Port Security for the Equinox Conferencing 9.x Solution

Release 9.0
Issue 1
January 2017

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. 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 Designated Processor that hosts 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 type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the

Software only on a number of Designated Processors up to the number indicated in the order. 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.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

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. Note that 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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

Introduction

This document provides the information you need to know to implement port security, including details of TCP/IP/UDP ports used throughout the Equinox Solution, organized by product name.

Unless a client program explicitly requests a specific port number for a TCP or UPD socket connection, the source port number used is an ephemeral port number.

Ephemeral ports are temporary ports assigned by the client machine's IP stack, and are assigned from a designated range of ports for this purpose. When the connection terminates, the ephemeral port is available for reuse, although most IP stacks will not reuse that port number until the entire pool of ephemeral ports have been used. So, if the client program reconnects, it will be assigned a different ephemeral port number for its side of the new connection.

Similarly, for UDP/IP, when a datagram is sent by a client from an unbound port number, an ephemeral port number is assigned automatically so the receiving end can reply to the sender.

The range of ephemeral ports depends on the client machine's IP stack, and can configured only in some operating systems (OS).

To determine which ports you should open to enable optimal product functionality, see the port entries for the specific product. The various components of the Equinox Solution can be combined to fit the existing network topology and the video requirements of the organization. For more information, see the Deployments of the Equinox Solution section of the Equinox Solution Guide.

Each port entry includes the following information:

- Port Range: Specifies the TCP/IP/UDP port/port range.
- Protocol: Specifies the protocol used by the port/port range.
- Destination: Specifies the recipient (client or server) of the traffic.
- Required: Specifies whether opening this port/port range is mandatory, recommended, or optional, relative to the standard usage of the Equinox Solution product. To obtain the functionality described for a particular port/port range, it is mandatory to open the particular port/port range.

Equinox Management ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Administrator Management Client	Ephemeral TCP ports	Equinox Management	TCP 80 (HTTP) TCP 8080 (HTTP) TCP 443 (HTTPS) TCP 9443 (HTTPS)	Enables administrator web client to access Equinox Management administrative web portal	Mandatory
XML Secure Clients	Ephemeral TCP Ports	Equinox Management	TCP 3336/3346 (XML over TLS)	Enables secure XML connection from secure clients	Mandatory for any XML secure clients
Equinox Management	TCP 7 (Management) TCP 32768-61000	Elite MCU	TCP 7 (management) TCP 1720 (RAS) UDP 1719 (RAS) TCP (H.245) 1024-1324 TCP (XML) 3336, 3338 TCP (XML over TLS) 3346, 3348	Management, registration, managing meetings via Equinox Management	Mandatory
	TCP (HTTPS) Ephemeral ports	Avaya Equinox Streaming and Recording (AESR) Manager	TCP (HTTPS) 443	Management communication (REST)	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Equinox Management	TCP (H.245) 32768-61000	H.323 Terminals	Consult the vendor documentation to confirm ports used.	Call setup, Signaling, Management	Mandatory
	TCP 5060 TCP TLS 5061	SIP terminals	TCP 5060 TCP TLS 5061 BFCP 5070. 5077	SIP call setup, signaling and management	Mandatory
	UDP 1719 (RAS) TCP 1720 (RAS) TCP 32768-61000 (H.245) Ephemeral ports	H.323 Edge	TCP 7 (management) UDP 1719 (RAS) TCP 1720 (RAS) UDP 53 (URI dialing/DNS) TCP 12000-15000*** TCP 8089 XML API	H.323 Edge Call setup and registration	Mandatory *** Default TCP port range - configurable via the H.323 Edge Server web interface
	TCP 7 (Management) TCP 32768-61000	Scopia Desktop Server	TCP 7 (management) UDP 161 (SNMP traps) TCP 3340 Equinox Management Meeting Control	Scopia Desktop Call Setup and Management	Mandatory *Default TCP Port range for Windows Server 2008 R2 or higher.

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Equinox Management			TCP 49152-65535* (H.245)		
	TCP 32768-61000	DNS Server LDAP Server Active Directory Email Server	DNS Server UDP 53 LDAP server 389 LDAP over SSL 636 AD Server TCP/UDP 445 NTLM SSO TCP 25 SMTP	DNS Name Resolution LDAP Integration LDAP over SSL Single Sign-On (SSO) Email Server Integration	Mandatory
	Ephemeral TCP ports	Sony PCS Address Book, MCM, Endpoints	TCP 23 (Telnet)	Enables use of Sony PCS Address Book	Recommended if Sony endpoints are deployed
	TCP 32768-61000	Scopia Video Gateway, Equinox TIP Gateway, Scopia SIP Gateway	TCP 3336 (XML)	Enables communication between Equinox Manager and Scopia Video, SIP and TIP Gateways	Mandatory if deployed with Scopia Video, SIP and/or TIP Gateways
	TCP 32768-61000	IBM Domino Server	TCP 63148 (DIIOP)	Enables connection with IBM Domino Server	Mandatory if deployed with Domino Server
	Ephemeral TCP ports	IBM SameTime	TCP 3341	Cannot communication with SameTime Server	Mandatory if deployed with SameTime Server

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Equinox Management	TCP 7 (management) UDP 162 (SNMP traps) TCP 32768-61000	Equinox Media Server / MCU	TCP 7 (management) TCP 1720 (RAS) (from / to ECS) UDP 1719 (RAS) (from / to ECS) TCP 1024-1324 (H.245) (from / to ECS) TCP 3336, 3338 (XML) TCP 3346, 3348 (XML over TLS) TCP 8080, 9443 TCP 80, 443	Management, registration, SNMP traps, managing meetings via Equinox Management. Enables receiving alarms from Web Collaboration Server	Mandatory
	TCP 5556, 8095, 8445 TCP 32768-61000	Equinox Media server / Web Collaboration Server WCS (with 6000)	TCP 7 (management) TCP 1720 (RAS) (from / to ECS) UDP 1719 (RAS) (from / to ECS) TCP 1024-1324 (H.245) (from / to ECS) TCP 3336, 3338, 3346, 3348 TCP 8080, 9443 TCP 80, 443	Management, registration, SNMP traps, managing meetings via Equinox Management. Enables receiving alarms from Web Collaboration Server	Mandatory when Web Collaboration Server is deployed

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Equinox Management	TCP 32768-61000	Equinox Media Server, Platform Manager (PMGR).	TCP 3358 (XML) TLS 3368 (XML) TCP 8095 TCP 8445	Administration & Control Internal File Transfer Upgrades Logs	PMGR is an internal component which manages the local platform and is controlled by Equinox Management. These ports are required for distributed servers on remote branches.
	TCP/UDP 5060 TLS 5061 TCP 32768-61000	Equinox Media Server AMS +WCS	TCP/UDP 5060 TLS 5061 TCP 7150 TLS 7151 TCP 7410 TLS 7411 TCP 8080, 9443 TCP 80, 443	SIP Signaling Web Admin GUI SOAP Management Server	
	TCP/UDP 5060 TLS 5061 TCP 32768-61000	Equinox Media Server / WebRTC Gateway (with 6000)	TCP/UDP 5060 TLS 5061 TCP 7150 TLS 7151 TCP 7410 TLS 7411	SIP Signaling Web Admin GUI SOAP Management Server	
	TCP 32768-61000	Web Gateway	TCP 3343 TLS 3353 SNMP UDP 161	Administration Control	
	TCP 32768-61000	Unified Portal	TCP 3341 TLS 3351	Administration Control	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Equinox Management			HTTPS 8446		
	TCP 32768-61000	Avaya AADS	TCP 3344 TLS 3354	Administration Control	
	TCP 32768-61000	Avaya SBCE	HTTP 80 HTTPS 443	Monitoring	
	TCP 32768-61000	DNS Server NTP Server	DNS 53 (UDP) NTP 123 (UDP)	DNS NTP	
	TCP 32768-61000	XT Series with no support for Cloud Provisioning	TCP 55099 (XT Software Upgrade) TCP 55003 (XT AT Commands)	Management of XT Series where Cloud Provisioning is not supported or disabled	Mandatory if managing XT Series 8.3.x or disabling XT Provisioning

Equinox Media Server Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Administrative Client	Ephemeral TCP Ports	Always blocked	TCP 8085 (HTTP) TCP 8445 (HTTPS - HTTP over SSL) TCP 21 (FTP) TCP 22 (SSH)	MCU web interface MCU web interface when using HTTPS Audio stream recording CLI Real-time access to MCU logs	Optional. If blocked, access to the MCU web interface; SSH and FTP access will not be possible.
Equinox Media Server/MCU with WCS /WCS only (for 6000)					
		H.323 Edge	UDP 12000-15000** Audio and Video media	Audio and Video Media from Elite MCU to H.323 Edge Server * Default ports used by H.323 Edge Server, can be modified. Configuring Ports on the H.323 Edge server	Mandatory for audio and video
		Elite 6000 MCU /Media server MCU (Cascade)	TCP 1024-1324 (H.245) UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	Audio and Video Media between cascaded Media server & Elite MCUs	Mandatory for audio and video
		Scopia Desktop Server	TCP 49152-65535(H.245) UDP 10000-65535 ** Default range	Scopia Desktop audio/video session with Equinox Media Server ** Default ports used by Scopia Desktop Server - configurable	Mandatory for media between Scopia Desktop Server and Equinox Media Server

