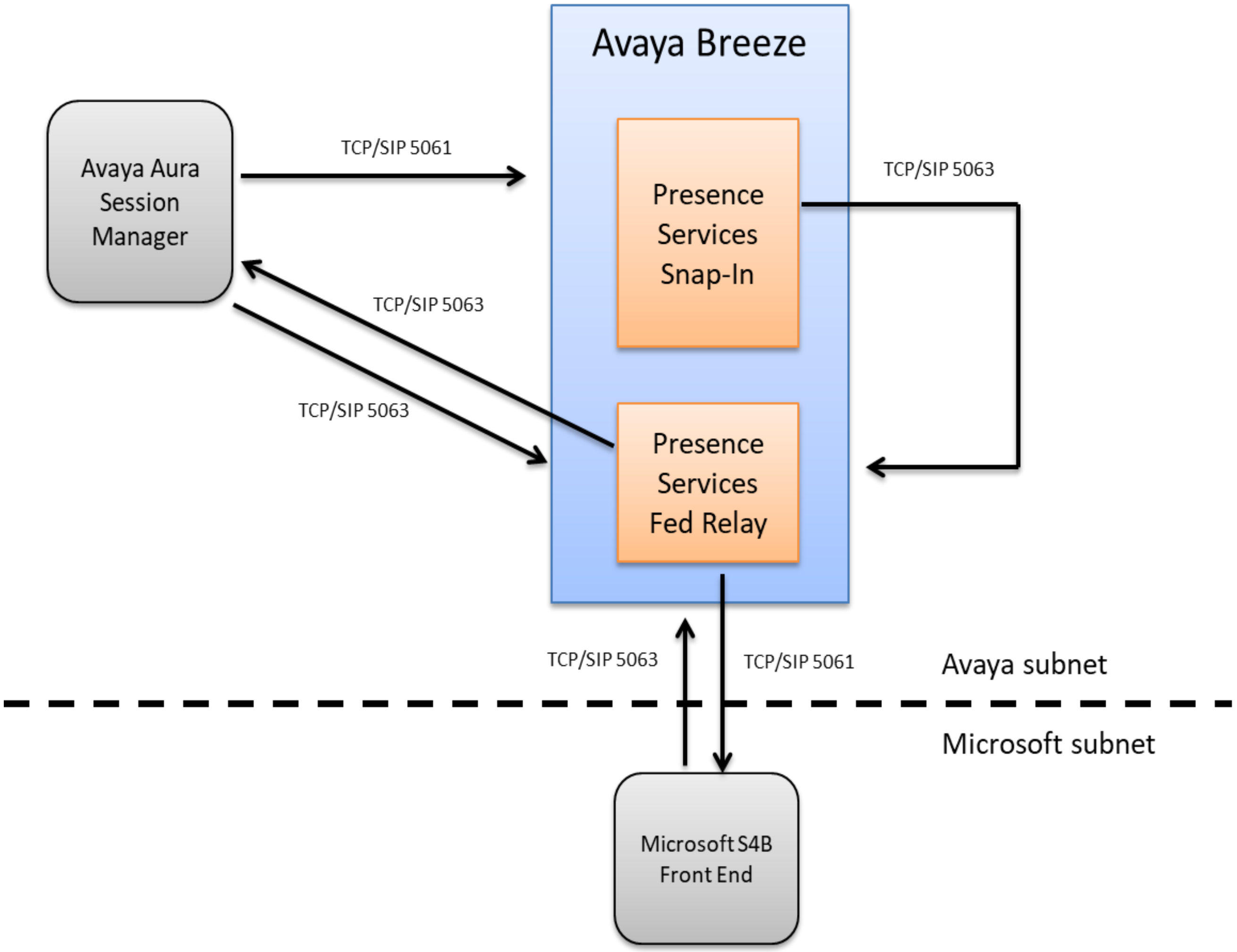
NOTES:

1. Some description 1.

3. Port Usage Diagram



Additional Port Usage when Microsoft Federation is enabled (with Avaya Aura in the same enterprise)



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) 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.

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: 172.16.16.14:123**5** - 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.

Socket Example Diagram

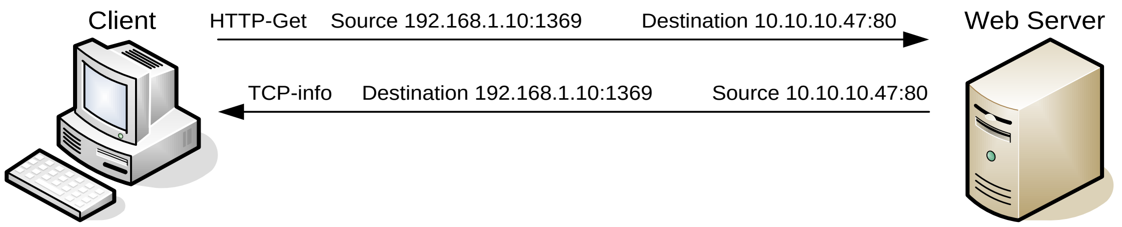


Figure 1. Socket example showing ingress and egress data flows from a PC to a web server

The client egress stream includes the client's source IP and socket (1369) and the destination IP and socket (80). The ingress stream from the server has the source and destination information reversed.

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[1].

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.