

Avaya Port Matrix:

Call Management System (CMS) R17

Issue 0.1
July 2014

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.

© 2014 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.

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

1. Call Management System Components

Data flows and their sockets are owned and directed by an application. Here a server running on RHEL 6.3 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, so the firewall (iptables service) should be running on the same server. Application components in the Call Management System Application Server are listed as follows. Note: CMS has four Ethernet interfaces and can be used in virtually any combination, it is generally recommended that SPI traffic be separated from user (Supervisor and Web and Mobile Client) as reflected in the table below.

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.
CMS Mobile Supervisor	Eth1	Mobile Supervisor is an iOS based iPad application which provides a “dashboard” type interface into the CMS for monitoring call center assets. It communicates using the same protocol as CMS Supervisor Web.
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. Note: CMS can have SAL embedded (run on the CMS itself) or it can use an existing SAL server that the customer has.
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.
Professional Services Offerings		Avaya Professional Services offers a number of CMS enhancements that open various ports and add various protocols. The more common Professional Services offerings are presented in the port matrix in this document, but this is not an all-inclusive list. Questions regarding Professional Services enhancements and offerings should be directed to Avaya Professional Services.

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

2. Port Usage Tables

2.1 Port Usage Table Heading Definitions

Ingress Connections (In): This indicates connection requests that are initiated from external devices to open ports on this product. From the point of view of the product, the connection request is coming "In". (Note that in most cases, traffic will flow in both directions.)

Egress Connections (Out): This indicates connection requests that are initiated from this product to known ports on a remote device. From the point of view of the product, the connection request is going "Out". (Note that in most cases, traffic will flow in both directions.)

Intra-Device Connections: This indicates connection requests that both originate and terminate on this product. Normally these would be handled on the loopback interface, but there may be some exceptions where modules within this product must communicate on ports open on one of the physical Ethernet interfaces. These ports would not need to be configured on an external firewall, but may show up on a port scan of the product.

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. Refer to the Notes section after each table for specifics on valid port ranges.

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, filtered or N/A.

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.

N/A is used for the egress default port state since these are not listening ports on the product.

External Device: This is the remote device that is initiating a connection request (Ingress Connections) or receiving a connection request (Egress Connections).

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

2.2 Port Tables

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

Table 1. Ports for Call Management System Management Interface

Note: Depending on the configuration, these network services could be using any of the Ethernet ports on the CMS server. Generally, it is recommended to separate communication between the CMS and CM from other network traffic, but there is no specific required configuration with regards to how the Ethernet ports are used.

No.	Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
INGRESS CONNECTIONS							
1	22	TCP/SSH	Yes	Open	Admin terminal, Avaya Supervisor, or SAL Gateway	System mgmt requiring shell access, Supervisor connection preferred method for call center administration	
2	23	TCP/Telnet	No (see Notes)	Open (see Notes)	Admin terminal, Avaya Supervisor	Supervisor connection for call center administration	1
3	111	TCP/UDP	No	Open	rpc services	The rpcbind utility is a server that converts RPC program numbers into universal addresses. It must be running on the host to be able to make RPC calls on a server on that machine.	
4	161,162	UDP	Yes	Closed	SAL Server	Used by embedded SAL gateway for alarming	7
5	443	TCP	Yes	Closed	SAL Server	Used by embedded SAL gateway for alarming	7
6	515	TCP/UDP	Yes	Closed	System Users	UNIX line printer spooler	4
7	631	TCP/UDP/IPP	Yes	Open	System Users	Internet Printing Protocol	
8	705	TCP/UDP/SNMP	Yes	Closed	SNMP Receiver	Used by both embedded SAL server and SNMP	7, 8
9	725	TCP/SNMP	Yes	Closed	SNMP	SNMP for alarming to customer NOC	8
10	8005, 8009, 8080, 8089	TCP/HTTPS	Yes	Open	CMS Web User	AJP (Apache JServ Protocol), MXI, used by CMS Web and Mobile clients	6
11	8443	TCP/HTTPS	Yes	Open	CMS Web User	Main listening port for CMS Web and CMS Mobile clients	6
12	9980	TCP/UDP/Proprietary	Yes	Closed	Admin User	Link Admin	4

