Avaya Port Matrix

Avaya Client SDK 4.x Communication Services Package

Issue 1.2

October, 2020

1. Avaya Client SDK Communication Services Components

The Communication Service Package provides APIs enabling application developers to embed advanced communications functionality in user and business applications and helping create a contextual and seamless user experience. It makes communications easy by abstracting the protocols and complexity out of application developer's hands. The Client SDK provides APIs supporting the following features, including:

- Enterprise Communications
  - Audio and Video calls
  - Messaging
  - Contacts and Presence
  - Desk phone control
  - Call logs
- Rich Conferencing and Avaya Equinox Meetings Online
  - Conference roster
  - Conference management and moderator controls
  - Web Collaboration

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.

Transport/Application Protocol: This is the name associated with the layer-4 protocol higher level application protocols.

Optionally Enabled / Disabled: This field indicates whether customers can enable or disable a layer-4 port by changing its default port state 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.

2.2 Port Tables

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

Table 1. Port for Avaya Client SDK Communication Services Package 4.x

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Communication Services Package	Ephemeral (1024 – 65535)	HTTP servers used to support Avaya Aura Device Services	443	TLS/HTTPS Web Sockets Server-Sent Events	No	Closed	File downloads for AADS
Communication Services Package	Ephemeral (1024 – 65535)	HTTP servers used to support Personal Profile Manager	80	TCP/HTTP	No	Closed	File downloads for PPM (7)
Communication Services Package	Ephemeral (1024 – 65535)	HTTP servers used to support Personal Profile Manager	443	TLS/HTTPS	No	Closed	File downloads for PPM (7)
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Session Manager (SM)	5060 (1024-65535)	TCP/SIP	Yes	Closed	SIP signaling traffic (7)
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Session Manager (SM)	5061 (1024-65535)	TLS/SIPS	Yes	Closed	SIP signaling traffic (7)
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Session Border Controller	3478	TCP/STUN TCP/TURN	No	Closed	STUN/TURN Nat Traversal (5)
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Session Border Controller	5349	TLS/STUN TLS /TURN	No	Closed	STUN/TURN Nat Traversal (5)
Communication Services Package	Default Range is (5004 – 5203) Available Range is	Media Gateway, Conferencing Server, Application Server, Desk Phone, Soft Client, Avaya	1024-65535	UDP/RTP, UDP/RTCP, UDP/SRTP, UDP/SRTCP	No	Closed	Media traffic (audio/video) for SIP calls. The destination port range listed in this document (1024-65535) highlights that the actual destination port for media traffic for any call is dependent on the destination of the call and negotiated in real-time during call setup. It is not possible to provide

	(1024-65535)	Session Border Controller.					the specific list of ports that will be negotiated for all possible call destinations in this document
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Session Border Controller.	443	HTTPS	No	Closed	Media tunneled over HTTPS.
Communication Services Package	Ephemeral (1024 – 65535)	LDAP Server	389	TCP	No	Closed	Enterprise Directory Contact Lookup [(6)]
Communication Services Package	Ephemeral (1024 – 65535)	LDAP Server	636	TLS	No	Closed	Enterprise Directory Contact Lookup [(6)]
Media Gateway, Conferencing Server, Application Server, Desk Phone, Soft Client, Avaya Session Border Controller.	1024-65535	Communication Services Package	Default Range is (5004 – 5203) Available Range is (1024-65535)	UDP/RTP, UDP/RTCP, UDP/SRTP, UDP/SRTCP	No	Closed	Media traffic (audio/video) for SIP calls. The destination port range listed in this document (1024-65535) highlights that the actual destination port for media traffic for any call is dependent on the destination of the call and negotiated in real-time during call setup. It is not possible to provide the specific list of ports that will be negotiated for all possible call destinations in this document
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Multimedia Messaging server	443 (1024-65535)	TLS/HTTPS WebSockets Server-Sent Events	Yes	Closed	Messaging traffic.
Communication Services Package	Ephemeral (1024 – 65535)	DNS Servers	53	UDP/DNS	No	Closed	Domain lookups, service discovery,
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Aura Web Gateway	443	TLS/HTTPS Web Sockets Server-Sent Events	No	Closed	HTTP to SIP Gateway supporting WebRTC [(7)]
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Aura Web Collaboration	80	TCP/HTTP Web Sockets Server-Sent Events	Yes	Closed	Web collaboration

