cisco

You make **possible**

Webex Teams Security in depth – Part One

Tony Mulchrone
Technical Marketing Engineer
CTG

BRKCOL-2795

Barcelona | January 27-31, 2020

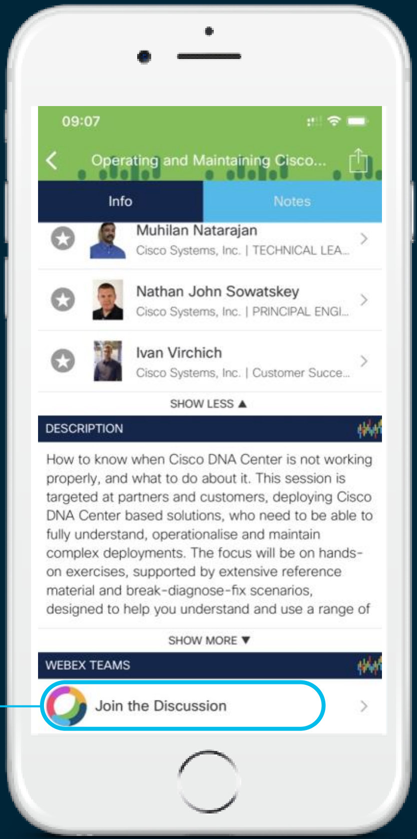
Cisco Webex Teams

Questions?

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

How

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



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

Agenda

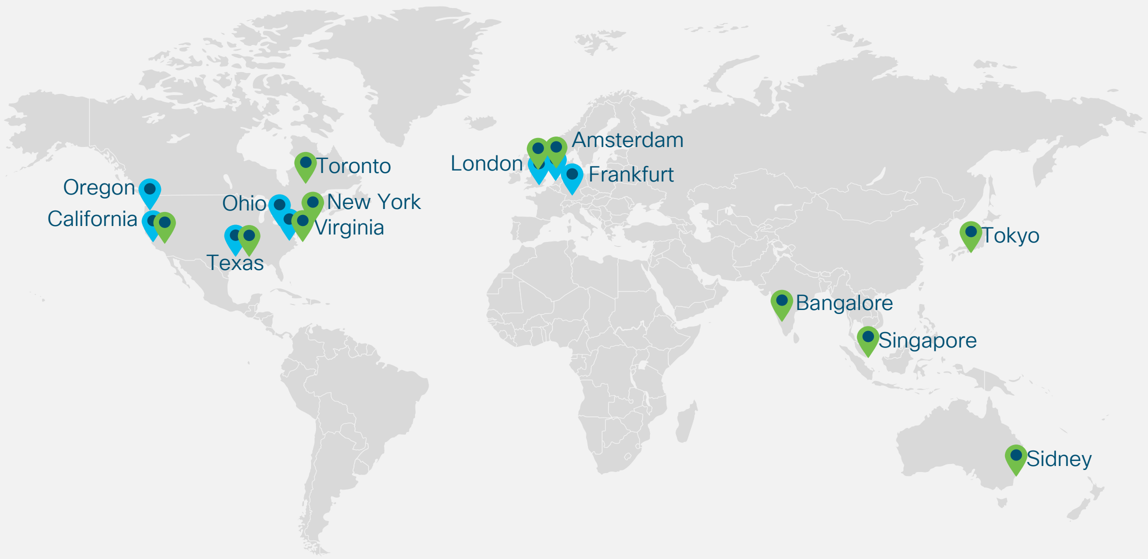
- Cisco's Secure Cloud Architecture for Webex Teams - Identity, End to End Encryption, Messaging and Meetings services, Voice, Video and Content Sharing
- Webex Teams Application Security - Securing messages, files and encryption keys stored on the OS platform, signed images, securing and authenticating Webex cloud connections. Proximity and paring to cloud and on-premises registered devices
- Webex Teams Device Security - Secure onboarding, signed images, securing and authenticating Webex cloud connections, security considerations for voice and face recognition
- Security at the Enterprise Network Edge for Webex Teams - Firewalls and Proxies - Enabling access to the Webex cloud from your network
- Additional Reading

Webex Cloud Architectural Overview

- Data Centres
- Micro-services
- Cloud Security

Webex Data Centre Locations

Regional Data Centre Locations



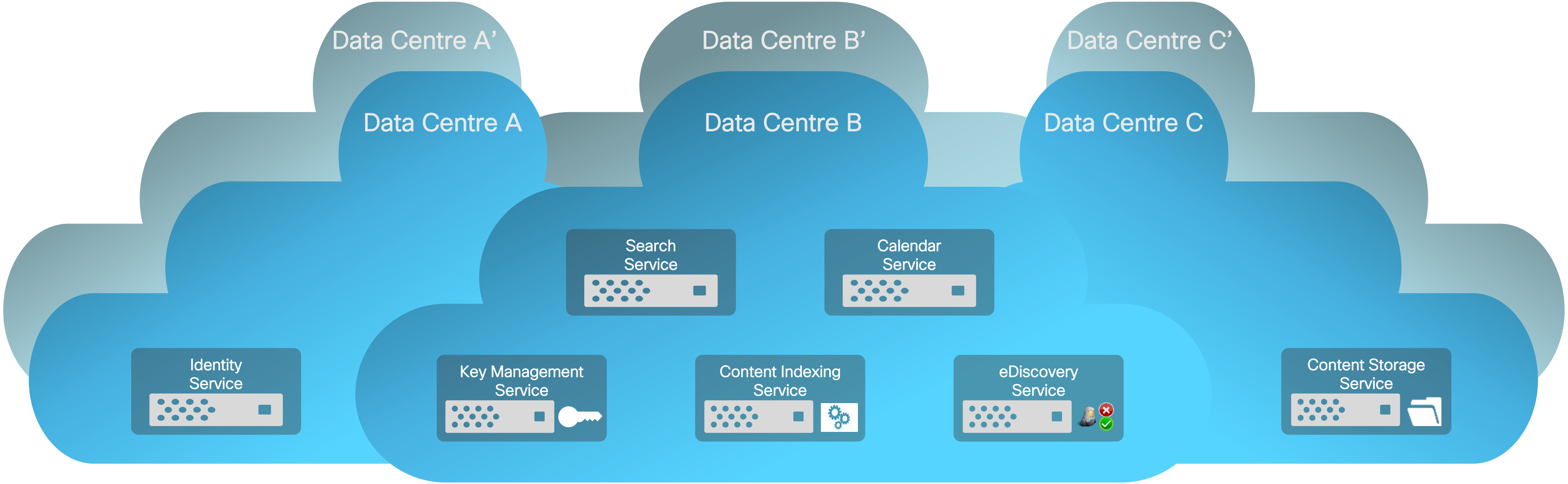
● Webex Teams services

● Webex Media services

- Webex Teams Services
- Microservices and content storage for Messages, Files, Whiteboards etc
- Two geographical areas (GEOs) :
- EMEA GEO :
  Data Centres in London, Frankfurt, and Amsterdam
- North America & Rest-of-World GEO :
  Multiple Data Centres in USA

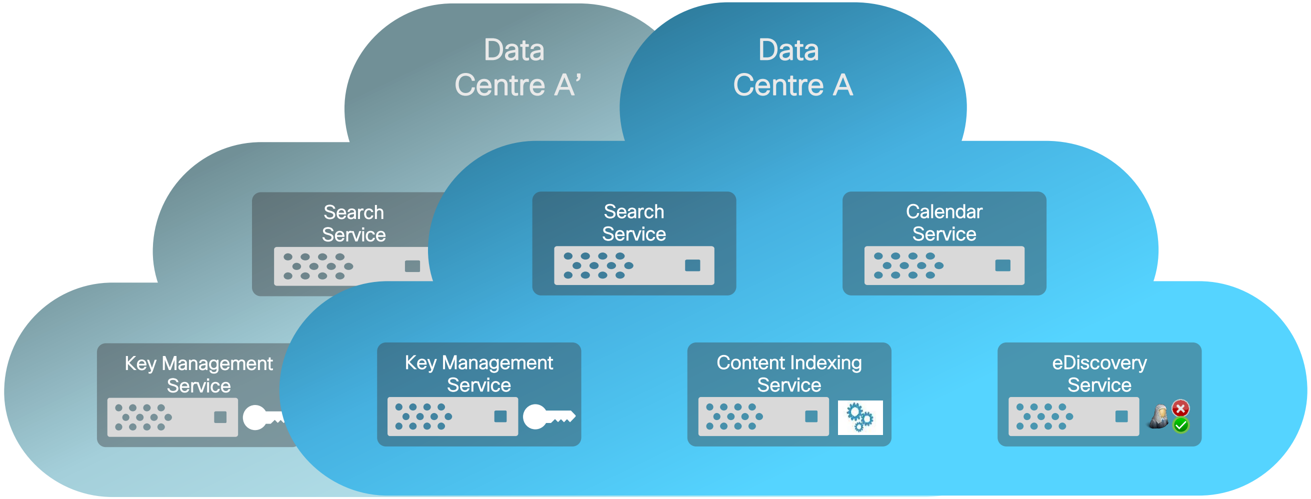
- Webex Media Services
- Media Nodes for Webex Meetings and Webex Teams :
- Voice, Video and Content Sharing services
- Multiple data centre locations worldwide

Webex Teams Services



Webex Teams services are distributed across multiple data centres
Key services are replicated between independent data centres
Core services are located in each GEO (EMEA, North America & ROW) e.g. Identity Service, Key Management Service (KMS), Content Storage Service
Other services reside in US data centres
All data is encrypted in transit and at rest

Webex Teams micro-service architecture

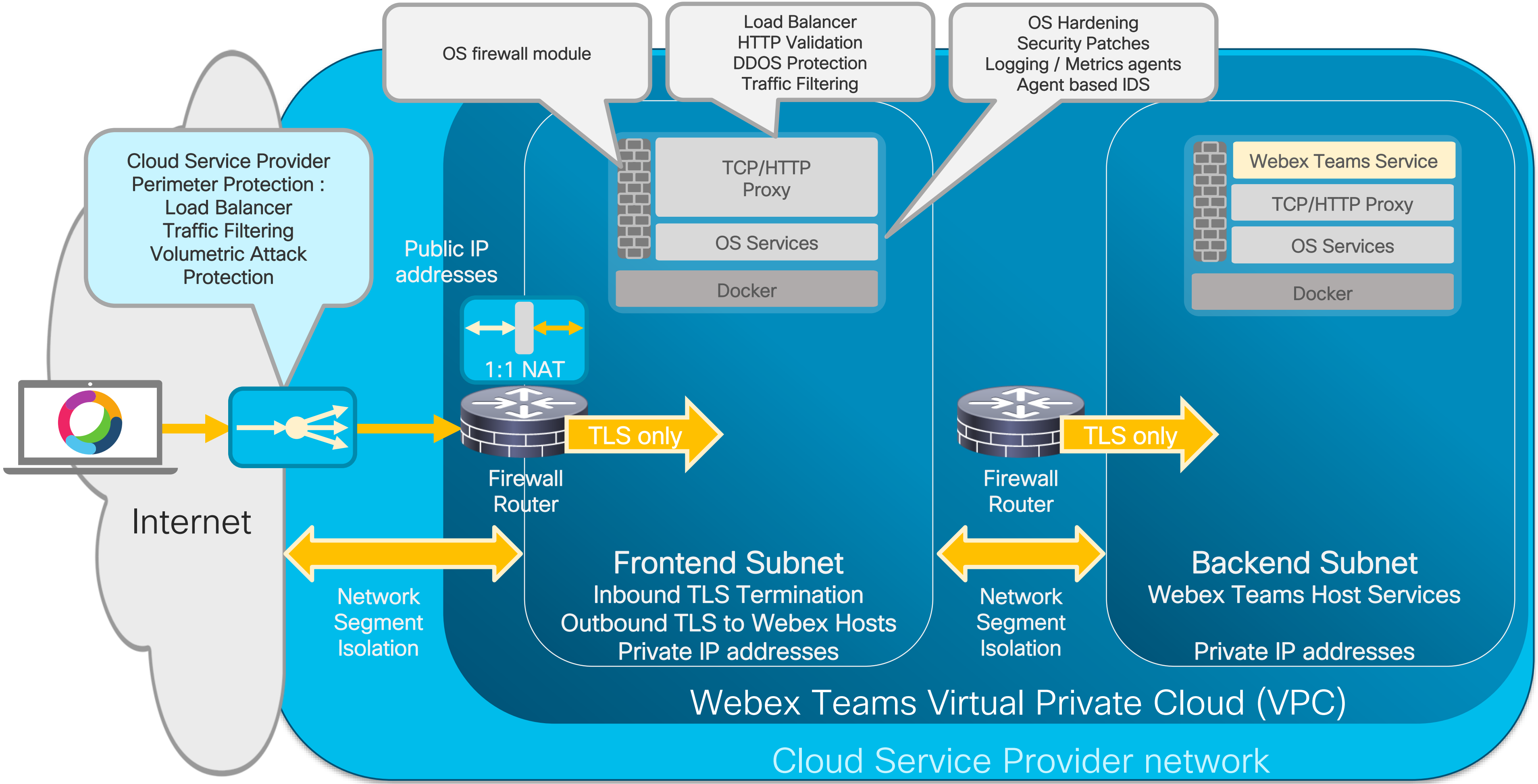


A micro-service is a small application that can be developed and deployed independently of other applications. Micro-services are loosely coupled to create a service architecture that allows for continuous development and deployment.

Approximately 200 micro-services make up the overall Webex Teams service

Examples of micro-services in addition those shown above : conversations, presence, avatars, whiteboards, client logs, client upgrades, integrations, meetings call control, proximity, face recognition, speech recognition, text to speech, data retention, document transcoding....

Webex Teams Signalling – Cloud Security and DMZ



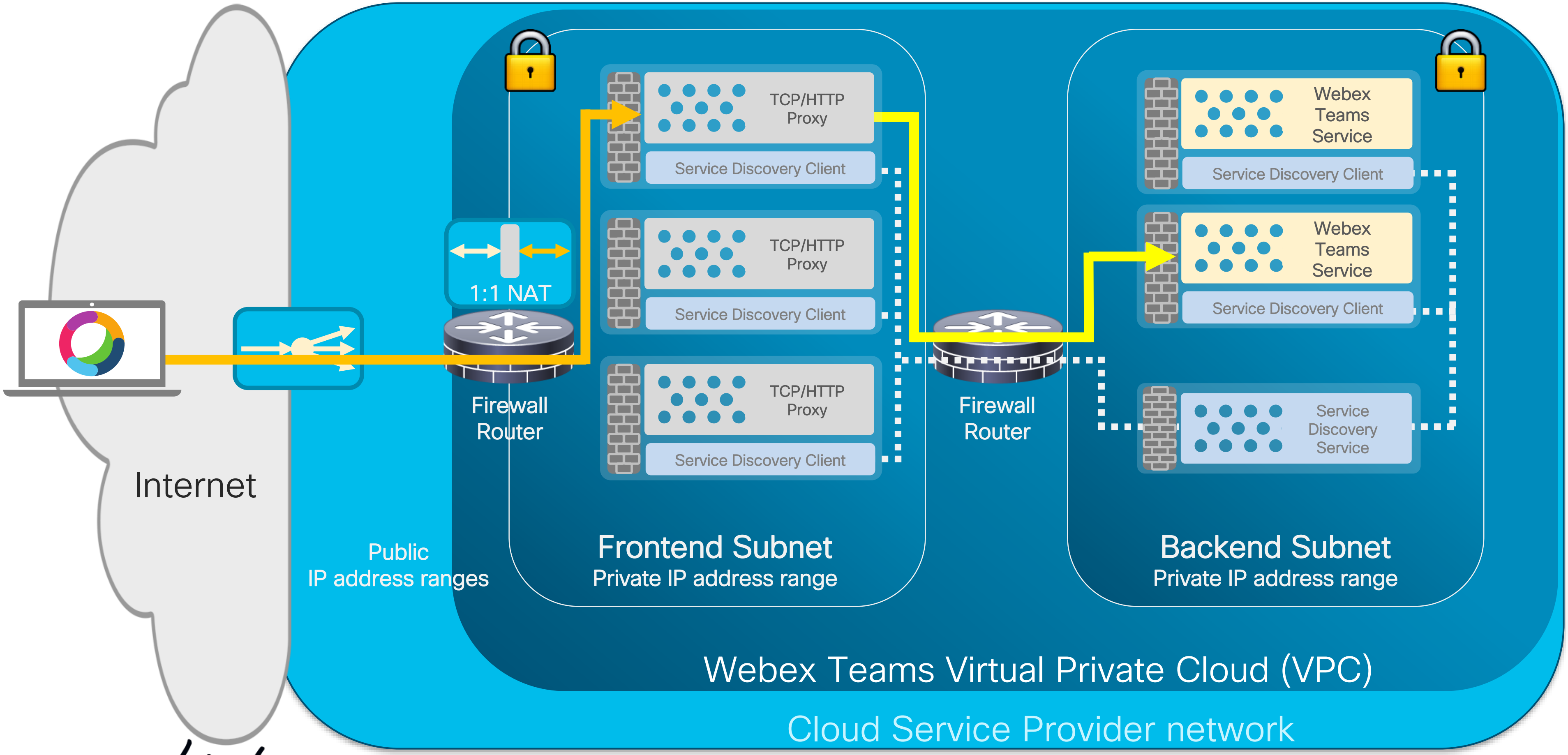
Frontend Subnet
Inbound TLS Termination
Outbound TLS to Webex Hosts
Private IP addresses

Backend Subnet
Webex Teams Host Services
Private IP addresses

Webex Teams Virtual Private Cloud (VPC)

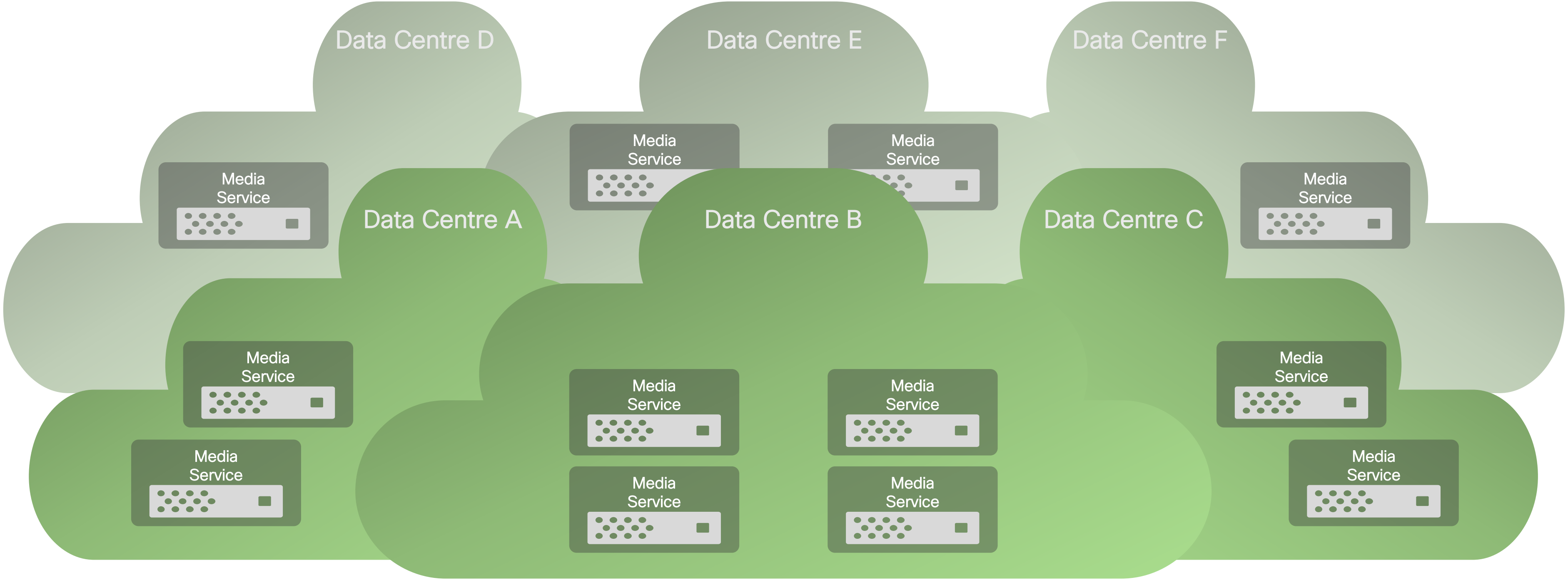
Cloud Service Provider network

Webex Teams – TLS Termination and Service Discovery



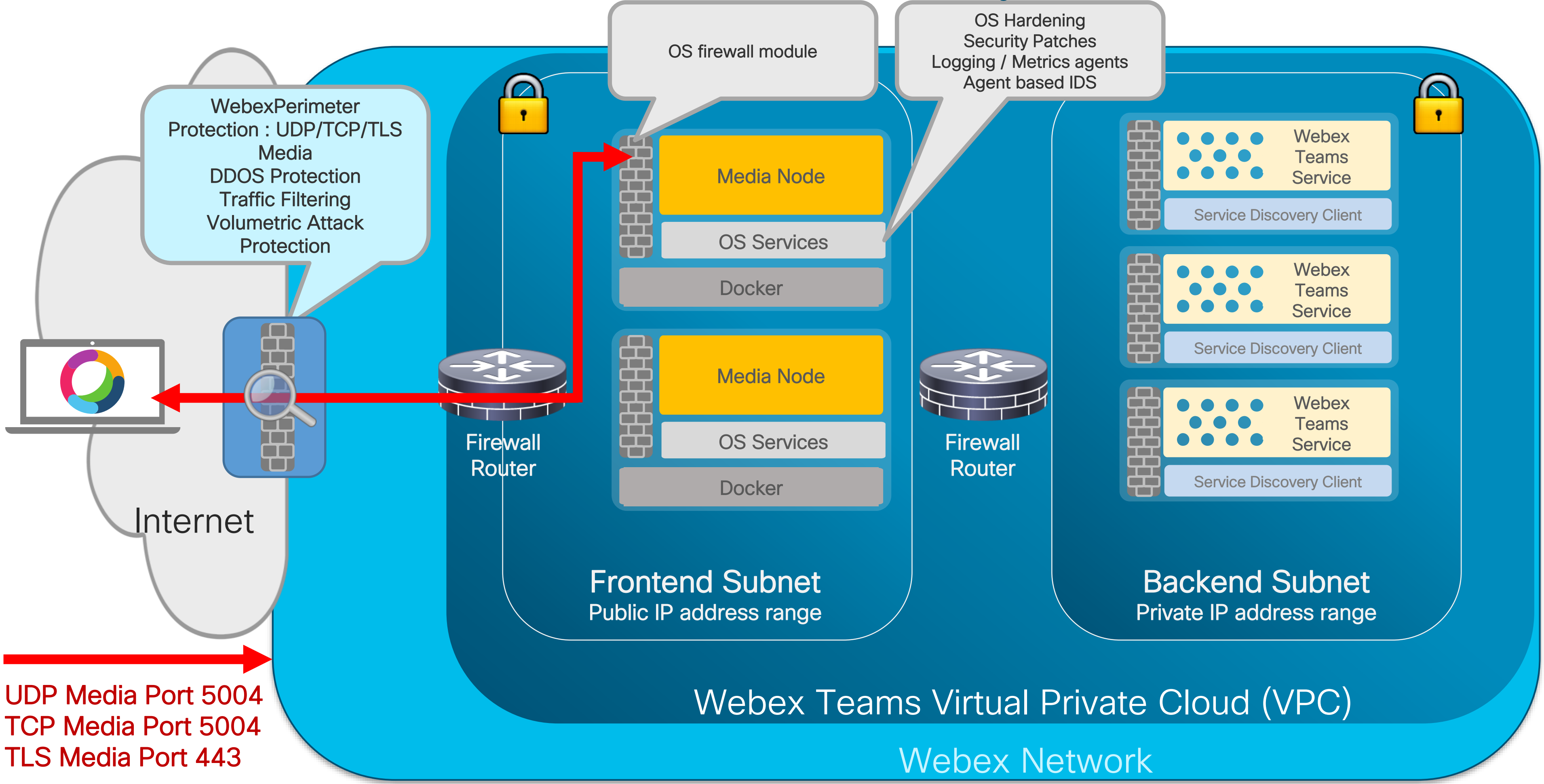
cisco Live!

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 voice, video and content sharing
All media is encrypted

Webex Media Services– Cloud Security and DMZ



WebexPerimeter Protection : UDP/TCP/TLS Media
DDOS Protection
Traffic Filtering
Volumetric Attack Protection

OS firewall module

OS Hardening
Security Patches
Logging / Metrics agents
Agent based IDS

Media Node
OS Services
Docker

Media Node
OS Services
Docker

Firewall Router

Firewall Router

Webex Teams Service
Service Discovery Client

Webex Teams Service
Service Discovery Client

Webex Teams Service
Service Discovery Client

Internet

Frontend Subnet
Public IP address range

Backend Subnet
Private IP address range

Webex Teams Virtual Private Cloud (VPC)

Webex Network

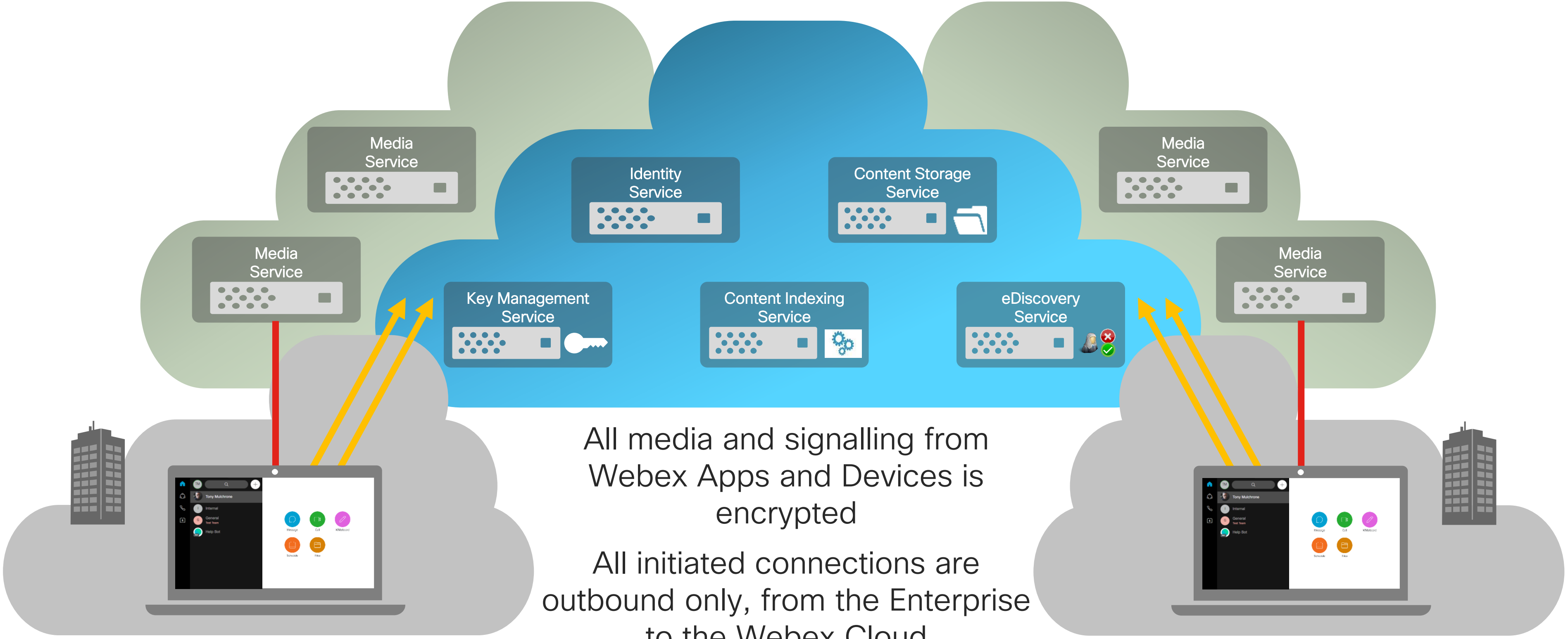
UDP Media Port 5004
TCP Media Port 5004
TLS Media Port 443

Webex Cloud Architectural Overview

Connecting to the cloud :

- Applications
- Devices
- Hybrid Services

Connecting to Webex Teams Services



All media and signalling from Webex Apps and Devices is encrypted

All initiated connections are outbound only, from the Enterprise to the Webex Cloud

SRTP Encrypted Media : AES_CM_128_HMAC_SHA1_80

TLS 1.2 Encrypted Signalling : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Connecting to the Webex cloud – Apps and Devices

Cisco Webex Apps :

- Windows, Mac
- iOS, Android
- Web

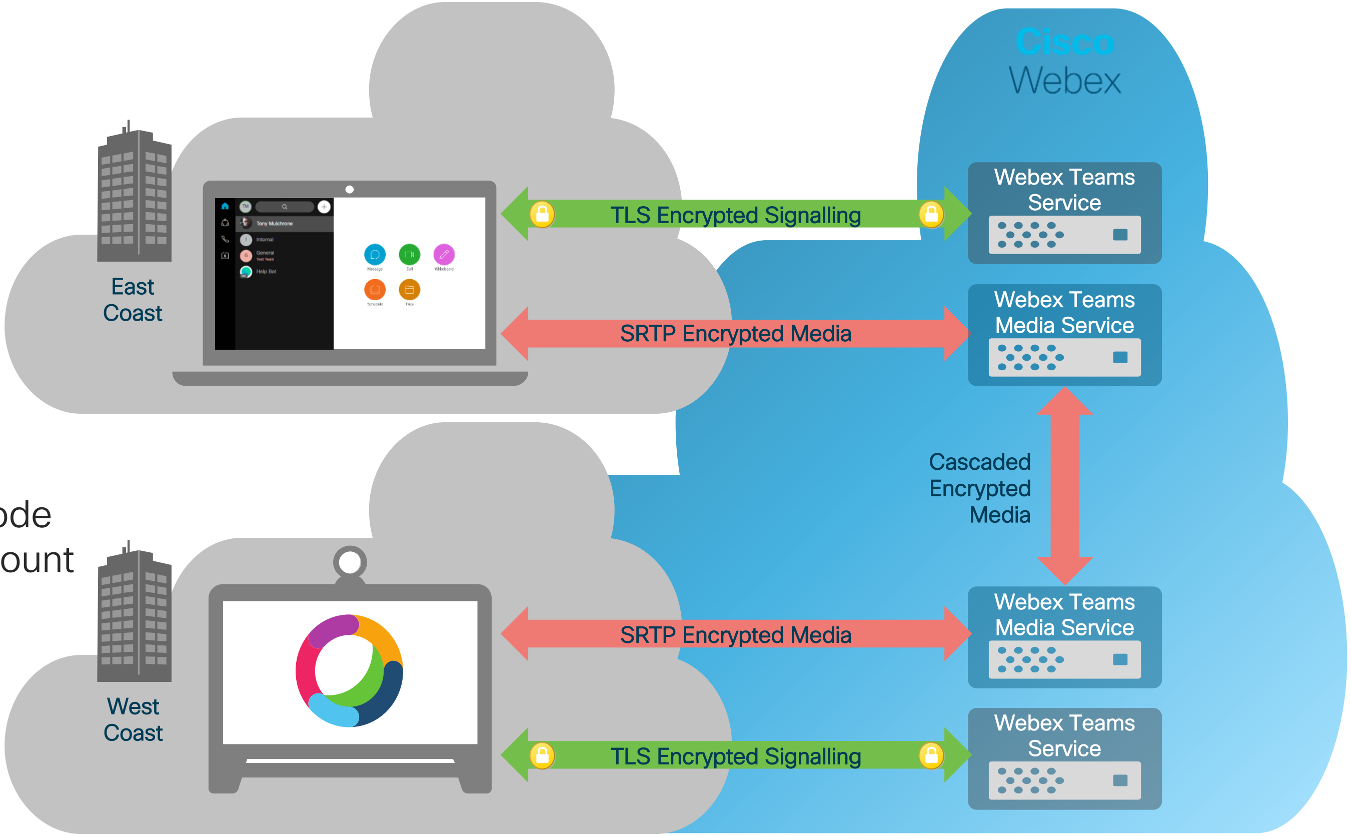
Authentication – User Sign In
Authorization – OAuth 2.0

Cisco Webex Devices :

- Webex Room Series
- Webex Desktop Series
- Webex Board

Onboarding – Activation Code
Authentication – Machine Account
Authorization – OAuth 2.0

All initiated connections are outbound only, from the Enterprise to Webex Cloud



Connecting to the Webex cloud – Hybrid Services Directory Connector

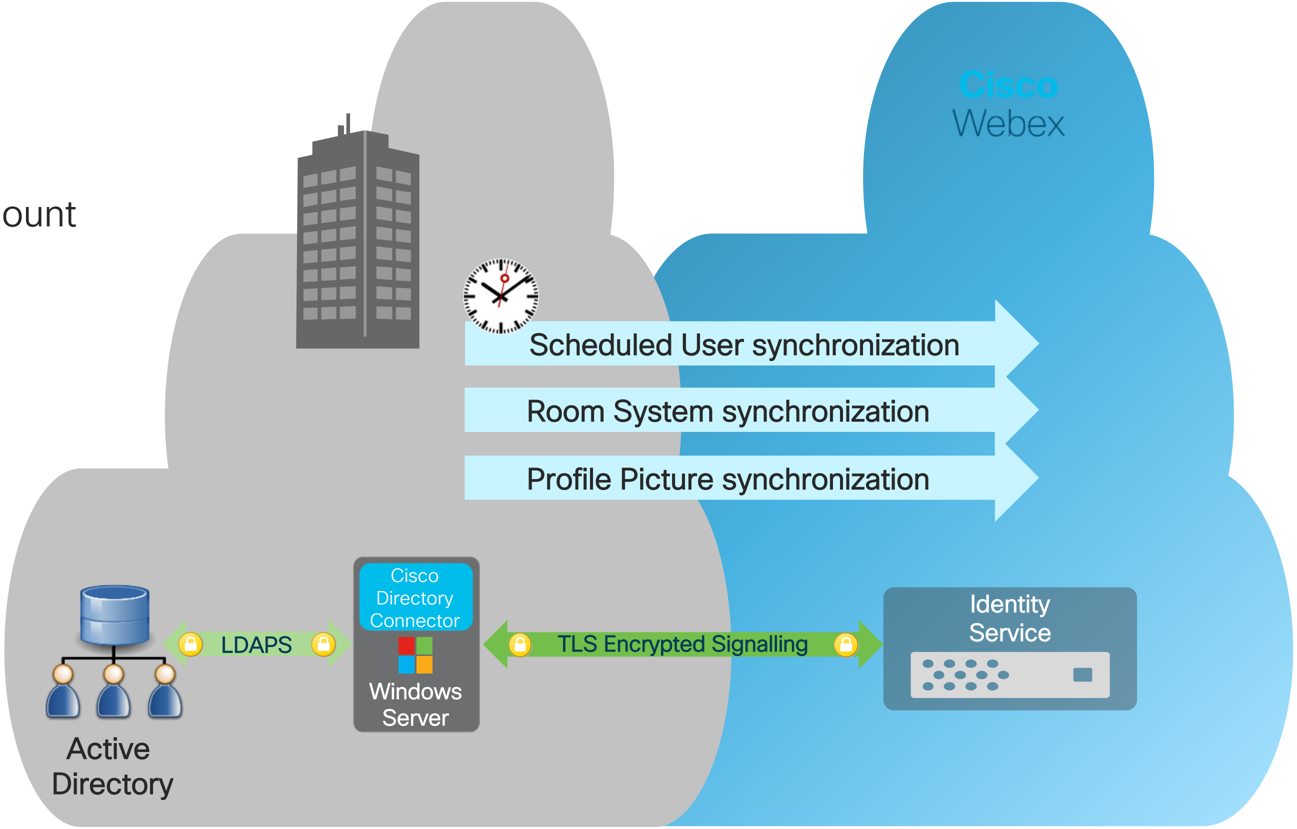
Cisco Directory Connector :
- Runs on Windows Server

TLS connection to Webex cloud
- Onboarding – CH admin
- Authentication – Machine Account
- Authorization – OAuth 2.0

LDAP/LDAPS connection to AD
- Authentication – AD domain account with directory read permissions

Synchronize from AD to Webex:
- Users
- User attribute mapping
- Room Devices
- Directory profile pictures

Multiple connectors for high availability



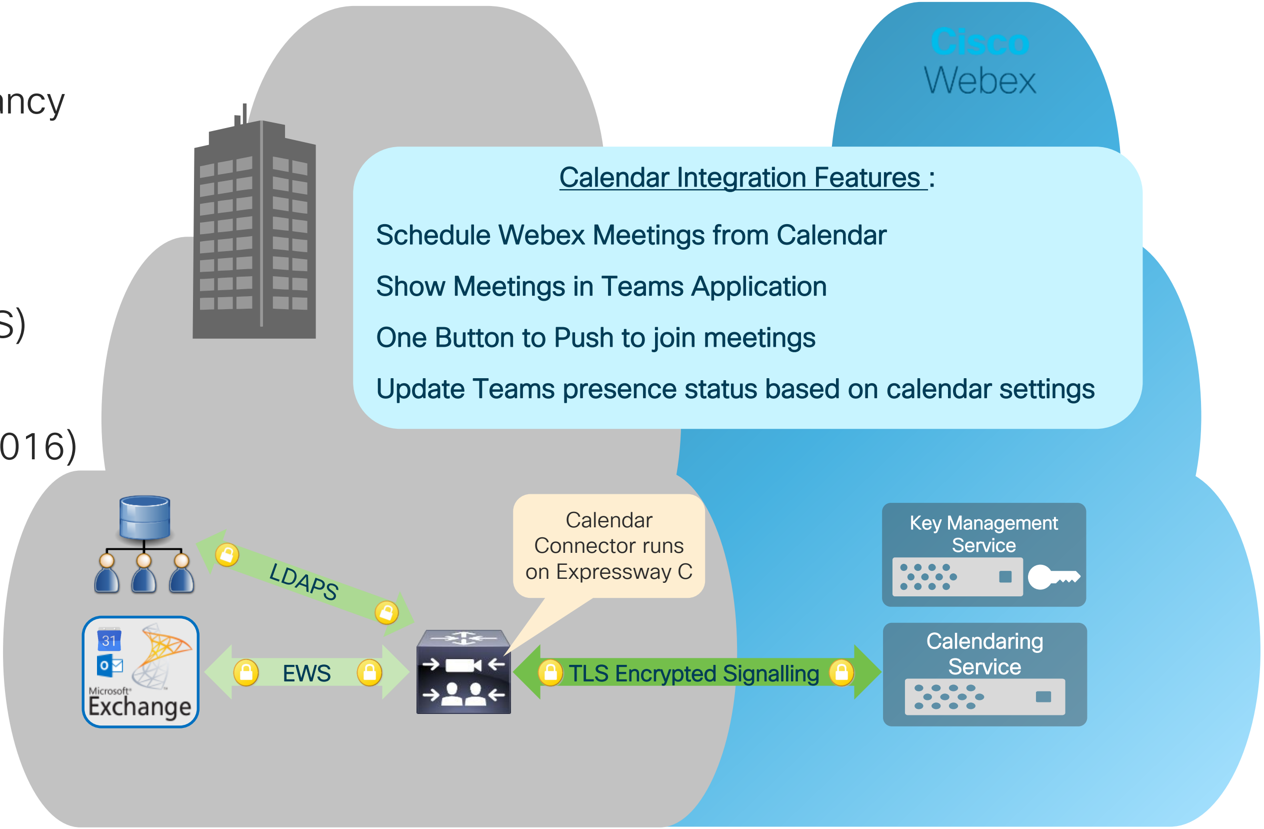
Cisco Webex
Scheduled User synchronization
Room System synchronization
Profile Picture synchronization
Cisco Directory Connector
Windows Server
LDAPS
TLS Encrypted Signalling
Identity Service
Active Directory

Connecting to the Webex cloud – Hybrid Services Calendar Connector

Calendar Connector
Runs on Expressway C
Two Expressway nodes for redundancy
TLS signalling to the Webex Cloud
Onboarding : CH Admin
Authentication : Machine account
Authorization : OAuth 2.0
Meeting details E2E encrypted (KMS)

On Premises Calendar Integration :
Microsoft Exchange (2010, 2013, 2016)
Uses Exchange Web Services API
AuthN : Service Account
AuthZ : Impersonation account
Uses LDAPS to Active Directory
TLS Transport

See notes for detailed documents on Data Handling, AuthN and AuthZ



Calendar Integration Features :

Schedule Webex Meetings from Calendar

Show Meetings in Teams Application

One Button to Push to join meetings

Update Teams presence status based on calendar settings

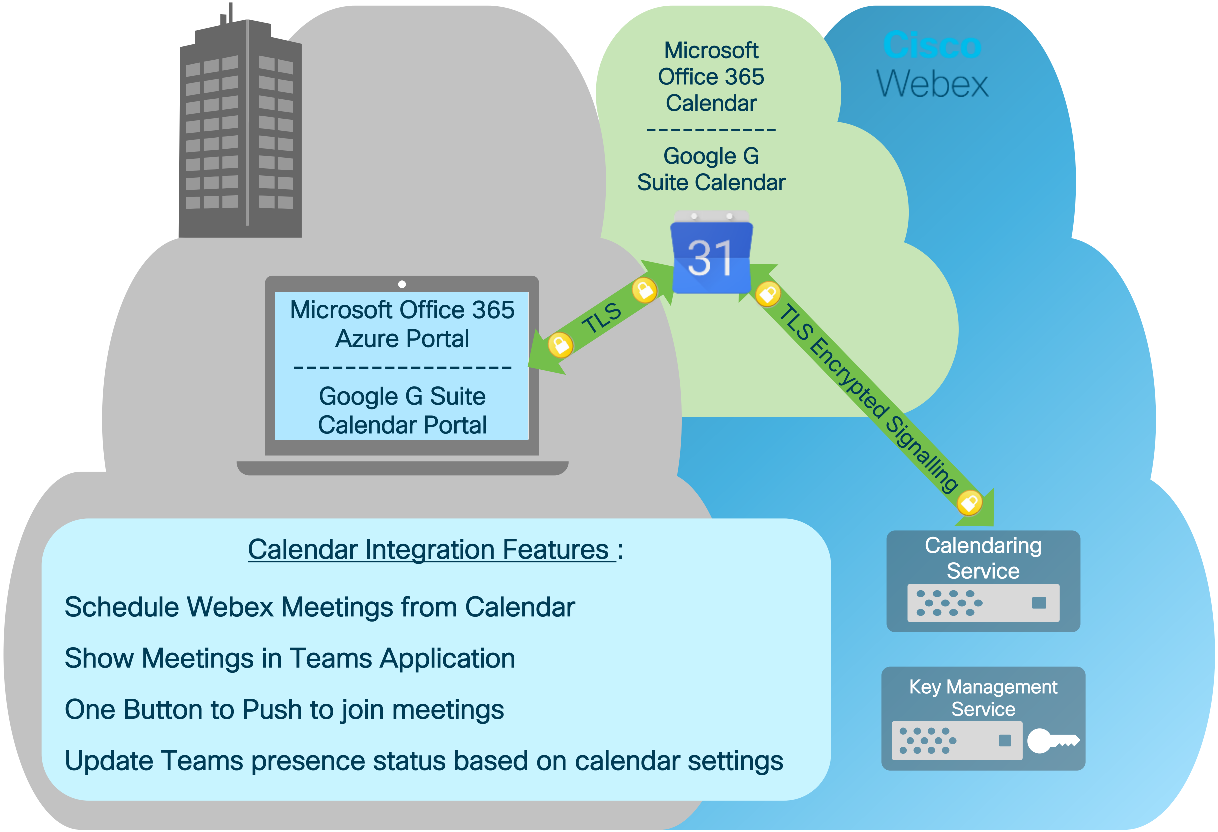
Connecting to the Webex cloud – Cloud Services
Cloud Calendar Integrations

Microsoft Office 365
Uses Microsoft Graph API
O356 Admin Teams Onboarding and Permissions Grant
OAuth 2.0 Authorization
TLS transport

Google G-Suite
Uses Google Calendar REST API
API Client service account Auth
OAuth 2.0 Authorization
TLS transport

Meeting details E2E encrypted (KMS)

See notes for detailed documents on Office 365/ Google Calendar Integration – Data Handling, Authentication and Authorization



Calendar Integration Features :

Schedule Webex Meetings from Calendar

Show Meetings in Teams Application

One Button to Push to join meetings

Update Teams presence status based on calendar settings

Connecting to the Webex cloud – Hybrid Services
Hybrid Data Security

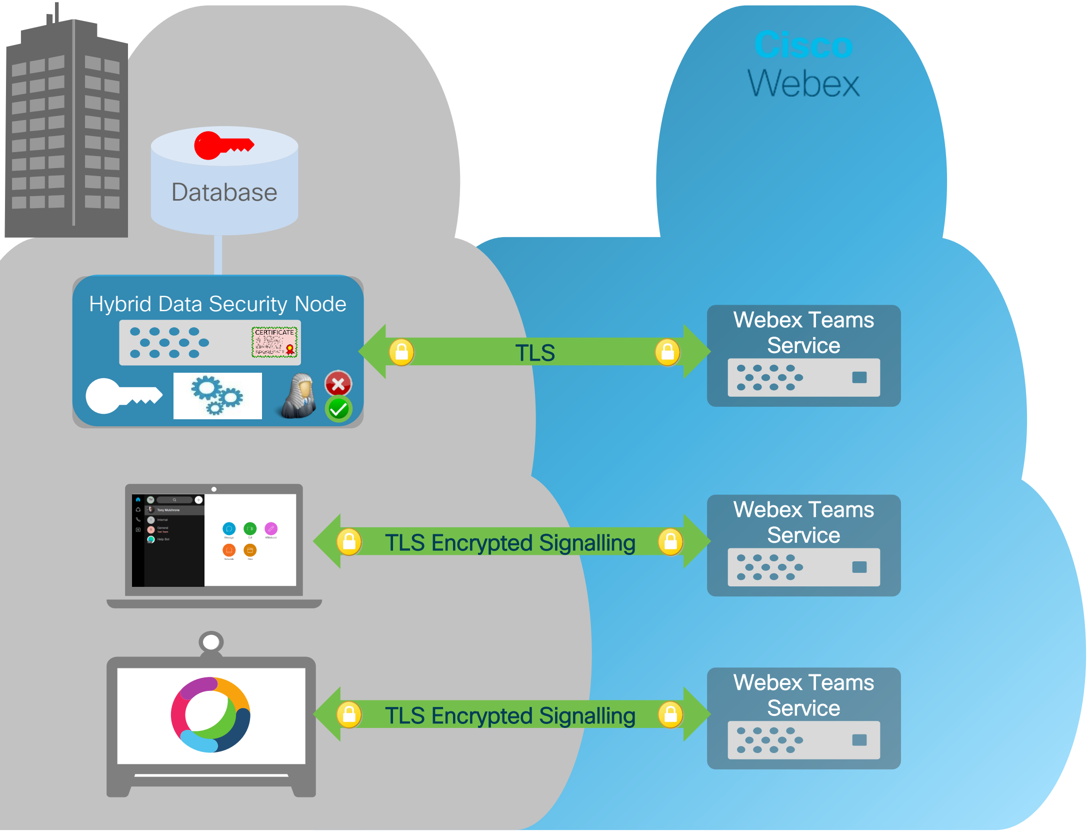
HDS nodes provide on premises :

E2E Encryption key generation
Encrypted search service
eDiscovery services

Encryption keys for :
- Spaces
- Meetings
- Whiteboards
Stored in on premises DB

HDS Cluster of up to 5 nodes

Webex Cloud TLS connections
- Onboarding – CH Admin
- Authentication – Machine Account
- Authorization – OAuth 2.0



cisco Live!

