Avaya Port Matrix

Avaya Session Border Controller for Enterprise (SBCE)

Release 8.x
Issue 1
December 2020

1. Avaya SBCE Components

Data flows and their sockets are owned and directed by an application. Here a server running on RHEL 7.2 has many applications, such as POSTGRES, SIP A/S, Apache, 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 Avaya SBCE are listed as follows.

Component	Interface	Description
AVAYA SBCE services	A1, A2, B1, B2	SIP, HTTP, TURN/STUN, XMPP and RTP/RTCP etc. traffic to/from traffic on these interfaces.
HA service	M2	Proprietary
AVAYA SBCE MGMT (Management)	M1	This is the management network interface. Used for • WebLM • SSH access • HTTPS for management • SNMP • Syslog • DB services • EMS and AVAYA SBCE secure communication

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.

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 AVAYA SBCE Management Interface (M1, M2)

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Admin terminal or SAL Gateway	Ephemeral	MGMT	222, 22	SSH	No	Open	System management requiring shell access
Admin terminal or NMS	Ephemeral	OAMP	161-162	UDP/SNMP	No	Open	SNMP queries to AVAYA SBCE
Client Web browser	Ephemeral	MGMT	443	TCP/HTTPS	No	Open	Apache Tomcat webserver running, Bidirectional between EMS-SBC
MGMT on AVAYA SBCE	Ephemeral	MGMT	443	TCP/HTTPS	No	Open	webservice running for syncing the certificates configured, Bidirectional between SBC-SBC ((SBC HA pair))
MGMT on EMS	Ephemeral	WebLM Server	52233	TCP	No	Open	Connectivity with WebLM server from EMS
MGMT on AVAYA SBCE	Ephemeral	WebLM server	52233	TCP	No	Closed	Connectivity with WebLM server from AVAYA SBCE
MGMT	123	External NTP server	123	UDP	No	Open	NTP time sync
MGMT on AVAYA SBCE	Ephemeral	MGMT on EMS	514	UDP	Yes	Closed	Syslog to EMS
MGMT on AVAYA SBCE	Ephemeral	External Syslog server	514	UDP	Yes	Closed	Syslog to external syslog server

MGMT on EMS	Ephemeral	External Syslog server	514	UDP	yes	Closed	Syslog to external syslog server
M2 on AVAYA SBCE	Ephemeral	M2 on AVAYA SBCE	1950	TCP	No	Open	Inter-AVAYA SBCE communication for HA
MGMT on AVAYA SBCE	53	DNS server	53	UDP	No	Closed	DNS service
MGMT on EMS/SBC	Ephemeral	MGMT	5432	TCP	No	Open	DB service – Bidirectional between EMS-SBC
MGMT on EMS/SBC	Ephemeral	MGMT	5432	TCP	No	Open	DB Service – Bidirectional Replication EMS-EMS (Active-Active EMS pair) and SBC-SBC(SBC HA pair)
MGMT on EMS/SBC	Ephemeral	MGMT	222	SSH	No	Open	Bidirectional between EMS-SBC and SBC-SBC
MGMT on AVAYA SBCE	Ephemeral	External RADIUS Server	1813 (1024-65535)	RADIUS	Yes	Closed	Radius Interface to send accounting DATA. Destination port range is configurable from 1024-65525
MGMT on AVAYA SBCE	Ephemeral	External SFTP server	22 (1-65535)	SFTP	Yes	Closed	SFTP from AVAYA SBCE to CDR Adjunct.
MGMT on AVAYA SBCE	Ephemeral	LDAP server	389	TCP/LDAP	yes	closed	LDAP interface for LDAP MAC auth and LDAP based routing feature
MGMT on AVAYA SBCE	Ephemeral	LDAP server	636	TCP/LDAPS	yes	closed	LDAP over TLS interface for LDAP MAC auth and LDAP based routing feature

Table 2. Ports for AVAYA SBCE data ports (A1, A2, B1, B2)

