Avaya Port Matrix

Avaya Equinox 3.x

Issue 1.0
June 30, 2017

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. Avaya Equinox Components

Avaya Equinox is a high-performance enterprise collaboration tool for office and mobile employees.

Avaya Equinox provides access to multiple modalities such as IM/presence, text and multimedia messaging, multi-party audio/video, and content sharing to give users real choice in h ow to connect and engage with other people and groups.

Avaya Equinox offers a single contemporary user experience across platforms and devices including desktops, smartphones and tablets.

2. Port Usage Tables

2.1 Port Usage Table Heading Definitions

Source System: System name or type that initiate 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.

Transport/Application Protocol: This is the name associated with the layer-4 protocol higher level application protocols.

Optionally Enabled / Disabled: This field indicates whether customers can enable or disable a layer-4 port by changing its default port state 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.

2.2 Port Tables

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

Source		Destination		Transport / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	HTTP servers used to support Auto-configuration, Personal Profile Manager	80	TCP/HTTP	No	Closed	File downloads for service discovery, PPM
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	HTTP servers used to support Auto-configuration, Personal Profile Manager	443	TLS/HTTPS	No	Closed	File downloads for service discovery, PPM
Avaya Equinox iOS, Android	Ephemeral	Client Enablement Services	7777 (1024-65535)	TLS/ (Proprietary)	Yes	Closed	Messaging between Avaya Equinox and the Client Enablement Services. 7777 is the default port on the CES server, however confirm with the CES system administrator that this is the port in use for your deployment
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Session Manager (SM)	5060 (1024-65535)	TCP/SIP	Yes	Closed	SIP signaling traffic
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Session Manager (SM)	5061 (1024-65535)	TLS/SIPS	Yes	Closed	SIP signaling traffic
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Session Border Controller	3478	TCP/STUN TCP/TURN	No	Closed	STUN/TURN Nat Traversal

Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Session Border Controller	5349	TLS/STUN TLS/TURN	No	Closed	STUN/TURN Nat Traversal
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Media Gateway, Conferencing Server, Application Server, Desk Phone, Soft Client	1024-65535	UDP/RTP, UDP/RTCP, UDP/SRTP, UDP/SRTCP	No	Closed	Media traffic (audio/video) for SIP calls. The destination port range listed in this document (1024-65535) highlights that the actual destination port for media traffic for any call is dependent on the destination of the call and negotiated in real-time during call setup. It is not possible to provide the specific list of ports that will be negotiated for all possible call destinations in this document
Avaya Equinox, Windows, macOS	Ephemeral	LDAP Server	389	TCP	No	Closed	Enterprise Directory Contact Lookup
Avaya Equinox, Windows, macOS	Ephemeral	LDAP Server	636	TLS	No	Closed	Enterprise Directory Contact Lookup
Media Gateway, Conferencing Server, Application Server, Desk Phone, Soft Client	Ephemeral	Avaya Equinox	1024-65535	UDP/RTP, UDP/RTCP, UDP/SRTP, UDP/SRTCP	No	Closed	Media traffic (audio/video) for SIP calls. The destination port range listed in this document (1024-65535) highlights that the actual destination port for media traffic for any call is dependent on the destination of the call and negotiated in real-time during call setup. It is not possible to provide the specific list of ports that will be negotiated for all possible call destinations in this document
Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Multimedia Messaging server	8443 (1024-65535)	TLS/HTTPS	Yes	Closed	Messaging traffic.
Equinox, Windows, macOS, iOS, Android	Ephemeral	DNS Servers	53	UDP/DNS	No	Closed	Domain lookups, service discovery
Equinox, Windows, macOS, iOS, Android	Ephemeral	Google Analytics	443	TCP/HTTPS	No	Closed	Google Analytics

