

The background features a vibrant, abstract design with overlapping, wavy bands of color in shades of blue, green, yellow, orange, and red. On the right side, a bright white light source radiates outwards, creating a starburst effect with sharp, colorful rays extending across the entire frame.

cisco *Live!*

Let's go

#CiscoLiveAPJC



“Reconciliation”- Dustin Koa Art

Cisco Webex App

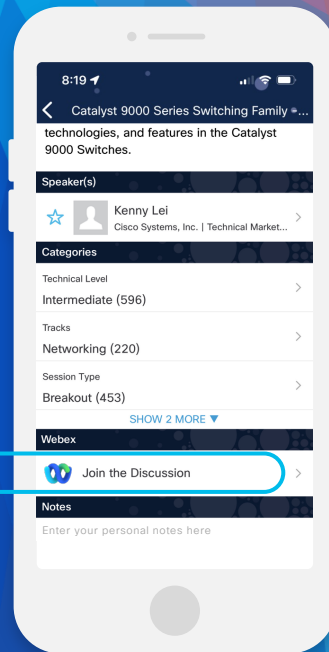
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2876>



The bridge to possible

Secure Webex Meetings and Webex Network Security

Exploring secure Webex Meeting types, Webex security settings and navigating secure network deployments

Nick Halbert-Lillyman, Technical Solutions Architect
BRKCOL-2876



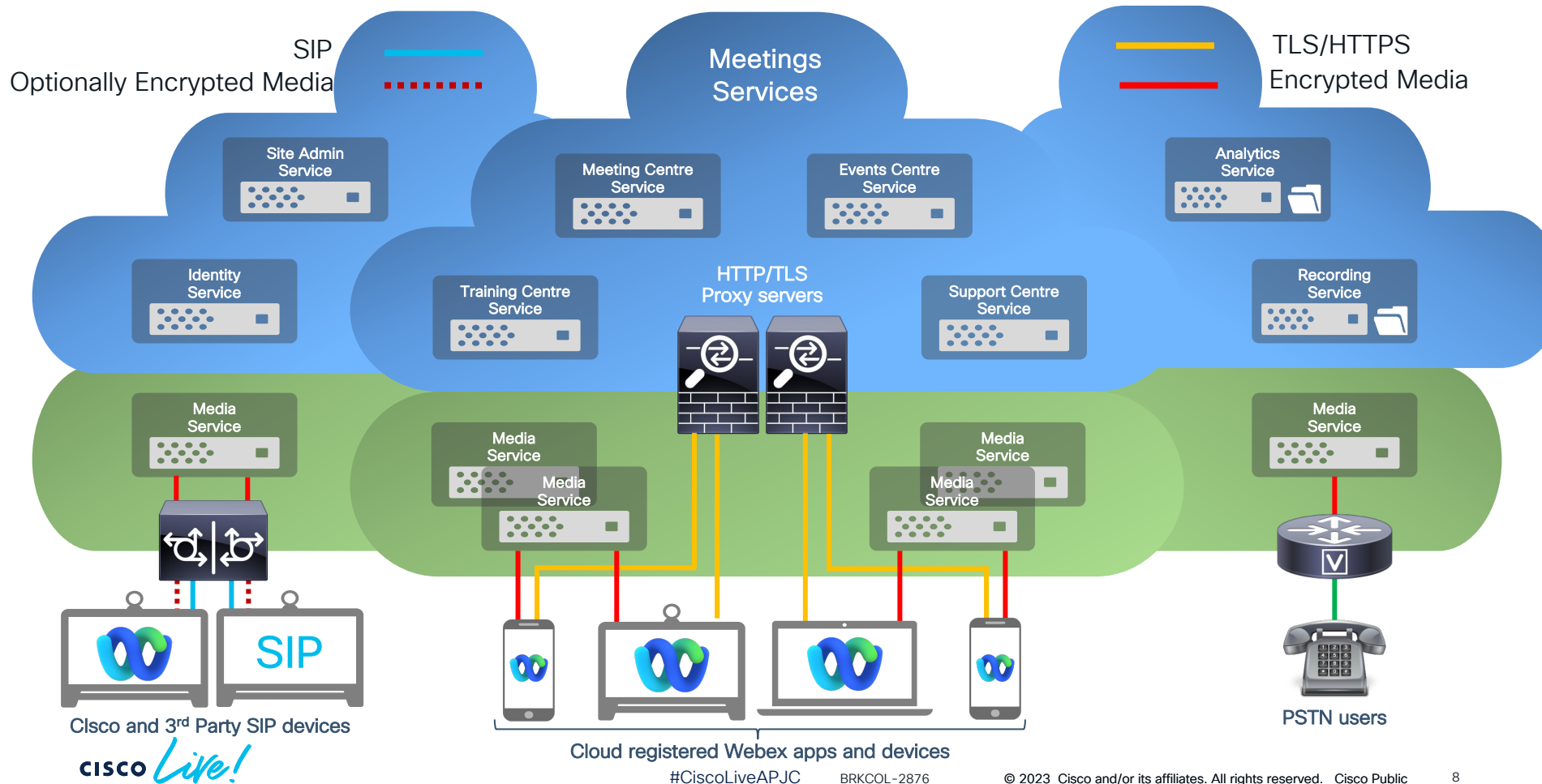
#CiscoLiveAPJC

Agenda

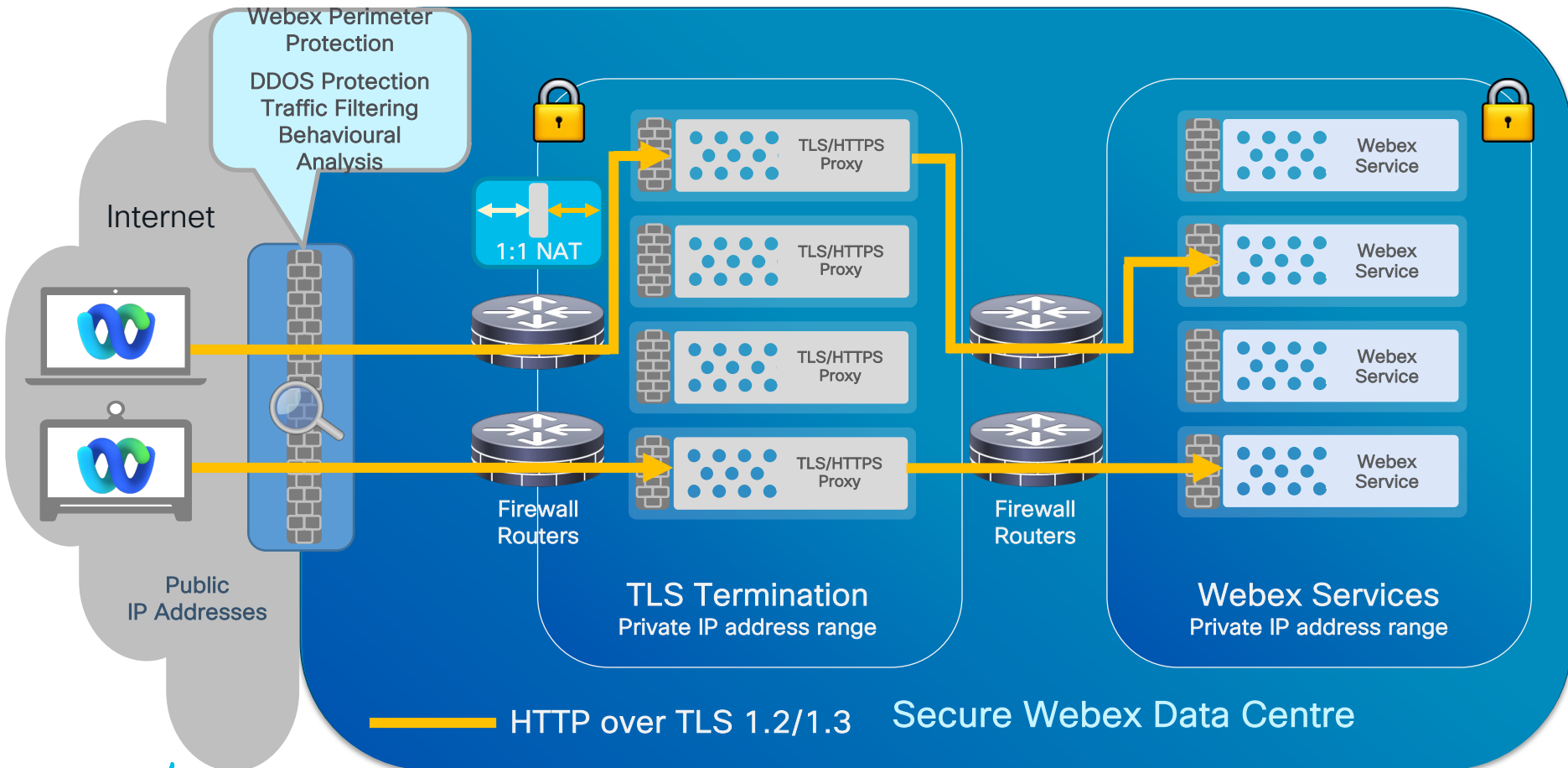
- Webex Meetings Platform and Architecture
- Webex Meeting Types
- Webex Meeting Security Features
- Fundamentals on firewall traversal
- Media and signaling considerations
- Traffic flows and network port usage
- Summary

