Avaya Port Matrix:

Avaya Aura® Messaging 7.0

Issue 1.0
18 August 2016

1. Avaya Aura® Messaging Components

Data flows and their sockets are owned and directed by Messaging. AAM components in the Avaya Aura® Messaging Server are listed as follows.

Component	Interface	Description
Application	Eth0 (public IP)	SIP/RTP traffic to/from Telephony. The relationship between TUI Application and AxC is based on Web services as well as in case of another Application in a cluster.
AxC	Eth0 (public IP) and Lo (Local Loopback)	AxC may interact with the following hosts: - TUI Application through Web services (eth0) - Outlook Form through HTTP (Play On Phone feature) (eth0) - User Preferences browser through HTTP (eth0) - WebLM server through Web services (eth0) - MsgCore through LDAP\SMTP\IMAP (lo) - External storage (Exchange) through HTTP (eth0)
Storage	Eth0 (public IP) and Lo (Local Loopback)	MsgCore may interact with the following hosts: - IMAP clients\one-X client through IMAP (eth0) - SMTP gateway through SMTP (eth0) - Voicemail networking (MN, peers) through SMTP (eth0) - AxC through LDAP\SMTP\IMAP (lo) - Provision through LDAP (eth0)

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. Refer to the footnotesection after tables 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.

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).

2.2 Port Tables

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

Table 1. Ports for Avaya Aura® Messaging Management Interface (eth0)

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	Support team requires shell access	
2	23	TCP/telnet	Yes	Filtered	Admin terminal	Processing telnet connection	
3	25 (1024-65534)	TCP/SMTP	Yes	Open	External email client	SMTP queries to Messagingl	
4	80	TCP/HTTP	No	Open	Application server , Web access (SMI)	User's access via SMI, Application server traffic	Redirects to HTTPS by default
5	110 (1024-65534)	TCP/POP3	Yes	Filtered	External email client	Email clients can be configured to received voice messages from AAM user's mailboxes.	
6	143 (1024-65534)	TCP/IMAP	Yes	Filtered	External email client	Email clients can be configured to receive voice messages from AAM user's mailboxes.	
7	161	UDP/SNMP	No	Open	Admin terminal or NMS	SNMP queries to Messaging	
8	389 (1024-65534)	TCP/LDAP	No	Open	The Provision tool, LDAP client	This protocol is used by the Provision tool. Also it may be used to access data via LDAP client.	
9	443	TCP/HTTPS	No	Open	Application server , Web access (SMI)	User's access via SMI, Application server traffic	
10	465 (1024-65534)	TCP/SMTPS	Yes	Open	External email client	SMTP queries to Messaging	
11	514	TCP/SYSLOG	No	Filtered	Syslog server	Using to send event info to Syslog server or syslog daemon	
12	636 (1024-65534)	TCP/LDAPS	Yes	Open	The Provision tool, LDAP client	This protocol is used by the Provision tool. Also it may be used to access data via LDAP client.	

No.	Default Destination Port (Configurable Range*)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
13	843	TCP/RAW	No	Open	Subscriber's Web Browser	Provides Flash Socket Policy for AAM Web Access	
14	993 (1024-65534)	TCP/IMAPS	Yes	Filtered	External email client	Email clients can be configured to receive voice messages from AAM user's mailboxes.	
15	995 (1024-65534)	TCP/POP3S	Yes	Filtered	External email client	Email clients can be configured to received voice messages from AAM user's mailboxes.	
16	2222	TCP/HP-SSHD	Yes	Open	Admin terminal	This port is used by CM only if a system is in trouble and it cannot gain access over port 22	Not used by AAM
17	2945	TCP/ H248-BINARY	No	Closed	Gateways (G850s)	Gateways handle media signaling	Not used by AAM
18	5060 (1024-65534)	TCP/SIP	No	Open	SIP endpoint	Using by SIP client to connect\disconnect calls	
19	5061 (1024-65534)	TCP/SIP TLS	No	Filtered	SIP endpoint	Using by SIP client to connect\disconnect calls	
20	8443	TCP/WSS	No	Open	Subscriber's Web Browser	SSL HTTP connector of Tomcat 7. Used for Web Socket over HTTPS (WSS) by WNS to send out notifications to subscriber's browser.	
21	8631	TCP/IPP	No	Open	Windows PC printer service	Accessed by end user Windows PCs in order to transfer outbound faxes to the AAM server to be sent to destination fax machines.	
22	10100	TCP/HTTPS	No	Open	Subscriber's Web Browser	Subscriber's access to AAM Web Access	
23	1024-65534	UDP/No	No	Filtered	It depends on specific protocol	Used by several protocols to reach clients, including RTP/SRTP	
24	N\A	ICMP/N\A	No	Open	SIP Servers	Used by SIP entities to verify connectivity to Messaging	
EGRESS CONNECTIONS							
1	25 (1024-65534)	TCP/SMTP	Yes	Open	External email client	SMTP queries from Messaging to Email client (i.e. MS Outlook)	
2	53	UDP/DNS	No	Filtered	DNS server	Looking DNS server for IP address resolution	