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

No.	Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
13	9999	TCP/UDP/Proprietary	Yes	Closed	CVLAN	CallVisor LAN client/server implementation of CallVisor API	4
14	50000, 50001	TCP	No	Open	ODBC / JDBC Client	Informix ODBC / JDBC Agent for CMS database	
EGRESS CONNECTIONS							
1	21	TCP/FTP	Yes	Closed	Various PSO offers	File Transfer Protocol	2
2	9100	TCP/UDP	Yes	Closed	HP Printers	Professional Services installation to communicate with HP print servers	4
3	700, 4046	TCP/UDP/NFS	Yes	Closed	Network File System	NFS used for CMS backups (Client Only)	
INTRA-DEVICE CONNECTIONS							
1	37	TCP/NTP	No	Closed	Network Time Server	Used to keep system time current	5, 4
2	514	TCP	Yes	Closed	CMS HA Pair Partner	High Availability option data sync utility	4
3	540	TCP/UUCP	Yes	Closed	ECH Receiver	External Call History file transfer mechanism	4
4	3077, 3078	TCP	Yes	Closed	CMS HA Pair Partner	High Availability option data sync utility	4
5	4046	TCP/NFS	Yes	Closed	NFS Server	Used by CMS when NFS backups are being used	
6	5001-5008	TCP/SPI (Proprietary)	No	Open	CM	5001-5009 are the default ports for ACD1-ACD8 connections to the CM	3
7	5011-5012	TCP/UDP/Proprietary	Yes	Closed	ASAI	Adjunct/Switch Application Interface	4
8	6001	TCP	Yes	Open	System user	X11 used between an X client and X server	
9	6060	TCP/UDP	Yes	Closed	GEOTEL	Professional Services installation for communication with Geotel call routing system	4
10	32771-32772	TCP/UDP	Yes	Open	NFS	NFS status daemon used for NFS backups	

NOTES:

1 Supervisor requires port to be open, but by default it is restricted to only localhost connections
2 FTP is used by a variety of Avaya Professional Service Offerings particularly with External Call History file transport
3 Only ports with active ACD connections need to be open. For example, a single ACD system would typically only use port 5001, and the remaining ports 5002-5009 would not be necessary
4 This is an offering from Avaya Professional Services and not part of standard CMS configuration, any questions regarding these services should be directed to Avaya Professional Services.
5 This is covered under Avaya's Permissive Use Policy.
6 If CMS Web and CMS Mobile clients are not being used, these ports can be closed by turning off CMS Web on the CMS server.
7 If Embedded SAL isn't being used on the CMS, these ports will not be open. Embedded SAL must be administered and activated for these ports to open.

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

8 If SNMP isn't being used on the CMS, these ports will not be open. Embedded SAL must be administered and activated for these ports to open

Note:

