Avaya Port Matrix

Call Management System (CMS) R20

Issue 1.0
May 17, 2023

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

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. CMS Components

Data flows and their sockets are owned and directed by an application. Here a server running on RHEL 6.4 has many applications, such as Tomcat, SSH, SAL, SNMP, 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. Application components in the CMS Application Server are listed as follows.

Component	Interface	Description
SPI (CM connection)	Eth0	This is the primary communication channel between the CMS and the CM. All call data and information is transferred over this link using a proprietary protocol. Additionally, administration changes (such as change agent skills) are sent over this link from the CMS to CM.
CMS Supervisor	Eth1	Supervisor is a thick-client application which communicates with CMS using either Telnet or SSH. It allows reporting and administrative capabilities.
CMS Supervisor Web	Eth1	Supervisor Web is a thin-client, browser-based reporting system for CMS. It communicates to the CMS using SSL.
SNMP-Agent	Eth1-3	SNMP (Simple Network Management Protocol) is an implementation of SNMP with a customized CMS MIB that can be used to send alarms to a SNMP Manager.
SAL-Agent	Eth1-3	The SAL Agent is a Java application which receives events and collects inventory information from the product and converts them to its own internal format, encapsulates the message into HTTPS, and sends it to an Enterprise Server, usually at Avaya.
ODBC/JDBC	Eth1-3	This is a direct connection into the CMS database via either ODBC or JDBC protocols. This allows third party applications to directly access CMS data without going through the CMS menu and reporting hierarchies.
Avaya CMS Connector Offerings		The Avaya CMS Connectors team offer a number of CMS enhancement applications that open various ports and add various protocols. These enhancement applications are used to provide some CMS add-on functionality and to provide communication with third-party vendors. The more common CMS Connector offerings are presented in the port matrix in this document, but this is not an all-inclusive list. Questions regarding CMS Connector enhancements and offerings should be directed to the Avaya CMS Connectors documentation and team.

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.

NOTE: By default, all ports on CMS are open. To close ports and manage exceptions according to the usage described in the table below, turn on the firewall. The firewall can be activated in CMS using the ‘cmssvc’ menu and choosing the ‘security’ option.

Ports not mentioned in this document are not critical for CMS operation and can be closed. The table notes port usage for various operations. If customers change or assign different ports (than listed in the table) to these operations, they do so at their own risk.

Table 1. Ports for Call Management System

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Admin terminal, Avaya Supervisor, or SAL Gateway, SSH, SFTP	Ephemeral	CMS	22	TCP/SSH/SFTP	No	Open	System management requiring shell access, Supervisor connection preferred method for call center administration n, Secure shell, Secure file transfer.
Admin terminal, Avaya Supervisor	Ephemeral	CMS	23	TCP/Telnet	No (Note 1)	Open (Note 1)	Supervisor connection for call center administration. Open only for localhost.
CMS	Ephemeral	WebLM	52233	TCP	No	Open	Connection from CMS to WebLM is outgoing and required for license authentication
CMS internal Web	Ephemeral	CMS	6001 (Note 6)	NA	Yes	Open	Used for internal communication only. See Note 6.
CMS Web User	Ephemeral	CMS	8443	TCP/HTTPS	Yes	Open	Main listening port for CMS Web.
ODBC / JDBC Client	Ephemeral	CMS	50000, 50001	TCP	Yes	Open	Informix ODBC / JDBC Agent for CMS database

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Netbackup	Ephemeral	CMS	1556/13724	TCP	Yes	Open	Netbackup and restore.
CMS	Ephemeral	CM	5001-64500	TCP/SPI (Proprietary)	No	Open	Used for ACD1-ACD8 connections to the CM. See Note 3.
CMS	Ephemeral	Network Time Server	123	UDP/NTP	Yes	Open	Used to keep system time current. See note 5
CMS	Ephemeral	SNMP NMS SNMP SAL Gateway	162	TCP/ SNMP Trap	Yes	Open	SNMP Trap for alarms
CMS	Ephemeral	HP Printers	9100	TCP/UDP	Yes	Open	Professional Services installation to communicate with HP print servers. See Note 4.
CMS	3077,3078, 3079	CMS (HA pair)	3077,3078, 3079	TCP	Yes	Open	High Availability option data sync utility. See Note 4.
CMS	22, Ephemeral	ECH Receiver	22	TCP/UUCP	Yes	Open	External Call History file transfer mechanism. See Note 4.
CMS	Ephemeral	Real-time Connectors	6000-7000	TCP/UDP	Yes	Open	Professional Services installation for real-time communication with third-party servers. See Notes 2, 4.
CMS	Ephemeral	Historical Connectors	22	TCP/SFTP	Yes	Open	Professional Services installation for historical communication with third-party servers. See Notes 2, 4.

NOTES:

1 Supervisor requires port to be open, telnet can be restricted to only localhost connections.
2 Real-time connectors send streams of data from CMS to a specific port on the receiving server. They data streams can be encrypted using the 'stunnel' open-source application.
3 ACD Ports are configured in CMs.
4 This is an offering from the Avaya CMS Connectors team and not part of standard CMS configuration, any questions regarding these services should be directed to the Avaya CMS Connectors team.
5 This is covered under Avaya's Permissive Use Policy.
6 Port 6001 can be closed without impacting CMS Web operations. If CMS is used to activate the internal firewall, port 6001 will be closed.

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.

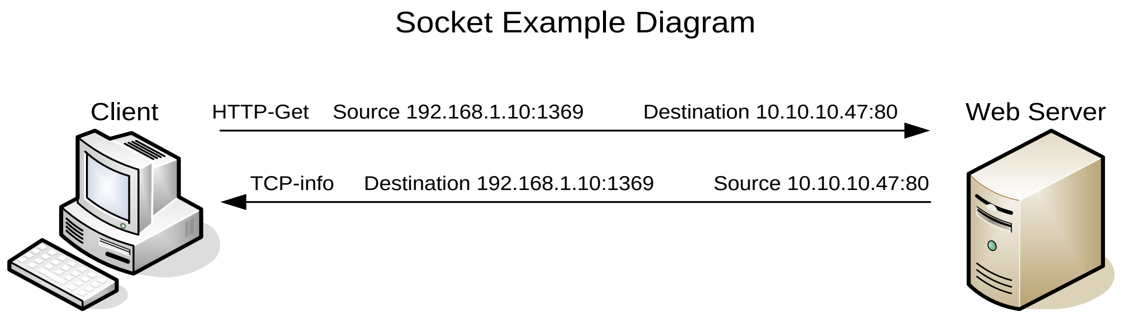

Figure 1. Socket example showing ingress and egress data flows from a PC to a web server

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.