No.	Default Destination Port (Configurable Range*)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
3	123	TCP/NTP	No	Filtered	NTP server	Using NTP server allows to sync AAM servers with precise time	
4	161	UDP/SNMP	No	Open	Admin terminal or NMS	SNMP acceptance and SNMP MIB II requests can be sent to a configured SNMP NMSs	
5	162	UDP/SNMPTRAP	No	Filtered	NMS	SNMP traps from Messaging	
6	465 (1024-65534)	TCP/SMTPS	Yes	Open	External email client	SMTPS queries from Messaging to Email client (i.e. MS Outlook)	
7	2222	TCP/SFTP	Yes	Open	Admin terminal	Outbound SFTP backups to external sources	
8	1024-65534	UDP/No	No	Filtered	It depends on specific protocol	Used by several protocols to reach clients, including RTP/SRTP	
INTRA-DEVICE CONNECTIONS							
1	4900/5070/5071/ 6075/6076/57990/ 10201/10202	TCP/NSSserver	No	Open	N/A	Avaya proprietary use - Used to translate text to speech (TTS)	
2	5022	TCP/SSH	Yes	Open	N/A	Avaya proprietary use (unused) - secure	
3	5023	TCP/SAT	Yes	Filtered	N/A	Avaya proprietary use (unused) – System Access Terminal	
4	7000	TCP/JAVA-TOMCAT-M	No	Filtered	N/A	Java HTTP web server environment for Java code to run in	
5	7117	TCP/JAVA-AIC	No	Open	N/A	Avaya proprietary use - AxC	
7	7121	TCP/JAVA-MWILISTENER	No	Open	N/A	Avaya proprietary use - MWI Listener	
8	7171	TCP/JAVA-AICWEB	No	Open	N/A	Avaya proprietary use - AxC web server	
9	7172	TCP/JAVA-FAXPRINTE	No	Open	N/A	Avaya proprietary use - used by the SMI to display the list of active faxes	
10	8000	TCP/VXIBROWSER	No	Open	N/A	Avaya proprietary use - VXIBROWSER	

No.	Default Destination Port (Configurable Range*)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
11	8006	TCP/JAVA-TOMCAT-M	No	Open	N/A	Java HTTP web server environment for Java code to run in	
12	8081	TCP/ ADCS-JAX	No	Filtered	N/A	Avaya proprietary use	
13	8083	TCP/ ADCS-FETCH	No	Filtered	N/A	Avaya proprietary use – cluster communications	
14	8161	TCP/JAVA-ACTIVEMQ	No	Open	N/A	Avaya proprietary use	
15	10000	TCP/JAVA-TOMCAT-W	No	Open	N/A	Tomcat Connector for Web Access REST service. Used by AxC to gather login statistics.	
16	8200/8201/50922	TCP/NUANCE-SERVER	No	Open	N/A	Avaya proprietary use - Used for automatic speech recognition (ASR)	
17	10006	TCP/JAVA-TOMCAT-W/ RAW	No	Open	N/A	Tomcat shutdown control port	
18	10009	TCP/JAVA-TOMCAT-W /AJP	No	Open	N/A	Tomcat Apach JServ Protocol (AJP) connector between Apach HTTPD and Tomcat hosting Web Access server apps (MWS and WNS). Apache proxies AJAX requests from 10100 to 10009.	
19	10101	TCP/HTTPD	No	Open	N/A	Avaya proprietary use - for the Aura Messaging Web Access	
20	55000 (1024-65534)	TCP/MCAPI	No	Open	N/A	Avaya proprietary use - legacy mail access API	
21	1024-65534	UDP/No	No	Filtered	It depends on specific protocol	Used by several protocols to reach clients, including RTP/SRTP	

