Avaya Port Matrix

Avaya Workforce Optimization Select 5.2.3

Issue 1.0
September 04, 2019

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. WFOS Components

Data flows and their sockets are owned and directed by an application. Here a server running on Windows OS has many applications, such as Recorder, Media Manager, Avaya Adapter, TAPI Adapter, AES Adapter and Process Checklist. For all applications, sockets are created on the network interfaces on the server.

Component	Interface	Description
Recorder	VOICE NIC DATA NIC	Recorder logs RTP traffic to the file system. It listens on the RTP traffic on the VOICE NIC for this functionality. Recorder exposes management ports on the DATA NIC to communicate with other AWFOS components
Media Manager	DATA NIC	Manages AWFOS media (Encryption, Compression, and Conversion). Exposes management ports on the DATA NIC to communicate with other AWFOS components
CTI Adapters	DATA NIC	Communicate with PBX/ACD systems to receive metadata related to interactions happening on the PBX/ACD systems. Exposes management ports on the DATA NIC to communicate with other AWFOS components
Oceana Adapter	DATA NIC	Communicates with Oceana Breeze UCM REF stream Topics and generates events for Recorder service
Unified Messaging	DATA NIC	Messaging component that integrates with Screen services running on Agent desktop. Exposes management ports on the DATA NIC to communicate with other AWFOS components
Web	DATA NIC	Hosts the web application service for AWFOS system. End users login to this service through the Apache httpd proxy.
SysAdmin	DATA NIC	Hosts the management web interface for the AWFOS system. End users login to this service using HTTP protocol. Exposes an HTTP interface for other AWFOS systems to send Alerts which are in-turn forwarded as SNMP alerts & Emails
Apache	DATA NIC	Apache httpd service, configured in reverse proxy mode with Web application running downstream. Handles SSL offloading for Web application access. Acts as a reverse proxy for all Web socket communication for the Unified Messaging service as well.
Speech Middleware	DATA NIC	Integrates with the Nuance Transcription Engine (NTE) to generate transcripts of the audio recordings made by AWFOS.

Note:

- **DATA NIC**: Network adapter in the system, used by recorder and all other adapters for processing the event messages and telephony signaling.
- **VOICE NIC**: Network adapter in the system, used by recorder service to capture voice packets. This is required for SPAN configuration, to port mirror the RTP packets from network switch.

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: 1 – 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: 1 – 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 or 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 WFOS

Source		**Destination**		**Network / Application Protocol**	**Optionally Enabled / Disabled?**	**Default Port State**	**Description**
System	**Port (Configurable Range)**	**System**	**Port (Configurable Range)**				
Recorder	Ephemeral	CTI Adapter	33012 33029 34301 33013 33022 33014 34101 34102 34103 34105 34106 34107	TCP/HTTP	NO	Open	Recorder connects to adapter to receive CTI events and data
CTI Adapter	Ephemeral	Recorder	33333 33334 33335	TCP/HTTP	NO	Open	CTI adapter connects to recorder to send CTI events and data
Recorder	Ephemeral	Media Manager	33047	TCP/HTTP	No	Open	Post call recording, Recorder Request Media Manger for Encryption
Media Manager	Ephemeral	Recorder	4444 4445 4446	UDP/Proprietary	NO	Open	Media Manager Request Live Streams from Recorder
Recorder	Ephemeral	Unified Messaging	33555	TCP/HTTP	No	Open	Recorder Request UM to start and stop screen captures on agent desktops
Unified Messaging	Ephemeral	Recorder	33024	TCP/HTTP	No	Open	UM notifies the Recorder of agent login on a desktop
CRM Services (Third Party Apps)	Ephemeral	Unified Messaging	33023	TCP/HTTP	No	Open	This is required to receives events from CRM Apps to integrate with WFOS System