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Equinox Media Server/MCU with WCS /WCS only (for 6000)		Equinox Streaming & Recording Server (CP)	UDP 4100-5000	RTP Audio, Video, Presentation Values can be changed in CP admin GUI (range is 1025 – 65535)	Mandatory when using AESR
		ISDN Video Gateway	TCP 1024-4999 TCP 1820 (Q931) UDP 7222-7422 UDP 7622-7822 UDP 12002-12952	H.245 signaling IVR Audio RTP (even numbered ports) and RTCP (odd numbered ports) IVR Video RTP (even numbered ports) and RTCP (odd numbered ports) Audio and Video Media (RTP - even numbered ports; RTCP - odd numbered ports)	Mandatory for media between ISDN Video Gateway and Equinox Media Server
	SIP PROTOCOL TCP/UDP 5060 (SIP signaling) TCP 5061 (SIP Signaling using TLS) TCP 3400-3580 (BFCP) UDP 12000-13200 (Video RTP) UDP 16384-16984	SIP Terminals	Endpoint TCP and UDP Ports	Audio and video media, RTCP	Mandatory for SIP calls
		Web Collaboration Server	TCP/UDP 5060 (SIP signaling) TCP 5061 (SIP TLS) TCP/UDP 3400-3580 (BFCP) UDP 12000-13599 (RTP Media)	RTP Audio/Video/Presentation	Mandatory when using WCS

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Equinox Media Server/MCU with WCS /WCS only (for 6000)	(Audio RTP)	Elite MCU Media server AMS	TCP 3400-3580 (BFCP - TCP) UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	Audio and Video Media between cascaded Equinox Media Servers for SIP calls	Mandatory for media between cascaded Equinox Media Servers
	TCP 1024-1324 (H.245) TCP 3336 3338 (XML APIs) TCP/UDP 5060 (SIP Signaling) TCP 5061 (SIP Signaling using TLS)	Equinox Management	TCP 7 (management) TCP 32768-61000 (H.245)		Mandatory for MCUs managed by Equinox Management
	TCP 1024-1324 (H.245) UDP 1719 (RAS) TCP 1720 (Q931)	ECS or H.323 Gatekeeper	UDP 1719 (RAS) TCP 1720 (Q931) TCP 32768-61000	Registration, Admission, Session Control, Q931 signaling	Mandatory for H.323 Calls
	TCP 32768-61000	DNS Server NTP Server	DNS 53 (UDP) NTP 123 (UDP)	DNS NTP	Optional
	Media Server/AMS - UDP Port range 6000 - 17999	Client or another media server	SIP: TCP/UDP 5060 SIP: TLS 5061 TCP 7150 TLS 7151 UDP port range depends	Administrator Web Interface SOAP Management Server	This is for audio media

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Equinox Media Server/MCU with WCS /WCS only (for 6000)			on client		
	Media Server/MCU - UDP Port range UDP 16384-16784 (Audio RTP) UDP 12000-13200 (Video RTP)	Client or another media server	SIP: TCP/UDP 5060 SIP: TLS 5061 TCP 3336, 3338 (XML) TCP 3346, 3348 (XML over TLS) UDP port range depends on client	XML Admin Management Server	This is for audio and video media
	Media Server/WebRTC Gateway - UDP Port range 6000 - 17999	Elite 6000	UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)		
	UDP 3478 for STUN/TURN	Avaya SBCE	UDP 3478	Monitoring	

Elite MCU Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Elite MCU	H.323 PROTOCOL TCP 1024-1324 (H.245) TCP 3337 (XML to Elite MCU)	H.323 Terminals	*Refer to Manufacturer's documentation for TCP and UDP ports used	Audio and video media, RTCP	Mandatory for audio and video

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Elite MCU	UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	H.323 Edge	UDP 12000-15000* Audio and Video media	Audio and Video Media from Elite MCU to H.323 Edge Server * Default ports used by H.323 Edge Server, can be modified.	Mandatory for audio and video
		Elite MCU (Cascade)	UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP) TCP 1024-1324 , 3337	Audio and Video Media between cascaded Elite MCUs	Mandatory for audio and video between two cascaded MCUs
		Scopia Desktop Server	UDP 10000-65535 ** Default range	Scopia Desktop audio/video session with Elite MCU ** Default ports used by Scopia Desktop Server -	Mandatory for media between Scopia Desktop Server and Elite MCUs
		Equinox Streaming & Recording Server (CP)	TCP 9090-9999 UDP 4100-5000	RTP Audio and video	Mandatory when using AESR
		ISDN Video Gateway	TCP 1024-4999 TCP 1820 (Q931) UDP 7222-7422 UDP 7622-7822 UDP 12002-12952	H.245 signaling IVR Audio RTP (even numbered ports) and RTCP (odd numbered ports) IVR Video RTP (even numbered ports) and RTCP (odd numbered ports) Audio and Video Media (RTP - even numbered ports; RTCP - odd numbered ports)	Mandatory for media between ISDN Video Gateway and Elite MCU

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Elite MCU	SIP PROTOCOL TCP/UDP 5060 (SIP signaling) TCP 5061 (SIP Signaling using TLS) TCP 3400-3580 (BFCP) UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	SIP Terminals	* Refer to Manufacturer's documentation for TCP and UDP ports used	Audio and video media, RTCP, BFCP	Mandatory for SIP calls
		Web Collaboration Server	TCP/UDP 5060 (SIP signaling) TCP 5061 (SIP TLS) TCP/UDP 3400-3580 (SIP BFCP) UDP 12000-13599 (RTP Media)	Audio and video media, RTCP, BFCP	Mandatory when using WCS
		Elite MCU (Cascade)	TCP 3400-3580 (BFCP - TCP) UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	Audio and Video Media between cascaded Elite MCUs for SIP calls	Mandatory for SIP Signaling and media
	TCP 1024-1324 (H.245) TCP 3336-3338 (XML APIs) TCP/UDP 5060 (SIP Signaling) TCP 5061 (SIP Signaling using TLS)	Equinox Management/ B2BUA	TCP 7 (management) TCP *Default Linux Ports (H.245)	Default Linux TCP port range is 32768- 61000 which can be modified.	Mandatory for MCUs managed by Equinox Management

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Mandatory
Elite MCU	TCP 1024-1324 UDP 1719 (RAS) TCP 1720 (Q931)	ECS Gatekeeper	UDP 1719 (RAS) TCP 1720 (Q931) Default Linux TCP port range is 32768- 61000 which can be modified.	Registration, Admission, Session Control, Q931 signaling	Mandatory for H.323 Calls
	TCP 1024-1324	Always blocked	TCP 8085 (HTTP) TCP 8445 (HTTPS - HTTP over SSL) TCP 21 (FTP) TCP 22 (SSH)	MCU web interface MCU web interface when using HTTPS Audio stream recording Real-time access to MCU logs	Optional. If blocked, access to the MCU web interface; SSH and FTP access will not be possible.
	TCP 1024-1324	DNS	TCP 53	DNS name resolution	Optional

Scopia Desktop Server Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Scopia Desktop Client	Ephemeral TCP Ports Ephemeral UDP Ports	Scopia Desktop Server	TCP 443 (HTTP over SSL) TCP 80 (HTTP) TCP 49152-65535* UDP 10000-65535 **	Enables access to Scopia Desktop Web Portal Enables audio and video media	Mandatory *Default TCP Port range for Windows Server 2008 R2 or higher. ** Default UDP port range which is configurable.
Scopia Desktop Server	TCP 49152-65535* UDP 10000-65535 **	Elite MCU/ Media Server (MCU)	UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	Scopia Desktop Audio and Video mediaTo Elite MCU	Mandatory *Default TCP Port range for Windows Server 2008 R2 or higher. ** Default UDP port range which is configurable.
	TCP 49152-65535*	Equinox Management	TCP 32768 - 61000 TCP 3340 Equinox Management Meeting Control UDP 161-162 SNMP	Scopia Desktop Registration, Call setup, Cascades to Elite MCU	Mandatory *Default TCP Port range for Windows Server 2008 R2 or higher.
	UDP 1719 (RAS) TCP 1720 (Q931) TCP 49152-65535*	ECS Gatekeeper	UDP 1719 (RAS) TCP 1720 (Q931) TCP 49152-65535* (H245)	Registration, Admission, Call Control	Mandatory *Default TCP Port range for Windows Server 2008 R2 or higher.
	Ephemeral TCP/UDP Ports	Active Directory	UDP 137-128 TCP 139. 445	Auto-discovery and authentication	Recommended for Active Directory Authentication
	UDP 6972-65553	Streaming Server		Cannot connect to the Desktop Streaming Server when separated by a Firewall	Recommendation is to place the Desktop Server and Streaming Server in the same zone