Webex Meetings Platform and Architecture

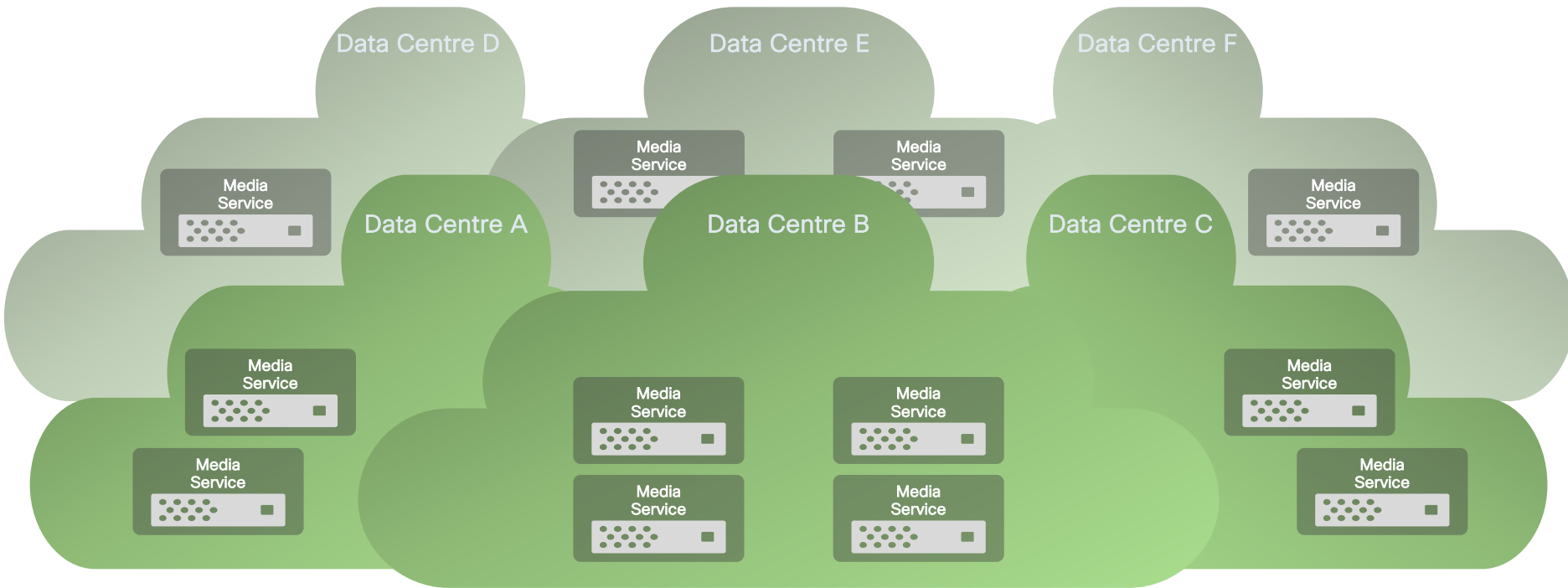
Webex Meetings Architecture



Webex encrypted HTTP signaling – TLS/HTTPS traffic

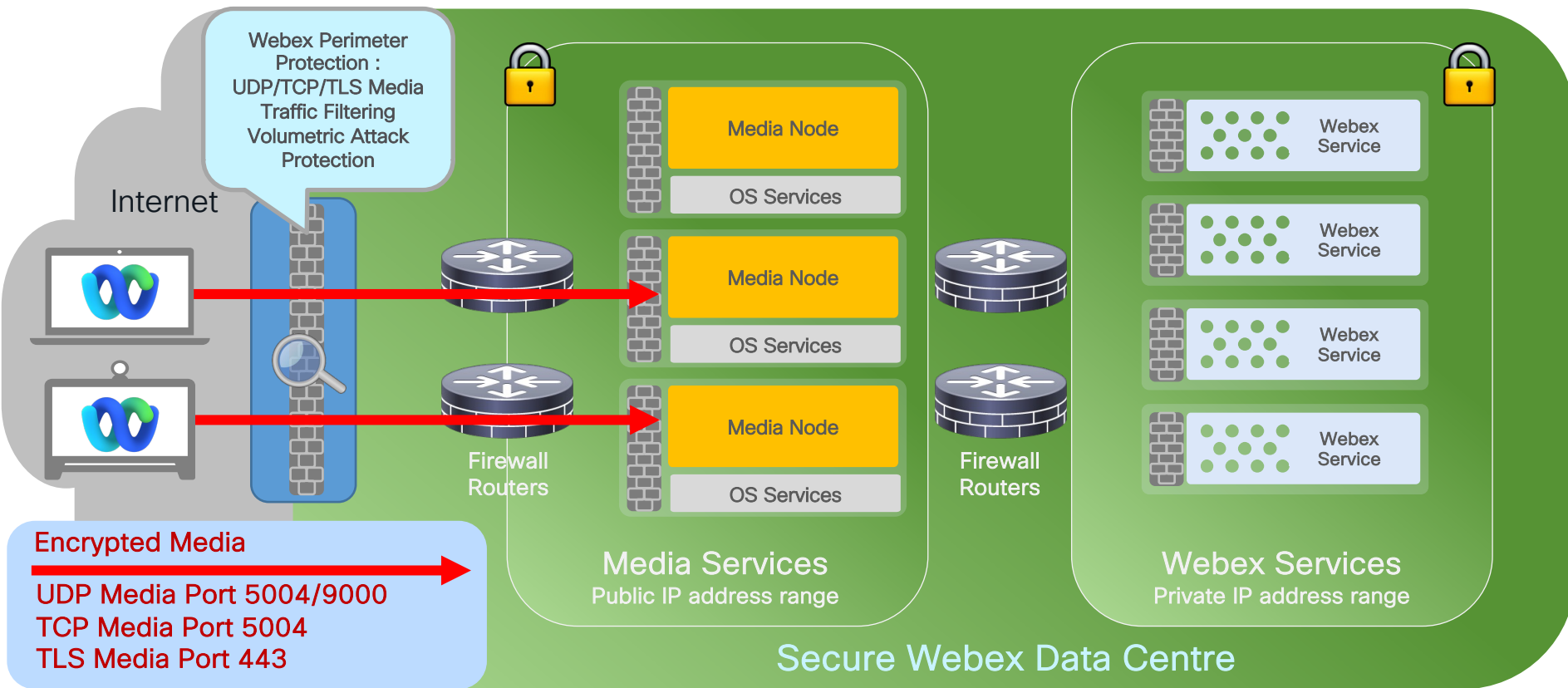


Webex Media Services



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

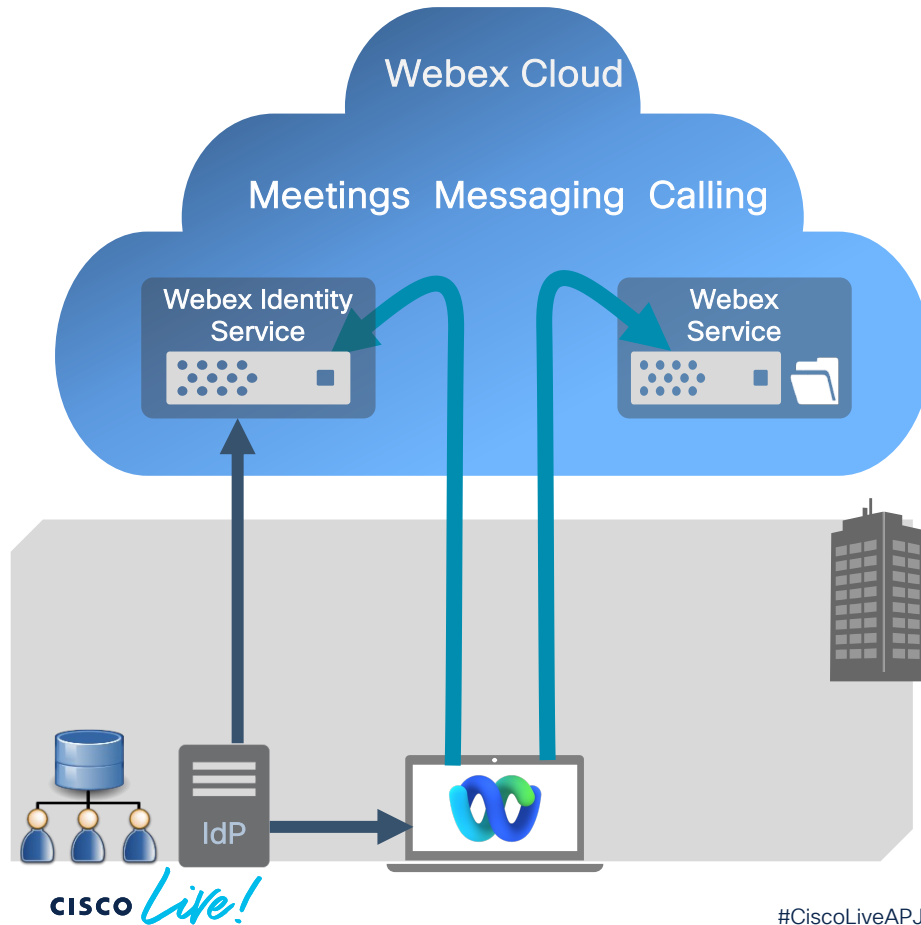
Webex Media Services : Encrypted Media



Webex Media Encryption cipher :

AEAD-AES-256-GCM

Webex App Login and Identity



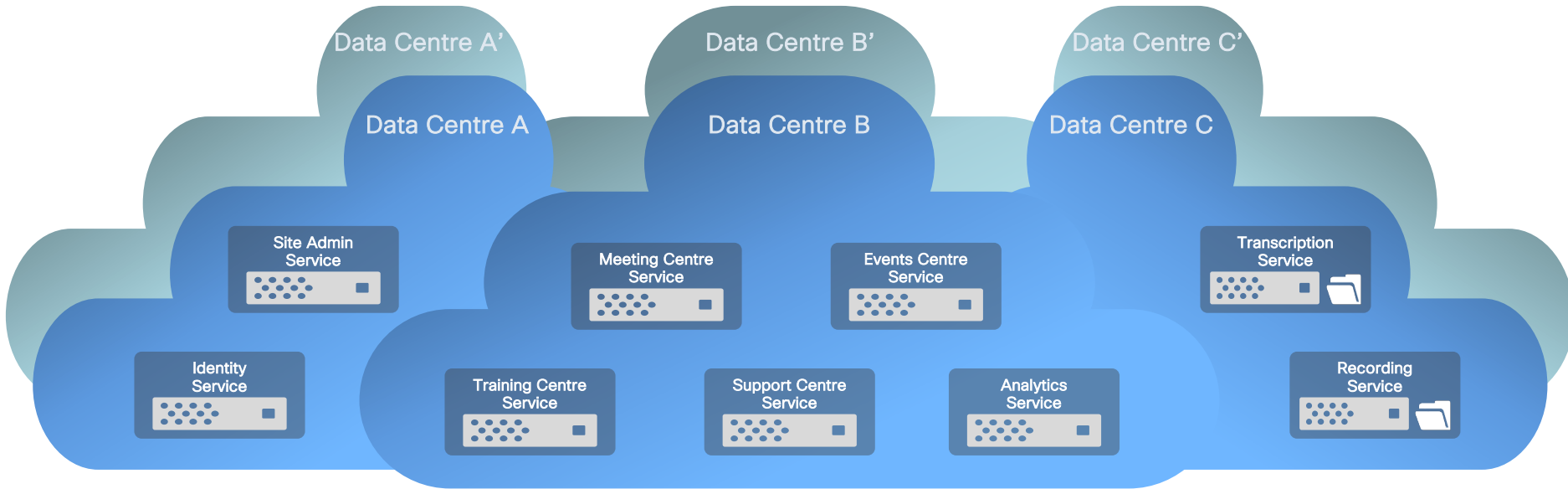
- 1) Webex app establishes a secure TLS connection with the Webex Cloud
- 2) Webex Identity Service prompts User for an e-mail ID
- 3) User Authenticated by Webex Identity Service, **or** Enterprise IdP (SSO)
- 4) Access Granted to Webex Services

For More: BRKCOL-2007

***Authentication, Authorization
and***

***Provision for Cisco
Collaboration***

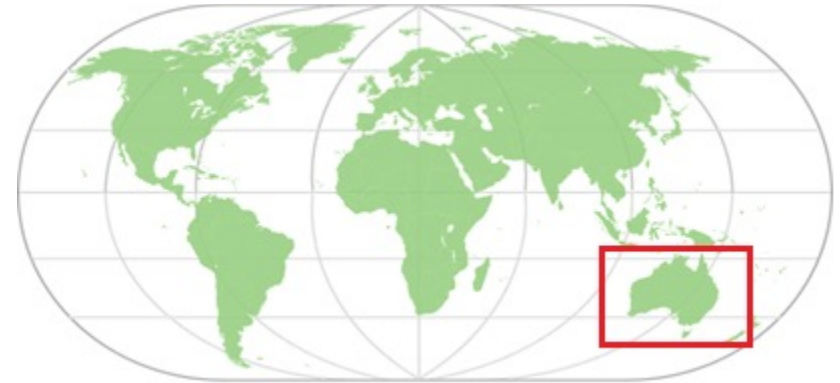
Webex Meetings Regions and Redundancy



- Webex Services for Webex Meetings/ Events/ Training/ Support, Identity, Recording, Transcription, are regionalized 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

- Webex Meetings usage, analytics, identity and billing information, including Webex Control Hub, served from additional global DC's in US/EU/Canada.
- Webex Messaging and Hybrid Calendar will also use these global DC's
- Australian customers currently use US DC's for these auxiliary functions, full Australian data residency planned for CY 2024
- Webex Calling and Contact Centre have additional regional data centers (including Australia)



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 government agencies
- Webex IRAP Assessment @ PROTECTED complete, includes Webex Meetings, Messaging, Calling, Control Hub, Webex for Developers
- Available at <https://trustportal.cisco.com>



Webex Meeting Types

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

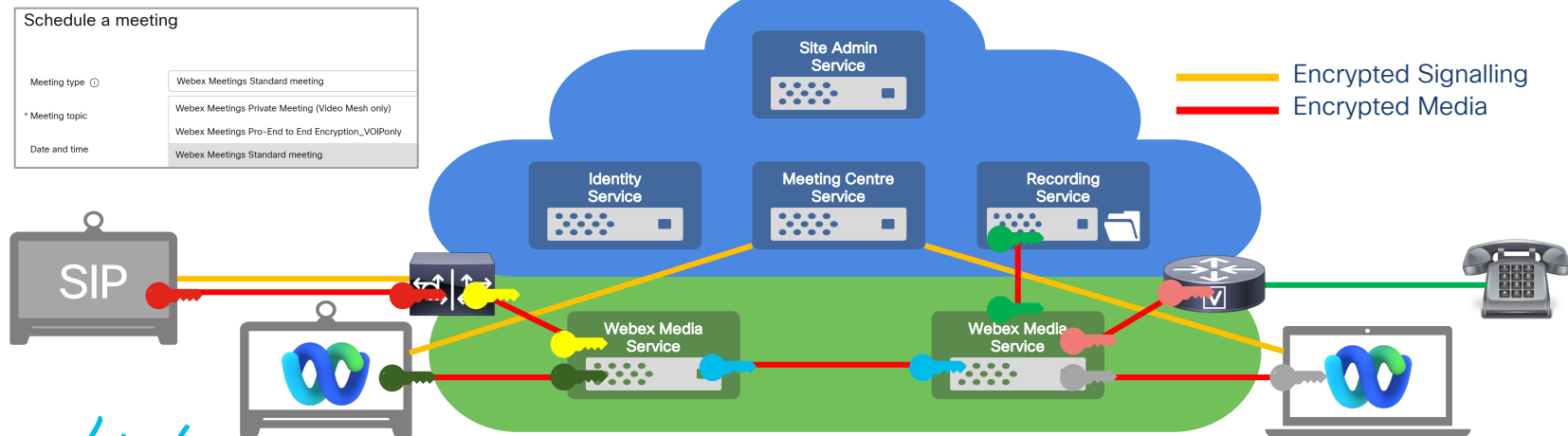
Encryption for standard Webex Meetings

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



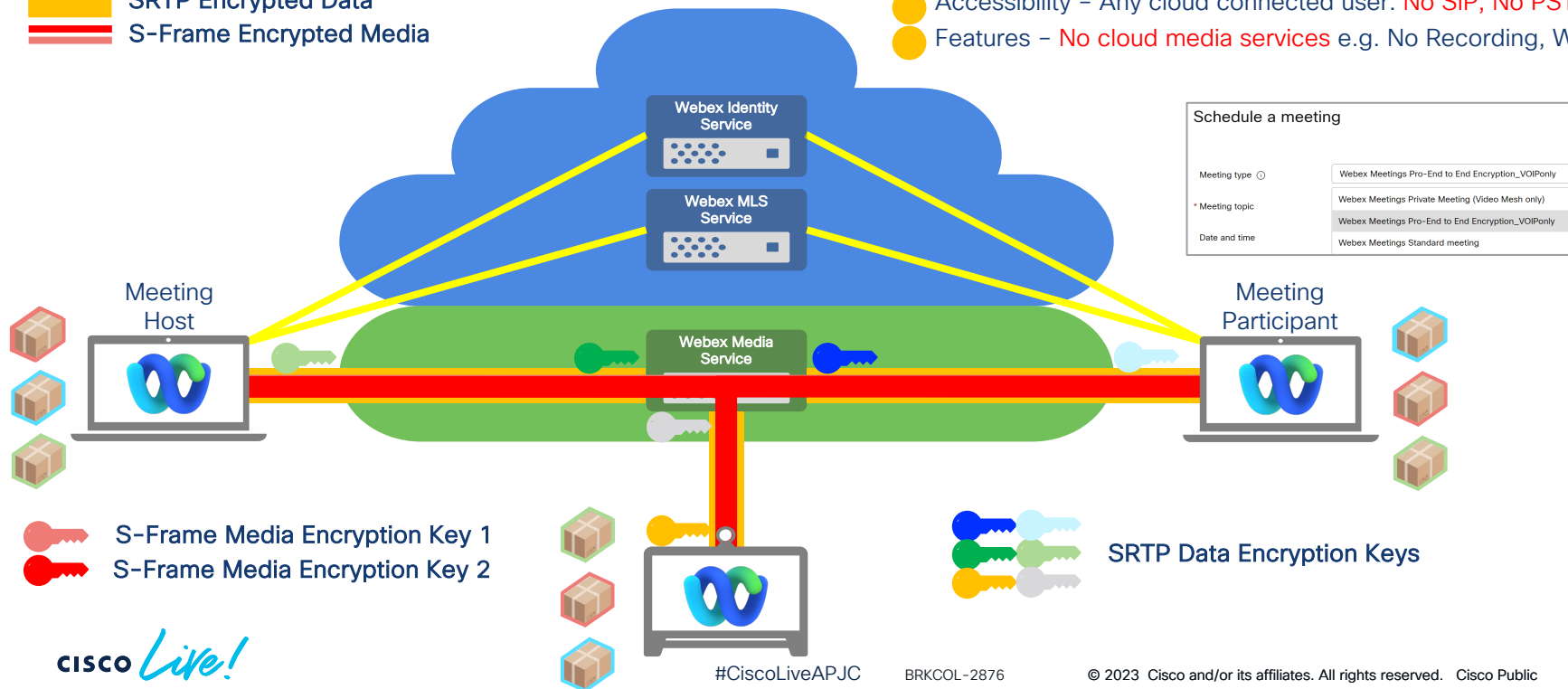
Webex Zero Trust End to End Encrypted Meetings