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
SIP endpoints	Ephemeral	SIP Signaling	5060 (1024-65535)	TCP/SIP	Yes	Closed	SIP signaling traffic – this is the default value, but other ports can be configured for SIP signaling using the AVAYA SBCE EMS
SIP endpoints	Ephemeral	SIP Signaling	5060 (1024-65535)	UDP/SIP	Yes	Closed	SIP signaling traffic – this is the default value, but other ports can be configured for SIP signaling using the AVAYA SBCE EMS
SIP endpoints	Ephemeral	SIP Signaling	5061 (1024-65535)	TCP/SIPS	Yes	Closed	SIP signaling traffic – this is the default value, but other ports can be configured for SIP signaling using the AVAYA SBCE EMS
SIP endpoints, WebRTC clients HTTP clients	Ephemeral	SIP Signaling	80	TCP/HTTP	Yes	Closed	Web Collab, Config file, firmware download, PPM configuration data downloaded to SIP endpoints, WebRTC
SIP endpoints, WebRTC clients HTTP clients	Ephemeral	SIP Signaling	443,9443	TCP/HTTPS	Yes	Closed	Web Collab, Config file, firmware download, PPM configuration data downloaded to SIP endpoints, WebRTC
SIP endpoints	Ephemeral	SIP Signaling	843	TCP/HTTPS	No	Open	Web Collab
SIP endpoints	Ephemeral	SIP Signaling	5222	TCP/XMPP	No	Open	XMPP
Device behind NAT	Ephemeral	STUN/TURN	3478	TCP/TURN-STUN	Yes	Closed	Used for STUN/TURN
Public Peer	Ephemeral	STUN/TURN	50000-55000	TCP/TURNSTUN	Yes	Closed	Used for Media Relay from and to public peer
Server behind NAT	Configured port	Reverse Proxy	40000-50000	TCP/HTTP	Yes	Closed	Used for connecting side
SIP end points, media servers	Configured port	Reverse Proxy	35000-50000 (1024-65535)	UDP/RTP, UDP/RTCP, UDP/SRTP, UDP/SRTCP	Yes	Closed	SIP voice traffic. The exact port is negotiated on a per call basis

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
AVAYA SBCE	Configured Port. Range 1024-65535	Avaya Media Server (AMS)	7150 (1024-65535)	HTTP/SOAP	Yes	Closed	External AMS – HTTP/SOAP Message exchange

2.3 Port Table Changes

NOTE:

There are no changes to the port tables for the following releases:

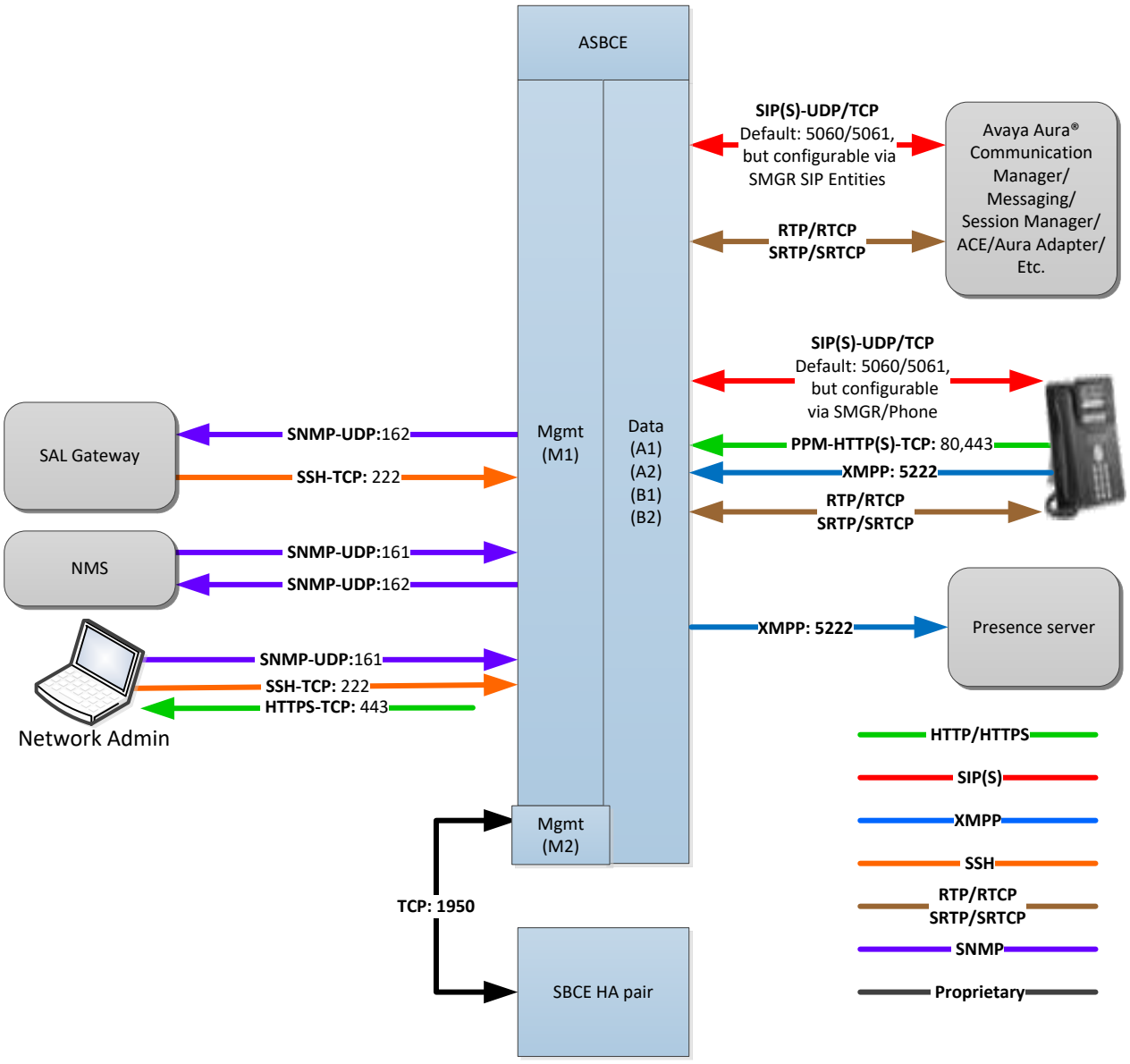
- Release 8.1.1 to 8.1.2
- Release 8.1.0 to Release 8.1.1
- Release 8.0.1 to R 8.1.0

Table 4. Port Changes from Avaya Session Border Controller 8.0.0 to 8.0.1

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Interface)				
Admin terminal or SAL Gateway	Ephemeral	MGMT	222, 22	SSH	No	Open	System management requiring shell access
MGMT on EMS/SBC	Ephemeral	MGMT	222,22	SSH	No	Open	Bidirectional between EMS-SBC and SBC-SBC

NOTE: Added SSH support on port 22

3. Port Usage Diagram



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 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 (like 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.

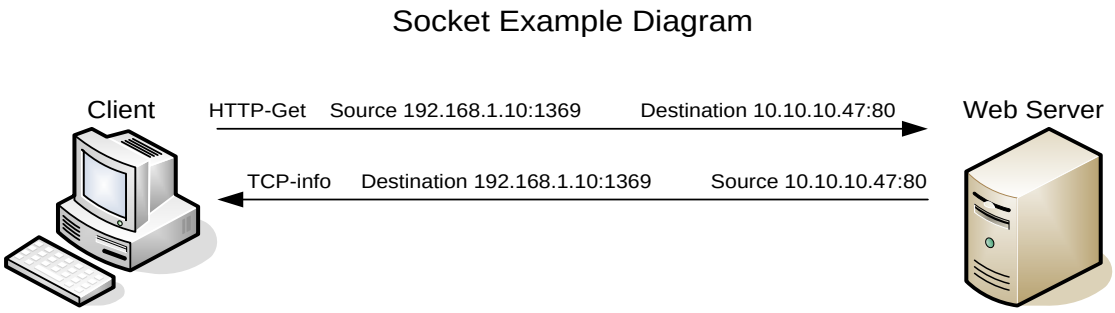


Figure 1. Socket example showing ingress and egress data flows from a PC to a web server

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[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.