

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Collaboration Security

Exploring Webex Meetings Architecture, Security and
Navigating Secure Networking Environments

Nick Halbert-Lillyman – Solutions Engineer, Collaboration
BRKCOL-2528

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 November 15, 2024.



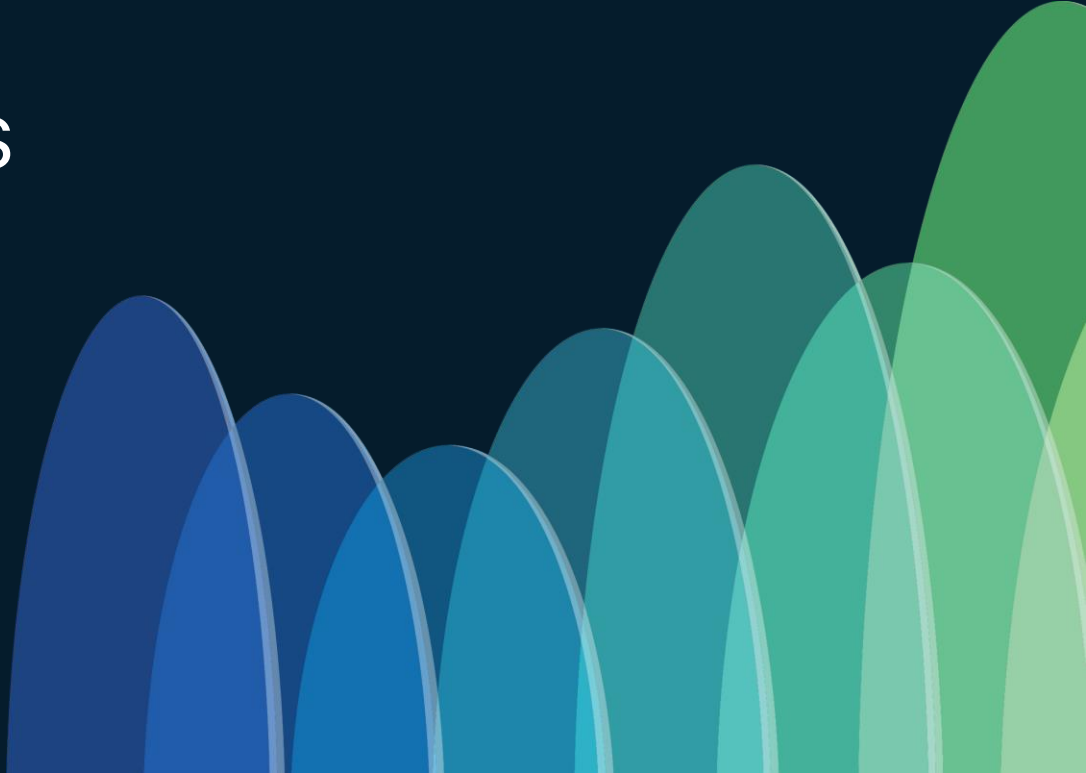
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2528>



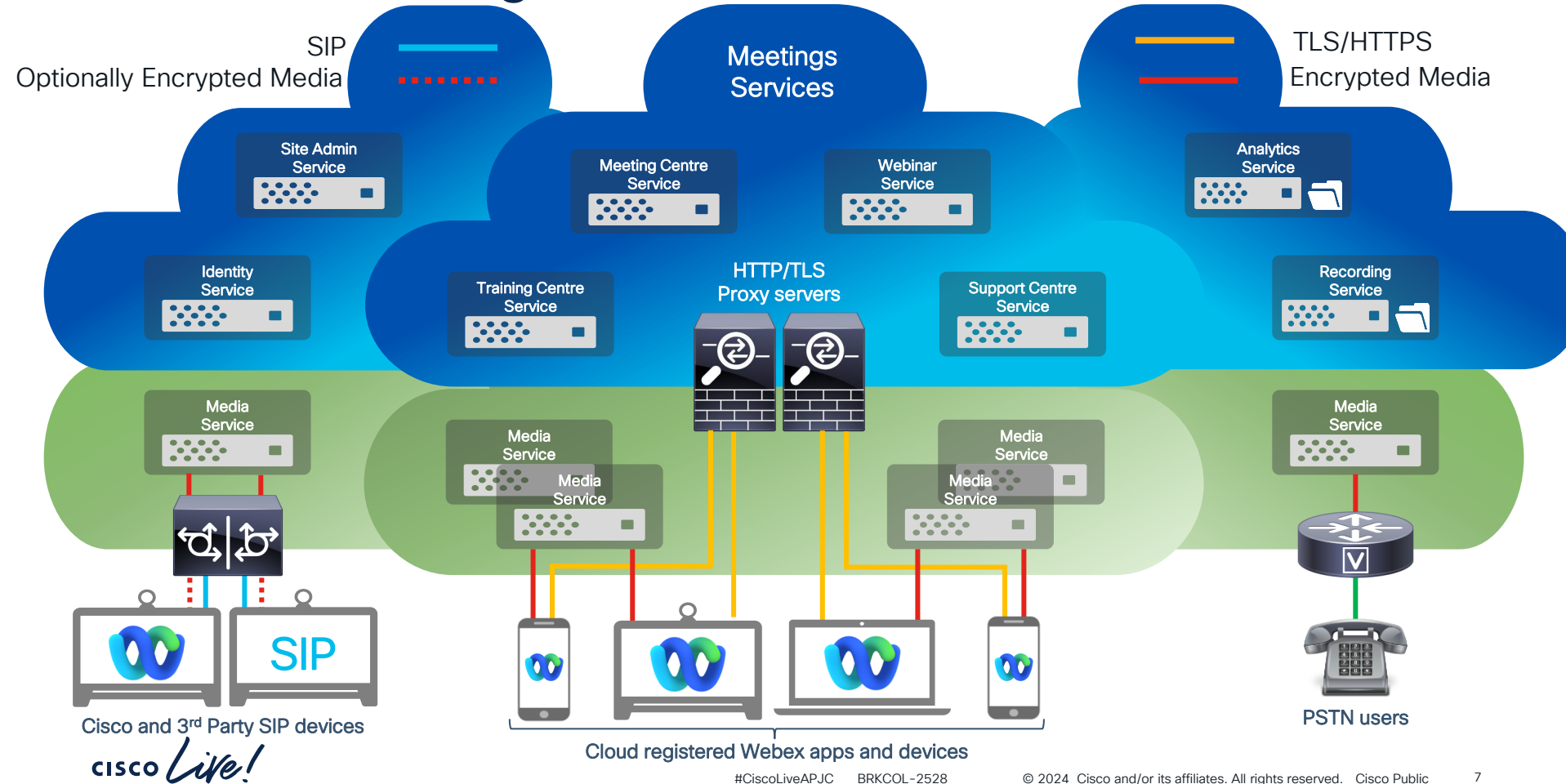
Agenda

- Webex Meetings platform and architecture
- Webex meeting types
- Webex meeting security features
- Fundamentals on firewall traversal
- Media and signaling considerations
- Traffic flows and network port usage
- Summary

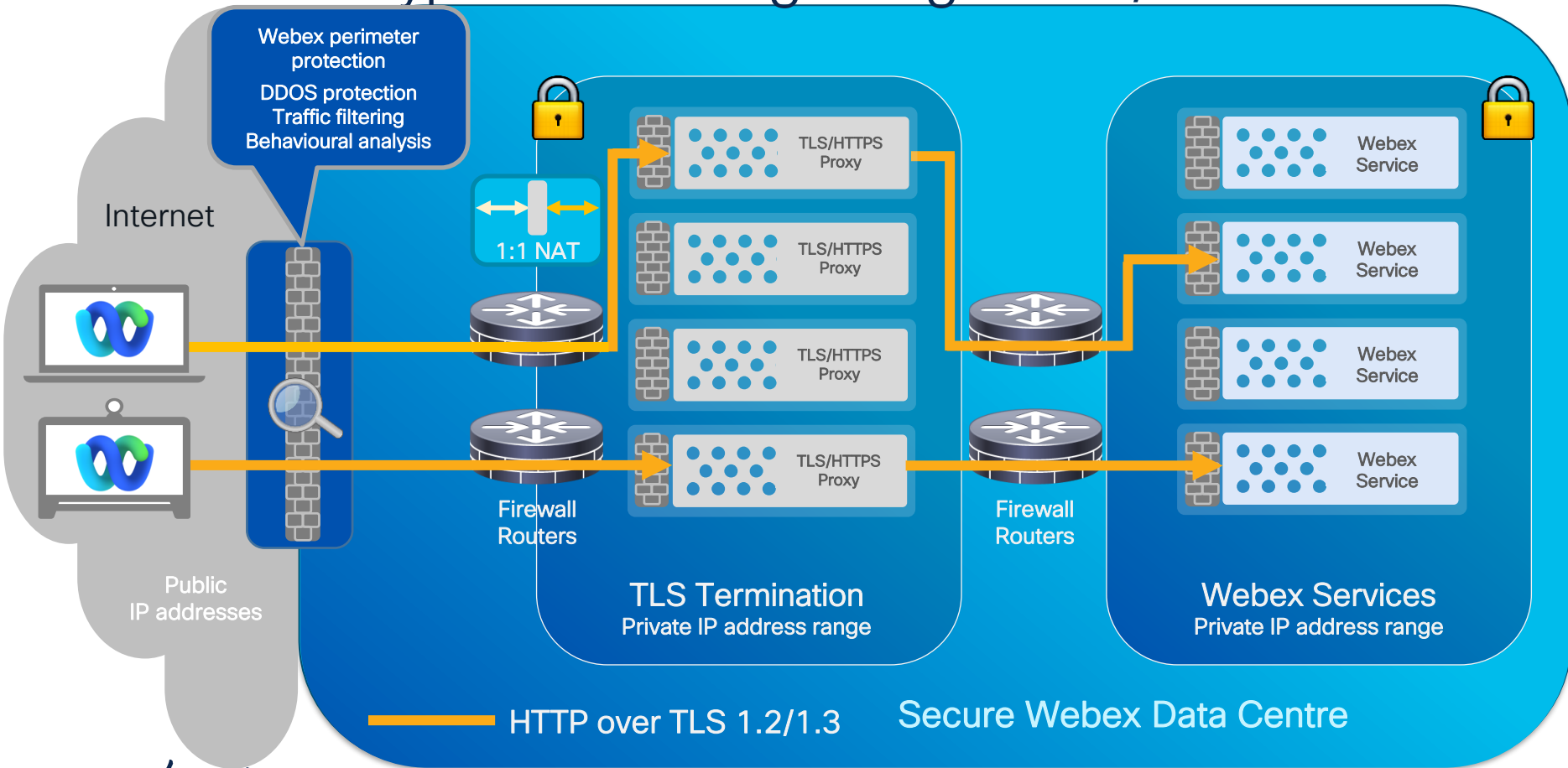
Webex Meetings Platform and Architecture



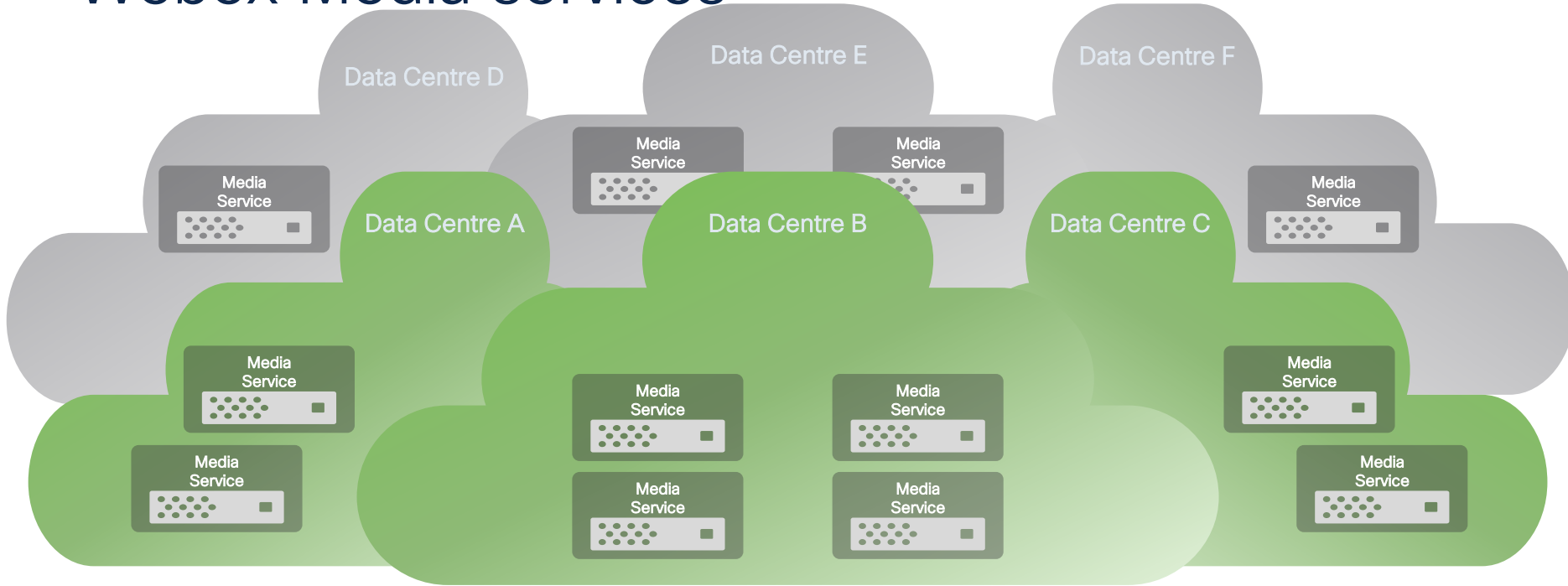
Webex Meetings architecture



Webex encrypted HTTP signaling – TLS/HTTPS traffic

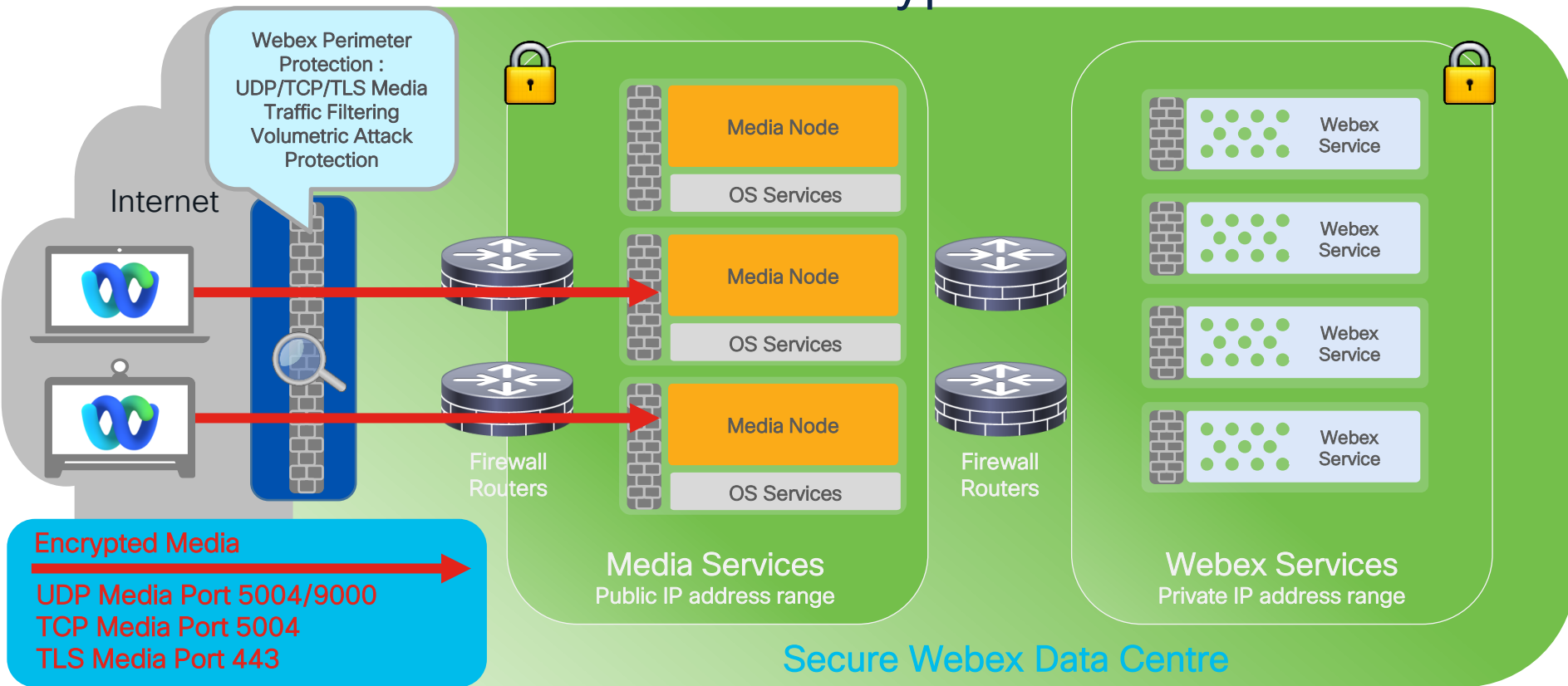


Webex Media services



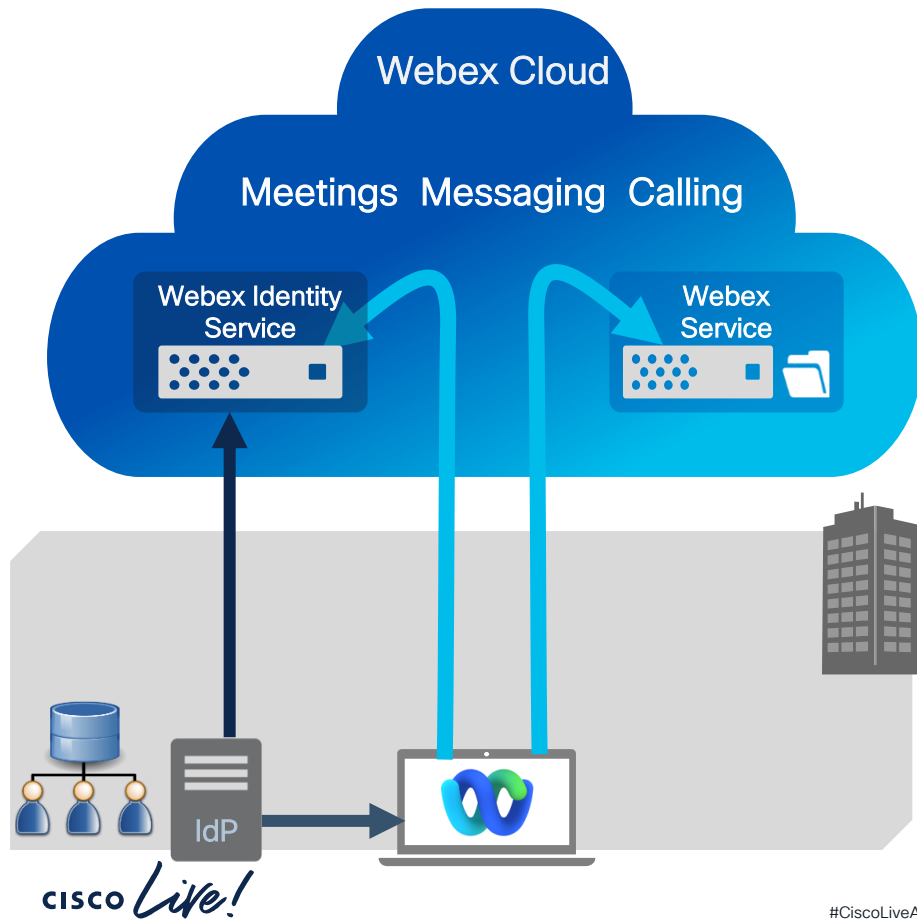
Webex Media services are globally distributed across multiple data centres
Media Server clusters in each data centre provide local and geographic redundancy
Media servers support real-time voice, video and content sharing
All media is encrypted

