

CISCO *Live!*



#CiscoLive



The bridge to possible

# Understanding Network Security Requirements for Webex Traffic

Laurent Pham, Technical Marketing Engineer  
BRKCOL-2057



#CiscoLive

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2057>

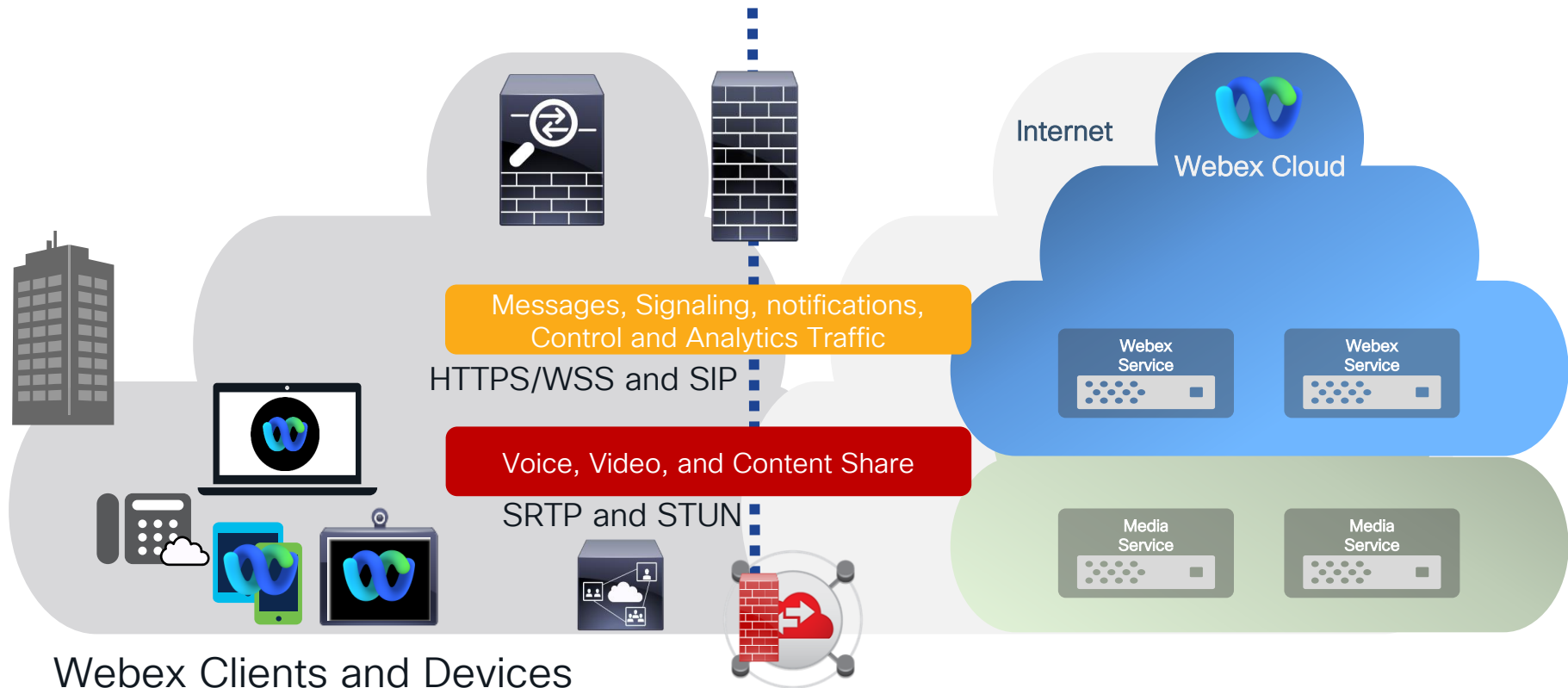


# Agenda

- Fundamentals on firewall traversal
- Media and signaling considerations
- Traffic flows and network port usage
- Conclusion