Connecting to the Webex cloud – Hybrid Services Video Mesh Node

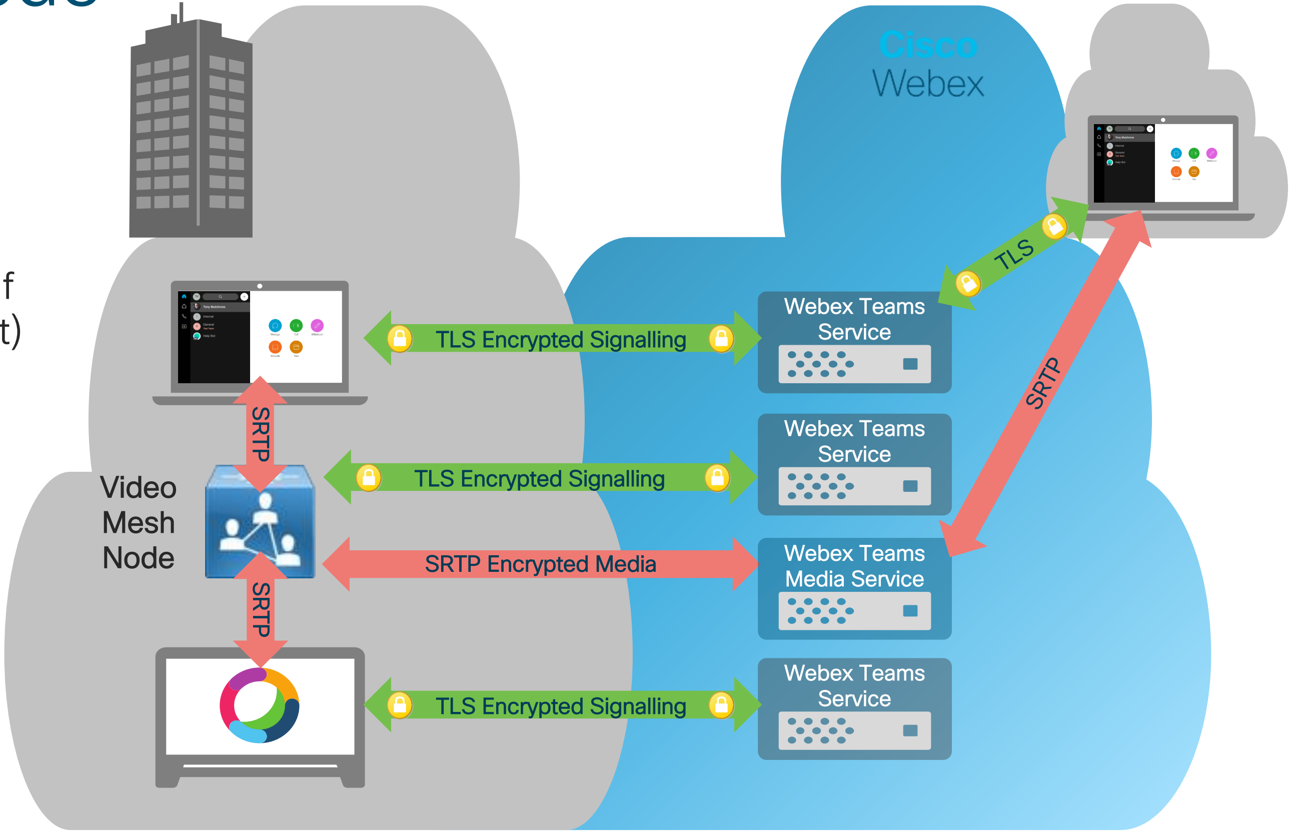
Video Mesh Node (VMN) provides on premises media resources for Apps and Devices

VMN establishes a cascade media connection to the cloud if needed (e.g. external participant)

VMNs can be clustered for scalability and redundancy

Video Mesh Node initiated TLS and SRTP connections are outbound only

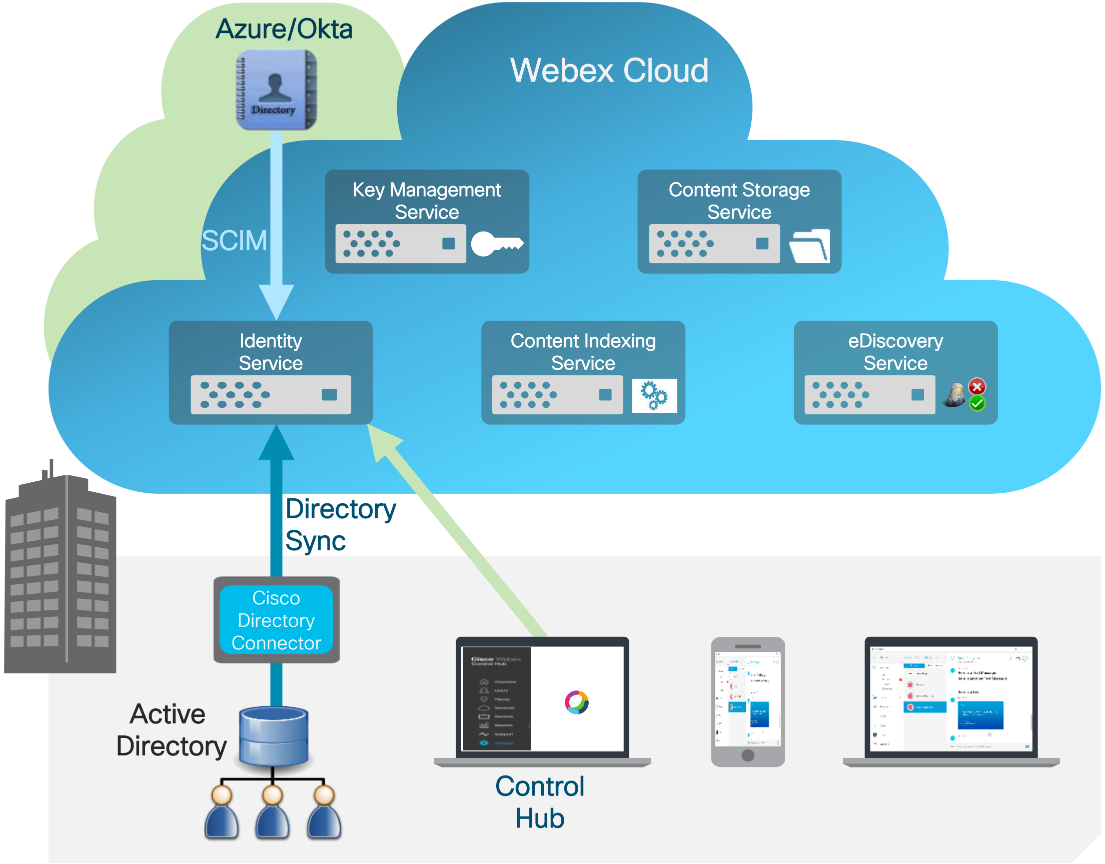
Onboarding – CH Admin
AuthN – Machine Account
AuthZ – OAuth 2.0



Onboarding and Authenticating Users

Connecting to the cloud : High Level overview for Apps & devices

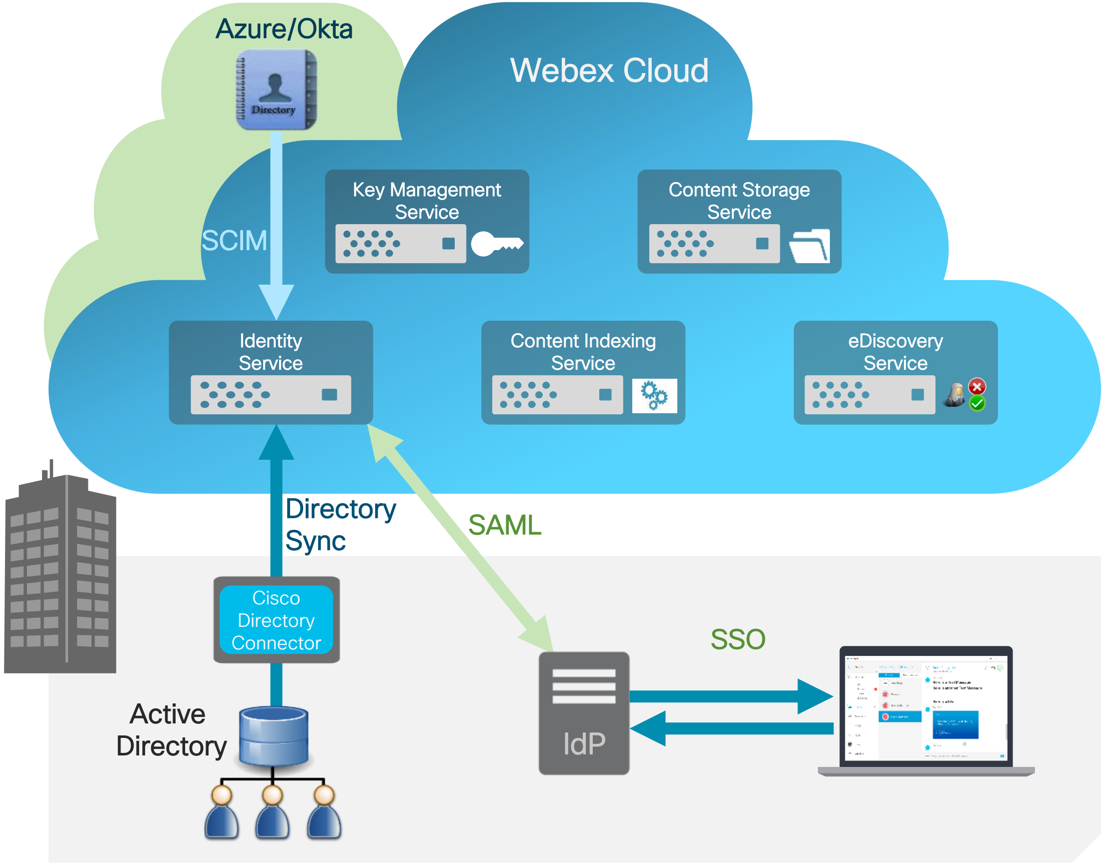
Webex Teams – User, Identity & Access Management



User accounts can be created in the Webex identity service and managed in several ways:

- Webex Directory Connector
  - Active Directory Sync Tool
- System for Cross-Domain Identity Management (SCIM) API
  - Sync from Cloud IdP
  - e.g. Azure AD, Okta User DB
- Webex Control Hub Admin
- Webex Teams People API
- CSV File upload

Webex Teams – SAML SSO Authentication



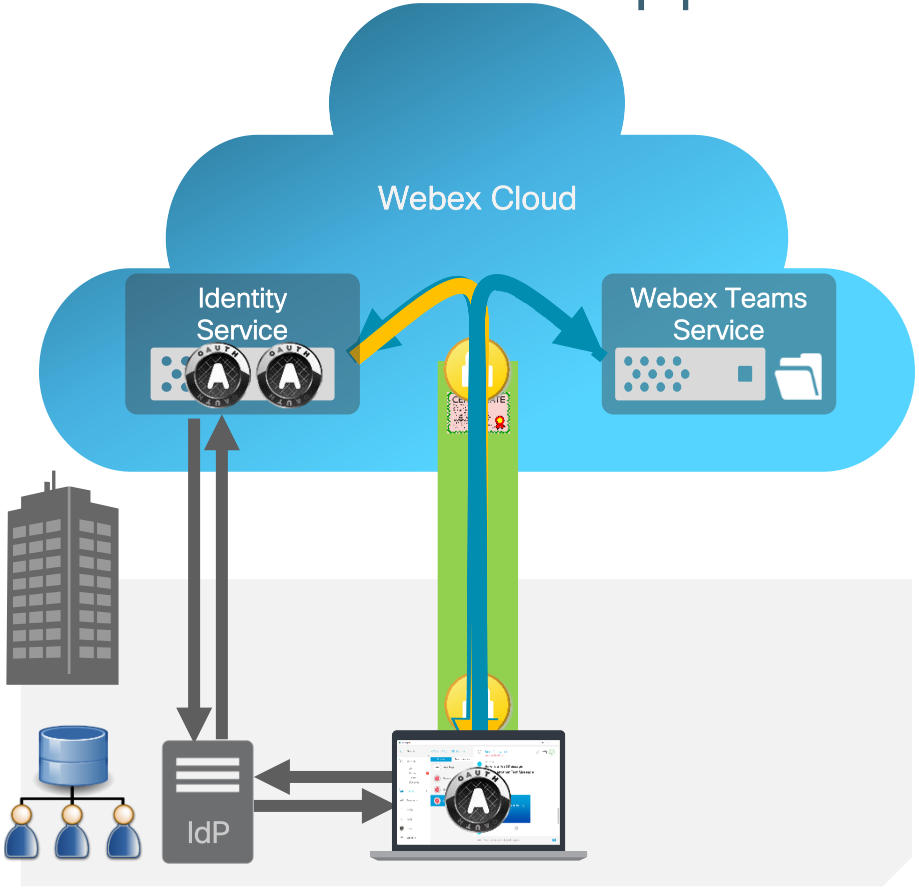
Single Sign On (SSO) for User Authentication :

Administrators can configure Webex Teams to work with their existing SSO solution

Webex Teams supports Identity Providers using Security Assertion Markup Language (SAML) 2.0 for Authentication and OAuth 2.0 Authorization

For list of supported IdPs see https://help.webex.com/en-us/lfu88u/Single-Sign-On-Integration-in-Cisco-Webex-Control-Hub

Webex Teams App – cloud connection – summary

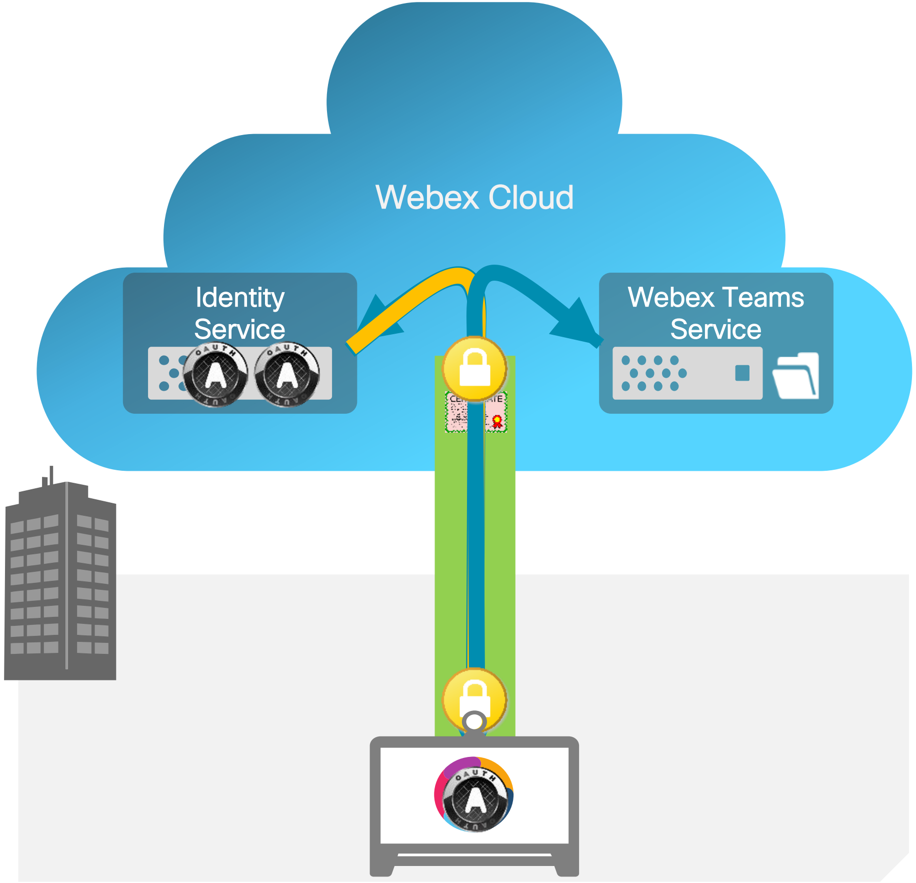


1) Customer downloads and installs the Webex Teams App
2) Webex Teams App establishes a secure TLS connection with the Webex Cloud
3) Webex Teams Identity Service prompts User for an e-mail ID
4) User Authenticated by Webex Teams Identity Service, or Enterprise IdP (SSO)
5) OAuth Access and Refresh Tokens created and sent to Webex Teams App

- The Access Token contain details of the Webex Teams resources the User is authorised to access

5) Webex Teams App presents its Access Token to register with Webex Teams Services over a secure channel

Webex Teams Device – cloud connection – summary



1) User enters 16 digit activation code received via e-mail from the Webex Teams provisioning service

2) Device authenticated by Identity Service (Trust anchors sent to device and TLS connection established)

3) OAuth Access and Refresh Tokens created and sent to Webex Teams Device

- The Access Token contain details of the Webex Teams resources the User is authorised to access

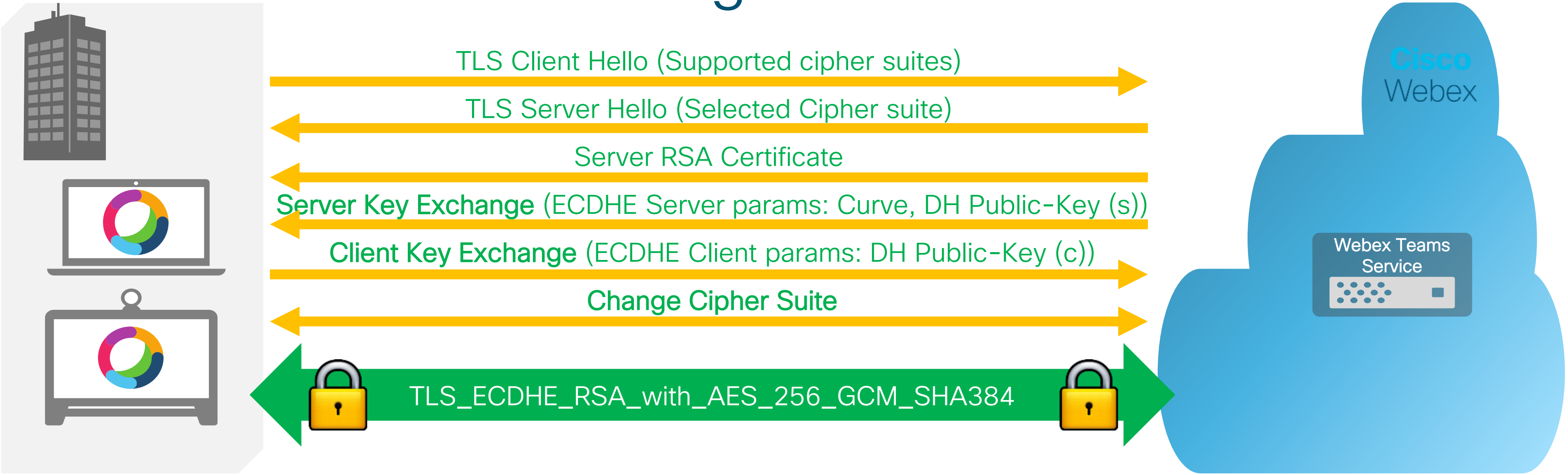
5) Webex Teams Device presents its Access Token to register with Webex Teams Services over a secure channel

cisco Live! 1234567890123456

Secure Signalling

TLS Signaling Connections : Authenticating Webex Services

Webex Teams TLS negotiation

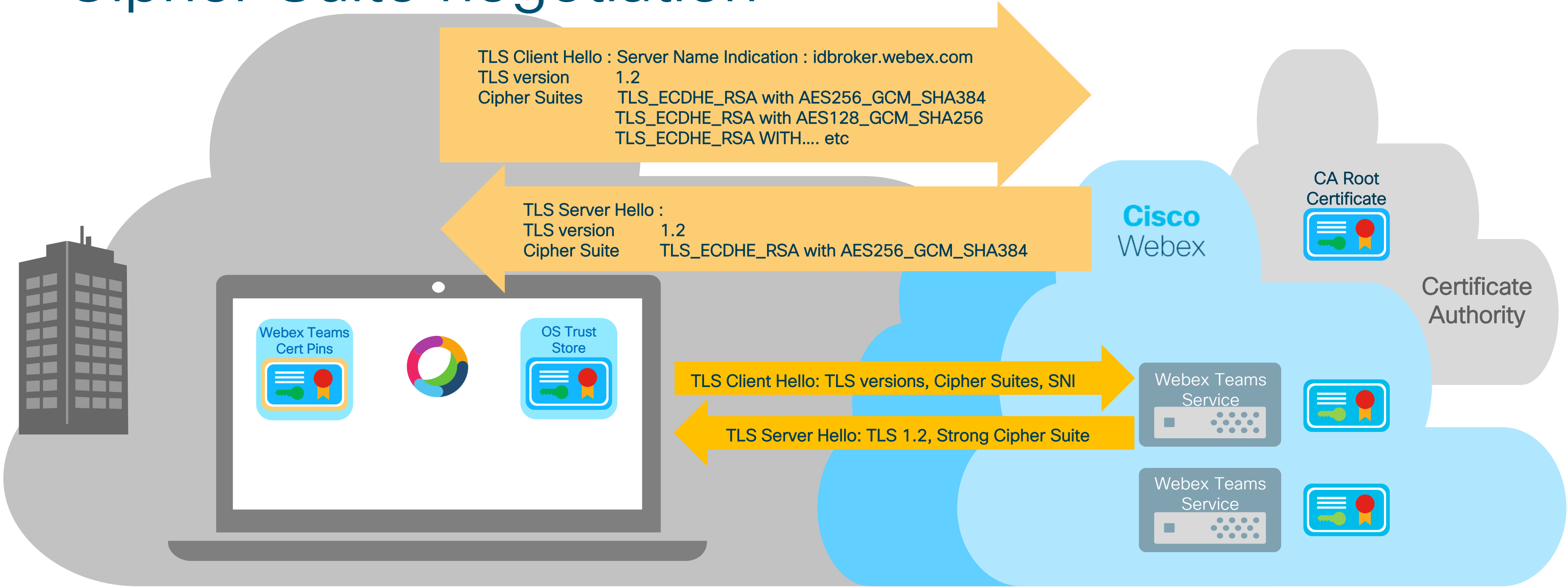

TLS Client Hello (Supported cipher suites)
TLS Server Hello (Selected Cipher suite)
Server RSA Certificate
Server Key Exchange (ECDHE Server params: Curve, DH Public-Key (s))
Client Key Exchange (ECDHE Client params: DH Public-Key (c))
Change Cipher Suite
TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
Cisco
Webex
Webex Teams
Service

Webex Teams : TLS version 1.2 only and supports only the following cipher suites in preference order :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

ECDHE : Key Negotiation with Forward Secrecy
RSA : Certificates (2048 bit key size)
AES_256 : NSA Top Secret Encryption Strength

Webex Teams: TLS Client and Server Hello Cipher Suite negotiation



TLS Client Hello : Server Name Indication : idbroker.webex.com
TLS version 1.2
Cipher Suites TLS_ECDHE_RSA with AES256_GCM_SHA384
TLS_ECDHE_RSA with AES128_GCM_SHA256
TLS_ECDHE_RSA WITH.... etc

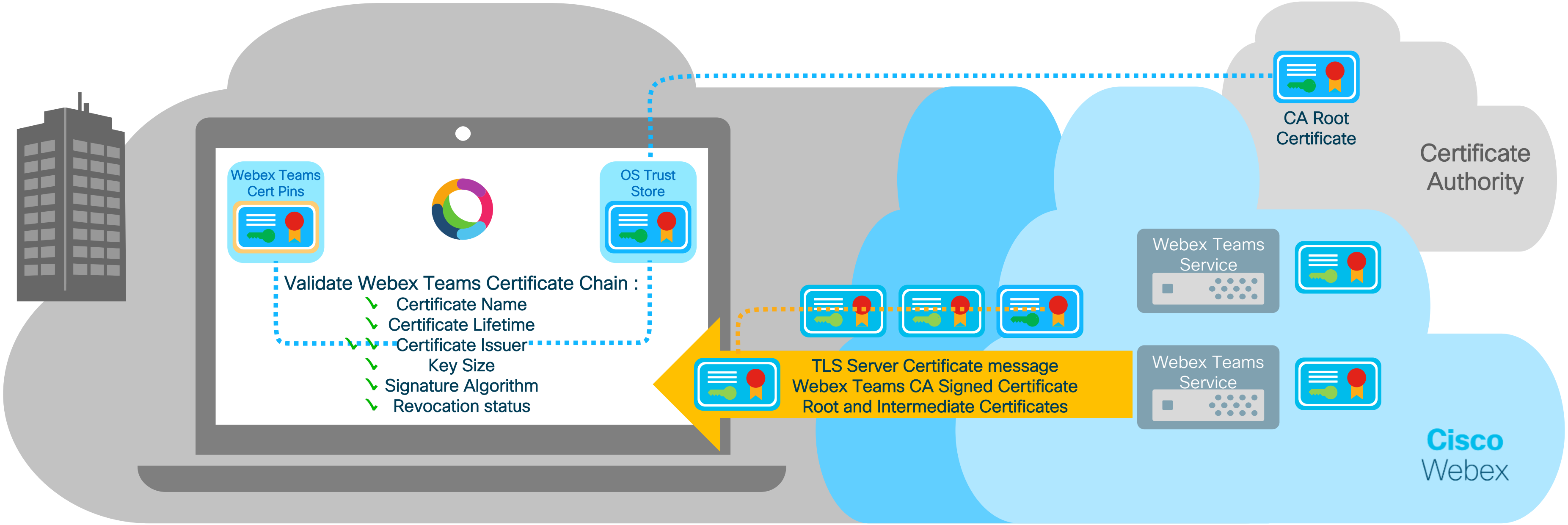
TLS Server Hello :
TLS version 1.2
Cipher Suite TLS_ECDHE_RSA with AES256_GCM_SHA384

TLS Client Hello: TLS versions, Cipher Suites, SNI

TLS Server Hello: TLS 1.2, Strong Cipher Suite

Webex Teams Certificates Pins for certificate and certificate authority validation
Webex Teams Apps : Embedded in software
Webex Teams Devices : Downloaded to device trust store during onboarding

Webex Teams : Service Certificate validation

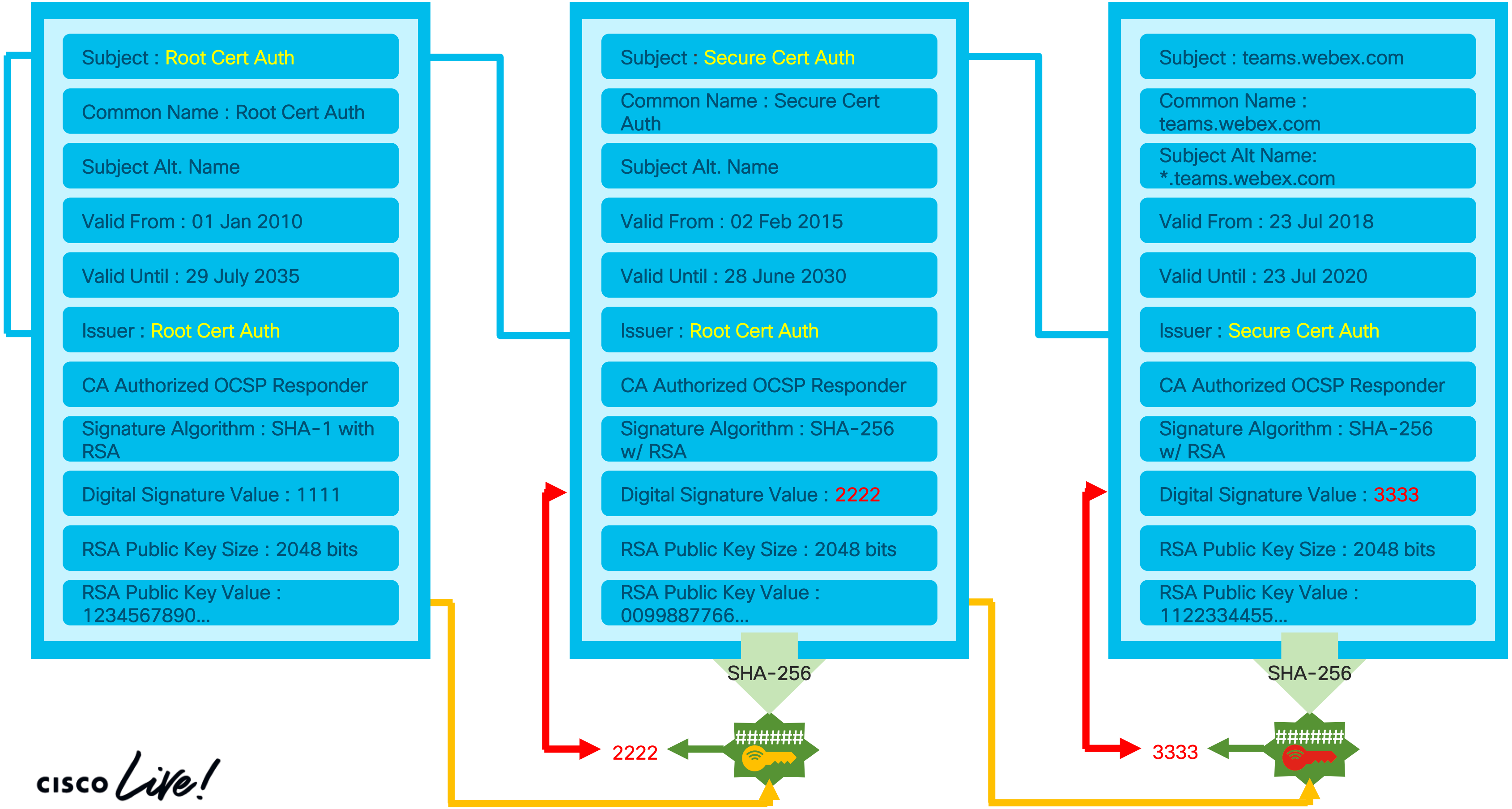


CA signed server cert, CA Root cert, and any intermediate certs are sent to the Webex Teams App/Device

The Webex Teams App/Device verifies the following in each certificate :

Digital Signature/ Certificate Issuer/ Certificate Validity Period/ Certificate Revocation status/ Key Size/ Key Usage Certificate Extensions/ Server Hostname/ Certificate Pins

Webex Teams : Service Certificate validation



CA Root Certificate	Intermediate Certificate	Server Certificate
Subject : Root Cert Auth	Subject : Secure Cert Auth	Subject : teams.webex.com
Common Name : Root Cert Auth	Common Name : Secure Cert Auth	Common Name : teams.webex.com
Subject Alt. Name	Subject Alt. Name	Subject Alt Name: *.teams.webex.com
Valid From : 01 Jan 2010	Valid From : 02 Feb 2015	Valid From : 23 Jul 2018
Valid Until : 29 July 2035	Valid Until : 28 June 2030	Valid Until : 23 Jul 2020
Issuer : Root Cert Auth	Issuer : Root Cert Auth	Issuer : Secure Cert Auth
CA Authorized OCSP Responder	CA Authorized OCSP Responder	CA Authorized OCSP Responder
Signature Algorithm : SHA-1 with RSA	Signature Algorithm : SHA-256 w/ RSA	Signature Algorithm : SHA-256 w/ RSA
Digital Signature Value : 1111	Digital Signature Value : 2222	Digital Signature Value : 3333
RSA Public Key Size : 2048 bits	RSA Public Key Size : 2048 bits	RSA Public Key Size : 2048 bits
RSA Public Key Value : 1234567890...	RSA Public Key Value : 0099887766...	RSA Public Key Value : 1122334455...

Onboarding and Authenticating Users and Devices : Detailed slides

Onboarding Devices
Authenticating Users
Authenticating Devices
App/Device Authorization
OAuth Access & Refresh Tokens

Webex Teams - Device Onboarding

Webex Device application software and embedded OS installed as a firmware binary image before leaving the factory

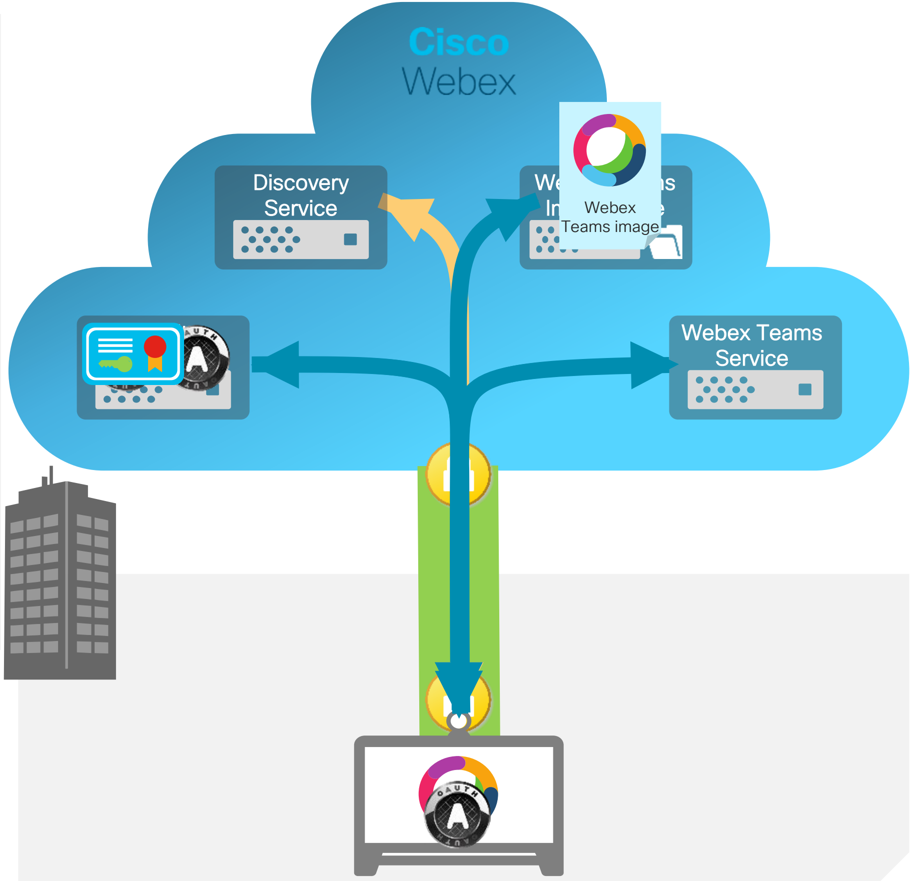
Control Hub Admin generates device activation code for the device

User prompted for activation code during device installation. Activation code sent to Webex discovery service, which determines the device's organization and redirects to the Identity Service

Identity Service sends OAuth tokens and Certificate Trust list (can include Enterprise CA Certs for TLS inspection) to device

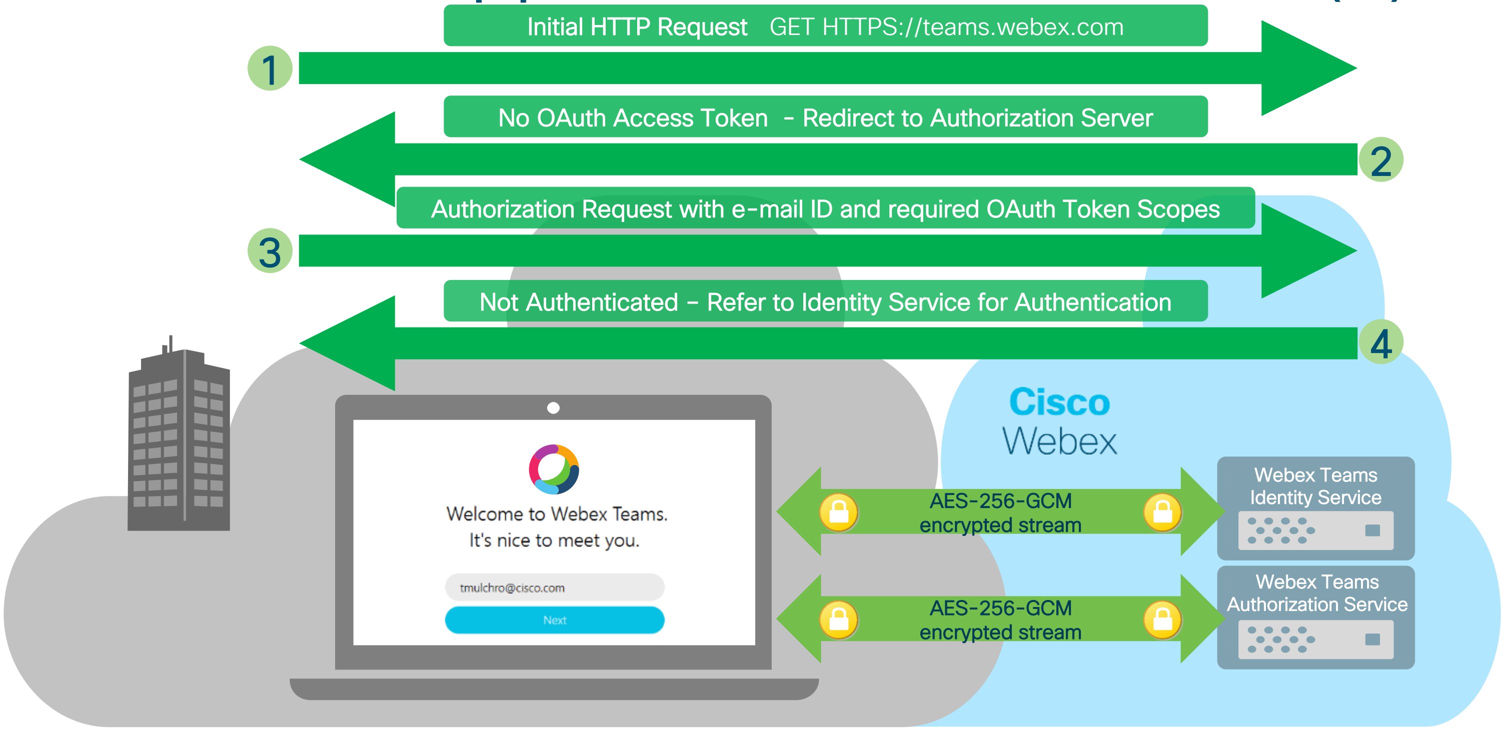
Device checks current software version. If upgrade required, a signed image is sent to the device.