H.323 Edge Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
H.323 Edge Client	Ephemeral Ports	H.323 Edge	TCP/UDP 3089	Required for H.323 Edge Client to Register with H.323 Edge Server	Mandatory when using H.323 Edge Client
Management PC	Ephemeral TCP ports	H.323 Edge	TCP 22 (SSH access)	Access to the H.323 Edge Server via SSH.	Mandatory. If blocked, SSH to the H.323 Edge will be unavailable.
Any External H.323 Devices	All TCP/UDP traffic	H.323 Edge	UDP1719,TCP1720, TCP/UDP 2776-2777(H.460 Signaling & Media), TCP/UDP 4000-5000(DPA Signaling & Media)	H.323 traffic from H.323 devices in public network inbound to H.323 Edge public interface.	Mandatory for signaling and media between external devices and H.323 Edge server.
H.323 Edge	UDP 1719 TCP 1720 TCP/UDP 2776-2777 (H.460 Signaling & Media) TCP/UDP 4000-5000 (DPA Signaling & Media)	Any External H.323 Devices	All TCP/UDP traffic allowed	Any traffic from H.323 Edge public interface outbound to public network (inbound traffic is restricted as described in the above row.)	Mandatory for media and signaling between external devices and H.323 Edge Server.
	TCP/UDP 12000 - 15000	Elite MCUs/ Media Server (MCU)	UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP) TCP 1024-1324	H.323 Edge Media to MCU and H.323 terminals All H.225 and H.245 traffic will be directed to	Mandatory for media and signaling between internal H.323 devices and the H.323 Edge

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
		Internal H.323 Devices	Refer to Manufacturer's documentation for TCP and UDP ports.	Gatekeeper	Server
	UDP 1719 (RAS) TCP 12000 – 15000	Equinox Management with ECS Gatekeeper	UDP 1719 (RAS) TCP 1720 (Q931) Default Linux TCP port range is 32768- 61000 which can be modified.	Registration of H.323 Edge and proxy registrations of external devices * Default Linux TCP Ports 32768-61000 Default Windows TCP ports 49152-61000	Mandatory for H.323 calls
	TCP 32768-61000*	DNS Server	TCP/UDP 53	Required for H.323 URI Dialing	Mandatory for H.323 URI Dialing

ASBCE Edge Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
XT EP , Equinox 3.x client or Any External SIP client	Ephemeral Ports	ASBCE Edge	TCP 5061, 5060 TCP/UDP	Required for external SIP connectivity	Mandatory when using SIP End point
XT EP , Equinox 3.x client or Any External SIP client	Ephemeral Ports	ASBCE Edge	UDP port Range 35000 - 40000 (configurable)	Required for external SIP connectivity – media	Mandatory when using SIP client
Web meet me (webRTC) / Equinox client 3.x / XT (for web collaboration) / Client access to the Unified Portal	Ephemeral Ports	ASBCE Edge	TCP 443 TCP 8443	Required for Unified Portal, web meet me (webRTC) signaling and web collaboration server	Mandatory for external http https Client access to the Unified Portal (includes scheduling, participating, and accessing recordings)
Web meet me (webRTC)	Ephemeral Ports	ASBCE Edge	UDP 3478 UDP port Range 50000 - 55000 (configurable)	Required for external web meet me connectivity – media	Mandatory when using web meet me client

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
ASBCE Edge	Ephemeral Ports	Management (Unified Portal/ web GW) or web gateway	TCP 443 TCP 8443	Required for Unified Portal, web meet me (webRTC) signaling	Mandatory when using web meet me client
ASBCE Edge	Ephemeral Ports	Media server / WCS only	TCP 443	Required for Unified Portal, web meet me (webRTC) signaling	Mandatory when using web meet me client
ASBCE Edge	Ephemeral Ports	Elite 6000 MCU Media server	UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	Audio and Video Media to Media server & Elite MCUs	Mandatory for audio and video media
ASBCE Edge	Ephemeral Ports	Management / B2BUA	TCP 5060 5061 UDP 5060	For external XT connectivity in OTT	Mandatory for XT SIP connectivity
ASBCE Edge	Ephemeral Ports	DNS Server	TCP/UDP 53	Required for H.323 URI Dialing	Mandatory for URI Dialing

XT Desktop Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
XT Desktop Server	Ephemeral TCP ports	XT Series	TCP 3336-3337 (XTD XML API) Sip/H.323 calls: TCP 1720 (H225/Q931) TCP/UDP Ephemeral Ports TCP 3230-3250* (H225/H245) UDP 3230-3313*(RTP/RTCP) TCP/UDP 5060 UDP 5070-5077*(BFCP)	Enables XML controls Allows H.323 and sip calls	Mandatory
XT Desktop Client	Ephemeral Ports	XT Desktop Server	TCP 80 (HTTP) TCP 443 (HTTPS) UDP 10000-65535 **	Provides access to the XT Desktop Web Portal Enables RTP media tunneling if UDP Ports are blocked Audio and video media	Mandatory

XT Series Ports

XT Series uses ephemeral ports in the range 32768- 61000.

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
XT Series or EP in an H.323 call	TCP/UDP Ephemeral Ports TCP 3230-3250* (H225/H245) UDP 3230-3313*(RTP/RTCP)	H.323 Gatekeeper PathFinder	RAS signaling UDP 1719 (RAS) UDP 1718 (RAS GK autodiscovery to multicast IPv4 address 224.0.0.41) Q931 and H245 call signaling (when managed by GK) TCP 1720 (H225/Q931) Ephemeral TCP ports	Enable gatekeeper/ PF services and call signaling	Mandatory for H.323 deployments
		H.323 EP/XT/Elite MCU	Q931 and H245 call signaling TCP 1720 (H225/Q931) TCP 3230-3250* (H225/H245)(XT) or Ephemeral TCP ports Media UDP 3230-3313*(RTP/RTCP)(XT) or ephemeral UDP ports _* Other EPs/MCUs may use different ephemeral port ranges_	H.323 signaling, audio and video media RTP/RTCP	Mandatory for H.323 calls
XT Series or endpoint in a SIP call	TCP/UDP Ephemeral Ports TCP 5070-5077*(BFCP) UDP 3230-3313* (RTP/RTCP)	SIP Clients/XT and Servers	SIP and BFCP call signaling TCP/UDP 5060 (SIP) TCP 5061 (SIP TLS) UDP 5070-5077*(BFCP) TCP/UDP ephemeral Ports Media UDP 3230-3313*(RTP/RTCP) or ephemeral UDP ports	SIP and BFCP signaling, audio and video media RTP/RTCP	Mandatory for SIP calls

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
			** Other EPs/MCUs may use different ephemeral port ranges*		
XT Series	Ephemeral ports	STUN Server	UDP 3478-3479	Discover the presence of a NAT and public IPv4 address assigned by the NAT	Recommended for auto-discovery of XT public IPv4 address
XT Series	Ephemeral ports	XMPP Presence Server	TCP 5222	TLS communication to XMPP server	Mandatory to use presence services with Aura, IPO or generic XMPP servers
XT Series	Ephemeral ports	FTP/SFTP Server AESR	TCP 21	File transfer from XT to a server (recorded files or NetLog files)	Recommended
XT Series	Ephemeral ports	DNS Server	UDP 53	Resolve DNS names	
XT Series	Ephemeral ports	Internet Servers/Scopia Desktop/ Web Collab Server/ Equinox Management	TCP 80** (HTTP) TCP 443** (HTTPS)	NAT autodiscovery and geolocalization services. Scopia Mobile service. Web Collab service. Cloud connection and provisioning services	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	Ephemeral ports	Simple Network Time Protocol Server	UDP 123 (SNTP)	Enables receiving Internet UTC time from SNTP server	Recommended
	Ephemeral ports	Equinox Management/ Management servers	UDP 162 (SNMP) TCP 389 (LDAP) TCP 3336 (SM XML API)	Enables management and SNMP traps. Enables receiving contact information from Equinox Management LDAP directory or from third party LDAP servers. Enable receiving roster information in a call.	Recommended when not using cloud connection.
	Ephemeral ports	SNMP Server	UDP 161	Enables sending of SNMP traps	Recommended
	Ephemeral ports	LDAP Server	TCP 389 (LDAP)	Enables requests to LDAP server for contact information	Mandatory if using external LDAP remote directory
	Ephemeral ports	Scopia Desktop Client/XTD client	TCP 8554 (RTSP)	Enables XT Series to receive a presentation from a PC/MAC via Screen Link	Mandatory for Screen Link
XT Desktop Server	Ephemeral ports	XT Series	TCP 3336-3337 (XTD XML API)	Enables XML controls and receives XT status	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Scopia Desktop Client or XTD client	Ephemeral ports	XT Series	TCP 80(HTTP) TCP 443 (HTTPS)	Manual activation of Screen link/Mobile Link	Mandatory
Equinox Management	Ephemeral ports	XT Series	TCP 3341 (SM XML API) TCP 55099 (Sw upgrade with unsigned packages) TCP 55003 (AT commands) UDP 161 (SNMP)	Enables notifications for Roster and calendar; software upgrade and XT management when not using Cloud Mode	Recommended when XT is not managed in Cloud Mode
Scopia Control Application (iPad/iPhone)	Ephemeral ports	XT Series	TCP 3338-3339	Enable the Scopia Control application to communicate with XT	Mandatory for Scopia Control
XT Sw Update Application (Windows PC)	Ephemeral ports	XT Series	TCP 55099 (Sw upgrade with unsigned packages) TCP 55090 (Sw upgrade with signed packages)	Enable upgrade of XT software using with a Windows PC application	Mandatory to upgrade XT using the PC app
XT SDK API Client (Creston/Extron)	Ephemeral ports	XT series	TCP 55003 (AT commands) TCP 22 (SSH)	Enables XT management from third party devices	Optional
Scopia XT PC Control Application (Windows PC/Mac)	Ephemeral ports	XTE240 in Personal or Shared Endpoint mode	TCP 55000 UDP 55001	Allow the Scopia XT Control app for Windows and Mac to manage XTE240	Mandatory
Any browser	Ephemeral ports	XT Series	TCP 80 (HTTP) TCP 443(HTTPS)	Allow to access the XT web server for remote management	Mandatory

*The maximum port range is specified. The used port range could be lower than the specified one, depending on available license and active settings. Please check on XT UI (Networks>Preferences>Dynamic ports> Manual mode) for the used range.

