Avaya Solutions Platform S8300 R5.1

Port Matrix – S8300

February 2022

Release 5.1

Rev 1.0

© 2022, Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya. "Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation,

Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third-Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third-Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third-Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third-Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD-PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD-PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries

Contents

1 S8300E Interface ports 5
2 Port Usage Table 5
2.1 Port Usage Table Heading Definitions 5
3 S8300E Port Information 6
3.1 Ports for Avaya Solutions Platform S8300E 6
4 VMware ESXi 7.0 Port Information 7
4.1 Incoming Firewall Connection 7
4.2 Outgoing Firewall Connection 10
5 Port Diagram 13

Version Control Table

Version Number	Author	Purpose/Change	Date
Rev 1.0	R&D Engineering Team	Initial revision	February 2022

Avaya – Proprietary

Use pursuant to the terms of your signed agreement or Avaya policy

1 S8300E Interface ports

Data flows and their sockets are owned and directed by an application. 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 Avaya Solutions Platform S8300E are listed as follows.

S8300E Server

Component	Interface	Description
Management	"Management Network" interface / vSwitch0 / Media Gateway LAN ports	The Avaya Solutions Platform S8300 can be managed from an Avaya Aura® System Manager, Solution Deployment Manager Client, or from a PC or laptop with an SSH client through the "Public" interface
Management	"Services" interface / vSwitch1 / Services Port on S8300E faceplate	The Avaya Solutions Platform S8300 can be managed from a Solution Deployment Manager Client or an SSH client on a laptop through the "Services" interface located on the server's front panel.
Guest VM Traffic	Media Gateway LAN ports	Guest Virtual Machines (applications) can be configured to use any of the ports for management and general traffic. Please see the applications' port matrix documents for further details.

2 Port Usage Table

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: 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.

Avaya – Proprietary

Use pursuant to the terms of your signed agreement or Avaya policy

3 S8300E Port Information

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

3.1 Ports for Avaya Solutions Platform S8300E

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	**Port (Configurable Range)**	**System**	**Port (Configurable Range)**				
Client PC	Ephemeral	ASP S8300	22	TCP / SSH	Yes	Open	SSH Server
ASP S8300	Ephemeral	DNS Server	53	UDP / DNS	No	N/A	DNS Client
Client PC	Ephemeral	ASP S8300	80	TCP / HTTP	No	Open	Redirect Web Browser to HTTPS Service (443)
ASP S8300	Ephemeral	NTP Time Server	123	UDP	No	N/A	NTP Client
SMGR, SDM Client	Ephemeral	ASP S8300	443	TCP /HTTPS	No	Open	VI / vSphere Client to ESXi/ESX Host management connection; Embedded Host Web UI
ASP S8300	Ephemeral	Syslog Server	514	UDP	No	N/A	Remote syslog logging
ASP S8300	Ephemeral	Syslog Server	514	TCP	No	N/A	Remote syslog logging
ASP S8300	Ephemeral	Syslog Server	6514	TLS	No	N/A	Remote syslog logging
vSphere Client	Ephemeral	ASP S8300	902	TCP	No	Open	vSphere Client access to virtual machine consoles (MKS). Legacy interface for VM console access. See https://kb.vmware.com/s/article/76672 for more information
CIM Server	Ephemeral	ASP S8300	5988	TCP	No	Open	CIM transactions over HTTP
CIM Secure Server	Ephemeral	ASP S8300	5989	TCP	No	Open	CIM transactions over HTTPS

Avaya – Proprietary

Use pursuant to the terms of your signed agreement or Avaya policy

4 VMware ESXi 7.0 Port Information

The VMware Host Client allow users to open and close firewall ports for each service or to allow traffic from selected IP addresses.

ESXi includes a firewall that is enabled by default. At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services thatare enabled in the host's security profile

NOTE: For further information please reference to the **ESXi 7.0 vSphere Security Guide** and VMware port matrix for vSphere 7

4.1 Incoming Firewall Connection

Table 1

Port	Protocol	Source	Target	Default Port State	Purpose	Classification
9	UDP	vCenter Server	ESXi Host Management Interface	Open	Wake-on-LAN for Dynamic Power Management	Bidirectional
22	TCP	SSH Client – Service Laptop	ESXi Host Management Interface	Open	Required for SSH access - Troubleshooting	Incoming
68	UDP	DHCPv4 Server	ESXi Host Management Interface	Closed	DHCPv4 client - DHCPOFFER, DHCPACK	Incoming
80	TCP	Management Workstations	ESXi Host Management Interface	Open	Redirect requests from HTTP to HTTPS	Incoming
161	UDP	SNMP Manage ment System	ESXi Host Management Interface	Closed	SNMP access for monitoring and management	Incoming
319,320	UDP	Precision Time Protocol Servers	ESXi Host Management Interface	Closed	High resolution timekeeping for ESXi and workloads	Incoming
427	TCP/UDP	Management Workstations	ESXi Host Management Interface	Open	The CIM client uses the Service Location Protocol, version2 (SLPv2) to find CIM servers. CIM/SLP access for monitoring and management	Incoming