Device registers to Webex Services



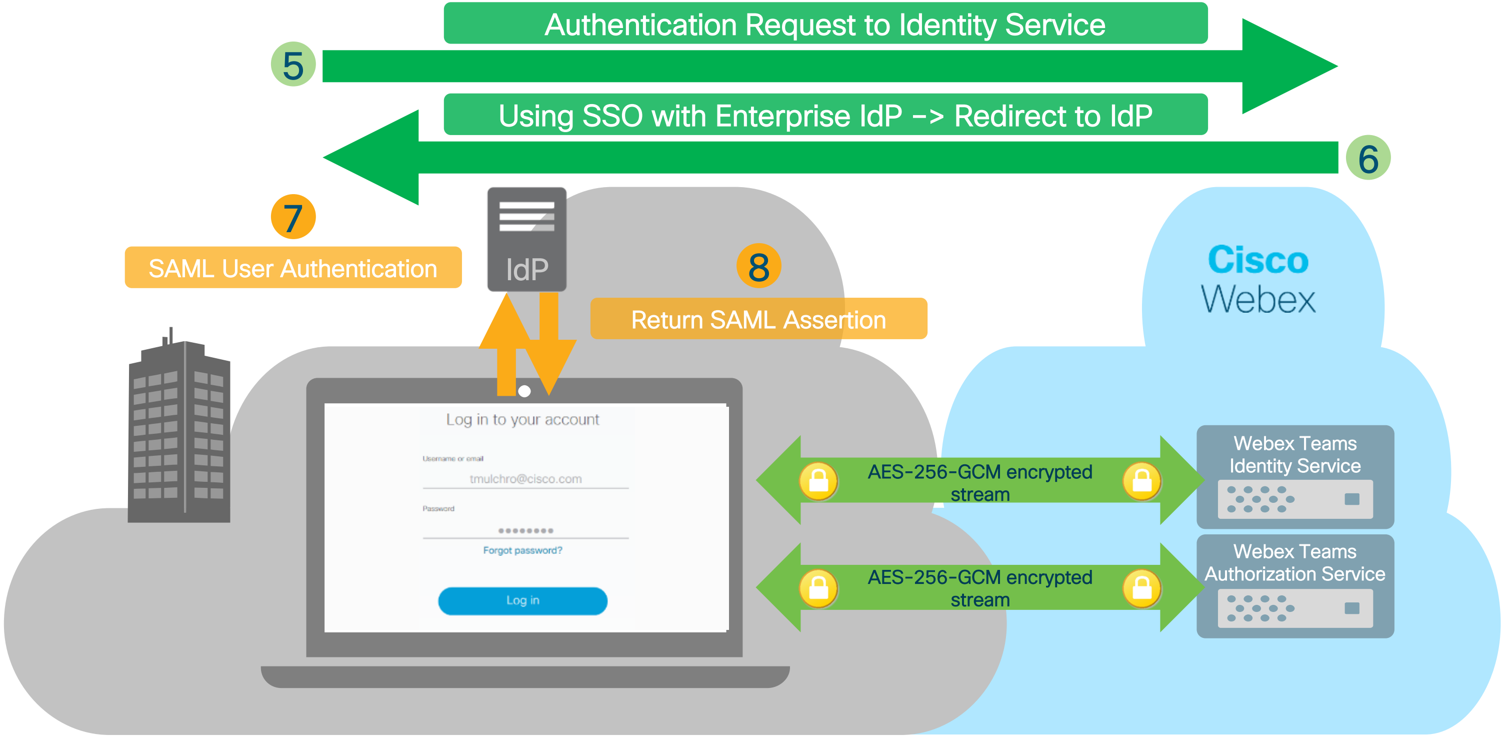
1234567890123456

Webex Teams App : User Authentication (1)


Initial HTTP Request GET HTTPS://teams.webex.com
1
No OAuth Access Token - Redirect to Authorization Server
2
Authorization Request with e-mail ID and required OAuth Token Scopes
3
Not Authenticated – Refer to Identity Service for Authentication
4
Welcome to Webex Teams.
It's nice to meet you.
tmulchro@cisco.com
Next
AES-256-GCM encrypted stream
AES-256-GCM encrypted stream
Cisco Webex
Webex Teams Identity Service
Webex Teams Authorization Service

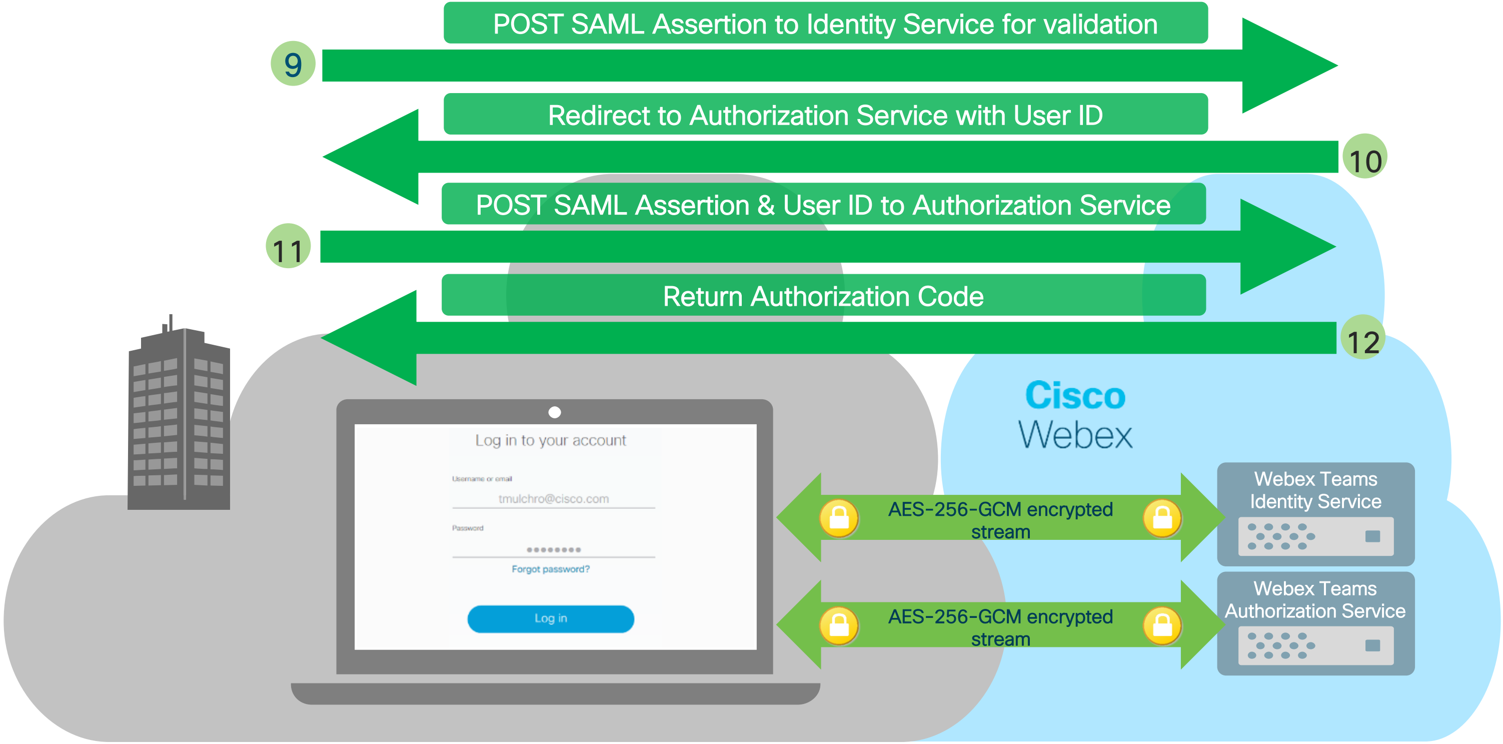
To access any Webex Teams service – the App/ Device must present a validate OAuth Access Token
If no Access Token is present - the App/Device is redirected to the Authorization Service
The e-mail address in the Authorization request determines the User's Org and Identity Service
App/ Device redirected to Identity service for Authentication

Webex Teams App : User Authentication (2)


Authentication Request to Identity Service
5
Using SSO with Enterprise IdP –> Redirect to IdP
6
7
SAML User Authentication
IdP
8
Return SAML Assertion
Cisco
Webex
Log in to your account
Username or email
tmulchro@cisco.com
Password
••••••••
Forgot password?
Log in
AES-256-GCM encrypted stream
AES-256-GCM encrypted stream
Webex Teams Identity Service
Webex Teams Authorization Service

Users can Authenticate to the Webex Teams Identity service (typically consumer accounts), or to an Enterprise (on-premises, or cloud) IdP that support Single Sign on (SSO) using Security Assertion Markup Language version (SAML) 2.0 (as shown above)

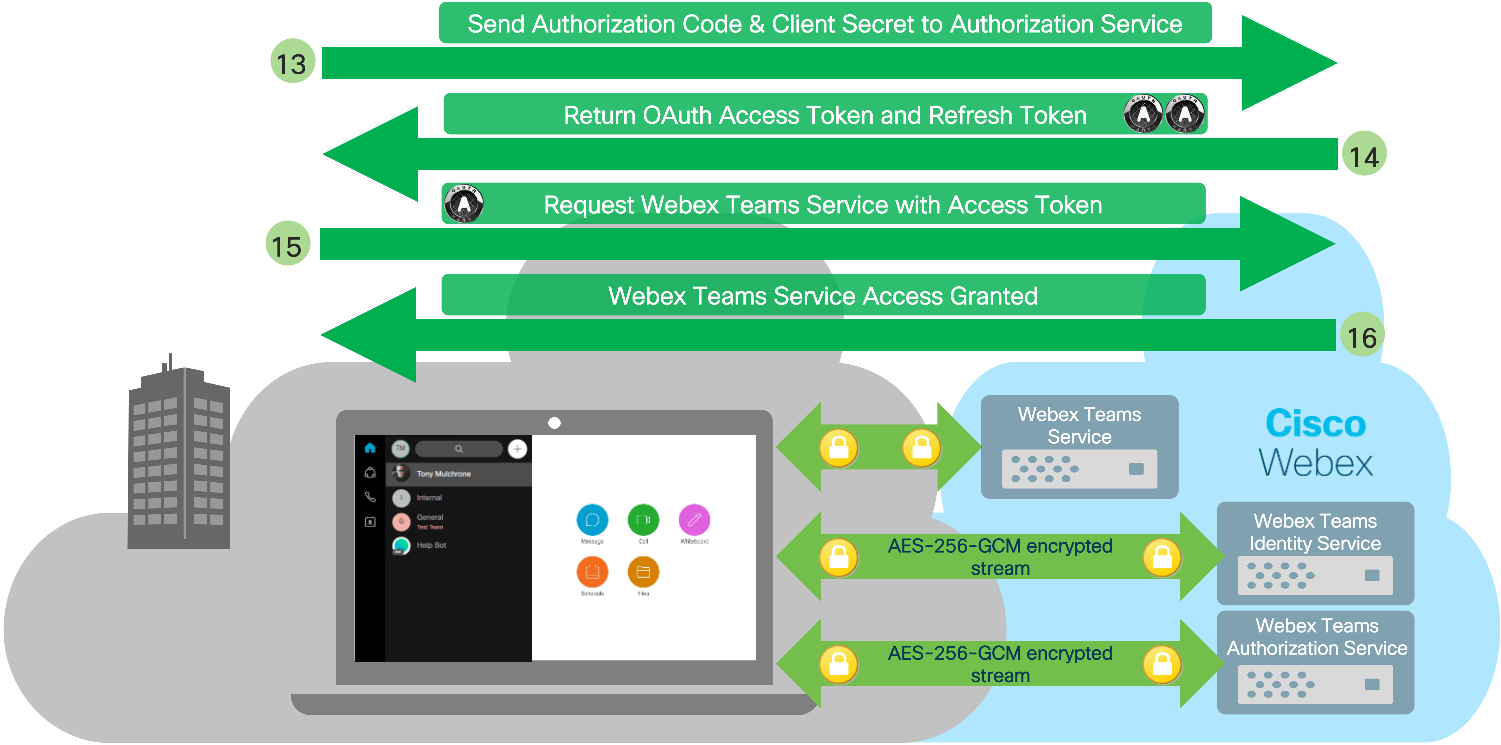
Webex Teams App : User Authentication (3)



9 POST SAML Assertion to Identity Service for validation
10 Redirect to Authorization Service with User ID
11 POST SAML Assertion & User ID to Authorization Service
12 Return Authorization Code
Log in to your account
Username or email
tmulchro@cisco.com
Password
••••••••
Forgot password?
Log in
AES-256-GCM encrypted stream
AES-256-GCM encrypted stream
Cisco Webex
Webex Teams Identity Service
Webex Teams Authorization Service

Webex Teams users using Single Sign On use a combination SAML for authentication and the OAuth Authorization Code Grant method for authorization (as shown above)

Webex Teams App : User/Device Authorization

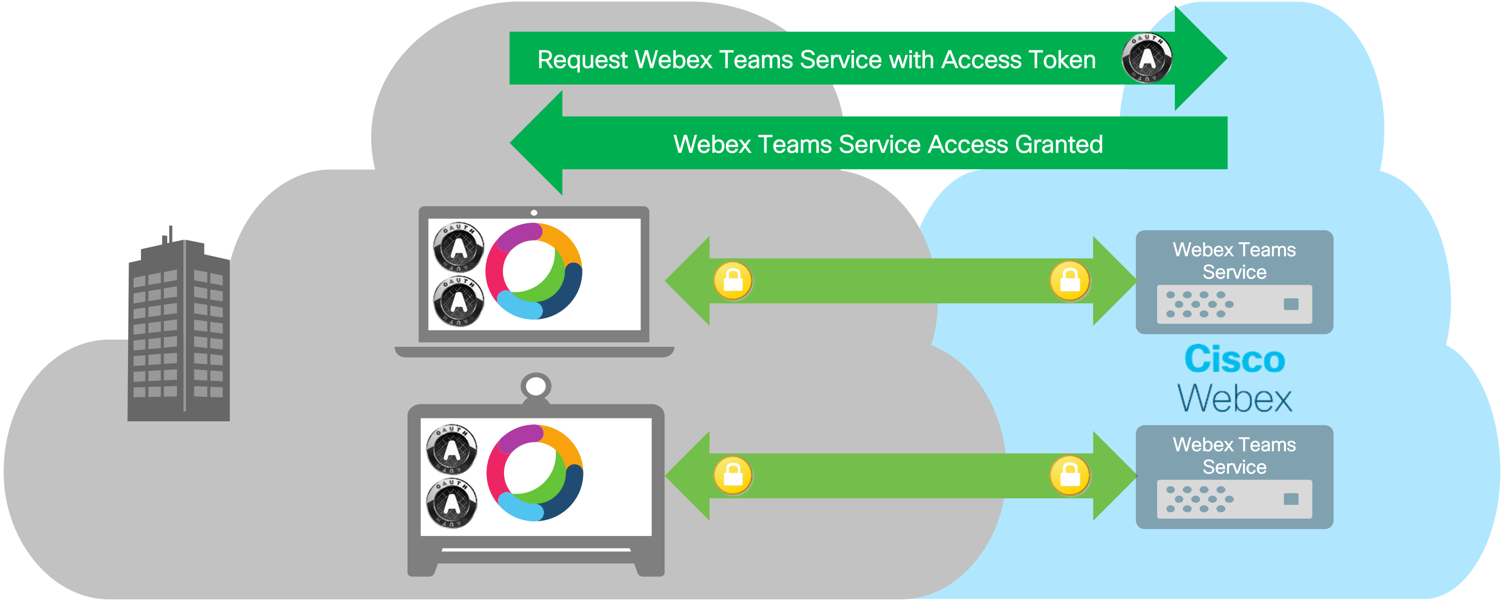


13
Send Authorization Code & Client Secret to Authorization Service
Return OAuth Access Token and Refresh Token
14
15
Request Webex Teams Service with Access Token
Webex Teams Service Access Granted
16
Webex Teams Service
Cisco Webex
Webex Teams Identity Service
Webex Teams Authorization Service
AES-256-GCM encrypted stream
AES-256-GCM encrypted stream
Tony Mulchrone
Internal
General
Test Team
Help Bot
Message
Call
Whiteboard
Schedule
Files

Once the Webex Teams App/ Device is authenticated the Authorization Code Grant flow is used to deliver OAuth Access and Refresh Token to the App/ Device

The Access Token must be presented to gain authorized access to Webex services

Webex Teams : OAuth Access and Refresh Tokens

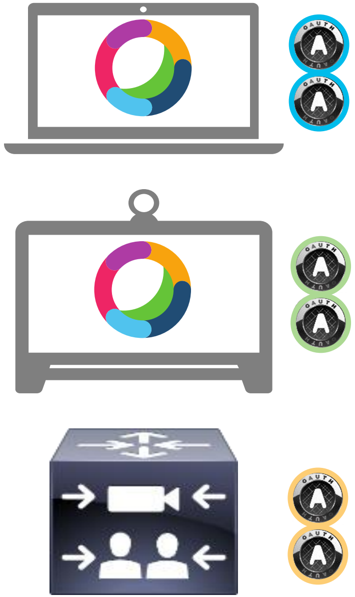

Request Webex Teams Service with Access Token
Webex Teams Service Access Granted
Webex Teams Service
Cisco Webex
Webex Teams Service

OAuth Access Token – Uses JSON Web Token (JWT) format, signed (JWS) and encrypted (JWE)

OAuth Refresh Token – Presented to the authorization service to renew the Access token

Access tokens allow apps and devices to gain access to authorized services
Access tokens contain scopes that define which services are authorized
Access tokens are renewed when they reach 75% of their lifetime

Webex Teams : OAuth Access and Refresh Tokens



Webex Access Token lifetimes vary by device e.g.
Teams App access token lifetime = 6 hours
Device access token lifetime = 6 hours
Directory Connector access token lifetime = 1 hour
Access Token renewed by sending Refresh Token when lifetime = 75%
Lifetime values can be reconfigured by service request

Webex Refresh Token lifetimes typically 60 days
Lifetime values can be reconfigured by service request
Refresh Token renewed when Access Token renewed
Refresh Token renewal (on/off) configurable by service request
If Refresh Token renewal = Off : App logged-out, Device off-boarded when Refresh Token lifetime expires

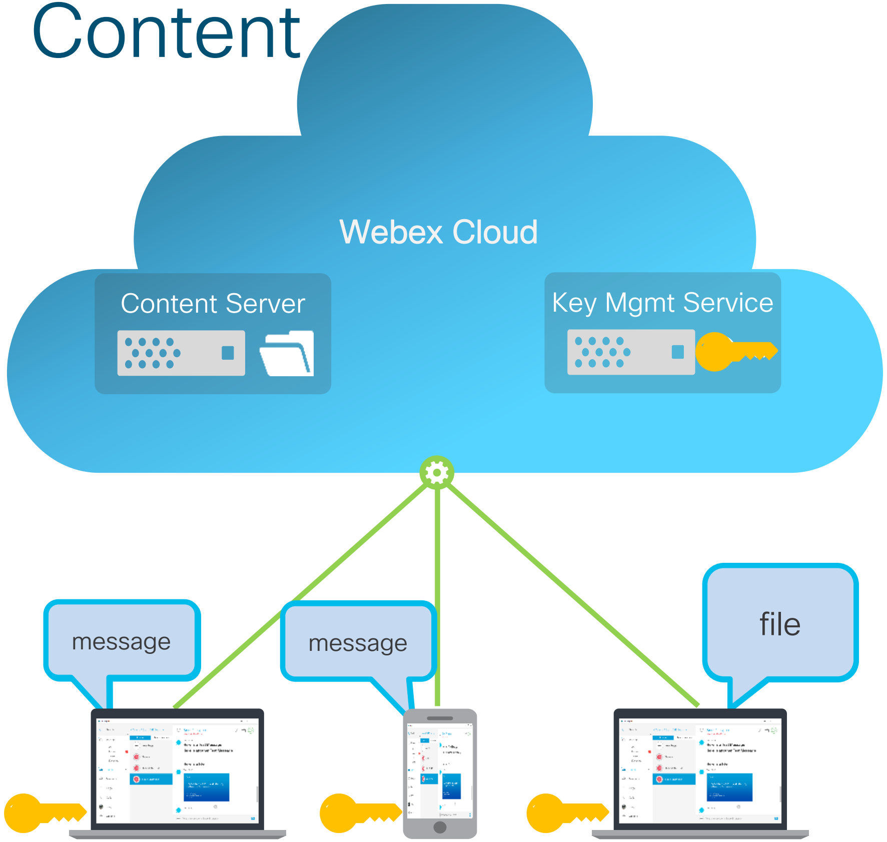
OAuth Access Token scopes define which services Apps and devices are permitted to use e.g :
Read messages/ Write messages/ Read space memberships/ Write space memberships

Apps and devices may have more than one access token e.g. Webex cloud services, Cloud/On Premises (HDS) Key Management Service (KMS), Third Party Apps (e.g. ECM, Cloud Calendar)

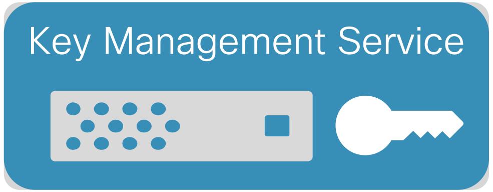
Webex Teams Platform Security

Securing Messages and Content with End to End Encryption

Webex Teams- Encrypting Messages and Content



AES256-GCM cipher used for Encryption

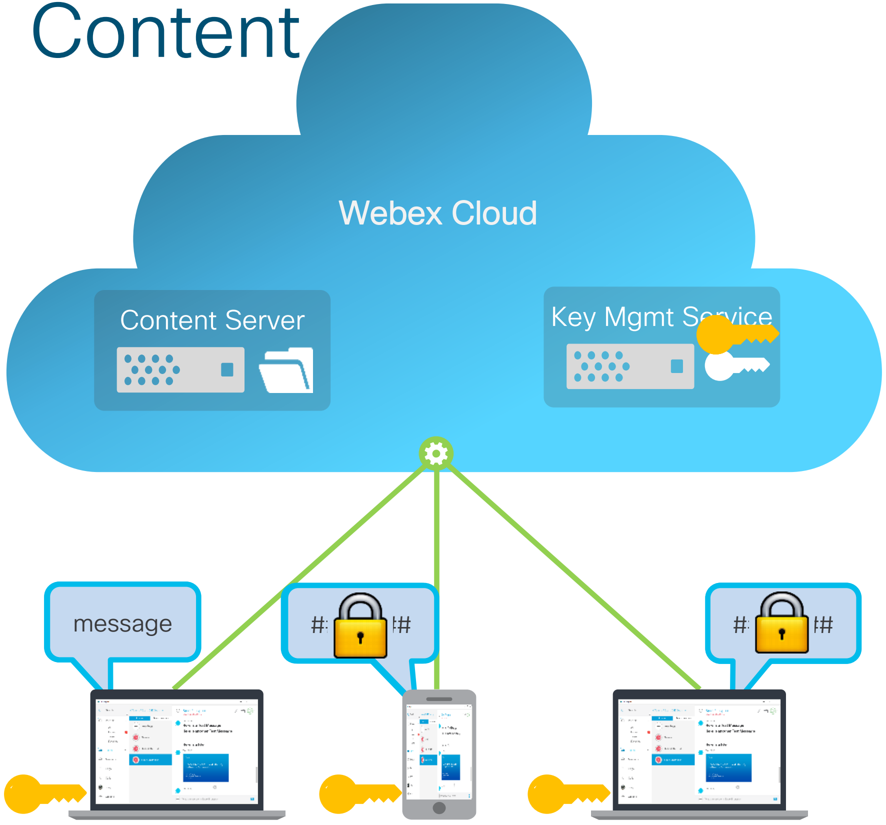


Any messages or files sent by an App are encrypted before being sent to the Webex Cloud

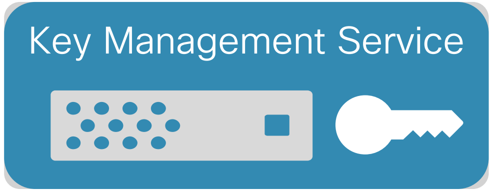
Webex Teams App requests a conversation encryption key from the Key Management Service

Each Webex Teams Space uses a different Conversation Encryption key

Webex Teams - Decrypting Messages and Content



AES256-GCM cipher used for Encryption

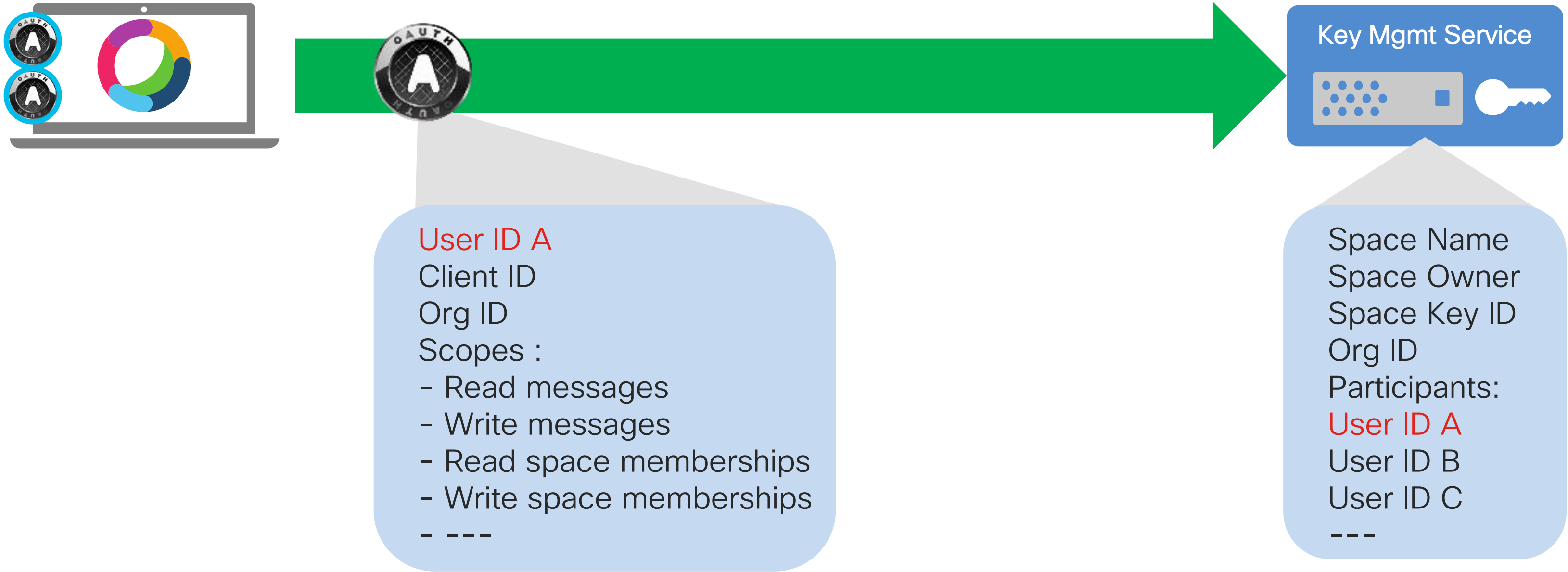


Encrypted messages sent by the App are stored in the Webex Cloud and also sent on to every other App in the Webex Teams Space

Each encrypted message also contains a link to the conversation encryption key

If needed, Webex Teams Apps can retrieve encryption keys from the Key Management Service

Webex Teams : Access Tokens and controlled access to User Generated Content



Key Mgmt Service

User ID A
Client ID
Org ID
Scopes :
- Read messages
- Write messages
- Read space memberships
- Write space memberships
- ---

Space Name
Space Owner
Space Key ID
Org ID
Participants:
User ID A
User ID B
User ID C

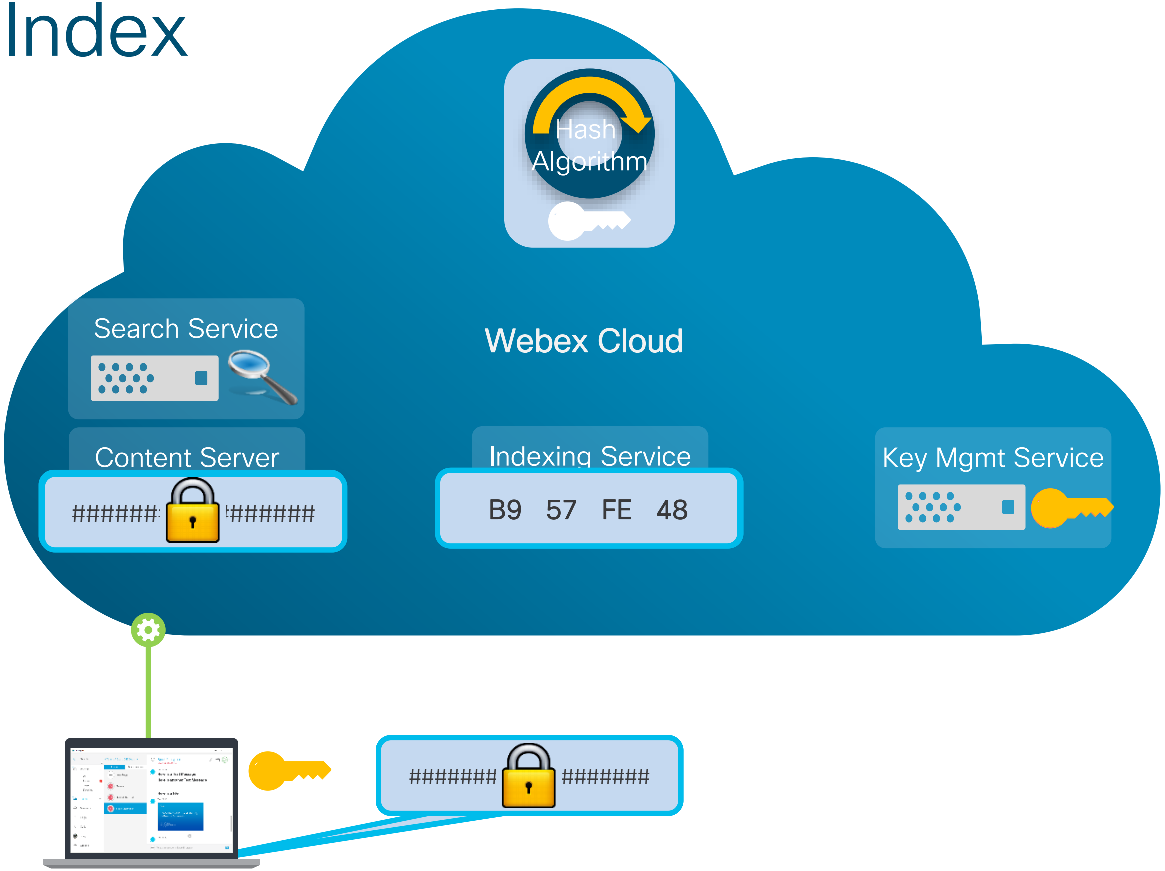
To gain access to any Webex Teams space and to read the content associated with that space, a user must first request the encryption key for that space using the KMS Access Token for their organization

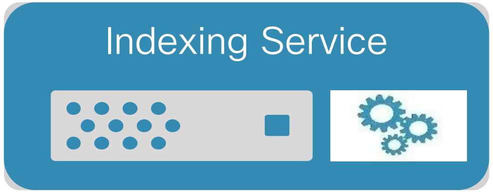
KMS Resource Object (KRO)

A data structure that is used to track the encryption key for a space and the people that are authorized to receive the key

Cloud Based Security : Secure Search and Indexing

Searching Webex Teams Spaces: Building a Search Index





The Indexing Service : Enables users to search for names and words in the encrypted messages stored in the Content Server without decrypting content

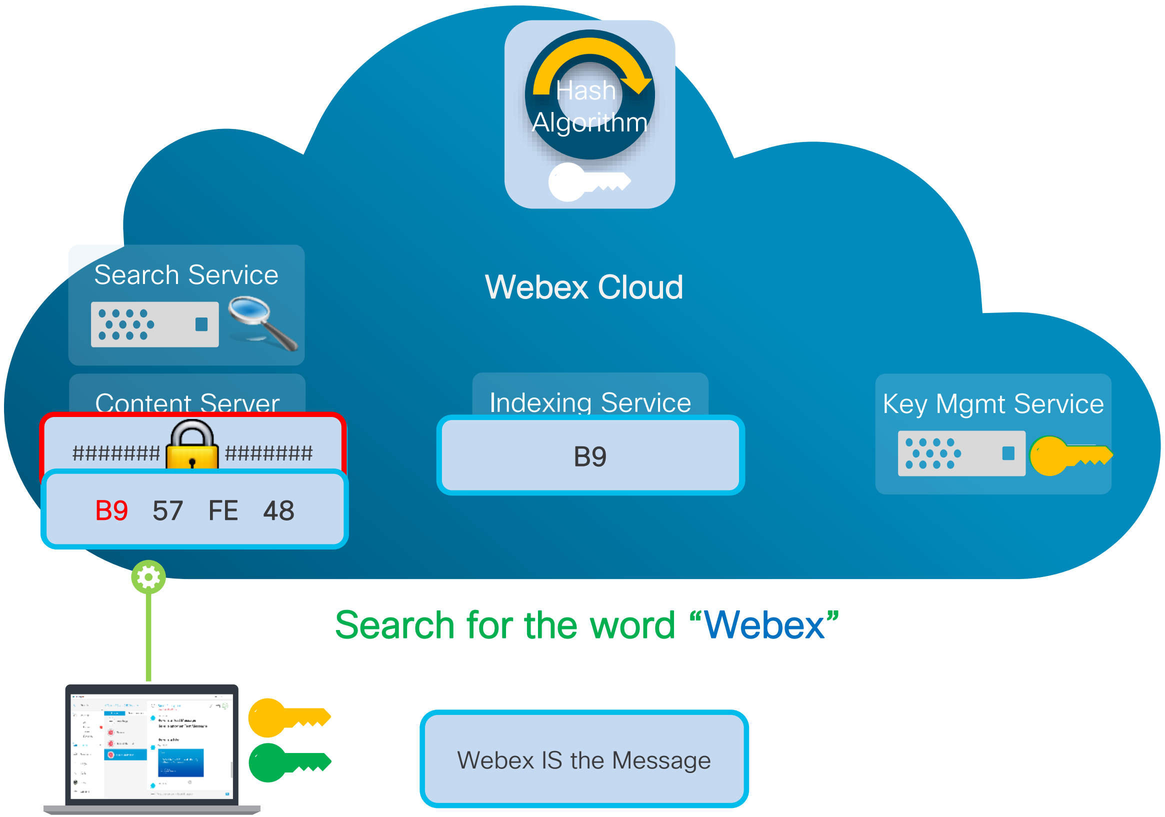
A Search Index is built by creating a fixed length hash* of each word in each message within a Space

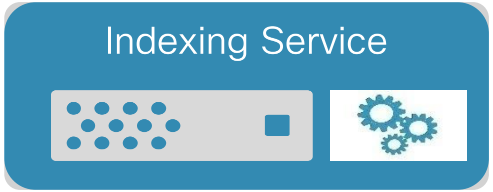
The hashed indexes for each Webex Teams Space are stored by the Content Service

*A new (SHA-256 HMAC) hashing key (Search Key) is used for each space

Webex Teams spaces : Querying a Search Index

Search for the word “Webex”





App sends search request over a secure connection to the Indexing Service

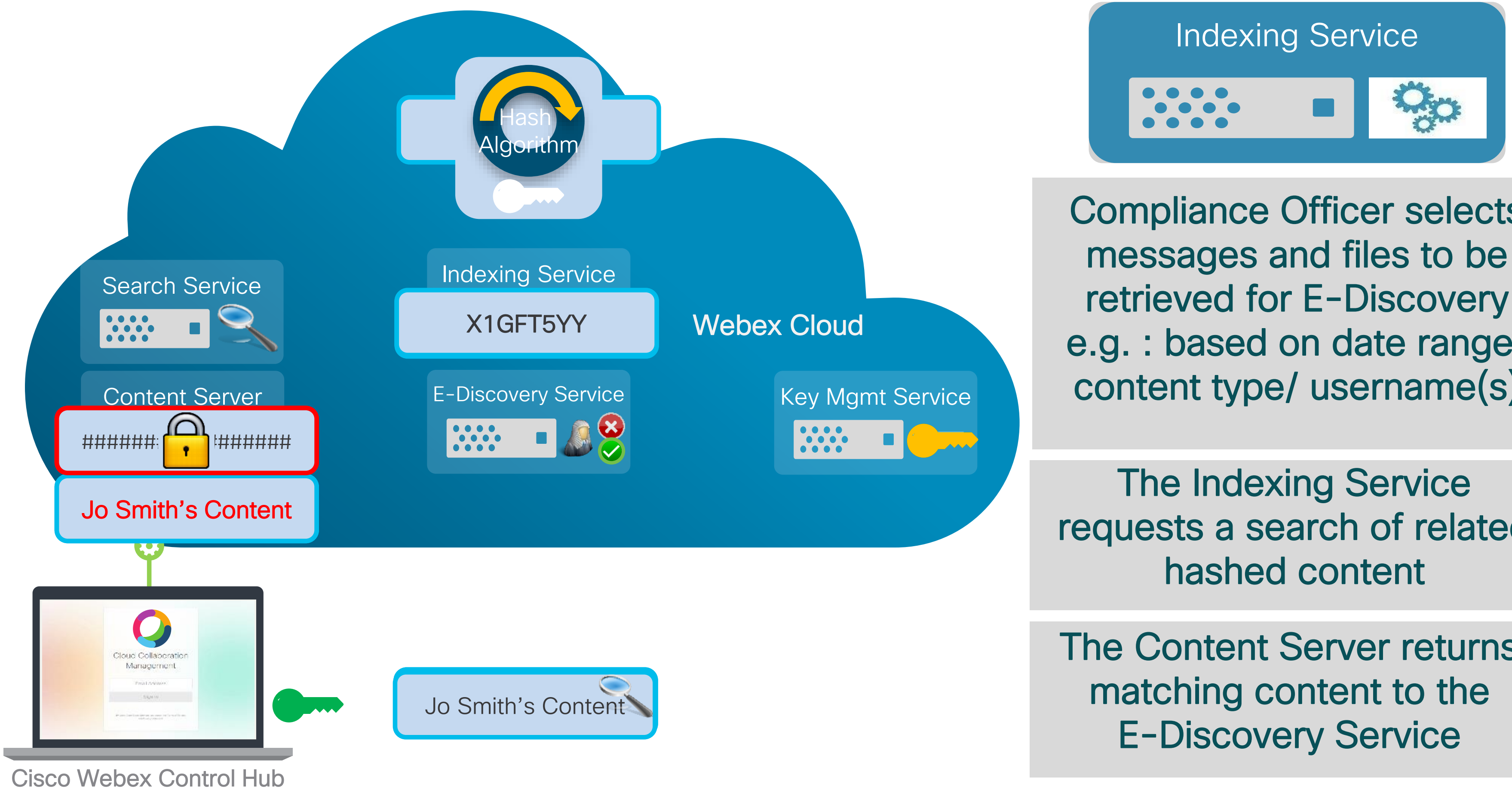
The Indexing Service uses per space search keys to hash the search terms

The Search Service searches the for a match in the hash tables and returns matching content to the App *

*A link to Conversation Encryption Key is sent with encrypted message

Cloud Based Security :
E Discovery Services

Webex Teams E-Discovery Service : (1)