** A different port can be configured on the Equinox Management server for Cloud Provisioning server.

ISDN Gateway Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Management PC	Ephemeral Ports	Scopia ISDN Gateway	TCP 21 (FTP)	Enables Gateway upgrades	Mandatory
Management PC	Ephemeral Ports	Scopia ISDN Gateway	TCP 23 (Telnet)	Enables viewing of logs	Recommended
Management PC/Web client	Ephemeral Ports	Scopia ISDN Gateway	TCP 80 (HTTP) TCP 443 (HTTPS)	Provides access to the Gateway web Interface	Mandatory TCP 443 Mandatory if using HTTPS
Management PC/Web client	Ephemeral Ports	Scopia ISDN Gateway	TCP 80 (HTTP) TCP 443 (HTTPS)	Provides access to the Gateway web Interface	Mandatory TCP 443 Mandatory if using HTTPS
Management PC or Equinox Management	Ephemeral Ports	Scopia ISDN Gateway	UDP 161 (SNMP)	Enables SNMP management	Mandatory
Scopia ISDN Gateway	Ephemeral Ports	Equinox Management or Traps Destination Server	UDP 162 (SNMP) Traps	Enables SNMP Traps	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	TCP 1024-4999 UDP 1619 (Q931) UDP 1719 (RAS) UDP 1820 (RAS) TCP 1620 (IVR) TCP 1503 (T.120) UDP 7222-7422 (RTP/RTCP - IVR audio) UDP 6722-7822 (RTP/RTCP - IVR video) UDP 120002-12952 (RTP/RTCP)	H.323 Devices	Ephemeral Ports	Enables H.245 signaling Enables Q.931 signaling Enables sending RAS messages Enables receiving RAS messages Enables IVR over TCP Enables T.120 data collaboration IVR Audio	Mandatory
	TCP 1024-4999 UDP 1619 (IVR registration) UDP 1719 (RAS)	Equinox Management	TCP 32768-61000	Management Enables H.245 signaling Enables IVR registration with Gatekeeper Enables RAS	Mandatory when communication with Gatekeeper

Scopia Classic MCU Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Management PC	Ephemeral TCP ports	Scopia Classic MCU	TCP 80 (HTTP) TCP 443 (HTTPS)	Provides access to the MCU Administrator and Conference Control web interfaces	Mandatory Mandatory if using HTTPS
Management PC FTP Server	Ephemeral TCP Ports	Scopia Classic MCU	TCP 21 (FTP)	Enables upgrade via utility Enables audio stream recording	Optional
Scopia Classic MCU	TCP 1720 (Q931) TCP 1024-4999 (H.245)	Any H.323 Device	Ephemeral TCP ports	Cannot connect H.323 calls	Mandatory
	UDP 6000-6999	Any H.323 or SIP device	Ephemeral UDP Ports	Enables audio and media streams	Mandatory
	TCP 2010 (MPI)	Any MP standalone units (MCUs in MP clustering mode)	TCP 1024-4999	Cannot use external MP	Mandatory if deployment is configured in MP clustering mode
	TCP/UDP 5060 (SIP)	Any SIP device	Ephemeral Ports	Enables SIP signaling	Mandatory for SIP Calls
	UDP 1719 (RAS)	H.323 Gatekeeper	UDP Ports	Enables RAS signaling	Mandatory
	TCP 3337 (XML)	Scopia Classic MCUs	TCP 1024-4999	Enables cascade between 2 Scopia Classic MCUs	Mandatory if deployment contains multiple Scopia Classic MCUs with Equinox Management

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	TCP 3336 (XML)	Equinox Management	Ephemeral TCP Ports	Enables management of the MCU via XML API	Mandatory if deployed with Equinox Management
	UDP 162 (SNMP)	SNMP Trap Server	UDP 161 (SNMP)	Enables SNMP traps to be sent to SNMP server	Recommended
	Scopia MCU	Telnet Client	Ephemeral TCP ports	Enables viewing of MCU logs and initial configuration tasks	Optional
	TCP 2946 TCP 3340	Scopia Classic MCU	TCP 1024-4999	Cannot connect to the MCU Cannot work with non-English Fonts	Mandatory
	UDP 10000-10575	Any H.323 or SIP device	Ephemeral UDP Ports	Cannot transmit/receive audio and video media streams	Mandatory

WCS Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Web Collaboration Client	Ephemeral TCP Ports	WCS Ports	TCP 80 (HTTP) TCP 443 (HTTPS) TCP 843	WCS web interface WCS web interface (HTTP over SSL) Client Flash Policy server	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Web Collaboration Server	TCP 3336, 3338, 3346, 3348 TCP 8080, 9443	Equinox Management	TCP 5556, 8095, 8445 TCP 32768-61000	Facilitates WCS Administration	Mandatory
	TCP/UDP 5060 (SIP) TCP 5061 (SIP over TLS)	Equinox Management Scopia Elite MCU	TCP 32768-61000 TCP 1024-1324 (Elite MCU)	SIP signaling	Mandatory
	UDP 12000-13599 (RTP) TCP/UDP 3400-3580	Scopia Elite MCU	UDP 12000-132000 (RTP) TCP 1024-1324	RTP presentation traffic BFCP presentation traffic	Mandatory
	TCP 3400-3580	DNS	UDP 53	FQDN resolution	Mandatory

Streaming and Recording Ports

In the tables below, an Equinox Streaming and Recording client is any web browser using the Streaming and Recording tab of the Equinox Unified Portal. The acronym SR stands for streaming and recording.

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Administrator web browser	TCP (HTTPS), Ephemeral TCP Ports	SR Manager	TCP (HTTPS) 8445	SR Manager Admin Web Interface	Mandatory for administrators
Administrator remote desktop client	TCP (RDP) Ephemeral TCP Ports	SR Manager	TCP (RDP) 3389	Remote Desktop to Manager	Optional

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Equinox SR Client	TCP (HTTP, HTTPS), Ephemeral TCP Ports	SR Manager	TCP 80 (HTTP) TCP 443 (HTTPS)	Communicate with Manager to list / watch recordings / broadcasts	Mandatory
SR Manager	Ephemeral TCP Ports	Conference Point	TCP (HTTPS) 443	XML for communication and push of media files	Mandatory
	Ephemeral TCP Ports	Delivery Node	TCP (HTTPS) 443	XML for communication and push of media files	Mandatory
	Ephemeral TCP Ports	Virtual Delivery Node	TCP (HTTPS) 443	XML for communication	Mandatory if using CDN
	Ephemeral TCP Ports	Equinox Management	TCP (HTTPS) 443	API for Management Communication – the TCP port is defined by Equinox Management	Mandatory
	Ephemeral TCP Ports	Equinox SR Transcoder	TCP (XML) 8443	XML Communication with transcoder	Mandatory
	Ephemeral TCP Ports	SMTP Server	TCP (SMTP) 25	SMTP (email) Communication	Optional
	Ephemeral UDP and TCP Ports	DNS Server	UDP (DNS) 53 TCP (DNS) 53	DNS name resolution	Optional
	Ephemeral UDP Ports	NTP Server	UDP (NTP) 123	Network Time Server	Optional

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Administrator web browser	TCP (HTTPS), Ephemeral TCP Ports	Conference Point (CP)	TCP (HTTPS) 8445	CP Admin Web Interface	Mandatory for administrators
Administrator remote desktop client	TCP (RDP) Ephemeral TCP Ports	Windows server hosting CP	TCP (RDP) 3389	Remote Desktop to Windows Host	Optional
Conference Point (CP)	Ephemeral TCP Ports	SR Manager	TCP (XML) 443	Management communications	Mandatory
	Ephemeral TCP Ports	Transcoder	TCP (XML) 8443	Communication between Devices Media Streams	Mandatory
	Ephemeral TCP Ports	Transcoder	TCP (Windows Media Stream) 9090 → 9XXXX	CP pulls media from the transcoder	Mandatory if multicast
	Ephemeral UDP Ports	Transcoder	UDP (AAC-LC) 9090 → 9XXXX	CP pulls media from the transcoder	Mandatory if multicast
	Ephemeral UDP Ports	ECS Gatekeeper	UDP (RAS) 1719	RAS communication with the gatekeeper	Mandatory
	Ephemeral TCP Ports	ECS Gatekeeper	TCP (Q.931) 1720	RAS communication with the gatekeeper (call setup)	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	Ephemeral TCP Ports	ECS Gatekeeper	1025 - 65535	RAS communication with the gatekeeper. You can limit the range on the gatekeeper.	Mandatory
	Ephemeral UDP and TCP Ports	DNS Server	UDP (DNS) 53 TCP (DNS) 53	DNS name resolution	Optional
	Ephemeral UDP Ports	NTP Server	UDP (NTP) 123	Network Time Server	Optional