Port	Protocol	Source	Target	Default Port State	Purpose	Classification
427	TCP/UDP	Management Workstations	ESXi Host Management Interface	Open	The CIM client uses the Service Location Protocol, version2 (SLPv2) to find CIM servers. CIM/SLP access for monitoring and management	Incoming
443	TCP	Management Workstations	ESXi Host Management Interface	Open	Primary management interface for ESXi, including theVMware Host Client. Primary interface for VM console access, using vSphereClient or VMRC version 11 or later. See https://kb.vmware.com/s/article/76672.	Incoming
546,547	UDP	DHCPv6 Server	ESXi Host Management Interface	Open	DHCPv6 client - DHCPDISCOVER, DHCPREQUEST	Incoming
902	TCP	vCenter Server Managemen t IP Address	ESXi Management IP addresses	Open	Core management communications between vCenterServer and ESXi. Legacy interface for VM console access. See https://kb.vmware.com/s/article/76672for moreinformation.	Incoming
902	TCP	Administrati on Systems Requiring VM Console Access	ESXi Management IP addresses	Open	Legacy interface for VM console access. See https://kb.vmware.com/s/article/76672for moreinformation.	Incoming
902	TCP	Backup Servers	ESXi Management IP addresses	Open	NFC/NBD-based Transfers for Backups	Incoming

Port	Protocol	Source	Target	Default Port State	Purpose	Classification
902	TCP	ESXi Management IP addresses	ESXi Management IP addresses	Open	NFC/NBD-based Transfers for Content Library	Incoming
902	TCP	vCenter Server Management IP address	ESXi Management IP addresses	Open	Core management communications between vCenter Server and ESXi	Incoming
988	TCP	CIM Administra tionSystem	ESXi Management IPaddresses	Closed	CIM/SLP access for monitoring and management	Incoming
5989	TCP	CIM Administra tionSystem	ESXi Management IPaddresses	Closed	CIM/SLP access for monitoring and management	Incoming
5988,8889	TCP	CIM Server 8889-OpenWSMAN Daemon	ESXi Management IPaddresses	Closed	5988-Server for CIM (Common Information Model) 8889-Web Services Management (WS-Management is a DMTF open standard for the management of servers,devices, applications, and Web services	Incoming
8000	TCP	ESXi vMotio n IP addres ses	ESXi vMotion IP addresse s	Open	Required for virtual machine migration with vMotion. ESXi hosts listen on port 8000 for TCP connectionsfrom remote ESXi hosts for vMotion traffic.	Bidirectional
8182	TCP/UDP	ESXi Management IP addresses	ESXi Management IP addresses	Closed	vSphere High Availability Communications	Bidirectional
8100,8200 8300	TCP	ESXi Managemen t IP addresses	ESXi Management IPaddresses	Open	vSphere Fault Tolerance Communications Traffic between hosts for vSphere Fault Tolerance (FT).	Bidirectional
8301 8302	UDP	ESXi Managemen t IP addresses	ESXi Management IPaddresses	Closed	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMwareFT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open.	Bidirectional
9080	TCP	vCenter Server Management IP address	ESXi Management IP addresses	Open	vSphere Replication Communications	Incoming

4.2 Outgoing Firewall Connection

Table 2

Port	Protocol	Source	Target	Default Port State	Purpose	Classification
9	UDP	vCenter Server	ESXi Host Management Interface	N/A Egress Traffic	Wake-on-LAN for Dynamic Power Management	Bidirectional
53	TCP/UDP	ESXi Management IP addresses	DNS Resolvers	N/A Egress Traffic	DNS client	Outgoing
67	UDP	ESXi Management IP addresses	DHCPv4 Server	N/A Egress Traffic	DHCPv4 client - DHCPDISCOVER, DHCPREQUEST	Outgoing
80	TCP	vCenter Server Management IP address	ESXi Management IPaddresses	N/A Egress Traffic	vSphere Lifecycle Manager Communications	Outgoing
88	TCP	Microsoft Active Directory Domain Controllers	ESXi Management Interface	N/A Egress Traffic	Kerberos for IWA	Outgoing
123	UDP	ESXi Management IP addresses	NTP Server	N/A Egress Traffic	NTP for time synchronization	Outgoing
319,320	UDP	ESXi Management IP addresses	Precision Time Protocol Servers	N/A Egress Traffic	High resolution timekeeping for ESXi and workloads	Outgoing
389	TCP/UDP	ESXi Management IPaddresses	Microsoft Active Directory Domain Controllers	N/A Egress Traffic	LDAP for IWA	Outgoing
445	TCP	ESXi Management IPaddress	Microsoft Active Directory Domain Controllers	N/A Egress Traffic	SMB for IWA	Outgoing
464	TCP/UDP	ESXi Management IPaddress	Microsoft Active Directory Domain Controllers	N/A Egress Traffic	Kerberos password change for IWA	Outgoing
514	TCP/UDP	ESXi Management IP addresses	Syslog Server	N/A Egress Traffic	Remote logging using syslog	Outgoing