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Unified messaging	Ephemeral	Media Manager	33047	TCP/HTTP	No	Open	Unified Messaging Notifies Media Manager of Agent's Desktop Screen Capture availability to move Screen to Voice folder, if encryption is enabled move screens to secure voice folder after encryption
Unified messaging	Ephemeral	Web	80 443	TCP/HTTP(S)	No	Open	Unified messaging pushes images for silent monitor screens to Web App Server
Unified Messaging	Ephemeral	Oceana Services	61617 443 80	TCP/SSL	No	Open	To connect with Breeze Admin REF stream
Oceana Adapter	Ephemeral	Oceana Services	61617 443 80	TCP/SSL	No	Open	To connect with Breeze UCM REF stream
Web	Ephemeral	Oceana Services	443/80	TCP/SSL	No	Open	To authenticate the token with Oceana Portal service
Web	Ephemeral	Media Manager	33025	TCP/HTTP	No	Open	Web Request for Media Preparation for Playback.
Apache	Ephemeral	Speech Middleware	9285, 9590	TCP/HTTP	No	Open	Apache acts as a reverse proxy for Speech Middleware services
Speech Middleware	Ephemeral	MediaManager	33025 34025	TCP/HTTP	No	Open	Speech Middleware Request for media to MediaManager service
Speech Middleware	Ephemeral	Nuance Transcription Engine	8080 443 8443	TCP/SSL	No	Open	Speech Middleware request to Nuance Transcription Engine for audio transcripts
Apache	Ephemeral	Web	9490 9390 34105 33066 9495	TCP/HTTP	No	Open	Apache acts as a reverse proxy for Web application services
Apache	Ephemeral	Analytics	9691 9391	TCP/HTTP	No	Open	Apache acts as a reverse proxy for Analytics application services

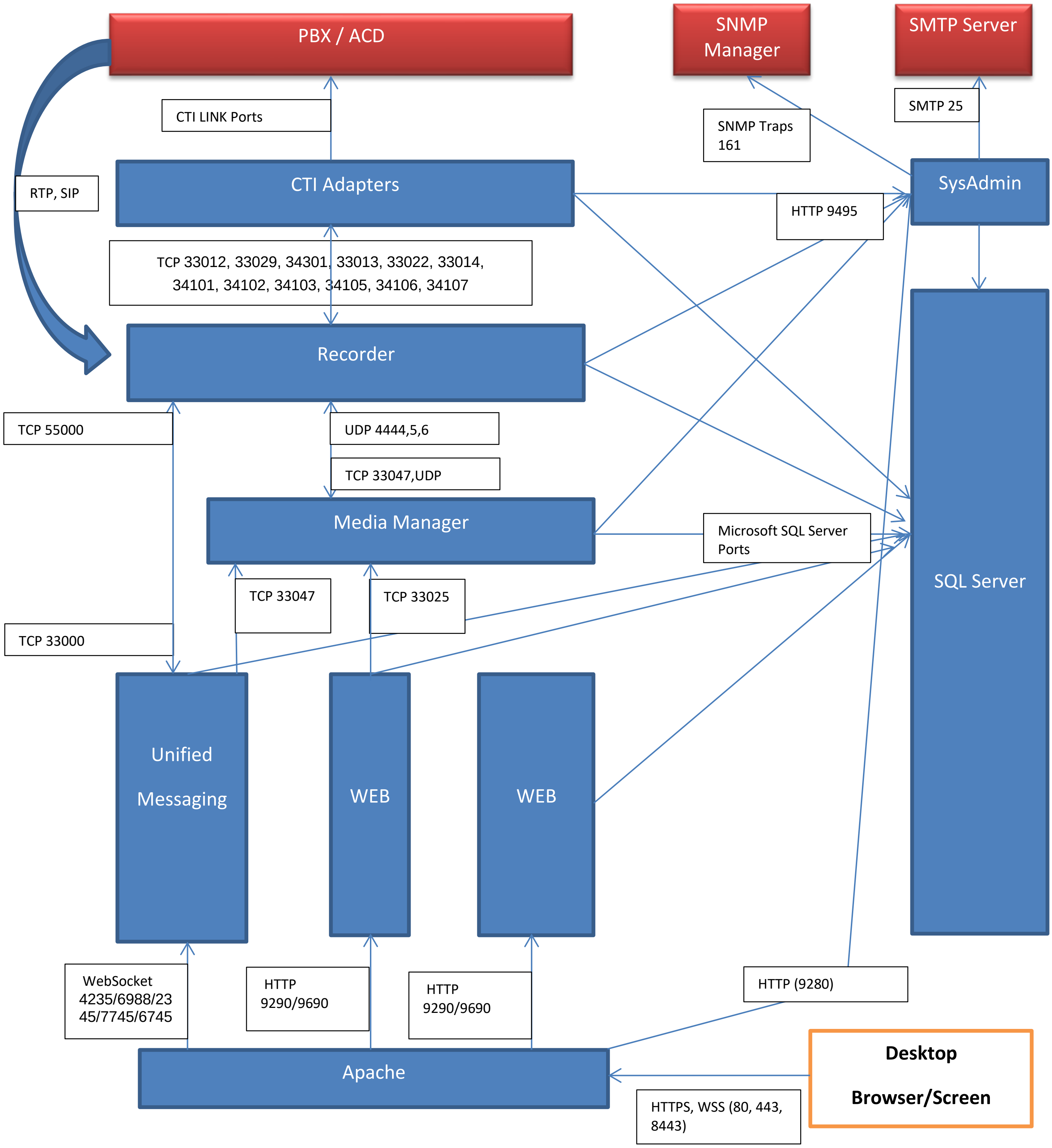
Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Apache	Ephemeral	Unified messaging	4235 6988 2345 7745 6745 33023 33090	WSS/HTTP TCP/HTTP	No	Open	Apache acts as a reverse proxy for Unified Messaging web socket services
Screen Capture App	Ephemeral	Apache	8443,443	WSS/HTTP, HTTPS	No	Open	Screen Capture running on Agent desktops connect to Apache on this port
Browser	Ephemeral	Apache	80 443	HTTP/HTTPS	No	Open	Browsers access AWFOS Application on these ports
Apache	Ephemeral	SysAdmin	9280	HTTP	No	Open	Browsers access SysAdmin Application on these ports to configure Tenant and ICM Components
All Components	Ephemeral	SQL Server	1433	TCP	No	Open	SQL Server port
All Components	Ephemeral	SysAdmin	9495	HTTP	No	Open	To Send alerts generated by all the components
SysAdmin	Ephemeral	NMS Server	161	SNMP	No	Open	SNMP Traps sent to external monitoring system
SysAdmin	Ephemeral	Email server	25	SMTP	No	Open	Email server port
CTI Adapter	Ephemeral	AES Server	450 1050-1065 4721 4722	TCP	No	Open	This is required to connect with AES Server for subscribing events
CTI Adapter	Ephemeral	AACC\ACCS Server	29373	TCP	No	Open	This is required to connect with AACC Server for subscribing events
CTI Adapter	Ephemeral	CS1k Server	3000	TCP	No	Open	This is required to connect with MLS Server for subscribing events
Local MediaManager	Ephemeral	Central MediaManager	33027 33028	TCP	No	Open	This is required to upload the interactions from local storage to central storage using MediaManager Services which are running on local and central servers.
Primary Recorder	Ephemeral	Secondary Recorder	33008	TCP	No	Open	This is required to communicate between recorders in case of Recorder HA is configured
CTI Adapter	Ephemeral	IPO	50797	TCP	No	Open	This is required to connect with IPO Server for subscribing events
CTI Adapter	Ephemeral	IPOCC	18080 18443	TCP	No	Open	This is required to connect with IPOCC Server for subscribing events
CTI Adapter	Ephemeral	PC Server	23201	TCP	No	Open	This is required to connect with PC Server for subscribing events