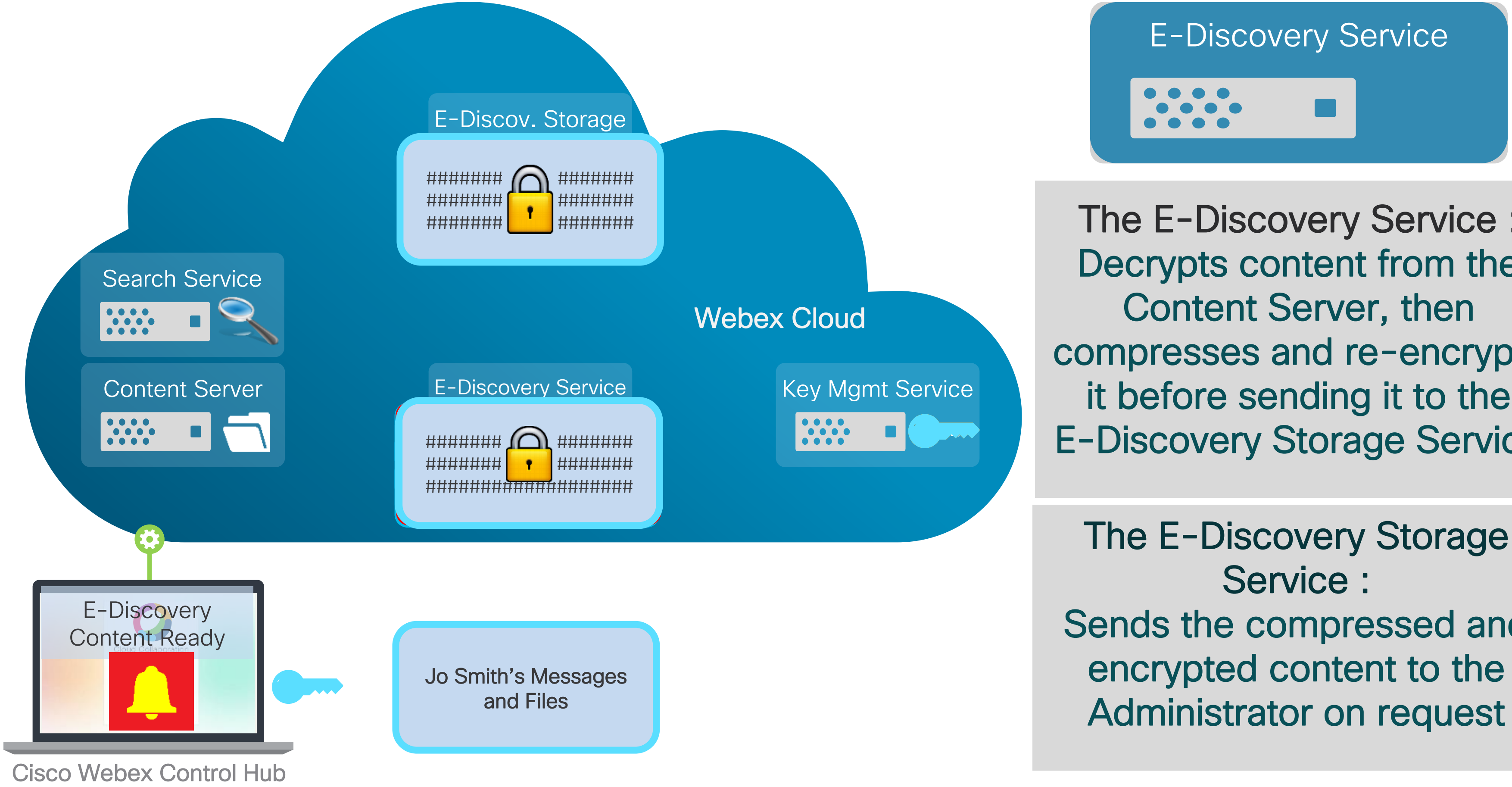


Compliance Officer selects messages and files to be retrieved for E-Discovery e.g. : based on date range/ content type/ username(s)

The Indexing Service requests a search of related hashed content

The Content Server returns matching content to the E-Discovery Service

Webex Teams E-Discovery Service : (2)



The E-Discovery Service :
Decrypts content from the Content Server, then compresses and re-encrypts it before sending it to the E-Discovery Storage Service

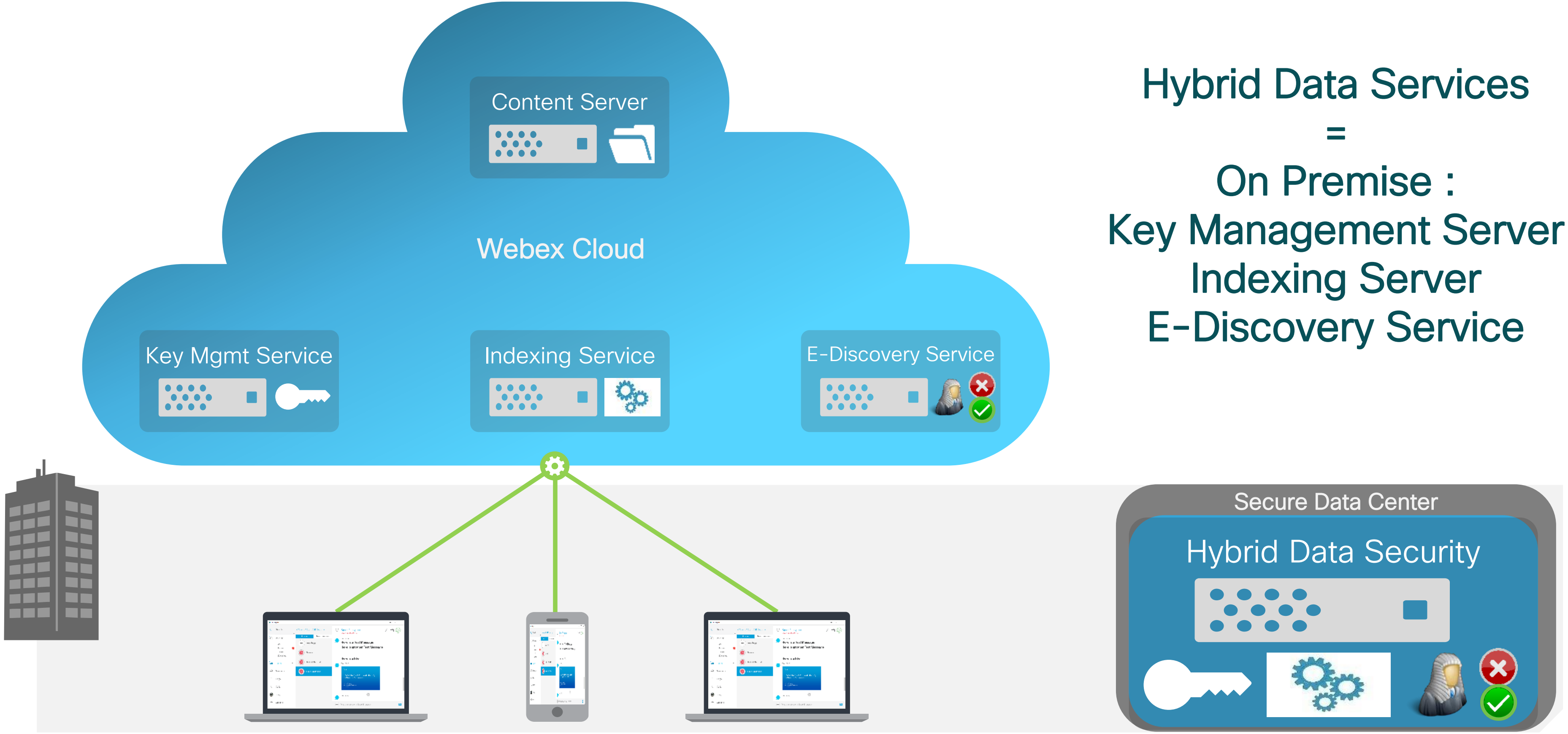
The E-Discovery Storage Service :
Sends the compressed and encrypted content to the Administrator on request

Webex Teams Platform Security

Hybrid Data Security

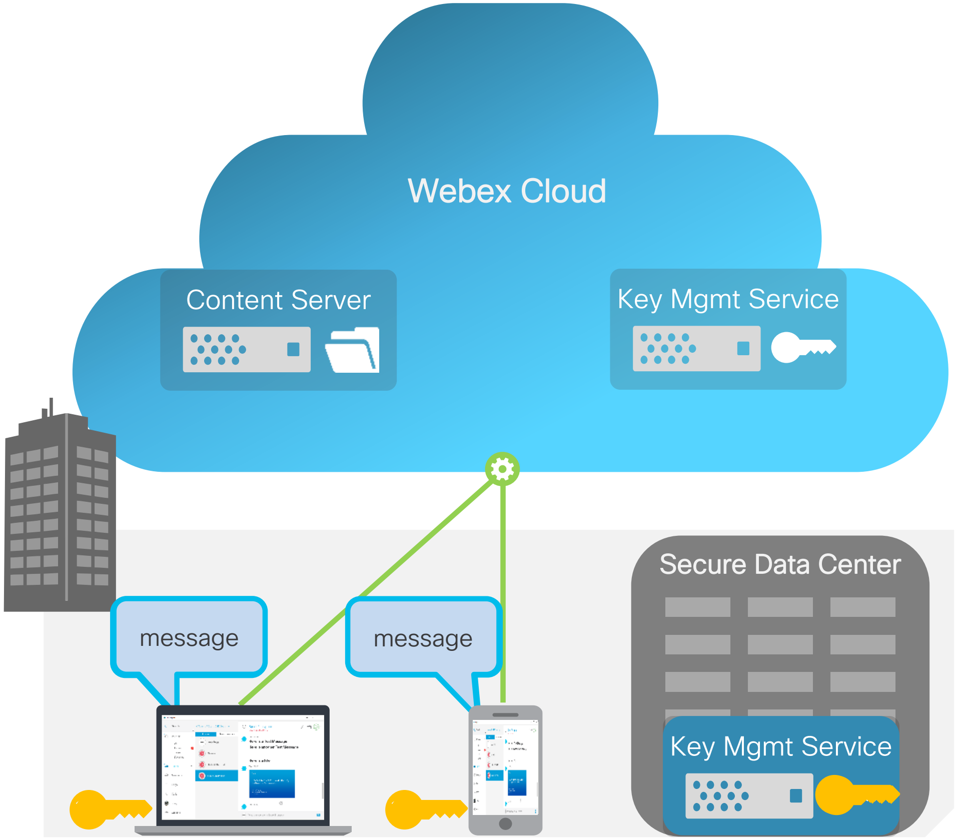
On Premises :
- Encryption Key Management
- Encryption Key Storage
- Content Indexing Service
- eDiscovery Service

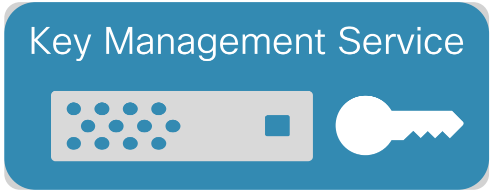
Webex Teams – Hybrid Data Security (HDS)



Hybrid Data Services
=
On Premise :
Key Management Server
Indexing Server
E-Discovery Service

HDS - Encrypting Messages & Content





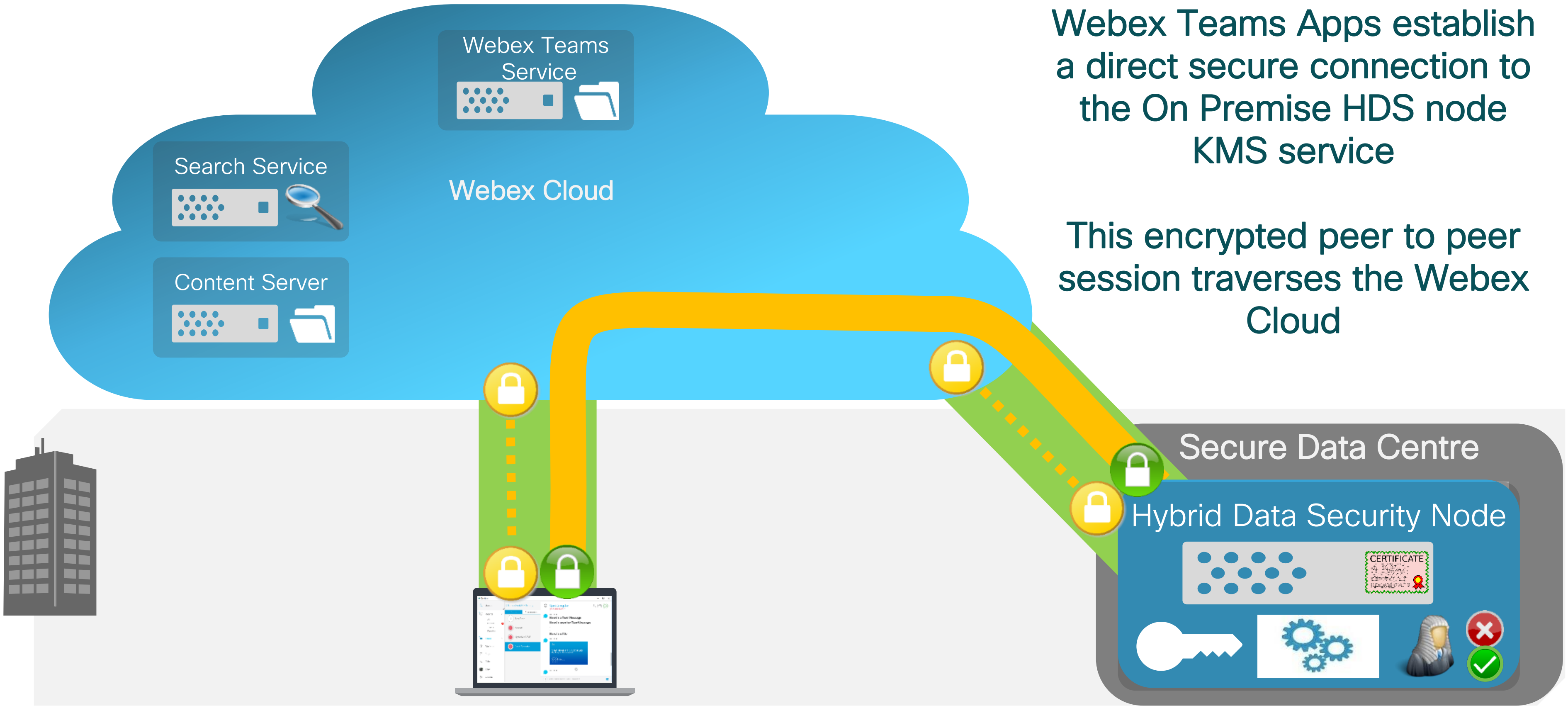
Webex Teams Apps request an encryption key from the HDS Key Management Server

Any messages or files sent by an App are encrypted before being sent to the Webex Cloud

Encrypted messages and content stored in the cloud

Encryption Keys stored locally

Hybrid Data Security – Secure App Connections



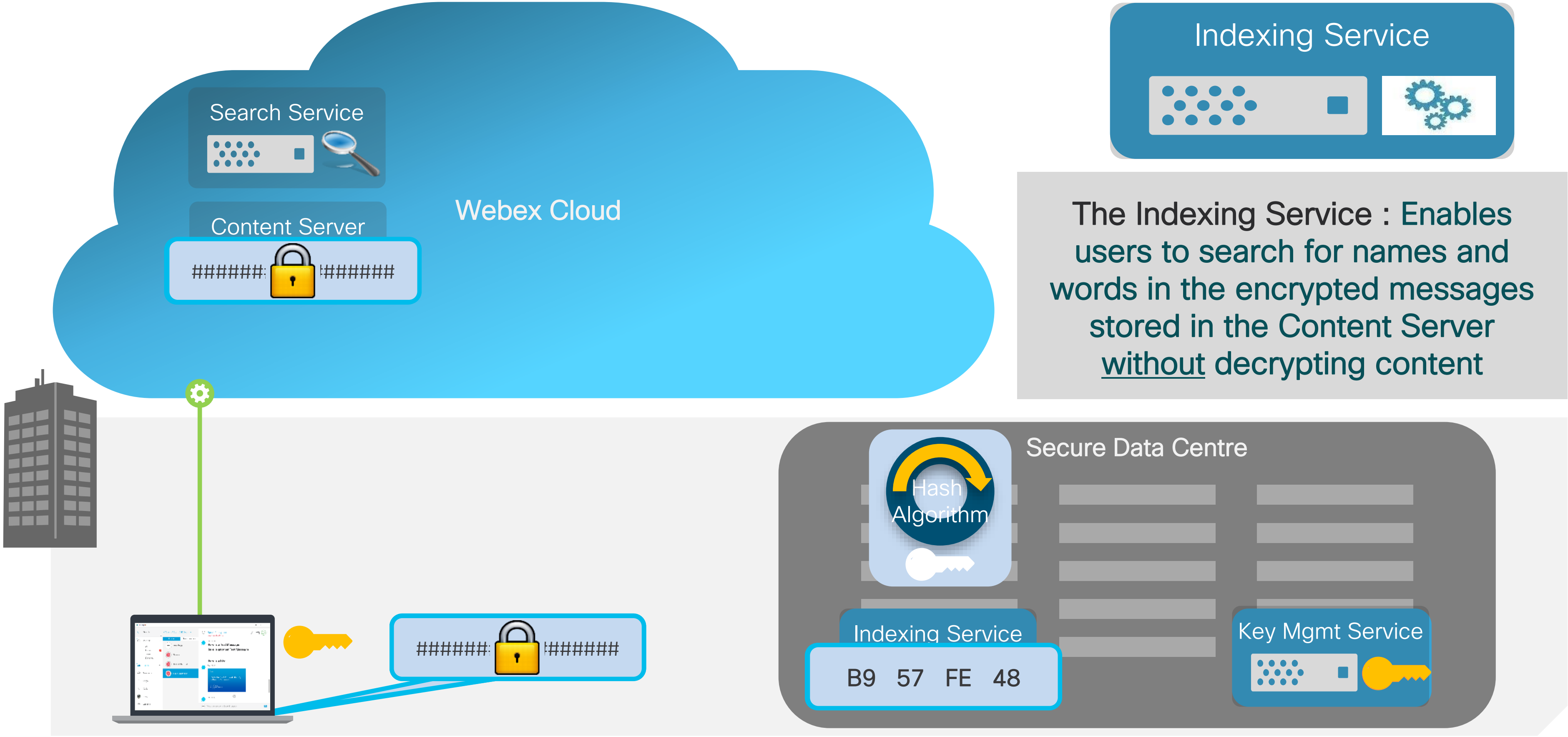
Webex Teams Apps establish a direct secure connection to the On Premise HDS node KMS service

This encrypted peer to peer session traverses the Webex Cloud

🟩 App to Cloud TLS connection

🟨 App to HDS secure connection (ECDHE- AES-256-GCM)

Hybrid Data Security: Search Indexing Service

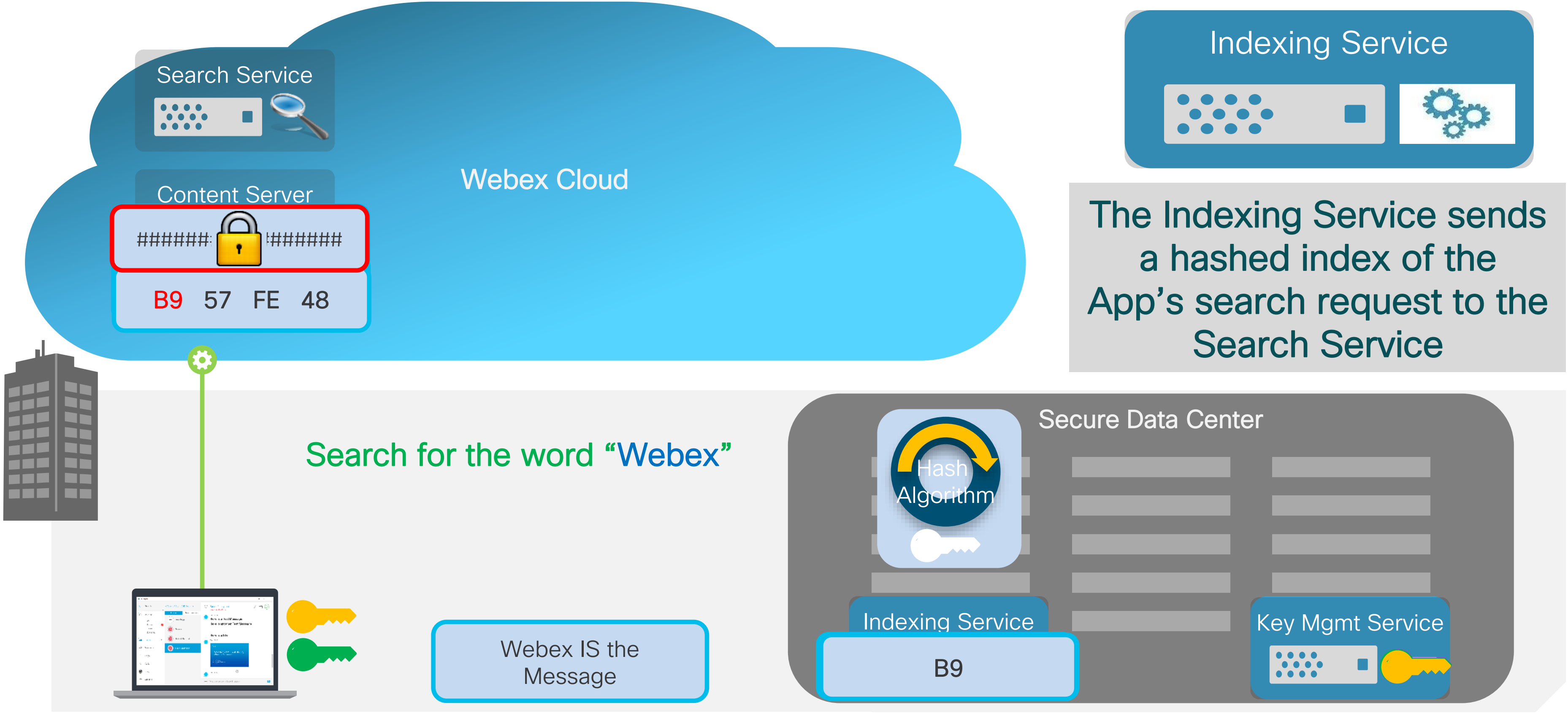


The Indexing Service : Enables users to search for names and words in the encrypted messages stored in the Content Server without decrypting content

* A new hashing key (Search Key) is used for each space

Hybrid Data Security: Querying a Search Index

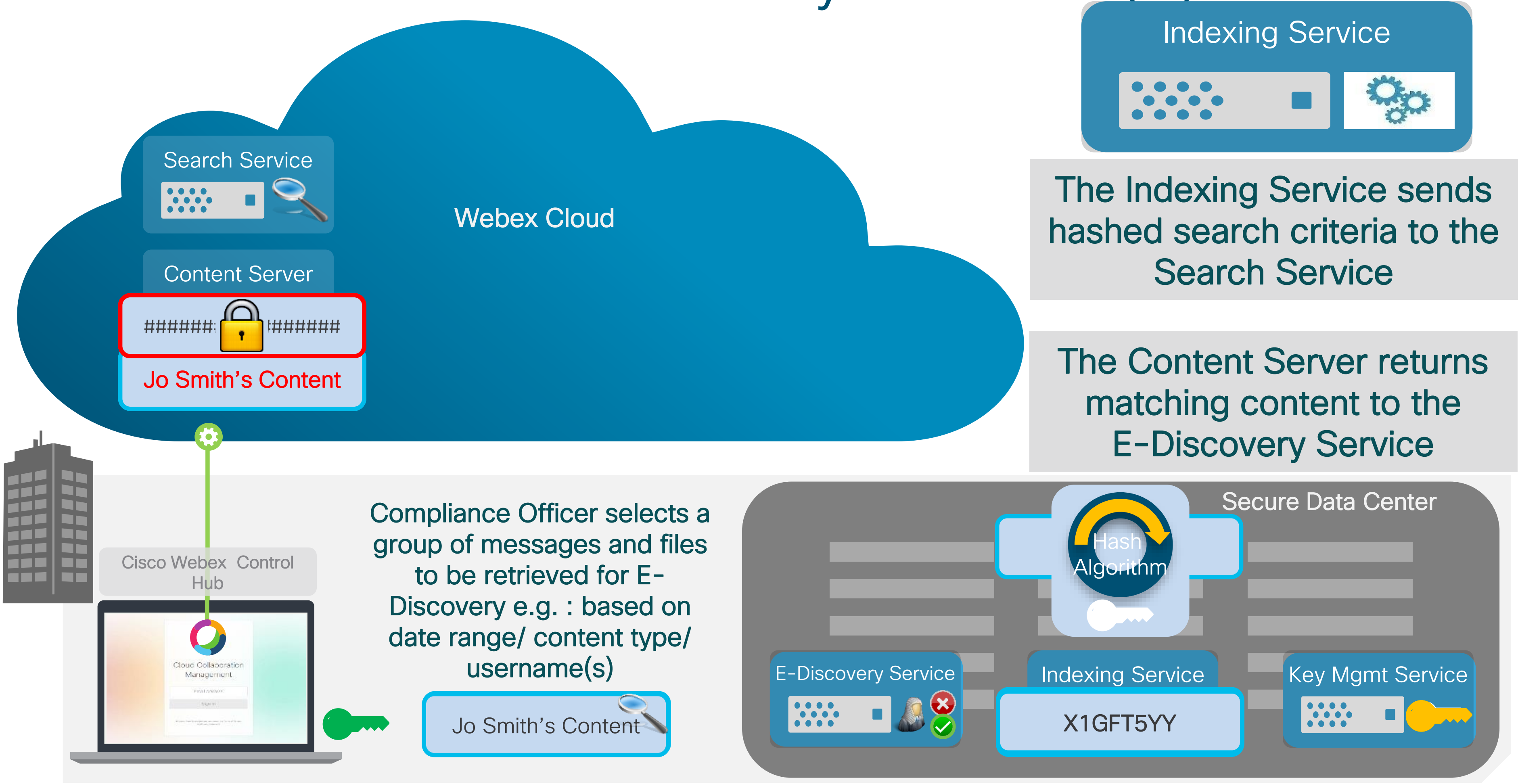
Search for the word “Webex”



The Indexing Service sends a hashed index of the App’s search request to the Search Service

*A link to Conversation Encryption Key is sent with the message

Webex Teams E-Discovery Service : (1)

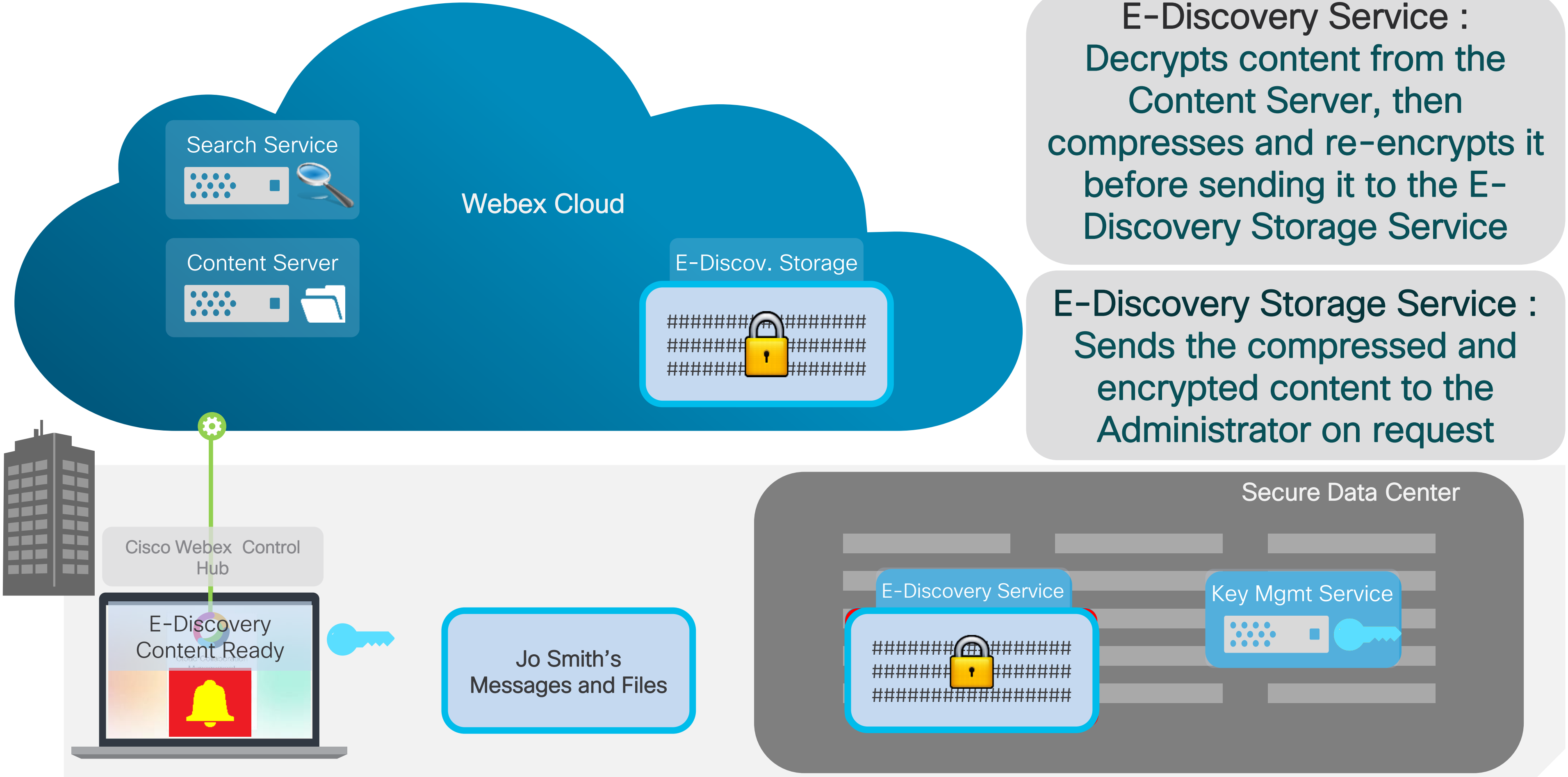


The Indexing Service sends hashed search criteria to the Search Service

The Content Server returns matching content to the E-Discovery Service

Compliance Officer selects a group of messages and files to be retrieved for E-Discovery e.g. : based on date range/ content type/ username(s)

Webex Teams E-Discovery Service : (2)



E-Discovery Service : Decrypts content from the Content Server, then compresses and re-encrypts it before sending it to the E-Discovery Storage Service

E-Discovery Storage Service : Sends the compressed and encrypted content to the Administrator on request

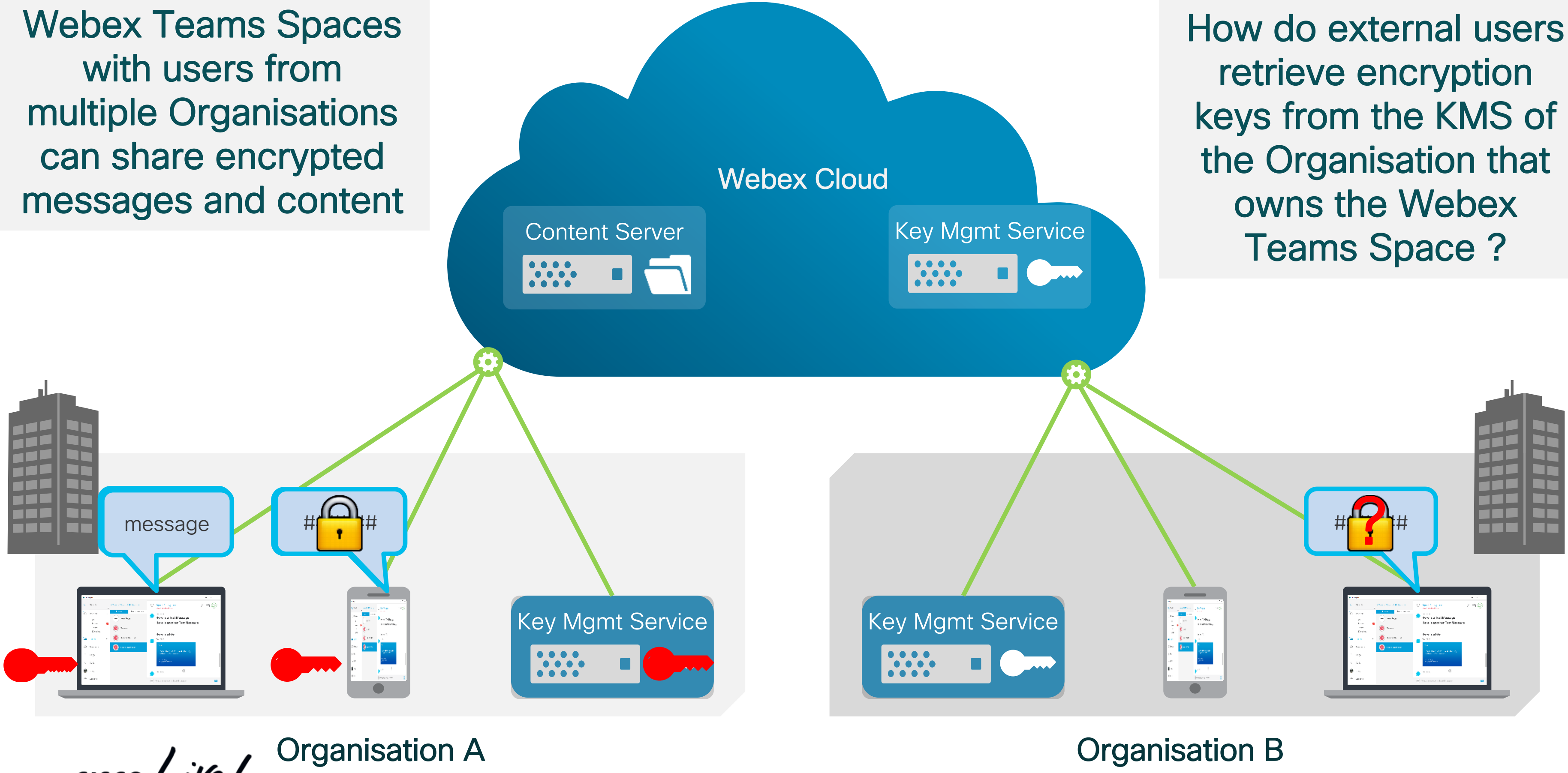
Customer Controlled Security :

Key Management Server Federation with other Webex Teams Orgs.

HDS: Encryption Keys & Users in other Organizations

Webex Teams Spaces with users from multiple Organisations can share encrypted messages and content

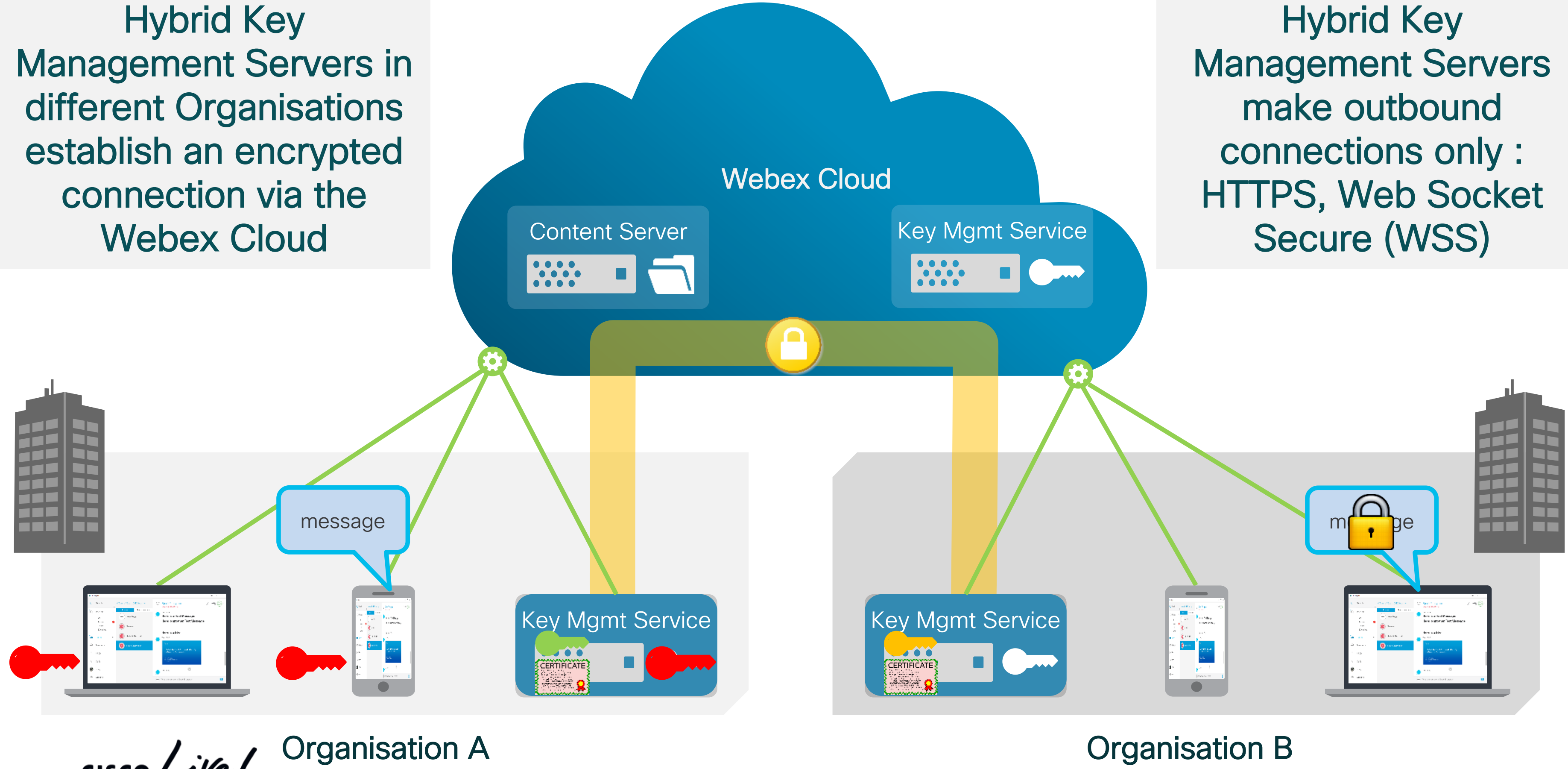
How do external users retrieve encryption keys from the KMS of the Organisation that owns the Webex Teams Space ?



HDS: Key Management Server Federation

Hybrid Key Management Servers in different Organisations establish an encrypted connection via the Webex Cloud

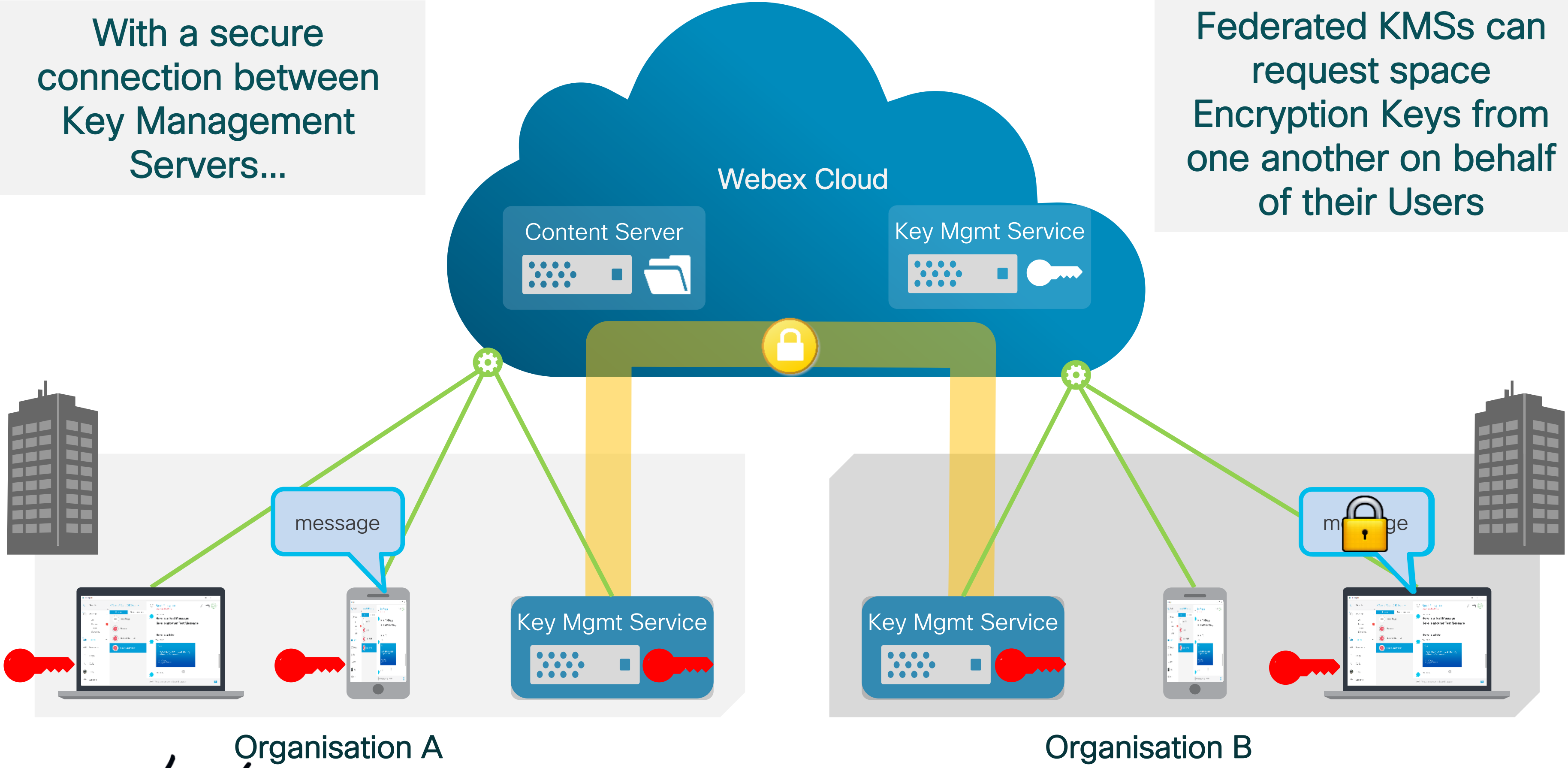
Hybrid Key Management Servers make outbound connections only : HTTPS, Web Socket Secure (WSS)



HDS: Key Management Server Federation

With a secure connection between Key Management Servers...