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Administrator web browser	TCP (HTTPS), Ephemeral TCP Ports	DN	TCP (HTTPS) 8445	DN Admin Web Interface	Mandatory for administrators
Equinox SR Client	TCP (HTTP, HTTPS), Ephemeral TCP Ports	Delivery Node (DN)	TCP (HTTP, HTTPS, HLS) 80, 443	media to clients for broadcasts and recordings (HLS, Progressive Download)	Mandatory
Equinox SR Client	TCP (Windows Media), Ephemeral TCP Ports	Delivery Node (DN)	TCP 80 TCP 554 TCP 1755	media to clients for broadcasts (using multicast, Windows Media Streaming) *** If Multicast is enabled	Mandatory for multicast
Administrator remote desktop client	TCP (RDP) Ephemeral TCP Ports	Windows server hosting DN	TCP (RDP) 3389	Remote Desktop to Windows Host	Optional

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Delivery Node (DN)	Ephemeral TCP Ports	CP	TCP 80	RTP media (windows media streaming). CP gets raw RTP from Scopia® Elite MCU then sends it to the transcoder to encode to Windows Media. Then, it pulls back from the transcoder and makes it available to the DN	Mandatory
	Ephemeral UDP Ports	Equinox SR Client	UDP - Multicast Port Range	When using MMS and the network is Multicast-capable, the standard port range for multicast will be used	
	Ephemeral TCP Ports	DN	TCP 80 (HLS, Windows Media) TCP 443 (HLS)	DN to DN media transfer	Mandatory
	Ephemeral UDP, TCP Ports	Equinox SR Client	UDP 1024-5000 TCP 1755 HTTP (Windows Media) 80	When doing Windows Media, Client will try UDP between port 1024-5000 (Only open the necessary number of ports), then TCP on port 1755, then TCP on port 80	Mandatory when doing MMS

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	Ephemeral TCP Ports	Equinox SR Transcoder	TCP 8080 TCP 8443	Communication between devices; access to HLS media	Mandatory
	Ephemeral TCP Ports	SR Manager	TCP 443 (XML)	Management communication	Mandatory
	Ephemeral UDP and TCP Ports	DNS Server	UDP (DNS) 53 TCP (DNS) 53	DNS name resolution	Optional
	Ephemeral UDP Ports	NTP Server	UDP (NTP) 123	Network Time Server	Optional

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Administrator remote desktop client	TCP (RDP) Ephemeral TCP Ports	Transcoder	TCP (RDP) 3389	Remote Desktop to Transcoder	Optional
Equinox SR Transcoder	Ephemeral TCP Ports	Conference Point	TCP 80	Transcoder pulls ASR Media Stream from the CP	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	Ephemeral TCP Ports	Conference Point	TCP 1755	Windows Media Stream	Mandatory for multicast
	TCP 8080 TCP 8443	Delivery Node			Mandatory
	Ephemeral TCP Ports	SR Manager	TCP 443 (XML)	Management communication	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Administrator web browser	TCP (HTTPS), Ephemeral TCP Ports	VDN	TCP (HTTPS) 8445	VDN Admin Web Interface	Mandatory for administrators
Virtual Delivery Node (VDN)	Ephemeral TCP Ports	Delivery Node	TCP 80 TCP 443	HLS Media Stream	Mandatory
	TCP 80	Session Border Controller (SBC)	TCP 443	Media Streams to clients	Mandatory
	Ephemeral TCP Ports	SR Manager	TCP 443 (XML)	Management communication	Mandatory
	Ephemeral UDP and TCP Ports	DNS Server	UDP (DNS) 53 TCP (DNS) 53	DNS name resolution	Optional
	Ephemeral UDP Ports	NTP Server	UDP (NTP) 123	Network Time Server	Optional

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Administrator remote desktop client	TCP (RDP) Ephemeral TCP Ports	Windows server hosting VDN	TCP (RDP) 3389	Remote Desktop to Windows Host	Optional
Content Delivery Network (CDN)	Ephemeral TCP Ports	Virtual Delivery Node	TCP (HLS Media) 80, 443	Uploading content from VDN to CDN If the VDN is not accessible from the outside, then you need a Session Border Controller (SBC) which will route from the CDN to the VDN	Mandatory
Session Border Controller (SBC)	Ephemeral TCP Ports	Virtual Delivery Node	TCP (HLS Media) 80, 443	Routes between the CDN and the VDN if the VDN is not accessible from CDN	Mandatory if VDN is not accessible from CDN

VC240 Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Management PC	Ephemeral Ports	VC240	TCP 80 (HTTP) TCP 22445 (HTTPS)	Access to the VC240 web interface via HTTP or HTTPS	Mandatory if accessing the VC240 web interface

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Equinox Management	Ephemeral Ports	VC240	TCP 23 (Telnet) UDP 4000 (RV Shell)	Management (including configuration) of VC240 from Equinox Management	Recommended
APC Client	Ephemeral Ports	VC240	TCP 22 (SSH)	SSH access to VC240; software upgrades	Recommended
VC240	Ephemeral Ports	TFTP Server	UDP 69 (TFTP)	Software upgrade via TFTP server	Optional
	Ephemeral Ports	Gatekeeper	UDP 1719 (RAS)	Enables RAS signaling	Recommended
	TCP 1720 (Q931) TCP 3230-3241 (H.245) UDP 3230-3251 (RTP/RTCP)	Any H.323 Devices	Ephemeral Ports	Enables Q931 signaling Enables H.245 signaling Audio and Video Media	Recommended
	TCP/UDP (5060) SIP	Any SIP device	Ephemeral Ports	Enables SIP signaling	Mandatory for SIP calls
	TCP 224444 (API)	API application	Ephemeral Ports	Access to API for remote access and upgrades	Mandatory if upgrading via the web
	UDP 161 (SNMP)	Any SNMP Trap server	UDP 162 (SNMP)	Enables sending SNMP traps	Mandatory if using SNMP servers

Video Gateway Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Scopia Video Gateway	Ephemeral ports	Microsoft STUN server	TCP 443 (STUN)	Enables remote SIP ICE connectivity	Mandatory for remote endpoint connectivity
	UDP 1719 (RAS) TCP 1720 (Q931) TCP 1024-1174 (H.245)	Any H.323 device	Ephemeral ports	Enables H.245 signaling, Registration with Gatekeeper	Cannot connect H.323 calls or register with Gatekeeper
	TCP 3336 (XML) TCP 3338 (XML) TCP 3346 (XML - TLS) TCP 3348 (XML - TLS)	Equinox Management	TCP 32768-61000	Enables management and configuration via Gateway XML API	Mandatory Mandatory if using TLS
	H.323 PROTOCOL TCP 1024-1324 (H.245) TCP 3337 (XML to Elite MCU) UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	Elite MCUs/Equinox Media Server (MCU)	TCP 3400-3580 (BFCP - TCP) UDP 12000-13200 (Video RTP) UDP 16384-16984 (Audio RTP)	Audio and Video Media between cascaded Elite MCUs for SIP calls	Mandatory for media between cascaded Elite MCUs
	UDP 3478 (STUN)	STUN Server	Ephemeral ports	Enables remote endpoints to connect	Mandatory
	TCP/UDP 5060 (SIP) TCP 5061 (SIP- TLS)	Any SIP device	Ephemeral ports	Enables SIP signaling Enables secure SIP signaling	Mandatory Mandatory if using TLS

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	UDP 12000-13200 (RTP/RTCP/SRTP) UDP 16384-16984 (RTP/RTCP/SRTP) TCP 20000-29000 (RTP/RTCP/SRTP) TCP 40000-46200 (RTP/RTCP/SRTP)	Any SIP or H.323 Device	Ephemeral ports	Audio media stream Video media stream Audio media over TCP Video media over TCP	Mandatory
	UDP 162 (SNMP)	SNMP Server	UDP 161 (SNMP)	SNMP traps	Recommended
	TCP 21 (FTP)	FTP Server	Ephemeral ports	Enables audio stream recording	Optional
	TCP 22 (SSH)	SSH Client	Ephemeral ports	Enables viewing of gateway logs in real time	Optional
	TCP 80 (HTTP)	Management PC	Ephemeral ports	Enables Gateway upgrade or download of customer support package	Mandatory

