Clients - Webex Evolve Anywhere - Firewall Guide

Foreword

This guide is designed to provide firewall recommendations for settings and port openings. Evolve strides to provide the most ideal settings for the most common firewalls. However, knowing the exact settings for customer firewalls, IT vendors, and ISP carriers is the responsibility of the customer and their contracted IT vendors

Port Openings

A Customer

Named Server List for ACLs	Ports	Purpose	Status
voip.evolveip.net	• 5061/UDP&TCP • 10000-65000/UDP • 10000-65000/UDP	• SIP - TLS • Audio SRTP • Video SRTP	Active
webex-adp-a.voip.evolveip.net	• 443 444 8012	HTTP(S)	Active
dms-adp-a.voip.evolveip.net	443	mTLS DMS	Active

B Customer

Named Server List for ACLs	Ports	Purpose	Status
voip-b.evolveip.net	• 5061/UDP&TCP • 10000-65000/UDP • 10000-65000/UDP	• SIP - TLS • Audio SRTP • Video SRTP	Active
webex-adp-b.voip.evolveip.net	• 443 444 8012	HTTP(S)	Active
dms-adp-b.voip.evolveip.net	443	mTLS DMS	Active

C Customer

Named Server List for ACLs	Ports	Purpose	Status
voip-c.evolveip.net	• 5061/UDP&TCP • 10000-65000/UDP • 10000-65000/UDP	• SIP - TLS • Audio SRTP • Video SRTP	Active
webex-adp-b.voip.evolveip.net	• 443 444 8012	HTTP(S)	Active
dms-adp-b.voip.evolveip.net	443	mTLS DMS	Active

D Customer

Named Server List for ACLs	Ports	Purpose	Status
Named Server List for ACLs	Ports	Purpose	Status
voip-d.evolveip.net	• 5061/UDP&TCP • 10000-65000/UDP • 10000-65000/UDP	• SIP - TLS • Audio SRTP • Video SRTP	Active
webex-adp-b.voip.evolveip.net	• 443 444 8012	HTTP(S)	Active
dms-adp-b.voip.evolveip.net	443	mTLS DMS	Active

F Customer

Named Server List for ACLs	Ports	Purpose	Status
voip-f.evolveip.net	• 5061/UDP&TCP • 10000-65000/UDP • 10000-65000/UDP	• SIP - TLS • Audio SRTP • Video SRTP	Active
webex-adp-b.voip.evolveip.net	• 443 444 8012	HTTP(S)	Active
dms-adp-b.voip.evolveip.net	443	mTLS DMS	Active

G Customer

Named Server List for ACLs	Ports	Purpose	Status
voip-g.evolveip.net	• 5061/UDP&TCP • 10000-65000/UDP • 10000-65000/UDP	• SIP - TLS • Audio SRTP • Video SRTP	Active
webex-adp-b.voip.evolveip.net	• 443 444 8012	HTTP(S)	Active
dms-adp-b.voip.evolveip.net	443	mTLS DMS	Active

MN/AiTech Customer

Named Server List for ACLs	Ports	Purpose	Status
bwsip.net	• 5061/UDP&TCP • 10000-65000/UDP • 10000-65000/UDP	• SIP - TLS • Audio SRTP • Video SRTP	Active
webex-adp.bwsip.net	• 443 444 8012	HTTP(S)	Active
bwsip.com	443	mTLS DMS	Active

Network Requirements for Webex Services

https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services#id_134894

Document Revision History

This article is intended for network administrators, particularly firewall and proxy security administrators who want to use Webex messaging and meetings services within their organization. It will help you configure your network to support the Webex Services used by HTTPS based Webex app and Webex Room devices, as well as Cisco IP Phones, Cisco video devices, and third-party devices that use SIP to connect to the Webex Meetings service.
This document primarily focuses on the network requirements of Webex cloud registered products that use HTTPS signaling to Webex cloud services, but also separately describes the network requirements of products that use SIP signaling to join Webex Meetings. These differences are summarized below:

Summary of device types and protocols supported by Webex

Transport protocols and encryption ciphers for cloud registered Webex apps and devices

---

Webex traffic through Proxies and Firewalls

Most customers deploy an internet firewall, or internet proxy and firewall, to restrict and control the HTTP based traffic that leaves and enters their network. Follow the firewall and proxy guidance below to enable access to Webex services from your network. If you are using a firewall only, note that filtering Webex signaling traffic using IP addresses is not supported, as the IP addresses used by Webex signaling services are dynamic and may change at any time. If your firewall supports URL filtering, configure the firewall to allow the Webex destination URLs listed in the section "*Domains and URLs that need to be accessed for Webex Services"*.