Communication Services Package	Ephemeral (1024 – 65535)	Avaya Aura Web Collaboration	443	TLS/HTTPS Web Sockets	No	Closed	Web collaboration
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Aura Media Server	1024-65535	UDP/RTP, UDP/RTCP, UDP/SRTP, UDP/SRTCP	Yes	Closed	WebRTC Media traffic [5]
Communication Services Package	Ephemeral (1024 – 65535)	Equinox Conferencing Unified Conference Control Avaya Unified Portal Avaya Equinox Meetings Online	443	TLS/HTTPS	No	Closed	Unified Conference Control Server (equinox conferencing) Unified Portal and Equinox Meetings Online interactions.
Communication Services Package	Ephemeral (1024 – 65535)	BFCP Peer	1024 -65503	UDP/BFCP	Yes	Closed	Binary Floor Control Protocol for sharing video. [7]
Communication Services Package	Ephemeral (1024 – 65535)	analytics.google.com	443	TCP/HTTPS	Yes	Closed	Google Analytics
Communication Services Package	Ephemeral (1024 – 65535)	Web Server used to support configuration file.	80	TCP/HTTP	No	Closed	File downloads for Configuration
Communication Services Package	Ephemeral (1024 – 65535)	Web Server used to support configuration file.	443	TLS/HTTPS	No	Closed	File downloads for Configuration
Communication Services Package	Ephemeral (1024 – 65535)	Web Server to support SCEP	80	TCP/HTTP	No	Closed	Simple Certificate Enrollment Protocol for certificate distribution.
Communication Services Package	Ephemeral (1024 – 65535)	Web Server to support SCEP	443	TLS/HTTPS	No	Closed	Simple Certificate Enrollment Protocol for certificate distribution.
Communication Services Package	Ephemeral (1024 – 65535)	Accounts.zang.io	443	TLS/HTTPS	Yes	Closed	Avaya Cloud/Zang account login
Communication Services Package	Ephemeral (1024 – 65535)	Spaces.zang.io	443	TLS/HTTPS	Yes	Closed	Avaya Cloud/Zang Spaces direct messaging.

Communication Services Package	Ephemeral (1024 – 65535)	HTTP Proxy	443	HTTPS	No	Closed	Proxy Configuration usage determined by configuration. Proxy configuration retrieved from Operating System.
Communication Services Package	Ephemeral (1024 – 65535)	HTTP Proxy	80	HTTP	No	Closed	Proxy Configuration usage determined by configuration. Proxy configuration retrieved from Operating System.
Communication Services Package	Ephemeral (1024 – 65535)	IP Office SIP Server	5060 (1024-65535)	TCP/SIP	Yes	Closed	SIP signaling traffic (7)
Communication Services Package	Ephemeral (1024 – 65535)	IP Office SIP Server	5061 (1024-65535)	TLS/SIPS	Yes	Closed	SIP signaling traffic (7)

An **ephemeral port** is a short-lived endpoint that is created by the operating system when a program requests any available user **port**. The operating system selects the **port** number from a predefined range, typically between 1024 and 65535, and releases the **port** after the related TCP connection terminates.