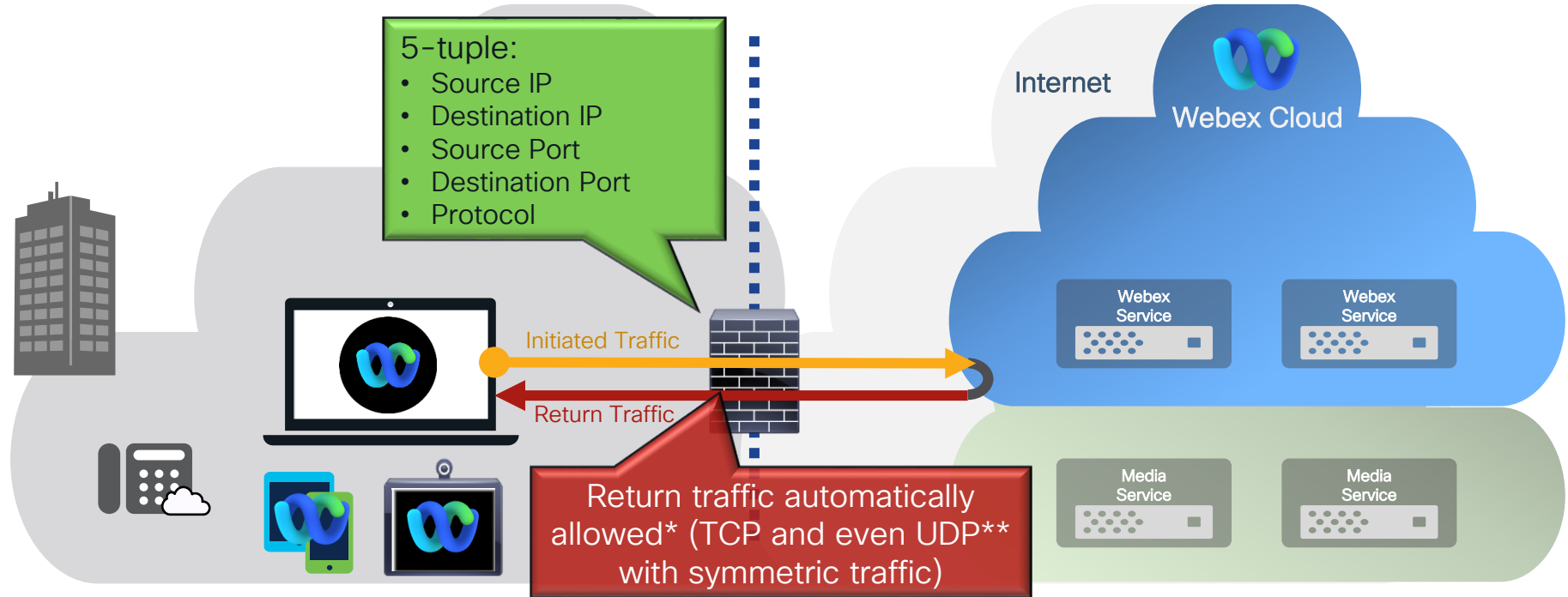
# Fundamentals on Firewall Traversal

# Types of Traffic



# Firewall Traversal

Return traffic automatically allowed



Webex Clients and Devices

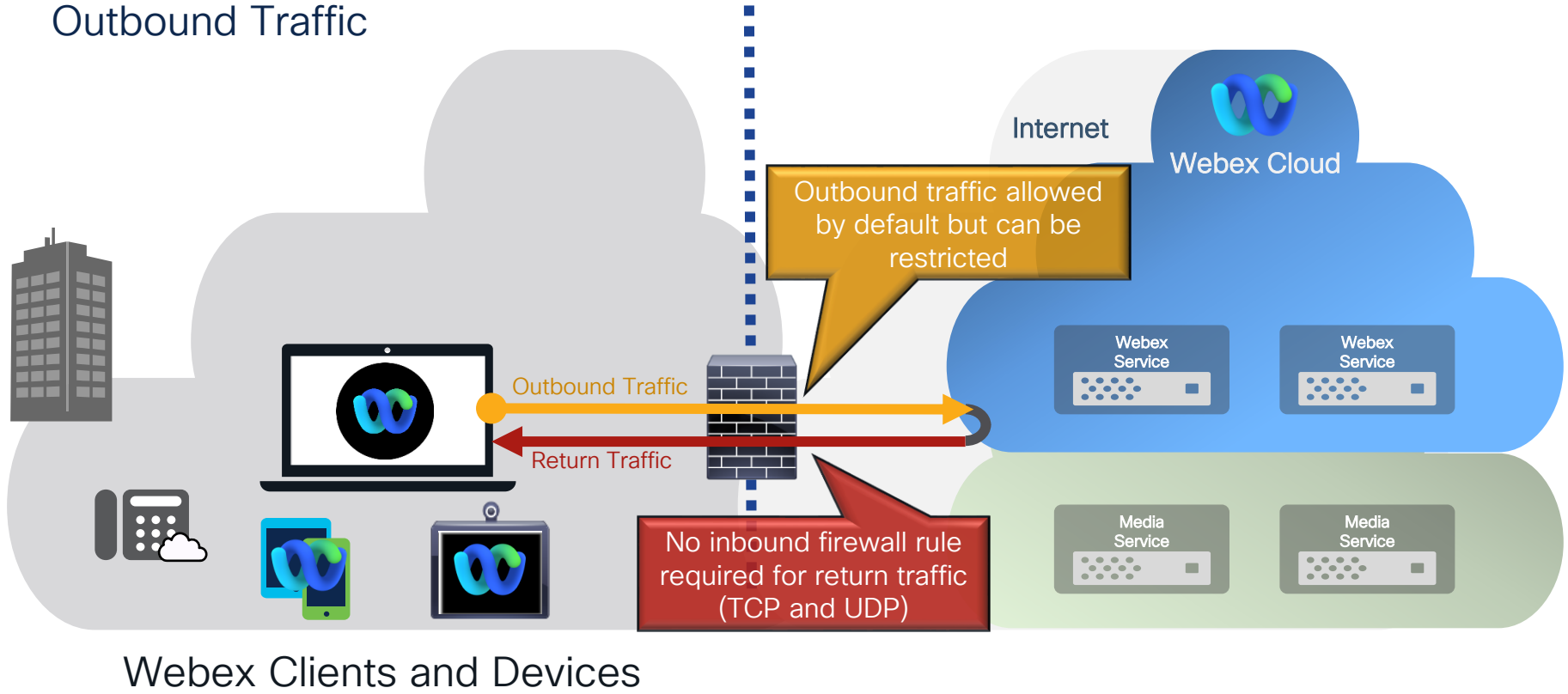
\* With most firewalls

\*\* Return UDP traffic allowed based on timer, not based on connection status



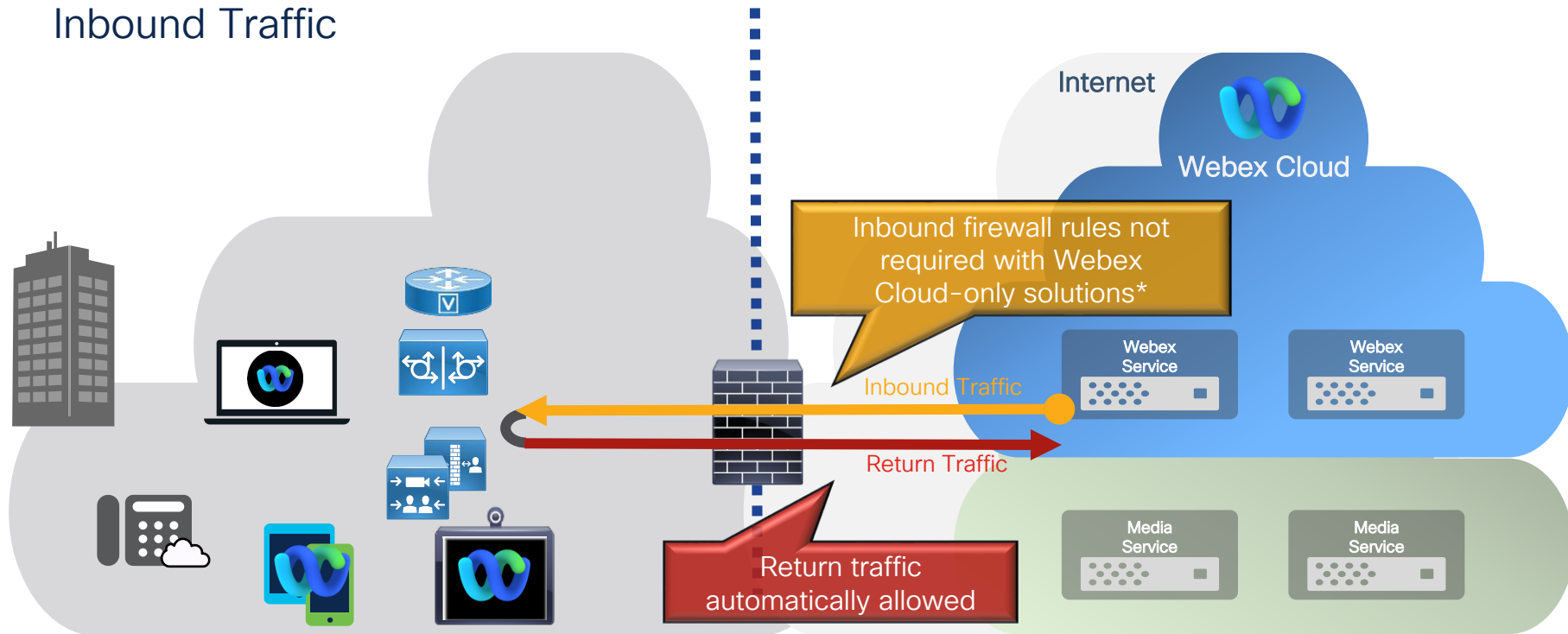
# Firewall Traversal

## Outbound Traffic



# Firewall Traversal

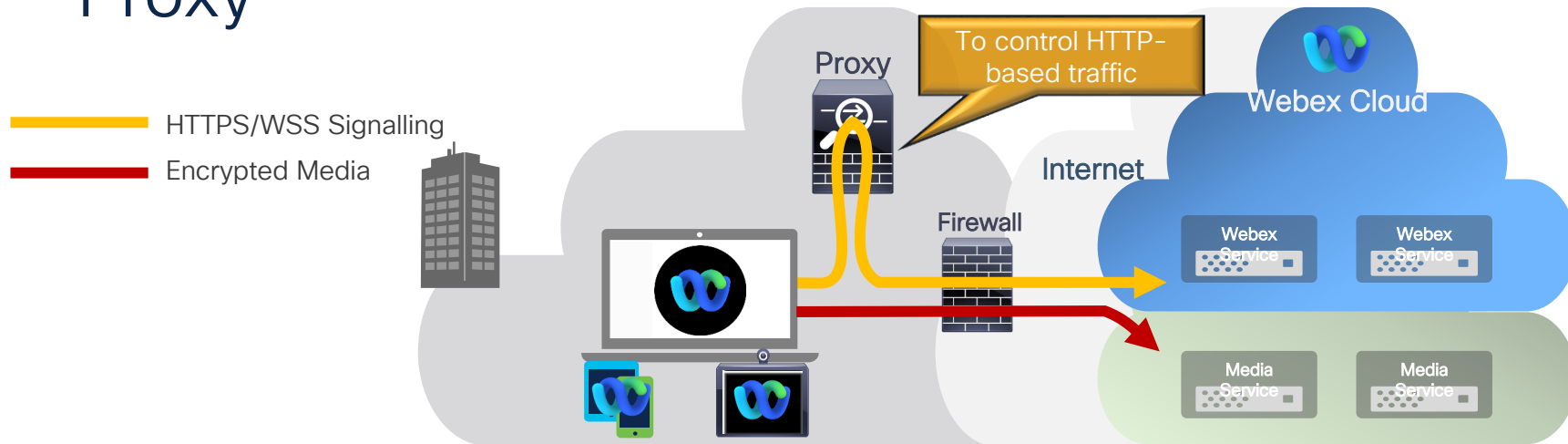
## Inbound Traffic



## Webex Clients and Devices

\* Inbound rules required for SIP calls:  
Webex Edge Audio, Webex Hybrid Calling, Expressway

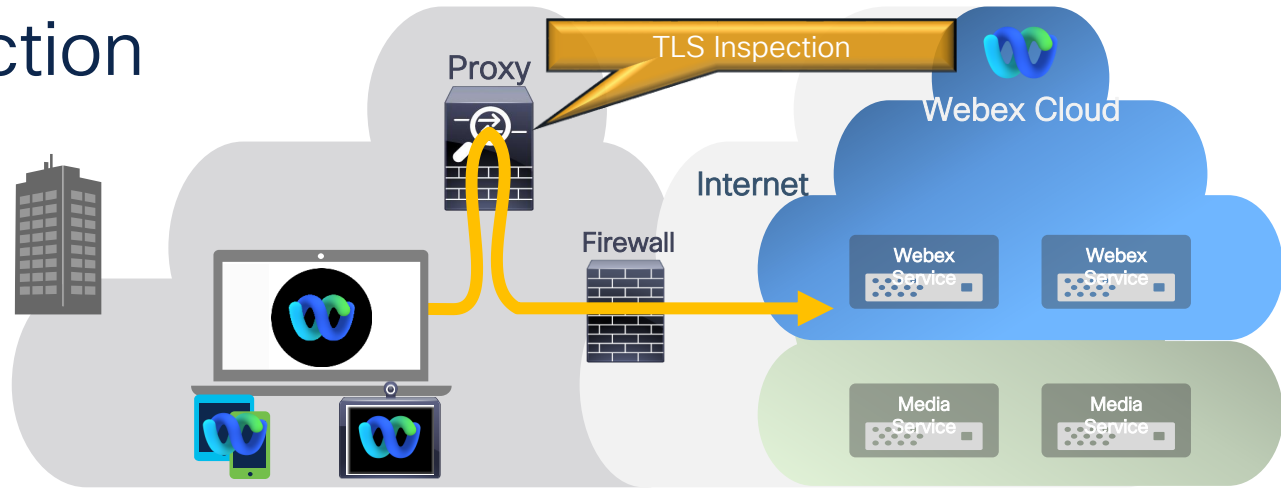
# Proxy



- Supported with Webex Messaging, Meetings, and Calling\*.
- Mainly to control HTTP-based traffic, avoid it for media.
- Typically, have limited bandwidth and CPU. Can cause excessive latency. HTTP proxy is not designed to handle interactive audio and video

\* With Webex Calling, proxy supported only with soft clients

# TLS Inspection



- TLS inspection (or TLS Interception) is supported with Webex devices and Webex App\* but its benefits are limited
  - User-generated Webex content (messages, files, and media) is encrypted inside the TLS connection, so TLS inspection provides no security benefits.
  - Therefore, the **recommendation is to bypass TLS inspection** on the proxy to alleviate proxy's resources.