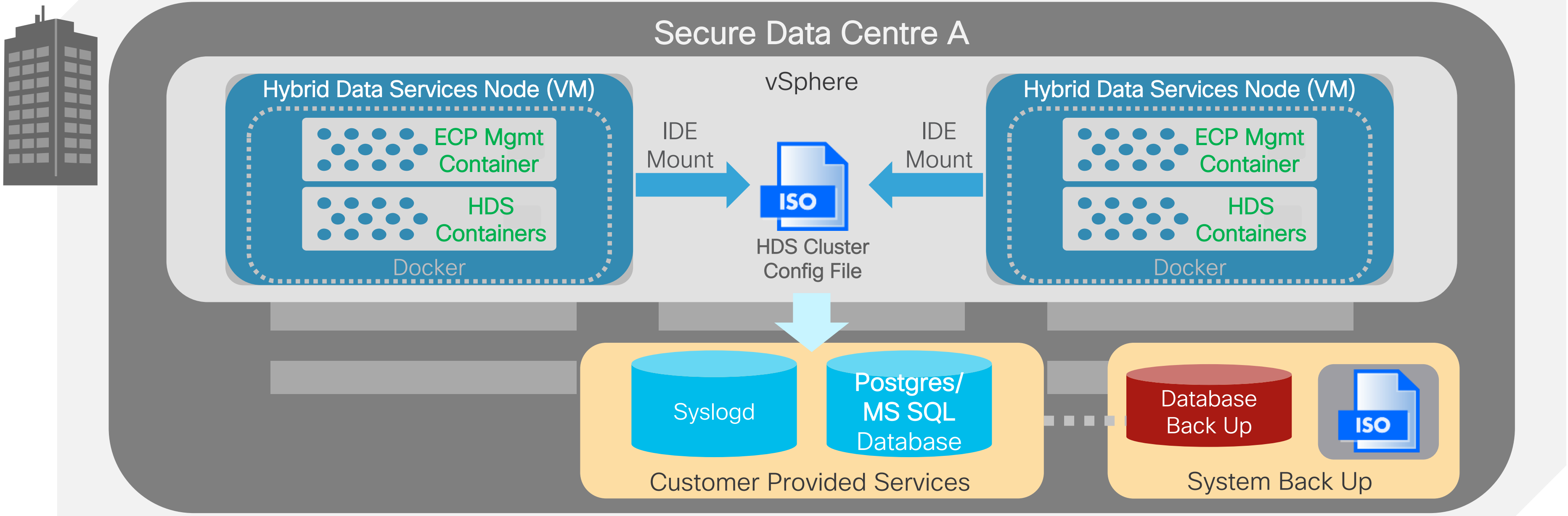
Federated KMSs can request space Encryption Keys from one another on behalf of their Users



Customer Controlled Security :

HDS Deployment Considerations

HDS System Architecture



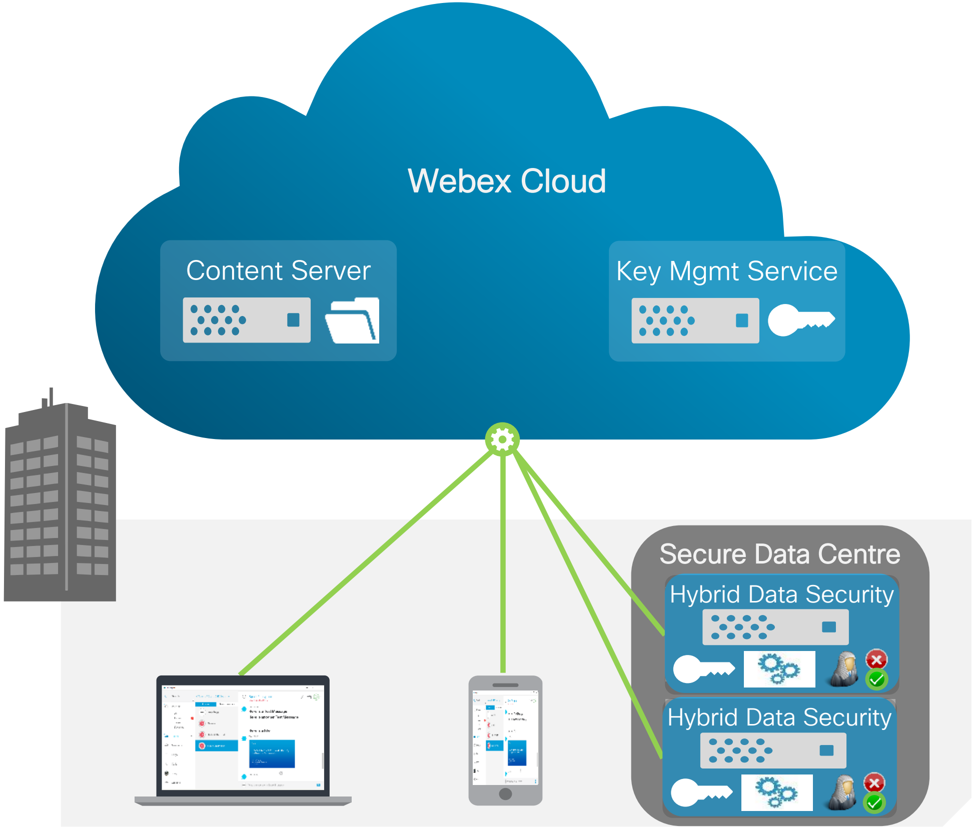
ECP (Enterprise Compute Platform): Management containers which communicate with the cloud and perform actions such as sending health checks and checking for new versions of HDS.

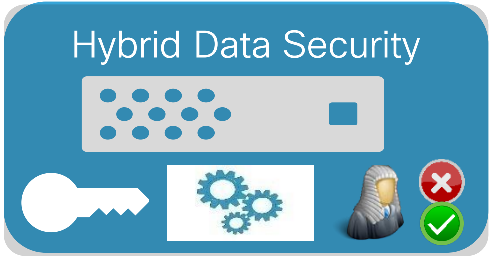
HDS (Hybrid Data Security): Key Management Service, Search Indexer, and eDiscovery Services.

HDS Cluster Config: An ISO file containing configuration information for the local HDS cluster. e.g. Database connection settings, Database Master Encryption key, etc.

IDE Mount: Mount point of the read-only HDS Cluster Config ISO file containing the configuration settings for HDS system.

Hybrid Data Security - Scalability





Multiple HDS servers (up to 5) can be provisioned for Scalability & Load Sharing

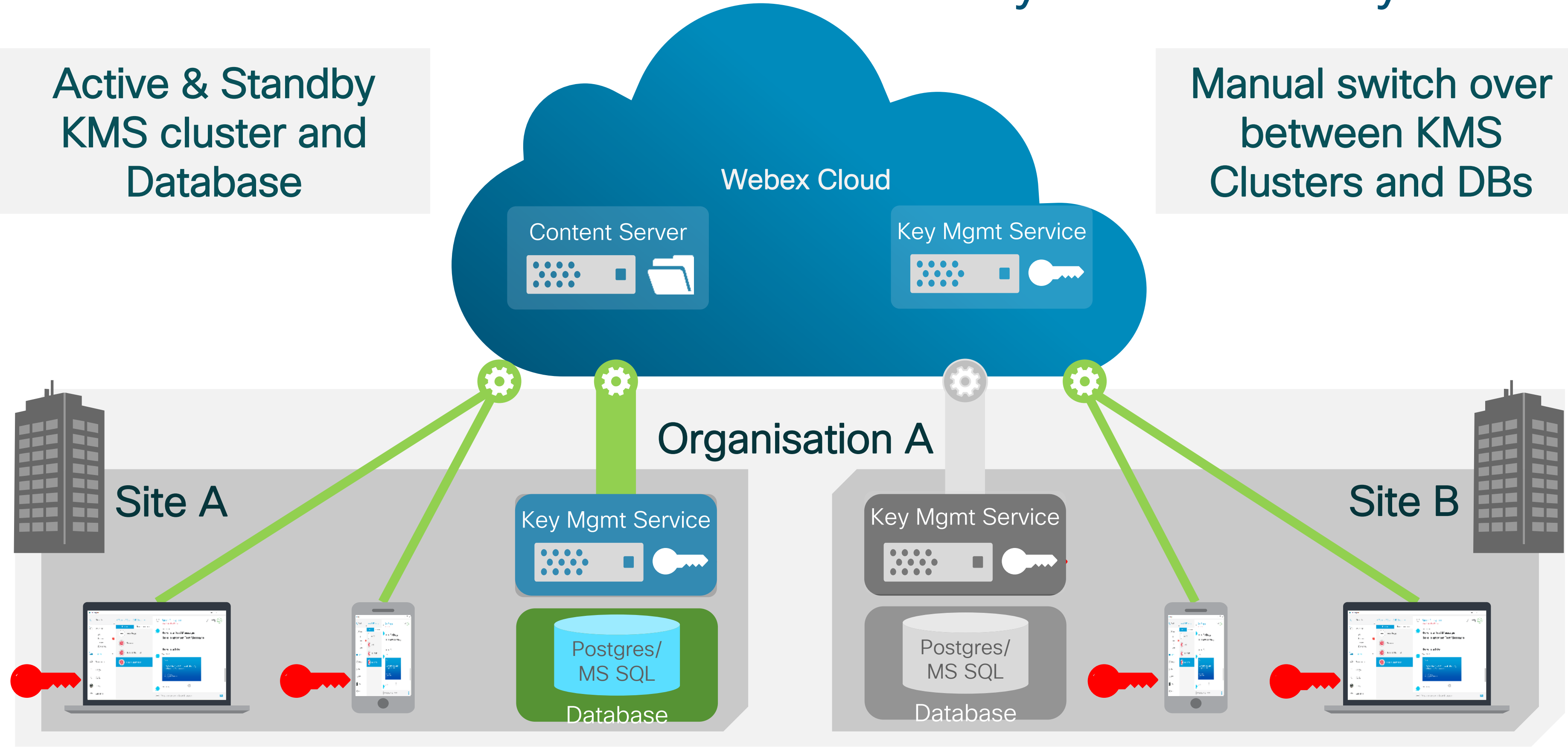
The Hybrid Data Security is managed and upgraded from the cloud

Customer's can access usage information for the HDS Servers via syslog and the Webex Teams Control Hub

HDS: KMS and Database standby redundancy

Active & Standby KMS cluster and Database

Manual switch over between KMS Clusters and DBs

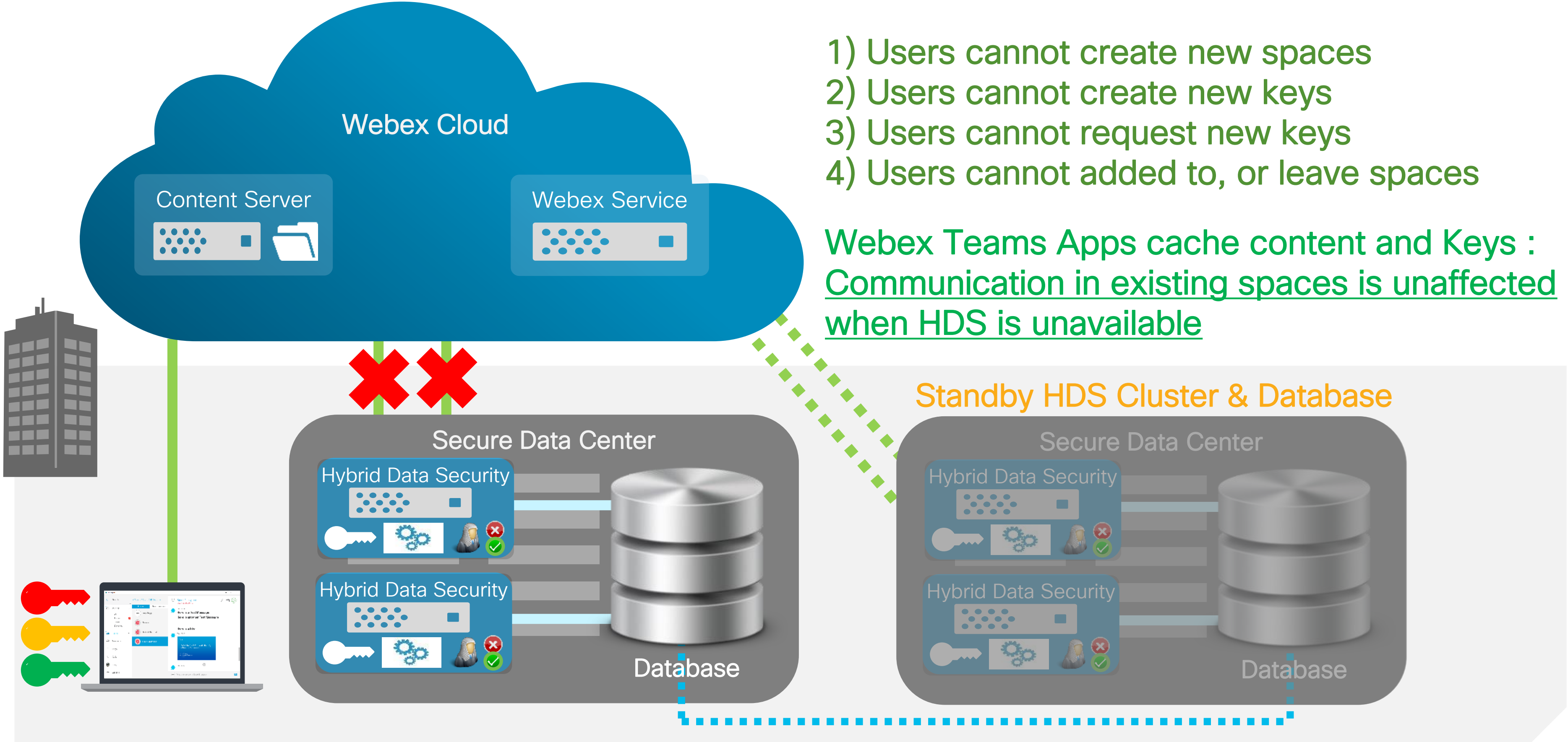


KMS - Hybrid Data Security – User impact of Cluster Failure

When a HDS cluster becomes unavailable :

1) Users cannot create new spaces
2) Users cannot create new keys
3) Users cannot request new keys
4) Users cannot added to, or leave spaces

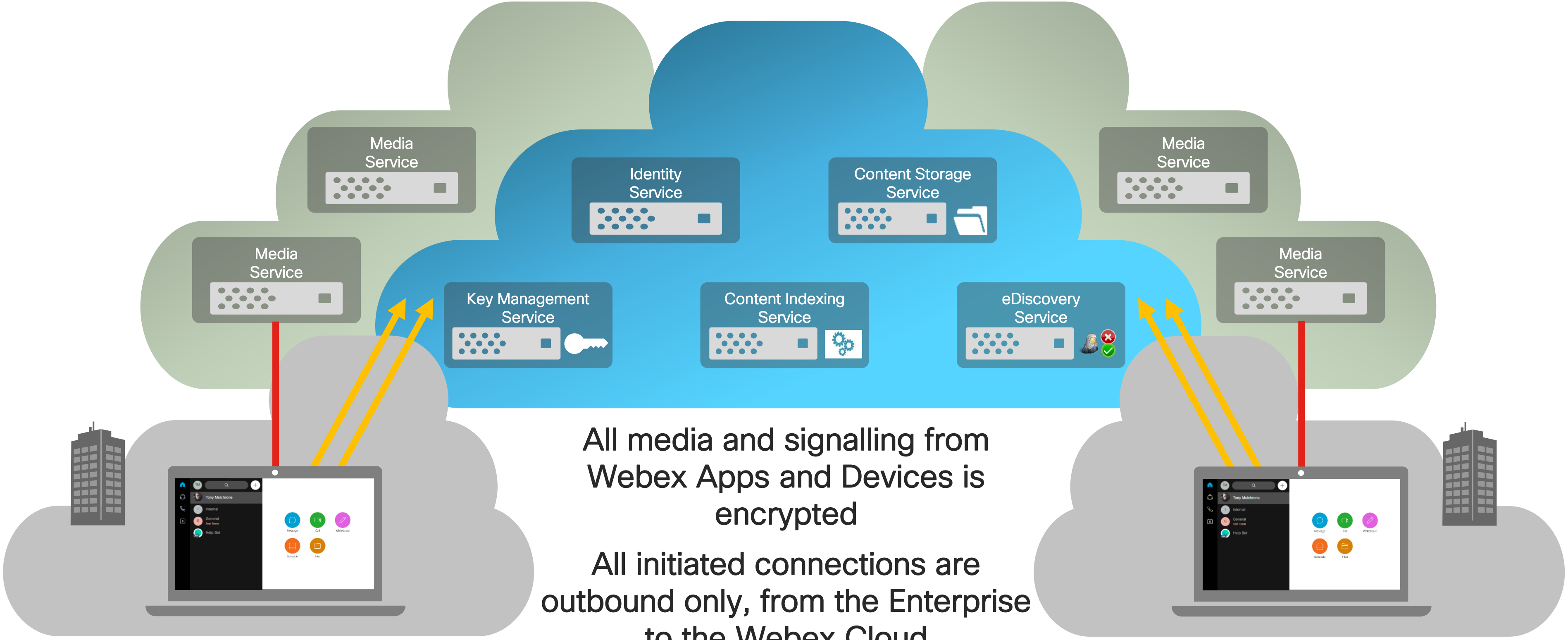
Webex Teams Apps cache content and Keys :
Communication in existing spaces is unaffected when HDS is unavailable



Webex Cloud Security

Connecting Media :
Voice, Video & Content Sharing

Connecting to Webex Teams Services



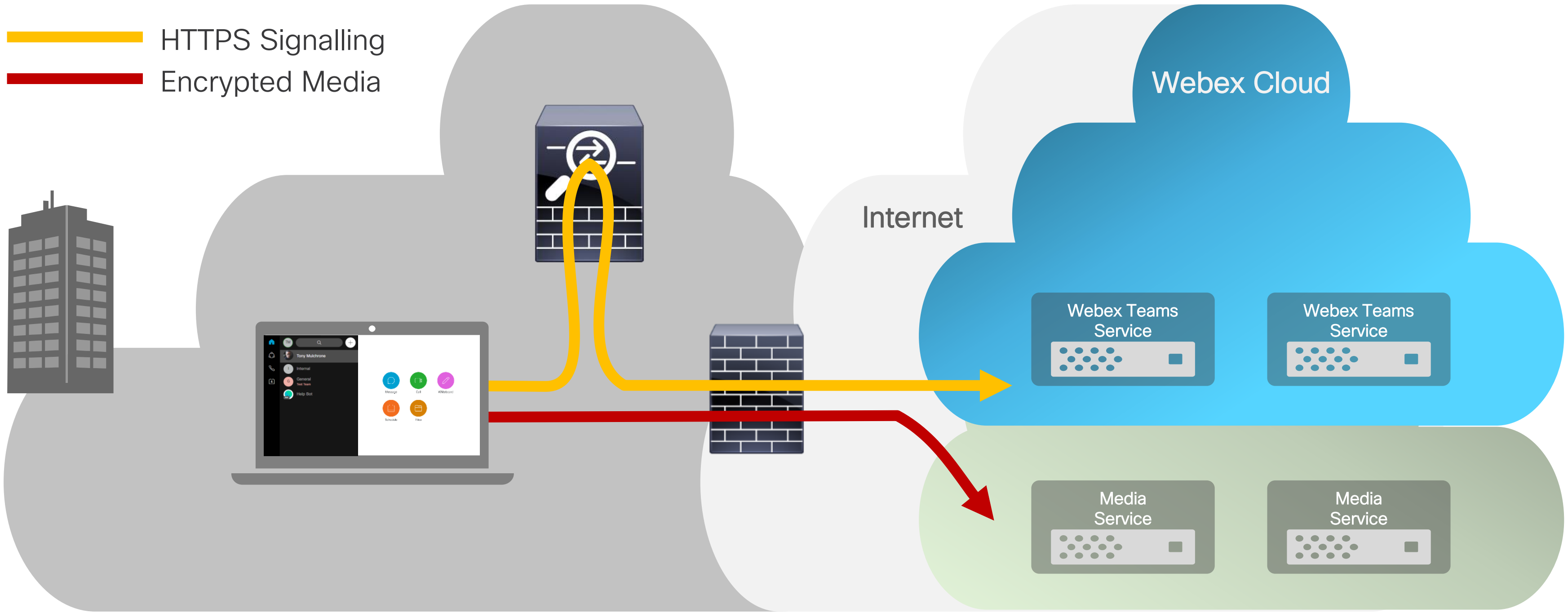
All media and signalling from Webex Apps and Devices is encrypted

All initiated connections are outbound only, from the Enterprise to the Webex Cloud

SRTP Encrypted Media : AES_CM_128_HMAC_SHA1_80

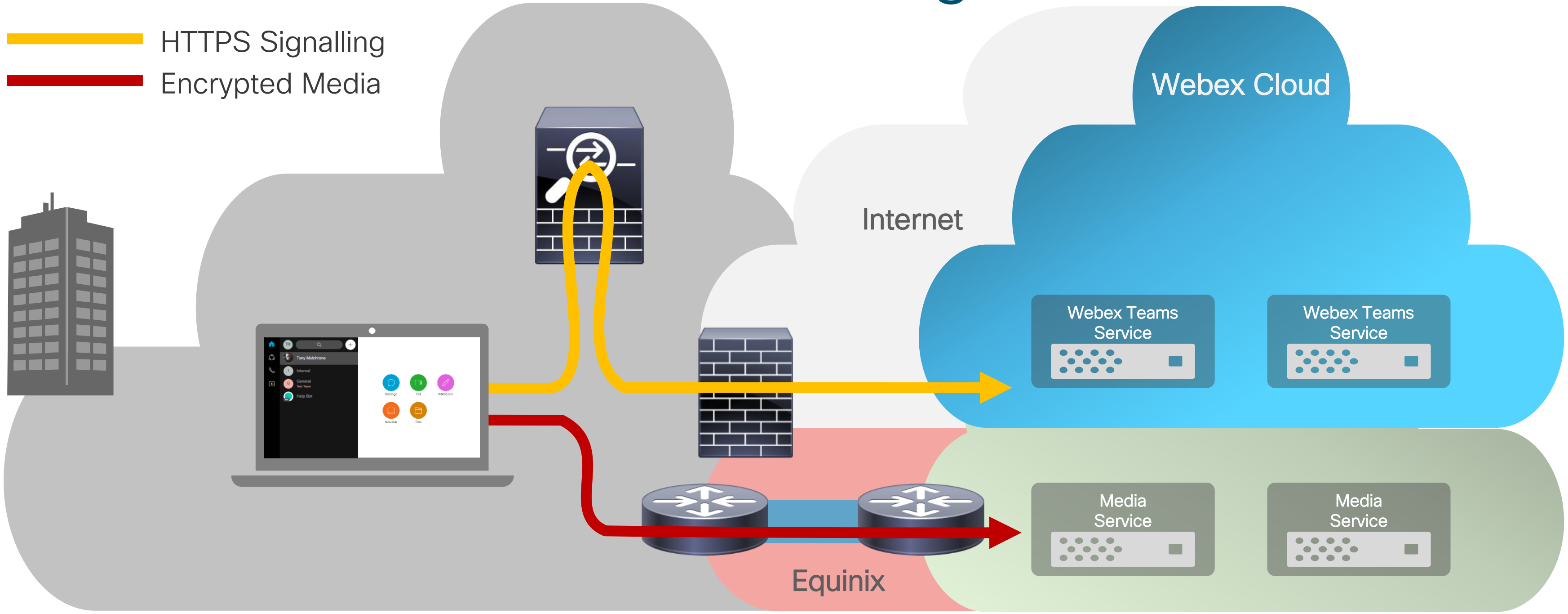
TLS 1.2 Encrypted Signalling : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Connecting to Webex from the Enterprise - Internet



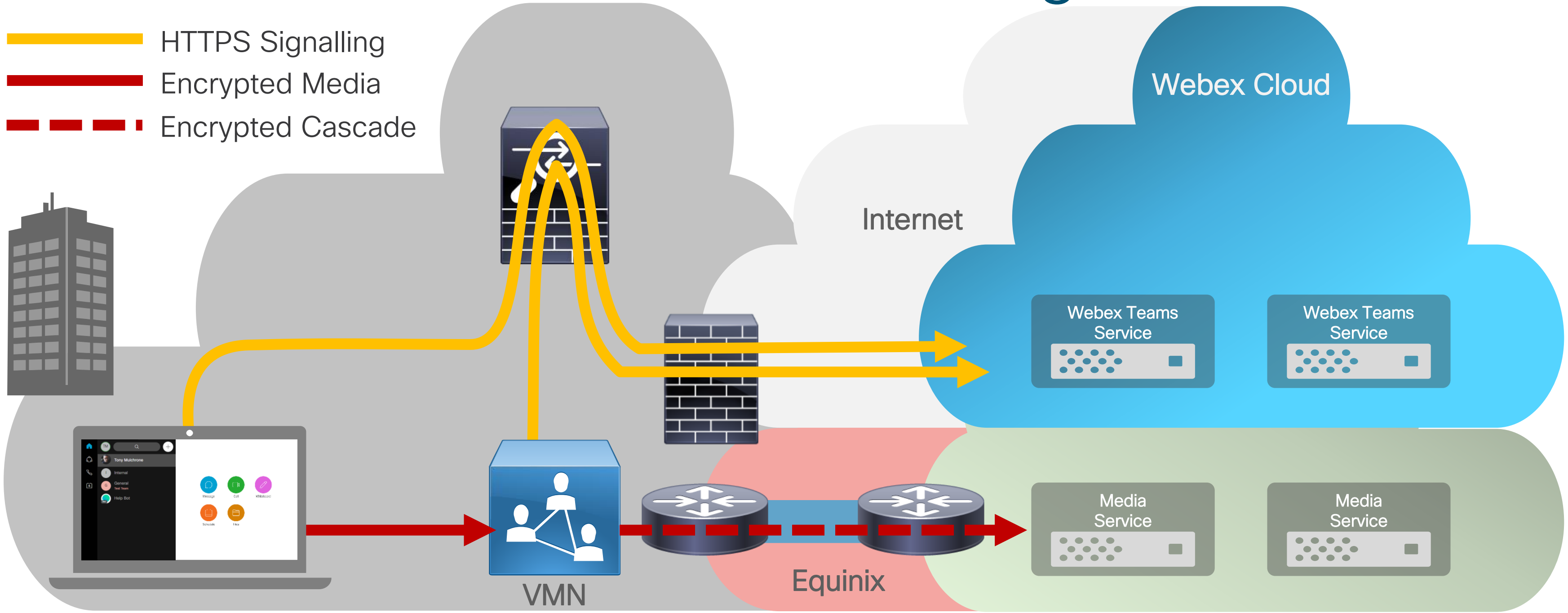
Encrypted HTTPS Signalling and Media traverse the internet to reach the Webex Cloud

Connecting to Webex from the Enterprise – Webex Teams with Webex Edge Connect



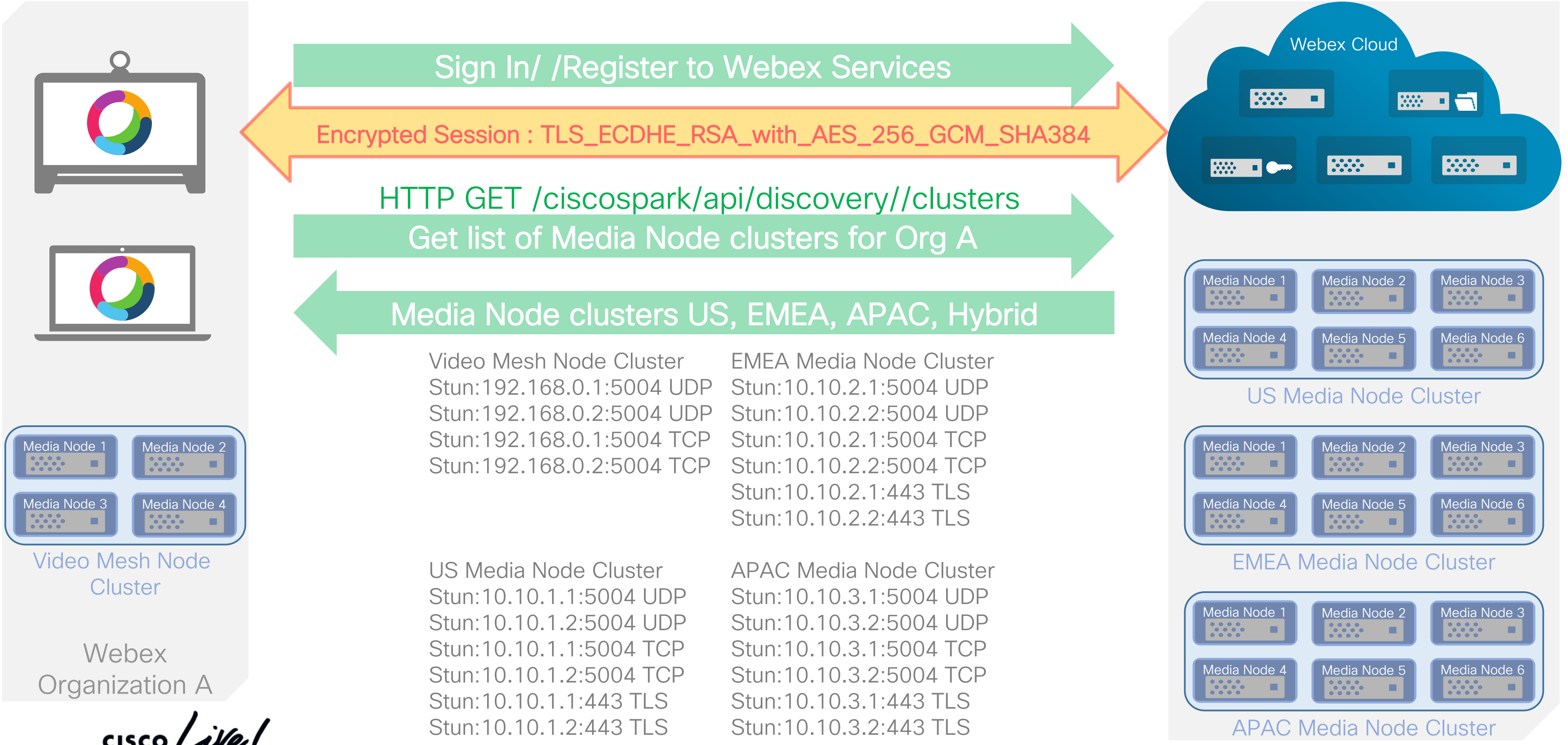
Encrypted HTTPS signalling traverses the internet to reach the Webex Cloud
Encrypted media traverses a dedicated private link via the Equinix SP cloud to reach Webex Media Services

Webex Teams with UC Calling – Call Flows with Video Mesh Node with Webex Edge Connect



Encrypted HTTPS signalling from Teams App and VMN traverses the internet to reach the Webex Cloud
Encrypted media from Teams App to Video Mesh Node
For external participants - Encrypted media cascade traverses the Equinix link to reach Webex Media Services

Webex Apps and Devices : Media Node Discovery



Sign In/ /Register to Webex Services

Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384

HTTP GET /ciscospark/api/discovery//clusters

Get list of Media Node clusters for Org A

Media Node clusters US, EMEA, APAC, Hybrid

Video Mesh Node Cluster
Stun:192.168.0.1:5004 UDP
Stun:192.168.0.2:5004 UDP
Stun:192.168.0.1:5004 TCP
Stun:192.168.0.2:5004 TCP

EMEA Media Node Cluster
Stun:10.10.2.1:5004 UDP
Stun:10.10.2.2:5004 UDP
Stun:10.10.2.1:5004 TCP
Stun:10.10.2.2:5004 TCP
Stun:10.10.2.1:443 TLS
Stun:10.10.2.2:443 TLS

US Media Node Cluster
Stun:10.10.1.1:5004 UDP
Stun:10.10.1.2:5004 UDP
Stun:10.10.1.1:5004 TCP
Stun:10.10.1.2:5004 TCP
Stun:10.10.1.1:443 TLS
Stun:10.10.1.2:443 TLS

APAC Media Node Cluster
Stun:10.10.3.1:5004 UDP
Stun:10.10.3.2:5004 UDP
Stun:10.10.3.1:5004 TCP
Stun:10.10.3.2:5004 TCP
Stun:10.10.3.1:443 TLS
Stun:10.10.3.2:443 TLS

Media Node 1, Media Node 2, Media Node 3, Media Node 4

Video Mesh Node Cluster

Webex Organization A

Webex Cloud

Media Node 1, Media Node 2, Media Node 3, Media Node 4, Media Node 5, Media Node 6

US Media Node Cluster

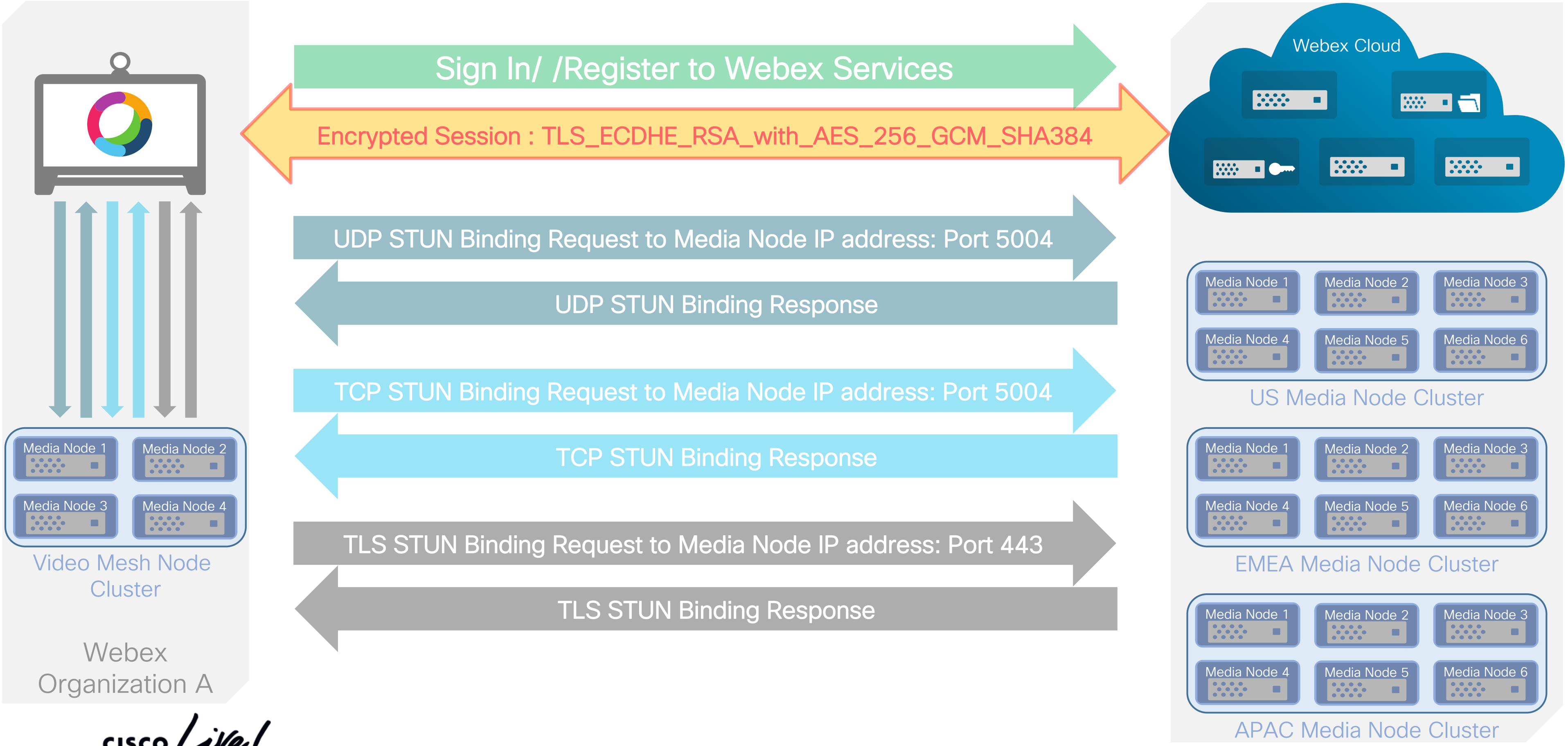
Media Node 1, Media Node 2, Media Node 3, Media Node 4, Media Node 5, Media Node 6

EMEA Media Node Cluster

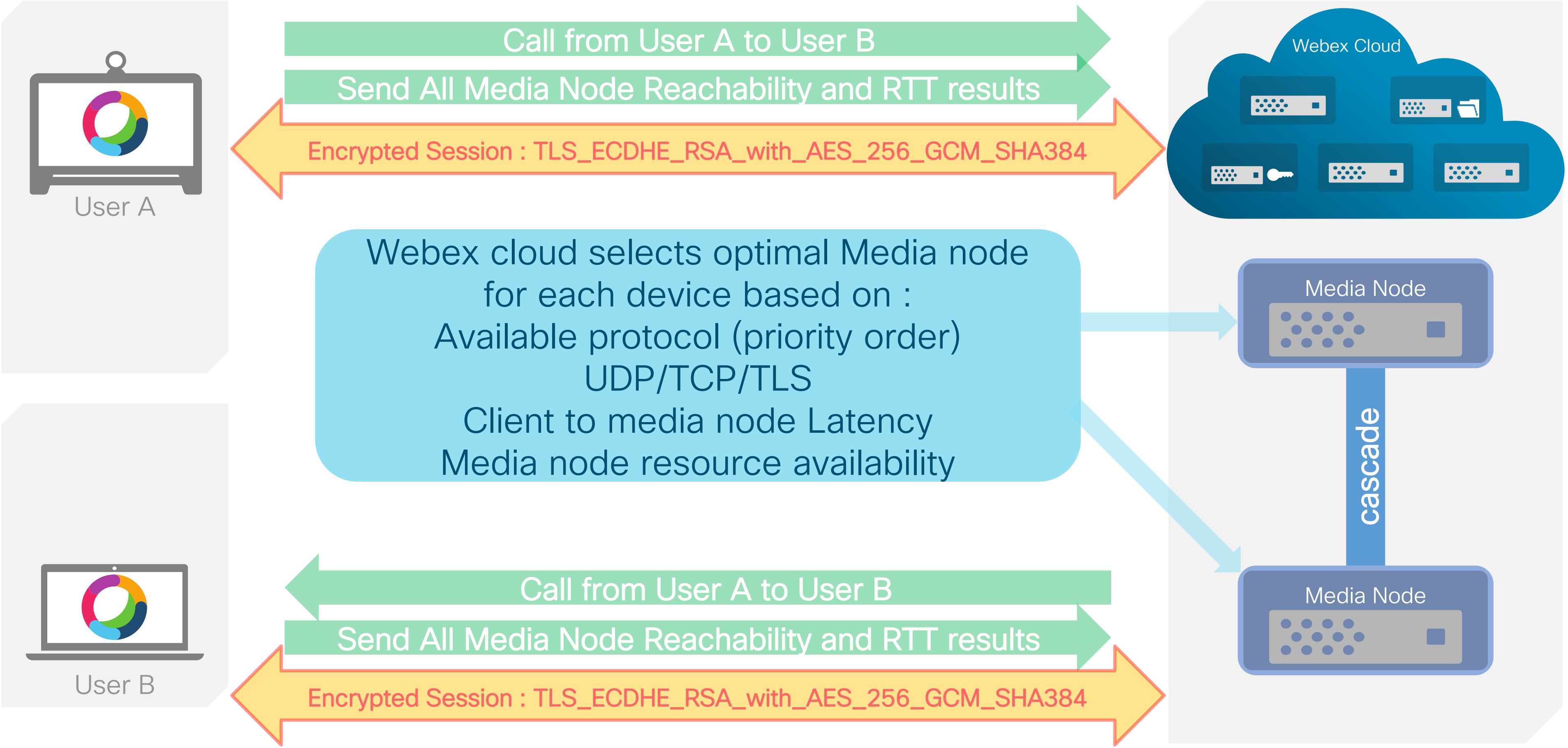
Media Node 1, Media Node 2, Media Node 3, Media Node 4, Media Node 5, Media Node 6