Webex Media Services: encrypted media



Webex Media encryption cipher : AEAD-AES-256-GCM

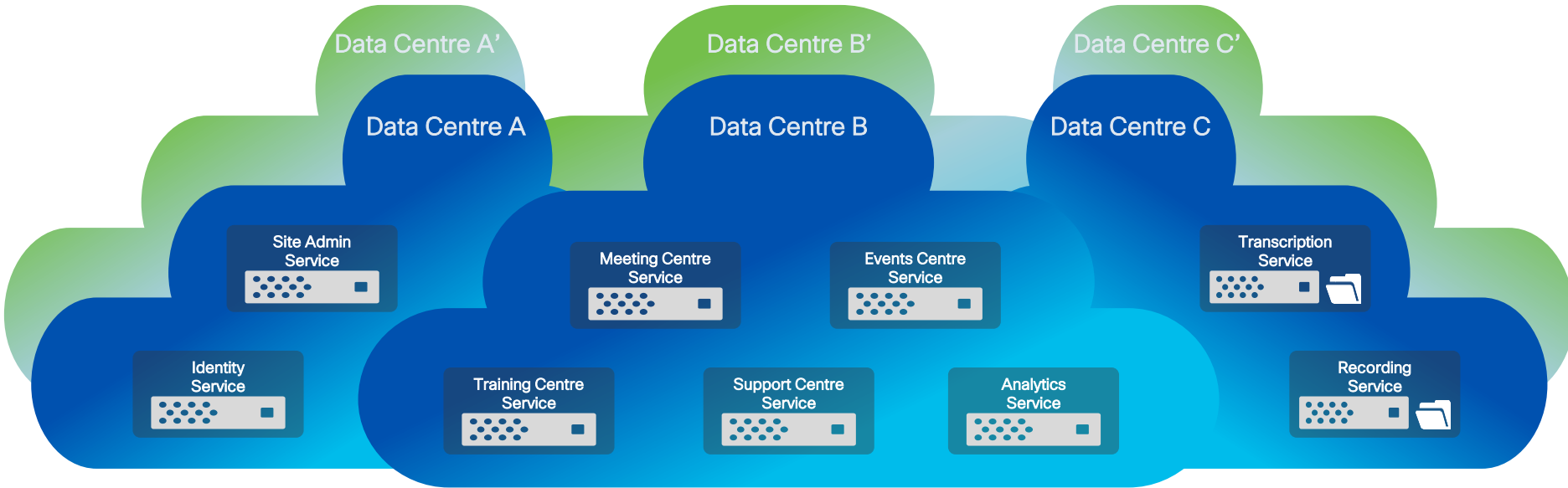
Webex app login and identity



- 1) Webex app establishes a secure TLS connection with the Webex Cloud
- 2) Webex Identity Service prompts User for an email ID
- 3) User Authenticated by Webex Identity Service, ***or*** Enterprise IdP (SSO)
- 4) Access Granted to Webex Services

*For More: Cisco Live Melbourne 2023 - BRKCOL-2007
Authentication, Authorization and
Provision for Cisco Collaboration
Paulo Jorge N. Correia*

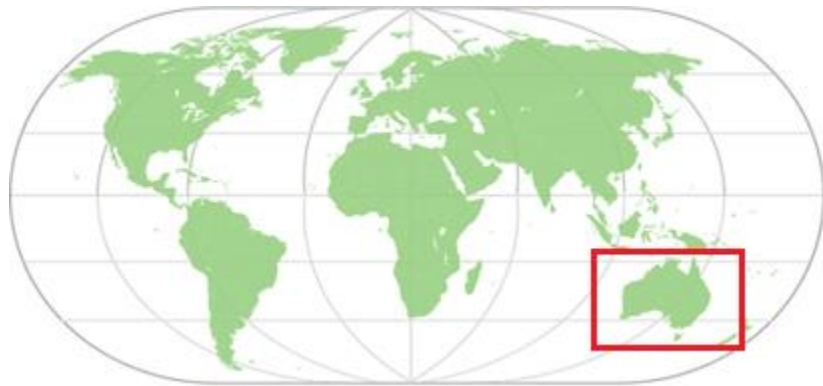
Webex Meetings regions and redundancy



- Webex Services for Webex Meetings/ Webinars / Training/ Support, identity, recording, transcription, are regionalised and replicated across independent data centres.
- User generated content (e.g. recordings, transcripts, uploaded files) is stored in the regional data center closest to a Customer's location as provided during the ordering process
- Webex Meetings regions: EU/ UK/ US/ Canada/ APAC/ Australia

Data residency for other Webex services

- Today - Webex Meetings usage, analytics, identity and billing information, including Webex Control Hub, served from additional global DCs in US/EU/Canada.
- Webex Messaging and Hybrid Calendar will also use these global DCs
- Australian customers currently use US DCs for these auxiliary functions
- Webex Calling and Contact Centre have additional regional data centres (including Australia)



Webex Suite : Australia data residency

Target Mid CY 25

Already exists

-  Calling
-  Meetings (Primary DC)
-  Webinars (Primary DC)
-  Contact Center
-  CPaaS

Coming soon!

-  Meetings (Secondary DC)
-  Webinars (Secondary DC)
-  Messaging + Calendar
-  Polling and Q&A
-  Identity
-  Analytics & Reporting



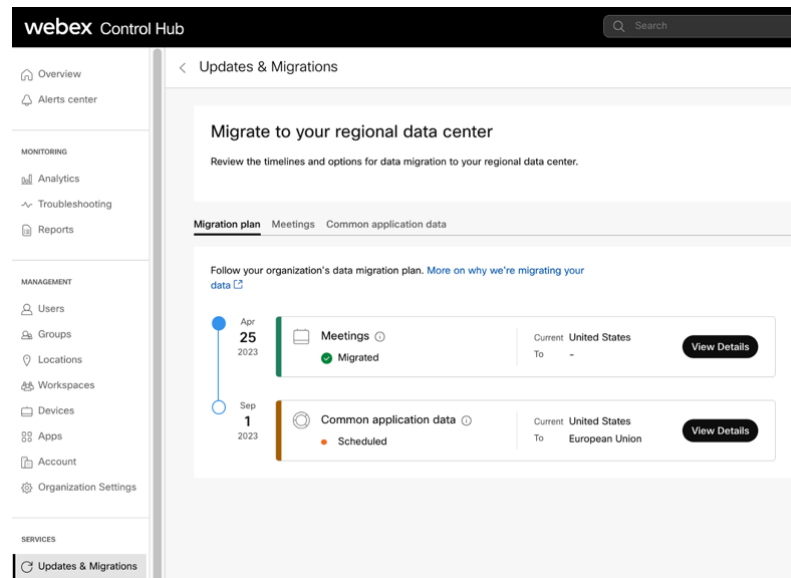
Identity + Analytics and Reporting will be first to be delivered – target Q1 2025

Identity and analytics data migration

US -> Australia

Self-service portal to enable existing customers to achieve data residency for user profiles, machine accounts and analytics

- Enable Australian customers to migrate their Common Identity (CI) location from US to Australia,.
- Fully automatic process once scheduled, with automatic rollback and email notification in case of errors



Messaging and Calendar Data Migration

US -> Australia

Target End of Q3Y25

Self-service portal to enable existing customers to achieve data residency for Messaging Content (Webex Spaces, messages, files etc.). This includes Hybrid Calendar.

- Enable Australian customers to migrate their Messaging data from US to Australia
- Fully automatic process once scheduled, with automatic rollback and email notification in case of errors

Migrate to your regional data center

Review the timelines and options for data migration to your regional data center.

Migration plan

Meetings

Common application data

Messaging

Follow your organization's data migration plan. [More on why we're migrating your data to the EU](#)

July 15 2021

Meetings

Migrated

Current: European Union

View details

Jan. 27 2022

Common application data

Migrated

Current: European Union

View details

Messaging

Available to schedule

Current: United States
To: European Union

View details

Webex IRAP assessment for Australia

- IRAP assesses security controls for a system (e.g. Webex) against documented security controls from the Information Security Manual (published by ASD).
- Targets security controls at a certain security level (e.g. OFFICIAL, PROTECTED etc). Especially relevant to public sector organisations
- Webex IRAP Assessment @ PROTECTED includes Webex Meetings, Messaging, Calling, Control Hub, Webex for Developers
- Available by application – contact your Cisco account team
- Webex Contact Center IRAP planned



Webex Meeting Types

Standard Meetings
End to End Encrypted Meetings
Private Meetings
Scheduled Meetings
Personal Room

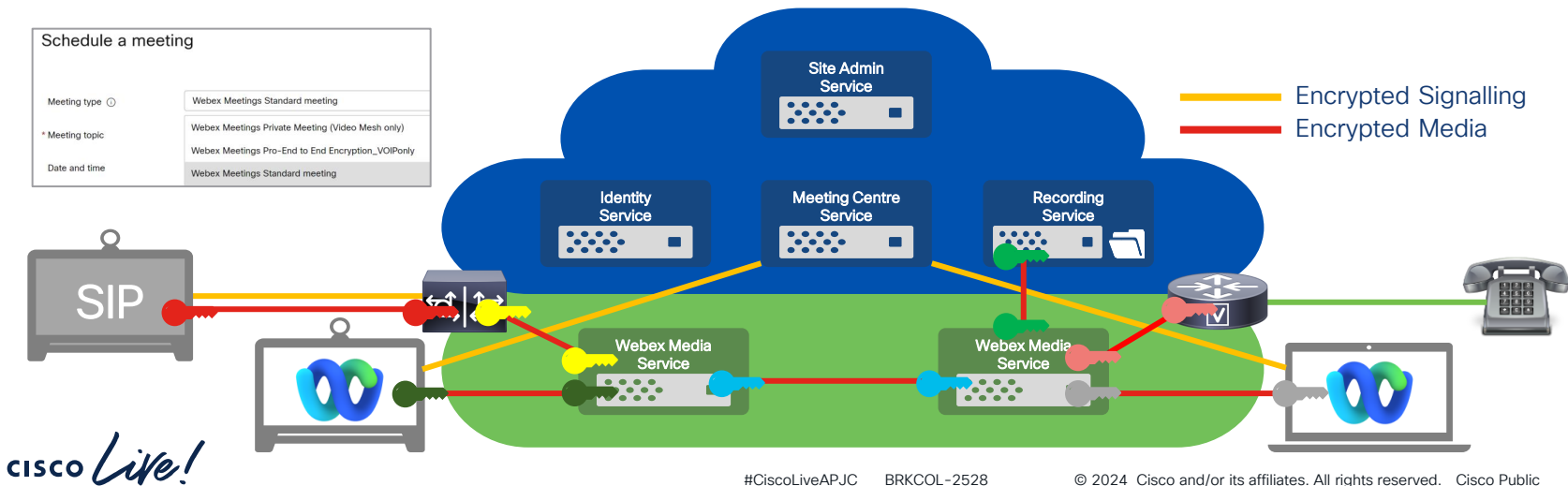
Encryption for standard Webex Meetings

With standard Webex Meetings, all signalling and media in the Webex cloud is encrypted
Webex apps and devices use encrypted signalling and encrypted media
SIP devices can encrypt signalling and media, PSTN audio is encrypted by the Webex cloud

With standard Webex Meetings, the cloud needs to access to encryption keys to decrypt SRTP media from SIP devices, PSTN gateways and for other services such as recording

Every vendor of cloud meeting services requires access to meeting encryption keys for SIP, H323, PSTN and other services

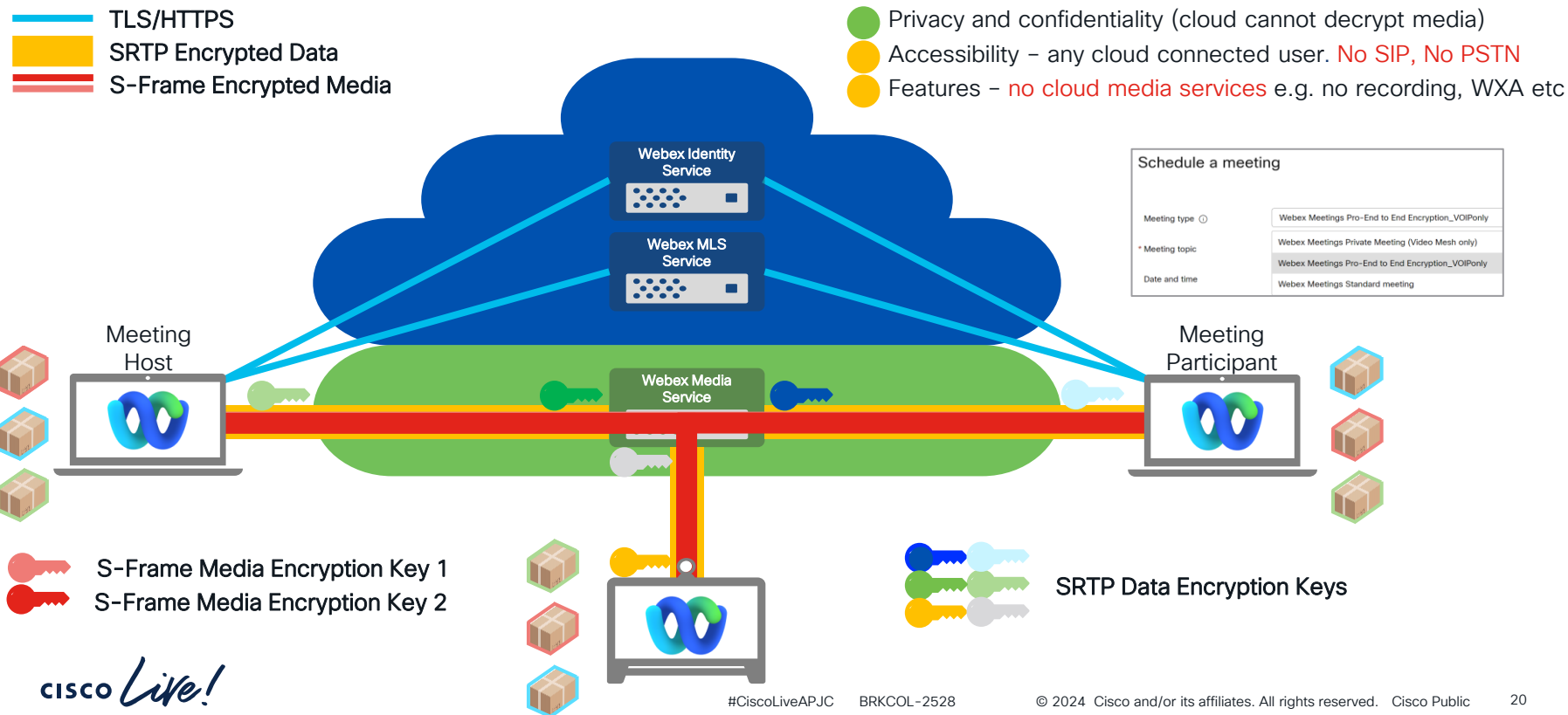
- Privacy and confidentiality (Hop by Hop encryption)
- Accessibility (Anyone : Cloud, SIP, PSTN users)
- Features (All : Recording, Transcripts, Webex Assistant etc)



Webex zero trust end to end encrypted meetings

With Webex Zero Trust E2E encrypted Meetings, the Webex cloud does not have access your meeting encryption key

For details see <https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html>



Zero trust security for Webex meetings

Summary of E2E encryption features

End to End Encryption meetings available to enterprise and consumer customers – no additional license
Supported by Webex App (desktop and mobile) and Webex devices
Up to 1000 participants
Audio Watermarking, Video Watermarking
Face recognition, Gesture recognition
In-Room interpretation, People presence detection
Proximity pairing, Background noise removal
Local Recording (Webex App)

Zero Trust E2EE does not give Webex access to meeting encryption keys. This means that cloud services and endpoints that need to decrypt meeting content cannot participate in E2EE meetings : e.g.