\* TLS Inspection not supported with Webex Meeting Media Services (TLS inspection exception rules to be configured), Hybrid Services – Directory, Calendar, Mgt connectors, see [Network Requirements](#) for details

# Media and Signaling Considerations



# Signaling



- Leverages HTTPS/WSS (WebSocket Secure) protocols, on TCP/TLS 443. Also SIP signaling with Webex Calling.
- With Webex Cloud-only workloads, outbound TCP connections only (clients/devices initiate outbound connections only). Return traffic automatically allowed.
- If restricting outbound traffic is required by your Infosec team, restrict destinations based on URLs

# Media

## UDP and fallback



- UDP preferred for media (delay and jitter sensitive)
- Webex devices, Webex App (Meetings, Cloud video calling) will:
  - First, try UDP 5004/9000 – Recommended
  - Then, fallback to other protocols/ports:
    - TCP 5004
    - ~~UDP / TCP 33434 – being deprecated~~
    - TLS 443
- With Webex Calling, no fallback to TCP

# Media

UDP is BETTER



- UDP provides better experience for real-time communications
  - UDP: No need to retransmit packets if packet loss
  - TCP: Connection-oriented protocol. Retransmission of lost packets.
  - TLS: Traffic might go through a Proxy, which will lead to additional latency and jitter. Should be avoided.
- In line with RFC 3550 RTP – A Transport Protocol for Real-Time Applications, **Cisco prefers and strongly recommends UDP as the transport protocol for all Webex voice and video media streams.**



# Firewall configuration options to allow media

## Firewall configuration of destination traffic for outbound media

## Notes

**ANY UDP - ANY IP**

Best media quality  
Very easy to configure 😊

**UDP Port Filtering - ANY IP**

(e.g: Only allow UDP 5004/9000 for Webex devices  
and Webex Meetings\*)

Best media quality  
Easy to configure

**UDP Port Filtering - IP Subnet Filtering**

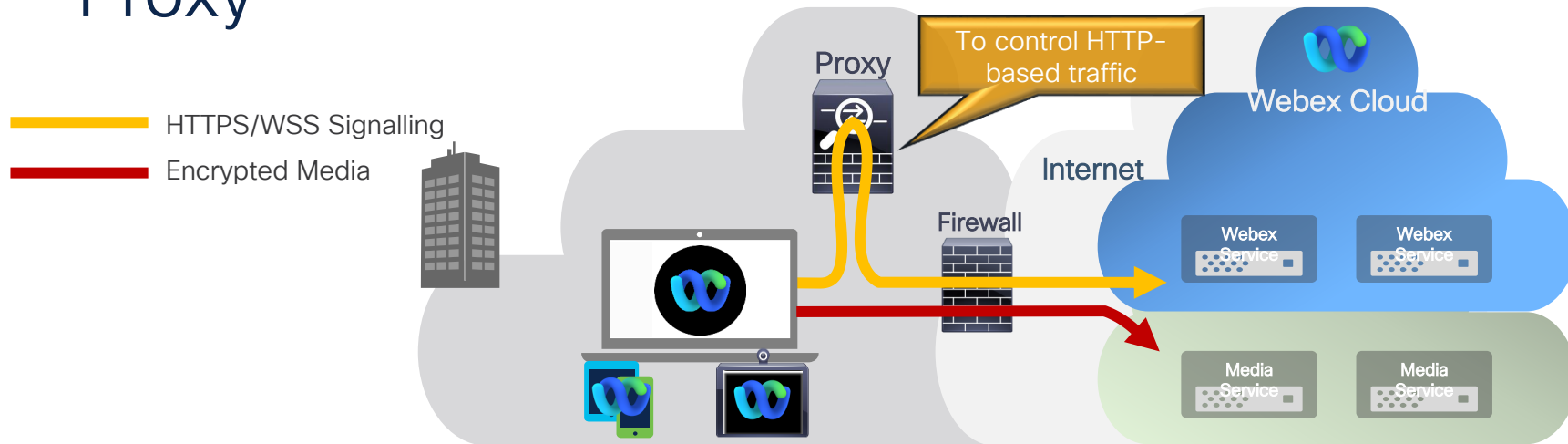
Best media quality but...  
Have to manually keep track of IP  
subnets to allow

**Block UDP\*  
Allow TCP 5004, 443**

Not recommended  
Potential bad media quality especially  
if going through a proxy

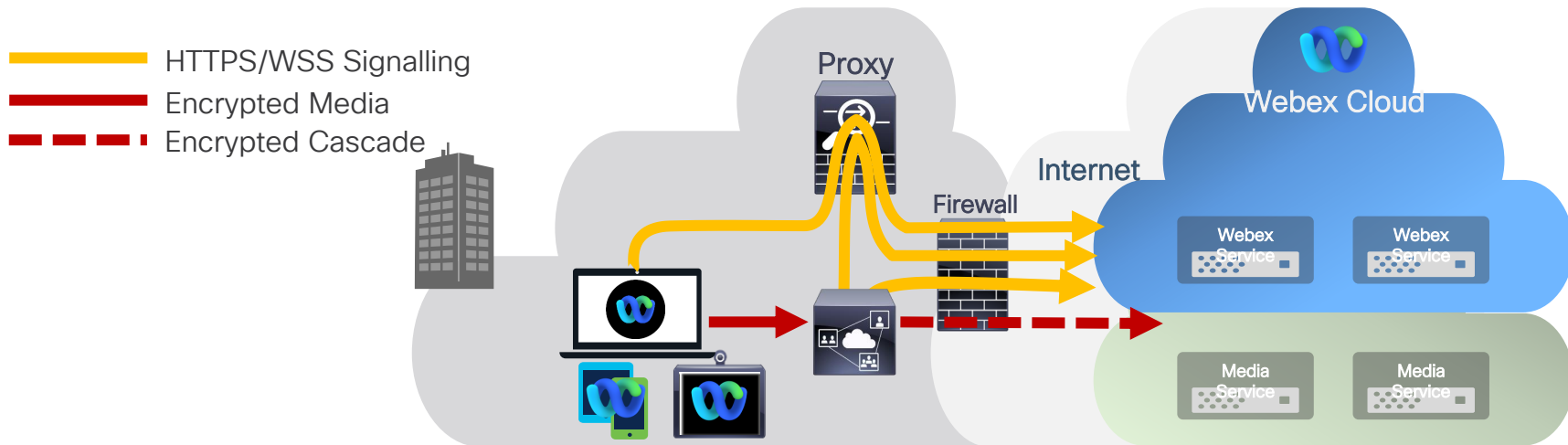
\*Allow UDP 5004 and UDP 19560-65535 for Webex Calling  
Allow UDP 5004 and 50000-53000 for VMN

# Proxy



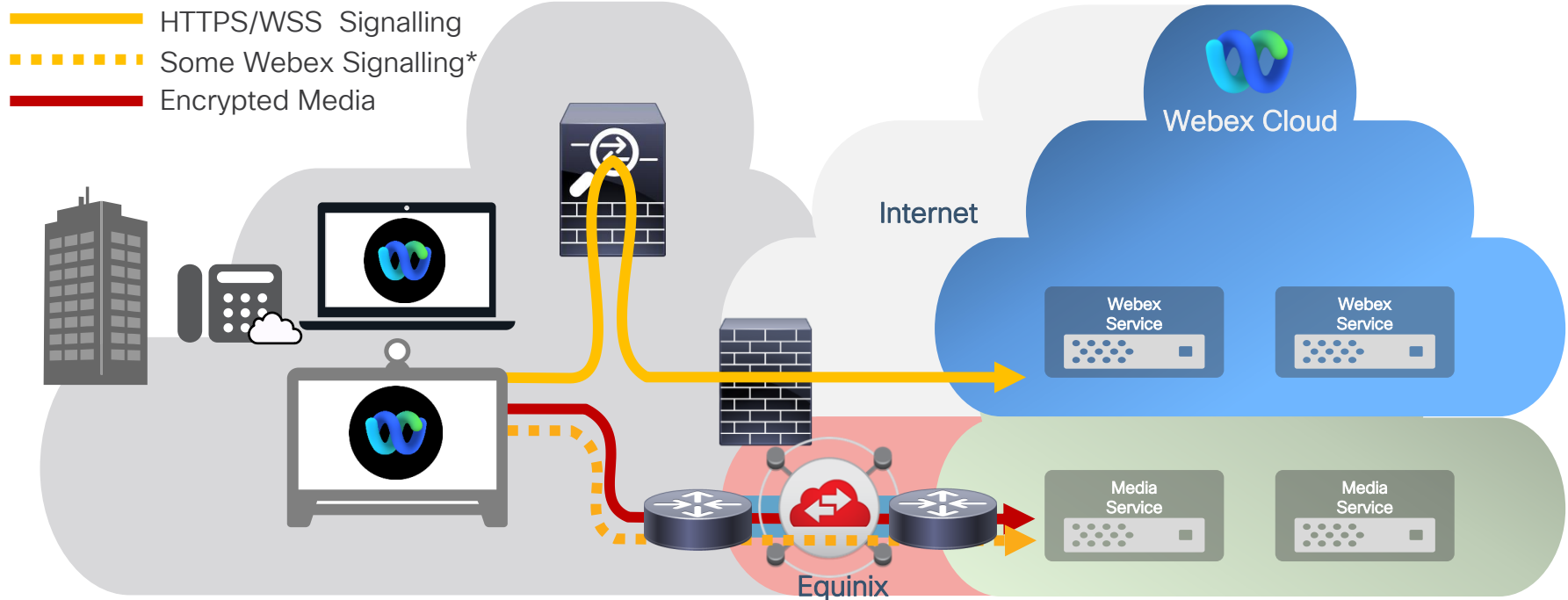
- Again, HTTP proxy is not designed to handle interactive audio and video, **avoid it for media**.
- Recommendation is to allow UDP for media (UDP 5400 and 9000). In this case, media will not flow through the proxy.
- If UDP/TCP 5004 and UDP 9000 are blocked and a proxy is deployed for HTTPS, the Webex soft clients will use TLS and traffic will go through the proxy which may result in bad media quality. The Webex room devices do not send media through the proxy, even if falling back to TLS.
- With Webex Calling, proxy is only supported with soft clients, and this is only for signaling

# Webex Edge Video Mesh (VMN)



- Media conferencing is processed by VMN, media traffic stays on-prem if no need to cascade media due to participants outside.
- Benefit for firewall rule: All outbound media traffic is now sourced from VMN