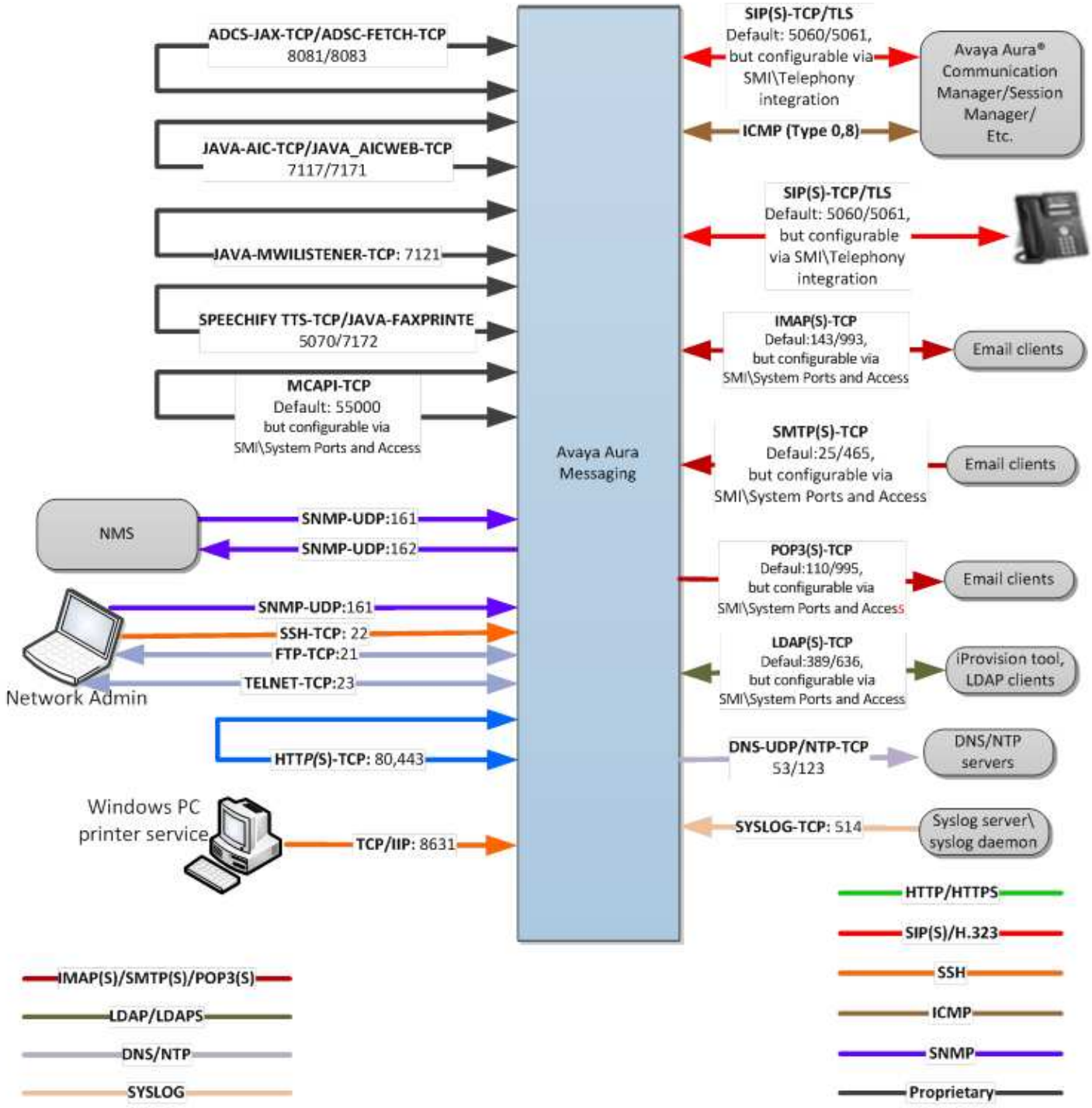
***** - If a specific port's description contain a configurable range in parenthesis (e.g. 1024-65534), it means the port can be configured to a different port number via the SMI. There is no need to open all ports in the range but only the actual port used for communication.