PSTN and SIP endpoints

Cloud Recording

Webex Assistant

Meeting Transcription, Real-time translation, Closed captioning, Highlights, Webex AI Assistant

Remote Desktop Control

Web Browser based Webex App

SX, DX, and MX series devices

Private Webex meetings

- All media is switched on-premises via Webex Video Mesh Node
- No media cascades to the Webex cloud
- Cloud registered Webex apps and devices always use encrypted signalling and encrypted media
- On Premise Webex and 3rd Party SIP apps and devices may use encrypted signalling and encrypted media

All apps and devices must have access to the Webex Video Mesh Node on premises

Schedule a meeting

Meeting type ⓘ

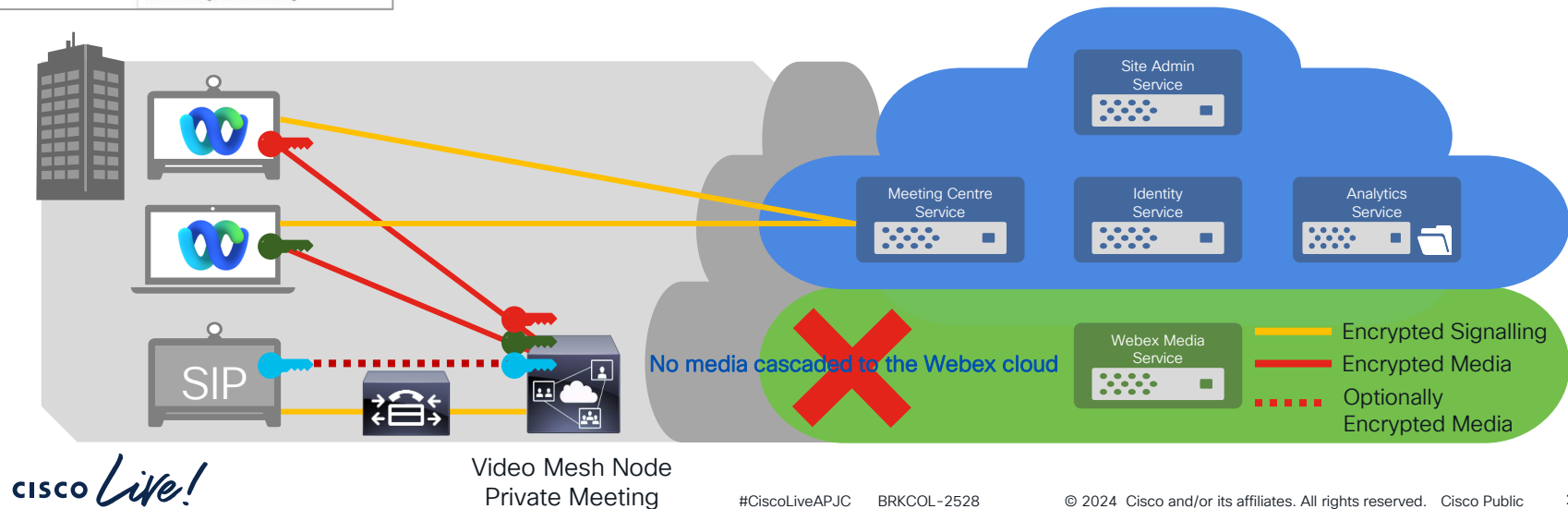
- Webex Meetings Private Meeting (Video Mesh only)
- Webex Meetings Private Meeting (Video Mesh only)
- Webex Meetings Pro-End to End Encryption_VOIPonly
- Webex Meetings Standard meeting

- Privacy and confidentiality - media kept on premises
- Accessibility - my org only : cloud and SIP based users
- Features - no cloud media services

Meeting type ⓘ

Webex Meetings Private Meeting (Video Mesh only)

This is a private meeting. All attendees must be members of the host organization and must be connected to its corporate network. They can only join the meeting from the Webex app or from an authenticated video system in the host organization.



Scheduled Webex meetings

- Multiple meeting types available (standard, private etc)
- One time meeting or recurring
- Password protected
- Auto lock feature
- Lobby controls
- Join before host controls
- Call in numbers
- Attendee mute controls
- Recording controls
- Enable breakout sessions
- Require invitees to register
- Simultaneous interpretation
- Meeting options
- Attendee privileges

The screenshot shows the 'Security' settings for a Webex meeting. The 'Meeting password' field contains 'sPmjBmc*839'. The 'Exclude password' checkbox is unchecked. The 'Automatic lock' section shows 'Automatically lock my meeting' set to 15 minutes after the meeting starts. The 'Unlocked meetings' section has a note that everyone in the organization can join unlocked meetings, and the 'Guests wait in the lobby until the host admits them' option is selected. The 'Join before host' section shows 'Attendees can join the meeting' set to 5 minutes before start time, and 'Attendees can connect to audio before start time' is unchecked. The 'Advanced options' section is expanded, showing 'View thumbnails', 'View any document', and 'View any page' all unchecked, and 'Contact operator privately' checked. Under 'Participate in private chat with', 'Host', 'Presenter', and 'Other participants' are all checked. 'Cancel' and 'OK' buttons are at the bottom right.

Security

* Meeting password

Exclude password ☐ Exclude password from email invitation

Automatic lock ⓘ ☐ Automatically lock my meeting 15 minutes after the meeting starts.

Unlocked meetings ⓘ Everyone in your organization can always join unlocked meetings.
When the meeting is unlocked,
☐ Guests can join the meeting
☒ Guests wait in the lobby until the host admits them
☐ Guests can't join the meeting

Join before host ☐ Attendees can join the meeting 5 minutes before start time
☐ Attendees can connect to audio before start time

Advanced options

☐ View thumbnails ⓘ
☐ View any document ⓘ
☐ View any page ⓘ
☒ Contact operator privately

Participate in private chat with
☒ Host
☒ Presenter
☒ Other participants

Cancel OK

Webex Personal Room meetings

- Personal Room Meetings
 - A persisted meeting
 - Always available
 - Activated by the host (or co-host)
- Limited security features :
 - Lobby (Admin controlled)
 - Lock (Admin/Host controlled)
 - CAPTCHA (Admin controlled)
- Mute attendee controls

A convenient meeting type, but recommended for meetings with trusted participants

The screenshot shows the 'My Personal Room' settings page in Webex. At the top, there are tabs for 'General', 'My Personal Room' (selected), 'Audio and Video', 'Scheduling', and 'Recording'. A light blue notification bar at the top states: 'Please note that your host PIN can now be found under the Audio and Video section.' Below this, the 'Personal Room name' is set to 'Tony Mulchrone's Personal Room' with a note that the name must be between 1 and 128 characters. The 'Personal Room link' is 'https://.webex.com/meet/abcdegh'. Under 'Automatic lock', the 'Automatically lock my meeting' checkbox is checked, set to '15' minutes after the meeting starts. A yellow warning box states: 'Based on your site settings, people who haven't signed in and external guests will be kept in the lobby until you admit them, whether your Personal Room is locked or unlocked.' Under 'Notification', the 'Notify me by email when someone enters my Personal Room lobby while I am away' checkbox is unchecked. Under 'Cohosts', the 'Allow cohosts for my Personal Room meetings' checkbox is checked, with a text box for 'Separate email addresses with a comma or semicolon'. Under 'Mute attendees', the 'Allow the host and cohosts to unmute participants (Moderated unmute mode)' checkbox is unchecked, 'Allow attendees to unmute themselves in the meeting' checkbox is checked, and the 'Always mute attendees when they join the meeting' checkbox is unchecked.

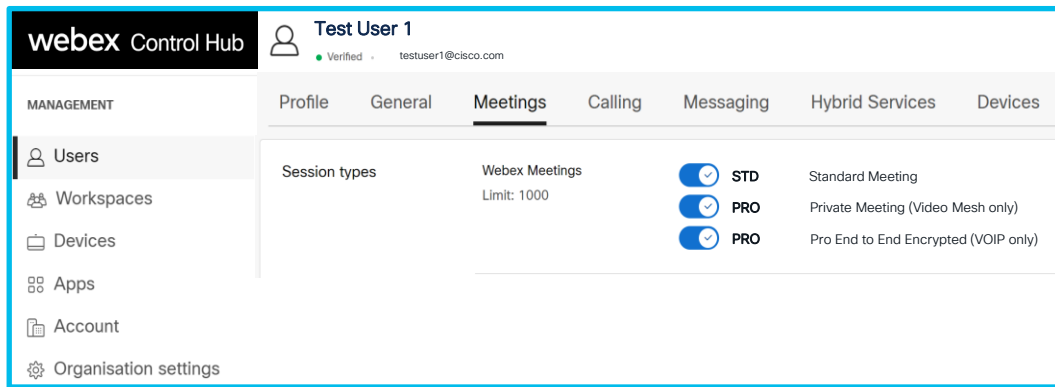
Assigning and selecting Webex meeting types

Webex Control Hub

Administrator can assign various default meeting session types to users

Administrator can also create new bespoke meeting session types and assign these to users

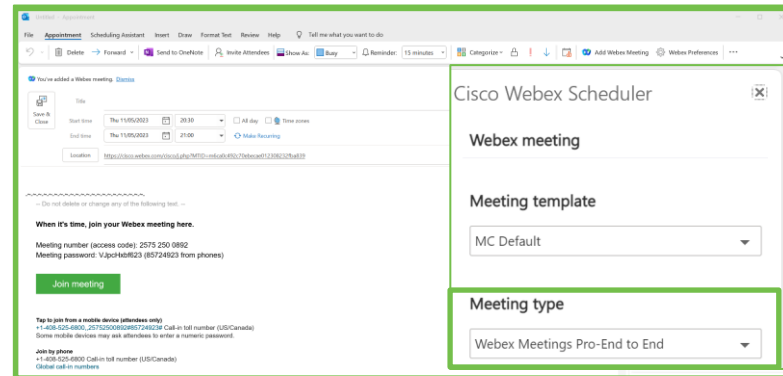
All available session types can be enabled/
disabled per user



Meeting Host/ Scheduler

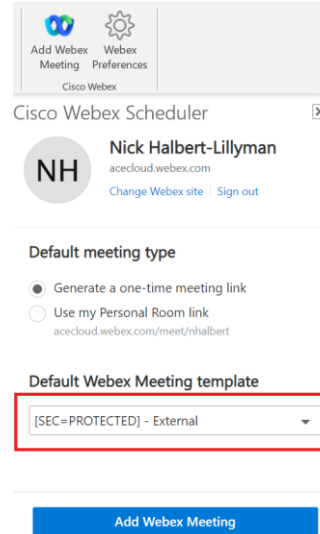
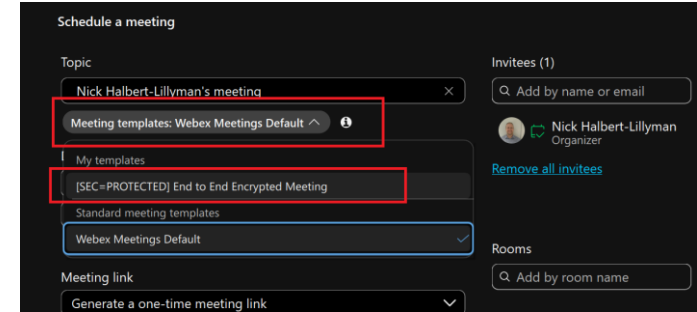
When scheduling a meeting, the user will see the selection of meeting session types assigned to them by the administrator

User selects their preferred meeting session type for the meeting



Webex Meeting templates

- Administrators can create and publish meeting templates based on certain meeting types and rules, and name them according to certain use cases
- E.g. Private or E2EE meeting for higher security classifications or other sensitive meetings
- Users can select appropriate template to use (Webex Scheduler in Outlook, Webex App or Web GUI)
- Users can also create their own templates, but cannot publish them to other users



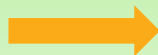
Webex Meeting Security Features

Secure meeting access : PSTN/ SIP/ cloud devices

*The richest meeting experience comes with the Webex app, but
Users can also join meetings from cloud registered Webex devices, SIP devices, phones...*

Cloud registered Webex devices

- Audio/ Video/ Desktop share
- Meeting Roster, Reactions,
- One Button to Push, Noise Reduction
- Webex Assistant, Closed Captions
- Recording etc



Cloud registered Webex device security

Webex recognises cloud registered devices and can apply security privileges such as Lobby bypass.

Also available for on-prem SIP with TLS domain verification

SIP devices

- Audio/ Video/ Desktop share



Security options for SIP devices and phone users

DTMF entered - meeting number & numeric password

PSTN/ IP Phones

- Audio only

Video system settings

Enforce numeric meeting password when joining

Phone settings

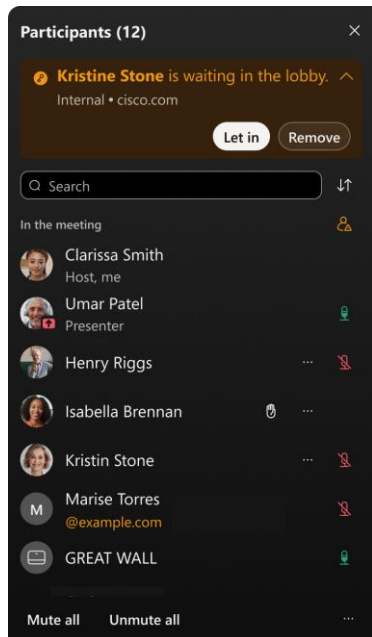
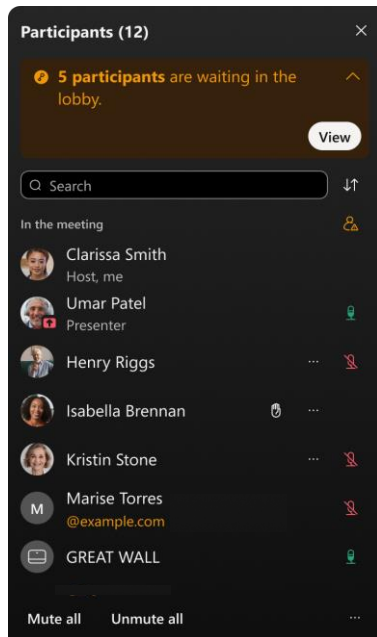
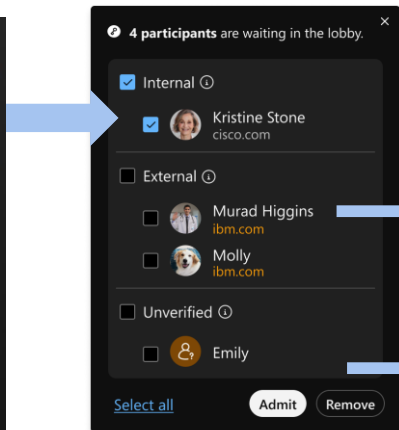
Require users to sign in before joining meeting

Enforce numeric meeting password when joining by phone

Webex Meetings: host controls

Admitting users from the lobby

Lobby: user categories and user identity information



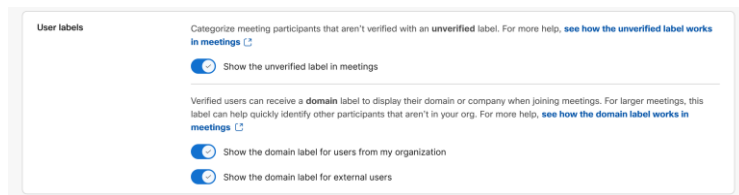
These users are signed in but are not part of your organization.

These participants aren't authenticated or signed in so Webex can't verify their identities.

Internal Users
(Authenticated)

External Users
(Authenticated)

Unverified Users
(Not Authenticated)
(Not Signed In)



New: disable/enable 'unverified' and domain labels in Control Hub

Webex Meetings security features: lock

 Automatically lock

☐ Automatically lock the meeting 15 minutes after the meeting starts

When a meeting is locked

☒ Everyone waits in the lobby until the host admits them

☐ No one can join the meeting

webex by cisco

Preferences

General **My Personal Room** Audio and Video Scheduling Recording

Home Calendar Recordings **Preferences** Insights Support Downloads Feedback

Personal Room name Nick Halbert-Lillyman's Personal Room

Automatic lock:  ☒ Automatically lock my meeting 5 minutes after the meeting starts.

0
5
10
15
20

Nick Halbert-Lillyman's Personal Room

 Automatically lock

☒ Automatically lock the meeting 5 minutes after the meeting starts

When a meeting is locked

☒ Everyone waits in the lobby until the host admits them

☐ No one can join the meeting

webex by cisco

Preferences

General **My Personal Room** Audio and Video Scheduling Recording

Home Calendar Recordings **Preferences** Insights Support Downloads Feedback

Personal Room name Nick Halbert-Lillyman's Personal Room

Automatic lock:  ☒ Automatically lock my meeting 5 minutes after the meeting starts.

 Based on your site settings, people who haven't signed in and external guests will be kept in the lobby until you admit them, whether your Personal Room is locked or unlocked.