Webex Services – Port Numbers and Protocols

The following table describes ports and protocols that need to be opened on your firewall to allows cloud registered Webex apps and devices to communicate with Webex cloud signaling and media services.

The Webex apps, devices, and services covered in this table include:
The Webex app, Webex Room devices, Video Mesh Node, Hybrid Data Security node, Directory Connector, Calendar Connector, Management Connector, Serviceability Connector.
For guidance on ports and protocols for devices and Webex services using SIP can be found in the section *"Network requirements for SIP based Webex services"*.

Webex Services - Port Numbers and Protocols			
Destination Port	**Protocol**	**Description**	**Devices using this rule**
443	TLS	Webex HTTPS signaling. Session establishment to Webex services is based on defined URLs, rather than IP addresses. If you are using a proxy server, or your firewall supports DNS resolution; refer to the section *"Domains and URLs that need to be accessed for Webex Services"* to allow signaling access to Webex services.	All
444	TLS	Video Mesh Node secure signaling to establish cascade media connections to the Webex cloud	Video Mesh Node
123 (1)	UDP	Network Time Protocol (NTP)	All
53 (1)	UDP TCP	Domain Name System (DNS) Used for DNS lookups to discover the IP addresses of services in the Webex cloud. Most DNS queries are made over UDP; however, DNS queries may use TCP as well.	All
5004 and 9000	SRTP over UDP	Encrypted audio, video, and content sharing on the Webex App and Webex Room devices For a list of destination IP subnets refer to the section *"IP subnets for Webex media services"*.	Webex App Webex Room Devices Video Mesh Nodes
50,000 – 53,000	SRTP over UDP	Encrypted audio, video, and content sharing – Video Mesh Node only	Video Mesh Node

5004	SRTP over TCP	Used for encrypted content sharing on the Webex App and Webex Room devices TCP also serves as a fallback transport protocol for encrypted audio and video if UDP cannot be used. For a list of destination IP subnets refer to the section *"IP subnets for Webex media services"*.	Webex App Webex Room Devices Video Mesh Nodes
443 (2)	SRTP over TLS	Used as a fallback transport protocol for encrypted audio, video and content sharing if UDP and TCP cannot be used. Media over TLS is not recommended in production environments For a list of destination IP subnets refer to the section *"IP subnets for Webex media services"*.	Webex App (2) Webex Room Devices

(1) If you are using NTP and DNS services within your enterprise network, then ports 53 and 123 do not need to be opened through your firewall.
(2) The Webex Web-based app and Webex SDK do not support media over TLS.

IP subnets for Webex media services

Webex signaling traffic and Enterprise Proxy Configuration

Most organizations use proxy servers to inspect and control the HTTP traffic that leaves their network. Proxies can be used to perform several security functions such as allowing or blocking access to specific URLs, user authentication, IP address/domain/hostname/URI reputation lookup, and traffic decryption and inspection. Proxy servers are also commonly used as the only path that can forward HTTP based internet destined traffic to the enterprise firewall, allowing the firewall to limit outbound internet traffic to that originating from the Proxy server(s) only. Your Proxy server must be configured to allow Webex signaling traffic to access the domains/ URLs listed in the section below:

Domains and URLs that need to be accessed for Webex Services

Additional URLs for Webex Hybrid Services

Your Proxy server must be configured to allow Webex signaling traffic to access the domains/ URLs listed in the previous section. Support for additional proxy features relevant to Webex services is discussed below:

follow this link for additional info below:

https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services#id_134759

Proxy Features:

802.1X – Port based Network Access control :

Network requirements for SIP based Webex services:

Network Requirements for Webex Edge Audio:

A summary of other Webex Hybrid Services and documentation:

Webex Services for FedRAMP customers:

Document Revision History - Network Requirements for Webex Services:

UPDATE FOR 7/2023

2New CIDR Range/Subnet for new Data Centers
TO AVOID DISRUPTION TO SERVICE Update by July 31st & August 15th
As part of Data Center Expansion there are newe proxy and media subnets for the following data centers.
New York (JFK): July 31st will be 23.89.40.192/26 which belongs to CIDR Range : 23.89.0.0/16 (CIDR) or 23.89.0.0 - 23.89.255.255 (net range).
Dallas (DFW2): August 15th , will be 150.253.179.192/27 belongs to CIDR:150.253.128.0/17 (CIDR) or 150.253.128.0 - 150.253.255.255 (net range).
See the Knowledge Article on help.webex.com.