Avaya Port Matrix:

VSP 9000 4.1

Issue 1.0
September 9, 2015

1. VSP 9000 Components

Table 1. VSP 9000 4.1 Components – SSH Image

No.	Component	Interface name	Description	Notes
1	SSH Server	TCP/SSH Management If	System mgmt requiring shell access	
2	Telnet Server	TCP/TELNET Management If	System mgmt requiring shell access	
3	HTTP Server	TCP/HTTP Management If	System mgmt	
4	SNMP Server	UDP/SNMP Management If	SNMP queries to VSP 9000	
5	HTTPS Server	TCP/HTTPS Management If	System mgmt	
6	BootP/DHCP Relay Server	UDP/DHCP L3 if	BootP/DHCP requests to VSP 9000	

Table 2. VSP 9000 4.1 Components – nonSSH Image

No.	Component	Interface name	Description	Notes
1	Telnet Server	TCP/TELNET Management If	System mgmt requiring shell access	
2	HTTP Server	TCP/HTTP Management If	System mgmt	
3	SNMP Server	UDP/SNMP Management If	SNMP queries to VSP 9000	
6	BootP/DHCP Relay Server	UDP/DHCP L3 if	BootP/DHCP requests to VSP 9000	

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).

2.2 Port Tables

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

Table 1. Ports for VSP 9000 4.1 –SSH Management Interface

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	Closed	Admin terminal	System mgmt requiring shell access	
2	23	TCP/TELNET	Yes	Open	Admin terminal	System mgmt requiring shell access	
3	80 (1024-65535)	TCP/HTTP	Yes	Open	Admin terminal	System mgmt	
4	161	UDP/SNMP	Yes	Closed	Admin terminal or NMS	SNMP queries to VSP 9000	
5	443 (1024-65535)	TCP/HTTPS	Yes	Closed	Admin terminal	System mgmt	
6	67	UDP/DHCP	Yes	Closed	BootP/DHCP Client	BootP/DHCP requests to VSP 9000 to be relayed	1
EGRESS CONNECTIONS							
1	162 (1-65535)	UDP/SNMP	Yes	N/A	NMS	SNMP traps from VSP 9000	2
2	514	UDP/Syslog	Yes	N/A	NMS	Syslog traps from VSP 9000	
3	1812 (1-65534)	UDP/RADIUS	Yes	N/A	RADIUS Server	RADIUS Authentication from VSP 9000	3, 6
4	1813	UDP/RADIUS	Yes	N/A	RADIUS Server	RADIUS Accounting from VSP 9000	6
5	49 (1-65535)	TCP/TACACS+	Yes	N/A	TACACS+ Server	TACACS+ Authentication & Accounting from VSP 9000	4, 6
6	23	TCP/TELNET	No	N/A	TELNET Server	TELNET connections from VSP 9000	
7	22	TCP/SSH	No	N/A	SSH Server	SSH connections from VSP 9000	
8	69	UDP/TFTP	Yes	N/A	TFTP Server	TFTP connections from VSP 9000	
9	22 (1-65535)	TCP/SFTP	Yes	N/A	SFTP Server	SFTP connections from VSP 9000	5
10	123	UDP/SNTP	Yes	N/A	SNTP Server	SNTP connections from VSP 9000	
11	53	UDP/DNS	Yes	N/A	DNS Server	DNS queries from VSP 9000	
12	67	UDP/DHCP	Yes	N/A	DHCP Server	BootP/DHCP requests from VSP 9000	6

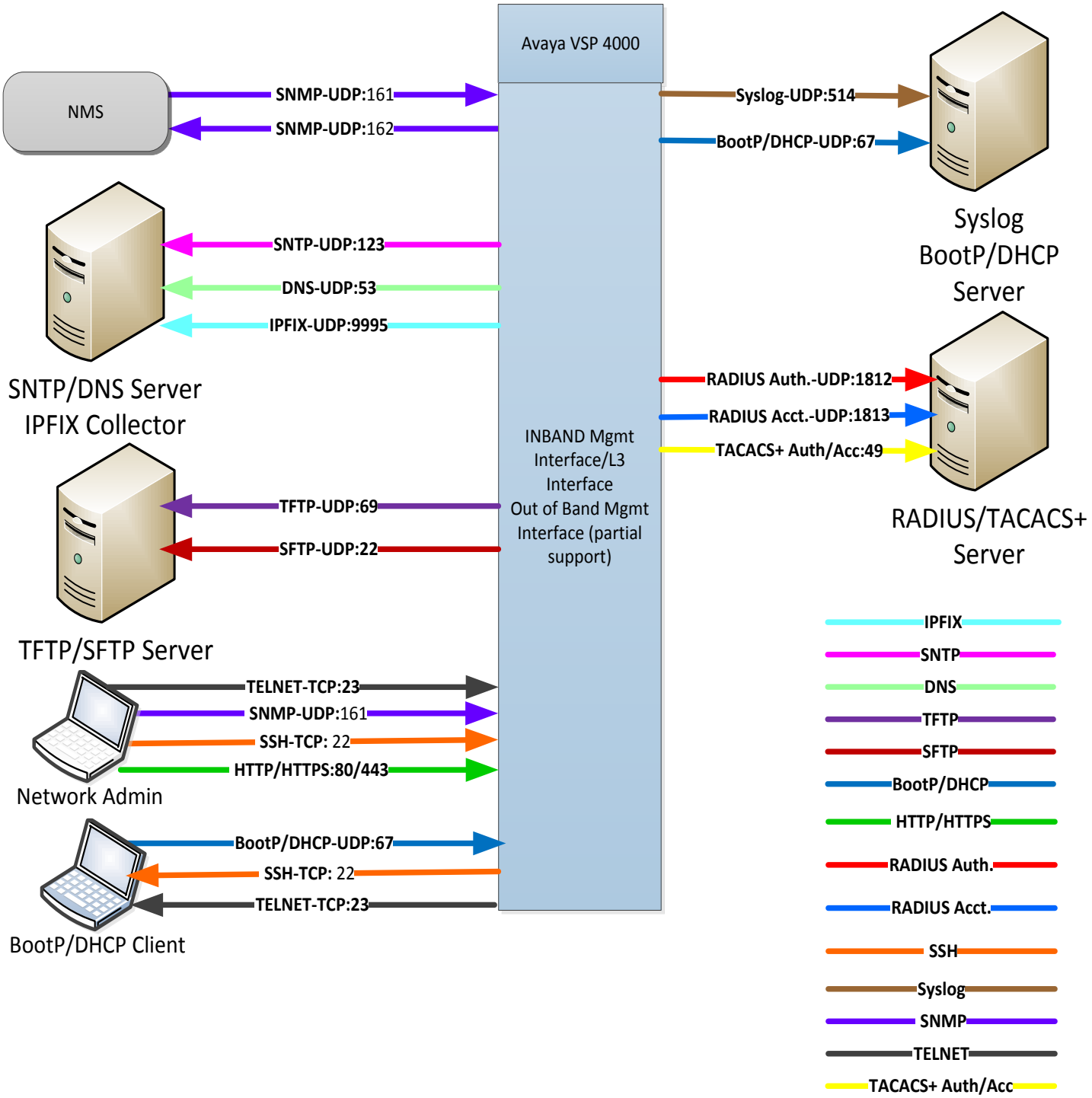
No.	Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
13	9995 (1-65535)	UDP/IPFIX	Yes	N/A	IPFIX Collector	IPFIX Flow exports from VSP 9000	1