Scheduled Meetings: Auto Admit feature

Authenticated, invited users and rooms listed on the meeting owner's calendar invite can join or start the meeting with or without host

Site admin – uninvited users:
wait in the lobby until the host admits them

Webex Meeting Security ⓘ

Auto admit All invited users can join the meeting.

Choose what happens for people who aren't on the invite:

☐ They can join the meeting

☒ They wait in the lobby until the host lets them in

☐ They can't join the meeting

☒ Participants in your organization can always join unlocked meetings



User page: scheduled meeting: auto admit

webex

Start a meeting Schedule a meeting

Home
Calendar
Recordings
Preferences
Insights
Support
Downloads
Feedback

Schedule a meeting

Security

Auto admit ⓘ All invited users can join the meeting.

Choose what happens for people who aren't on the invite:

☒ They wait in the lobby until the host lets them in

☐ They can't join the meeting

Uninvited users: cannot join the meeting

Webex Meeting Security ⓘ

Auto admit All invited users can join the meeting.

Choose what happens for people who aren't on the invite:

☐ They can join the meeting

☐ They wait in the lobby until the host lets them in

☒ They can't join the meeting

☒ Participants in your organization can always join unlocked meetings



User page: scheduled meeting: auto admit

webex

Start a meeting Schedule a meeting

Home
Calendar
Recordings
Preferences
Insights
Support
Downloads
Feedback

Schedule a meeting

Security

Auto admit ⓘ All invited users can join the meeting.

Choose what happens for people who aren't on the invite:

☒ They can't join the meeting

Recording – local and network based

Meeting host recording entitlements

Start/Stop – auto or manual

Record audio and content only, or audio, video and content

Recorded meeting file editing options: include/exclude:
Chat, Q&A, polling, participants, transcripts

Admin meeting recording options

Recordings can be password protected

Recordings can be streamed or downloaded

Downloading of recordings can be blocked

Viewing can be restricted to signed in users only

Network based recordings

Stored in regional Webex data centres

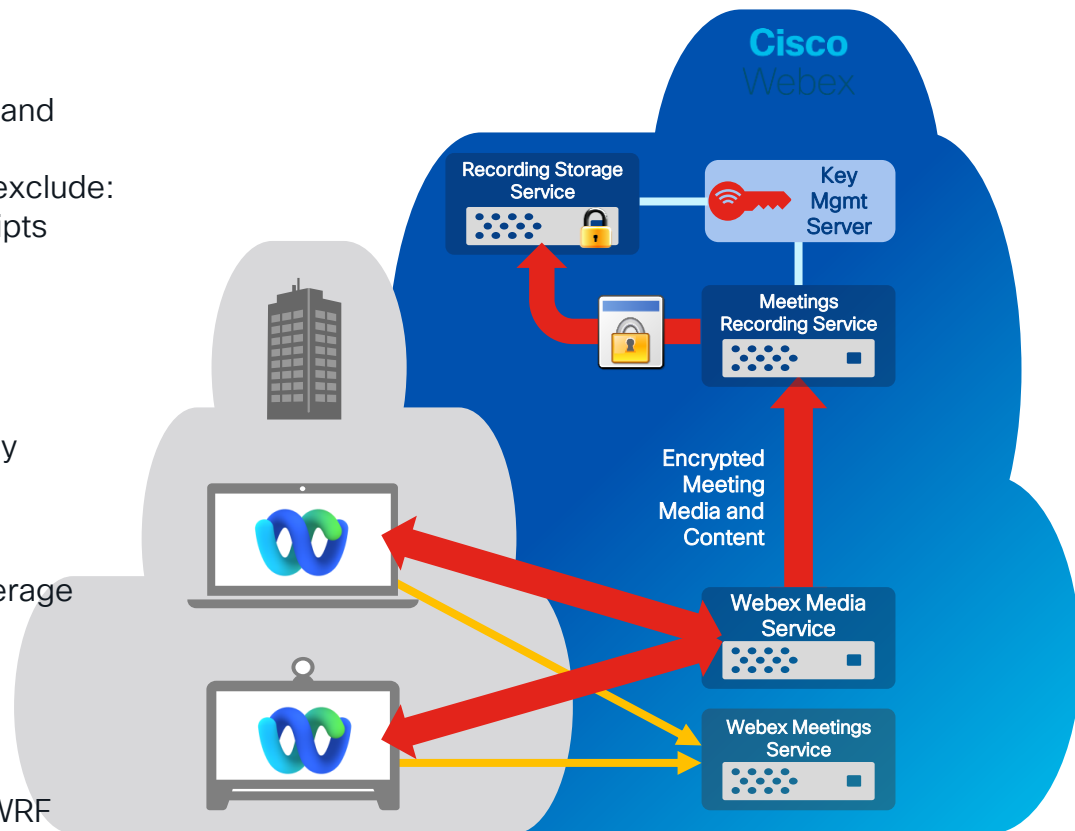
Encrypted using AES-256-GCM, optionally leverage customer managed keys (HDS, BYOK etc)

Configurable retention period

Local recording

Optionally enabled by site admin

Meeting saved on host's computer as MP4 or WRF

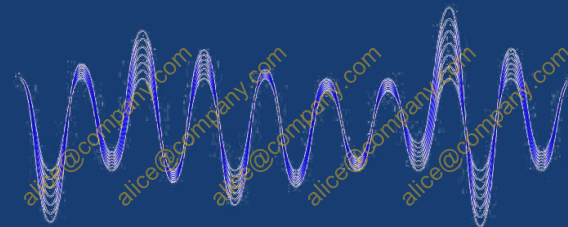
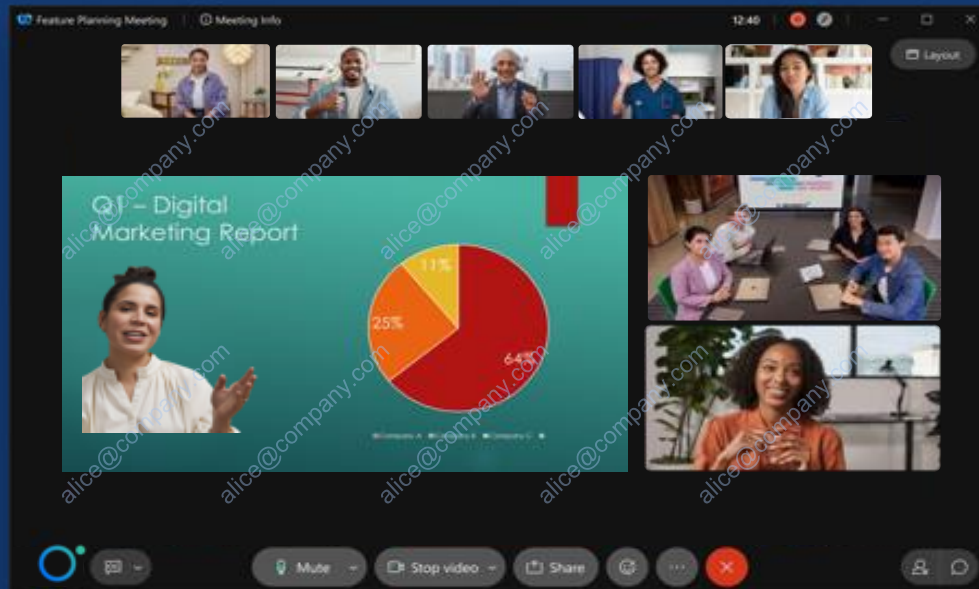


Audio a video watermarking

Keep your content private

Watermarking prevents unwanted leakage of meeting data

Identifies source of:
Screenshots
Video recordings
Audio recordings



Webex Meetings – Audio Watermarking

Available today for Webex E2E Encrypted Meetings

Schedule a meeting ▾ Meeting templates ⓘ Webex Meetings Default ▾

Meeting type ⓘ Webex Meetings Pro-End to End Encryption_VOIPOnly ▾

Security

Digital Watermarking ⓘ ☒ Audio

Add audio watermark

Add audio watermark

When enabled, add watermarks to subsequent meetings. The watermark can be detected by uploading an audio file. Only Webex Meetings with End to End Encryption enabled support this analysis.



When Audio Watermarking is enabled, the meeting audio includes a unique identifier for each participant. An admin can upload audio recordings to Control Hub, which then analyses the recording and looks up unique identifiers. The results of the analysis show which participant shared the meeting content externally.

Troubleshooting

Q Meetings & Calls ▢ Live Meetings ⓘ Status ⓘ Admin Activities ⓘ Logs ⓘ **Analyze watermark**

Q Search analysis results Filter 3 Results

Result name	Uploaded by	Status	Note	Upload time
Norsk Take 2	Darrick Deel	Analysis succe...	Case 003	3/7/2023 12 PM
Norsk P8 1-2-3	Darrick Deel	Analysis succe...	Case 002	3/7/2023 11 AM
Unauthorized R...	Darrick Deel	Analysis succe...	Case 001	3/7/2023 11 AM

- In order to be analysed, the recording must be an AAC, MP3, M4A, WAV, MP4, AVI, or MOV file no larger than 500MB.
- The recording must be longer than 90 seconds.
- You can only analyse recordings for meetings hosted by people in your organisation.
- Analysed recordings are deleted as soon as the analysis is complete.

Analyze audio watermark

Analysis name
I.e. Meeting analysis

Name your analysis to search for in the watermark analysis list.

Note
I.e. case number or case owner

Upload an audio file
Start the analysis by uploading an audio or video file. The file must be in .wav, .aac, .mp3, .m4a, .mp4, .avi or .mov format and less than 500MB.

Drag and drop a file to upload or
Choose file

Webex Meetings – video watermarking

All meeting types supported

Visual watermark for both shared content and video

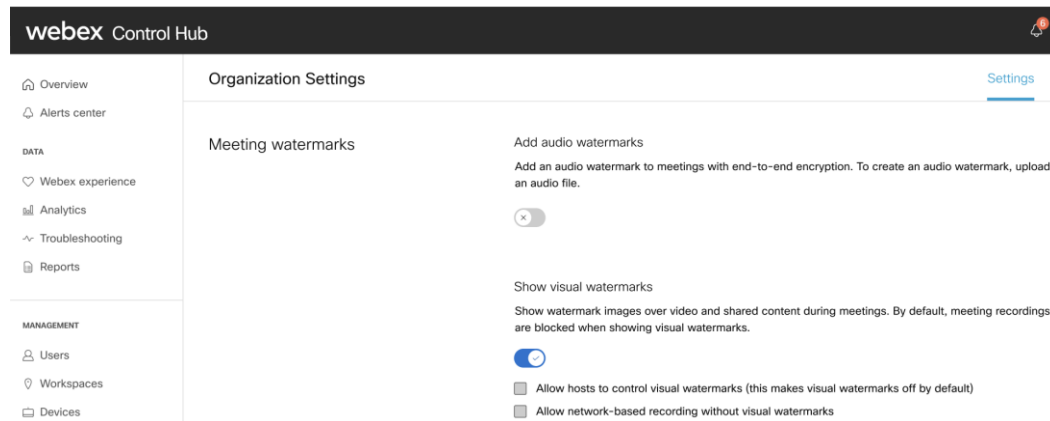
Webex app – desktop, mobile, web

Authenticated users display email watermark

Unverified users display email and username

Local recording automatically disabled

Network recording optional



Control Hub organisation wide/user group/user: Internal Webex meeting access controls

Allow external users from any email domain, or whitelist/blacklist which email domains can join your internal Webex meetings

Apply to all internal meetings, or only to personal rooms

webex Control Hub

Meeting

Settings

Automatically Step Away from a Meeting

Meetings

Internal

For meetings from your organization's sites.

Choose which external users can join internal meetings

Block external users with selected email domains

Meetings

Internal

For meetings from your organization's sites.

Choose which external users can join internal meetings

Block external users with selected email domains

Apply these settings to Personal Room Meetings only

untrustworthy-company.com

Blocked Email domain

dodgy-company.com

Choose which external users can join internal meetings

Block external users with selected email domains

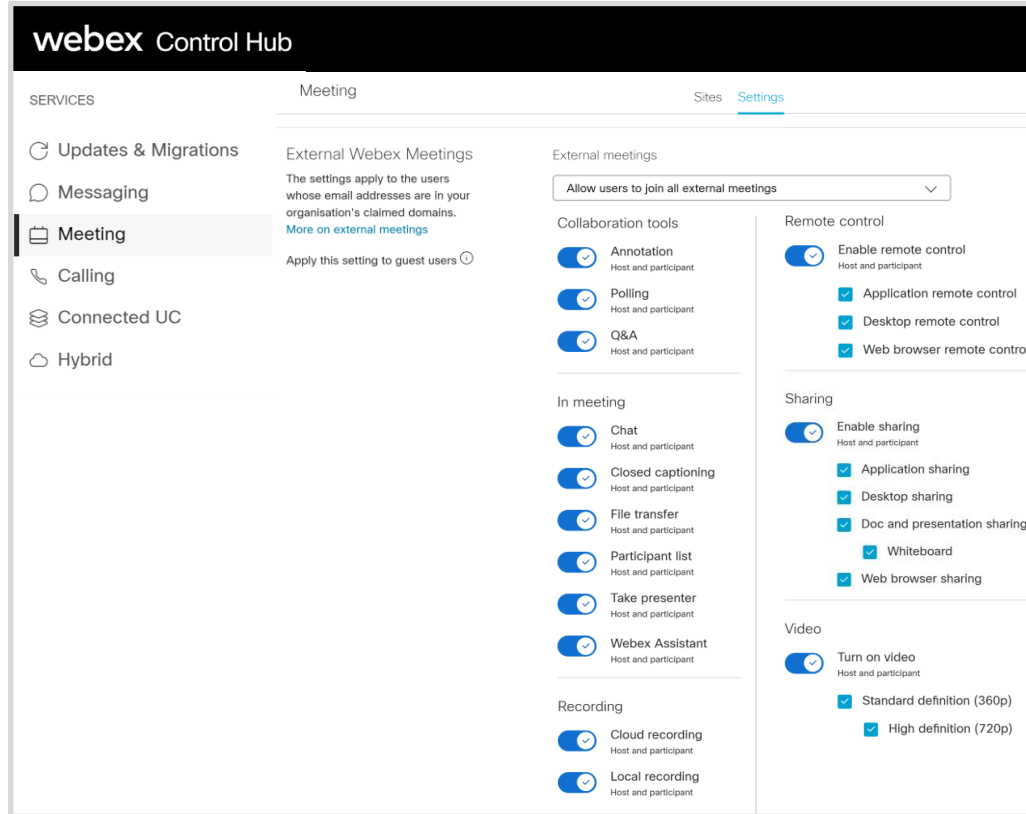
Apply these settings to Personal Room Meetings only

Control Hub organisation wide/user group/user: External Webex meeting access controls

Allow your internal users to join any external Webex meeting, or whitelist/blacklist which external Webex meeting sites they can join

The screenshot shows the Webex Control Hub interface. The top navigation bar includes the Webex logo and a search bar. The left sidebar contains navigation links for 'Return to Partner Hub', 'Overview', 'Alerts center', 'MONITORING' (Analytics, Troubleshooting, Reports), and 'MANAGEMENT' (Users, Groups, Locations, Workspaces). The main content area is titled 'Meeting' and includes tabs for 'Sites', 'Settings' (highlighted with a red box), 'Manage Meetings and Webinars', and 'Templates'. Below the 'Settings' tab, a red circle highlights a note: 'All settings apply to hosts and participants, except where otherwise indicated.' The 'External' section is visible, with a dropdown menu (highlighted with a red box) for 'Choose which external meeting sites your internal users can join'. The dropdown menu options are: 'Allow all external sites', 'Allow approved external sites', 'Block selected external sites', and 'Block all external sites'. The 'Blocked Email domain' section shows 'dodgy-company.com'.