2.3 Port table changes from Avaya Communicator 2.1 to Avaya Equinox 3.0

Port Changes from Avaya Communicator 2.1 to Avaya Equinox 3.0

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Aura Device Services	8443	TLS/HTTPS	No	Closed	Device services e.g. Add, Remove, Search AADS Contacts
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Aura Web Collaboration	80	TCP/HTTP	No	Closed	Web collaboration
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Aura Web Collaboration	443	TLS/HTTPS Web Sockets	No	Closed	Web collaboration
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Equinox Conferencing Unified Conference Control	443	TLS/HTTPS	No	Closed	Unified Conference Control Server (equinox conferencing)
Avaya Equinox, macOS	Ephemeral	BFCP Peer	2070-2080	TCP/BFCP	Yes	Closed	Binary Floor Control Protocol for sharing video
Avaya Equinox, macOS	Ephemeral	BFCP Peer	1024 -65503	UDP/BFCP	Yes	Closed	Binary Floor Control Protocol for sharing video

2.4 Port table changes from Avaya Equinox 3.0 to Avaya Equinox 3.1

Port Changes from Avaya Equinox 3.0 to Avaya Equinox 3.1

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Avaya Equinox, macOS, iOS, Android	Ephemeral	Microsoft Exchange	443	TCP/HTTPS	No	Closed	Exchange Calendar meetings through Microsoft Exchange Exchange Web Services (EWS)

2.5 Port table changes from Avaya Equinox 3.1 to Avaya Equinox 3.2

Port Changes from Avaya Equinox 3.1 to Avaya Equinox 3.2

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	~~Avaya Aura Conferencing Web Collaboration,~~ Web Server to support configuration file.~~Avaya Aura Conferencing Web Collaboration, Google Analytics, and HTTP servers used to support Auto-~~	80	TCP/HTTP	No	Closed	~~Web CollaboratioFn,~~ file downloads for Configuration ~~Web Collaboration, usage traffic and file downloads for service discovery~~

Formatted Table

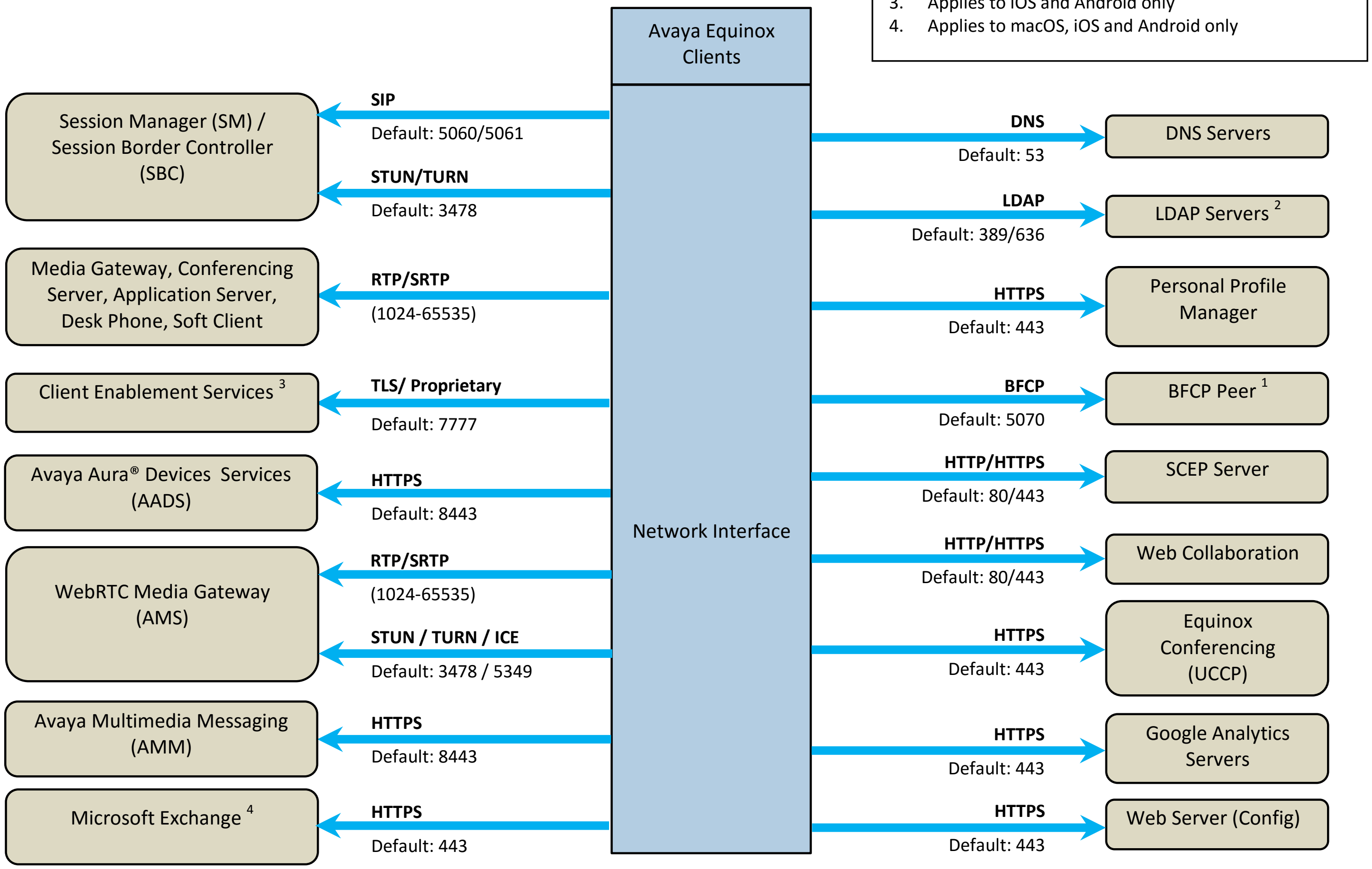
		~~configuration~~					
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Web Server to support configuration file.	443	TLS/HTTPS	No	Closed	F~~n,~~ file downloads for Configuration