APAC Media Node Cluster

Webex Apps and Devices : Media Node Reachability



Call Set Up (1) – Send media node reachability info

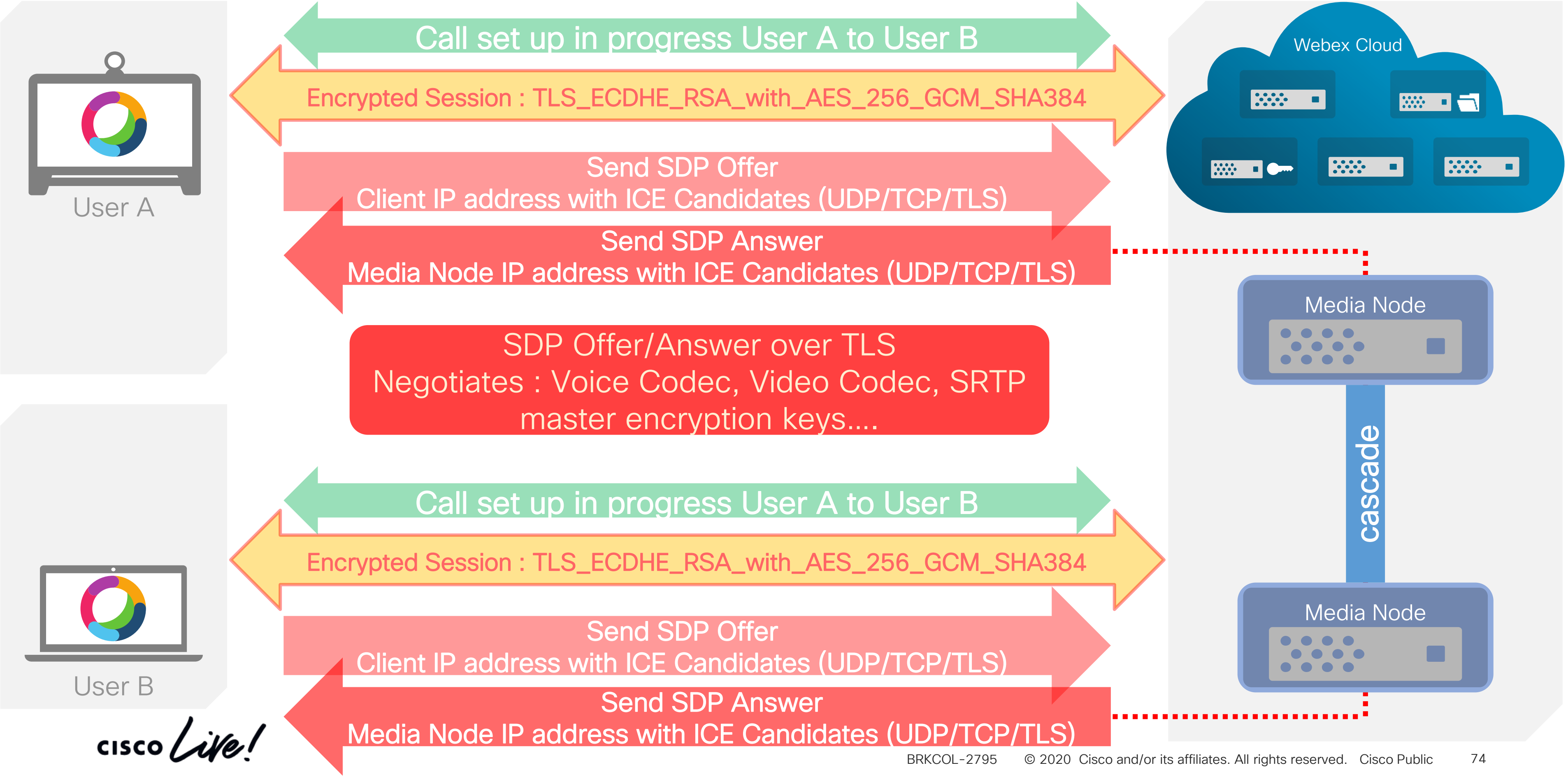


User A
Call from User A to User B
Send All Media Node Reachability and RTT results
Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
Webex Cloud

Webex cloud selects optimal Media node for each device based on :
Available protocol (priority order)
UDP/TCP/TLS
Client to media node Latency
Media node resource availability

Media Node
cascade
Media Node
User B
Call from User A to User B
Send All Media Node Reachability and RTT results
Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384

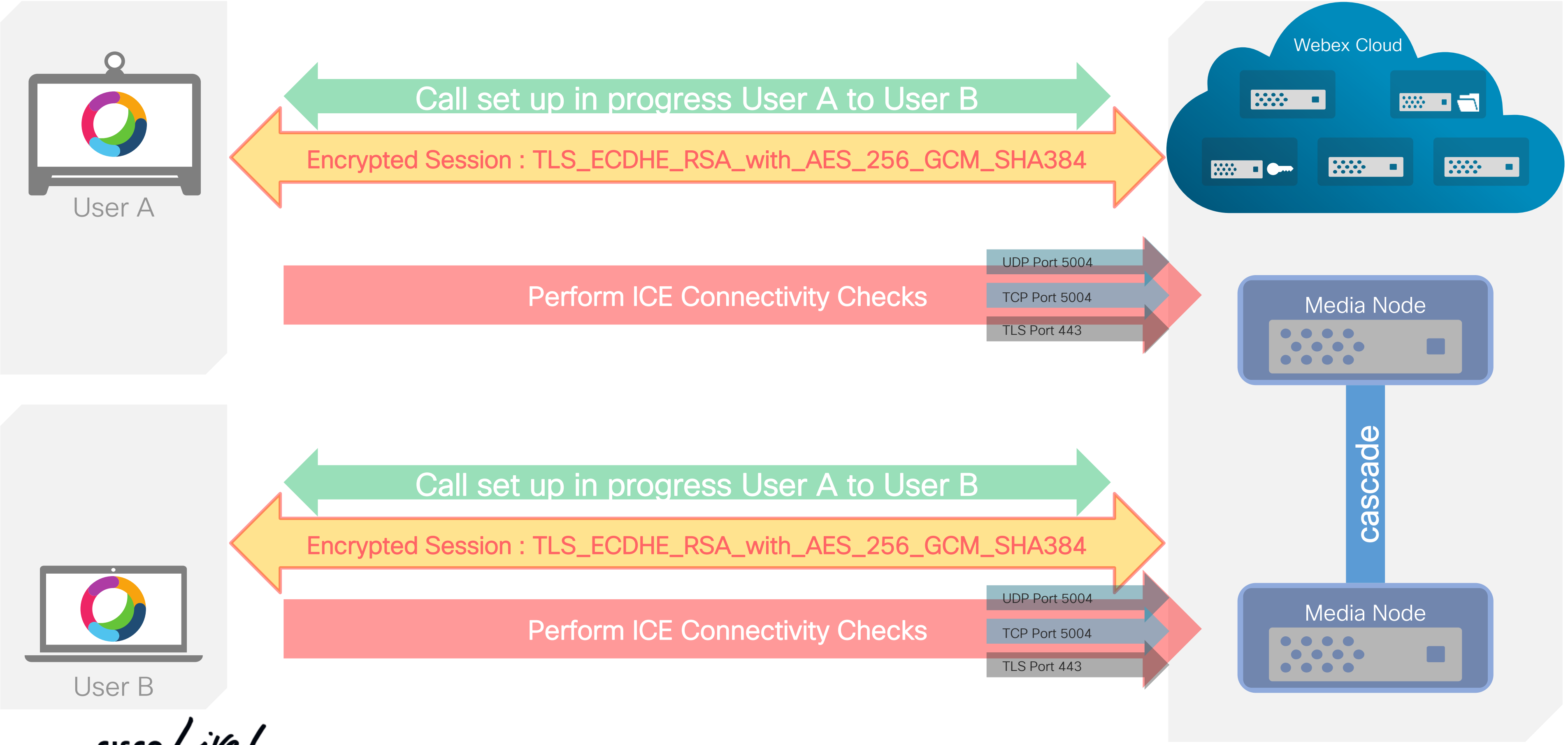
Call Set Up (2) – SDP Offer/Answer exchange



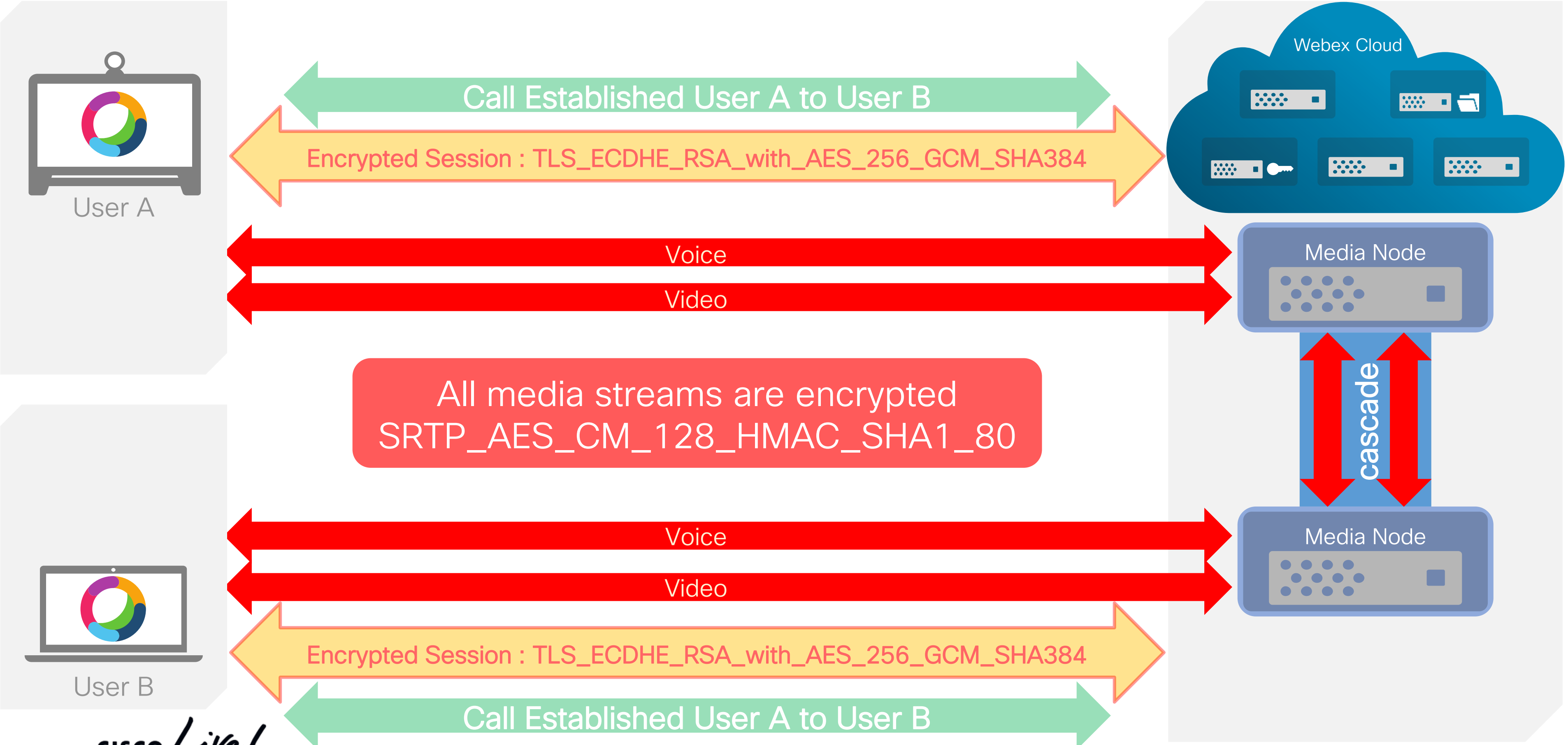
User A
Call set up in progress User A to User B
Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
Send SDP Offer
Client IP address with ICE Candidates (UDP/TCP/TLS)
Send SDP Answer
Media Node IP address with ICE Candidates (UDP/TCP/TLS)
Webex Cloud
Media Node
cascade
Media Node
User B
Call set up in progress User A to User B
Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
Send SDP Offer
Client IP address with ICE Candidates (UDP/TCP/TLS)
Send SDP Answer
Media Node IP address with ICE Candidates (UDP/TCP/TLS)

SDP Offer/Answer over TLS
Negotiates : Voice Codec, Video Codec, SRTP master encryption keys....

Call Set Up (3) – ICE Connectivity checks


User A
Call set up in progress User A to User B
Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
Webex Cloud
Perform ICE Connectivity Checks
UDP Port 5004
TCP Port 5004
TLS Port 443
Media Node
cascade
User B
Call set up in progress User A to User B
Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
Perform ICE Connectivity Checks
UDP Port 5004
TCP Port 5004
TLS Port 443
Media Node

Call Set Up (4) – Media Connect



Webex Cloud

User A

Call Established User A to User B

Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384

Voice

Video

Media Node

cascade

All media streams are encrypted
SRTP_AES_CM_128_HMAC_SHA1_80

Media Node

Voice

Video

Encrypted Session : TLS_ECDHE_RSA_with_AES_256_GCM_SHA384

Call Established User A to User B

User B

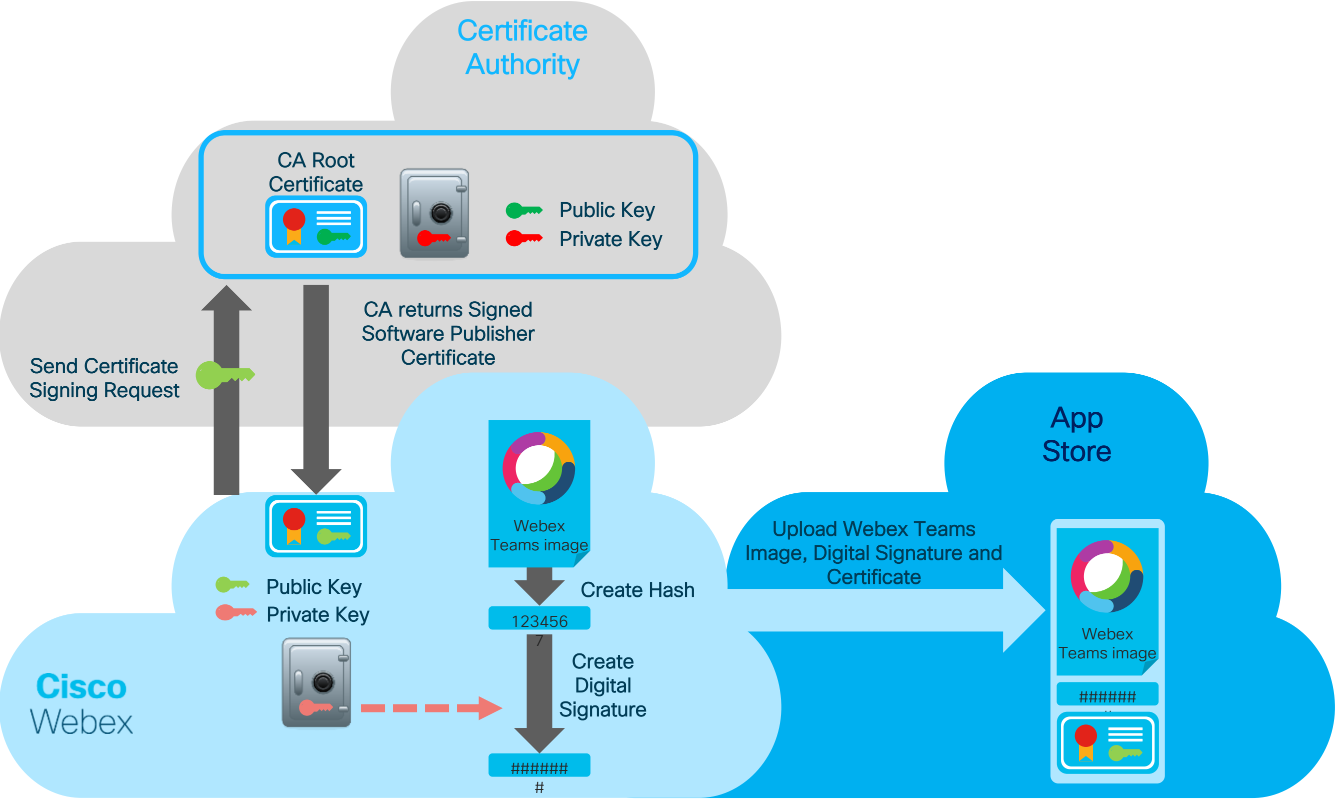
Webex Teams App Security

Software verification
Encryption of data at Rest
Proximity
Cognitive Collaboration

Webex Teams Apps – Co-signed software images

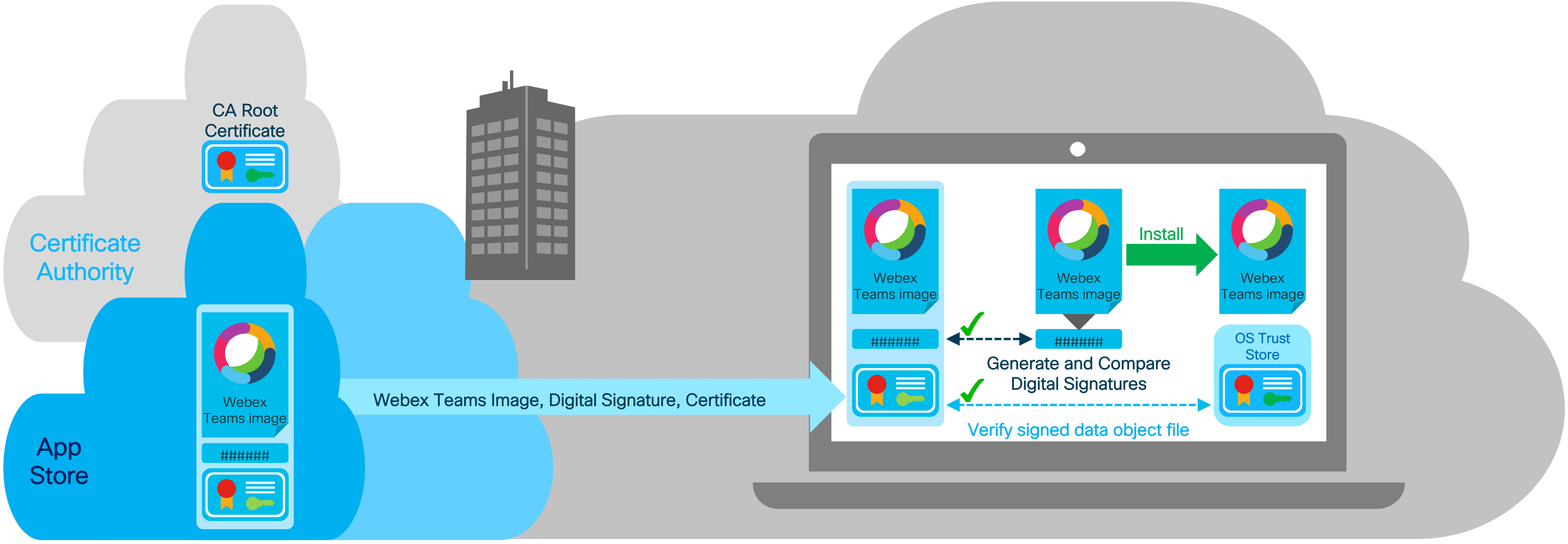
Cisco uses a CA-signed software publishing certificate to digitally sign the software image.

And then uses the code-signing infrastructure of each platform vendor (Microsoft/Apple/Google) to co-sign a PKCS #7-signed data object file containing the signed Webex Teams image, digital signature, and software publishing certificate.



Webex Teams App: Software image verification

When a user downloads the Webex Teams software image, the platform operating system verifies the digital signature PKCS #7-signed data object file ands then verifies the digital signature of the Webex Teams image



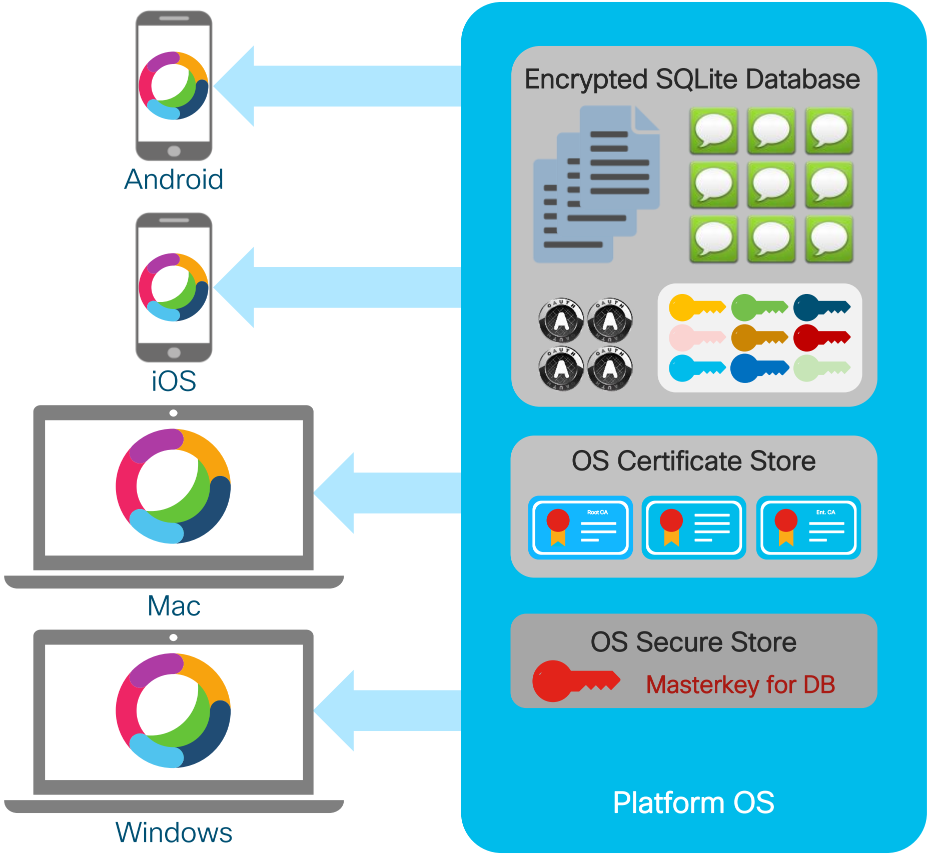
Webex Teams Apps : Encryption of Data at Rest

What data is cached and encrypted :

Space details and Encryption Keys
Meeting details and Encryption Keys
Whiteboard details and Encryption Keys
Messages
Transcoded Files
(Downloaded File location: user selected)
OAuth Tokens

Stored Data encrypted using :
AES-256-OFB
Windows, Mac, iOS, Android
(Teams Web App does not store data)
Master Key stored in OS secure Store

Data Wipe capability for mobile Apps

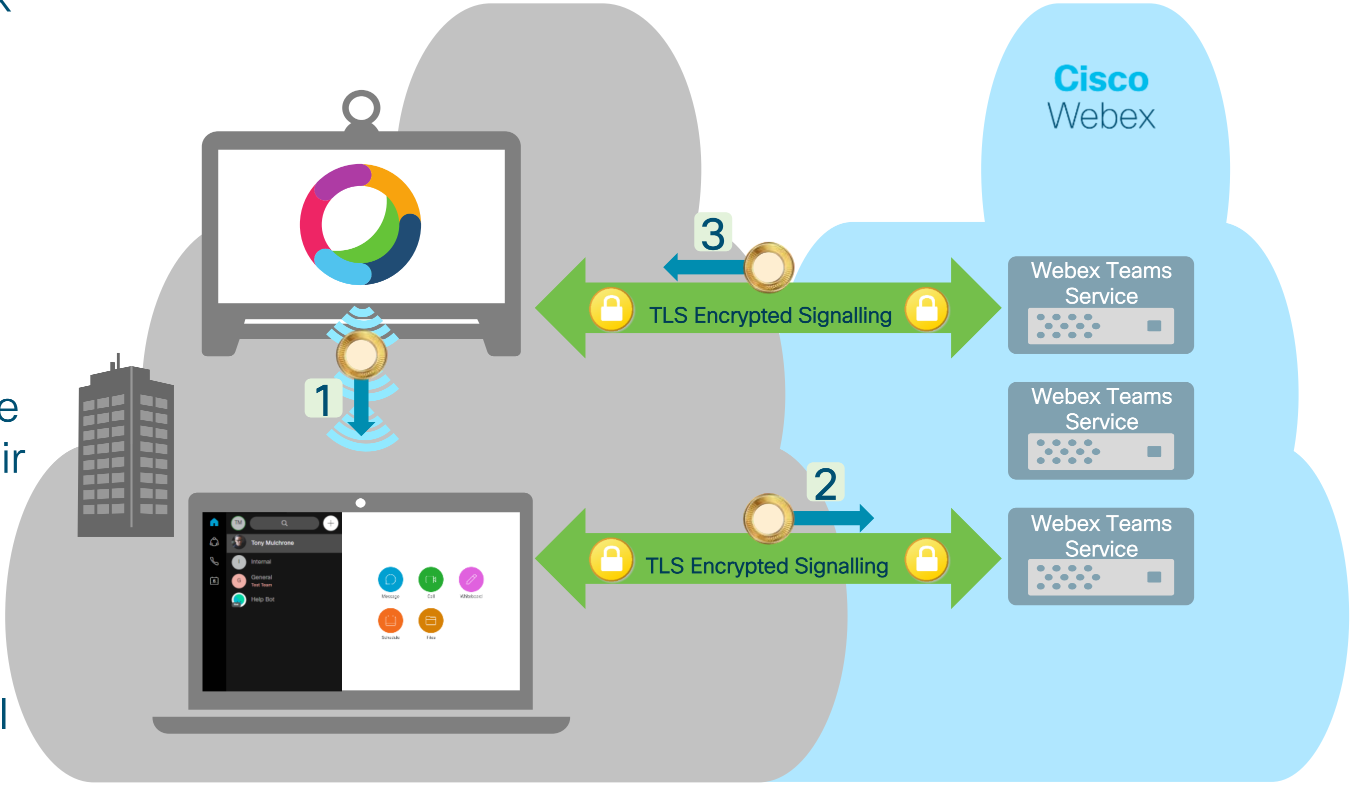


Webex Teams App and devices Proximity – Device detection and pairing

Cloud-registered Webex devices use ultrasonic signalling and tokens to discover* and pair with Webex Teams apps

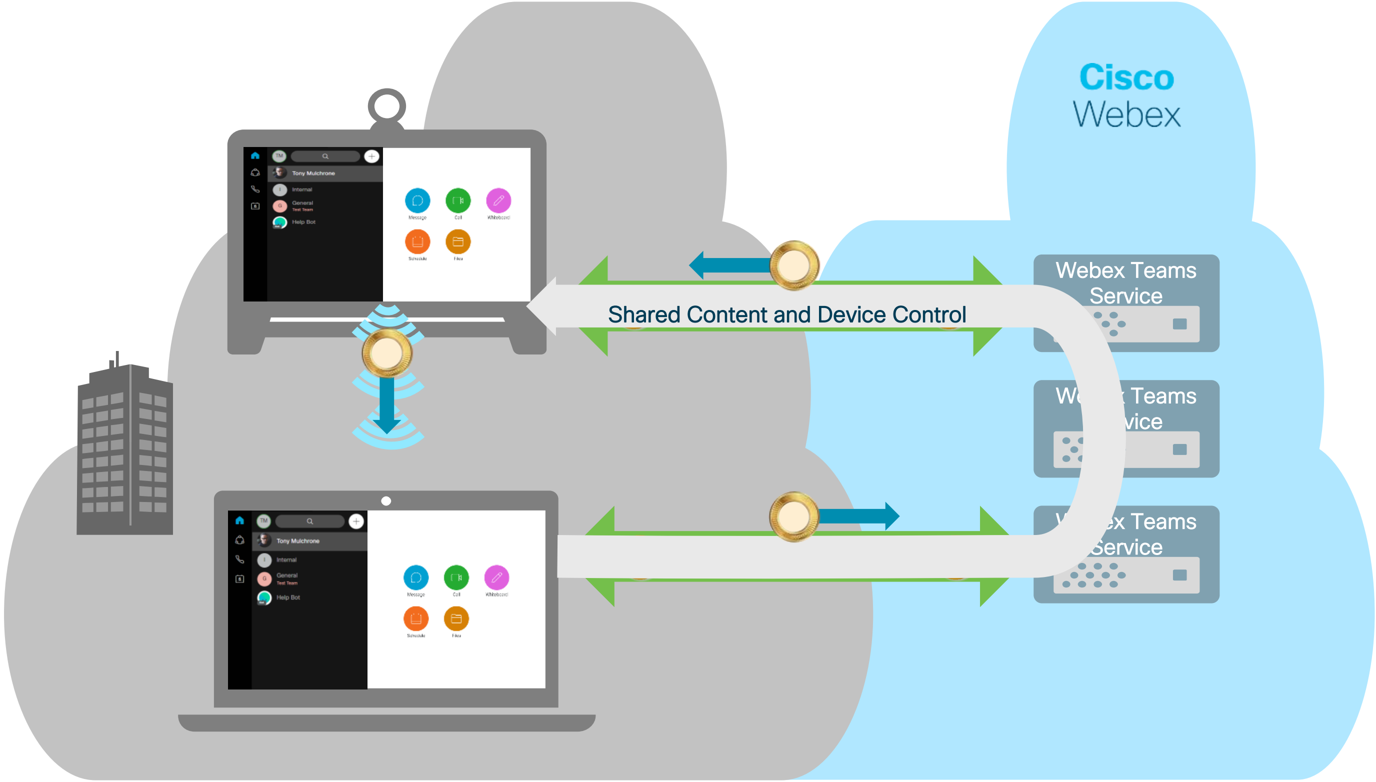
A Webex Teams app within range of the ultrasound signal can use the received token to pair with Webex device, by sending the token to the Webex cloud service.

* WiFi discovery optional



Webex Teams Apps and Devices – Content sharing and device control

Once the paired via the Webex cloud, the Webex Teams app can control the Webex device, for example to make calls, mute etc, and also share content on the Webex device. Both the app and device use their existing TLS connections to the Webex cloud, to exchange call control signalling and media for content sharing.

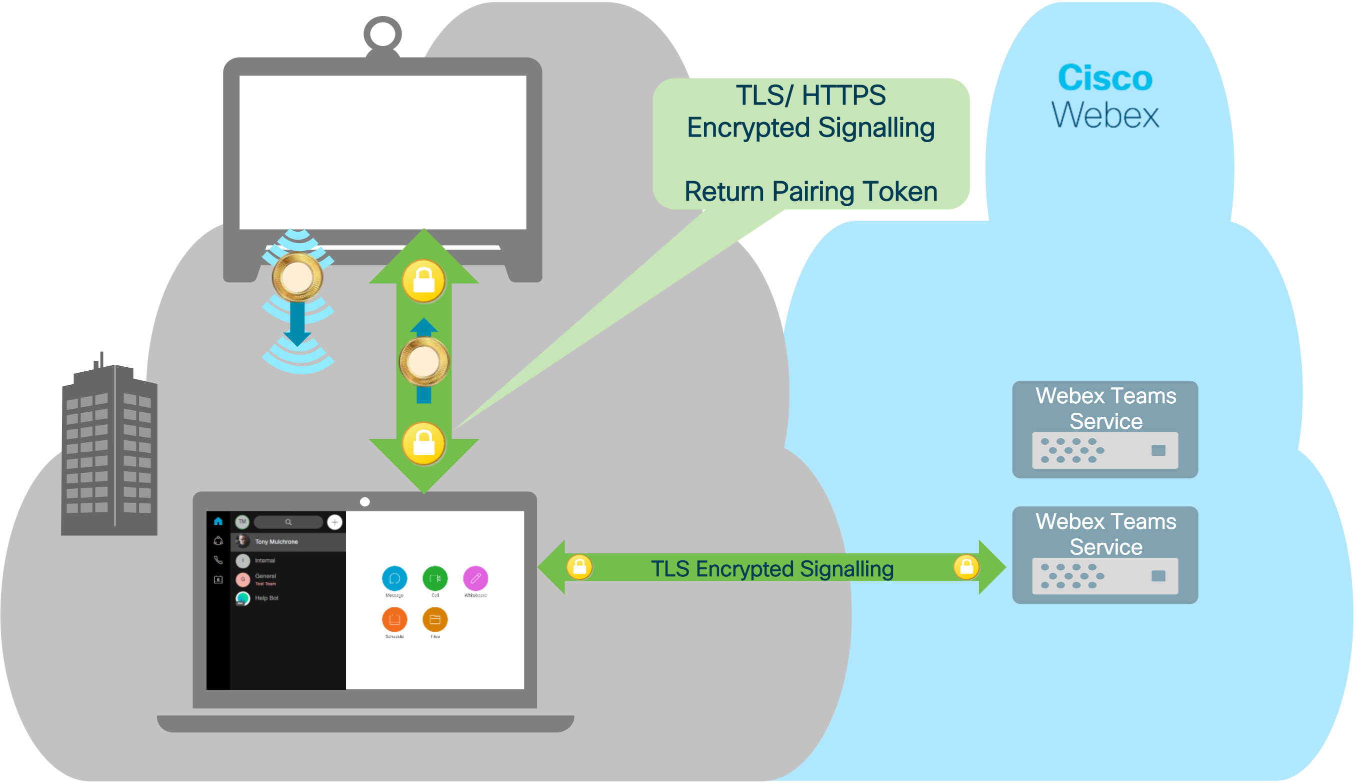


Webex Teams App and On Premises devices Proximity – Device detection and pairing

Unified CM registered video devices also use ultrasonic signalling for discovery* and tokens for proximity pairing with Webex Teams apps.

The Webex Teams app and video device use a directly established HTTPS connection to exchange call control signalling and media for content sharing.

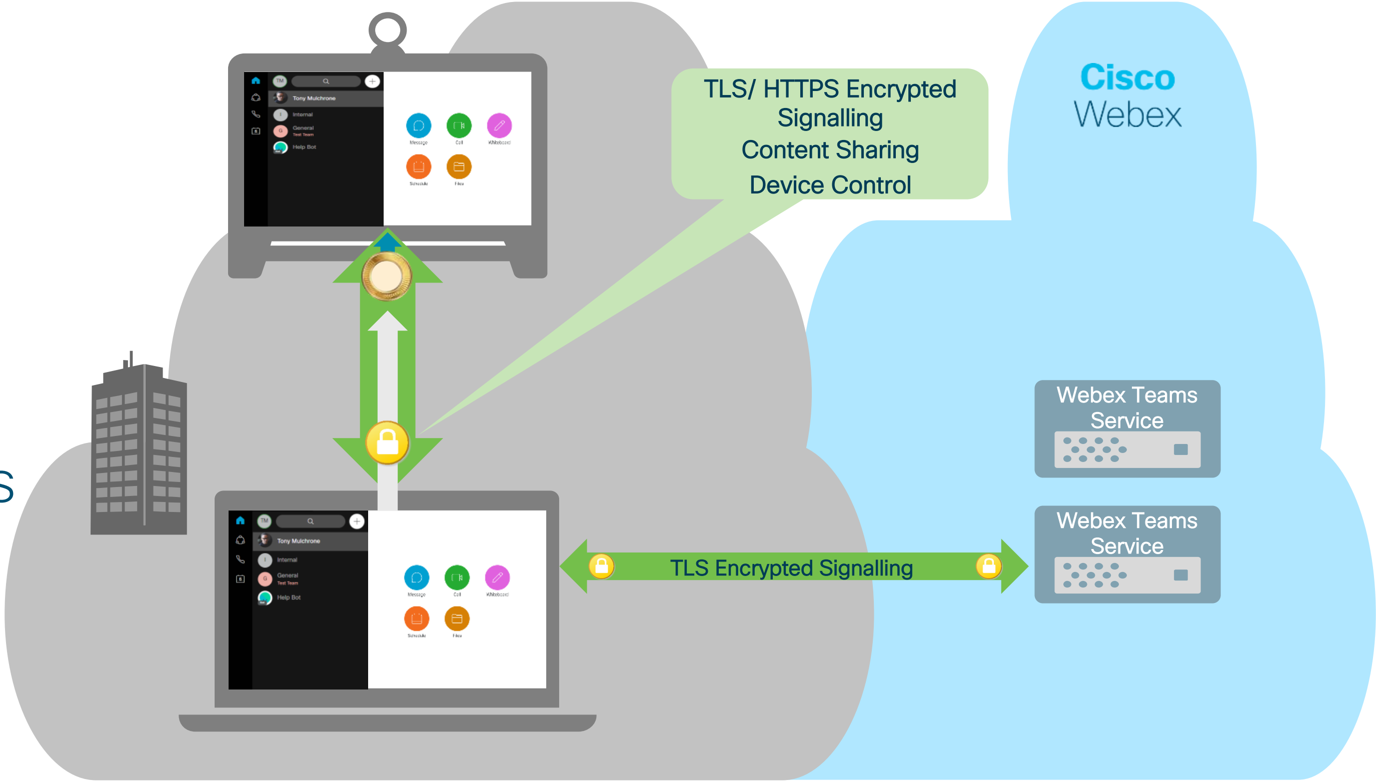
* WiFi discovery optional



Webex Teams Apps and On Premises Devices – Content sharing and device control

When connecting to an on-premises device, the content shared between the Webex Teams app and device is always encrypted (HTTPS).

However, we don't enforce certificate verification for the HTTPS session, as this would prevent pairing with guest devices and would be complex to deploy and maintain.



Defining Cognitive Collaboration

AI and machine learning in collaborative environments

Audio & Speech Technologies

Noise Detection

Speech Integration

Meeting Transcription

Multi-modal Bots & Assistants

Collaboration Assistants

Care Assistants

Computer Vision

Face, Gesture and Object Recognition

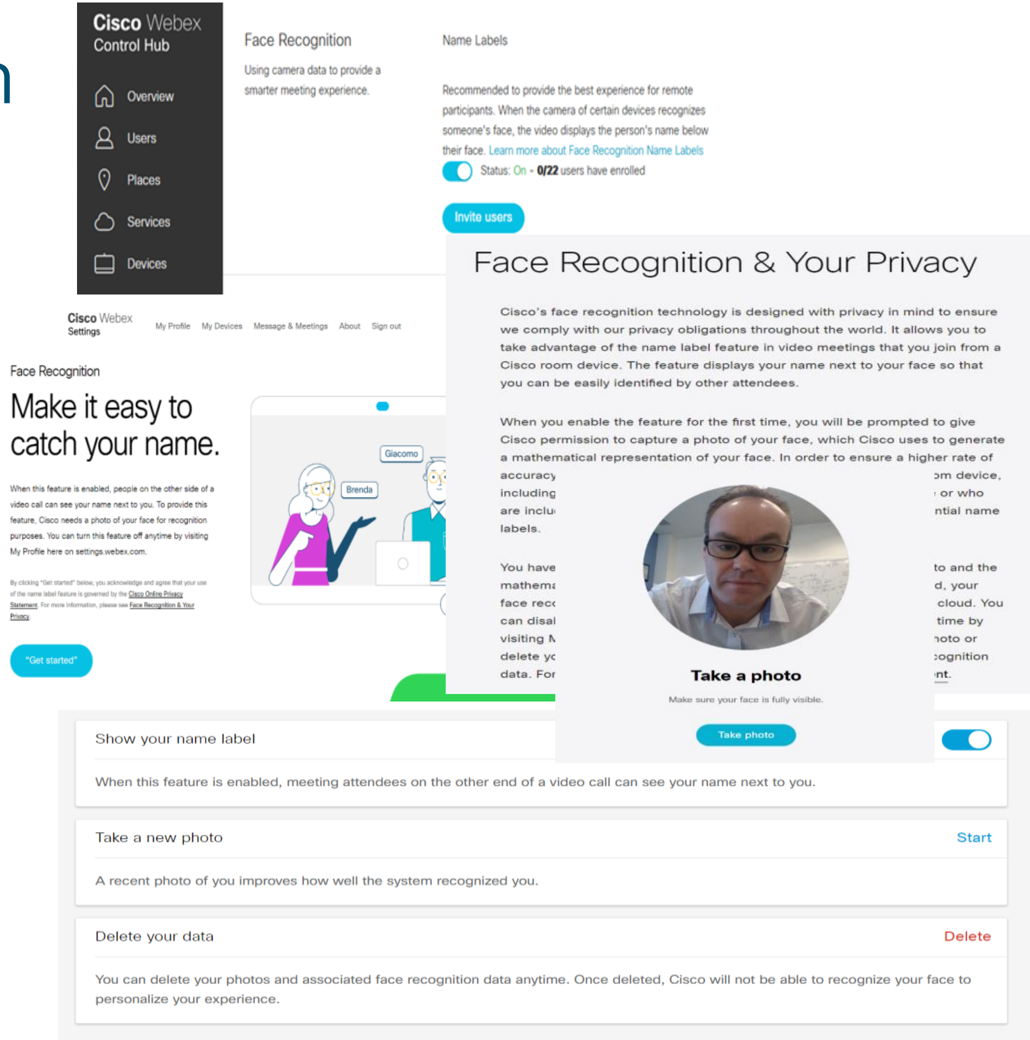
Relationship Intelligence

People Profiles

Company Information

Cognitive Collaboration Data Privacy Principles

- Machine Learning is based on data and algorithms
- Don’t retain data if you don’t have to
- If you do, keep it for the shortest possible time
- Be transparent about data usage
- Provide Deletion Controls
- Empower end users
- See Cognitive Data Privacy Session



Cisco Webex Control Hub

Face Recognition

Using camera data to provide a smarter meeting experience.

Name Labels

Recommended to provide the best experience for remote participants. When the camera of certain devices recognizes someone's face, the video displays the person's name below their face. Learn more about Face Recognition Name Labels

Status: On • 0/22 users have enrolled

Cisco Webex Settings

Face Recognition

Make it easy to catch your name.

When this feature is enabled, people on the other side of a video call can see your name next to you. To provide this feature, Cisco needs a photo of your face for recognition purposes. You can turn this feature off anytime by visiting My Profile here on settings.webex.com.

By clicking "Get started" below, you acknowledge and agree that your use of the name label feature is governed by the Cisco Online Privacy Statement. For more information, please see Face Recognition & Your Privacy.

Face Recognition & Your Privacy

Cisco's face recognition technology is designed with privacy in mind to ensure we comply with our privacy obligations throughout the world. It allows you to take advantage of the name label feature in video meetings that you join from a Cisco room device. The feature displays your name next to your face so that you can be easily identified by other attendees.