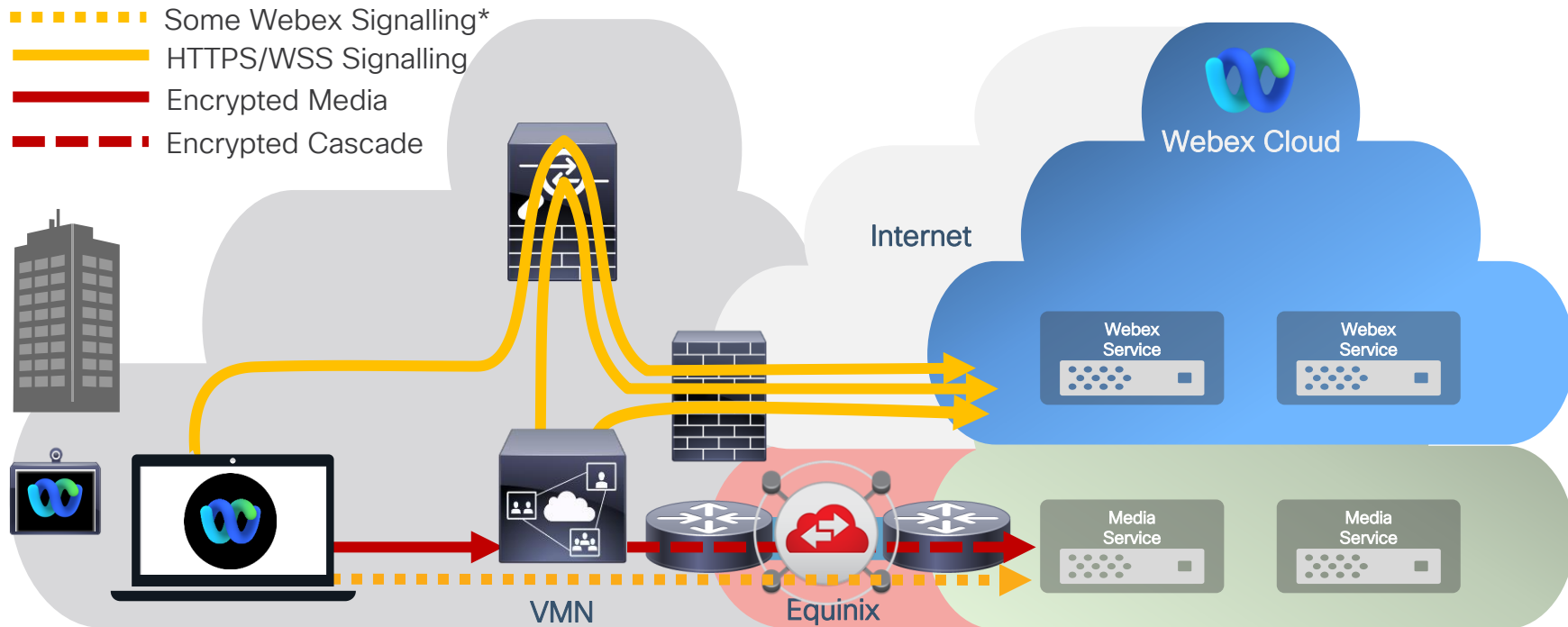
# Webex Edge Connect



- Private link, better QoS, and insulated from the Internet

\*Note: Signalling traffic to services in the webex.com domain (e.g. Identity services, Webex Meetings, Webex Calling) also traverse the Equinix link

# Webex Edge Connect w/ Webex Edge Video Mesh



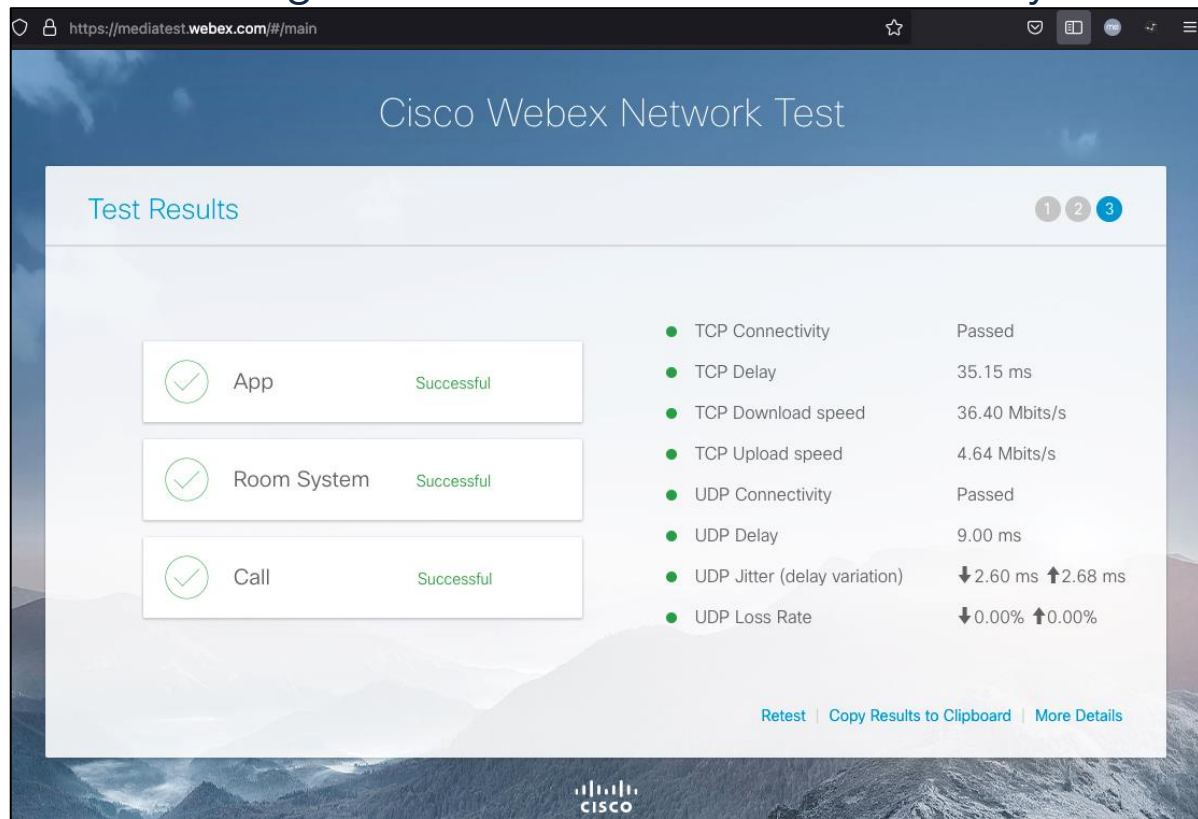
\*Note: Signalling traffic to services in the webex.com domain (e.g. Identity services, Webex Meetings, Webex Calling) also traverse the Equinix link

- Other variations may exist, refer to the [Preferred architecture CVD on Webex Edge Connect](#)

# Cisco Webex Network Test

Good Starting Point to test Internet connectivity

<https://mediatest.webex.com>



Cisco Webex Network Test

Test Results

1 2 3

✓ App	Successful	TCP Connectivity	Passed
✓ Room System	Successful	TCP Delay	35.15 ms
✓ Call	Successful	TCP Download speed	36.40 Mbits/s
		TCP Upload speed	4.64 Mbits/s
		UDP Connectivity	Passed
		UDP Delay	9.00 ms
		UDP Jitter (delay variation)	↓ 2.60 ms ↑ 2.68 ms
		UDP Loss Rate	↓ 0.00% ↑ 0.00%

Retest | Copy Results to Clipboard | More Details

CISCO

Will not test all IP subnets and all URLs

But checks if UDP 5004, 9000 is allowed, measures bandwidth, tests delay, jitter, UDP loss rate, etc

# CSCAN Webex Calling Network Test

<https://cscan.webex.com>

The screenshot shows the results of a network test performed by CSCAN. The browser address bar indicates the URL is <https://cscan.webex.com>. The main content area displays the following information:

Your connection **meets requirements**. Your network is ready for Webex Calling.

Ensure all required ports are open. For more details, please refer to the [port requirements](#) documentation.

Estimate of concurrent possible calls: 10 ⓘ

Your Public IP: [REDACTED]

Firefox 100.0, Mac OS X, United States Dallas

Latency (RTT) ⓘ	Download	Upload
70.43 ms	34.43 Mbps	5.73 Mbps

Packet loss	Jitter
Download - 0.00 %	Download - 7.00 ms
Upload - 0.00 %	Upload - 5.00 ms

Ready	Port	Use
✓	80	Device configuration and firmware management
✓	443	Device configuration and firmware management
✓	8934	Call Signalling to Webex Calling

At the bottom, there are two buttons: "Test Again" and "Test Another Server". Below these buttons is a link: "Download this Report".