Feature controls for external Webex meetings



These meeting feature controls apply when users in your organisation join any external Webex meeting

These controls do not apply to users joining internal meetings

These controls can be applied to :

- All users in the organisation
- Groups of users – using templates
- Individual users – user profiles

Feature controls for internal Webex meetings

The screenshot displays the Webex Control Hub interface. The top navigation bar includes 'webex Control Hub' and a 'Meeting: Disable Recording' header. Below this, a sidebar lists services: Updates & Migrations, Messaging, Meeting (selected), Calling, Connected UC, and Hybrid. The main content area is divided into sections for 'Collaboration tools', 'Remote control', 'In meeting', 'Sharing', 'Recording', and 'Video'. Each section contains a list of features with toggle switches and checkboxes, all of which are currently enabled. The 'Meeting' section is highlighted in the sidebar.

webex Control Hub

Meeting: Disable Recording
No Recording : Int & Ext · Rank 3

SERVICES

- Updates & Migrations
- Messaging
- Meeting**
- Calling
- Connected UC
- Hybrid

Settings Applied groups

Collaboration tools

- ☒ Annotation
Host and participant
- ☒ Polling
Host and participant
- ☒ Q&A
Host and participant

Remote control

- ☒ Enable remote control
Host and participant
- ☒ Application remote control
- ☒ Desktop remote control
- ☒ Web browser remote control

In meeting

- ☒ Chat
Host and participant
- ☒ Closed captioning
Host and participant
- ☒ File transfer
Host and participant
- ☒ Participant list
Host and participant
- ☒ Take presenter
Host and participant
- ☒ Webex Assistant
Host and participant

Recording

- ☒ Cloud recording
Host and participant
- ☒ Local recording
Host and participant

Sharing

- ☒ Enable sharing
Host and participant
- ☒ Application sharing
- ☒ Desktop sharing
- ☒ Doc and presentation sharing
- ☒ Whiteboard
- ☒ Web browser sharing

Video

- ☒ Turn on video
Host and participant
- ☒ Standard definition (360p)
- ☒ High definition (720p)

These meeting feature controls apply when users join internal Webex meetings in your organisation

Telephony controls (not shown)

- Call In
- Call Back
- VoIP

These controls do not apply to users joining external meetings

These controls can be applied to:

- All users in the organisation
- Groups of users – using templates
- Individual users – user profile

Webex Basic Meetings

Apply security to users without paid Webex licenses

You can import your entire organisation's user base into Webex Control Hub, without applying a paid license

Allows users to join Webex Meetings, use SSO and show up as 'verified'

Security/Feature Controls applied to all imported users – free and paid

Avoid users joining external Webex meetings as a 'guest' with no security controls or authentication

Use free Webex 'Basic Meetings' license for unlicensed users, or 'Active User' subscription where only meeting hosts are measured against license consumption

Feature	Basic meetings	Paid meetings
Meeting duration limit	40 minutes per meeting. Meetings automatically end at 40 minutes.	24 hours
Meetings participant limit	100	1000
Webinar participant limit	✗ N/A	5000
Webinar 10k+	✗ N/A	✓ Add-on purchase
Local recording	✓ Available	✓ Available
Cloud recording	✗ N/A	✓ Available
File transfer	✗ N/A	✓ Available
Join before host	✗ N/A	✓ Available
Schedule on behalf	✗ N/A	✓ Available
Alternate host/co-host	✓ Available (✗ N/A for online meeting sites)	✓ Available
PMR link change	✓ Available	✓ Available
Lock room setting	✓ Available	✓ Available
Schedule PMR (calendar plugin)	✓ Available	✓ Available
Webex Assistant for Meetings	✗ N/A	✓ Available
Closed captioning	✗ N/A	✓ Available
Toll dial-in	✗ N/A	✓ Add-on purchase
Included NBR storage	✗ N/A	✓ Available
NBR storage overage	✗ N/A	✓ Available
Retention period for NBR	✗ N/A	✓ 1 year standard. 10 years with Pro Pack.
Real-time translation	✗ N/A	✓ Add-on purchase
Simultaneous interpretation	✗ N/A	✓ Add-on purchase

Webex Meetings – delete meeting host and usage data

Webex meetings: host and usage data examples

IP address

User agent identifier

Hardware type

Operating system type and version

Client version.....

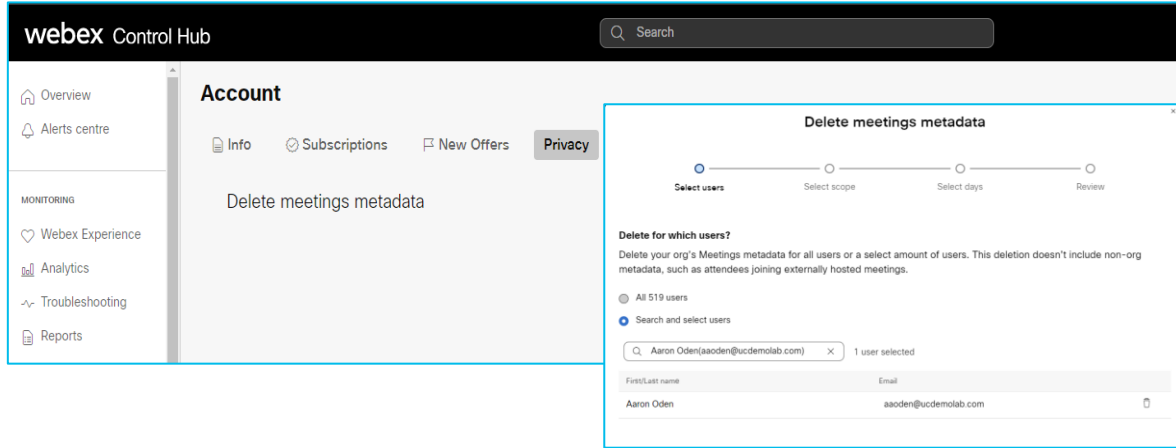
Host name and email address

Meeting site URL

Meeting start/end time

Meeting title

Call attendee information



For full details see the Webex Meetings Privacy Data Sheet

<https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf>

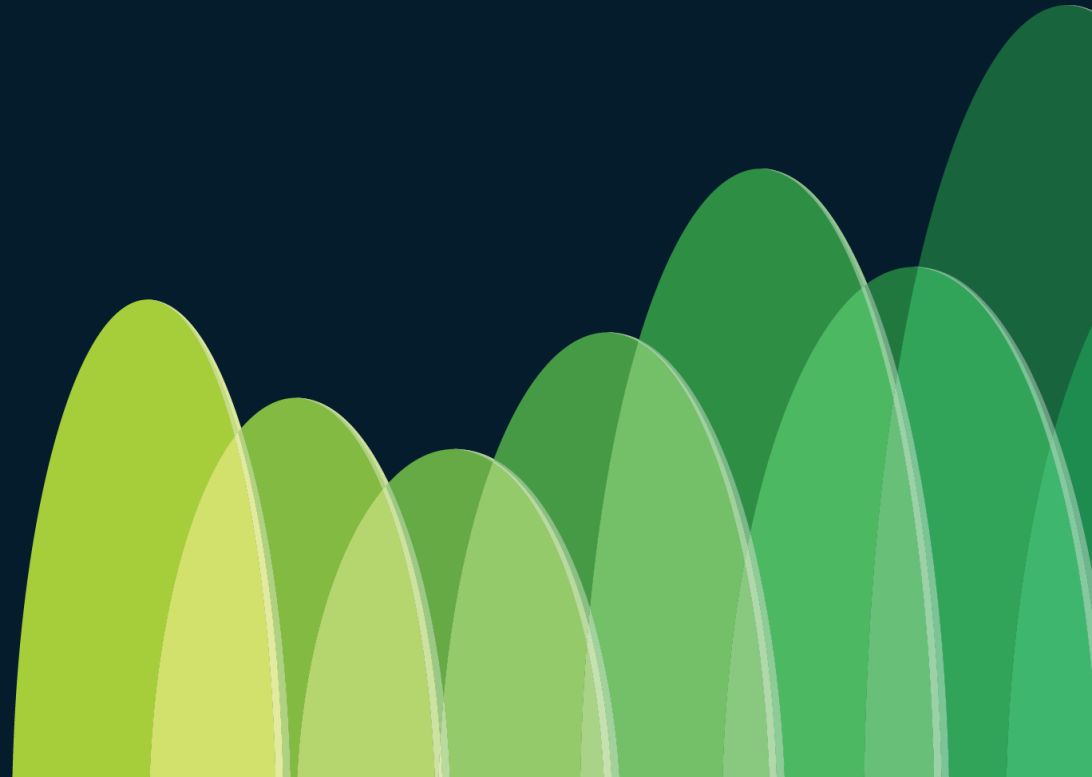
Control Hub -> Account -> Privacy

Allows and administrator to delete Meeting Host and Usage Information based on Meeting Host name

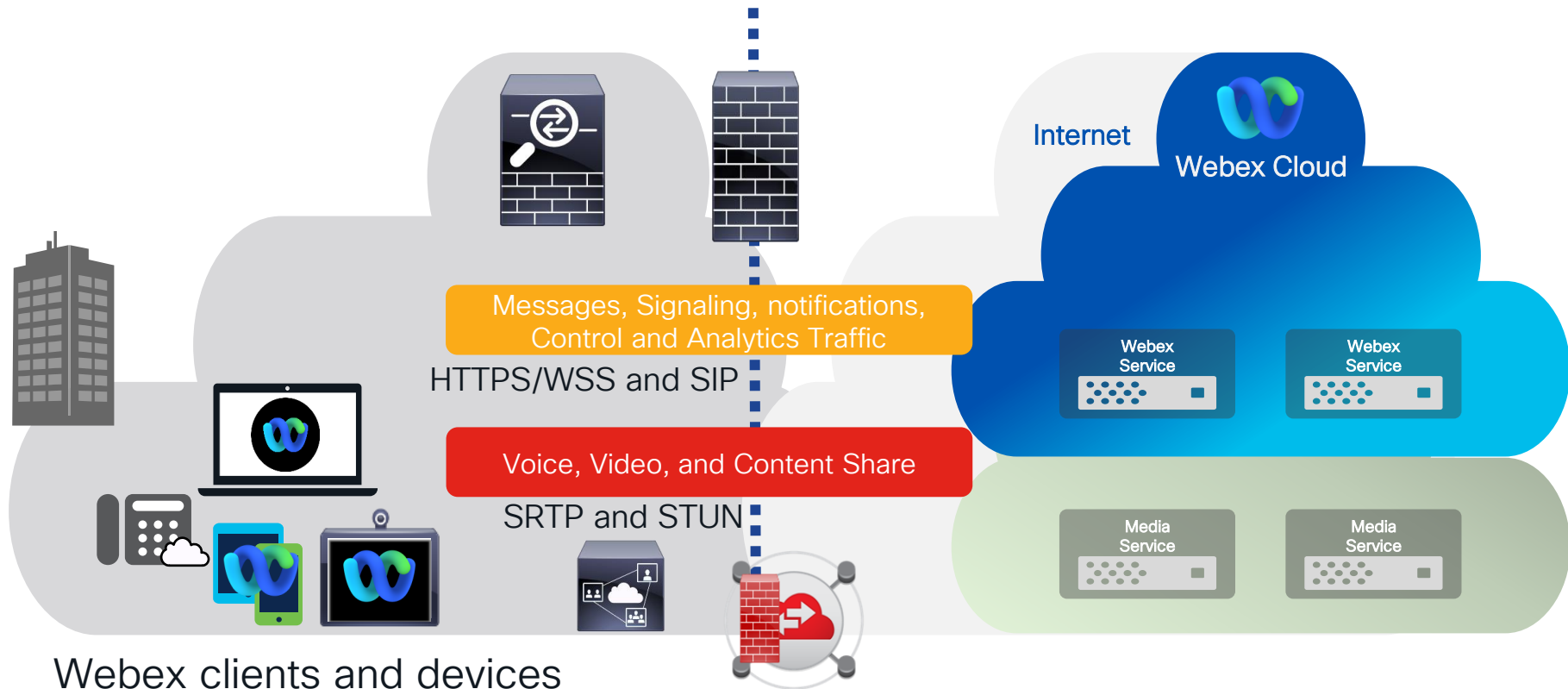
Deleted data cannot be retrieved

<https://help.webex.com/en-us/article/l4pqoi/Delete-Webex-Meetings-host-and-usage-information-of-users-in-Control-Hub>