NOTES:

1. Used when encryption is not required.
2. Used for encrypted communication.
3. The SIP signaling port can be configured to use any valid port number in the range 1024-65535.
4. For SIP communications, the alternative transport options are TCP or TLS.
5. Applies to JavaScript platform only
6. Applies to MacOS and Windows platform only
7. Does not apply to JavaScript platform

2.3 Port Table Changes

Table 2. Port Changes From Avaya Client SDK Communication Services Package 3.3

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				

Communication Services Package	Ephemeral (1024 – 65535)	Accounts.zang.io	443	TLS/HTTPS	Yes	Closed	Avaya Cloud/Zang account login
Communication Services Package	Ephemeral (1024 – 65535)	Spaces.zang.io	443	TLS/HTTPS	Yes	Closed	Zang Spaces Direct messaging.
Communication Services Package	Ephemeral (1024 – 65535)	Equinox Conferencing Unified Conference Control Avaya Unified Portal Avaya Equinox Meetings Online	443	TLS/HTTPS	No	Closed	Unified Conference Control Server (equinox conferencing) Unified Portal and Equinox Meetings Online interactions.
Communication Services Package	Ephemeral (1024 – 65535)	HTTP Proxy	443	HTTPS	No	Closed	Proxy Configuration usage determined by configuration. Proxy configuration retrieved from Operating System.
Communication Services Package	Ephemeral (1024 – 65535)	HTTP Proxy	80	HTTP	No	Closed	Proxy Configuration usage determined by configuration. Proxy configuration retrieved from Operating System.
Communication Services Package	Ephemeral (1024 – 65535)	IP Office SIP Server	5060 (1024-65535)	TCP/SIP	Yes	Closed	SIP signaling traffic [8]
Communication Services Package	Ephemeral (1024 – 65535)	IP Office SIP Server	5061 (1024-65535)	TLS/SIPS	Yes	Closed	SIP signaling traffic [8]

Table 3. Port Changes From Avaya Client SDK Communication Services Package 3.2

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Communication Services Package	Ephemeral (1024 – 65535)	Web Server to support configuration file.	443	TLS/HTTPS	No	Closed	File downloads for Configuration