# Traffic Flows and Network Port Usage

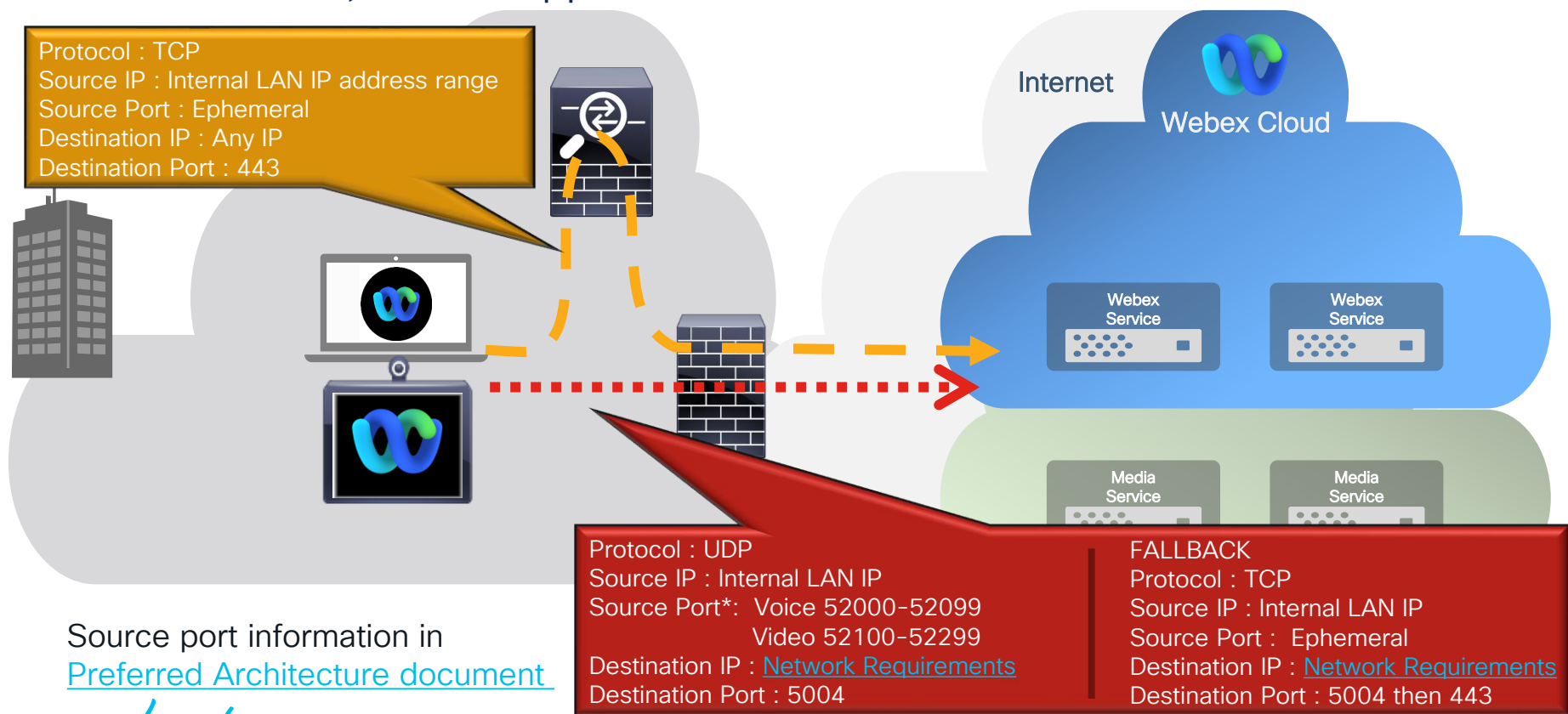




# Protocols and Ports used by Webex

## Webex Devices, Webex App

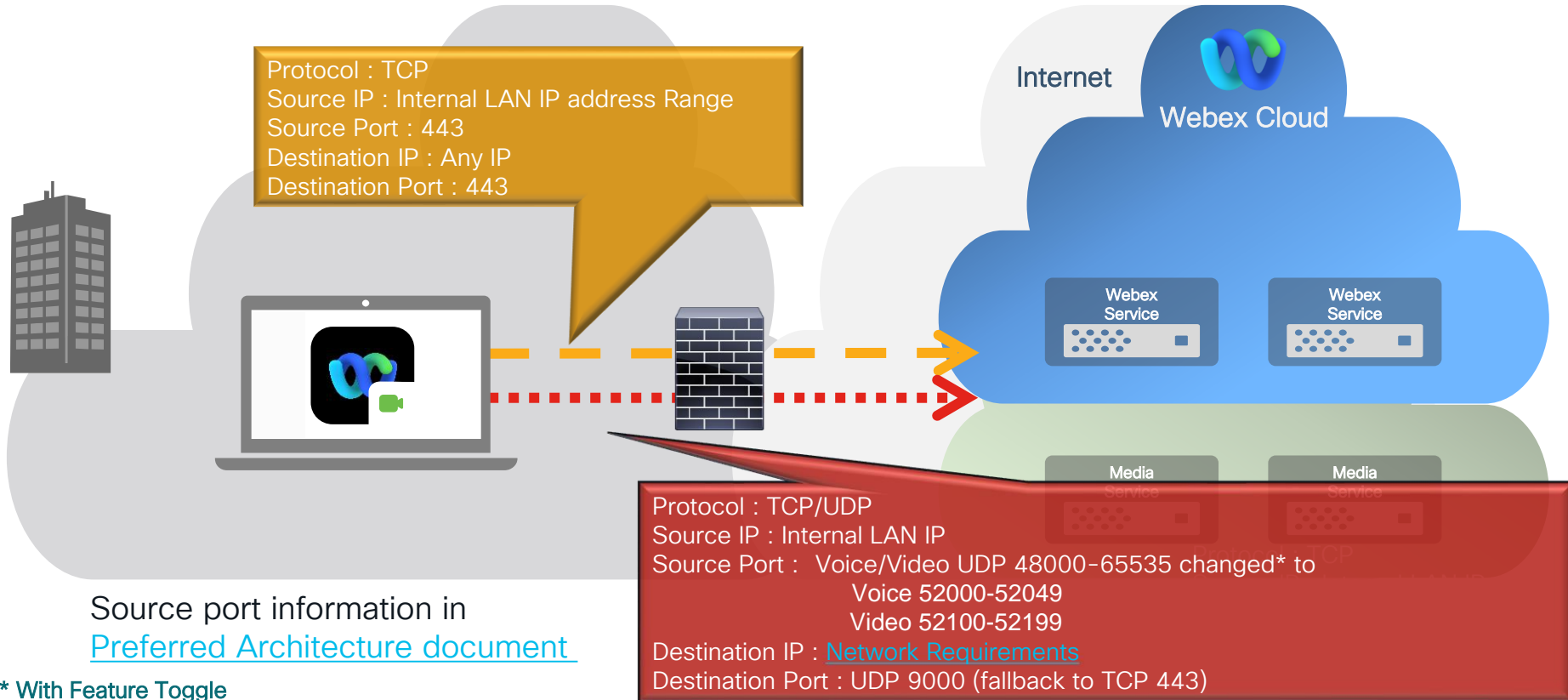
— Signaling/Other Control  
- - - Real Time Traffic



# Protocols and Ports used by Webex

— Signaling/Other Control  
- - - Real Time Traffic

## Webex Meetings App, Webex App (Full-Featured Meetings)



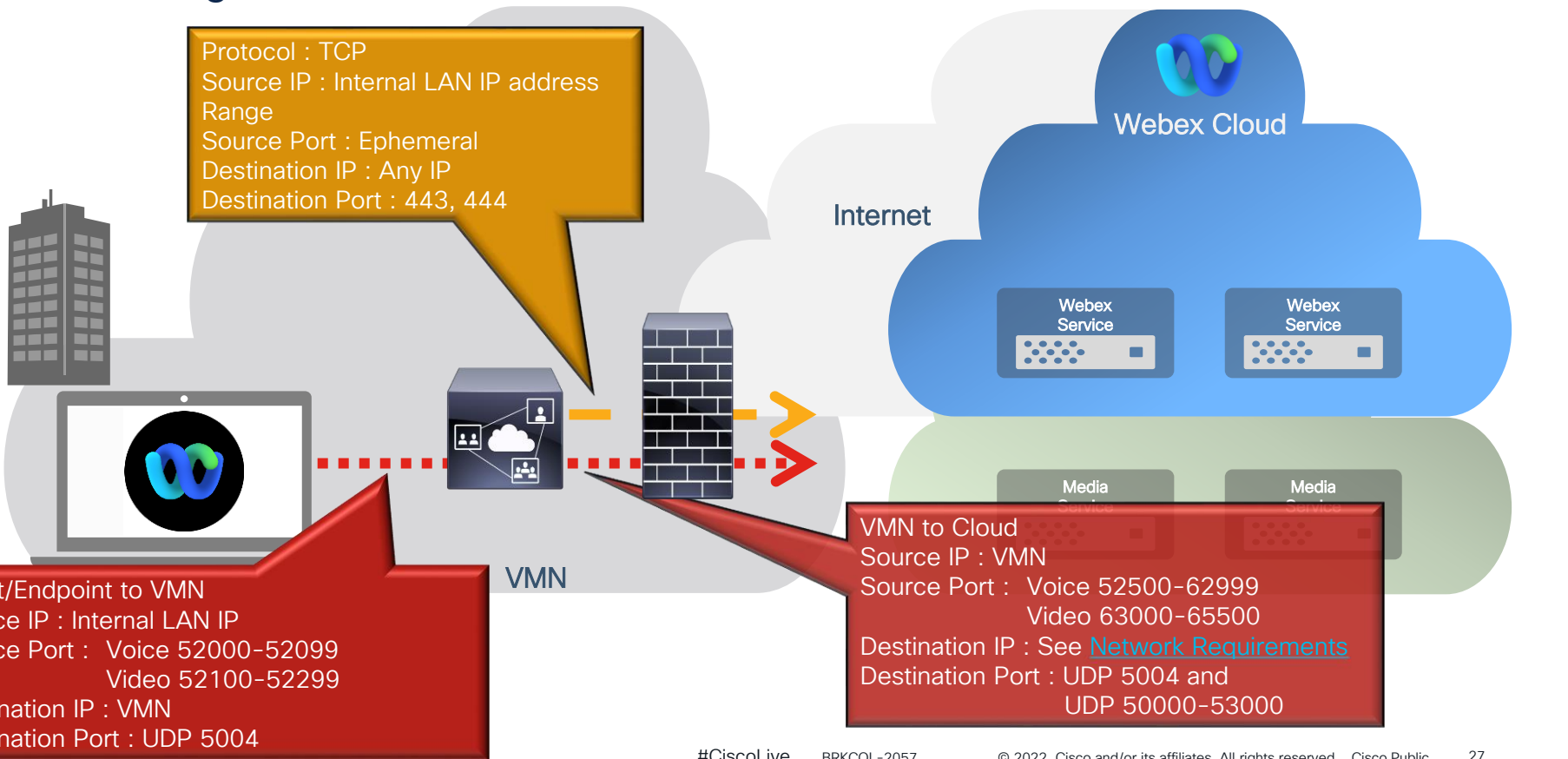
\* With Feature Toggle

**CISCO** *Live!*

# Protocols and Ports used by Webex

## Webex Edge Video Mesh

— Signaling/Other Control  
- - - Real Time Traffic



# Protocols and Ports used by Webex

## Webex Calling

— SIP Control  
— Other Control  
- - - Real Time Traffic

Usage: Device Config

Protocol : TCP

Source IP : Internal LAN IP address Range

Source Port : Ephemeral

Destination IP : Refer to doc below

Destination Port : 80, 443, 8443

Usage: Call Signaling

Protocol : TCP

Source IP : Internal LAN IP address Range

Source Port : 5060-5080

Destination IP : Refer to doc below

Destination Port : 8934

Protocol : UDP

Source IP : Internal LAN IP

Device Source Port : 19560-19660 |

Local GW Source Port : 8000-48000 (configurable using rtp-port range command)