Fundamentals on Firewall Traversal

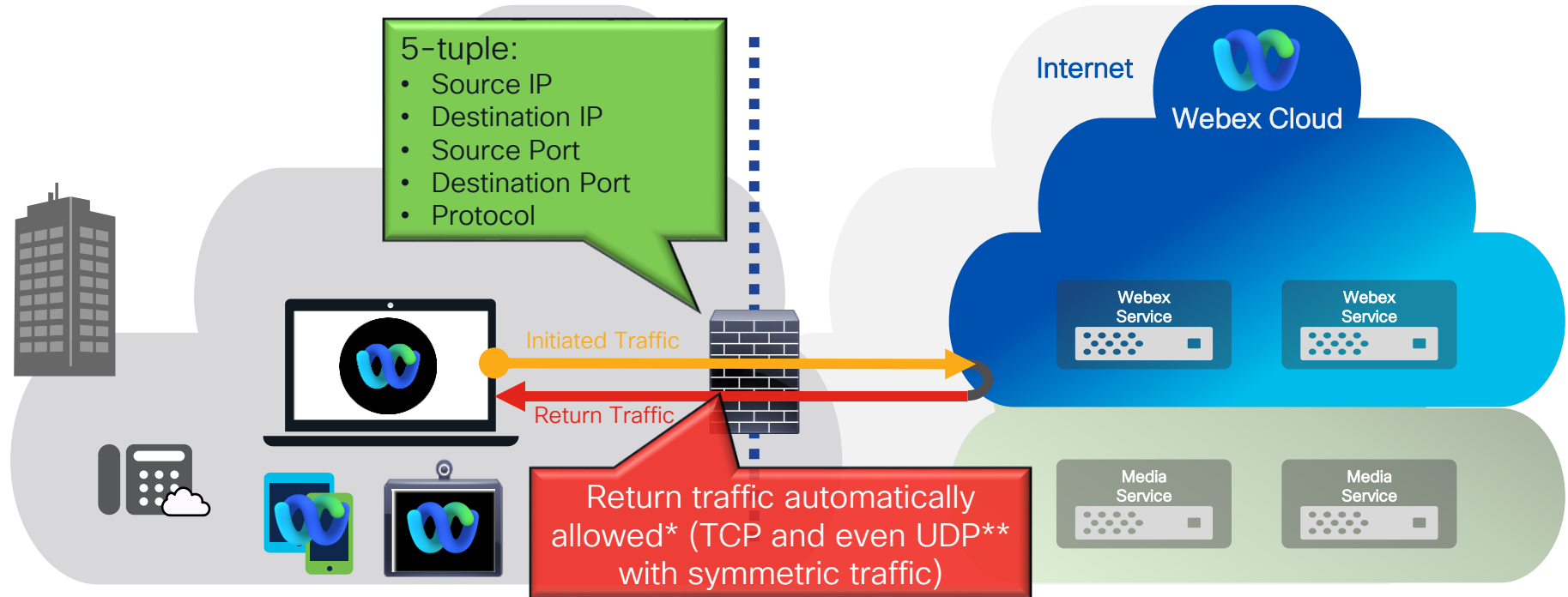


Types of traffic



Firewall traversal

Return traffic automatically allowed

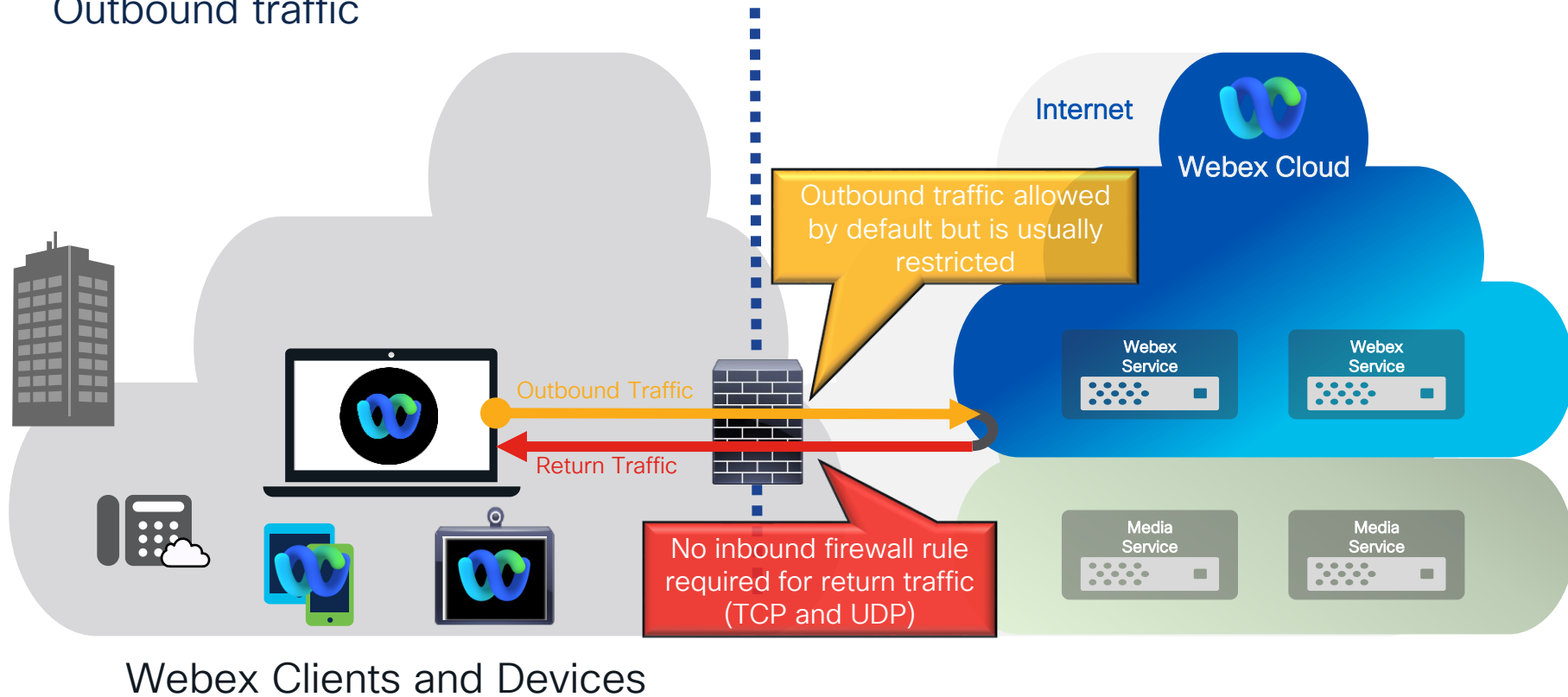


* With most firewalls

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

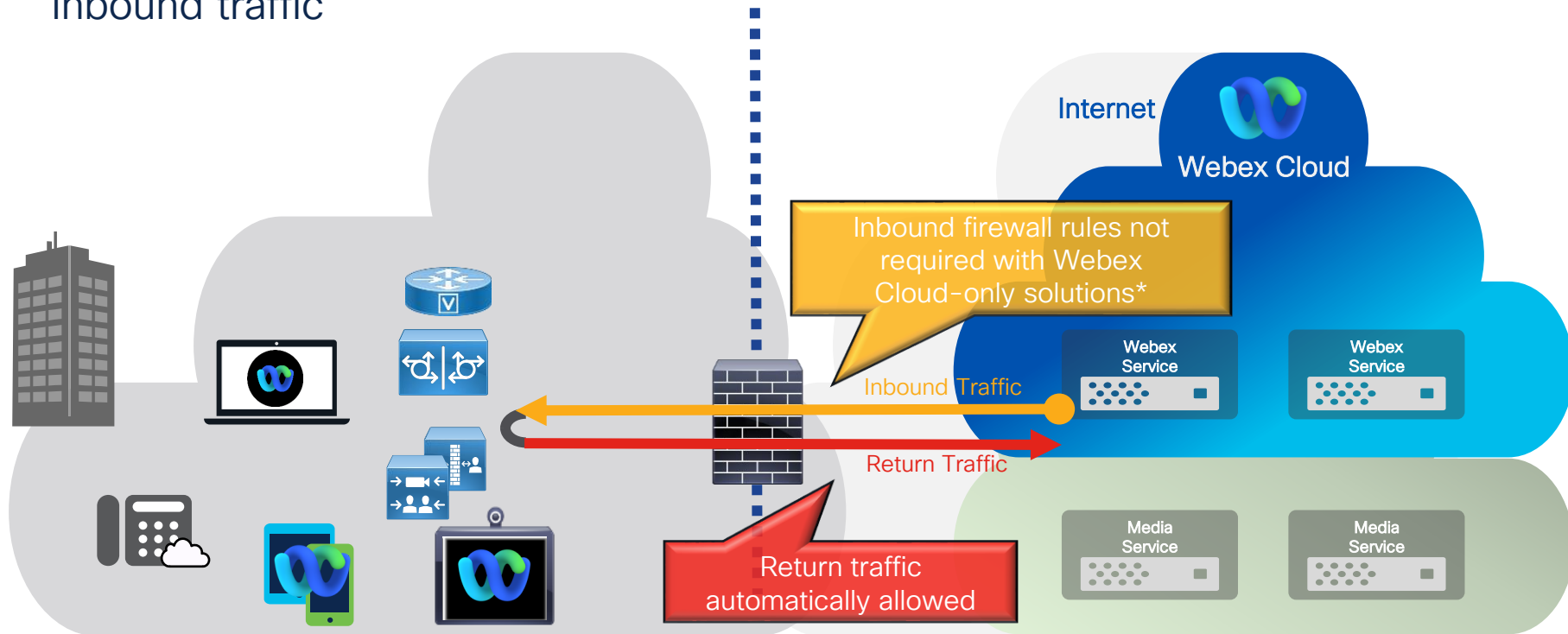
Firewall traversal

Outbound traffic



Firewall traversal

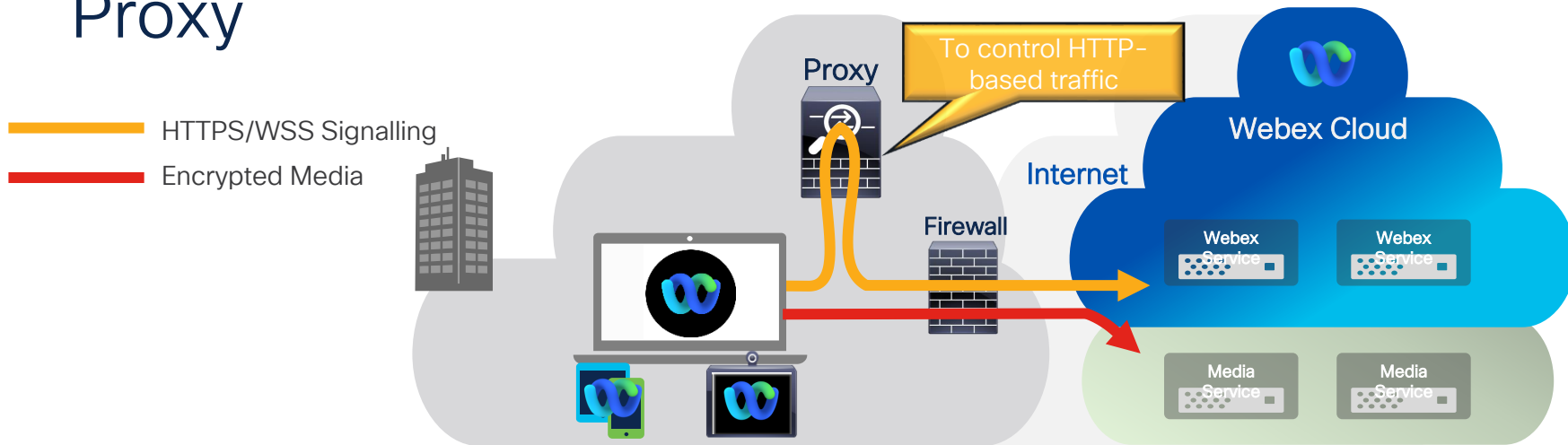
Inbound traffic



Webex Clients and Devices

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

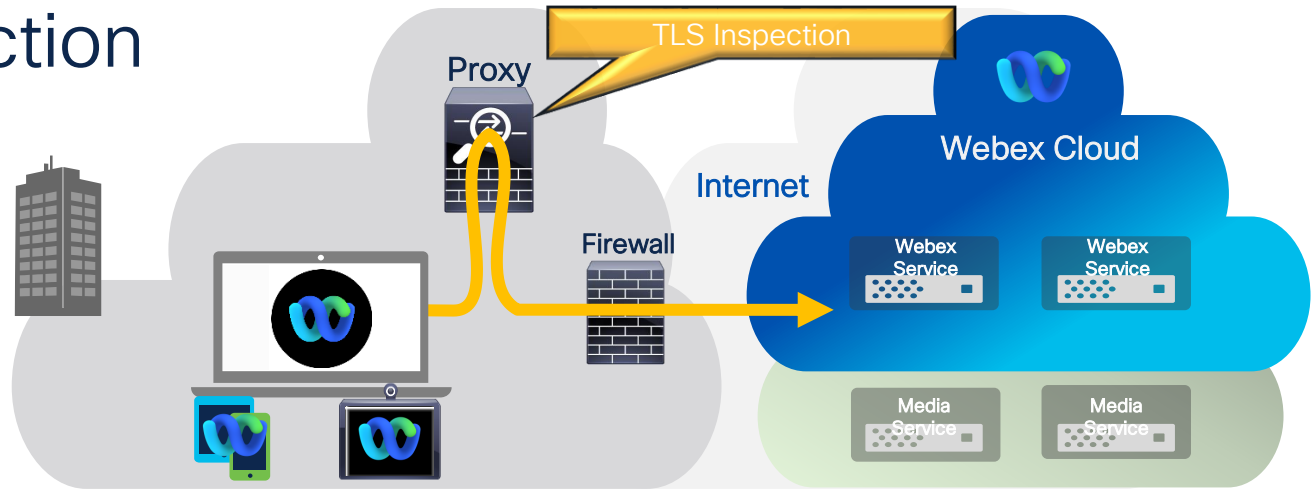
Proxy



- Supported with Webex Messaging, Meetings, Devices 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 and it is highly recommended to permit media directly

* 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 for these workloads.
 - TLS inspection not supported for media. If not permitting media directly, TLS inspection must be disabled for relevant Webex domains.

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 TCP/TLS 443 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
 - TLS 443
- With Webex Calling, no fallback to TCP
- Restrict outbound media by destination IP

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
<u>UDP Port Filtering</u> - ANY IP (e.g. only allow UDP 5004/9000 for Webex devices and Webex Meetings*)	Best media quality Easy to configure
UDP Port Filtering - <u>IP Subnet Filtering</u>	Best media quality but... Have to keep track of IP subnets to allow - manual or programatically
<u>Block UDP*</u> 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

Automated and predefined firewall rules

- Be wary of pre-defined or automated definitions for Webex traffic on firewalls
- Almost always missing ports/addresses, and/or or “over-permitting”
- If you need to automate – pull subnets from here:

<https://info.net-int.infra.webex.com/v1/pr efixes>

Number of IP ranges: 6612									
2.16.19.40-2.16.19.41	country(300)	region(137)	city(1194)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.16.19.40-2.16.19.41	country(300)	region(137)	city(1194)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.16.66.192-2.16.66.192	country(752)	region(1806)	city(23098)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.16.66.192-2.16.66.192	country(752)	region(1806)	city(23098)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.16.124.50-2.16.124.50	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.16.124.50-2.16.124.50	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.16.147.55-2.16.147.55	country(380)	region(1727)	city(17934)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.16.147.55-2.16.147.55	country(380)	region(1727)	city(17934)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.16.165.124-2.16.165.124	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.16.165.124-2.16.165.124	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.16.165.155-2.16.165.155	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.16.165.155-2.16.165.155	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.16.172.169-2.16.172.170	country(616)	region(1150)	city(25906)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.16.172.169-2.16.172.170	country(616)	region(1150)	city(25906)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.17.34.102-2.17.34.102	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(0)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.17.34.102-2.17.34.102	country(250)	region(742)	city(18071)	blacklist(0x0)	reputation(5)	popularity(5)	domain(0)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.17.37.113-2.17.37.113	country(724)	region(423)	city(14129)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.17.37.113-2.17.37.113	country(724)	region(423)	city(14129)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)
2.17.37.170-2.17.37.170	country(724)	region(423)	city(14129)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(6) port(53 80 443 1719-1720 5004 5060-5070 8000-59999)
2.17.37.170-2.17.37.170	country(724)	region(423)	city(14129)	blacklist(0x0)	reputation(5)	popularity(5)	domain(531)	botnet(0)	proto(17) port(53 1719-1720 5004 9000 8000-59999)

See above for a real-world example from a third party firewall in a customer’s deployment;

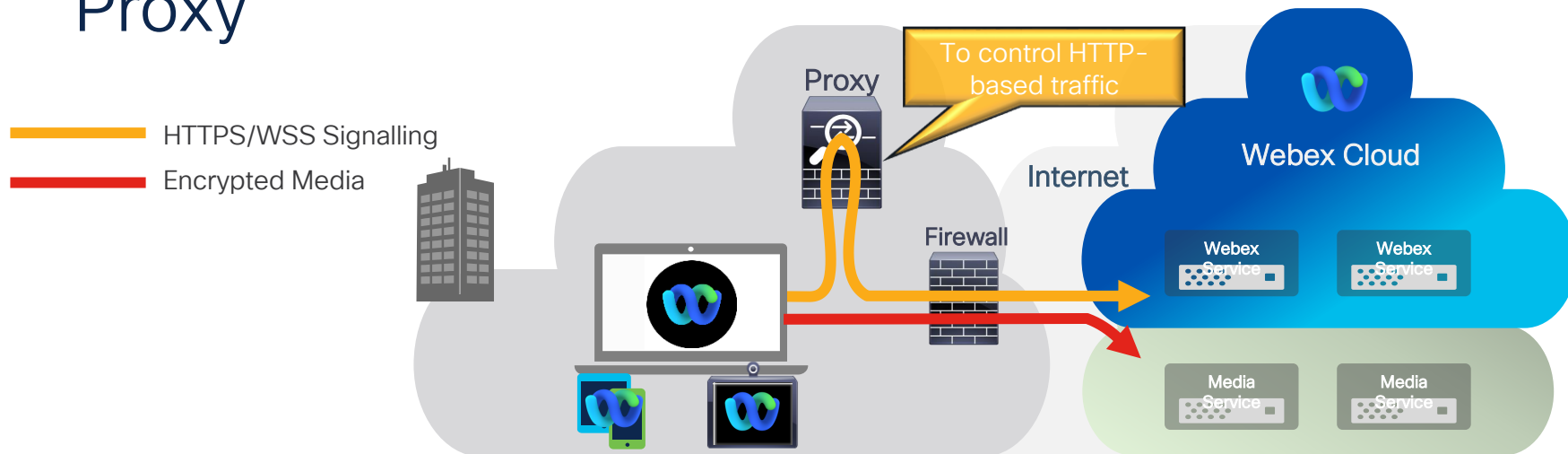
Pre-canned “Webex” definition had 6000+ small IP ranges, some missing IP ranges, causing intermittent media failure

Included Ports:

5004, 9000, 443

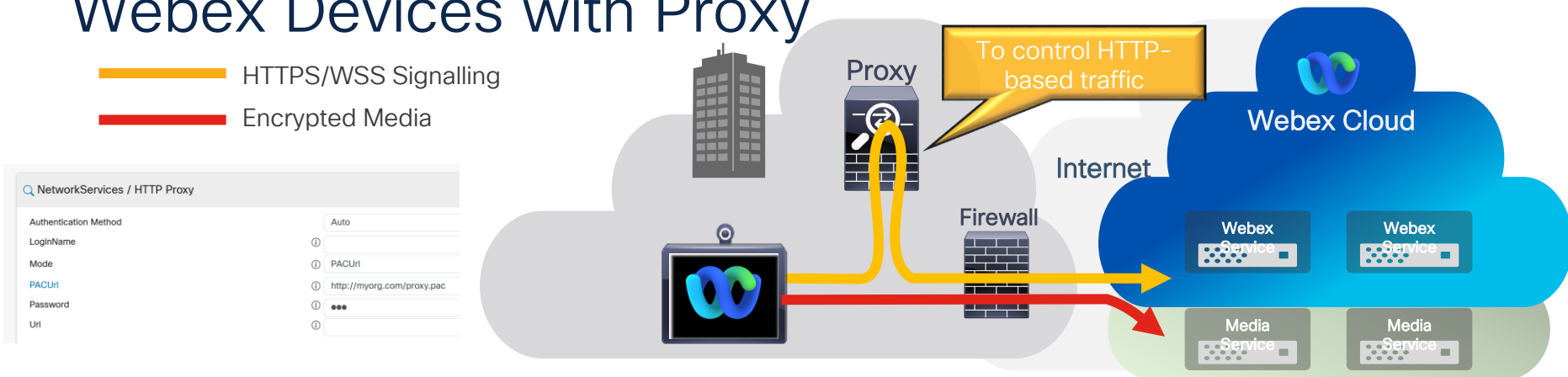
1719-1720,5060-5070, 8000 – 59999

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 5004 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.
- With Webex Calling, proxy is only supported with soft clients, and this is only for signaling

Webex Devices with Proxy



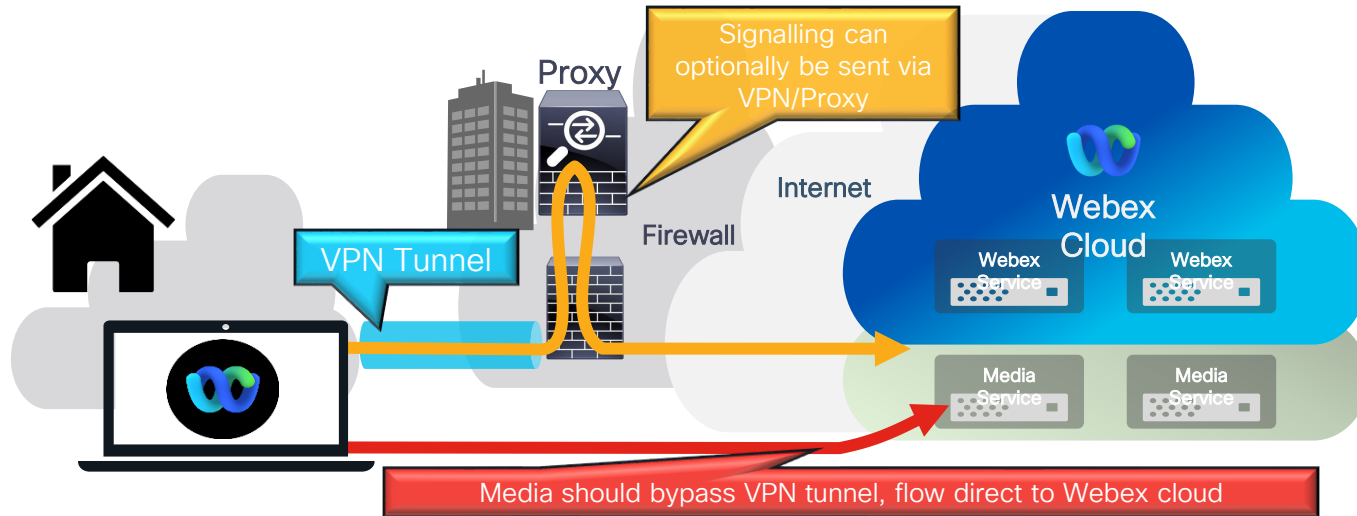
- Webex devices support basic and digest auth – no NTLM/Windows authentication. Proxy will likely need to permit via service account or IP/subnet. WPAD supported, can optionally use custom WPAD for devices
- Authenticated Proxy not supported on MTR – can optionally restrict via subnet/IP or use custom WPAD
- Either disable TLS inspection, or manually load enterprise CA to Webex Device trust ***and*** log TAC case to upload customer certificates to Webex cloud
- Media via proxy is supported for Webex devices but off by default – **direct UDP still highly recommended for media:**
xConfiguration Webex Meetings HttpProxyForMedia Allowed: True
xConfiguration Webex Meetings HttpProxyForMedia Mode: Auto

Media via Proxy vs Direct Security Considerations

- Some organization may hesitate to permit media to flow directly and prefer to use a Web Proxy
- Web Proxies are not designed for real-time media
- In order to provide good performance, we must solve for the security functions provided by Web Proxies while permitting media directly
- If users have poor media quality, we risk them moving to a less secure medium to make it work, e.g. PSTN

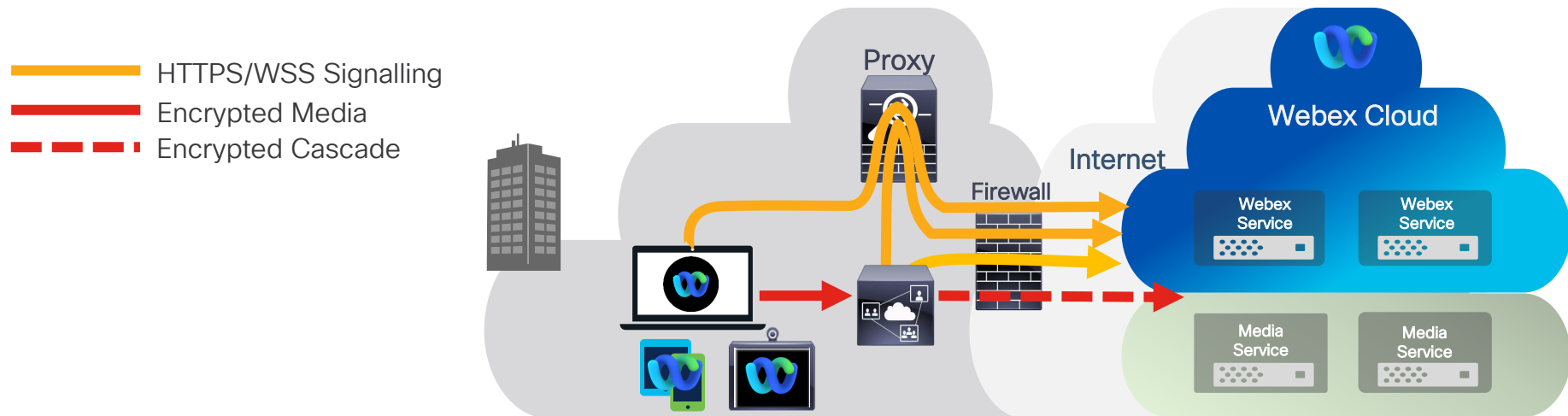
Function	Web Proxy Deployment	Direct Media Deployment
Traffic Filtering	Destination URL	5-tuple (source/dest port, source/dest IP, protocol)
TLS Inspection	Can inspect signaling. Media encrypted, cannot be inspected, inspection may be disabled entirely due to this.	Can still send signaling via Web Proxy. Media encrypted, cannot be inspected.
Source Address translation	Web Proxies terminate traffic, changing source IP, destination IP	Firewall performs source-NAT on existing outbound flow, changing source address. Destination IP is not altered, - no need to hide destinations as they are listed publicly.