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Web Server to support SCEP	443	TLS/HTTPS	No	Closed	Simple Certificate Enrollment Protocol for certificate distribution.
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Web Server to support SCEP	80	TCP/HTTP	No	Closed	Simple Certificate Enrollment Protocol for certificate distribution.
Avaya Equinox, Windows, macOS, iOS, Android	Ephemeral	Avaya Session Border Controller.	443	HTTPS	No	Closed	Media tunneled over HTTPS.

Formatted Table

3. Port Usage Diagram

1. BFCP is supported for macOS only
2. Applies to macOS and Windows platform only
3. Applies to iOS and Android only
4. Applies to macOS, iOS and Android only



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) 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. Consider your desktop PC. Multiple applications may be simultaneously receiving information. In this example, email may use destination TCP port 25, a browser may use destination TCP port 80 and a telnet session may use destination TCP port 23. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streams inside the PC. Furthermore, each of the mini-streams is directed to the correct high-level application because the port numbers identify which application each data mini-stream belongs. 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 (discussed later). 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 to a destination (server) using a specific port that has a known protocol associate with that 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 Type Ranges

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic Ports (sometimes called Private Ports).

Well Known Ports are those numbered from 0 through 1023.

Registered Ports are those numbered from 1024 through 49151

Dynamic Ports are those numbered from 49152 through 65535

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

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

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, 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
Data Flow 2:	172.16.16.14.123**5**	-	10.1.2.3:2345
Data Flow 3:	172.16.16.14:1234	-	10.1.2.4:2345

Data flow 1 has two different port numbers and two different IP addresses and is a valid and typical socket pair.
Data flow 2 has the same IP addresses and the same port number on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique.
Therefore, if one IP address octet changes, or one port number changes, the data flow is unique.

Figure 1, below, is an example showing ingress and egress data flows from a PC to a web server.

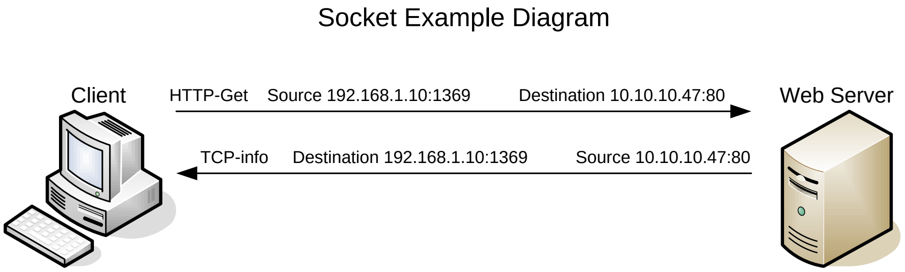


Figure 1. Socket Example

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

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[i].

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.

[i] 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.