Destination IP : Refer to doc

Destination Port : 5004 (STUN), 19560-65535 (SRTP)

Internet

Webex Cloud

Webex  
Service

Webex  
Service

Media  
Service

Media  
Service

Protocol : TCP

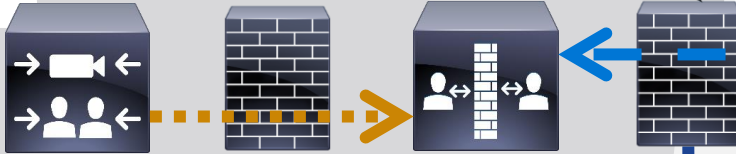
Reference link:

[Port Reference Information for Webex Calling](#)

# Protocols and Ports used by Cisco Expressway

SIP: TCP 5061 (Call signaling)  
HTTPS: TCP 8443 (Visual voicemail, directory)  
XMPP: TCP 5222 (IM & Presence)  
Media: UDP 36000 to 59999 (Voice and video)  
TURN server control: UDP 3478 - 3483  
TURN server media : UDP 24000 - 24999

No inbound port required to be opened on the internal firewall

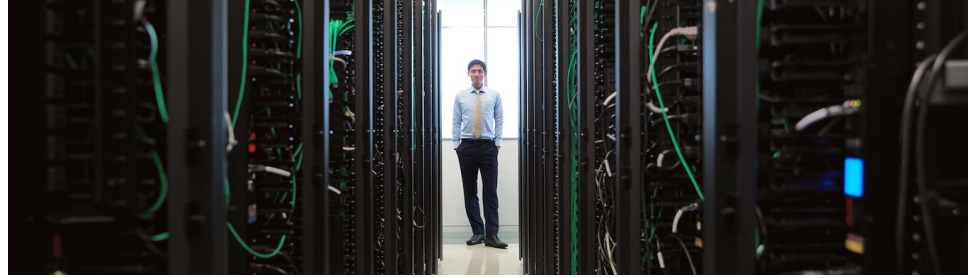


SIP: TCP 7001, 7003  
Traversal Media: UDP 2776-2777 or 36000-36011  
XMPP: TCP 7400  
HTTPS (tunneled over SSH between Expressway-C and Expressway-E): TCP 2222

Refer to [Cisco Expressway IP Port Usage Configuration Guide](#)

# Conclusion

# Conclusion



- Most Webex Traffic is inside-initiated
- Return traffic is automatically allowed
- Allow outbound UDP for media for best media quality
  - Avoid TCP and especially TLS with proxy
- You can restrict outbound traffic mainly by using:
  - Port and IP subnet filtering for media
  - URL filtering for signaling
- For even more security and media quality, you can also deploy Webex Edge connect and/or Webex Edge Video Mesh

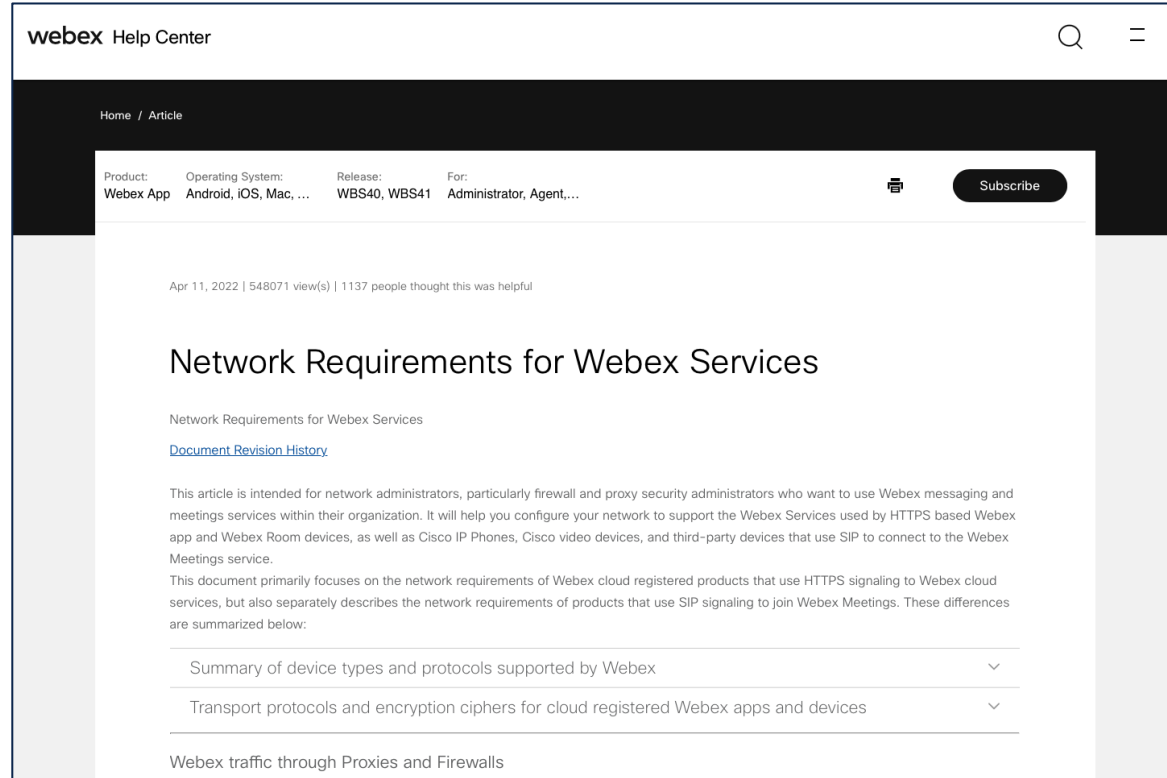
# Links to visit regularly / to subscribe

## Network Requirements for Webex Services

What are the **Webex media IP addresses** that should be allowed through the firewall?

What **domains** should be allowed in the proxy for proper Webex operations?

For answers to these questions and for more information about Webex services network requirements, refer to the *Network Requirements for Webex Services* article



The screenshot shows the Webex Help Center interface. At the top, there's a navigation bar with 'webex Help Center', a search icon, and a menu icon. Below this is a breadcrumb trail 'Home / Article'. A metadata bar contains fields for Product (Webex App), Operating System (Android, iOS, Mac, ...), Release (WBS40, WBS41), and For (Administrator, Agent,...), along with a 'Subscribe' button. The main content area shows the article title 'Network Requirements for Webex Services' with a date and view count. Below the title is a link to 'Document Revision History'. The article text explains its purpose for network administrators and lists topics like device types, transport protocols, and traffic through proxies and firewalls.

webex Help Center

Home / Article

Product: Webex App | Operating System: Android, iOS, Mac, ... | Release: WBS40, WBS41 | For: Administrator, Agent,...

Apr 11, 2022 | 548071 view(s) | 1137 people thought this was helpful

### Network Requirements for Webex Services

Network Requirements for Webex Services

[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:

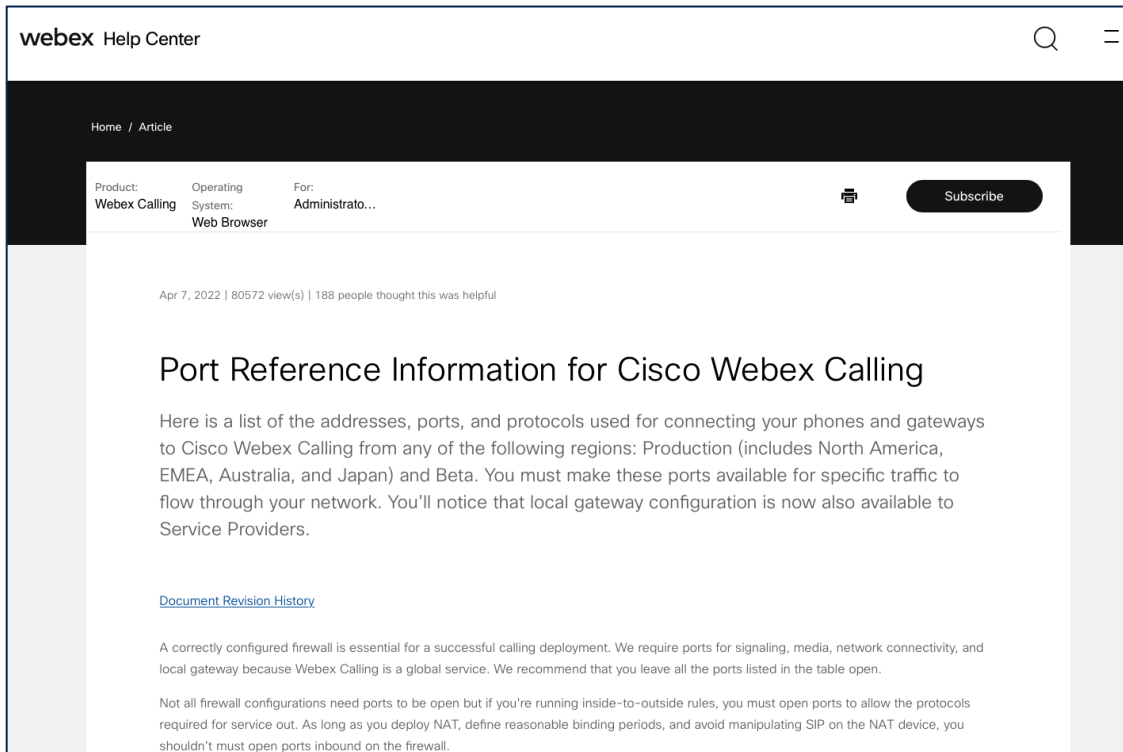
- Summary of device types and protocols supported by Webex
- Transport protocols and encryption ciphers for cloud registered Webex apps and devices