SIP Gateway Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	UDP 1719 (RAS) TCP 1720 (Q931) TCP 1024-1174 (H.245)	Any H.323 device	Ephemeral ports	Enables H.245 signaling, Registration with Gatekeeper	Cannot connect H.323 calls or register with Gatekeeper.
	TCP 3336 (XML) TCP 3338 (XML) TCP 3346 (XML - TLS) TCP 3348 (XML - TLS)	Equinox Management	Ephemeral ports	Enables management and configuration via Gateway XML API	It is mandatory to open the management port. Use 3336 and 3338 if not using TLS, use 3346 and 3348 if using TLS.
	UDP 3478 (STUN)	STUN Server	Ephemeral ports	Enables remote endpoints to connect	Mandatory
	TCP/UDP 5060 (SIP) TCP 5061 (SIP- TLS)	Any SIP device	Ephemeral ports	Enables SIP signaling Enables secure SIP signaling	It is mandatory to open the management port. Use 5060 if not using TLS, use 5061 if using TLS.
	UDP 12000-13200 (RTP/RTCP/SRTP) UDP 16384-16984 (RTP/RTCP/SRTP)	Any SIP or H.323 Device	Ephemeral ports	Audio media stream Video media stream Audio media over TCP Video media over TCP	Mandatory
	UDP 162 (SNMP)	SNMP Server	UDP 161 (SNMP)	SNMP traps	Recommended

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	TCP 21 (FTP)	FTP Server	Ephemeral ports	Enables audio stream recording	Optional
	TCP 22 (SSH)	SSH Client	Ephemeral ports	Enables viewing of gateway logs in real time	Optional
	TCP 80 (HTTP)	Management PC	Ephemeral ports	Enables Gateway upgrade or download of customer support package	Mandatory

TIP Gateway Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Scopia TIP Gateway	TCP 443 (STUN)	Microsoft STUN server	Ephemeral ports	Enables remote SIP ICE connectivity	Mandatory for remote endpoint connectivity
	UDP 1719 (RAS) TCP 1720 (Q931) TCP 1024-1174 (H.245)	Any H.323 device	Ephemeral ports	Enables H.245 signaling, Registration with Gatekeeper	Cannot connect H.323 calls or register with Gatekeeper.
	TCP 3336 (XML) TCP 3338 (XML) TCP 3346 (XML - TLS) TCP 3348 (XML - TLS)	Equinox Management	Ephemeral ports	Enables management and configuration via Gateway XML API	Mandatory Mandatory if using TLS
	UDP 3478 (STUN)	STUN Server	Ephemeral ports	Enables remote endpoints to connect	Mandatory
	TCP/UDP 5060 (SIP) TCP 5061 (SIP- TLS)	Any SIP device	Ephemeral ports	Enables SIP signaling Enables secure SIP signaling	Mandatory Mandatory if using TLS
	UDP 12000-12718 (RTP/RTCP/SRTP) UDP 16384-17280 (RTP/RTCP/SRTP)	Any SIP or H.323 Device	Ephemeral ports	Audio media stream Video media stream	Mandatory
	UDP 162 (SNMP)	SNMP Server	UDP 161 (SNMP)	SNMP traps	Recommended

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	TCP 21 (FTP)	FTP Server	Ephemeral ports	Enables audio stream recording	Optional
	TCP 22 (SSH)	SSH Client	Ephemeral ports	Enables viewing of gateway logs in real time	Optional
	TCP 80 (HTTP)	Management PC	Ephemeral ports	Enables Gateway upgrade or download of customer support package	Mandatory

Unified Portal/Web Gateway Ports

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
Unified Portal	TCP 3341 (XML) TCP 3343 (XML) TCP 3351 (XML - TLS) TCP 3353 (XML - TLS) HTTPS 8446	Equinox Management	Ephemeral ports	Enables management and configuration via XML API	Mandatory Mandatory if using TLS
	HTTPS 8443 HTTPS 8444	Web Browser	Ephemeral ports	Enables browser to access	Mandatory

Source Device	Source Network (or application) Protocol and Port	Destination Device	Destination Network (or application) Protocol and Port	Description	Requirement
	TCP/UDP 5060 (SIP) TCP 5061 (SIP- TLS)	Any SIP device	Ephemeral ports	Enables SIP signaling Enables secure SIP signaling	Mandatory Mandatory if using TLS
	TCP 22 (SSH)	SSH Client	Ephemeral ports	Enables viewing of logs in real time	Optional

Procedures for limiting port ranges

Limiting the TCP Port Range for H.245/Q.931 on the Scopia® Desktop Server and Scopia® XT Desktop Server

About this task

The Scopia® Desktop and XT Desktop server has designated ports 1024-65535 for TCP for H.245 and Q.931 signaling. To provide additional security for your firewall, you can limit this range.

For each conference, the Scopia® Desktop server uses 2 ports. In addition, add extra ports for:

- Add 2 ports for each participating Scopia® Desktop Client.
- Add 1 port per conference when presenting using the content slider.

Procedure

1. Navigate to <Scopia® Desktop installation directory>\ConfSrv.
2. Edit the **config.val** file as follows:
   a. Locate the text `1 system`
   b. At the bottom of that section, add two lines:

      ```
      2 portFrom = <lowest range limit>
      2 portTo = <highest range limit>
      ```

      Where <lowest range limit> is the base port of your port range and <highest range limit> is the upper value of your port range.

3. Access the Windows services and restart the Scopia® Desktop - Conference Server service.

Configuring Ports on the H.323 Edge server

This section provides instructions of how to configure the following ports and port ranges on the Avaya Equinox H.323 Edge server.

Configuring the UDP Port for RAS on the H.323 Edge server

About this task

The Avaya Equinox H.323 Edge server assumes the gatekeeper uses 1719 as the designated port for RAS (communication with the gatekeeper). You can configure a different port for RAS (if, for example, port 1719 is busy).

Procedure

If the H.323 Edge server is managed in Equinox Management, you can configure it as follows:

1. Login to Equinox Management and click the on the **Devices** tab.
2. Select and click on the name of the H.323 Edge in the list.
3. Click on the **Configuration** tab.
4. Locate the **Gatekeeper Settings** area.
5. Modify the value of the **Gatekeeper Port** field.
6. Click **Apply**.

Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the H.323 Edge server

About this task

The Avaya Equinox H.323 Edge server has designated ports 4000-5000 for H.323 Direct Public Access (DPA), which allows non-H.460 public endpoints to call internal endpoints without being registered to the H.323 Edge server. To provide additional security for your firewall, you can limit this range.

To calculate approximately how many ports the H.323 Edge server uses, multiply the number of simultaneous DPA calls by 10. The multiplication factor is lower for audio-only calls and higher for calls with dual video. We recommend using 10 as an approximation.

Procedure

If the H.323 Edge server is managed in Equinox Management, you can configure it as follows:

1. Login to Equinox Management and click the on the **Devices** tab.
2. Select and click on the name of the H.323 Edge in the list.
3. Click on the **Configuration** tab.
4. Locate the **Direct Public Access** area.
5. Modify the value of the **Port Range Minimum Port** and **Port Range Maximum Port** fields.
6. Click **Apply**.

Defining the H.323 Edge internal TCP/UDP port range

About this task

Avaya Equinox H.323 Edge server uses a separate set of TCP and UDP ports communicate with devices on the enterprise network. There are two rules relating to the TCP/UDP port range, as follows:

- The value for the minimum port must be greater than 8000.
- The port range must contain at least 300 ports and no more than 6000 ports.

The steps are to define the port range are as follows:

1. Login to Equinox Management and click the on the **Devices** tab.
2. Select and click on the name of the H.323 Edge in the list.

3. Click on the **Configuration** tab.
4. Locate the **Internal Communication** section, enter the port range desired in the **Internal Port Range Minimum Port** and **Internal Port Range Maximum Port** fields.

Limiting the default TCP Port Range for Scopia applications installed on Windows servers

About this task

Avaya 8.x platform applications installed on Windows Servers (ECS Gatekeeper, Scopia Management, Scopia Desktop Server, and Scopia XT Desktop Server) use the same TCP port range as the underlying Windows system TCP port ranges for H.245/Q.931, which depends on the version of Windows you are running:

- If you have Windows XP or Windows Server 2003, use the Windows default dynamic port range: 1025-5000.
- If you have Windows Vista or Windows Server 2008 or 2012, use the Windows default dynamic port range: 49152-65535.

To provide additional security for your firewall, you can limit this range. To calculate how many ports the applications use, multiply the maximum calls allowed by your license by four. Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls, and H.245 is a Control Protocol used for multimedia communication that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams.

Procedure

1. Access the Windows Services and stop the **Scopia product Service**.
2. Open the **Windows registry**.
3. Navigate to:
   - HKEY_LOCAL_MACHINE\SOFTWARE\RADVISION\Enhanced Communication Server\Storage\Config\Stack on a 32-bit Windows system.
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RADVISION\Enhanced Communication Server\Storage\Config\Stack on a 64-bit Windows system.

7. Create a new string, as follows:
   a. Right-click the **Stack** folder and select **New > String Value**.
   b. Name the new string **PortMin**.
   c. Right-click **PortMin** and select **Modify**.
   d. In the **Value data** field, enter the value of the minimum port number the ECS should use.
8. Create a new string, as follows:
   a. Right-click the **Stack** folder and select **New > String Value**.
   b. Name the new string **PortMax**.

c. Right-click **PortMax** and select **Modify**.

d. In the **Value data** field, enter the value of the maximum port number the ECS should use.

