Avaya Port Matrix:

Avaya Aura®
CC Elite Multi Channel 6.6

Document Status: Published

Issue 0.1

June 18, 2019

Change History

Issue	Date	Author	Description
0.1	Feb 26 2019	Pankaj Gandhe	Initial draft – added post for secure AES

1. Elite Multi Channel (EMC) Components

Data flows and their sockets are owned and directed by an application. Here a server running on Windows Server Platforms has many applications. 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 should be running on the same server.

Application components in the Elite Multi Channel are listed as follows.

Component	Interface	Description
Desktop -Call Center Elite Multichannel Desktop -Call Center Elite Multichannel Reporting -Call Center Elite Multichannel Control Panel)	IPv4 – Ethernet (Private IP)	There are three Desktop components which communicates with server using TCP (.Net Remoting) connection
Application Management Director	IPv4 – Ethernet (Private IP)	This component used by all services and Control Panel to publish itself to other EMC services.
License Director	IPv4 – Ethernet (Private IP)	This server communicates with Avaya WebLM server and gets the licenses and manages licenses for EMC server and Desktops.
Call Routing	IPv4 – Ethernet (Private IP)	This adds additional routing logic for calls on configuration
Configuration	IPv4 – Ethernet (Private IP)	Provides configuration to the EMC Agents. Connects to EMC Desktop through TCP port

Task Director	IPv4 – Ethernet (Private IP)	This manages the automated reporting task for EMC reporting server.
Media Director	IPv4 – Ethernet (Private IP)	Communicates with XML Server, all the Media Stores, and Desktop using pre-defined TCP port. And manages the Media Licenses and Multimedia workitem data.
XML	IPv4 – Ethernet (Private IP)	It core EMC Component, this connects with AES TSAPI client using pre-defined port. Also accepts TCP connection for Telephony operations.
Virtual Agent	IPv4 – Ethernet (Private IP)	Automated Agent which can be used or predefined work schedules.
Experience Portal Config	IPv4 – Ethernet (Private IP)	Provides interface to connect to management web page of Experience portal server.
Call Recording Config Service	IPv4 – Ethernet (Private IP)	Provides On demand recording option to EMC Desktop.
Interaction Data Service -Interaction Data Server - Multimedia -Interaction Data Server - Voice and Presence -Interaction Data Server – View	IPv4 – Ethernet (Private IP)	Manages all the Historical and Realtime Database. This connects with multiple EMC Server components like XML server, Media stores. And also with SQL database server.

Media Stores -Preview Contact -Simple Messaging -Email -Voice	IPv4 – Ethernet (Private IP)	Media Store accepts .Net Remoting connections on the predefined port and also communicates with external servers to get multimedia work item.
Gateways -Web Chat -Short Message Service -XMPP	IPv4 – Ethernet (Private IP)	Interfaces implemented to connect to remote media services and Simple Messaging Media Store. It creates a .Net Remoting channel using the published pre-defined port.
Plug-ins -SQL -Rules -SOAP -Script)	IPv4 – Ethernet (Private IP)	Custom plugin can be added to the Elite Multichannel Desktops to execute their own process/program.
Trace System -TTrace Console -TTraceConfig -TTrace Log2Zip	IPv4 – Ethernet (Private IP)	This is logging application server which will get the Traces sent by the multiple application and can be monitored using one console application.
Databases -ASMSControl -ASContact -ASMSDataX -ACS(Optional)	IPv4 – Ethernet (Private IP)	SQL Databases are accessed by Server components as well as Desktop component. It is used to save Historical data, Contact Database, and Configuration Database for Agents.
Developer -Developer Tools	N/A	No connection required outside the system. This component provides environment custom Desktop plugin.

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 Elite Multi-Channel

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	**Port (Configurable Range)**	**System**	**Port (Configurable Range)**				
EMC– Desktops	Ephemeral	Microsoft CRM Connector	29027	IP–Multicast Multicast group address : 239.29.9.67	Yes	Closed	The Realtime Phonebook Synchronizer component installed on the Microsoft CRM Server uses multicasting to send Contact and Account updates to all Call Center Elite Multichannel Desktops. This allows the cached phonebook (contacts and accounts phone numbers with non-numerics stripped out) to be up-to-date in real-time.
EMC - Applications	Ephemeral	EMC - Application Management Service	29075	IP–Multicast Multicast group address : 239.29.9.67	Yes	Open	Application Management Service uses multicasting to locate and identify Call Center Elite Multichannel applications that are running on the network. All applications join the multicast group at the specified IP address/port. Application Management Service broadcasts the IP address and port number that it can be contacted on. This port can be specified by the administrator but will default to the value specified.
			29074	.Net Remoting	No		
EMC – Desktops	Ephemeral	EMC - Configuration Server	29091	TCP	No	Open	Configuration Server receives inbound client connections for configuration data.
			39091	**Secure TCP**	Yes		
EMC Desktop	Ephemeral	EMC - Email Media Store	**39097**	**Secure TCP (.Net Remoting)**	Yes	Open	Email Media Store accepts .Net Remoting connections on the predefined port.
Media Director / Desktops / Control Panel			29097	TCP (.Net Remoting)	No		