Webex App with VPN or Cloud SIG



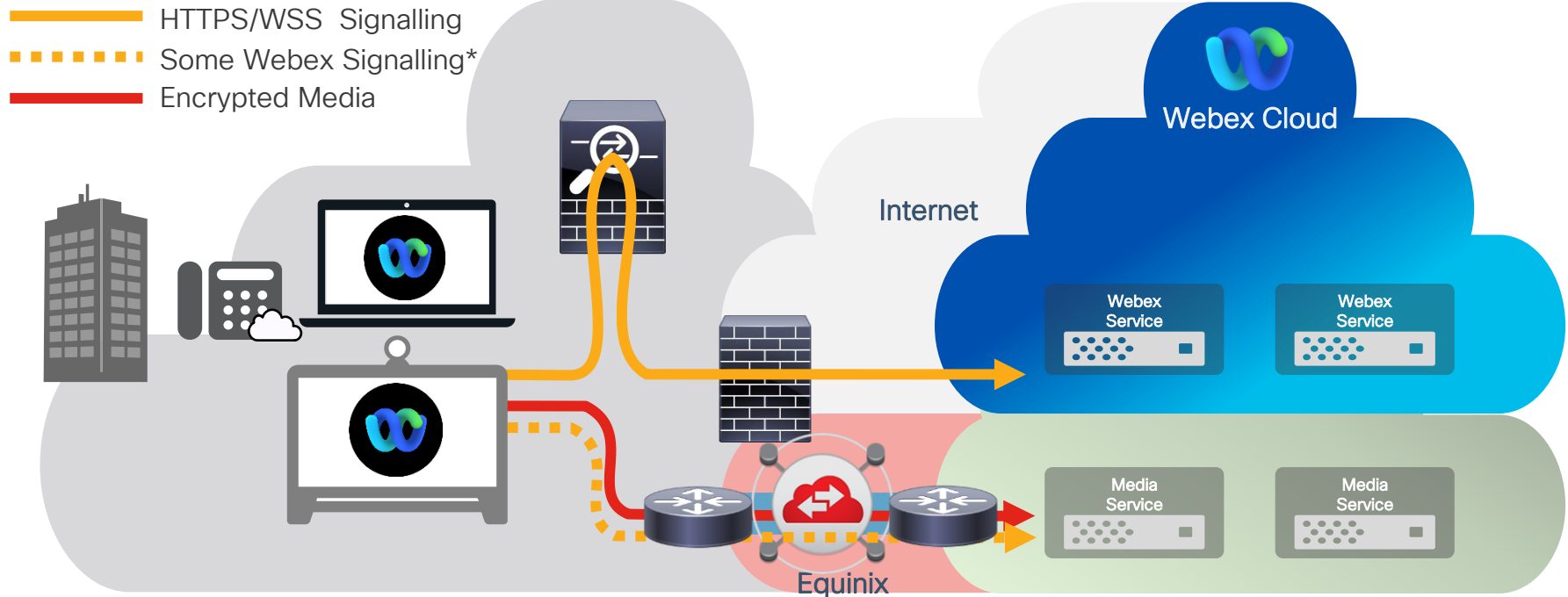
- For home/remote Webex app users with VPN, media should bypass VPN via split or selective tunneling. Signaling can optionally use VPN and/or web proxy (pictured). Similar principles apply for cloud SIG/Proxy deployments e.g. Cisco Umbrella, Zscaler.
- VPN or SIG config can use port-based (UDP5004/9000 etc), IP destination based (Webex media subnets) or application based (Webex app) split tunneling. Webex App will always use proxy for signalling if proxy is defined on workstation – be aware if using app-based rules.
- If you absolutely can't use split tunnel – ensure your VPN/SIG tunnel uses UDP for best performance!

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: Supported outbound media traffic is now sourced from VMN
- *Now supports Webex App for Meetings (requires Webex Suite Meeting Platform)*

Webex Edge Connect

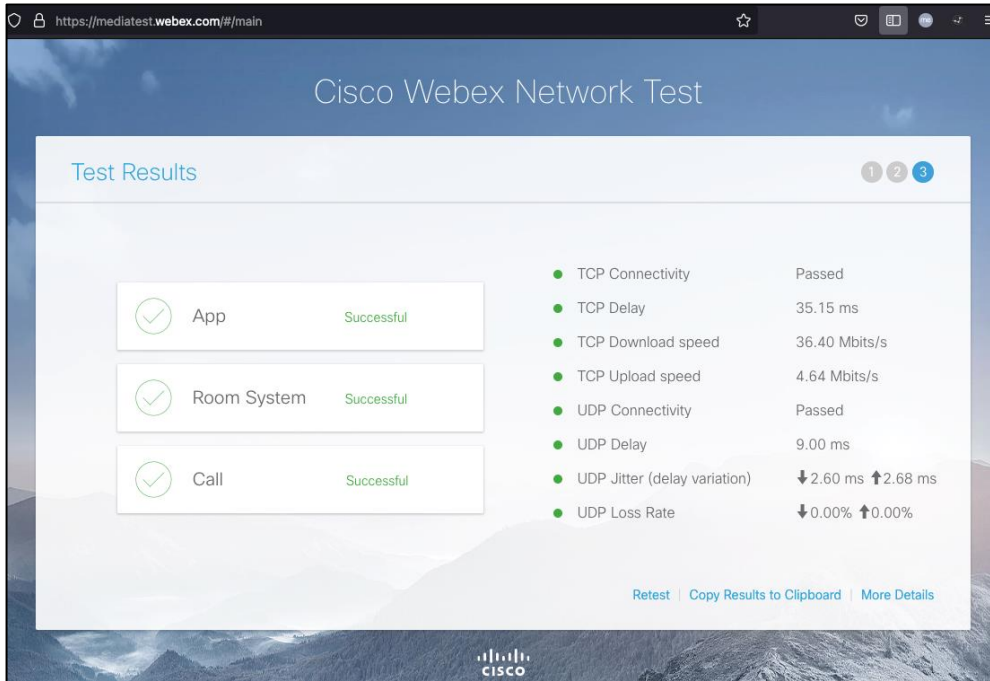


- Private link, better QoS, and insulated from the Internet

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

Cisco Webex network test

Good starting point to test Internet connectivity



<https://mediatest.webex.com>

Will not test all IP subnets
and all URLs

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 Webex Calling. The page is titled "Your connection meets requirements. Your network is ready for Webex Calling." and provides a summary of the test results, including a table of network metrics and a table of port usage.

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: 192.168.1.100 ⓘ

Firefox 100.0, Mac OS X, United States Dallas

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

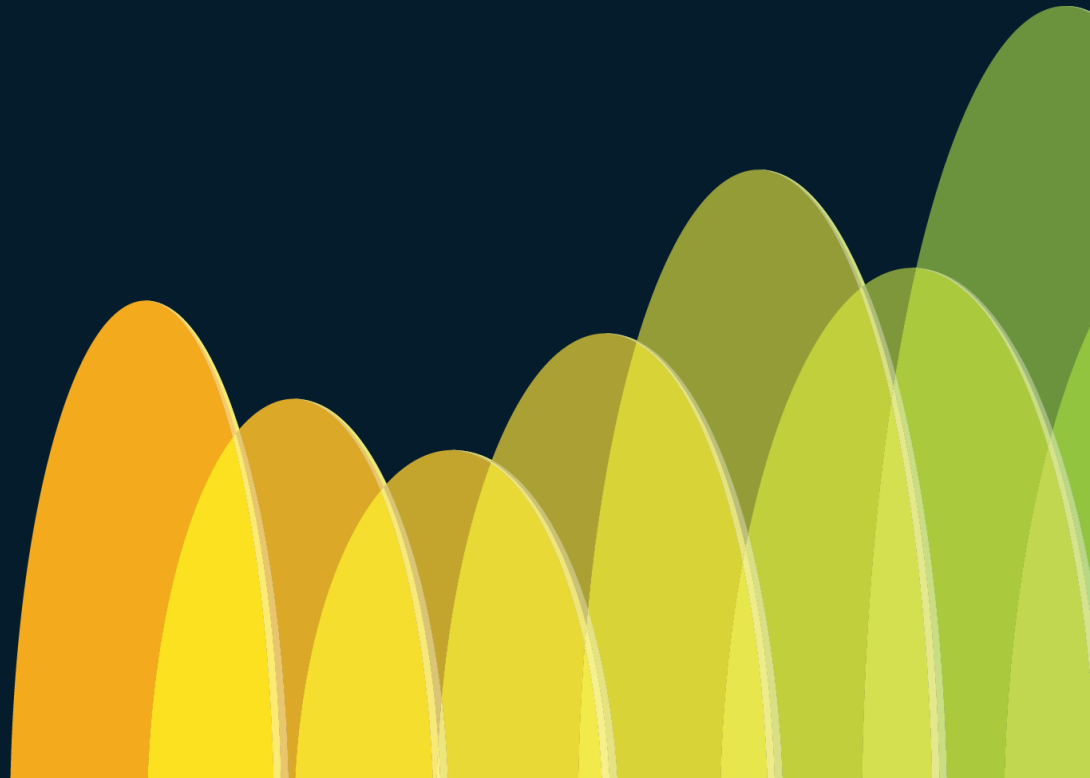
Packet loss	Jitter
Download - 0.00 % Upload - 0.00 %	Download - 7.00 ms Upload - 5.00 ms

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

[Test Again](#) [Test Another Server](#)

[Download this Report](#)

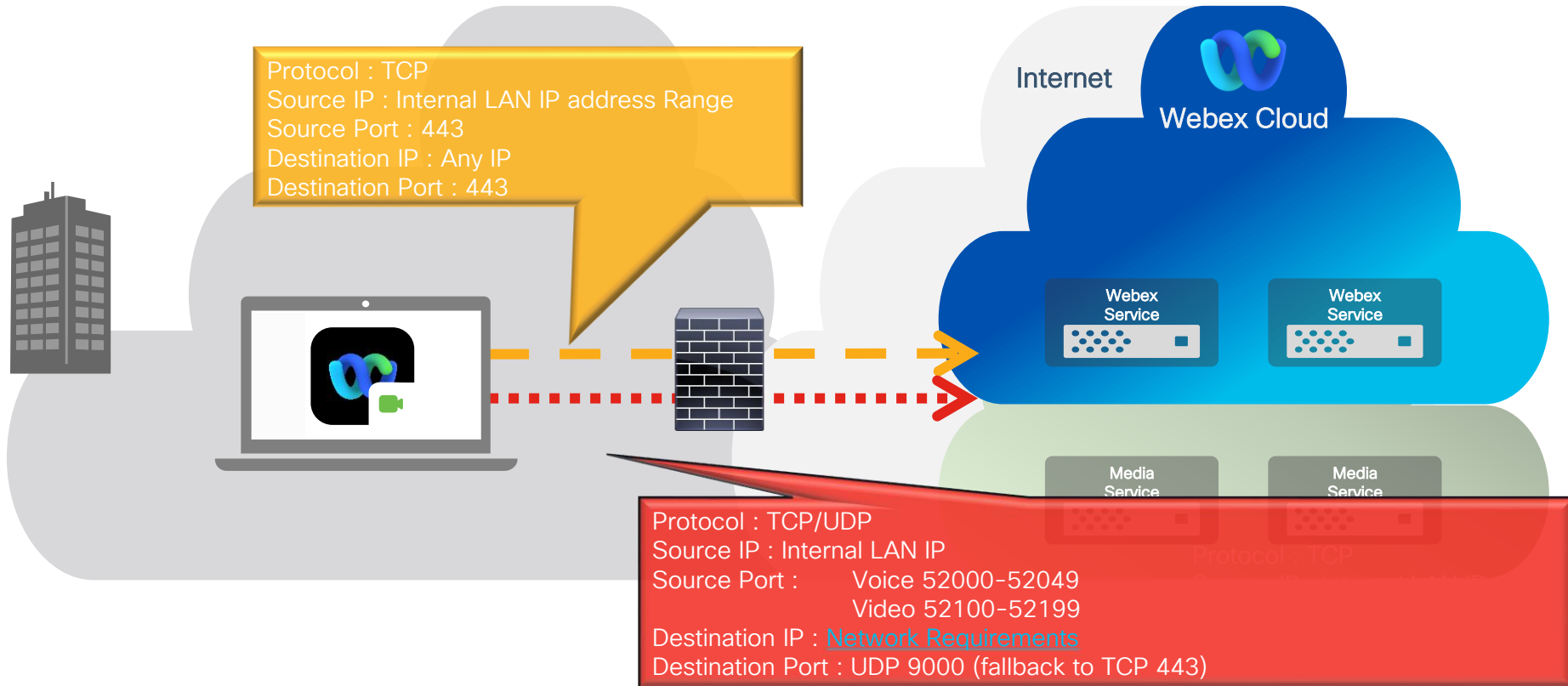
Traffic Flows and Network Port Usage



Protocols and Ports used by Webex

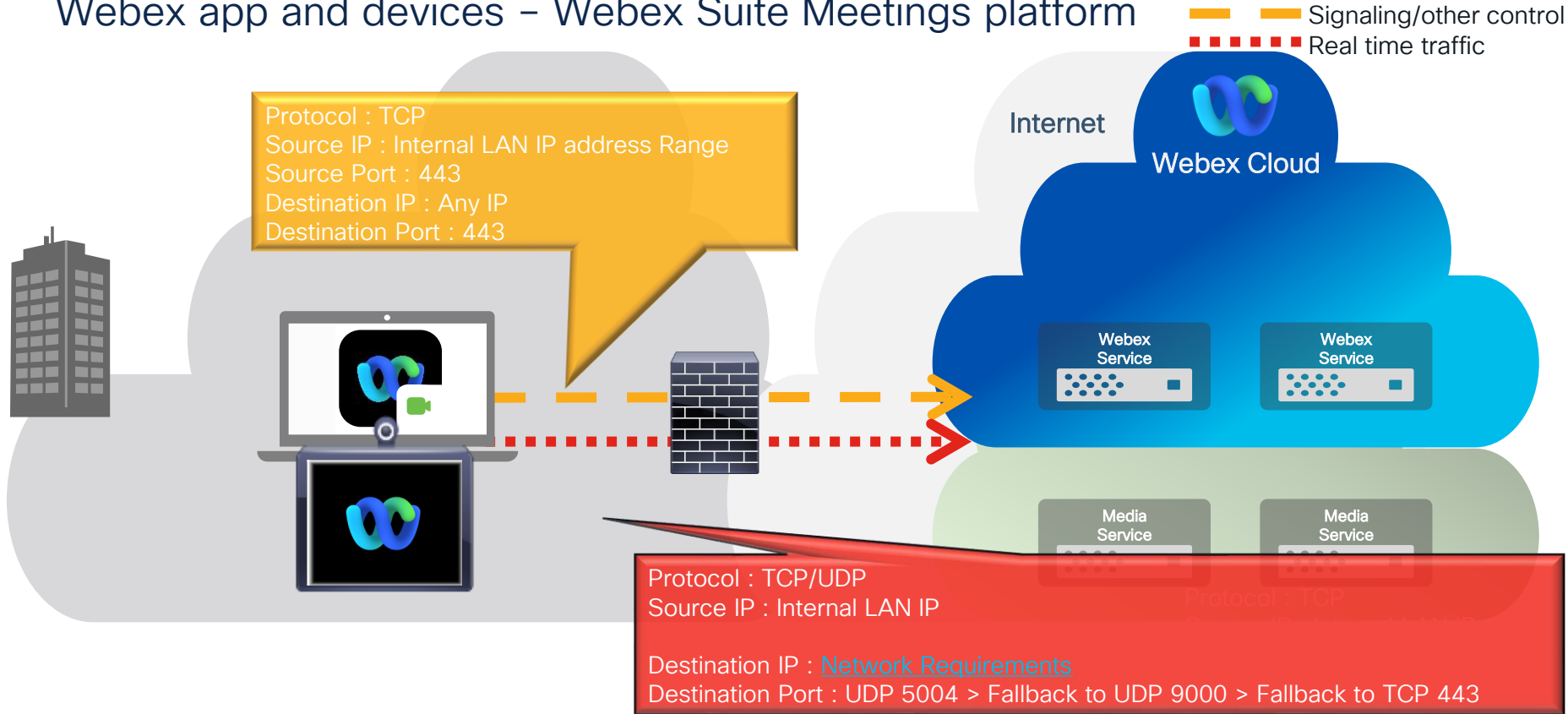
Webex Meetings app, Webex app (old meeting platform – Meeting Centre)