Webex traffic through Proxies and Firewalls



# Links to visit regularly / to subscribe

## Port Reference Information for Cisco Webex Calling



The screenshot shows the Cisco Webex Help Center interface. At the top, the header reads "webex Help Center" with a search icon and a menu icon. Below the header, a breadcrumb trail shows "Home / Article". The main content area has a dark header with "Product: Webex Calling", "Operating System: Web Browser", and "For: Administrato...". A "Subscribe" button is visible on the right. The article title is "Port Reference Information for Cisco Webex Calling". Below the title, it says "Apr 7, 2022 | 80572 view(s) | 188 people thought this was helpful". The article text begins with "Here is a list of the addresses, ports, and protocols used for connecting your phones and gateways to Cisco Webex Calling from any of the following regions: Production (includes North America, EMEA, Australia, and Japan) and Beta. You must make these ports available for specific traffic to flow through your network. You'll notice that local gateway configuration is now also available to Service Providers." A link for "Document Revision History" is provided. The article concludes with a paragraph about firewall configuration: "A correctly configured firewall is essential for a successful calling deployment. We require ports for signaling, media, network connectivity, and local gateway because Webex Calling is a global service. We recommend that you leave all the ports listed in the table open. Not all firewall configurations need ports to be open but if you're running inside-to-outside rules, you must open ports to allow the protocols required for service out. As long as you deploy NAT, define reasonable binding periods, and avoid manipulating SIP on the NAT device, you shouldn't must open ports inbound on the firewall."

# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](https://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

### Cisco Guided Study Groups

180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*



#CiscoLive

# Appendix

# Domains and URLs to allow in FW/Proxy

REFERENCE

## Mandatory URLs to allow in Proxy/FW

Reference:

[Network Requirements](#) Webex help article

Domain URLs	Description	Services
<ul style="list-style-type: none"><li>*.wbx2.com</li><li>*.ciscospark.com</li></ul>	<p>Webex micro-services, for example :</p> <ul style="list-style-type: none"><li>• Messaging service</li><li>• File management service</li><li>• Key management service</li><li>• Software upgrade service</li><li>• Profile picture service</li></ul> <ul style="list-style-type: none"><li>• Whiteboarding service</li><li>• Proximity service</li><li>• Presence service</li><li>• Registration service</li><li>• Calendaring service</li><li>• Search service</li></ul>	All
<ul style="list-style-type: none"><li>*.webex.com</li><li>*.cisco.com</li></ul>	<ul style="list-style-type: none"><li>• Webex Meetings services</li><li>• Identity provisioning</li><li>• Identity storage</li><li>• Authentication</li></ul> <ul style="list-style-type: none"><li>• OAuth services</li><li>• Device onboarding</li><li>• Cloud Connected UC</li></ul>	All
<ul style="list-style-type: none"><li>*.webexcontent.com</li></ul>	<ul style="list-style-type: none"><li>• User files</li><li>• Transcoded files</li><li>• Images</li><li>• Screenshots</li><li>• Whiteboard content</li><li>• Client &amp; device logs</li></ul> <ul style="list-style-type: none"><li>• Profile pictures</li><li>• Branding logos</li><li>• Log files</li><li>• Bulk CSV export files &amp; import files (Control Hub)</li></ul>	All



# Domains and URLs to allow in FW/Proxy

REFERENCE

Optional URLs to allow in Proxy/FW, based on services/functions used (1/2)

Domain URLs	Description	Services
*.accompany.com	<ul style="list-style-type: none"><li>People Insights Integration</li></ul>	Webex Apps
*.sparkpostmail1.com *.sparkpostmail.com	<ul style="list-style-type: none"><li>e-mail service for newsletters, registration info, announcements</li></ul>	All
*.giphy.com	<ul style="list-style-type: none"><li>Allows users to share GIF images.</li></ul>	Webex App
safebrowsing.googleapis.com	<ul style="list-style-type: none"><li>Used to perform safety-checks on URLs before unfurling them in the message stream.</li></ul>	Webex App
speech.googleapis.com texttospeech.googleapis.com speech-services-manager-a.wbx2.com	<ul style="list-style-type: none"><li>Google Speech Services. Used by Webex Assistant to handle speech recognition and text-to-speech.</li></ul>	Webex Devices
msftncsi.com/ncsi.txt captive.apple.com/hotspot-detect.html	<ul style="list-style-type: none"><li>Third-party internet connectivity check to identify cases where there is a network connection, but no connection to the Internet.</li></ul>	Webex App

Reference: [Network Requirements](#) Webex help article

# Domains and URLs to allow in FW/Proxy

REFERENCE

Optional URLs to allow in Proxy/FW, based on services/functions used (2/2)

Domain URLs	Description	Services
*.appdynamics.com *.eum-appdynamics.com	<ul style="list-style-type: none"><li>Performance tracking, error and crash capture, session metrics</li></ul>	Webex App Webex Web App
*.amplitude.com	<ul style="list-style-type: none"><li>A/B testing &amp; metrics</li></ul>	Webex Web App Webex Android App
*.vbrickrev.com	<ul style="list-style-type: none"><li>This domain is used by attendees viewing Webex Events Webcasts</li></ul>	Webex Events
*.slido.com *.sli.do *.data.logentries.com	<ul style="list-style-type: none"><li>Used for Slido PPT add-in and to allow Slido webpages to create polls/quizzes in pre-meeting</li></ul>	All
*.quovadisglobal.com *.digicert.com *.godaddy.com *.identrust.com *.lencr.org	<ul style="list-style-type: none"><li>Used to request Certificate Revocation Lists from these Certificate Authorities</li></ul>	All

Reference: [Network Requirements](#) Webex help article

# Domains and URLs to allow in FW/Proxy

REFERENCE

## Webex Calling URLs to allow in Proxy/FW (1/2)

Domain URLs	Description	Services
*.webexcallingpbx.com	<ul style="list-style-type: none"><li>Webex authorization micro-services for cross-launch from Control Hub to Calling Admin Portal.</li></ul>	Control Hub
*.webexcallingpbx.com.au	<ul style="list-style-type: none"><li>Webex Calling services in Australia.</li></ul>	Webex Calling
*.webexcallingpbx.eu	<ul style="list-style-type: none"><li>Webex Calling services in Europe.</li></ul>	Webex Calling
*.webexcallingpbx.net	<ul style="list-style-type: none"><li>Calling client configuration and management services.</li></ul>	Webex Apps
*.cisco.com	<ul style="list-style-type: none"><li>For phone activation and provisioning</li></ul>	MPP Phones, Control Hub
*.ucmgmt.cisco.com	<ul style="list-style-type: none"><li>Webex Calling services</li></ul>	Control Hub
*.webex.com	<ul style="list-style-type: none"><li>Webex Core Services for Calling, Meeting, and Messaging like Authentication, etc.</li></ul>	Webex Calling
*.wbx2.com and *.ciscospark.com	<ul style="list-style-type: none"><li>Webex micro-services, like Software upgrade service</li></ul>	Webex Calling

For the latest info: [Port Reference Information for Cisco Webex Calling](#)

# Domains and URLs to allow in FW/Proxy

REFERENCE

## Webex Calling URLs to allow in Proxy/FW (2/2)

Domain URLs	Description	Services
*.appdynamics.com *.enum-appdynamics.com	<ul style="list-style-type: none"><li>Performance tracking, error and crash capture, session metrics.</li></ul>	Control Hub
*.huron-dev.com	<ul style="list-style-type: none"><li>Webex Calling micro services like toggle services, phone number ordering, and assignment services.</li></ul>	Control Hub
*.sipflash.com	<ul style="list-style-type: none"><li>Device management services (mostly for US)</li></ul>	Webex Apps
*.walkme.com *.walkmeusercontent.com	<ul style="list-style-type: none"><li>Webex user guidance client. Provides onboarding and usage tours for new users.</li></ul>	Webex Apps

For the latest info: [Port Reference Information for Cisco Webex Calling](#)

# HTTP Traffic Inspection with Destinations to allow and TLS Intercept

REFERENCE

Webex Hybrid Services URLs to allow in Proxy/FW

Domain URLs	Description	Services
*.docker.com *.docker.io	<ul style="list-style-type: none"><li>Hybrid Services Containers</li></ul>	Video Mesh Node Hybrid Data Security Node
*s3.amazonaws.com	<ul style="list-style-type: none"><li>Log File uploads</li></ul>	Video Mesh Node Hybrid Data Security Node
*.cloudconnector.webex.com	<ul style="list-style-type: none"><li>User Synchronization</li></ul>	Directory Connector

Reference: [Network Requirements](#) Webex help article

# Webex Clients – Other Security Features

Config Type	Webex Meetings Mobile	Webex Meeting Desktop	Webex Room Devices	Webex Board	Webex App Windows	Webex App Mac	Webex App iOS	Webex App Android
802.1x								
TLS Intercept								
CDP								
Media over HTTPS								