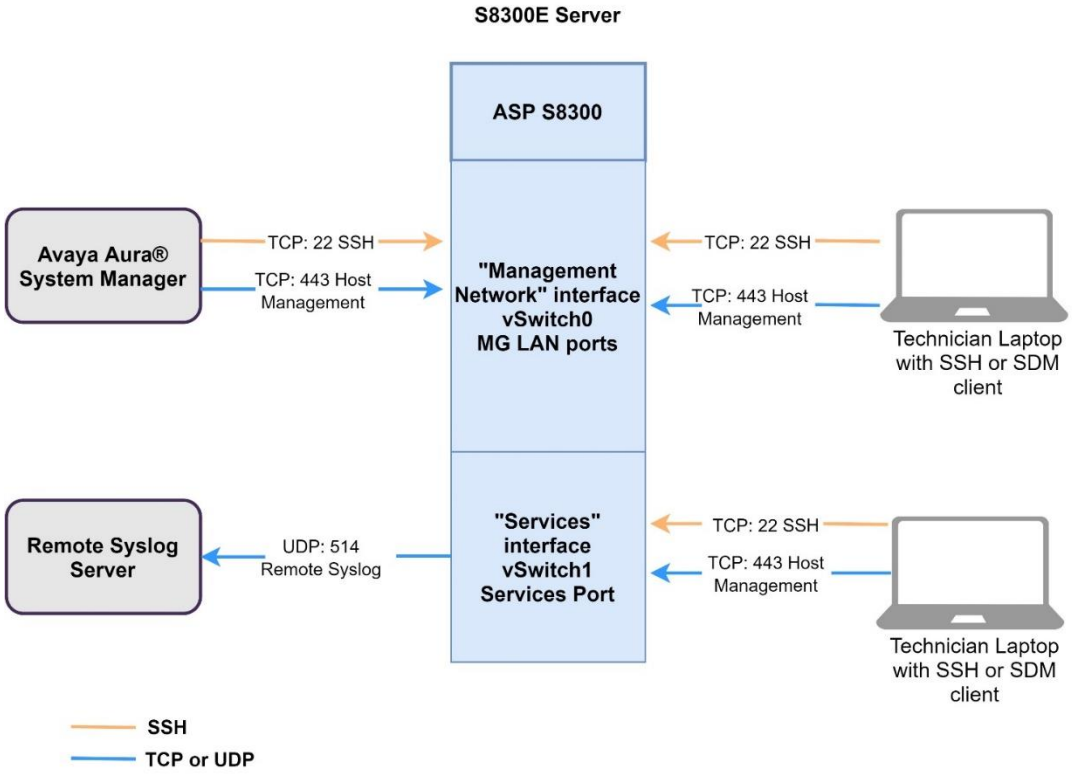
Avaya – Proprietary
Use pursuant to the terms of your signed agreement or Avaya policy

Port	Protocol	Source	Target	Default Port State	Purpose	Classification
636	TCP	ESXi iSCSI IP addresses	Microsoft Active Directory Domain Controllers	N/A Egress Traffic	LDAPS for IWA	Outgoing
902	TCP	ESXi Management IP addresses	ESXi Management IP addresses	N/A Egress Traffic	NFC/NBD-based Transfers for Content Library	Bidirectional
902	TCP	ESXi iSCSI IP addresses	Backup Servers	N/A Egress Traffic	NFC/NBD-based Transfers for Backups	Outgoing
3260	TCP	ESXi iSCSI IP addresses	iSCSI Storage Server	N/A Egress Traffic	Core storage iSCSI Client / Supports software iSCSI	Outgoing
3268,3269	TCP	ESXi Management IPaddresses	Microsoft Active Directory Domain Controllers	N/A Egress Traffic	LDAP GC interface for IWA	Outgoing
8000	TCP	ESXi vMotion IP addresses	ESXi vMotion IP addresses	N/A Egress Traffic	Required for virtual machine migration with vMotion. ESXi hosts listen on port 8000 for TCP connections from remote ESXi hosts for vMotion traffic.	Bidirectional
8182	TCP/UDP	ESXi Management IP addresses	ESXi Management IP addresses	N/A Egress Traffic	vSphere High Availability Communications	Bidirectional
8100,8200 8300	TCP	ESXi Management IP addresses	ESXi Management IP addresses	N/A Egress Traffic	vSphere Fault Tolerance Communications	Bidirectional
8301 8302	UDP	ESXi Management IPaddresses	ESXi Management IP addresses	N/A Egress Traffic	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open.	Bidirectional

9080	TCP	vCenter Server Management IP Address	ESXi Management IP addresses	N/A Egress Traffic	vSphere Replication Communications	Outgoing

5 Port Diagram

Note: Limited TCP/UDP ports have been listed in this diagram. For a complete list of ports, refer to tables in section 3 and 4 of this document



Use pursuant to the terms of your signed agreement or Avaya policy