Table 2. Ports for VSP 9000 4.1 –nonSSH Management Interface

No.	Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
INGRESS CONNECTIONS							
1	23	TCP/TELNET	Yes	Open	Admin terminal	System mgmt requiring shell access	
2	80 (1024-65535)	TCP/HTTP	Yes	Open	Admin terminal	System mgmt	
3	161	UDP/SNMP	Yes	Open	Admin terminal or NMS	SNMP queries to VSP 9000	
4	67	UDP/DHCP	Yes	Closed	BootP/DHCP Client	BootP/DHCP requests to VSP 9000 to be relayed	1
EGRESS CONNECTIONS							
1	162 (1-65535)	UDP/SNMP	Yes	N/A	NMS	SNMP traps from VSP 9000	2
2	514	UDP/Syslog	Yes	N/A	NMS	Syslog traps from VSP 9000	
3	1812 (1-65534)	UDP/RADIUS	Yes	N/A	RADIUS Server	RADIUS Authentication from VSP 9000	3, 6
4	1813	UDP/RADIUS	Yes	N/A	RADIUS Server	RADIUS Accounting from VSP 9000	6
5	49 (1-65535)	TCP/TACACS+	Yes	N/A	TACACS+ Server	TACACS+ Authentication & Accounting from VSP 9000	4, 6
6	23	TCP/TELNET	No	N/A	TELNET Server	TELNET connections from VSP 9000	
7	69	UDP/TFTP	Yes	N/A	TFTP Server	TFTP connections from VSP 9000	
8	123	UDP/SNTP	Yes	N/A	SNTP Server	SNTP connections from VSP 9000	
9	53	UDP/DNS	Yes	N/A	DNS Server	DNS queries from VSP 9000	
10	67	UDP/DHCP	Yes	N/A	DHCP Server	BootP/DHCP requests from VSP 9000	6
11	9995 (1-65535)	UDP/IPFIX	Yes	N/A	IPFIX Collector	IPFIX Flow exports from VSP 9000	1

NOTES:
1. The SNMP port to which traps are sent is configurable to any valid port number (1-65535), but will usually be port 162.
2. The RADIUS Authentication port to which RADIUS authentication messages are sent is configurable to any valid port number (1-65534), but will usually be port 1812.
3. The TACACS+ Authentication & Accounting port to which TACACS+ authentication & accounting messages are sent is configurable to any valid port number (1-65535), but will usually be port 49.
4. The SFTP port to which SFTP messages are sent is configurable to any valid port number (1-65535), but will usually be port 22.
5. Not supported on Out of Band management interface.

3. Port Usage Diagram



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.

Figure 1, below, is an example showing ingress and egress data flows from a PC to a web server.

Socket Example Diagram

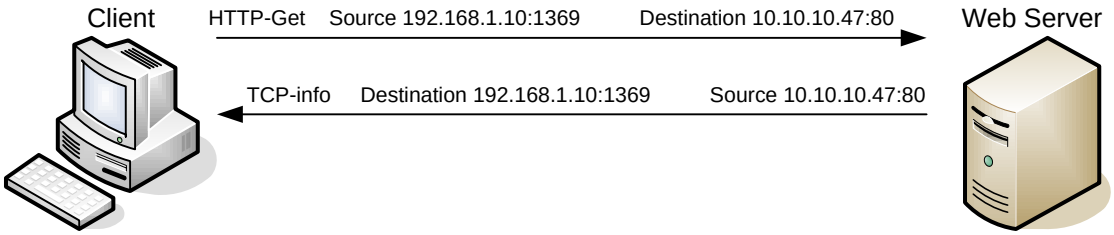


Figure 1. Socket Example

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

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.