When you enable the feature for the first time, you will be prompted to give Cisco permission to capture a photo of your face, which Cisco uses to generate a mathematical representation of your face. In order to ensure a higher rate of
accuracy om device,
including or who
are inclu ntial name
labels.

You have to and the
mathema d, your
face reco cloud. You
can disal time by
visiting M hoto or
delete yo cognition
data. For nt.

Take a photo

Make sure your face is fully visible.

Show your name label

When this feature is enabled, meeting attendees on the other end of a video call can see your name next to you.

Take a new photo — Start

A recent photo of you improves how well the system recognized you.

Delete your data — Delete

You can delete your photos and associated face recognition data anytime. Once deleted, Cisco will not be able to recognize your face to personalize your experience.

Webex Cloud Access :

Enterprise Proxies and Firewalls

Network Requirements

Webex Cloud Access : Enterprise Proxy and Firewall Network Requirements

Webex Teams Network Requirements doc :

https://collaborationhelp.cisco.com/article/en-us/WBX00002

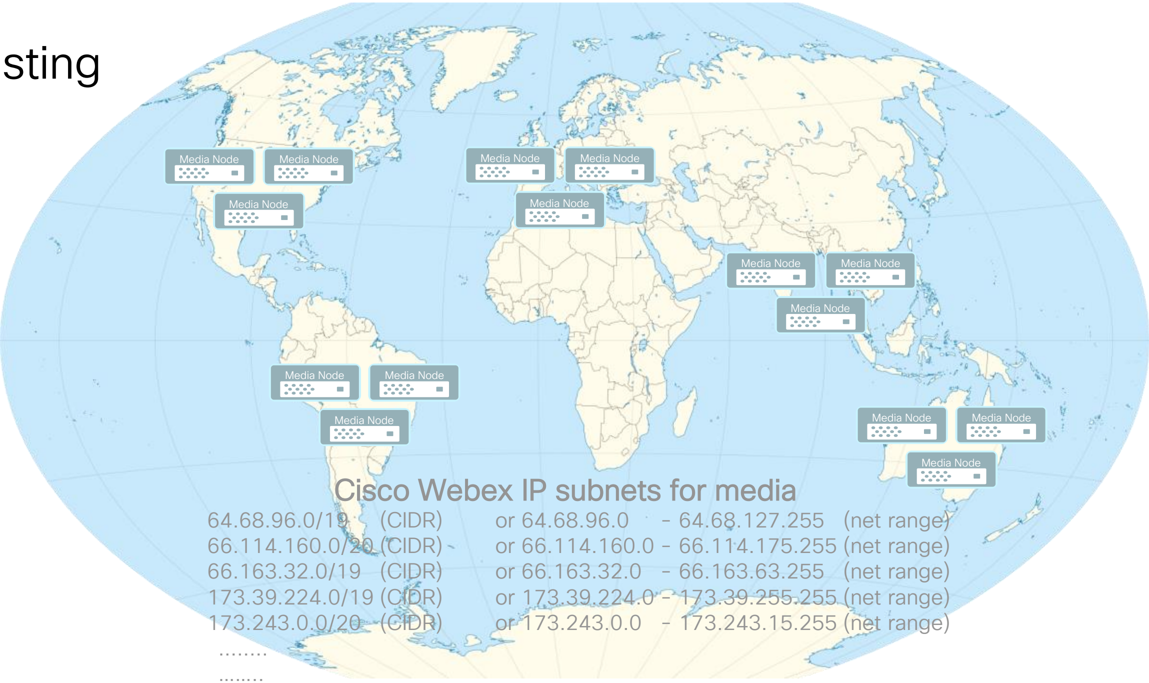
Subscribe To This Article

Destination URLs for domain whitelisting

e.g. *.webex.com
*.ciscowebex.com
*.wbx2.com
*.ciscospark.com

Destination IP subnets for Media
Media protocol port numbers
Signalling protocol port numbers

Proxy feature support
802.1X feature support
Webex Hybrid Services



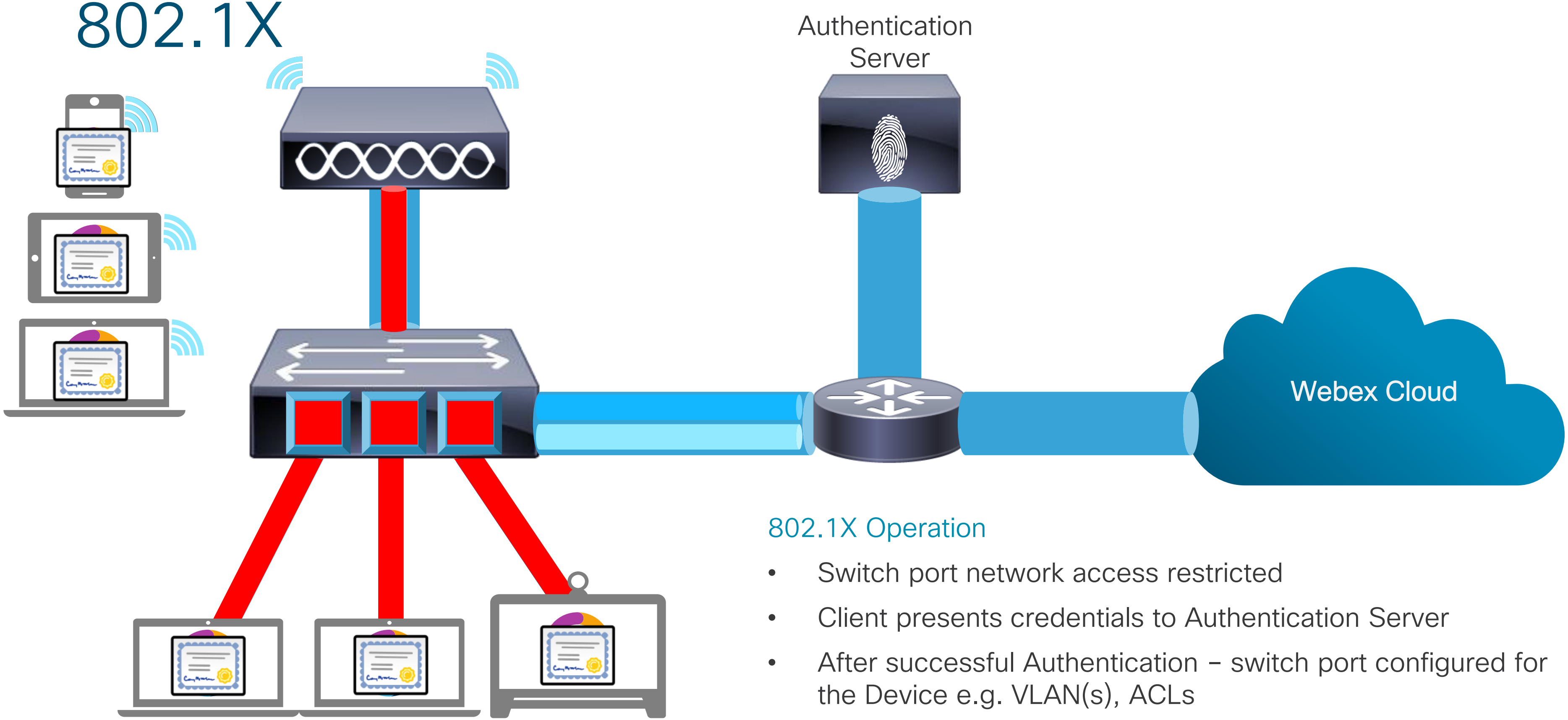
Cisco Webex IP subnets for media

64.68.96.0/19	(CIDR)	or 64.68.96.0 - 64.68.127.255	(net range)
66.114.160.0/20	(CIDR)	or 66.114.160.0 - 66.114.175.255	(net range)
66.163.32.0/19	(CIDR)	or 66.163.32.0 - 66.163.63.255	(net range)
173.39.224.0/19	(CIDR)	or 173.39.224.0 - 173.39.255.255	(net range)
173.243.0.0/20	(CIDR)	or 173.243.0.0 - 173.243.15.255	(net range)

....
....

Webex Cloud Access : Network Access Control 802.1X

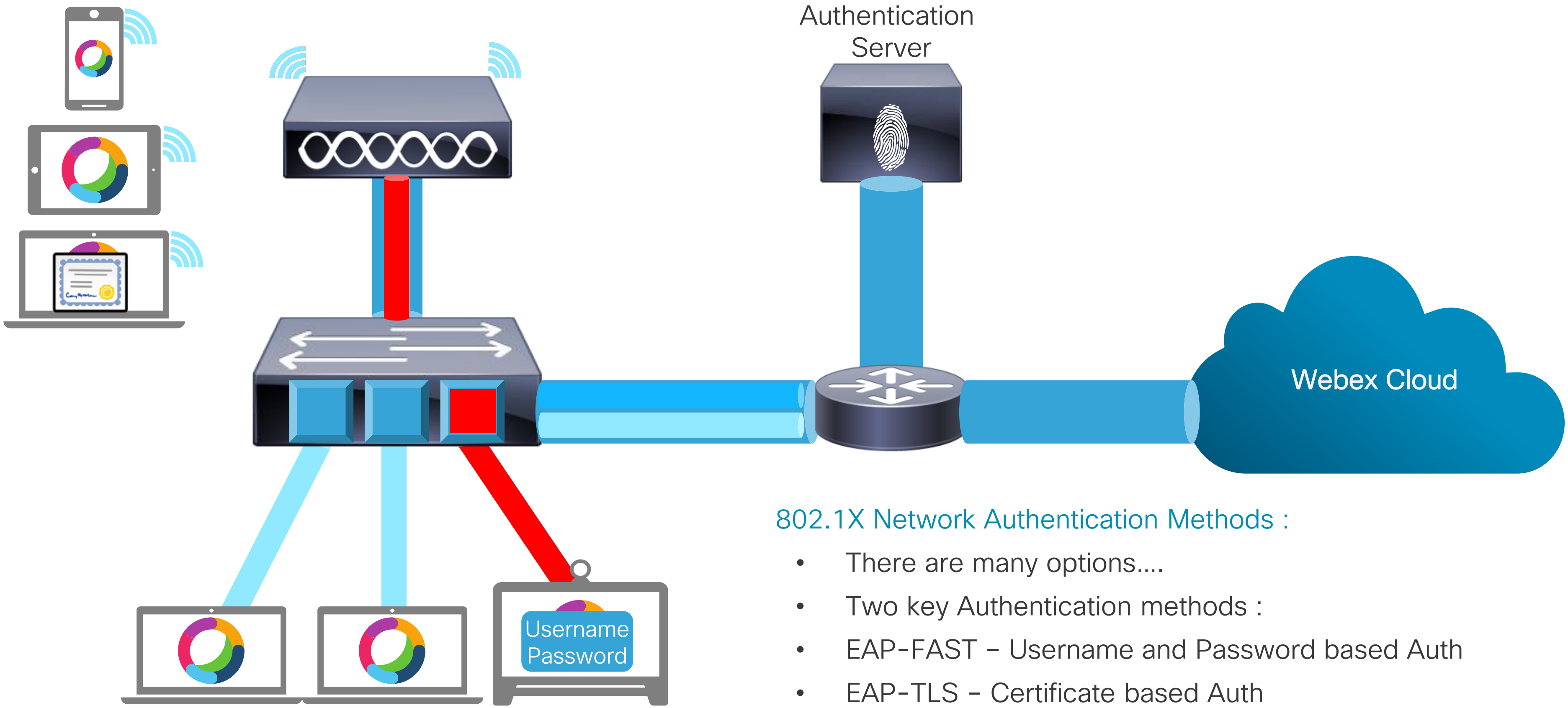
Connecting to Webex from the Enterprise – 802.1X



802.1X Operation

- Switch port network access restricted
- Client presents credentials to Authentication Server
- After successful Authentication – switch port configured for the Device e.g. VLAN(s), ACLs
- VLANs required internet access

802.1X Network Authentication Methods



802.1X Network Authentication Methods :

- There are many options….
- Two key Authentication methods :
- EAP-FAST – Username and Password based Auth
- EAP-TLS – Certificate based Auth

Webex Cloud Access :
Enterprise Firewalls

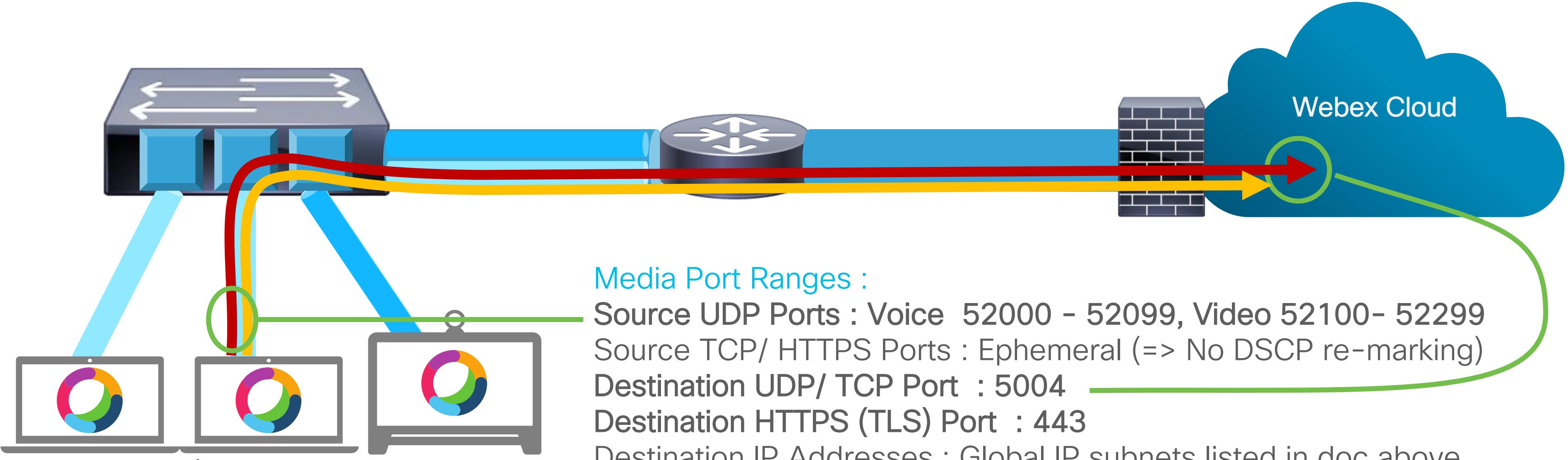
Connecting to Webex through Enterprise Firewalls : Webex Teams Apps and Devices

Firewalls : Whitelisting Ports and Destinations

🟨 Signalling
🟥 UDP Media

You will need to allow Webex Teams media and signalling traffic to pass through your Enterprise Firewall – For white listing details refer to :

Webex Teams Network Requirements doc : https://collaborationhelp.cisco.com/article/en-us/WBX000028782



Media Port Ranges :

Source UDP Ports : Voice 52000 – 52099, Video 52100– 52299

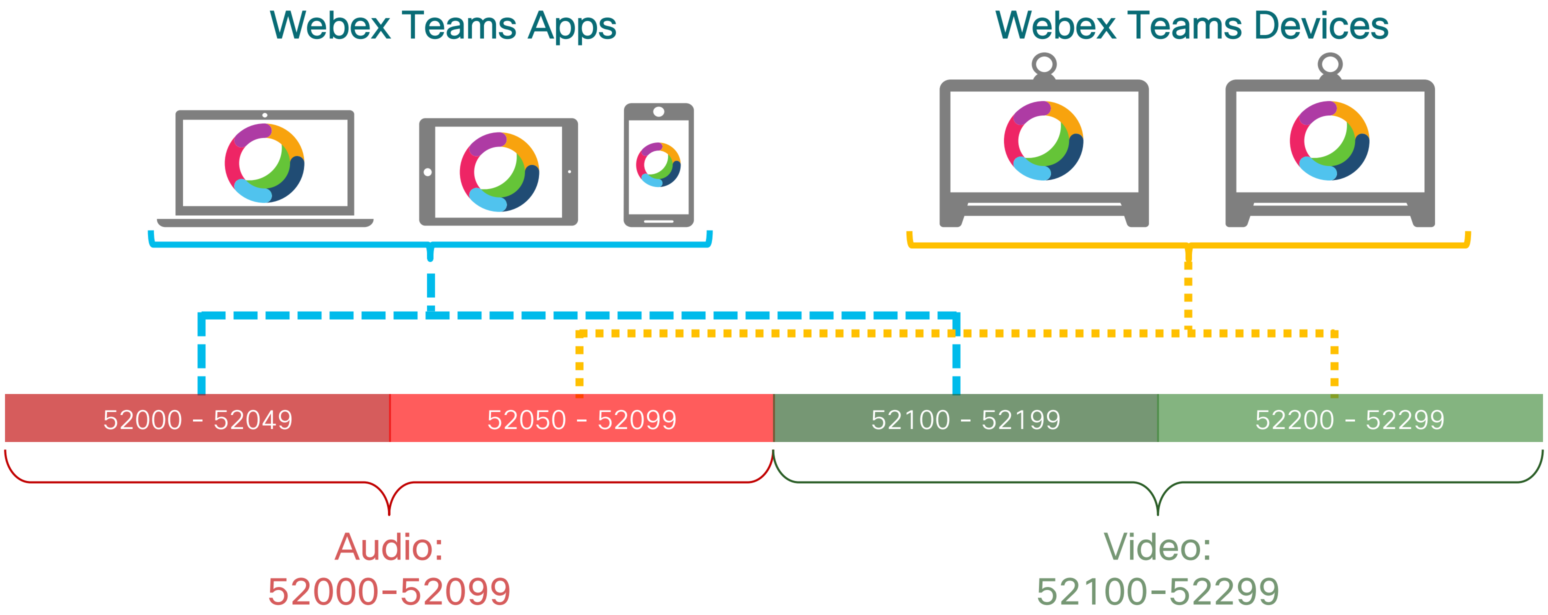
Source TCP/ HTTPS Ports : Ephemeral (=> No DSCP re-marking)

Destination UDP/ TCP Port : 5004

Destination HTTPS (TLS) Port : 443

Destination IP Addresses : Global IP subnets listed in doc above

Webex Teams Endpoint Media Source UDP Port Ranges for Apps and Devices



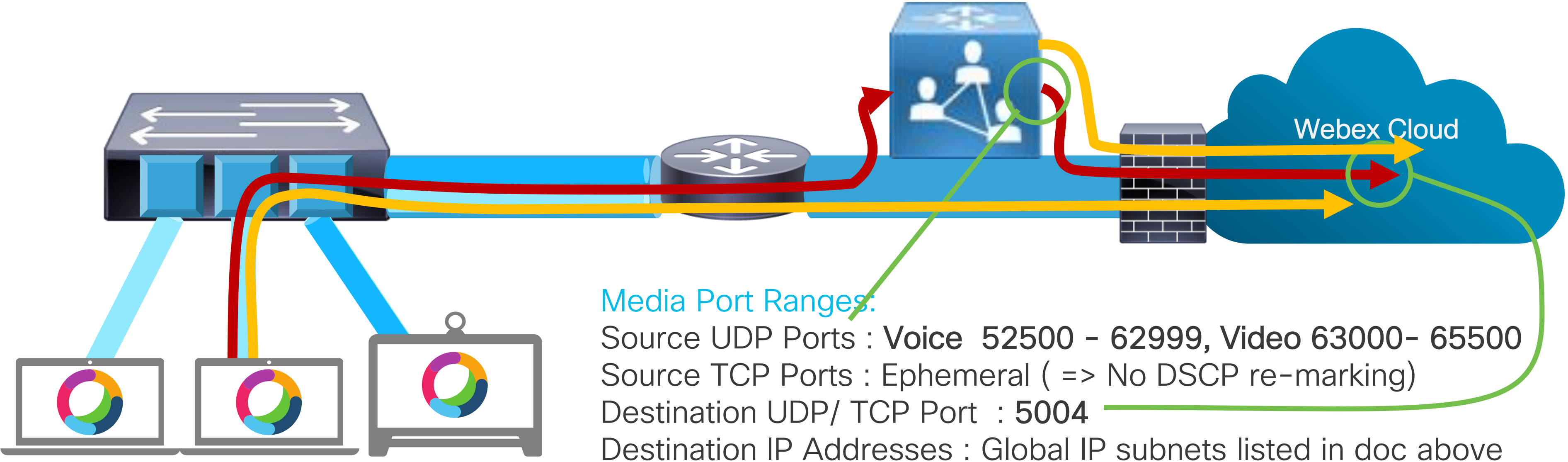
Connecting to Webex through Enterprise Firewalls : Cisco Webex Video Mesh

🟨 Signalling

🟥 UDP Media

Webex Video Mesh Node Source voice and video UDP ports are different to those used by endpoints – Used for cascade media links to the Webex Cloud

Webex Teams Network Requirements doc :
https://collaborationhelp.cisco.com/article/en-us/WBX000028782



Media Port Ranges:

Source UDP Ports : **Voice 52500 – 62999, Video 63000– 65500**

Source TCP Ports : Ephemeral (=> No DSCP re-marking)

Destination UDP/ TCP Port : **5004**

Destination IP Addresses : Global IP subnets listed in doc above

Webex Video Mesh Deployment Guide
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/mediaservice/deployment/cmgt_b_hybrid-media-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_0100.html

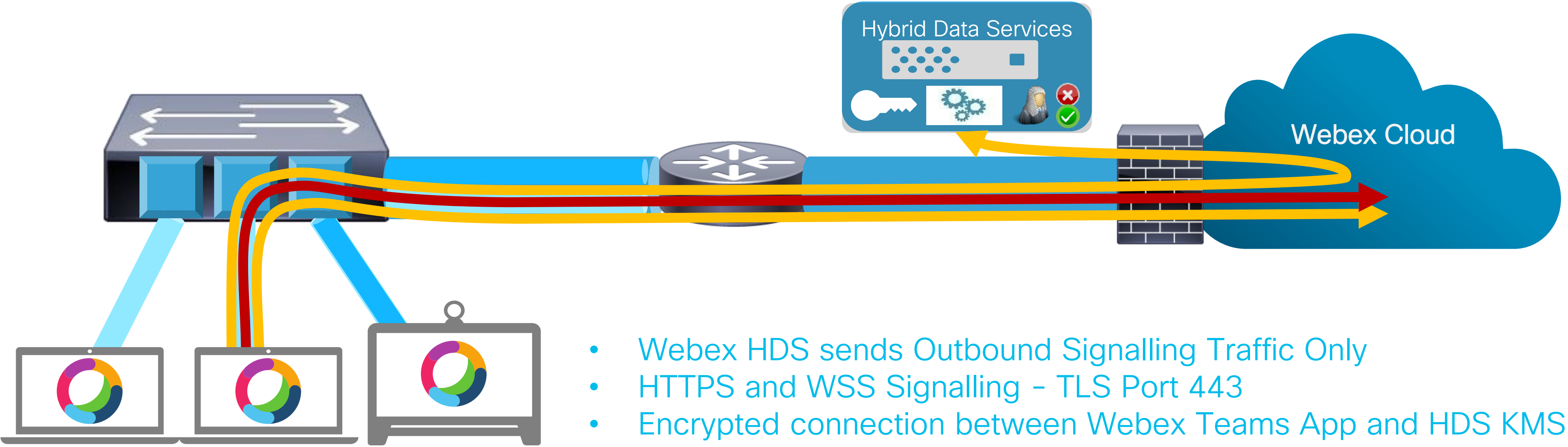
Connecting to Webex through Enterprise Firewalls: Cisco Webex Hybrid Data Security Node

🟨 Signalling

🟥 UDP Media

For Webex Hybrid Data Security Node network Requirements see :

Webex Teams Network Requirements doc :
https://collaborationhelp.cisco.com/article/en-us/WBX000028782



- Webex HDS sends Outbound Signalling Traffic Only
- HTTPS and WSS Signalling – TLS Port 443
- Encrypted connection between Webex Teams App and HDS KMS

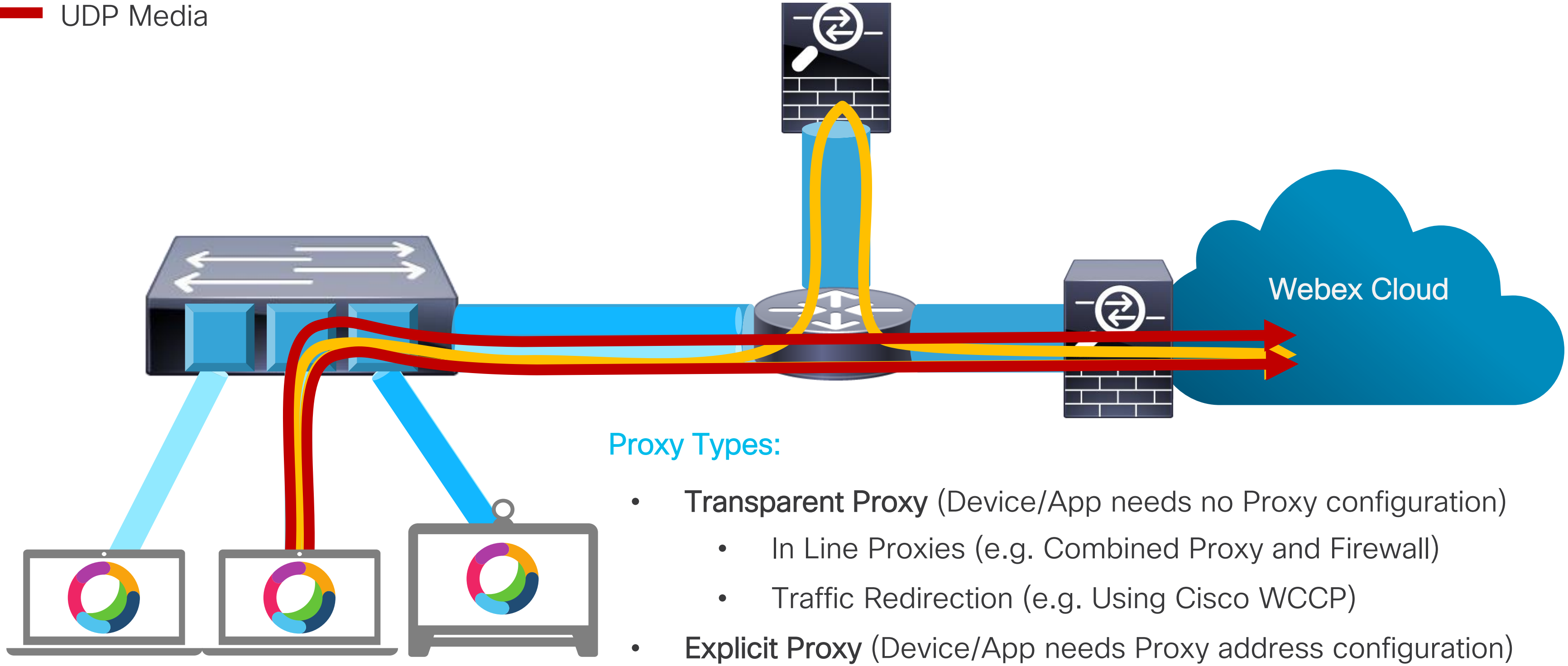
Webex Cloud Access :
Enterprise Proxies

Connecting to Webex - Enterprise Proxy Types

🟨 Signalling

🟥 UDP Media

HTTP/HTTPS traffic only sent to the Proxy server
e.g. Destination ports 80, 443, 8080, 8443

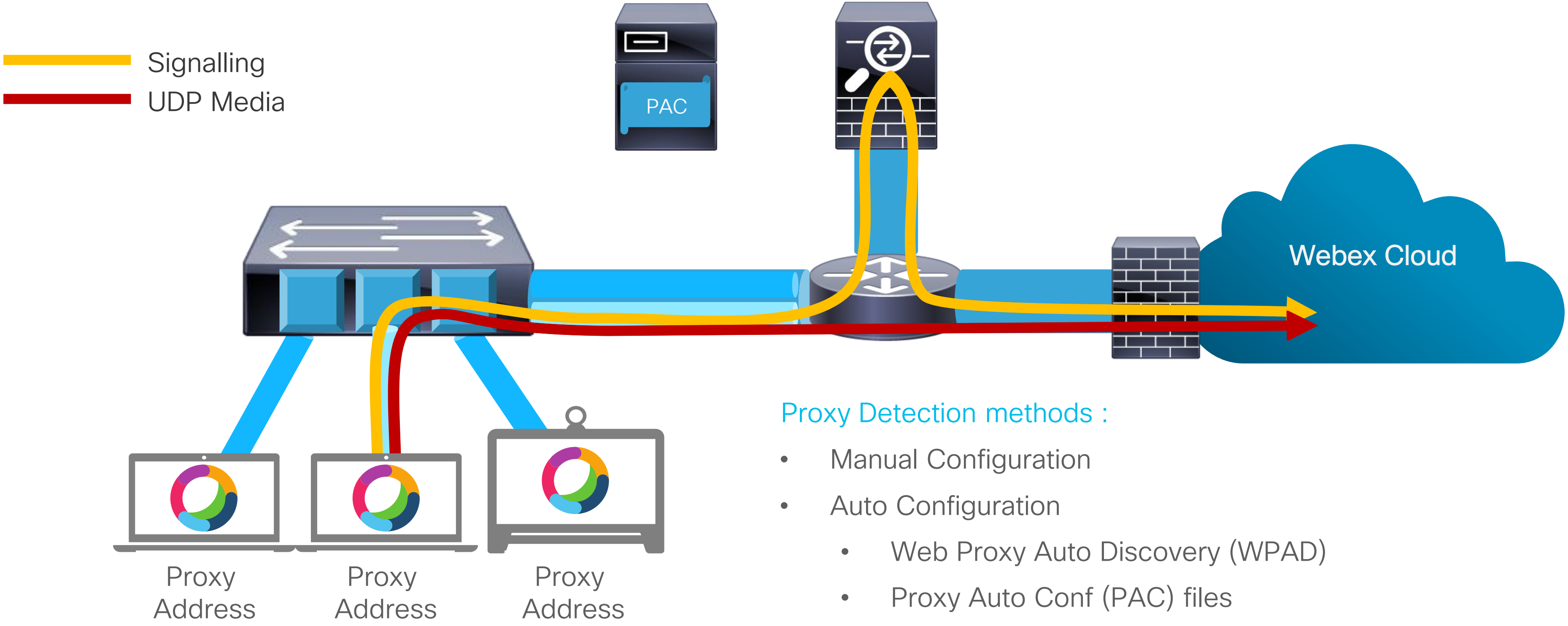


Proxy Types:

- **Transparent Proxy** (Device/App needs no Proxy configuration)
  - In Line Proxies (e.g. Combined Proxy and Firewall)
  - Traffic Redirection (e.g. Using Cisco WCCP)
- **Explicit Proxy** (Device/App needs Proxy address configuration)

Connecting to Webex - Enterprise Proxy Detection

Proxies can be configured manually via the platform OS or device UI, or automatically discovered using mechanisms such as Web Proxy Auto Discovery (WPAD) and/or Proxy Auto Config (PAC) files. See notes for details.



Proxy Detection methods :

- Manual Configuration
- Auto Configuration
  - Web Proxy Auto Discovery (WPAD)
  - Proxy Auto Conf (PAC) files

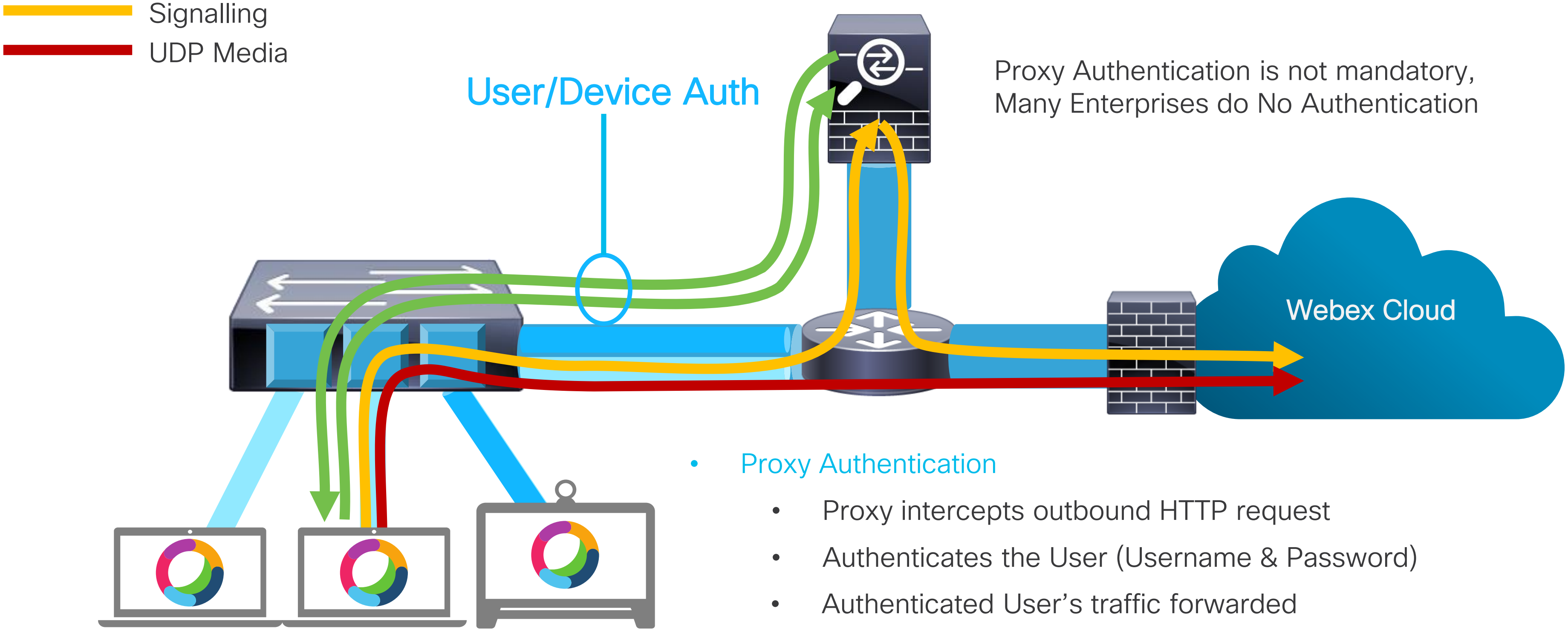
For Webex Teams App/Device Proxy support see doc : https://collaborationhelp.cisco.com/article/en-us/WBX000028782

Webex Teams : Device and App Proxy configuration

	Room OS	Webex Board	Windows	Mac	iOS	Android	HDS & VMN
Manual Configuration	✓	✓	✓	✓	✓	✓	✓
GPO	✗	✗	✓	✗	✗	✗	✗
PAC	✓	✓	✓	✓	✓	✓	✗
WPAD	✓	✓	✓	✓	✓	✗	✗

Refer to https://collaborationhelp.cisco.com/article/en-us/WBX000028782 for up to date details of feature support

Connecting to Webex – Enterprise Proxy Authentication



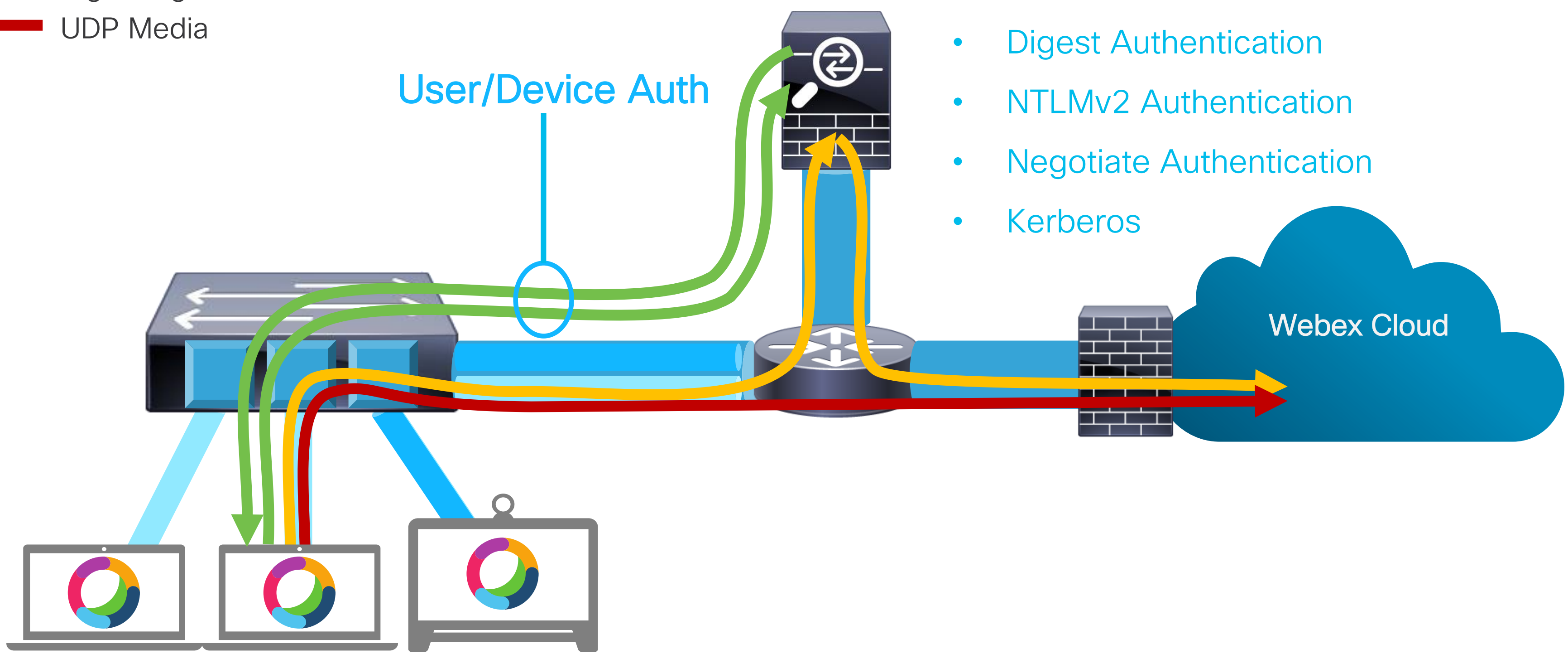
Proxy Authentication is not mandatory,
Many Enterprises do No Authentication

- Proxy Authentication
  - Proxy intercepts outbound HTTP request
  - Authenticates the User (Username & Password)
  - Authenticated User’s traffic forwarded
  - Unauthenticated User’s traffic dropped/blocked

Common Enterprise Proxy Authentication Methods

🟨 Signalling

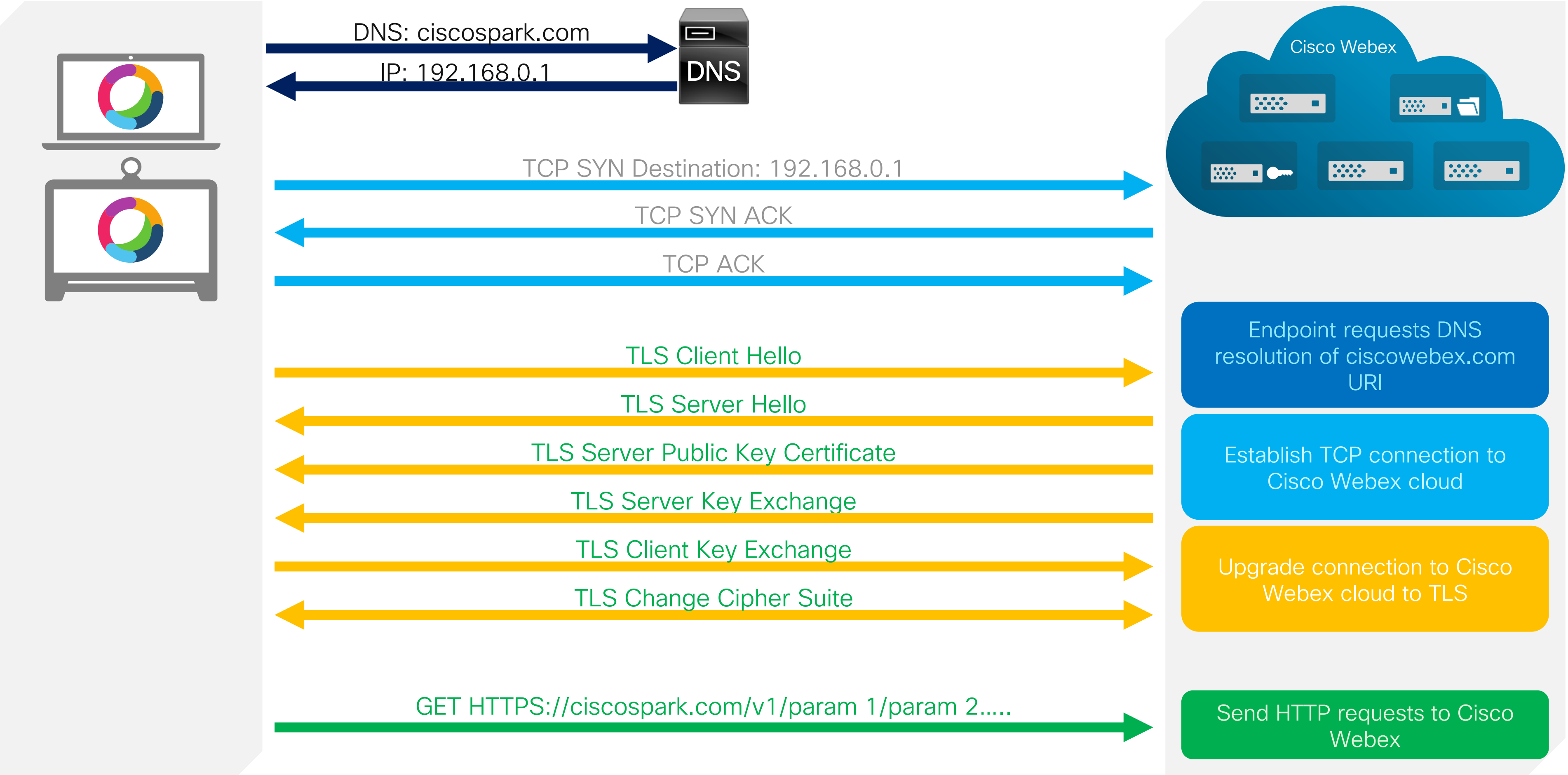
🟥 UDP Media



- Basic Authentication
- Digest Authentication
- NTLMv2 Authentication
- Negotiate Authentication
- Kerberos

For Webex Teams Proxy Auth support see doc : https://collaborationhelp.cisco.com/article/en-us/WBX000028782

Endpoint to Webex Cloud Connection – No Proxy



DNS: ciscospark.com

IP: 192.168.0.1

DNS

Cisco Webex

TCP SYN Destination: 192.168.0.1

TCP SYN ACK

TCP ACK

TLS Client Hello

TLS Server Hello

TLS Server Public Key Certificate

TLS Server Key Exchange

TLS Client Key Exchange

TLS Change Cipher Suite

GET HTTPS://ciscospark.com/v1/param 1/param 2.....