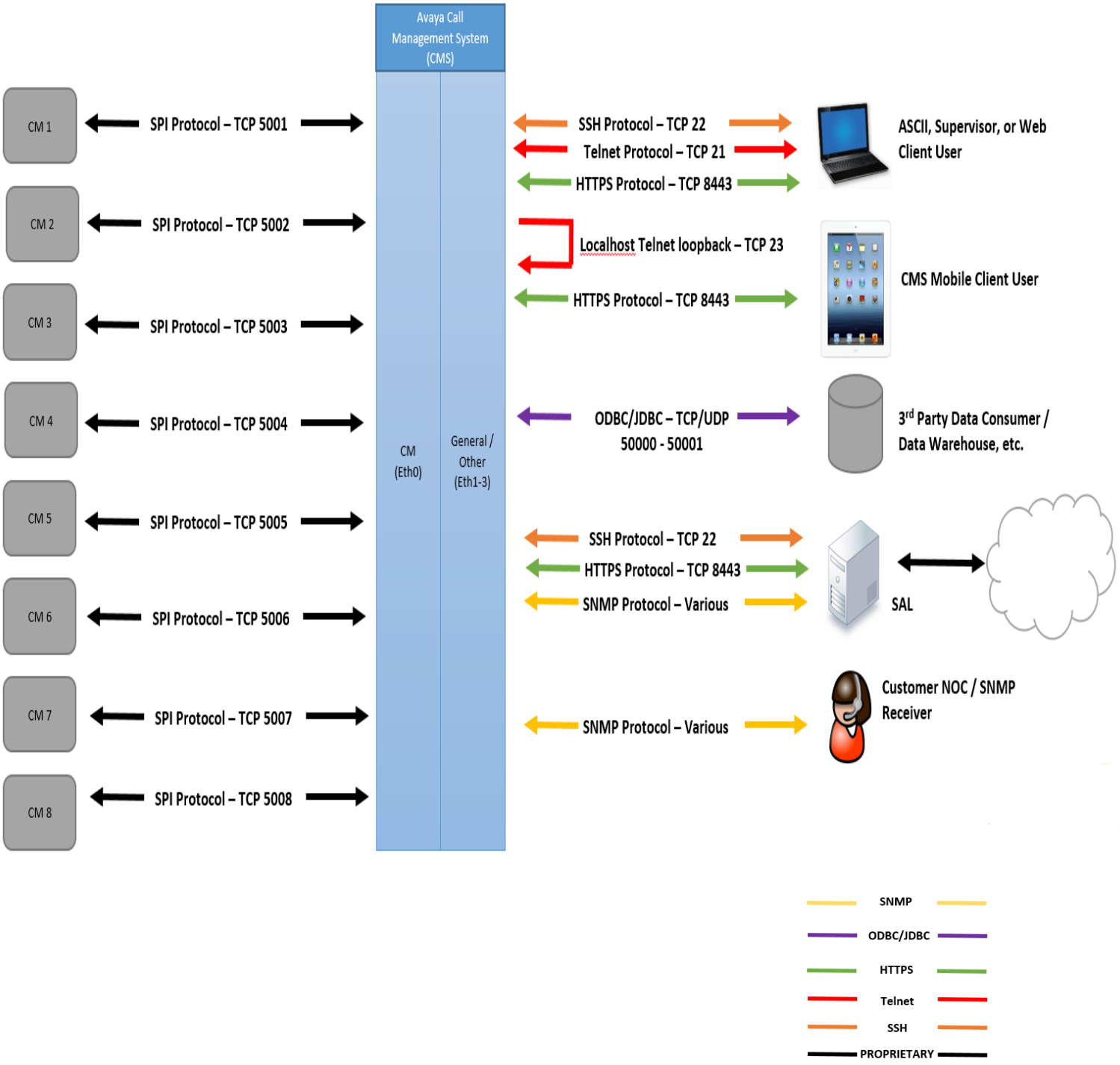
Many processes/applications open private ports in the range of 49152 to 65535 as temporary communication channels. It is not uncommon to see a number of ports in this range open.

If one wishes to determine what CMS process is using a particular port, the fuser command will provide the PID of the process using the port. Please see the man page for fuser for more information.

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

3. Port Usage Diagram

NOTE: This presents a typical usage of CMS. Configurations will vary. Also note that no Avaya Professional Services Offerings or NFS/Network backup methods are included on this diagram.



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.

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

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.

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

Socket Example Diagram

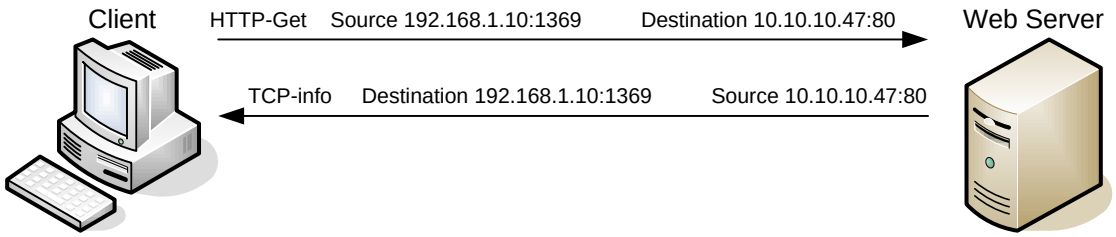


Figure 1. Socket Example

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

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

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.

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