9. Verify the **PortMax** value is within the Windows port range:
   - On Windows XP or Windows Server 2003, navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**.
     If **MaxUserPort** is not defined there, its default is **5000**. To change the system's default maximum port number, define and set a value for **MaxUserPort**. Then restart the computer.
   - On Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2012, check the system's maximum port value in a command line window by entering:

     ```
     netsh int ipv4 show dynamicportrange protocol=tcp
     ```

     To change the system's default maximum, open the command line prompt as an administrator by right-clicking on **cmd** and selecting **Run as administrator**, and enter the following command:

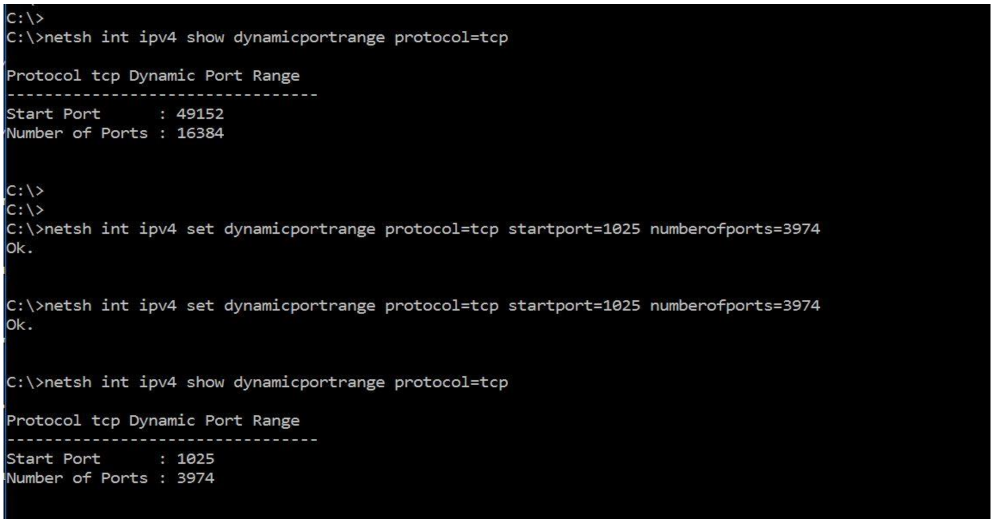
     ```
     netsh int ipv4 set dynamicportrange protocol=tcp
     startport=1025 numberofports=3975
     ```

     Enter the show command to verify the maximum port has changed.

   - **Important**: If the value you defined in **PortMax** is higher than 5000, increase the value of the number of ports in the command. For example, if you defined the value of **PortMax** as 6000, change the value of numberofports in the command to 4975.

     In either case, **PortMax** should be lower than the system's maximum port number.

10. Access the Windows Services and restart the **Scopia applications service**.



```
C:\>
C:\>netsh int ipv4 show dynamicportrange protocol=tcp

Protocol tcp Dynamic Port Range
---------------------------------
Start Port      : 49152
Number of Ports : 16384


C:\>
C:\>
C:\>netsh int ipv4 set dynamicportrange protocol=tcp startport=1025 numberofports=3974
Ok.


C:\>netsh int ipv4 set dynamicportrange protocol=tcp startport=1025 numberofports=3974
Ok.


C:\>netsh int ipv4 show dynamicportrange protocol=tcp

Protocol tcp Dynamic Port Range
---------------------------------
Start Port      : 1025
Number of Ports : 3974
```

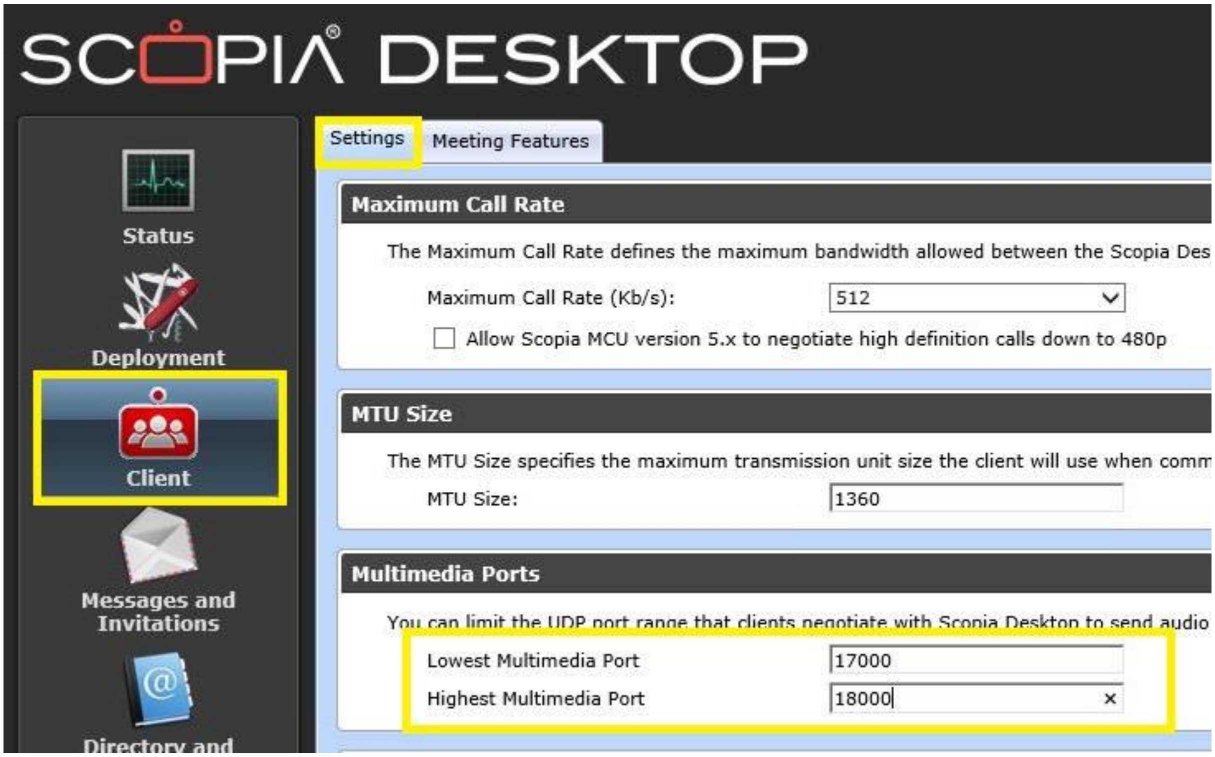
Limiting the UDP Port Range for RTP/RTCP on the Scopia® Desktop and XT Desktop Server

About this task

The Scopia® Desktop server has designated 10000-65535 as the default port range for UDP (RTP/RTCP). To provide additional security for your firewall, you can limit this range. To calculate approximately how many ports the Scopia® Desktop server uses, multiply the number of license connections by 14, which amounts to reserving 14 ports per client.

Procedure

1. Log in to the Scopia® Desktop/XT Desktop Sserver Administrator web user interface.
2. Select **Client > Settings**.
3. Locate the **Multimedia Ports** section.
4. Configure your port range (using any values between 2326 and 65535) by doing the following:
    a. Enter the base port value in the **Lowest Multimedia Port** field.
    b. Enter the upper port value in the **Highest Multimedia Port** field.
5. Select **OK** or **Apply**.



Maximum Call Rate

The Maximum Call Rate defines the maximum bandwidth allowed between the Scopia Des

Maximum Call Rate (Kb/s): 512

☐ Allow Scopia MCU version 5.x to negotiate high definition calls down to 480p

MTU Size

The MTU Size specifies the maximum transmission unit size the client will use when comm