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>

- TLS/HTTPS
- SRTP Encrypted Data
- S-Frame Encrypted Media

- Privacy & Confidentiality (Cloud cannot decrypt media)
- Accessibility – Any cloud connected user. **No SIP, No PSTN**
- Features – **No cloud media services** e.g. No Recording, WXA etc



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 required
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)

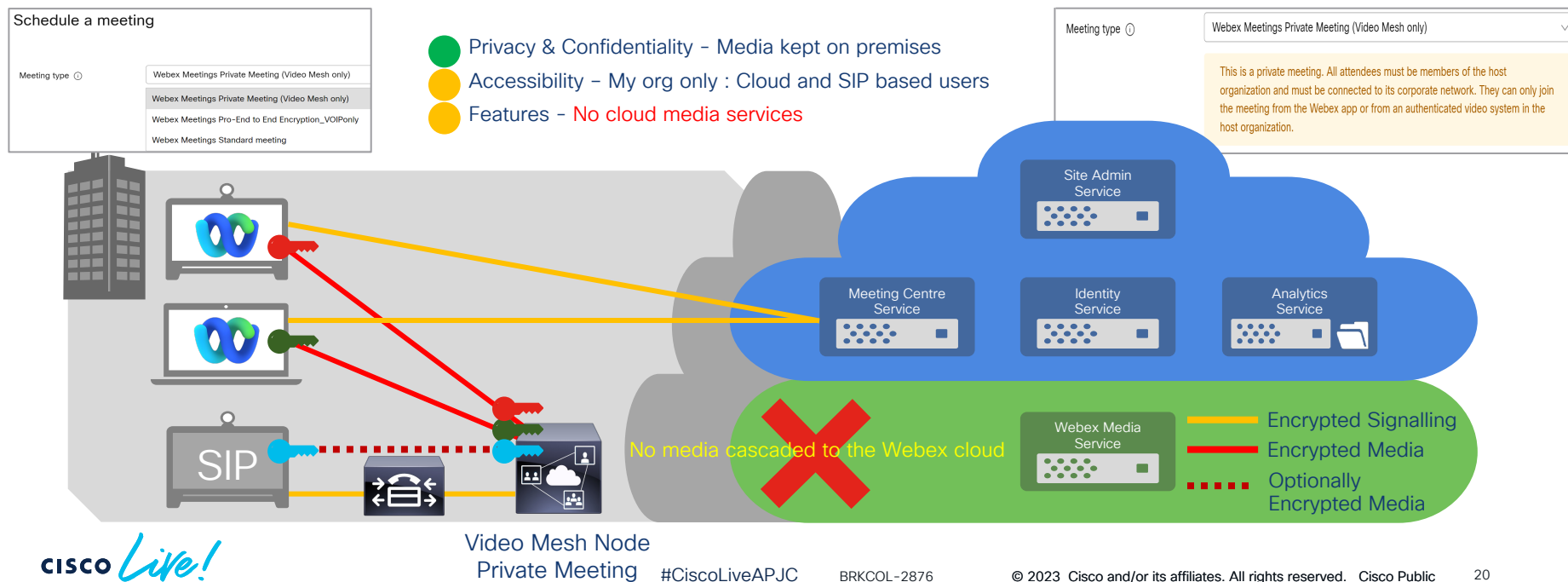
Zero Trust E2EE does not give Webex access to meeting encryption keys. This means that cloud services and endpoints that need to decrypt meeting content cannot participate in E2EE meetings : e.g.

PSTN and SIP endpoints
Cloud Recording
Webex Assistant
Meeting Transcription, Real-time translation, Closed captioning, Highlights
Remote Desktop Control (planned)
Web Browser based Webex App
SX, DX, and MX series devices

Private Webex Meetings

- All media is switched in the on premise 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



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'. Under 'Exclude password', the checkbox 'Exclude password from email invitation' is unchecked. The 'Automatic lock' section shows 'Automatically lock my meeting' set to 15 minutes after the meeting starts. The 'Unlocked meetings' section has the option 'Guests wait in the lobby until the host admits them' 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' (which is 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 settings are organized into sections. The 'Personal Room name' section shows 'Nick Halbert-Lillyman's Personal Room' with a note that the name must be between 1 and 128 characters. The 'Personal Room link' section shows a URL starting with 'https://', followed by '.webex.com/meet/' and a text input field containing 'abcdefgh'. The 'Automatic lock' section has a checked checkbox for 'Automatically lock my meeting' and a dropdown menu set to '15' minutes. A yellow warning box below this 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.' The 'Notification' section has an unchecked checkbox for 'Notify me by email when someone enters my Personal Room lobby while I am away'. The 'Cohosts' section has a checked checkbox for 'Allow cohosts for my Personal Room meetings' and a text input field with the placeholder 'Separate email addresses with a comma or semicolon'. The 'Mute attendees' section has three options: 'Allow the host and cohosts to unmute participants (Moderated unmute mode)' (unchecked), 'Allow attendees to unmute themselves in the meeting' (checked), and 'Always mute attendees when they join the meeting' (unchecked).

General My Personal Room Audio and Video Scheduling Recording

Please note that your host PIN can now be found under the Audio and Video section.

Personal Room name Nick Halbert-Lillyman's Personal Room
Your Personal Room name must be between 1 and 128 characters

Personal Room link https:// .webex.com/meet/ abcdefgh

Automatic lock: ☒ Automatically lock my meeting 15 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.

Notification: ☐ Notify me by email when someone enters my Personal Room lobby while I am away

Cohosts: ☒ Allow cohosts for my Personal Room meetings
Separate email addresses with a comma or semicolon

Mute attendees ☐ Allow the host and cohosts to unmute participants (Moderated unmute mode)
☒ Allow attendees to unmute themselves in the meeting
☐ Always mute attendees when they join the meeting

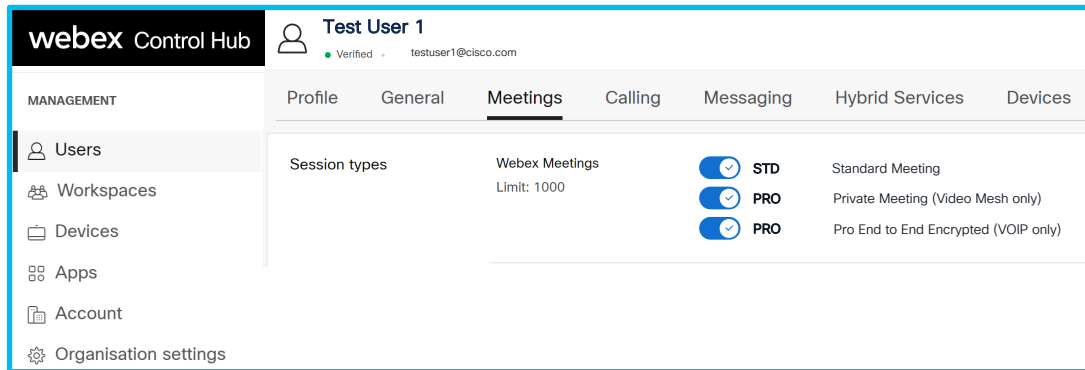
Assigning and Selecting Webex Meeting Types

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

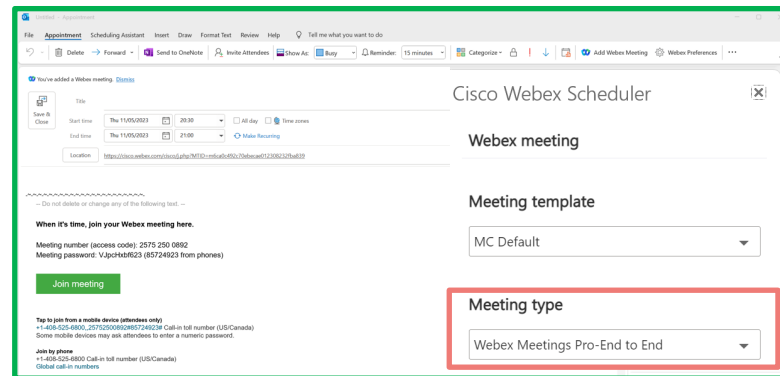


The screenshot shows the 'webex Control Hub' interface for 'Test User 1' (Verified, testuser1@cisco.com). The 'Meetings' tab is selected, showing 'Session types' with three options: 'Webex Meetings' (Limit: 1000), 'STD' (Standard Meeting), and 'PRO' (Private Meeting (Video Mesh only)). All three are enabled with blue checkmarks. The 'PRO' option is also labeled 'Pro End to End Encrypted (VOIP only)'.

Meeting Host/ Scheduler

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

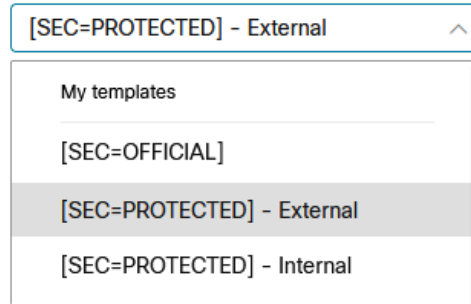
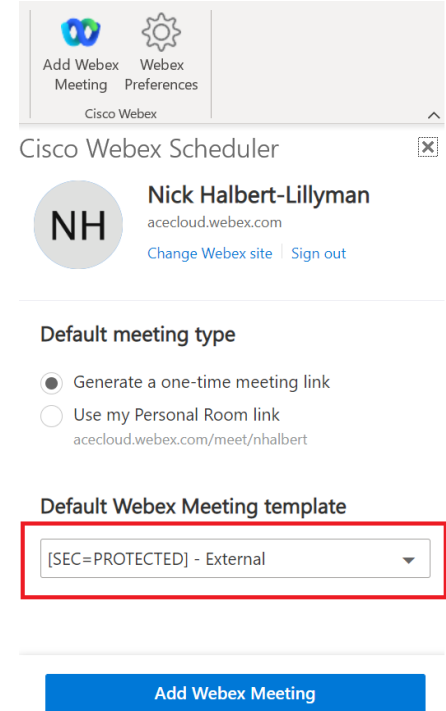
User selects their preferred meeting session type for the meeting



The screenshot shows the 'Cisco Webex Scheduler' interface. The 'Meeting type' dropdown is highlighted with a red box, showing 'Webex Meetings Pro-End to End' as the selected option. The interface also displays a 'Meeting template' dropdown set to 'MC Default' and a 'Join meeting' button.

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 or web GUI only)
- Users can also create their own templates, but cannot publish them to other users



Webex Meetings 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 recognizes 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 & Phone users

DTMF entered - meeting number & numeric password

PSTN/ IP Phones

- Audio only

Video system settings :

Enforce numeric meeting password when joining

Phone settings :

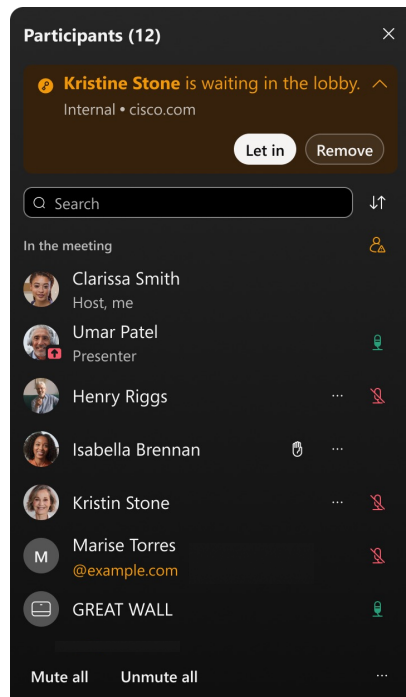
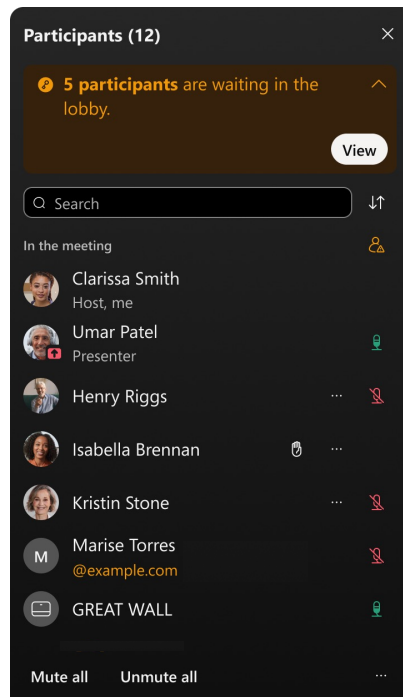
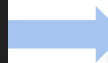
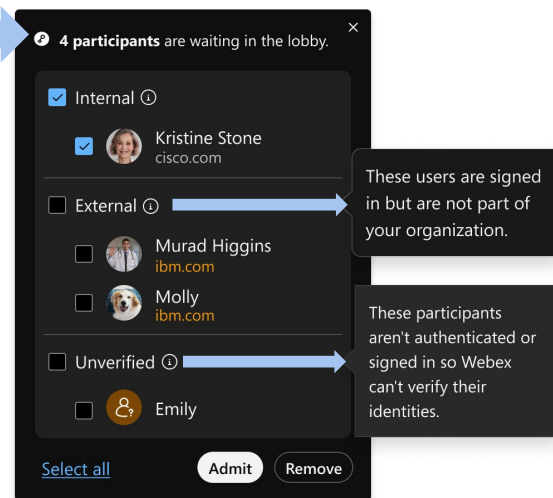
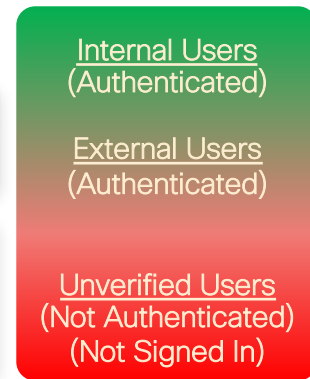
Require users to sign in before joining meeting

Enforce numeric meeting password when joining by phone

Webex Meetings : Host Controls

Admitting Users from the Lobby

Lobby : User Categories and User Identity information



Scheduled Meetings : Auto Admit feature

Authenticated, invited users & 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.