2.3 Port Table Changes

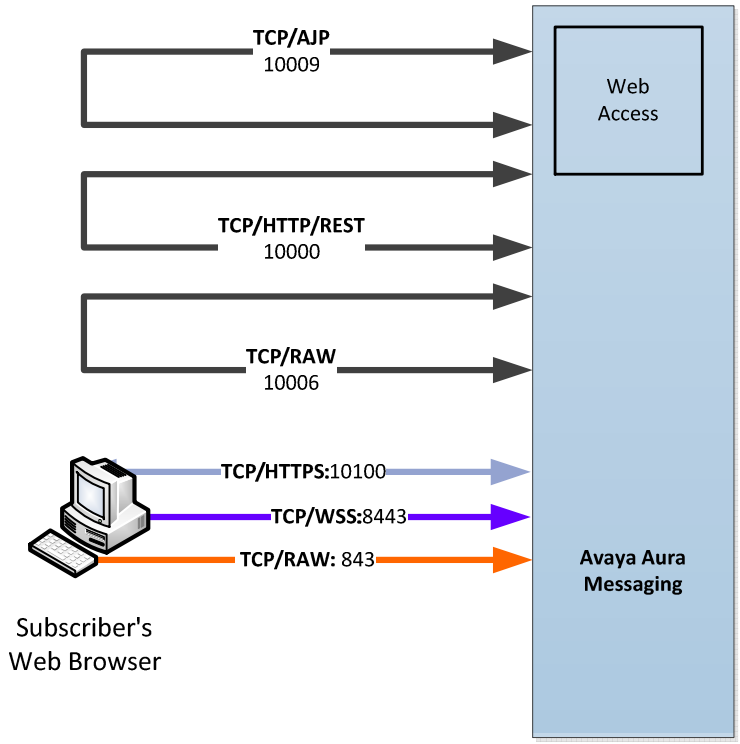
Table 3. Port Changes From Avaya Aura® Messaging 6.3 to 7.0

No.	Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED							
1	4900/5070/5071/ 6075/6076/57990/ 10201/10202	TCP/NSSserver	No	Open	N/A	Avaya proprietary use - Used to translate text to speech (TTS)	
2	8200/8201/50922	TCP/NUANCE-SERVER	No	Open	N/A	Avaya proprietary use - Used for automatic speech recognition (ASR)	
PORTS DELETED							
1	5555	TCP/TTS	No	Open	N/A	Avaya proprietary use - Used to translate text to speech	

3. Port Usage Diagram



Port Usage Diagram. Cont'(Web Access)



4. 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:	172.16.16.14.1235	-	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.

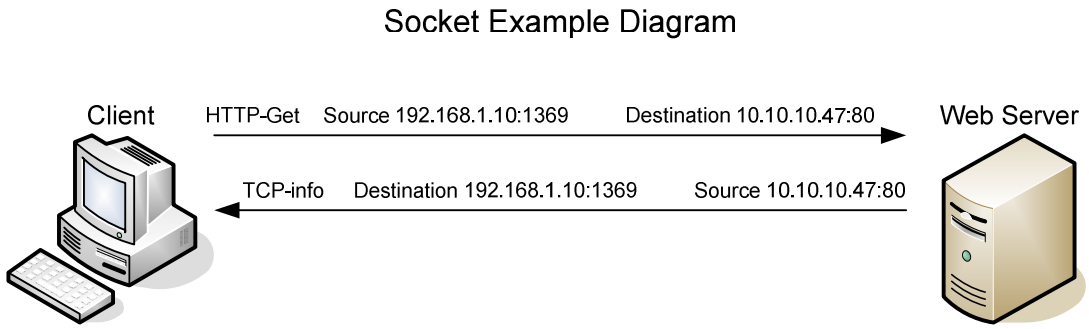


Figure 1. Socket Example

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[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.