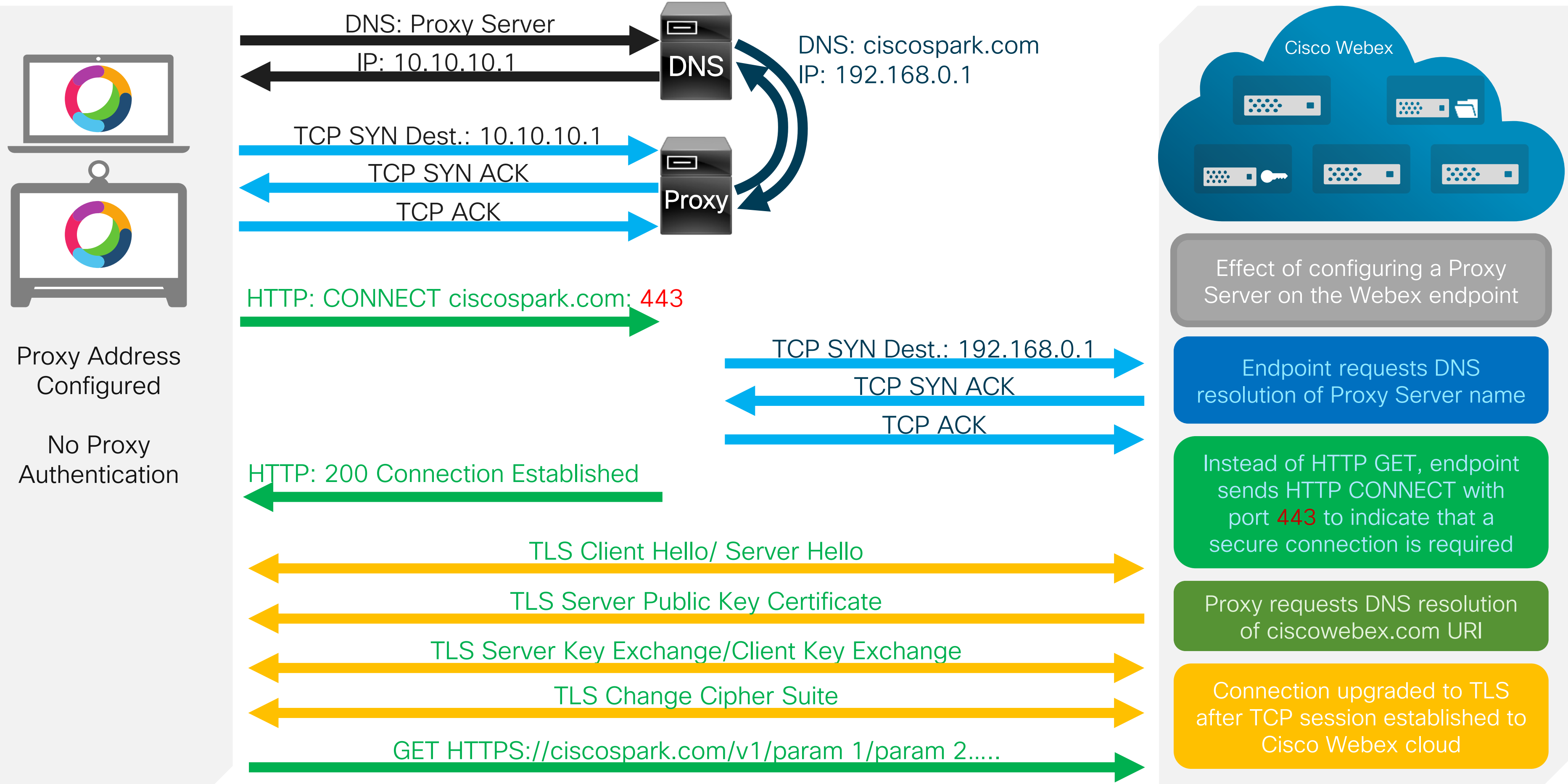
Endpoint requests DNS resolution of ciscowebex.com URI

Establish TCP connection to Cisco Webex cloud

Upgrade connection to Cisco Webex cloud to TLS

Send HTTP requests to Cisco Webex

Webex Cloud Connection via Proxy – No AuthN


DNS: Proxy Server
IP: 10.10.10.1
DNS
DNS: ciscospark.com
IP: 192.168.0.1
TCP SYN Dest.: 10.10.10.1
TCP SYN ACK
TCP ACK
Proxy
Cisco Webex
HTTP: CONNECT ciscospark.com: 443
TCP SYN Dest.: 192.168.0.1
TCP SYN ACK
TCP ACK
HTTP: 200 Connection Established
TLS Client Hello/ Server Hello
TLS Server Public Key Certificate
TLS Server Key Exchange/Client Key Exchange
TLS Change Cipher Suite
GET HTTPS://ciscospark.com/v1/param 1/param 2.....

Proxy Address Configured

No Proxy Authentication

Effect of configuring a Proxy Server on the Webex endpoint

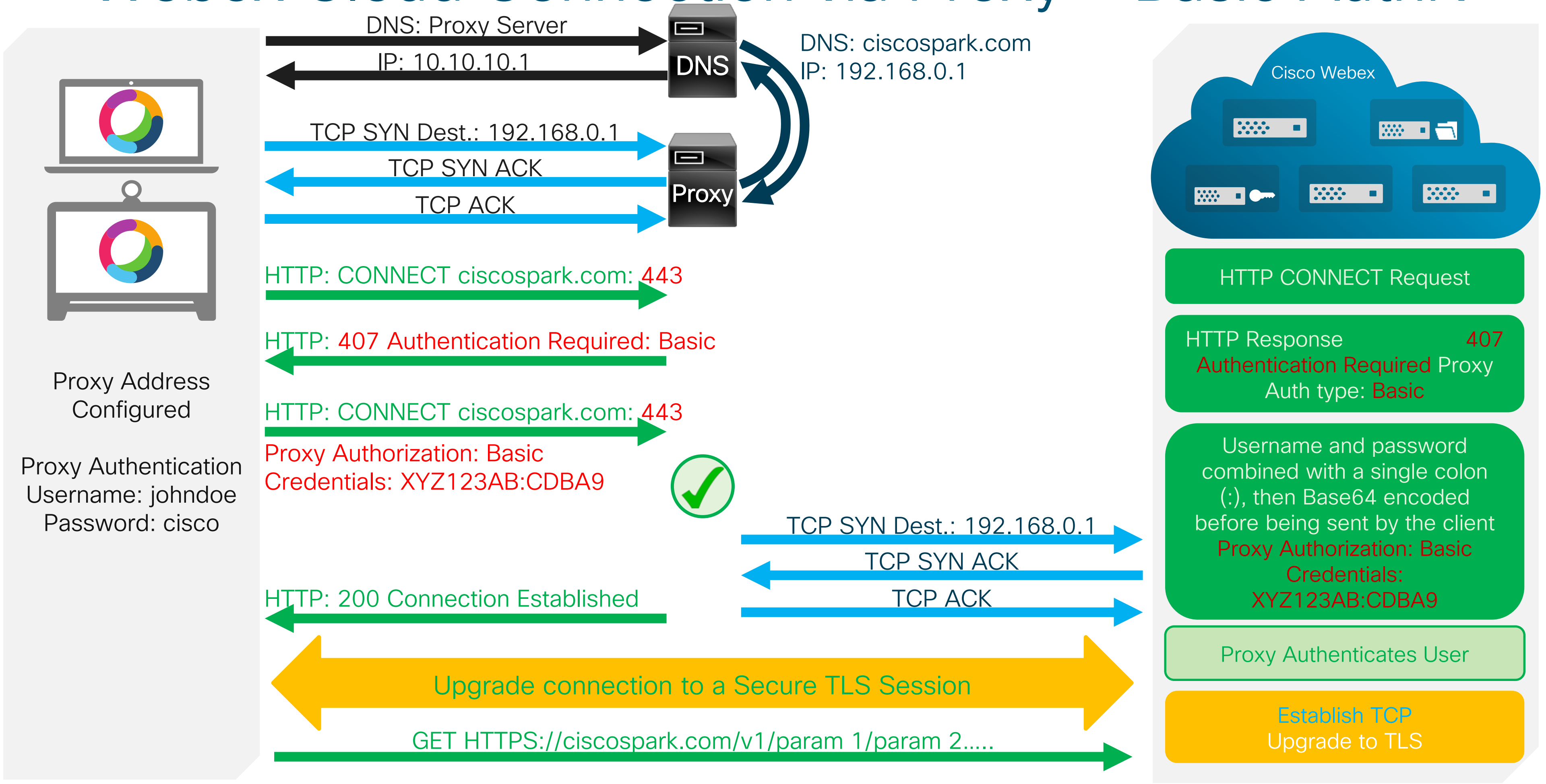
Endpoint requests DNS resolution of Proxy Server name

Instead of HTTP GET, endpoint sends HTTP CONNECT with port 443 to indicate that a secure connection is required

Proxy requests DNS resolution of ciscowebex.com URI

Connection upgraded to TLS after TCP session established to Cisco Webex cloud

Webex Cloud Connection via Proxy – Basic AuthN



DNS: Proxy Server

IP: 10.10.10.1

DNS: ciscospark.com

IP: 192.168.0.1

TCP SYN Dest.: 192.168.0.1

TCP SYN ACK

TCP ACK

HTTP: CONNECT ciscospark.com: 443

HTTP: 407 Authentication Required: Basic

HTTP: CONNECT ciscospark.com: 443

Proxy Authorization: Basic

Credentials: XYZ123AB:CDBA9

TCP SYN Dest.: 192.168.0.1

TCP SYN ACK

TCP ACK

HTTP: 200 Connection Established

Upgrade connection to a Secure TLS Session

GET HTTPS://ciscospark.com/v1/param 1/param 2.....

Proxy Address Configured

Proxy Authentication
Username: johndoe
Password: cisco

HTTP CONNECT Request

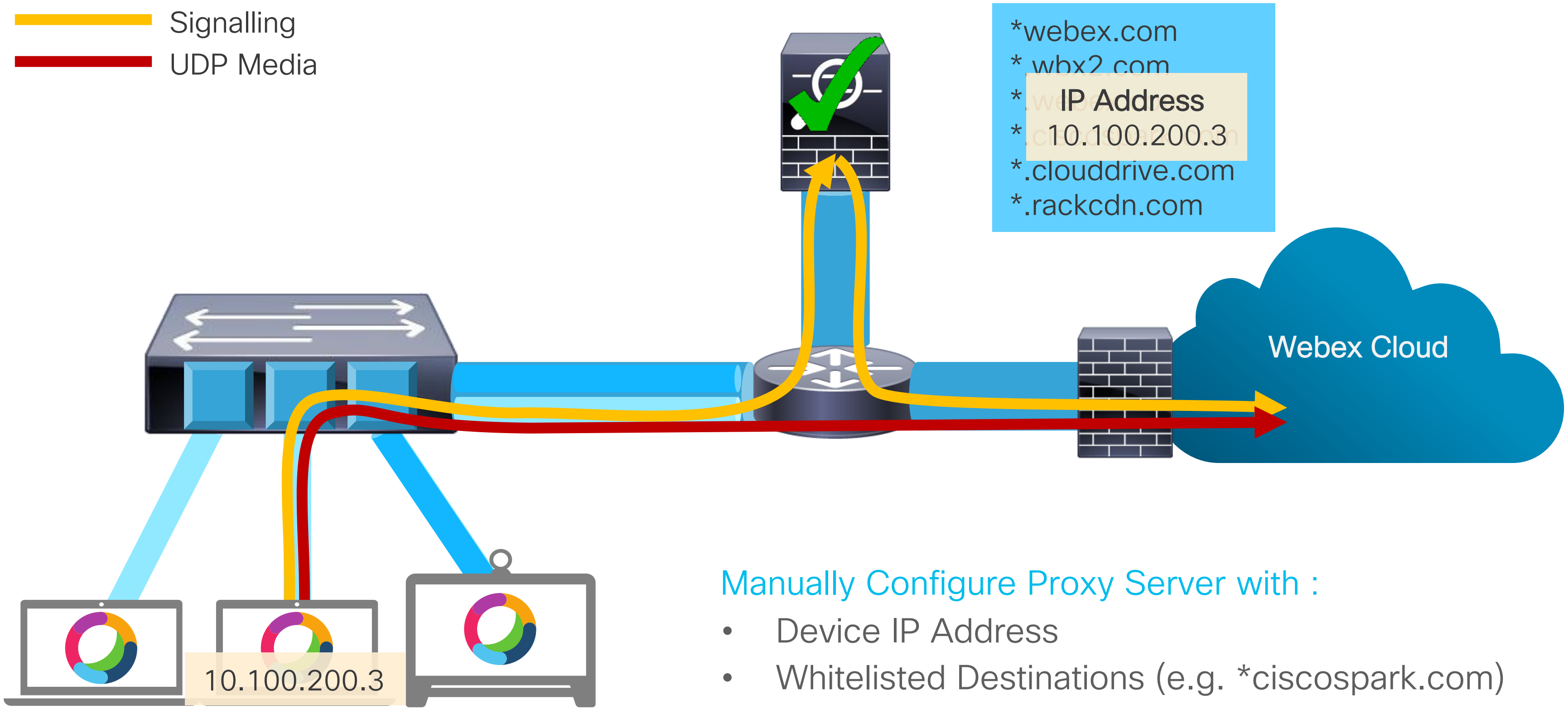
HTTP Response 407 Authentication Required Proxy Auth type: Basic

Username and password combined with a single colon (:), then Base64 encoded before being sent by the client Proxy Authorization: Basic Credentials: XYZ123AB:CDBA9

Proxy Authenticates User

Establish TCP
Upgrade to TLS

Proxy Authentication Bypass Methods



*webex.com
*.wbx2.com
*.webex.com
*.ciscospark.com
*.clouddrive.com
*.rackcdn.com

IP Address
10.100.200.3

Manually Configure Proxy Server with :

- Device IP Address
- Whitelisted Destinations (e.g. *ciscospark.com)

For Webex Teams Destination URLs see doc : https://collaborationhelp.cisco.com/article/en-us/WBX000028782

Webex Teams : Proxy Authentication Support

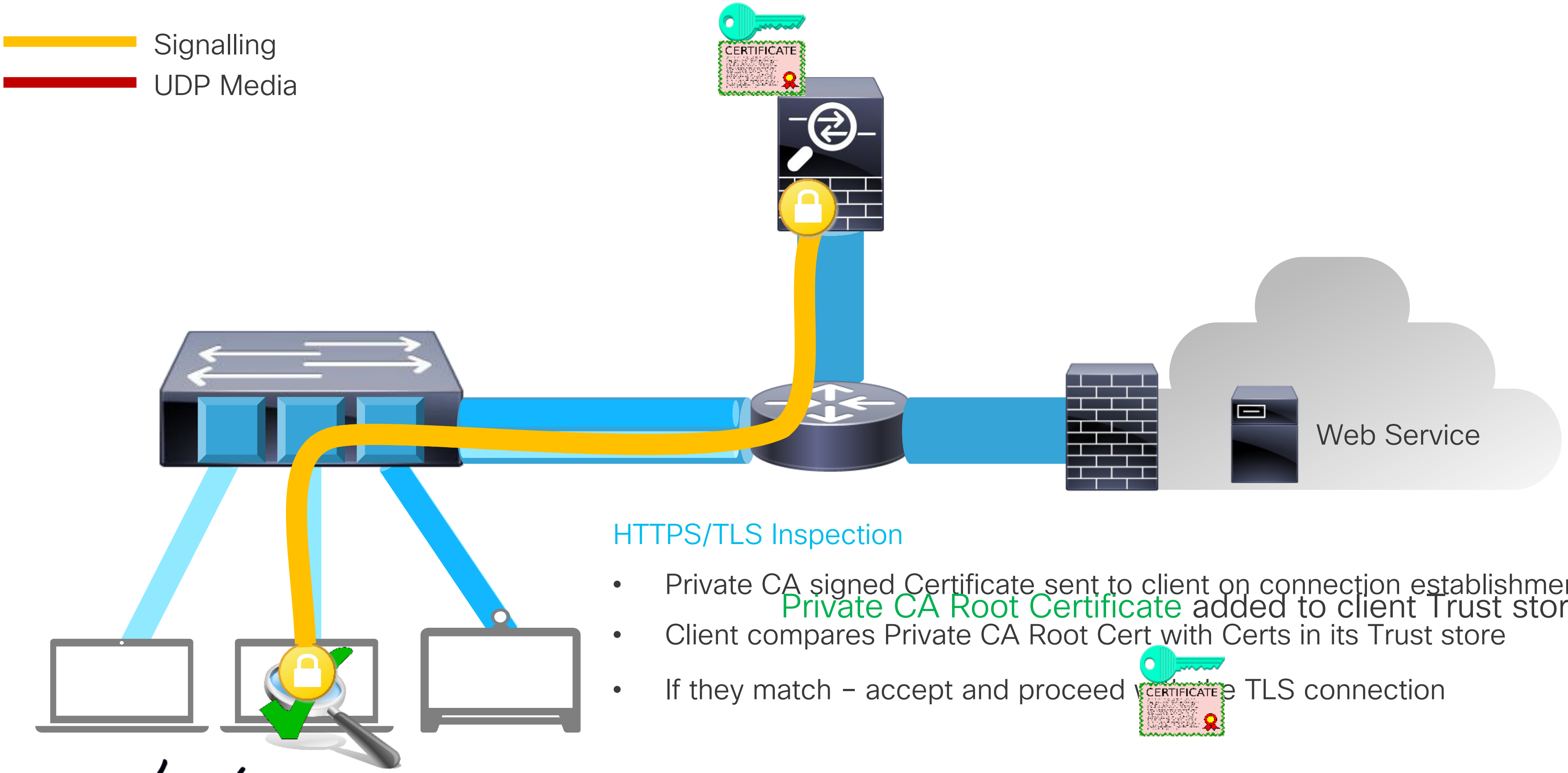
	Room OS	Webex Board	Windows	Mac	iOS	Android	HDS & VMN
No Authentication	✓	✓	✓	✓	✓	✓	✓
Basic	✓	✓	✓	✓	✓	✓	✓
Digest	✓	✓	TBD	TBD	✓	✓	✓
NTLM	Planning	Planning	✓	✓	✓	✓	✓
TLS Inspection	✓	✓	✓	✓	✓	✓	✓

Refer to https://collaborationhelp.cisco.com/article/en-us/WBX000028782 for up to date details of feature support

Proxy TLS/HTTPS Inspection – General Operation (1)

🟨 Signalling

🟥 UDP Media



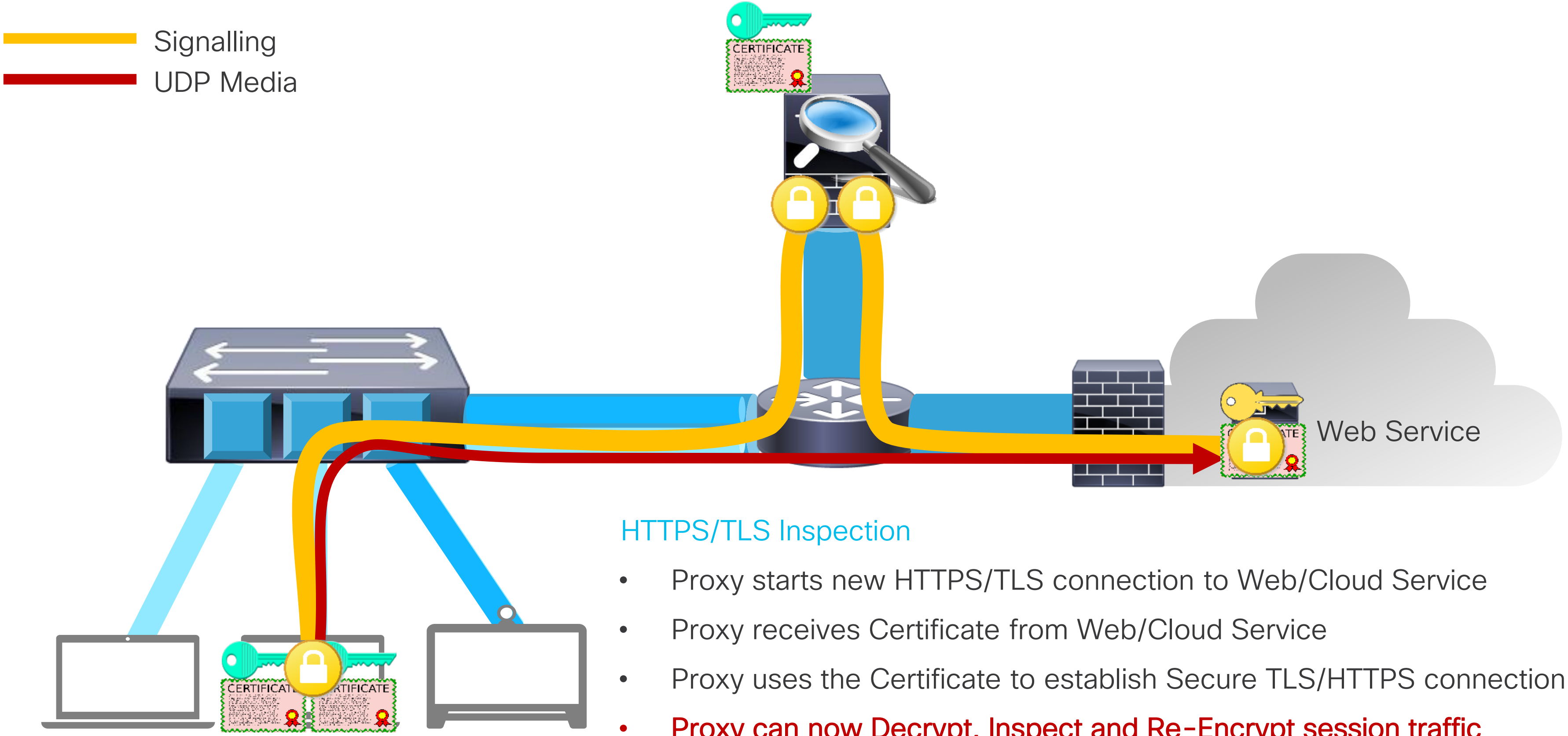
HTTPS/TLS Inspection

- Private CA signed Certificate sent to client on connection establishment

Private CA Root Certificate added to client Trust store

- Client compares Private CA Root Cert with Certs in its Trust store
- If they match – accept and proceed with the TLS connection

Proxy TLS/HTTPS Inspection – General Operation (2)

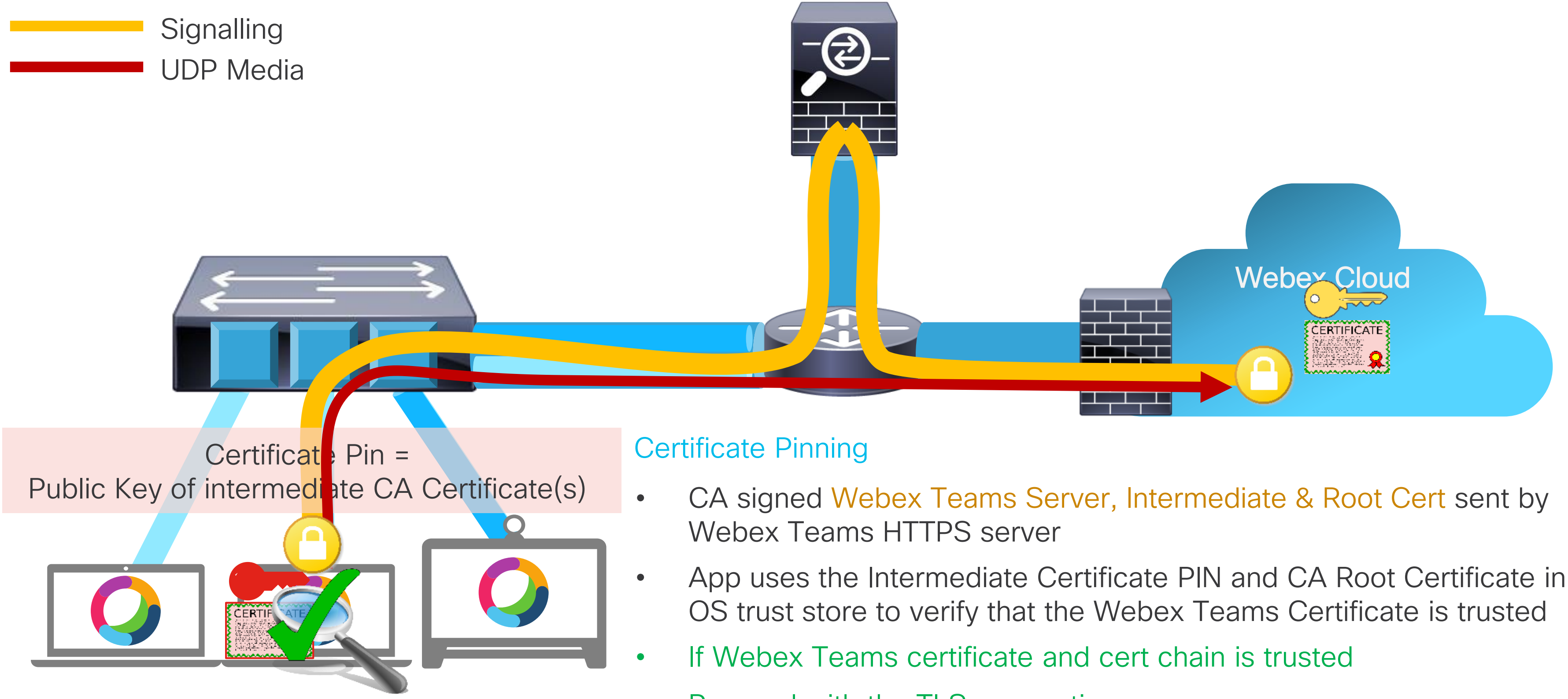


HTTPS/TLS Inspection

- Proxy starts new HTTPS/TLS connection to Web/Cloud Service
- Proxy receives Certificate from Web/Cloud Service
- Proxy uses the Certificate to establish Secure TLS/HTTPS connection
- Proxy can now Decrypt, Inspect and Re-Encrypt session traffic

Webex Teams Certificate Pinning

No HTTPS Proxy Inspection

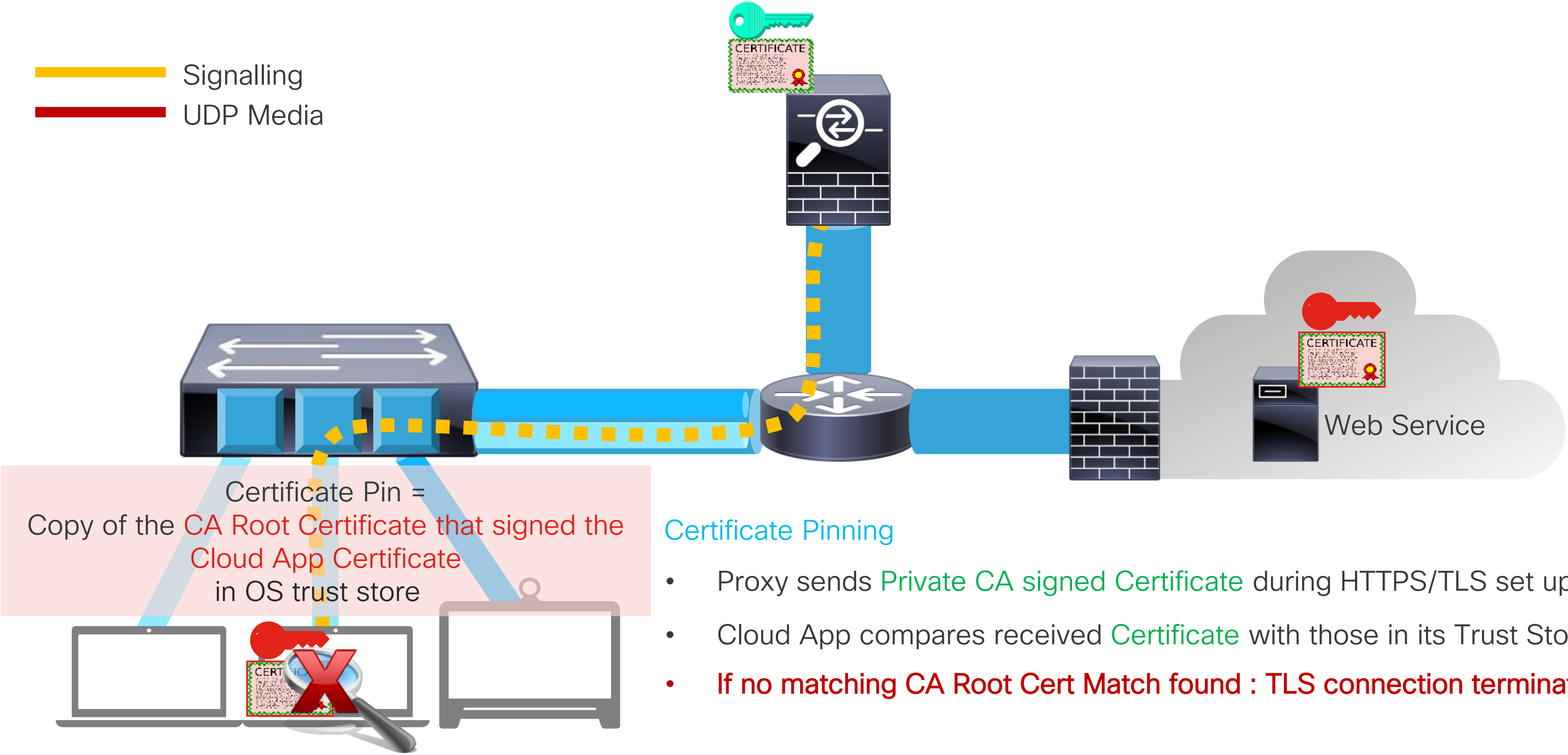


Certificate Pin =
Public Key of intermediate CA Certificate(s)

Certificate Pinning

- CA signed Webex Teams Server, Intermediate & Root Cert sent by Webex Teams HTTPS server
- App uses the Intermediate Certificate PIN and CA Root Certificate in OS trust store to verify that the Webex Teams Certificate is trusted
- If Webex Teams certificate and cert chain is trusted
- Proceed with the TLS connection

HTTPS Inspection – TLS Certificate Mismatch

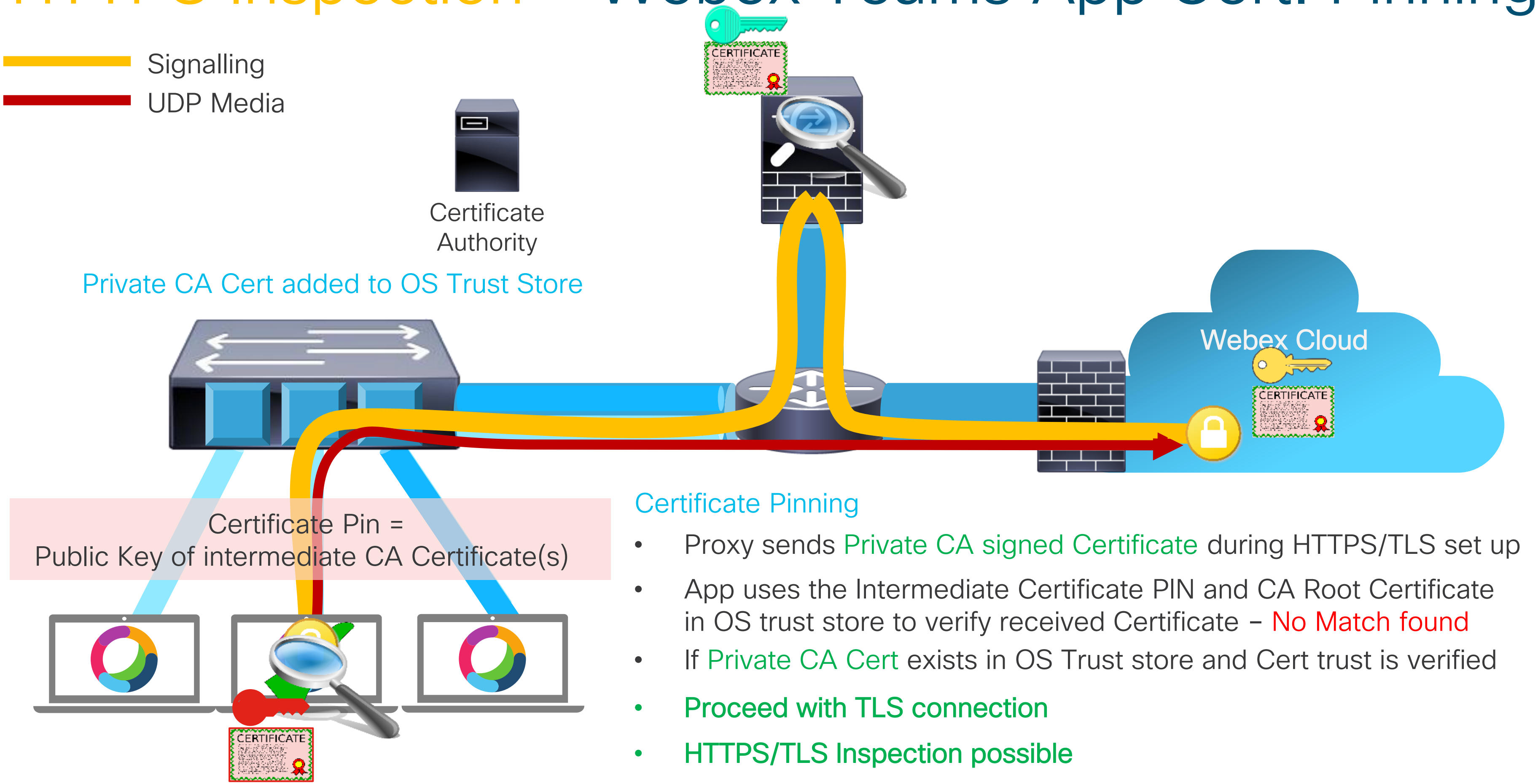


Certificate Pin =
Copy of the CA Root Certificate that signed the Cloud App Certificate
in OS trust store

Certificate Pinning

- Proxy sends Private CA signed Certificate during HTTPS/TLS set up
- Cloud App compares received Certificate with those in its Trust Store
- If no matching CA Root Cert Match found : TLS connection terminated

HTTPS Inspection – Webex Teams App Cert. Pinning



Certificate Pin =
Public Key of intermediate CA Certificate(s)

Certificate Pinning

- Proxy sends Private CA signed Certificate during HTTPS/TLS set up
- App uses the Intermediate Certificate PIN and CA Root Certificate in OS trust store to verify received Certificate – No Match found
- If Private CA Cert exists in OS Trust store and Cert trust is verified
- **Proceed with TLS connection**
- **HTTPS/TLS Inspection possible**

Webex Teams Proxy Inspection support details : https://collaborationhelp.cisco.com/article/en-us/WBX000028782

Online Documents :

Webex Teams Security and Privacy

Webex Teams Security – Documentation

Webex Teams Privacy and Security White Paper

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf Foundational document covering the Webex Cloud platform

Webex Teams Applications – Security White Paper

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Webex-Apps-Security-White-Paper.pdf (Teams Apps – Windows/Mac/iOS/Android)

Data Handling and Privacy for Cognitive Collaboration White Paper

https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-742369.html

Webex Teams Privacy Data sheet

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf Details on the processing, storage and encryption of Personal Data

Webex Teams Tech Ops and Security – Frequently Asked Questions (FAQs)

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Spark-Security-Frequently-Asked-Questions.pdf

Network Requirements for Webex Teams Services

https://collaborationhelp.cisco.com/article/WBX000028782

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

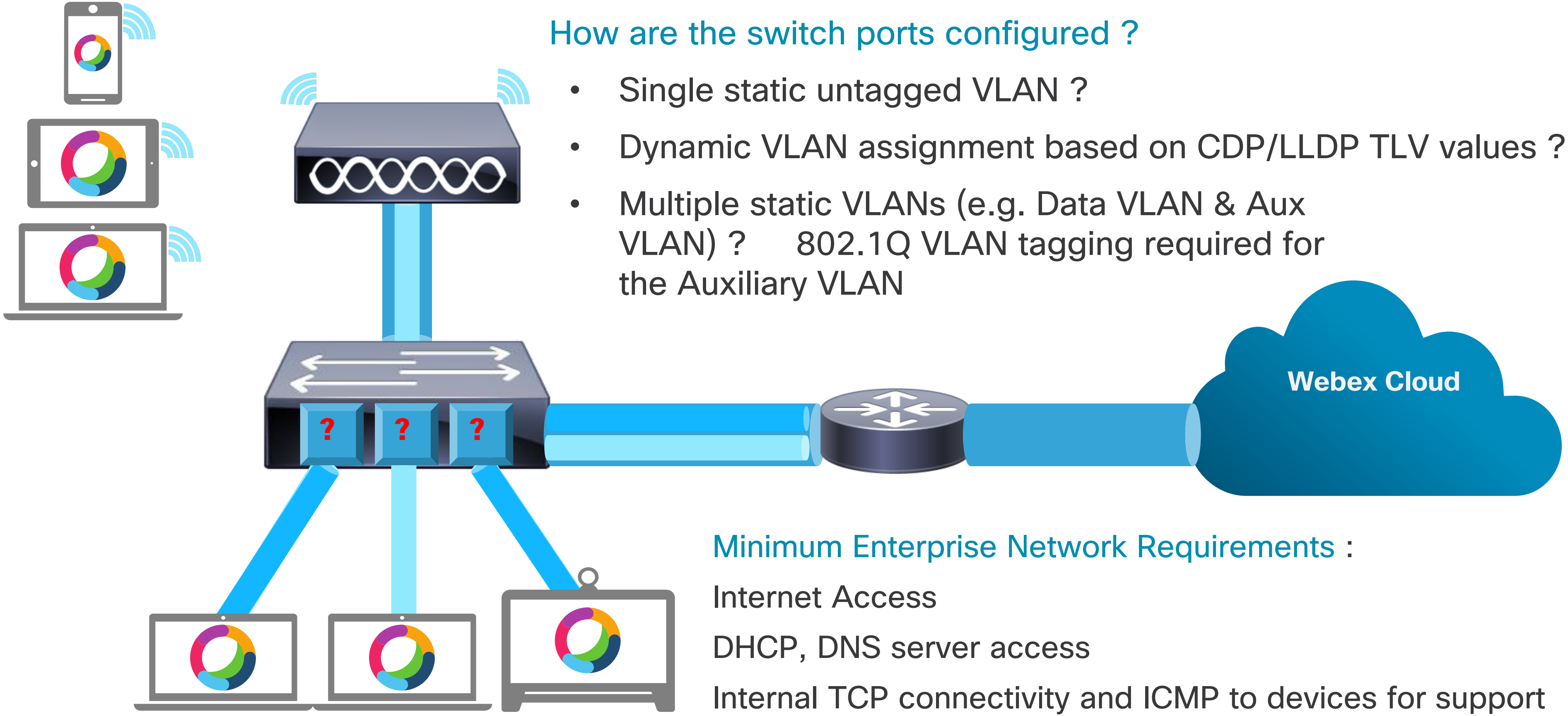
- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**

Webex Cloud Access : Enterprise VLANs

Connecting to Webex from the Enterprise - VLANs



How are the switch ports configured ?

- Single static untagged VLAN ?
- Dynamic VLAN assignment based on CDP/LLDP TLV values ?
- Multiple static VLANs (e.g. Data VLAN & Aux VLAN) ? 802.1Q VLAN tagging required for the Auxiliary VLAN

Minimum Enterprise Network Requirements :

Internet Access

DHCP, DNS server access

Internal TCP connectivity and ICMP to devices for support

Network Capabilities Webex Teams Devices

Webex Teams Device	Protocol	Software Train	CDP	802.1Q	Ethernet PC Port	Granular Configuration
Windows, Mac, iOS, Android, Web	HTTPS	WME	No	N/A	N/A	Static Untagged (Data) VLAN
DX	HTTPS	Room OS	Yes	Yes	Yes	Dynamic VLAN assignment, 802.1Q Tagging, Connected PC supported
SX	HTTPS	Room OS	Yes	Yes	No	Dynamic VLAN assignment, 802.1Q Tagging
MX	HTTPS	Room OS	Yes	Yes	No	Dynamic VLAN assignment, 802.1Q Tagging
Room Kits	HTTPS	Room OS	Yes	Yes	No	Dynamic VLAN assignment, 802.1Q Tagging
Webex Board	HTTPS	Room OS	Yes	Yes	No	Dynamic VLAN assignment, 802.1Q Tagging

You make **possible**