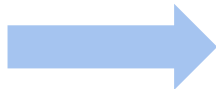
Choose what happens for people who aren't on the invite:

☐ 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.

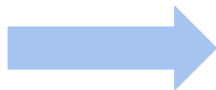
Choose what happens for people who aren't on the invite:

☐ 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

Webex Meetings Security Features : Lock

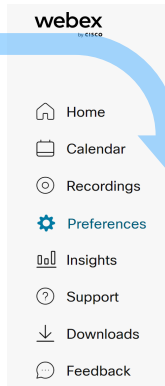
 Automatically lock

☐ 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



Preferences

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

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

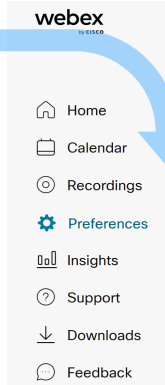
 Automatically lock

☒ 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



Preferences

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

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.

Personal Room Meeting Lobby Controls

New : Personal Room Lobby settings

Personal Room Security

Everyone in your organization can always join unlocked meetings.

Choose what happens for unverified users for unlocked meetings:

- ☐ They can join the meeting
- ☒ They wait in the lobby until the host lets them in
- ☐ They can't join the meeting

Choose what happens for verified external users for unlocked meetings:

- ☐ They can join the meeting
- ☒ They wait in the lobby until the host lets them in
- ☐ They can't join the meeting

Previously :

Guests = Unverified Users and verified (authenticated) External Users.

This can lead to lobby bloat in large meetings and a tendency for hosts to “admit all” rather than vet individual users

New settings :

Separate lobby controls unverified users and verified external users.

Allows administrators to apply different sets of controls for these groups of users, to reduce lobby bloat and meeting fraud

Recording – Local and Network Based

Meeting Host Recording entitlements

Start/Stop – Auto or manual

Record Audio & content only, or Audio, Video & 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 Centers

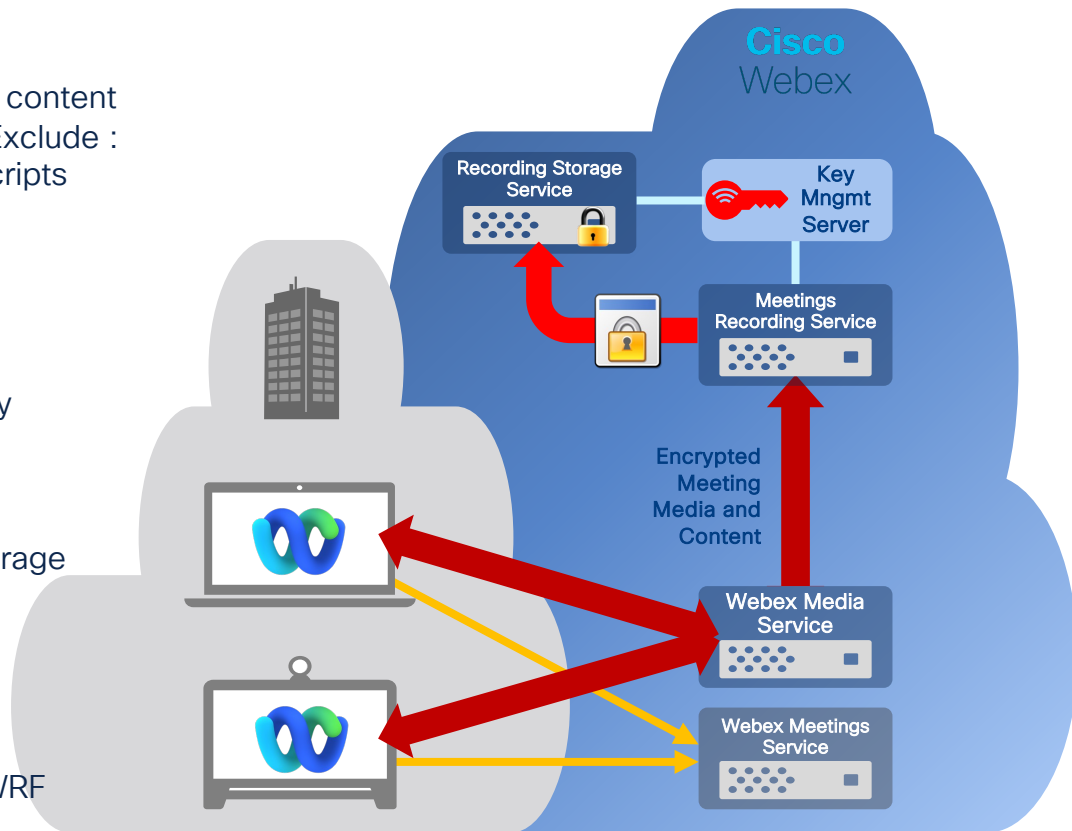
Encrypted using AES-256-GCM, optionally leverage customer managed keys (HDS, BYOK etc)

Configurable Retention period

Local Recording

Optionally enabled by site Admin

Meeting saved on host's computer as MP4 or WRF

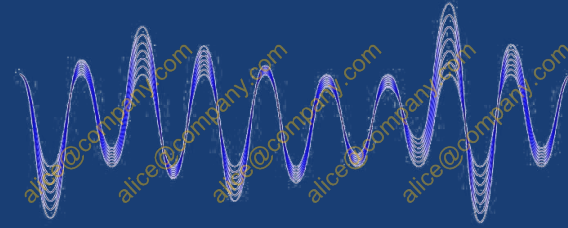


Audio & Video Watermarking

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 analyzes the recording and looks up unique identifiers. The results of the analysis show which participant shared the meeting content externally.

- In order to be analyzed, 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 analyze recordings for meetings hosted by people in your organization.
- Analyzed recordings are deleted as soon as the analysis is complete.

Analyze audio watermark x

Analysis name

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

Note

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

Overview

Alerts center

MONITORING

Webex Experience

Analytics

Troubleshooting

Reports

Troubleshooting

Meetings & Calls Live Meetings Status Admin Activities Logs Analyze watermark

Filter 3 Results

Analyze

Result name	Uploaded by	Status	Note	Upload time ▾
Norsk Take 2	Darrick Deel	Analysis succe...	Case 003	3/7/2023 12 PM
Norsk På 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

Webex Meetings – Video Watermarking

All Meeting Types supported

Visual Watermark for both shared content and video

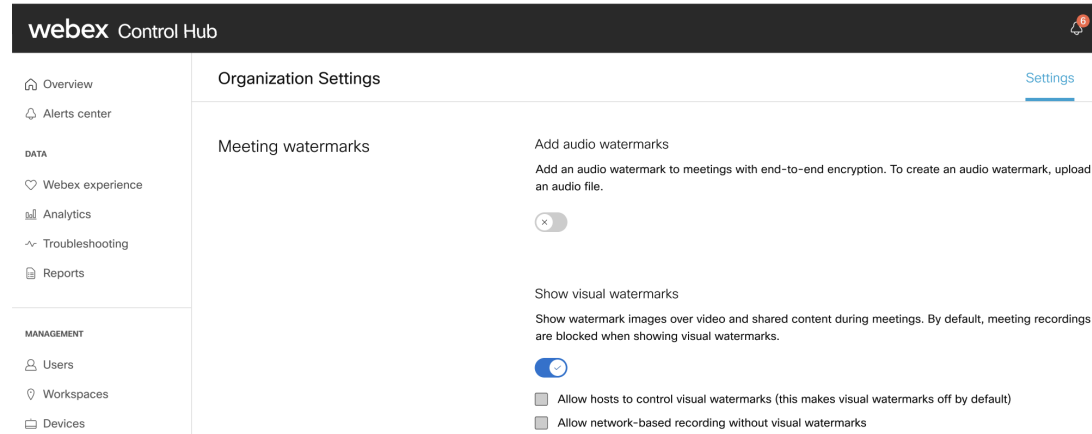
Webex app – Desktop, Mobile, Web

Authenticated users display email watermark

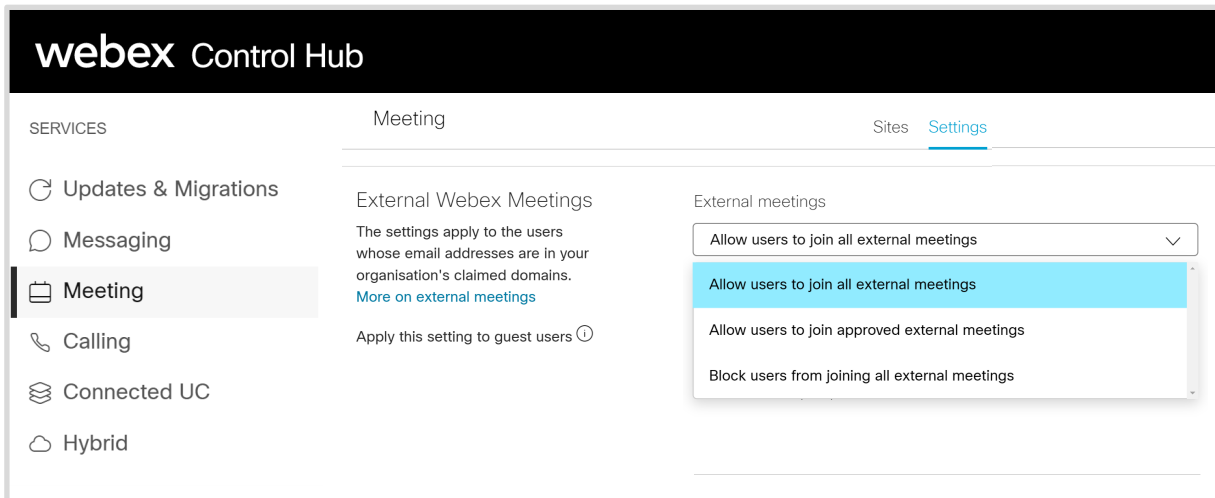
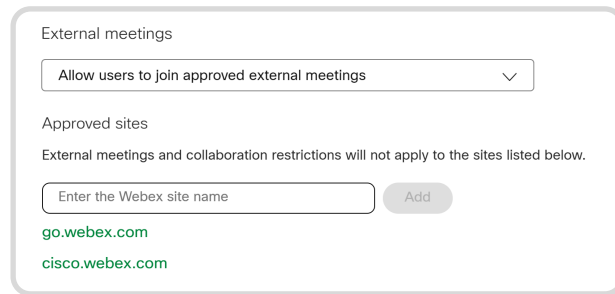
Unverified users display email and username

Local Recording automatically disabled

Network Recording optional



Controls for External Meetings



Default setting : Allow users to join all external meetings

Approved external sites only : All users in the org can join meetings hosted on these external sites*

- Templates can be used to apply external site restrictions to groups of users

Internal meetings only : Block users from joining all external meetings

Controls for External Meetings

The screenshot displays the Webex Control Hub interface. The top navigation bar is black with 'webex Control Hub' in white. Below it, a sidebar on the left lists 'SERVICES' including Updates & Migrations, Messaging, Meeting (highlighted), Calling, Connected UC, and Hybrid. The main content area is titled 'Meeting' and has tabs for 'Sites' and 'Settings' (selected). Under 'Settings', there's a section for 'External Webex Meetings' with a description and a link to 'More on external meetings'. Below this, a toggle switch 'Apply this setting to guest users' is shown. The 'External meetings' section contains a dropdown menu set to 'Allow users to join all external meetings'. The interface is divided into three columns of settings, each with a toggle switch and a list of options: 'Collaboration tools' (Annotation, Polling, Q&A), 'In meeting' (Chat, Closed captioning, File transfer, Participant list, Take presenter, Webex Assistant), and 'Recording' (Cloud recording, Local recording). The 'Remote control' section includes 'Enable remote control' (toggled on) with sub-options for Application, Desktop, and Web browser remote control. The 'Sharing' section includes 'Enable sharing' (toggled on) with sub-options for Application, Desktop, Doc and presentation sharing, Whiteboard, and Web browser sharing. The 'Video' section includes 'Turn on video' (toggled on) with sub-options for Standard definition (360p) and High definition (720p).

webex Control Hub

SERVICES

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

Meeting

Sites Settings

External Webex Meetings

The settings apply to the users whose email addresses are in your organisation's claimed domains.
[More on external meetings](#)

Apply this setting to guest users ⓘ

External meetings

Allow users to join all external meetings ▼

Collaboration tools

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

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

Remote control

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

Sharing

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

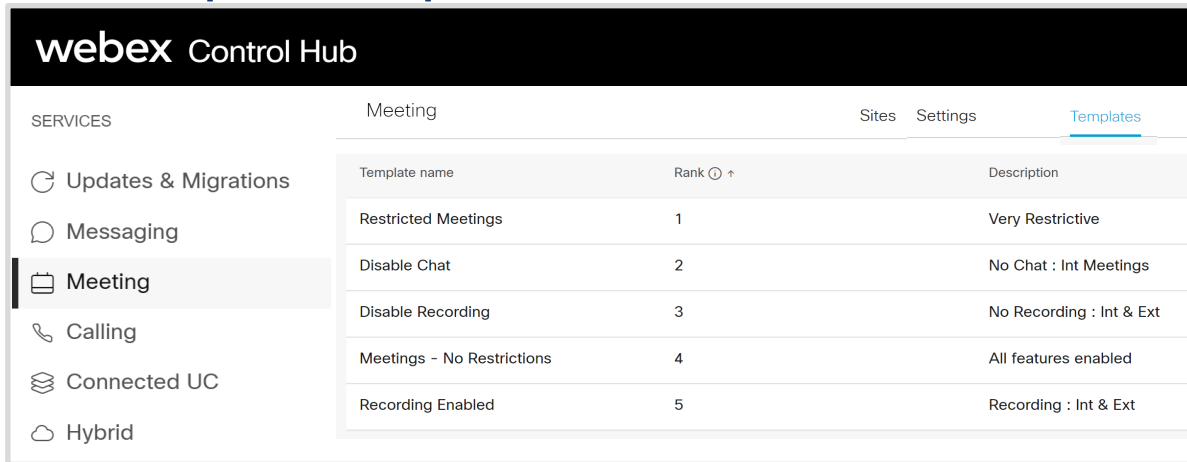
Video

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

These controls apply when users in your org join any external meeting

These controls do not apply to users joining internal meetings

Group Templates & Controls for Meetings



The screenshot shows the Webex Control Hub interface. On the left is a sidebar with a 'SERVICES' menu containing: Updates & Migrations, Messaging, Meeting (highlighted), Calling, Connected UC, and Hybrid. The main content area is titled 'Meeting' and has tabs for 'Sites', 'Settings', and 'Templates' (which is selected). Below the tabs is a table of meeting templates.