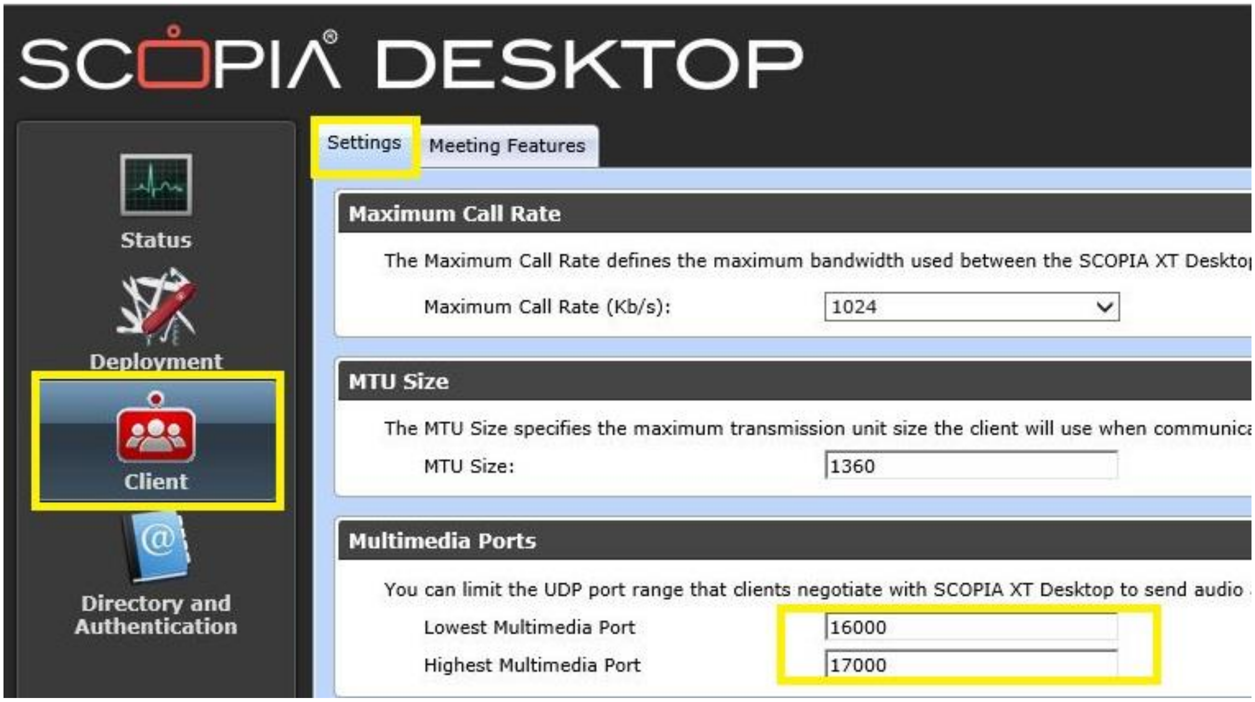
MTU Size: 1360

Multimedia Ports

You can limit the UDP port range that clients negotiate with Scopia Desktop to send audio

Lowest Multimedia Port 17000

Highest Multimedia Port 18000



Maximum Call Rate

The Maximum Call Rate defines the maximum bandwidth used between the SCOPIA XT Deskto

Maximum Call Rate (Kb/s): 1024

MTU Size

The MTU Size specifies the maximum transmission unit size the client will use when communica

MTU Size: 1360

Multimedia Ports

You can limit the UDP port range that clients negotiate with SCOPIA XT Desktop to send audio

Lowest Multimedia Port 16000

Highest Multimedia Port 17000

Configuring RTP/RTCP/SRTP Ports on the Scopia® Video Gateway, SIP Gateway and Avaya Scopia® TIP Gateway

About this task

The Scopia® Video Gateway, Avaya Scopia® SIP Gateway and Avaya Scopia® TIP Gateway designate ports 16384-17584 for UDP audio media, and 12000-13200 for UDP video media. In addition, the Scopia® Video Gateway uses ports 20000-29000 for TCP audio and 40000-46200 for TCP video.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select **Devices**.
3. Select **Gateways** in the sidebar menu.
4. Select the relevant gateway from the **Gateways** list.
5. Select the **Configure** tab.
6. Select **Advanced Parameters Settings**. The **Advanced Parameters** dialog box appears.
7. Set the UDP video base port by doing the following:
    a. For SIP Gateway and TIP Gateway deployments: Enter the **advcmdmvpsetval** command in the Command field.
    b. For Scopia® Video Gateway deployments: Enter the **advcmdmpcsetval** command in the Command field.
    c. Enter the **mf.BasePort** parameter in the **Parameter** field to set the UDP video base port.

Important: For Scopia® Video Gateway deployments: To set the TCP video base port, enter mf.MvpTcpBasePort in the **Parameter** field.

   d. Enter the port value in the **Value** field.
   e. Select **Save**.

8. For SIP Gateway and TIP Gateway deployments: Complete the video base port configuration as follows:
   a. Enter the mvpconfigcompletedcommand command in the Command field.
   b. Enter 1 in the **Value** field.
   c. Select **Save**.
   d. Clear the value in the Parameter field before proceeding to the next step.
9. For SIP Gateway and TIP Gateway deployments: Set the audio base port by doing the following:
   a. Enter the **advcmdmapsetval** command in the **Command** field.
   b. Enter the **mf.UdpBasePort** parameter in the **Parameter** field.
   c. Enter the port value in the **Value** field.
   d. Select **Save**.
   e. Enter the **mapconfigcompleted** command in the **Command** field.
   f. Enter 1 in the **Value** field.
   g. Select **Save**.
10. For Scopia® Video Gateway deployments: Set the UDP audio base port by doing the following:
    a. Enter the **setmprtpbaseport** command in the **Command** field.
    b. Modify the port value in the **Value** field.
    c. Select **Save**.
11. For Scopia® Video Gateway deployments: Set the TCP audio base port by doing the following:
    a. Enter the **setmptcpbaseport** command in the **Command** field.
    b. Modify the port value in the **Value** field.
    c. Select **Save**.
12. Select **Close**.

Configuring TCP Port for Q.931 on the Scopia® Video Gateway, SIP Gateway, and Avaya Scopia® TIP Gateway

About this task

The Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and Avaya Scopia® TIP Gateway designate port 1720 for Q.931. Q.931 is a telephony protocol used for establishing and terminating the connections in H.323 calls. You can configure a different port for Q.931 (if, for example, port 1720 is busy).

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select **Devices**.
3. Select **Gateways** in the sidebar menu.
4. Select the relevant gateway from the **Gateways** list.
5. Select the **Configure** tab.
6. Select **Advanced Parameters** Settings. The **Advanced Parameters** dialog box appears.
    a. Select **h323sigport** from the **Command ID** list.
    b. Enter the port value in the **Value** field.
    c. Select **Save**.
    d. Select **Close**.

Limiting TCP Port Range for H.245 on the Scopia® Video Gateway, Avaya Scopia® SIP Gateway, and Avaya Scopia® TIP Gateway

About this task

The Scopia® Video Gateway, Avaya Scopia® SIP Gateway and Avaya Scopia® TIP Gateway designate ports 1024-1174 for H.245 (signaling). H.245 is a control protocol used for multimedia communications that enables transferring information about the device capabilities, as well as opening/closing the logical channels that carry media streams. To provide additional security for your firewall, you can limit this range.

Procedure

1. Log in to the Equinox Management administrator portal.
2. Select **Devices > Devices by Type > Gateways**.
3. Select the relevant gateway from the **Gateways** list.
4. Select the **Configure** tab.
5. Select **Advanced Parameters**. The **Advanced Parameters** dialog box appears
6. To set the base port for the H.245 control channel protocol, do the following:
    a. Clear the values before proceeding to the next step.
    b. Enter h245baseport in the **Command ID** field.
    c. Enter the port value in the **Value** field.

    d. Select **Save**.
    e. Select **Close**

7. To set the port range for H.245, do the following:
    a. Clear the values before proceeding to the next step.
    b. Enter h245portrange in the **Command ID** field.
    c. Enter the port value in the **Value** field.
    d. Select **Save**.
    e. Select **Close**

Limiting RTP/UDP Ports on the Streaming and Recording Conference Point

Procedure

1. Log in the conference point administration page.
2. Type https://<CP FQDN/IP Address>:8445/ in a web browser.
3. Log in using the following credentials:
    - Username: administrator
    - Password: administrator
4. Navigate to **System Configuration** > **Enable Services**.
5. In the **RTP Ports** panel, enter the base port value in the **From** field, and the upper port value in the **To** field.
6. Click Save.

Glossary

Old Name	**New Name**
Avaya Communicator <for iOS> <for Android> <for Mac OS> <for Windows>	Avaya Equinox <for iOS> <for Android> <for Mac OS> <for Windows> <Meetings for Web>
Avaya Aura Communicator <for Web>	Avaya Equinox <for Web>
Avaya Cloud Application Link	Avaya Cloud Application Link
Avaya Scopia Desktop	Avaya Scopia Desktop
Avaya Scopia Mobile	Avaya Scopia Mobile
Scopia Management	Avaya Equinox Management Server

New	Avaya Equinox Media Server (This consists of the MCU7000 and AMS and WCS.)
New	Avaya Aura Web Gateway
Pathfinder H.323 Firewall Traversal	Avaya Equinox H.323 Edge
Avaya Scopia Streaming and Recording (Scopia SR)	Avaya Equinox Streaming and Recording (AESR)
Scopia Desktop Server	*No change*
Scopia XT 4300/5000/7100/ XTE240	*No change*
Scopia Elite 5XXX MCU	*No change*
Scopia Web Collaboration Server (WCS)	In this release, WCS is part of the Avaya Equinox Media Server. (This consists of the MCU7000 and AMS and WCS.)
Other Aura elements	*No change*

Port Security for the Equinox Solution

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

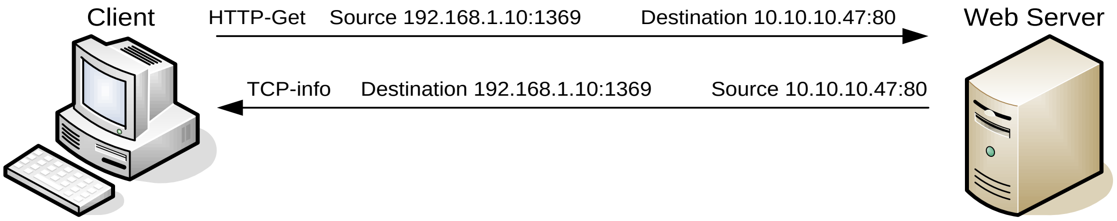


Figure 1. Socket example showing ingress and egress data flows from a PC to a web server

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.