# Proxy Configuration

Config Type	Webex Meetings Mobile	Webex Meeting Desktop	Webex Room Devices	Webex Board	Webex App Windows	Webex App Mac	Webex App iOS	Webex App Android
Manual Config								
GPO								
PAC								
WPAD								

Note: Webex Calling supports Web Proxy only with the Webex App

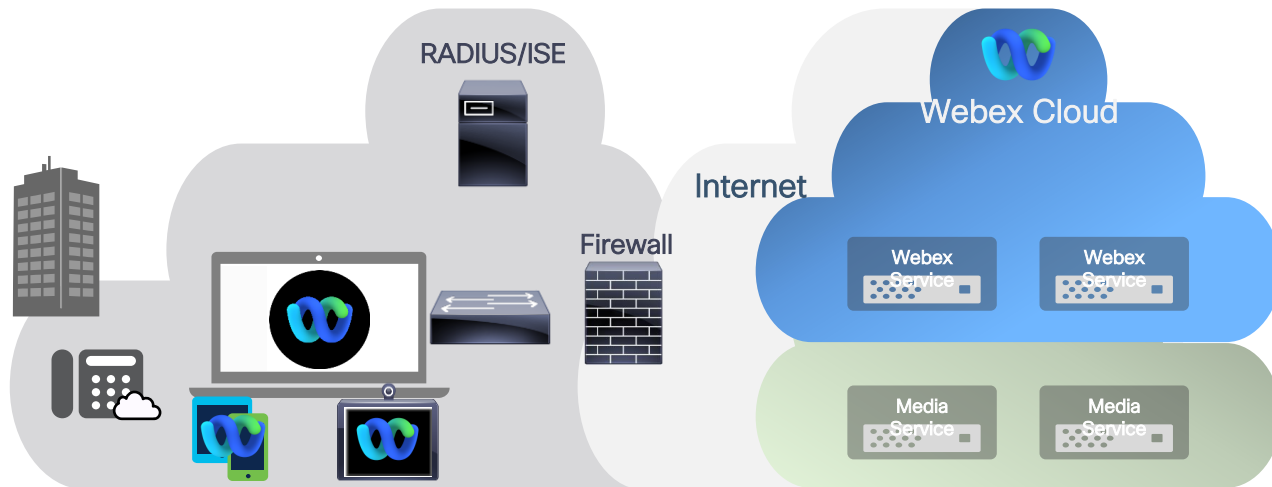
# Proxy Authentication

Config Type	Webex Meetings Mobile	Webex Meeting Desktop	Webex Room Devices	Webex Board	Webex App Windows	Webex App Mac	Webex App iOS	Webex App Android
No Auth								
Basic								
Digest								
NTLM								
Negotiate								

Note: Webex Calling supports Web Proxy only for the Webex App



# 802.1x



- 802.1x supported on
  - Webex App and Webex Meetings App (Windows, Mac, iOS, Android, Web, via OS)
  - Webex Room Devices and Webex Board (EAP-FAST, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-TTLS)
  - Cisco IP Phones 7800/8800 with Multiplatform Phone firmware

# A note about Webex App and Webex Devices



Webex Devices include Webex Room Series, Board Series and Desk Series



Webex Meetings App in this context is our previous meetings app still widely deployed and used.

Webex App  
(Workloads)









Webex App (Teams) refers to the native calling functionality for Webex App. It is used for Webex Space Meetings, 1:1 calls to a Webex Account holder (“Call on Webex” calling option in Webex App) as well as SIP URI dialing. **This workload was formerly accomplished with Webex Teams.**

Webex App (Meetings) Full-Featured Meetings or Meetings Experience is a feature enhancement to Webex App. When you start or join a Webex scheduled or Personal Room meeting from the Webex app, you get access to advanced features. This workload was formerly accomplished with **Webex Meetings Desktop and Mobile App**

# Media Signatures for Cisco Webex App and Webex Devices

Client/Device to Cloud (Reverse for Cloud to Client/Device)







Source IP	Destination IP	Source UDP Ports	Destination UDP Ports	Recommended DSCP	Media Type
Webex App* 	Webex cloud and Video Mesh Media Services	52000 to 52049	5004	EF	Audio
Webex App* 	Webex cloud and Video Mesh Media Services	52100 to 52199	5004	AF41	Video
Webex App (Meetings)** 	Webex cloud	52000 to 52049	9000	EF	Audio
Webex App (Meetings)** 	Webex cloud	52100 to 52199	9000	AF41	Video
Webex Devices 	Webex cloud and Video Mesh Media Services	52050 to 52099	5004	EF	Audio
Webex Devices 	Webex cloud and Video Mesh Media Services	52200 to 52299	5004	AF41	Video

\* Webex App for Windows requires Org feature enablement

\*\* Webex App (Meetings) for ALL platforms requires Org feature enablement

# Media Signatures for Cisco Webex App and Webex Devices

Client/Device to Cloud (Reverse for Cloud to Client/Device)

Source IP		Destination IP	Source UDP Ports	Destination UDP Ports		
Webex App*		Webex cloud and Video Mesh Media Services	52000 to 52049	5004		
Webex App*		Webex cloud and Video Mesh Media Services	52100 to 52199	5004		
Webex App (Meetings)**		Webex cloud	52000 to 52049	9000	EF	Audio
Webex App (Meetings)**		Webex cloud	52100 to 52199	9000		
Webex Devices		Webex cloud and Video Mesh Media Services	52050 to 52099	5004		
Webex Devices		Webex cloud and Video Mesh Media Services	52200 to 52299	5004	AF41	Video

Webex App And Webex Devices Audio source ports are separate but combined form a contiguous block to facilitate firewall or ACL configurations **52000 to 52099**







Webex App And Webex Devices Video source ports are separate but combined form a contiguous block to facilitate firewall or ACL configurations **52100 to 52299**

\* Webex App for Windows requires Org feature enablement

\*\* Webex App (Meetings) for ALL platforms requires Org feature enablement

# Media Signatures for Cisco Webex App and Webex Devices

Client/Device to Cloud (Reverse for Cloud to Client/Device)

Source IP		Destination IP	Source UDP Ports	Destination UDP Ports	Recommended DSCP	Media Type
Webex App*		Webex cloud and Video Mesh Media Services	52000 to 52049	5004	EF	Audio
Webex App*		Webex cloud and Video Mesh Media Services	52100 to 52199	5004	EF	Audio
Webex App (Meetings)**		Webex cloud	52000 to 52049	9000	EF	Audio
Webex App (Meetings)**		Webex cloud	52100 to 52199	9000	EF	Audio
Webex Devices		Webex cloud and Video Mesh Media Services	52050 to 52099	5004	EF	Audio
Webex Devices		Webex cloud and Video Mesh Media Services	52200 to 52299	5004	AF41	Video

Webex App for Windows requires Org feature enablement

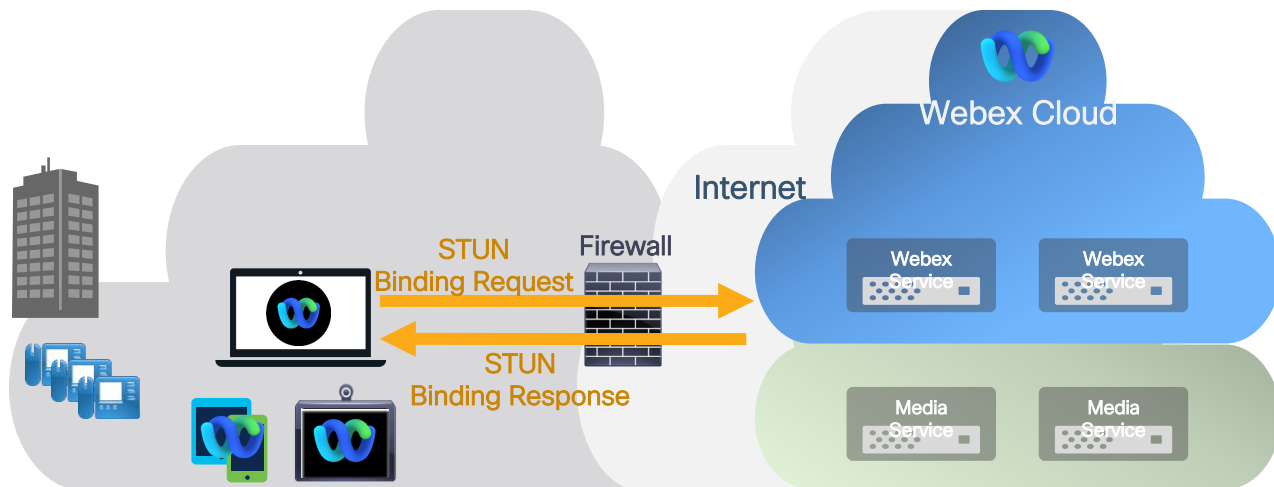
Webex App (Meetings) for ALL platforms requires Org feature enablement

\* Webex App for Windows requires Org feature enablement

\*\* Webex App (Meetings) for ALL platforms requires Org feature enablement

# STUN – Session Traversal Utilities for NAT

- Allows NAT traversal
- Used for media node discovery



- Allows to dynamically open firewall pinholes:
  - Allows to create firewall bindings by sending outbound STUN probes and allow corresponding inbound traffic (return traffic)
  - Allows the FW pinhole to stay open by periodically sending UDP probes
- STUN inspection can be used to dynamically open ports on the firewall

# Media not sent to Proxy with Webex Devices

- For Webex devices (Webex Board, Desk, or Room Series): Proxy server support is only for HTTP(S) signalling traffic. Media traffic (UDP/TCP/TLS) still needs direct access to the internet.
- <https://help.webex.com/en-us/article/no5dwuq/Connect-your-Cisco-Webex-Board,-Desk,-or-Room-Series-device-to-a-proxy-server>
- <https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/webex/webex-rooms-security-white-paper.pdf>