Template name	Rank 	Description
Restricted Meetings	1	Very Restrictive
Disable Chat	2	No Chat : Int Meetings
Disable Recording	3	No Recording : Int & Ext
Meetings - No Restrictions	4	All features enabled
Recording Enabled	5	Recording : Int & Ext

Templates are an easy way to apply bulk settings to multiple users and groups

When a user belongs to multiple groups, they'll get their settings from the highest ranked template.

For example, John belongs to two groups. Only one meeting template can be applied to a group. While Template A and Template B are applied to two separate groups, John receives his settings from the highest-ranked template : e.g. Template A.

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 & Version

Client Version.....

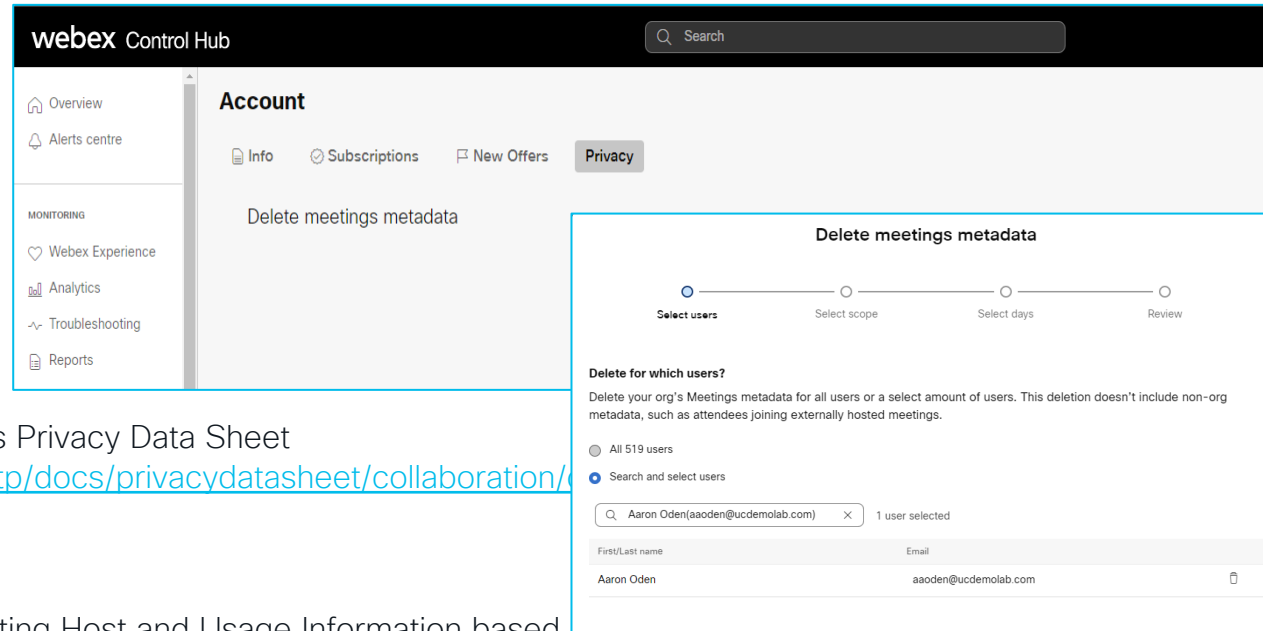
Host Name and email address

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/sheet.pdf>

Control Hub -> Account -> Privacy

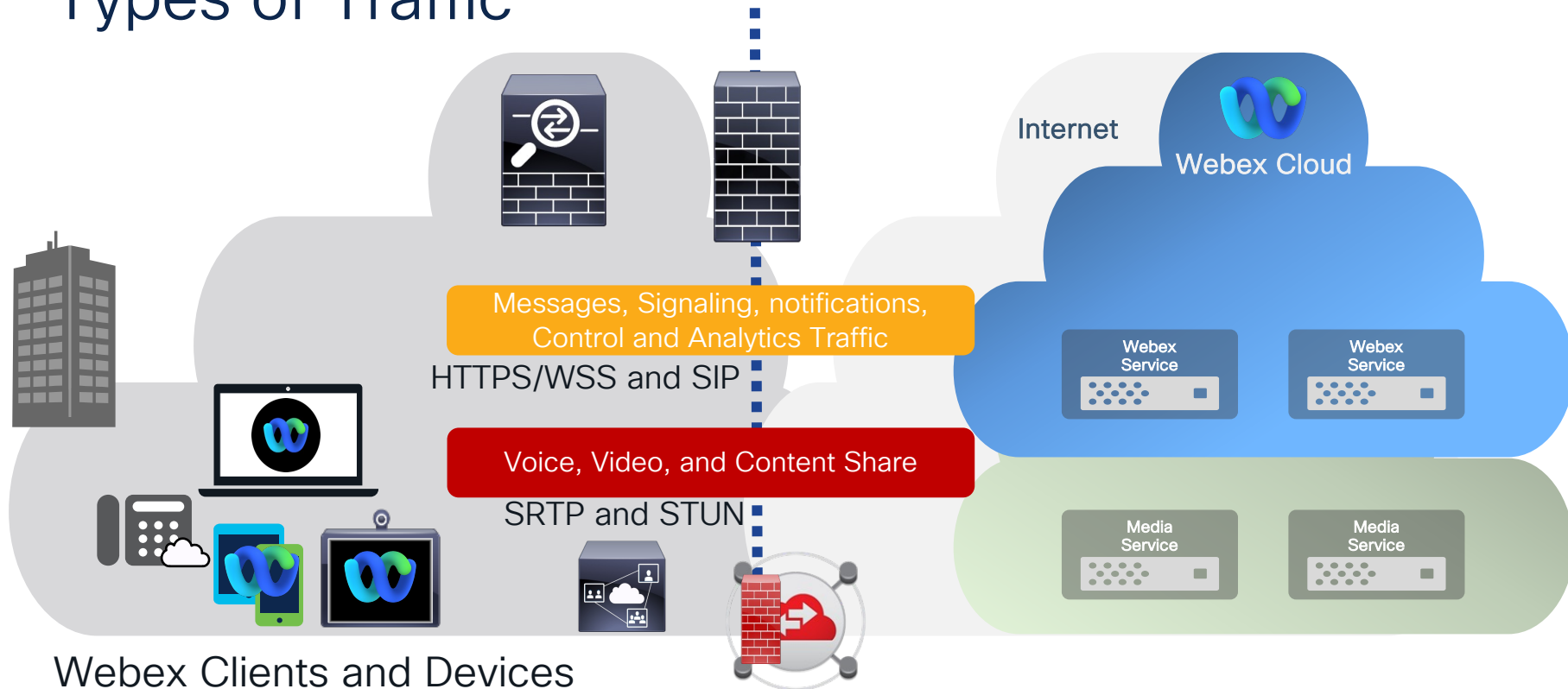
Allows and administrator to delete Meeting Host and Usage Information based on meeting host name

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

5-tuple:

- Source IP
- Destination IP
- Source Port
- Destination Port
- Protocol

Initiated Traffic

Return Traffic

Return traffic automatically allowed* (TCP and even UDP** with symmetric traffic)