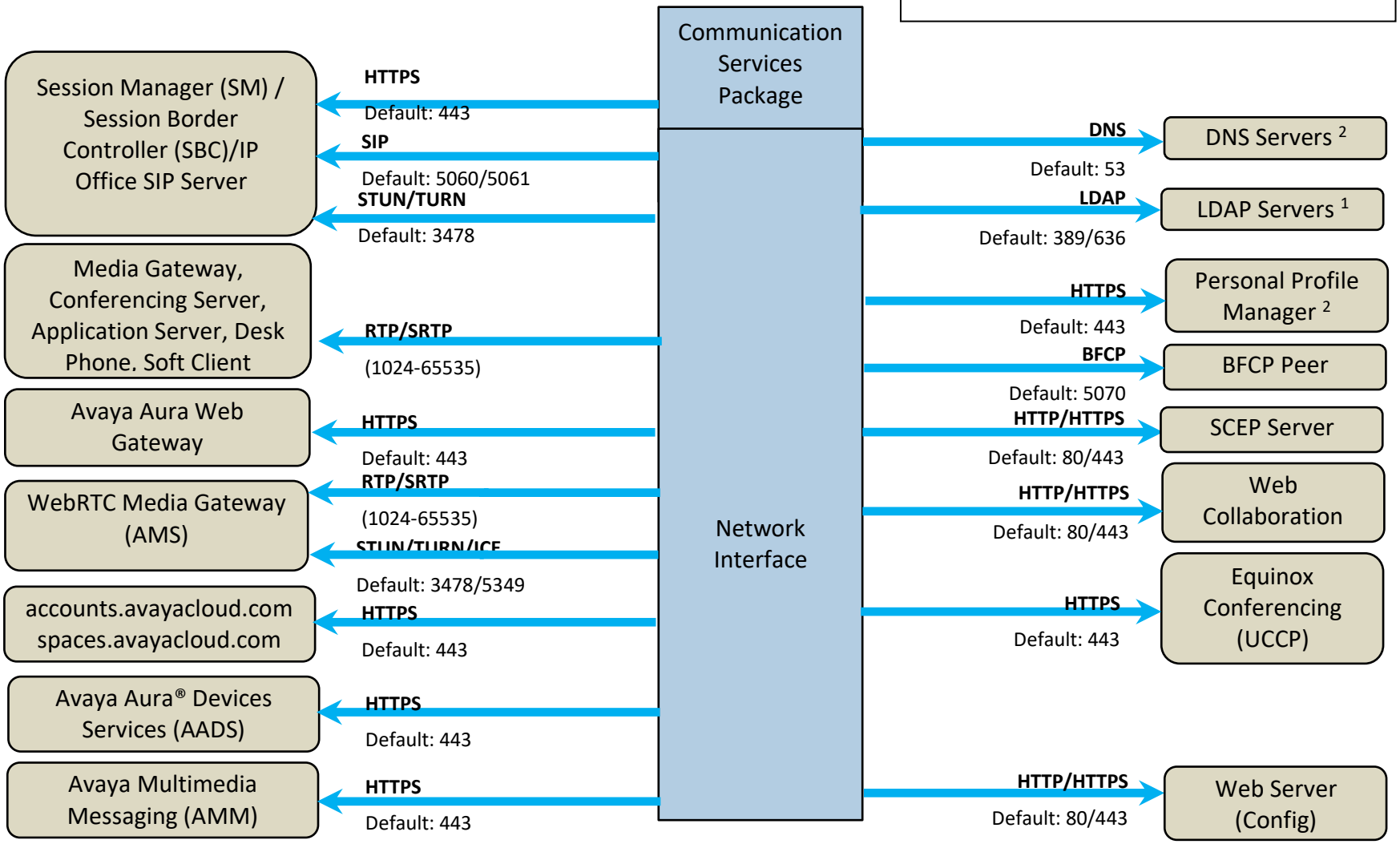
Communication Services Package	Ephemeral (1024 – 65535)	Web Server to support SCEP	443	TLS/HTTPS	No	Closed	Simple Certificate Enrollment Protocol for certificate distribution.
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Session Border Controller.	443	HTTPS	No	Closed	Media tunneled over HTTPS.
Communication Services Package	Ephemeral (1024 – 65535)	Avaya Aura Web Gateway Avaya Unified Portal	443	TLS/HTTPS Web Sockets Server-Sent Events	No	Closed	HTTP to SIP Gateway supporting WebRTC [8]

Table 4. Port Changes From Avaya Client SDK Communication Services Package 4.6

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Communication Services Package	Ephemeral (1024 – 65535)	Accounts.avayacloud.com	443	TLS/HTTPS	Yes	Closed	Avaya Cloud account login
Communication Services Package	Ephemeral (1024 – 65535)	Spaces.avayacloud.com	443	TLS/HTTPS	Yes	Closed	Avaya Cloud Spaces Direct messaging.

3. Port Usage Diagram

1. Applies to MacOS and Windows platform only
2. Does not apply to JavaScript platform



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

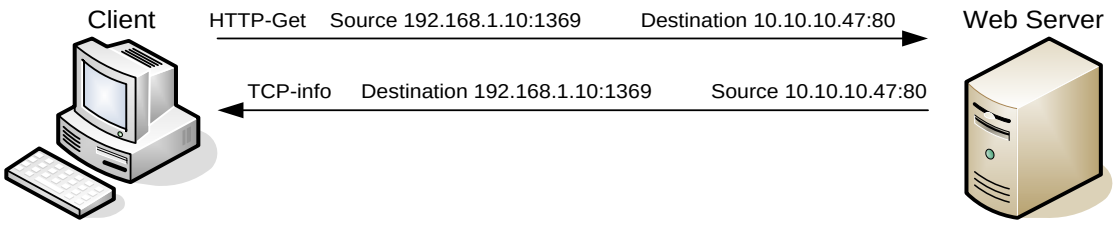


Figure 1. Socket example showing ingress and egress data flows from a PC to a web server

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.

[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.

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.