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
CTI Adapter	Ephemeral	POM Server	7999	TCP	No	Open	This is required to connect with POM Server for subscribing to events
Web	Ephemeral	POM Server	22	TCP	No	Open	This is required to connect with POM Server to copy the POM Reports to web server
SysAdmin	Ephemeral	WebLM Server	52233	TCP	No	Open	This is required by sysadmin service to connect with WebLM Server to get the license details.
SBC/IPOffice	Ephemeral	SIPAdapter	5060	TCP	No	Open	This is required by SIPAdapter to receive SIP Message from SBCE or IPOffice Server
IPOffice/SBCE	Ephemeral	SIPAdapter	16384-32766	UDP	No	Open	This is required to receive the interactions voice traffic from the IPO or SBCE server
Avaya Media Gateway	Ephemeral	AvayaAdapter(DMCC)	16384-32766	UDP	No	Open	This is required to receive the interactions voice traffic from Media Gateway using DMCC API

2.3 Port Table Changes

N/A

3. Port Usage 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. 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.

Socket Example Diagram

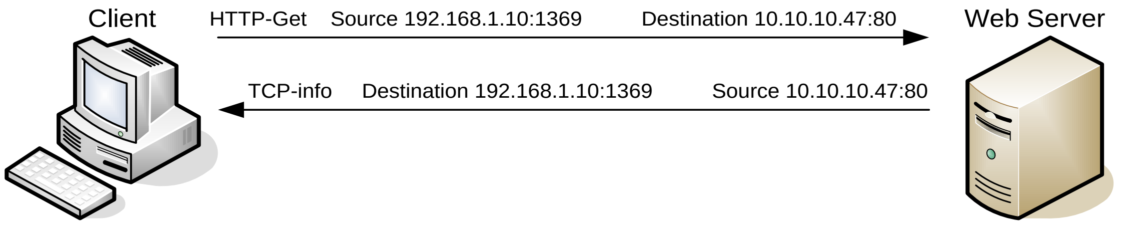


Figure 1. Socket example showing ingress and egress data flows from a PC to a web server

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.