Internet

Webex Cloud

Webex Service

Webex Service

Media Service

Media Service

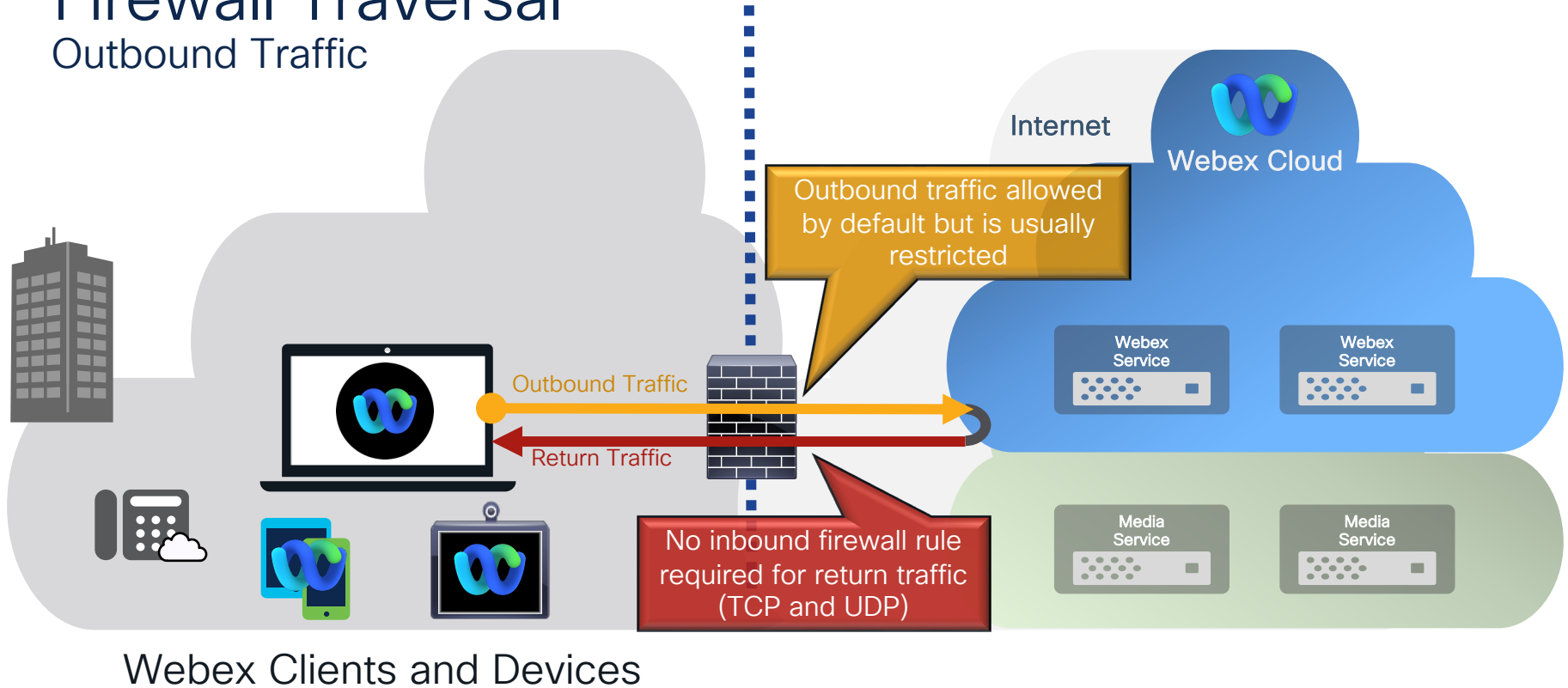
Webex Clients and Devices

* With most firewalls

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

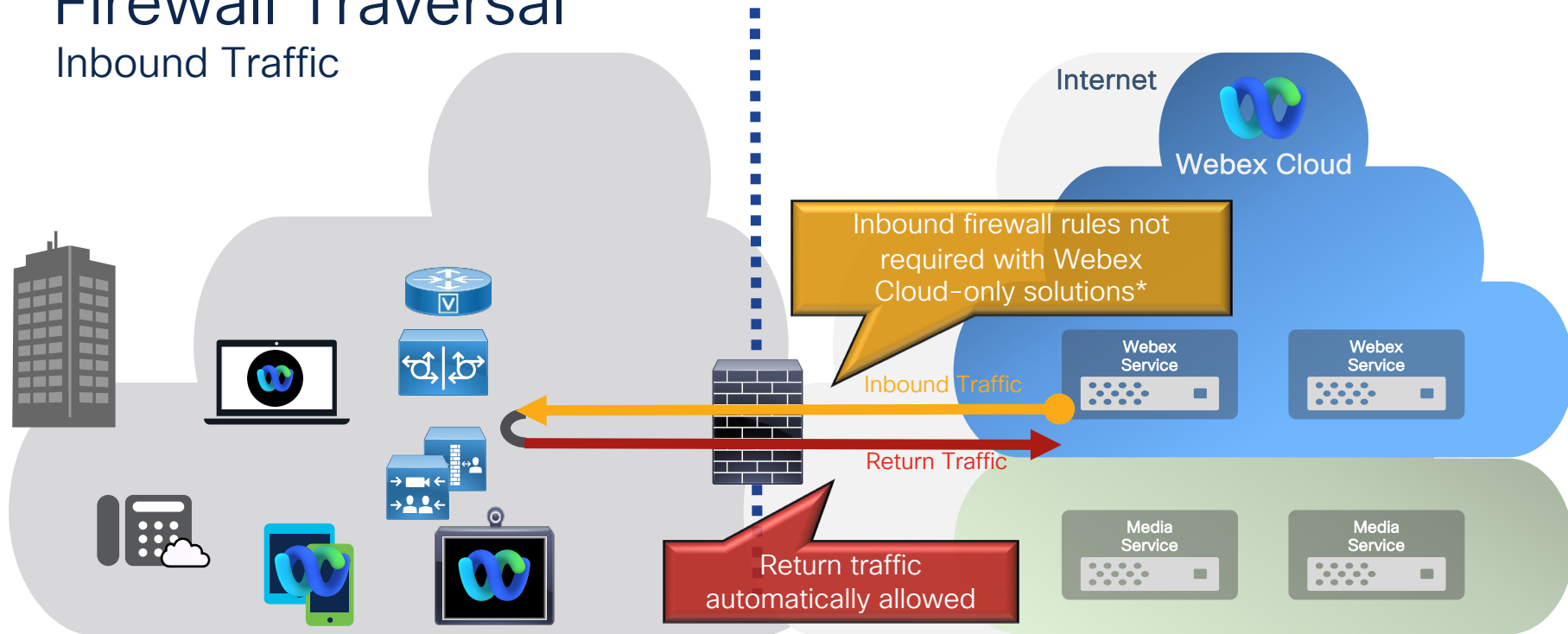
Firewall Traversal

Outbound Traffic



Firewall Traversal

Inbound Traffic

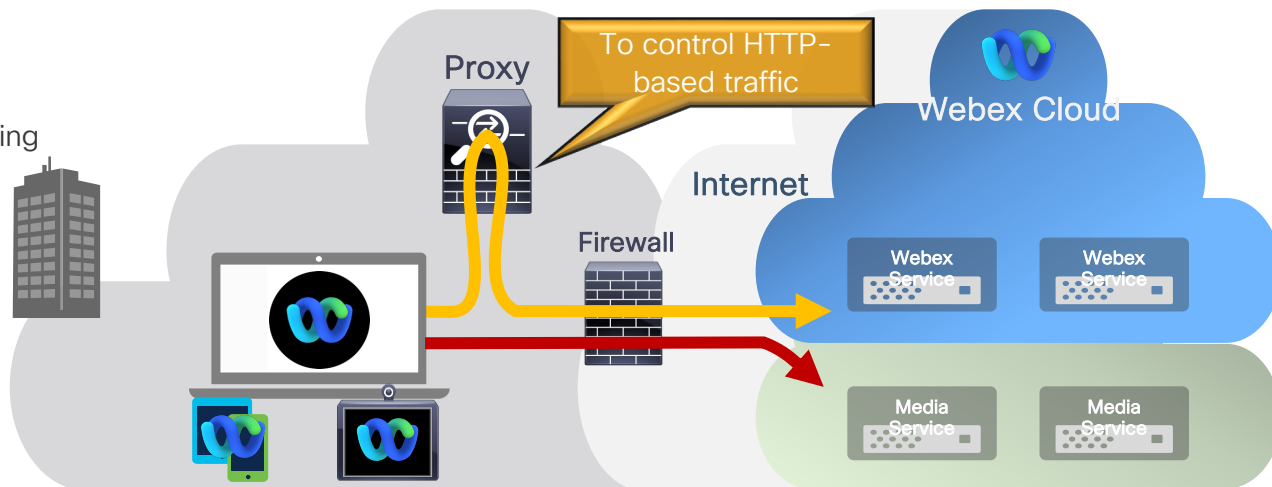


Webex Clients and Devices

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

Proxy

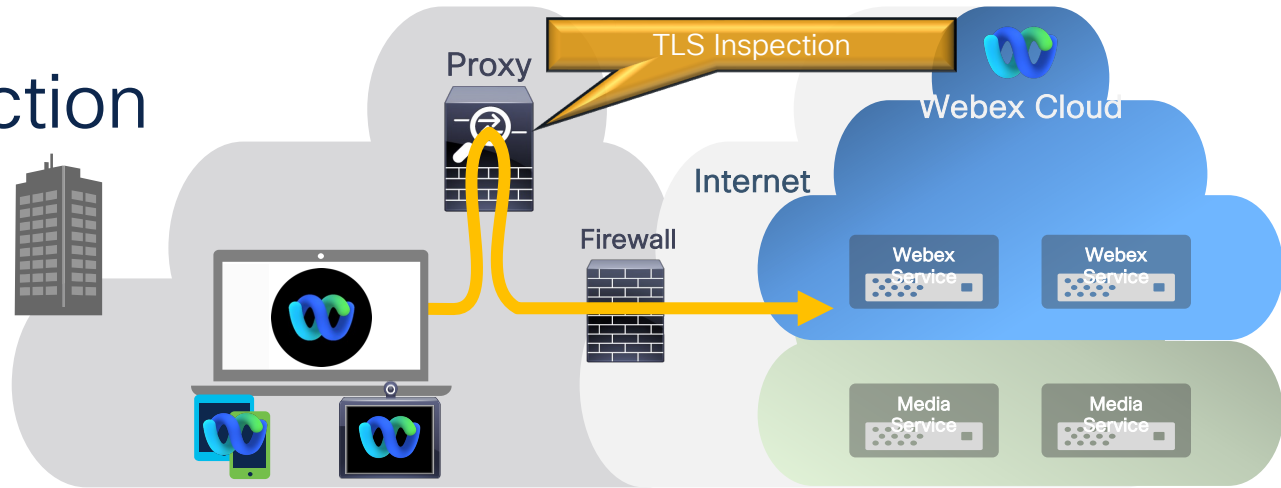
- HTTPS/WSS Signalling
- Encrypted Media



- 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
 - ~~UDP / TCP 33434 – being deprecated~~
 - 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 😊

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

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”
- Still preferable than sending media via proxy!

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)													

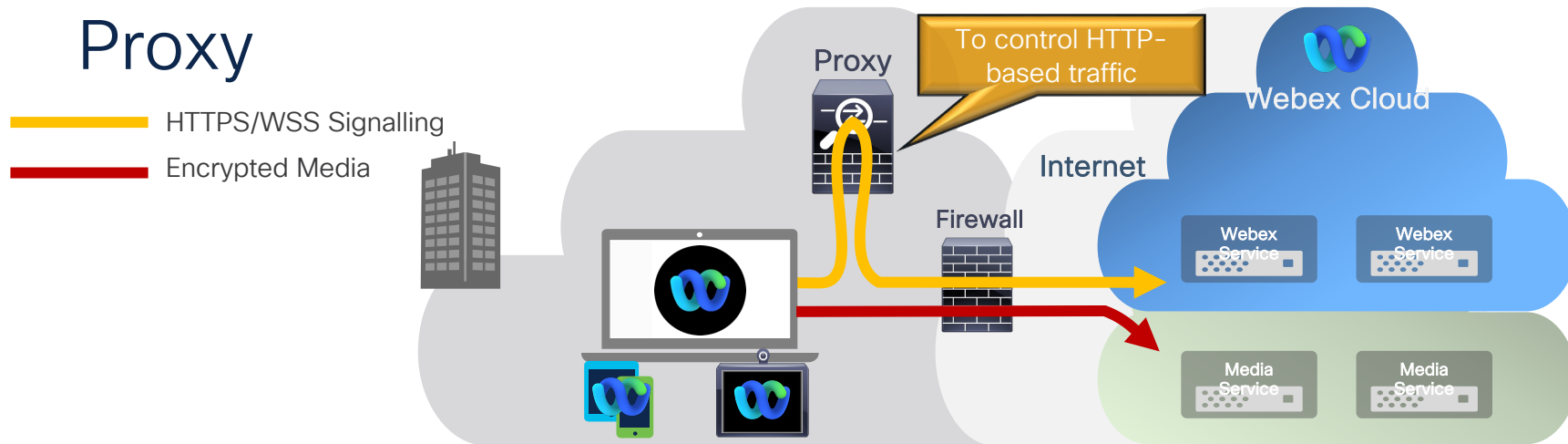
See above for a real-world example from a third party firewall in a customer’s deployment;

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

Included Ports:

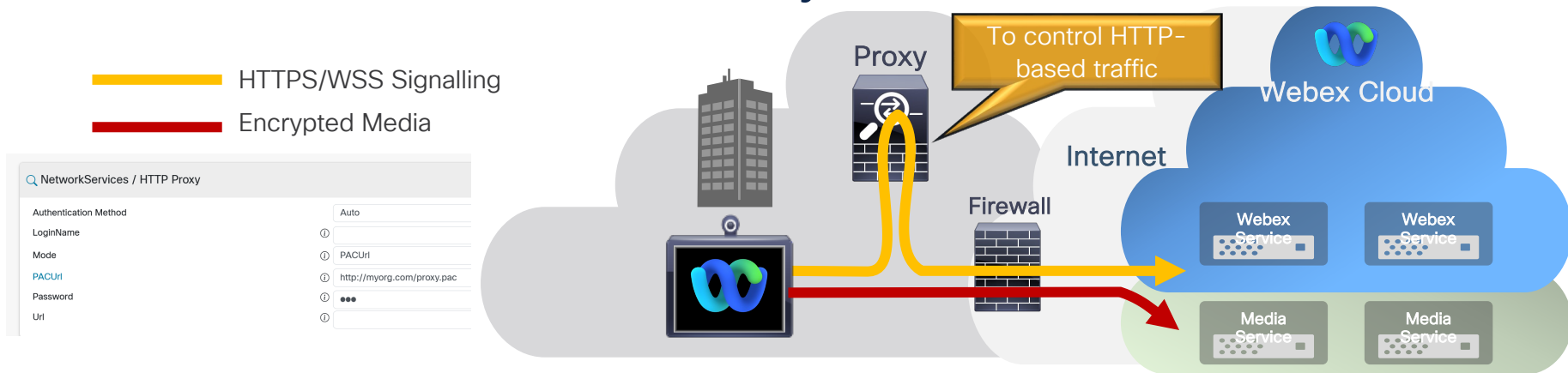
5004, 9000, 443
1719-1720, 5060-5070, 8000 – 59999

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
- Either disable TLS inspection, or manually load enterprise CA to Webex Device trust ***and*** log TAC case to upload customer certificates to Webex cloud
- As of October RoomOS 11.8, media via proxy is supported for Webex devices but off by default – **direct UDP still highly recommended for media:**

CLI commands:

```
xConfiguration Webex Meetings HttpProxyForMedia Allowed: True
```

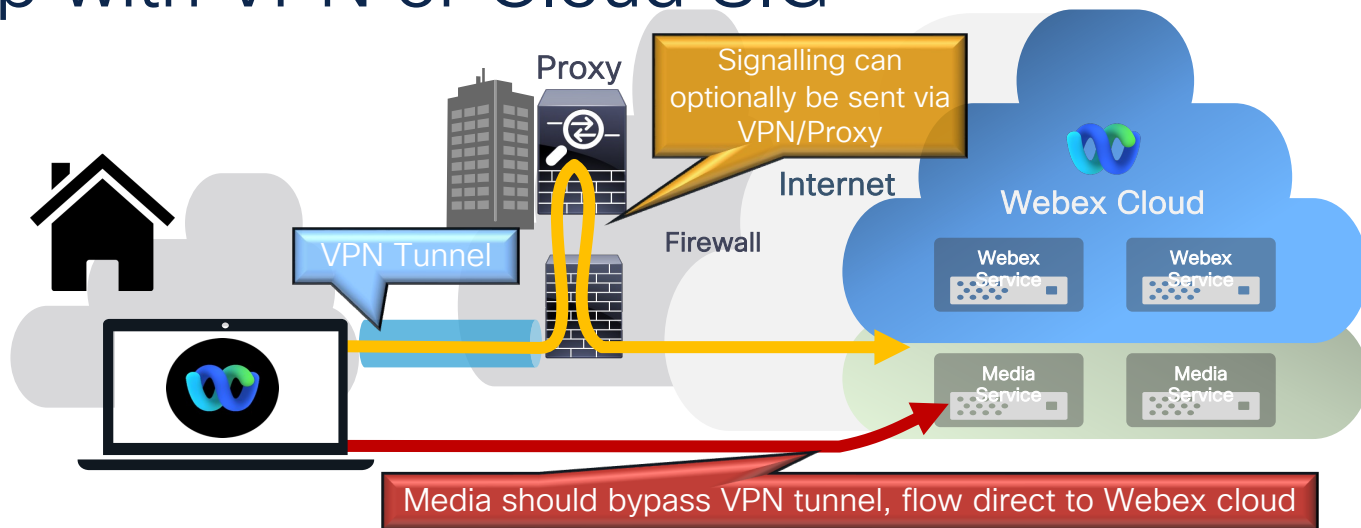
```
xConfiguration Webex Meetings HttpProxyForMedia Mode: Auto
```

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

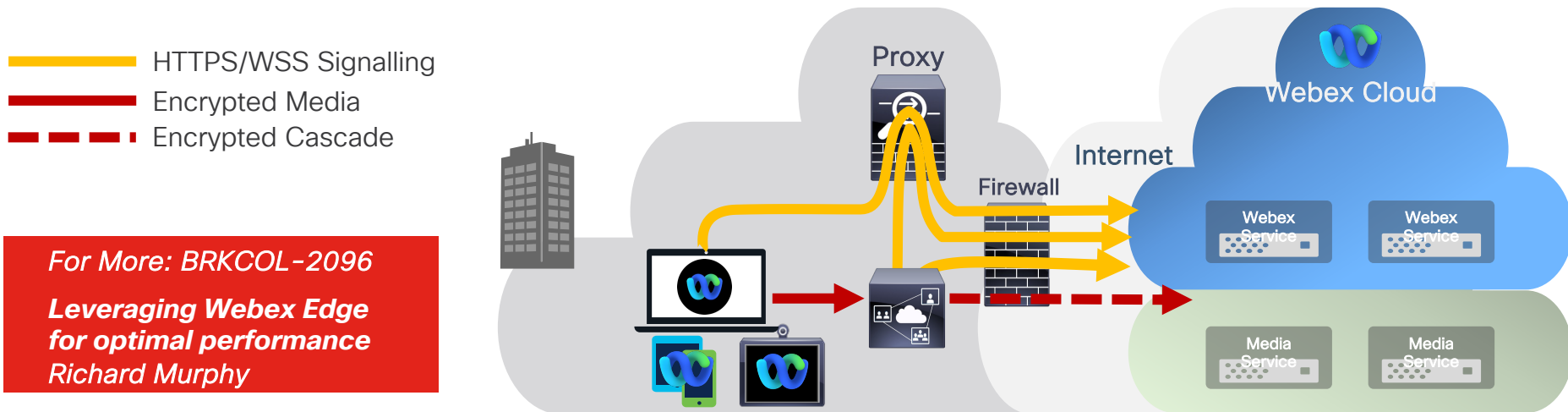
Function	Web Proxy Deployment	Direct Media Deployment
Traffic Filtering	Destination URL	5-tuple (source/dest port, source/dest IP, protocol)
TLS Inspection	Can inspect signaling. Media encrypted, cannot be inspected, inspection may be disabled entirely due to this.	Can still send signaling via Web Proxy. 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 principals 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)



For More: BRKCOL-2096

***Leveraging Webex Edge
for optimal performance
Richard Murphy***

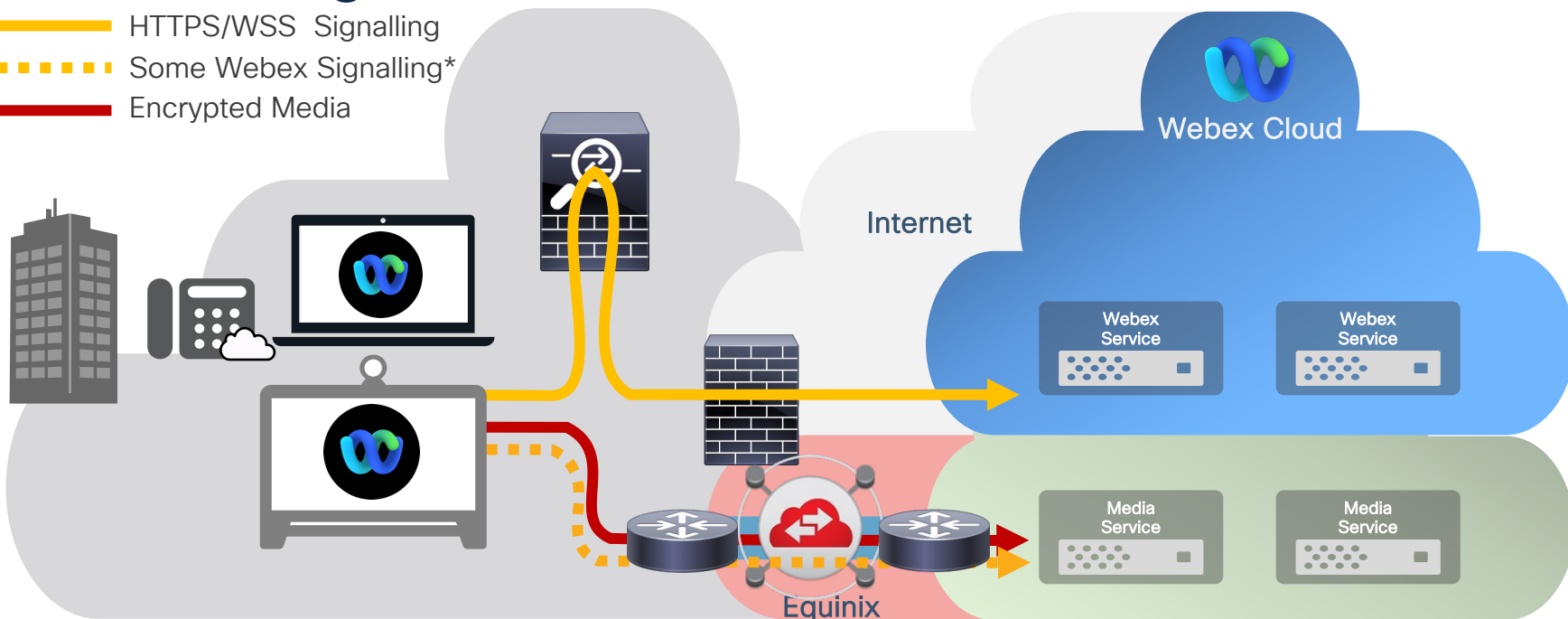
- Media conferencing is processed by VMN, media traffic stays on-prem if no need to cascade media due to participants outside.
- Benefit for firewall rule: Supported outbound media traffic is now sourced from VMN
- *Now supports Webex App for Meetings (requires Webex Suite Meeting Platform)*

Webex Edge Connect

———— HTTPS/WSS Signalling

..... Some Webex Signalling*

———— Encrypted Media



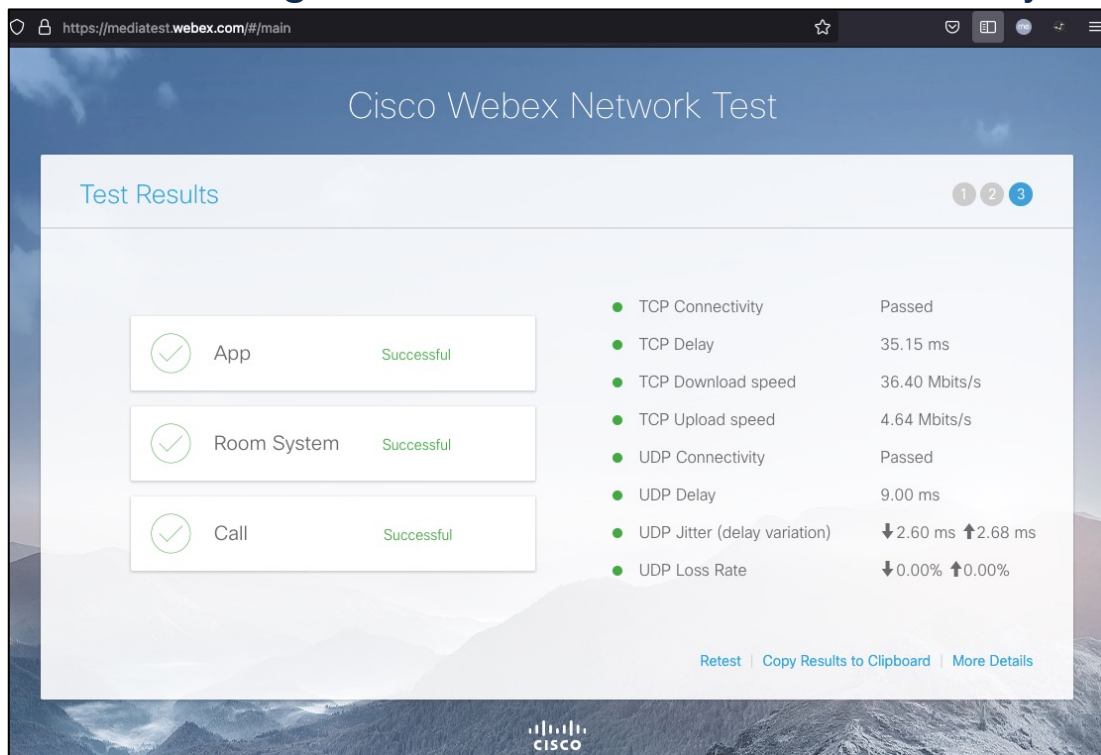
- Private link, better QoS, and insulated from the Internet

*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

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>

← → ↺

🔒 📄 📄 https://cscan.webex.com

☆ 📄 📄 📄

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: 100.0.0.0

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

Test Again

Test Another Server

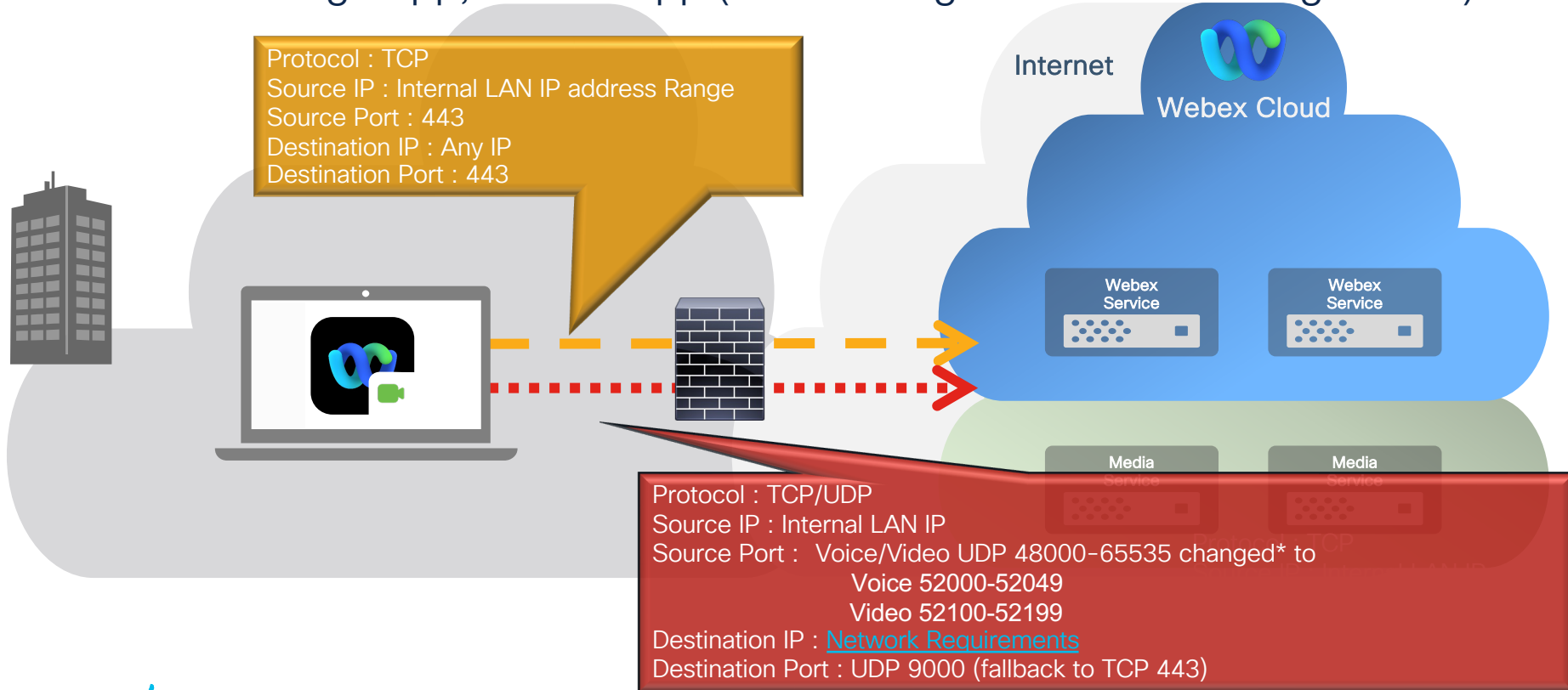
Download this Report

Traffic Flows and Network Port Usage

Protocols and Ports used by Webex

Webex Meetings App, Webex App (Old Meeting Platform – Meeting Centre)

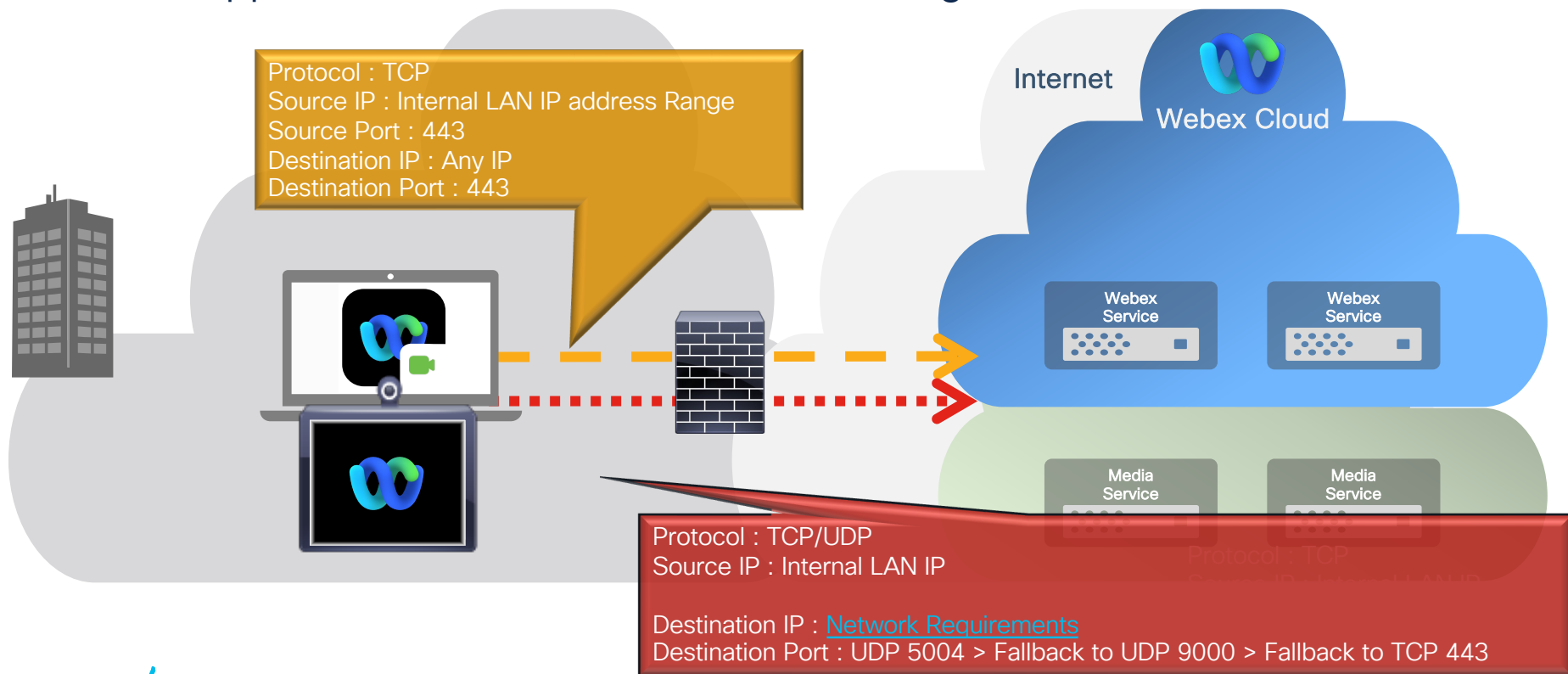
— Signaling/Other Control
- - - Real Time Traffic



Protocols and Ports used by Webex

Webex App and Devices – Webex Suite Meetings Platform

— 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)

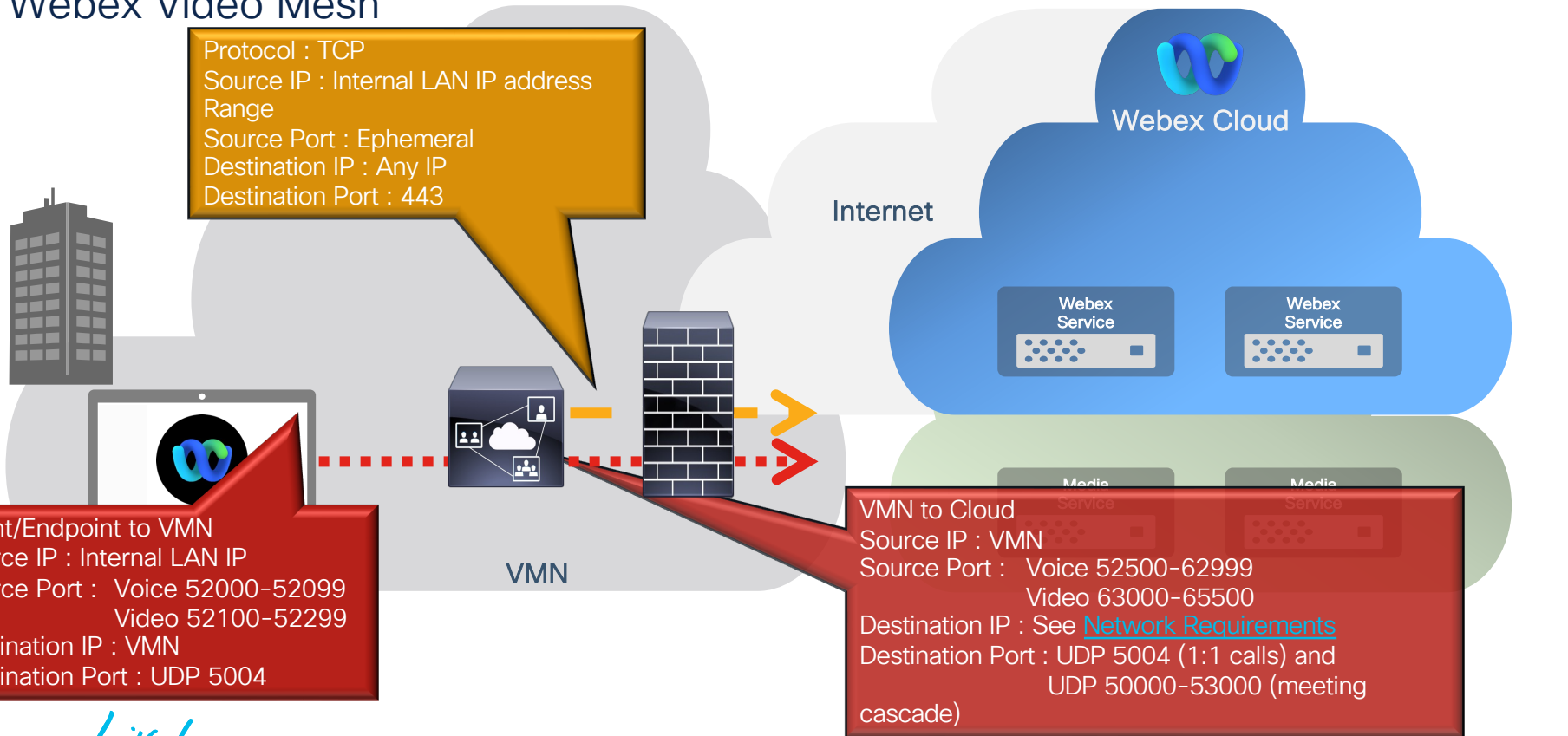
Reference link:

[Port Reference Information for Webex Calling](#)

Protocols and Ports used by Webex

Webex Video Mesh

— Signaling/Other Control
- - - Real Time Traffic



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



Internet

MS Teams Cloud

Webex Cloud

Service: Webex

Protocol : TCP + UDP

Destination IP : [Webex Requirements](#)

Destination Port : TCP + UDP 5004, UDP 9000

Service: MS Teams

Protocol: UDP

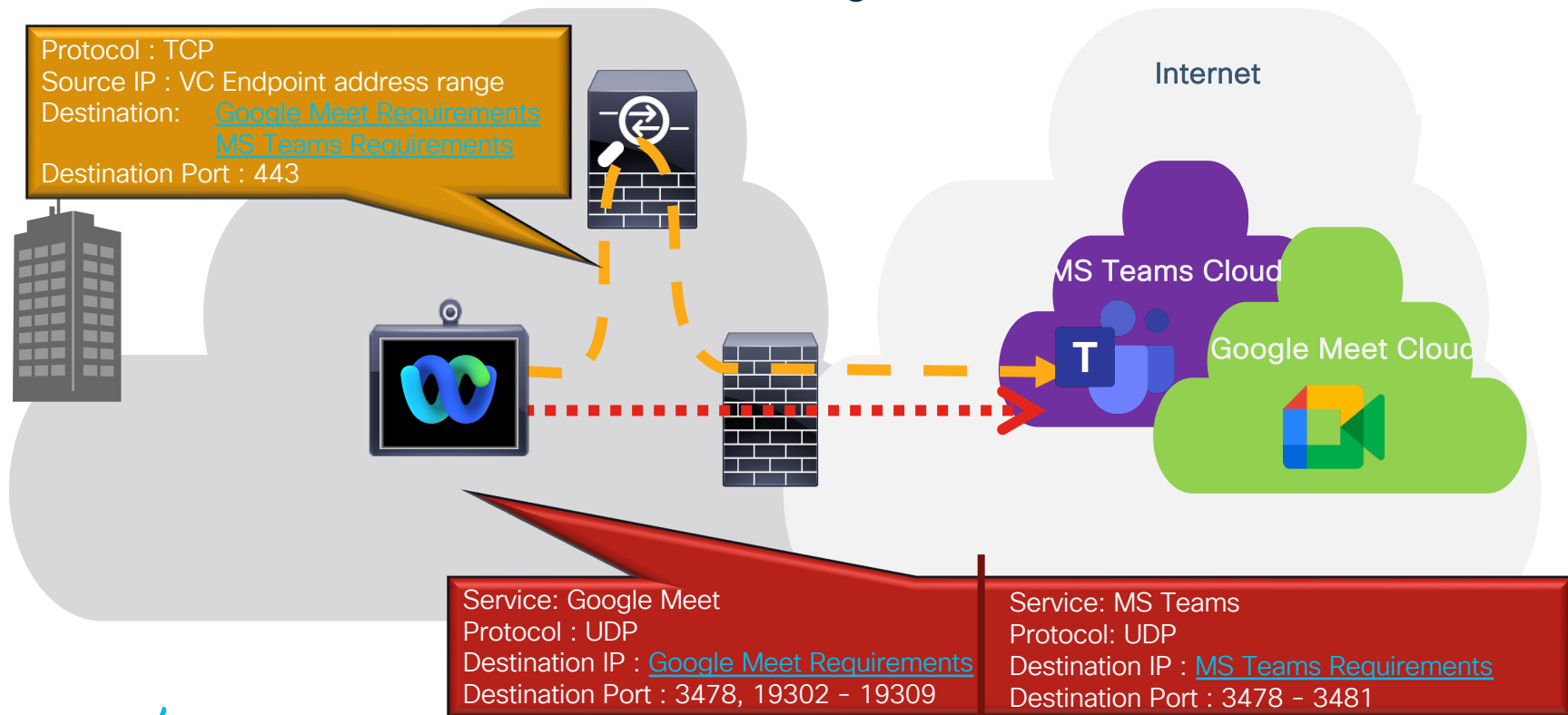
Destination IP : [MS Teams Requirements](#)

Destination Port : UDP 3478 - 3481

Protocols and Ports used by Webex

Cisco Video Devices to MS Teams/Google Meet

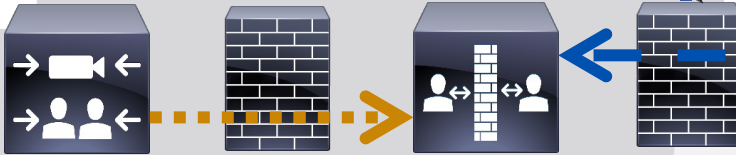
— Signaling/Other Control
- - - Real Time Traffic



Protocols and Ports used by Cisco Expressway

SIP: TCP 5061 (Call signaling)
HTTPS: TCP 8443 (Visual voicemail, directory)
XMPP: TCP 5222 (IM & 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
- 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

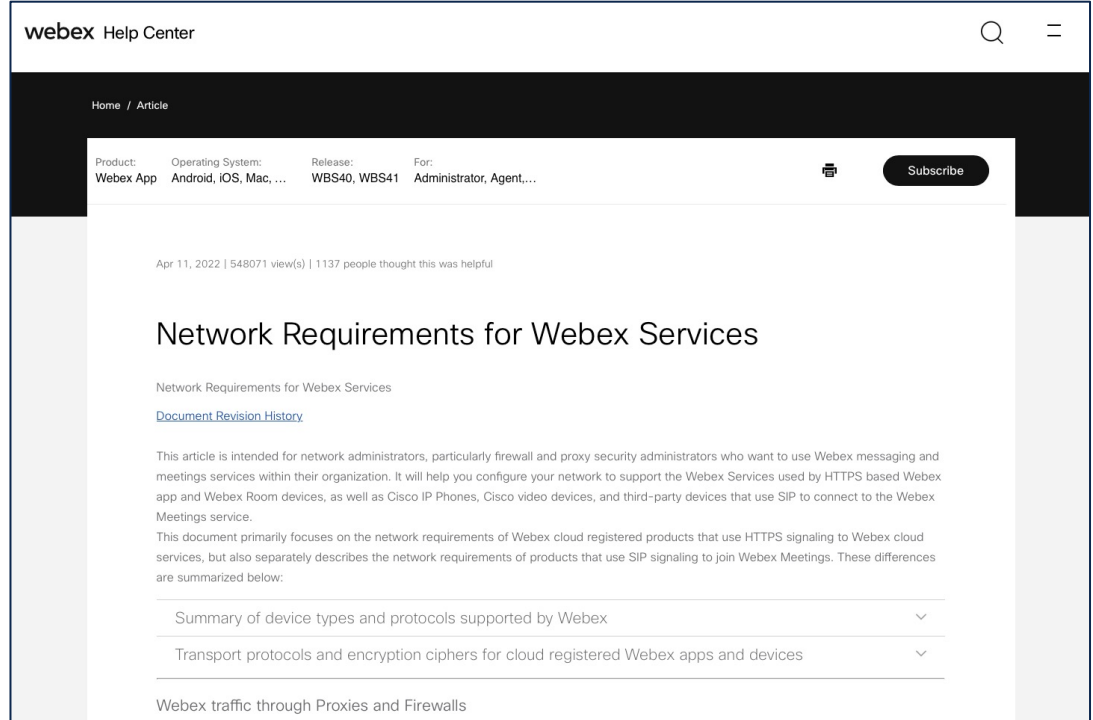
Links to visit regularly / to subscribe

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?

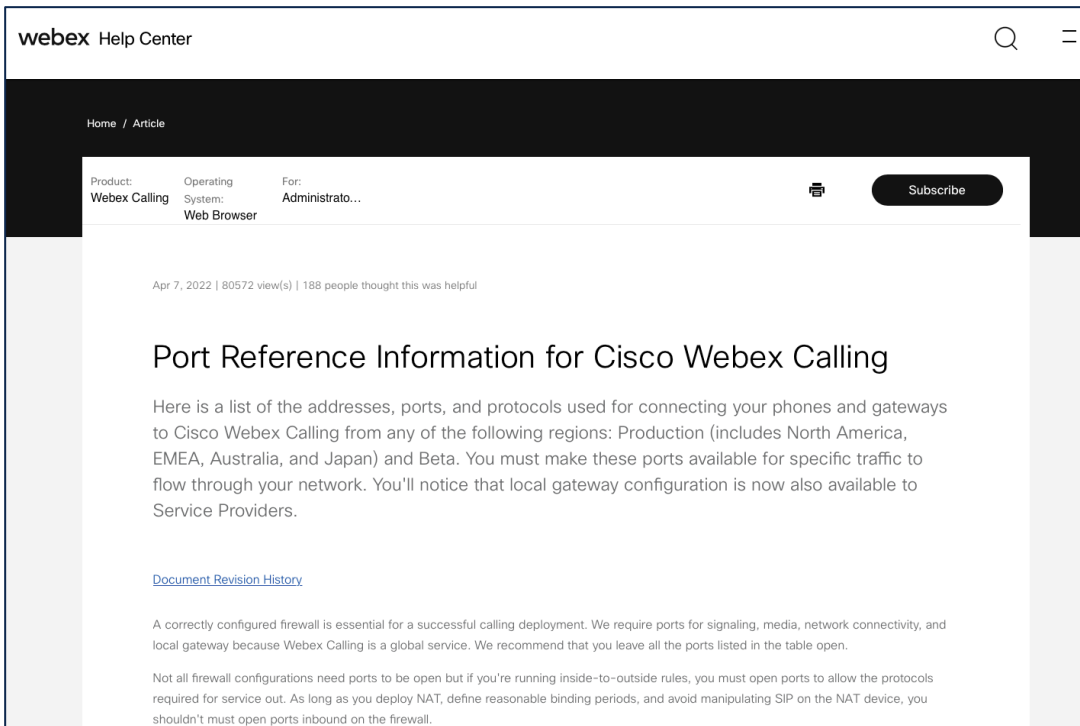
For answers to these questions and for more information about Webex services network requirements, refer to the *Network Requirements for Webex Services* article



<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





Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from red at the top to blue at the bottom. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, creating a sunburst or starburst effect that blends into the wavy bands.

cisco *Live!*

Let's go

#CiscoLiveAPJC