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
IDS-View	Ephemeral	EMC- IDS - Voice and Presence	29090	TCP	No	Open	Interaction Data Server (IDS) - Voice and Presence (V&P) receives connections from various Call Center Elite Multichannel applications and Media Director. It receives, via these connections, data that allows voice calls to be reported on.
Remoting (for management)			29068	.Net Remoting (for management)	No		
Media Director / Media Stores/ Gateways	Ephemeral	EMC -IDS - Multimedia	29081	TCP	No	Open	Interaction Data Server (IDS) - Multimedia (MM) accepts inbound connections from Media Director as well as various media stores and gateways. It receives, via these connections, data that allows the flow of media tasks to be reported on.
IDS - View			29078/ 29077	IP–Multicast/.Net Remoting (for management)	No		
EMC Desktop/ IDS View Client	Ephemeral	EMC- IDS - View	29083/ 29084	TCP/ IP–Multicast Multicast group address : 239.29.9.67	Yes	Open	Interaction Data Server (IDS) - View is a single point of connection for applications that wish to extract data from the Interaction Data Server - Voice and Presence and Interaction Data Server - Multimedia. Initial connection will be made via the client connection port; however, data that is being consumed via multiple clients may be distributed via the multicast functionality.
			29076	.Net Remoting (for management)	No		
			39076	**Secure .Net Remoting (for management)**	Yes		
EMC - Applications	Ephemeral	EMC - License Director	29095	TCP (.Net Remoting)	No	Open	License Director receives client connections on a single port for licensing.
			29073	.Net Remoting (for management)	No		
			39095	**Secure TCP (.Net Remoting)**	Yes		
EMC – Desktop / Applications	Ephemeral	EMC- Media Director	29087	TCP (.Net Remoting)	No	Open	Media Director accepts .Net Remoting connections from both clients and media stores. The published port number is required for both these connections.
EMC Desktop	Ephemeral	EMC- Media Director	**39087**	**Secure TCP (.Net Remoting)**	Yes		

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
EMC - Desktop	Ephemeral	EMC - Media Proxy (Windows Service)	29079	TCP (.Net Remoting)	No	Open	Media Proxy (Windows Service) runs at the agent desktop to distribute remoting information from the Media Director to the various client applications. Client applications connect to the Media Proxy on the local system through the following port number. This performs the same function as the Media Proxy above but runs as a Windows Service.
			39079	**Secure TCP (.Net Remoting)**	Yes		
EMC - Desktop	Ephemeral	EMC - Preview Contact Media Store	**39098**	**Secure TCP (.Net Remoting)**	Yes	Open	Preview Contact Media Store accepts .Net Remoting connections on a predefined port.
Media Director / Desktops/ Control Panel			29098	TCP (.Net Remoting)	No		
EMC - Short Message Service Gateway	Ephemeral	EMC- Simple Messaging Media Store	29064	TCP (.Net Remoting)	No	Open	Short Message Service Gateway interfaces remote media services to Simple Messaging Media Store. It creates a .Net Remoting channel using a pre-defined port.
EMC – Other Gateways (XMPP)	Ephemeral	EMC- Simple Messaging Media Store	29085	TCP (.Net Remoting)	No	Open	Simple Messaging Media Store accepts connections from Call Center Elite Multichannel gateways.
EMC - Applications	Ephemeral	EMC- Virtual Agent	29056	TCP (.Net Remoting)	No	Open	Virtual Agent accepts .Net Remoting connections on a predefined port.
EMC Desktop	Ephemeral	EMC-Voice Media Store	**39072**	**Secure TCP (.Net Remoting)**	Yes	Open	Voice Media Store accepts .Net Remoting connections on a predefined port.
Media Director/ Desktops/ Control Panel			29072	TCP (.Net Remoting)	No		
EMC - Web Chat Gateway	Ephemeral	EMC- Simple Messaging Media Store	29063	TCP (.Net Remoting)	No	Open	Web Chat Gateway interfaces remote media services to Simple Messaging Media Store. It creates a .Net remoting channel using a pre-defined port.
EMC - Desktop	Ephemeral	EMC- Simple Messaging Media Store	29085	TCP (.Net Remoting)	Yes	Open	Short Message Service Gateway interfaces remote media services to Simple Messaging Media Store. It creates a .Net Remoting channel using a pre-defined port.
Media Director / Desktops/ Control Panel			39085	**Secure TCP (.Net Remoting)**			

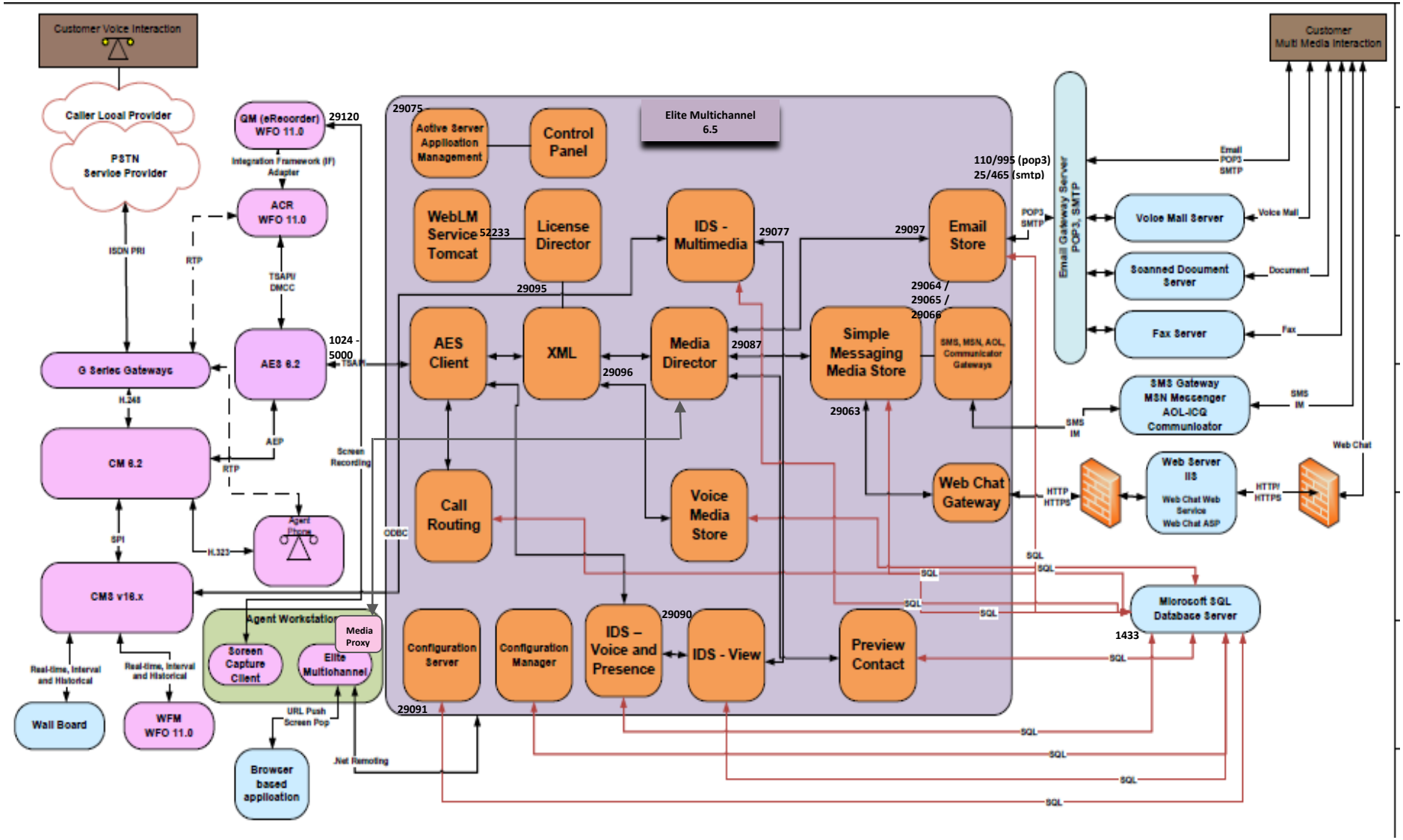
Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
EMC – XML Clients (Desktop / Media Director / Voice Media Store/ Virtual Agent)	Ephemeral	EMC- XML Server	29096	TCP	No	Open	XML Server uses one port. It is assigned to an XML naming service to operate in a similar manner to the current Avaya AES naming service on port 450. Clients will connect to this port to receive a list of real IP Address/Port combinations that can be connected to for service.
			39096	**Secure TCP**	Yes		
			29069	.Net Remoting (for management)	No		
EMC- AES Tsapi Client XML Client (XML Server / IDS V&P / Call Routing Server)	1024-5000	Avaya AES Server	450 (configon AES)	TCP	No	Open	The telephony connections represent a connection to an Avaya AES stream. These will have a single IP Port (XML Client Port) for each Avaya AES Stream and will ideally be taken from the OS free pool on server startup. These port numbers will be dynamic in the 1024-5000 range. Information on the correct (current) port will be provided to the client through the static naming service port. In this manner, the connection in the client can be name based and not rely on a static IP Address/IP Port. Optionally, you can define XML Client Port to a fix value.
EMC- AES DMCC Client XML Client (Desktop / Virtual Agent)	Ephemeral	Avaya AES Server	4721 (configon AES)	TCP	Yes	Open	First party call control
			4722 (configon AES)	Secure TCP	No		
EMC – License Director	Ephemeral	Avaya WebLM Server	52233	TCP/SSL	No	Open	WebLM server accepts remote connections on a SSL port.
EMC - Applications	Ephemeral	Avaya - Experience Portal Management Server	29110	TCP (.Net Remoting)	Yes	Open	The Experience Portal service exposes a .Net Remoting port for management purposes.
EMC - Desktops	Ephemeral	Avaya - Call Recording Config Service	29120	TCP/ .Net Remoting (for management)	No	Open	The Call recording Config Service exposes a .Net Remoting port for management purposes.
			39120	**Secure TCP (.Net Remoting)**	Yes		
EMC– Applications	Ephemeral	EMC - TTrace Server	10400	TCP	Yes	Open	TTrace Server uses a Socket port for the connection of an application to the TTrace server. A second Socket Port is used for the connection of the TTrace

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
EMC-TTrace Console			10401		Yes		Console to TTrace Server and a third port is used for data connection.
EMC - TTrace Data			10403		Yes		
EMC – Applications (Desktop/IDS Server/ Media store)	Ephemeral	MS SQL Server	1433	TCP **Secure TCP**	No	Open	The MS SQL server uses the SQL server port.
EMC – Email Media Store - POP3	Ephemeral	MS Exchange	110	TCP / POP3	No	Open	POP3 connection to retrieve emails.
EMC – Email Media Store – Secure POP3	Ephemeral	MS Exchange	**995**	**TCP / TLS-POP3**	Yes	Open	Secure (TLS) POP3 connection to retrieve emails.
EMC – Email Media Store - IMAP	Ephemeral	MS Exchange	143	TCP / IMAP	No	Open	IMAP connection to retrieve emails.
EMC – Email Media Store – Secure IMAP	Ephemeral	MS Exchange	**993**	**TCP / TLS-IMAP**	Yes	Open	Secure (TLS) IMAP connection to retrieve emails.
EMC – Email Media Store – SMTP	Ephemeral	MS Exchange	25	TCP / SMTP / STARTTLS-SMTP	No	Open	Secure (StartTLS) / Unsecure SMTP connection to send emails.
EMC – Email Media Store – Secure SMTP	Ephemeral	MS Exchange	**465**	**TCP / TLS-SMTP**	Yes	Open	Secure (TLS) SMTP connection to send emails.
EMC CS Portal Client Web Pages	Ephemeral	CSPortal API Server	9609	HTTP **HTTPS**	Yes	Open	The CS Portal Client Javascript pages connect to the CS Portal API server on this port if using the Http protocol.
EMC CS Portal Client Web Pages	Ephemeral	CSPortal API Server	9699	AJP	No	Open	The CS Portal Client Javascript pages connect to the CS Portal API server on this port if using the AJP protocol

Notes

- The ephemeral ports are used on the client side.

3. Port Usage Diagram – with port data where applicable from above list.



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.

Socket Example Diagram

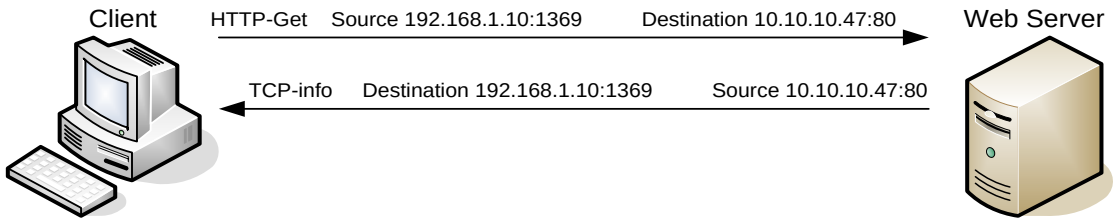


Figure 1. Socket example showing ingress and egress data flows from a PC to a web server

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 the 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.