— Signaling/other control
- - - Real time traffic



Protocols and Ports used by Webex

Webex app and devices – Webex Suite Meetings platform



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)

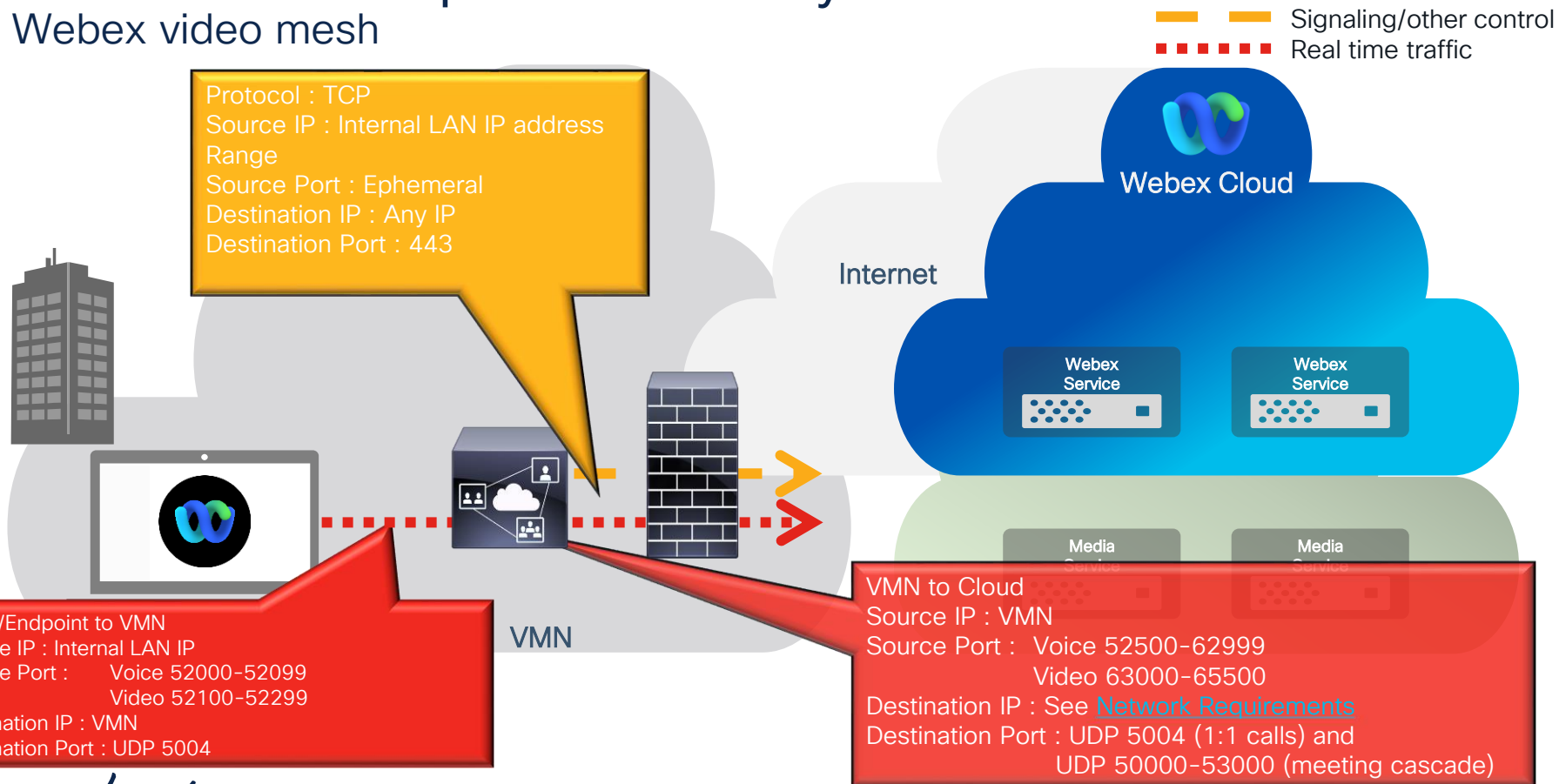
Reference link:

[Port Reference Information for Webex Calling](#)

CISCO Live!

Protocols and ports used by Webex

Webex video mesh

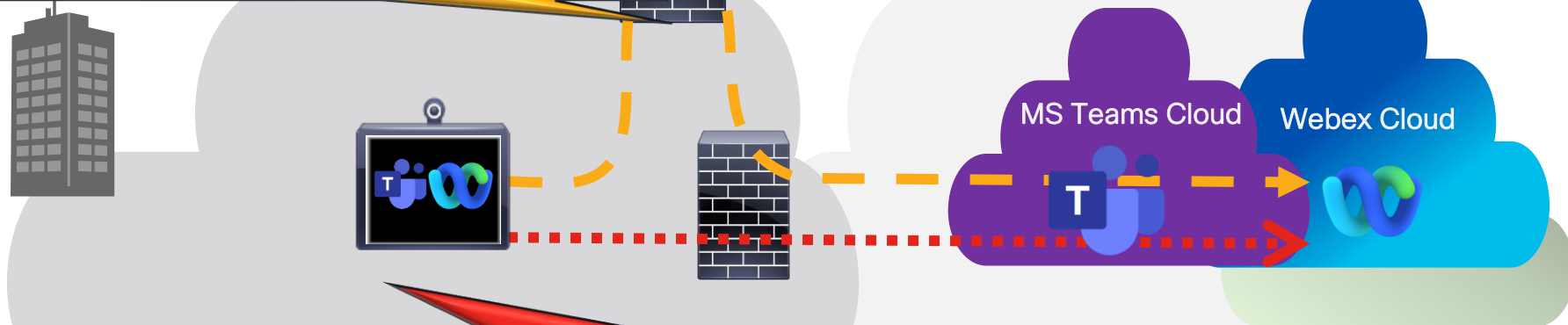


Protocols and ports used by Webex

Cisco devices certified for Microsoft Teams (MTR)

— Signaling/other control
- - - Real time traffic

Protocol : TCP
Source IP : VC Endpoint address range
Destination URLs: [Webex Requirements](#) (CH reg)
[MS Teams Requirements](#) (MS TAC Reg)
Destination Port : 443



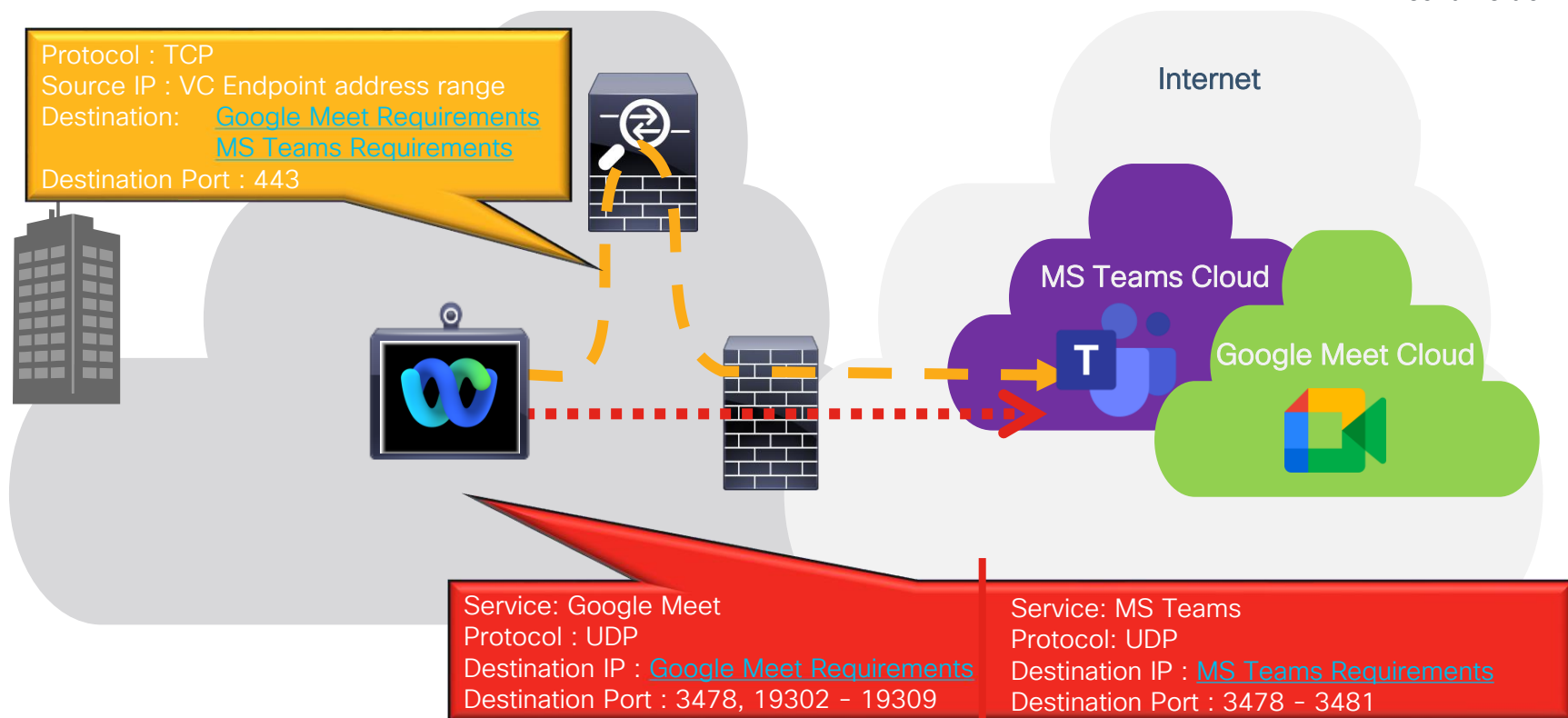
Service: Webex
Protocol : TCP + UDP
Destination IP : [Webex Requirements](#)
Destination Port : TCP + UDP 5004, UDP 9000

Service: MS Teams
Protocol: UDP
Destination IP : [MS Teams Requirements](#)
Destination Port : UDP 3478 - 3481

Protocols and Ports used by Webex

Cisco Video Devices to MS Teams/Google Meet WebRTC

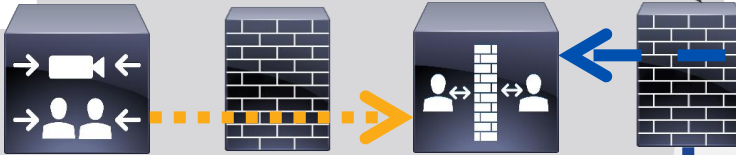
— Signaling/other control
- - - Real time traffic



Protocols and ports used by Cisco Expressway

SIP: TCP 5061 (call signaling)
HTTPS: TCP 8443 (visual voicemail, directory)
XMPP: TCP 5222 (IM and 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

- Inbound traffic required to Expressway-E
- Harden with in-built security features + CPL
- Refer to [Cisco Expressway IP Port Usage Configuration Guide](#)

Conclusion



Conclusion



- Leverage Webex Meeting security settings and secure meeting types to enhance your security posture, including for users who only join external Webex meetings
- Webex traffic is inside-initiated, return traffic is automatically allowed
- Securely allow outbound UDP for media for best media quality
 - Avoid TCP, TLS and web proxies for media
 - Apply outbound IP and URL restrictions
 - Web proxy OK for signaling

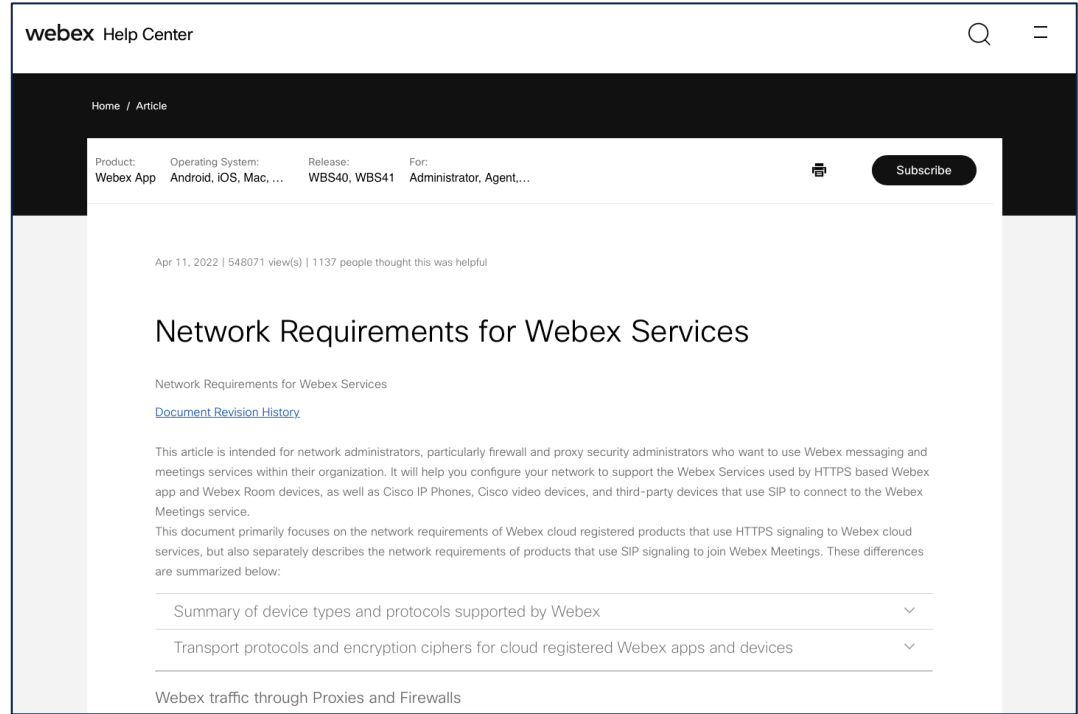
Links to visit regularly / to subscribe

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?

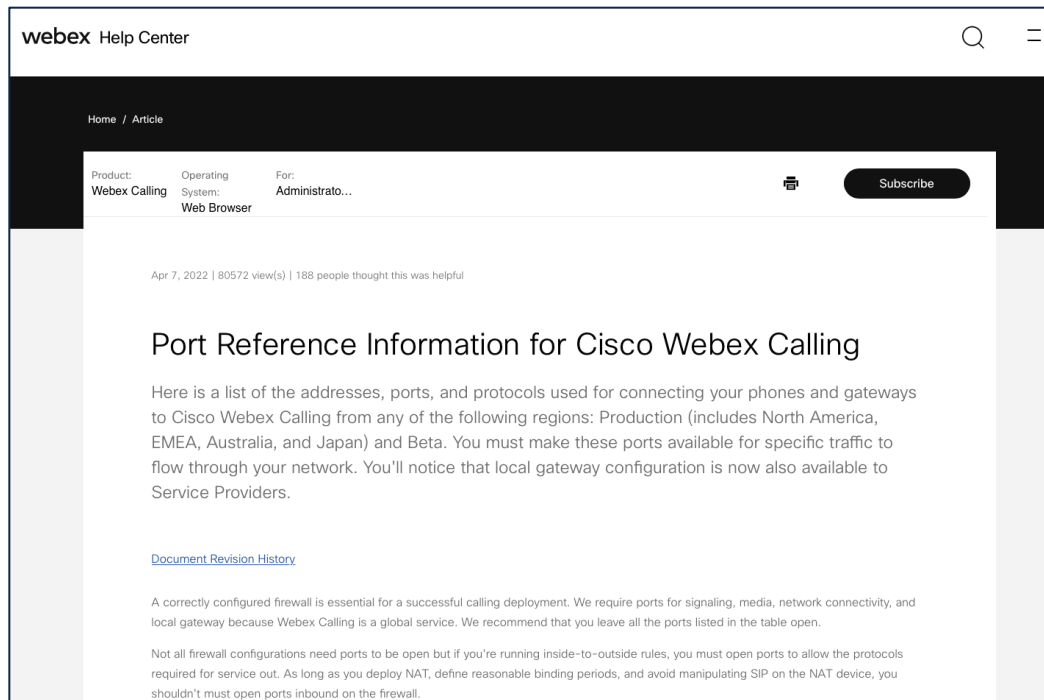
For answers to these questions and for more information about Webex services network requirements, refer to the *Network Requirements for Webex Services* article



<https://help.webex.com/en-US/article/WBX000028782/Network-Requirements-for-Webex-Services>

Links to visit regularly / to subscribe

Port reference information for Cisco Webex Calling



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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

Contact me at: nhalbert@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC