

TOMORROW starts here.



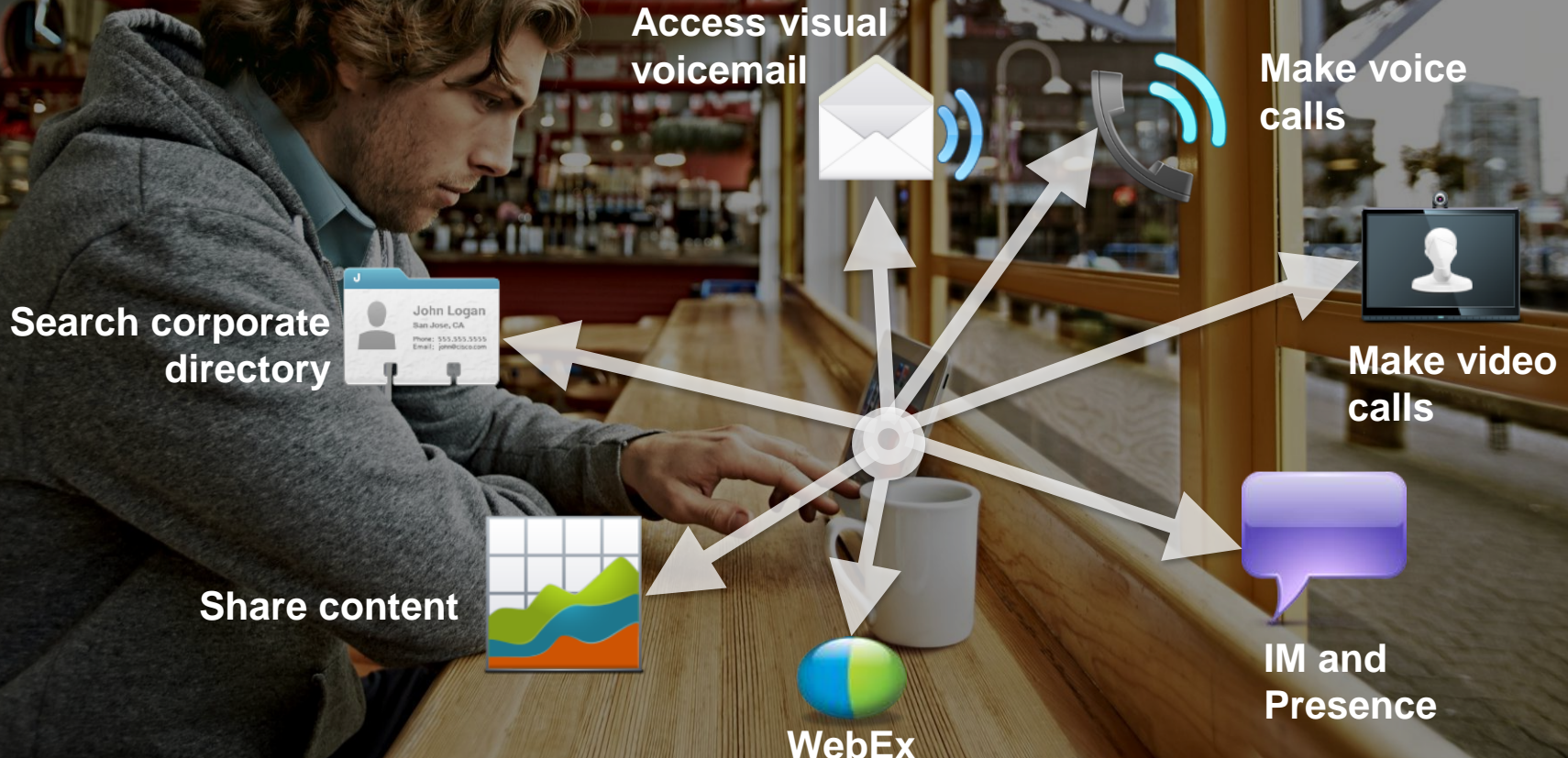
Cisco *live!*

Federation and Remote Access for Unified Communications Leveraging Collaboration Edge

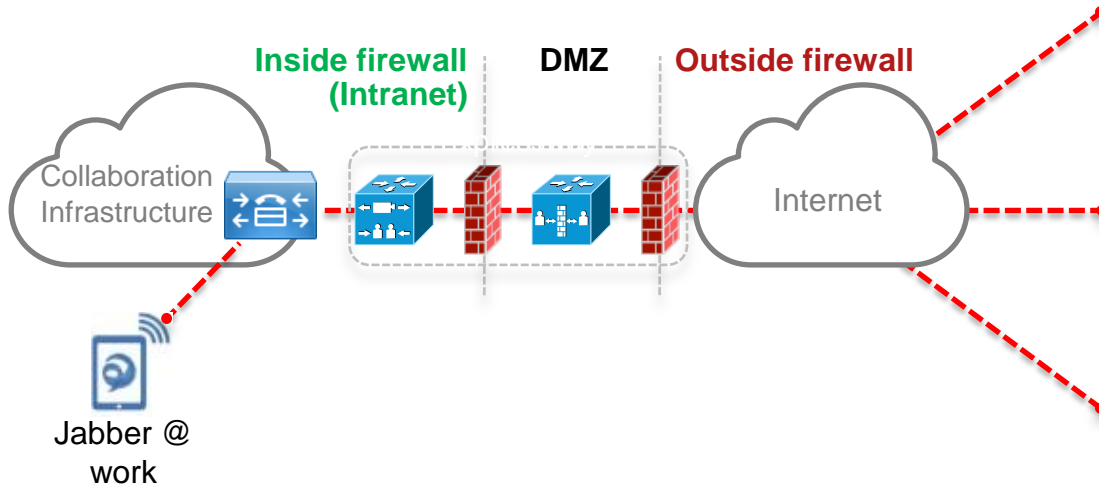
BRKUCC-2666

Darren Henwood
Consulting Systems Engineer

Making Collaboration as Easy & Effective Outside the Network as it is Inside with Jabber



Make Jabber Mobile Users as Productive on the Road



Jabber @
the café

- Jabber moves between networks

- Uses TLS technology

- Security Choice: No VPN required

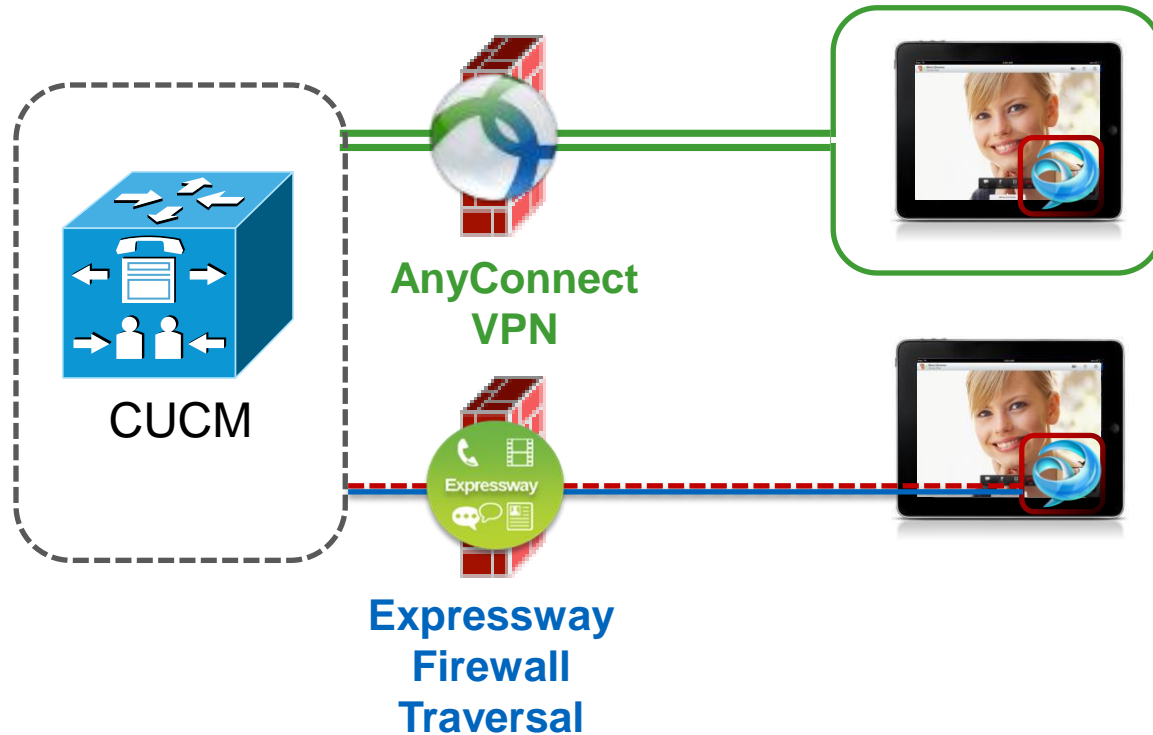
- Secure only Jabber application
- Personal data is not connected to the network

Jabber @
Home

Jabber @
the airport

- Automatic Service Discover

Cisco Jabber Remote Access Options



- Layer 3 VPN Solution
- Secures the entire device and its contents
- AnyConnect allows users access to any permitted applications & data
- **New Complementary Offering**
- Session-based firewall traversal
- Allows access to collaboration applications ONLY
- Personal data not routed through enterprise network

Branding Terminology Decode

Collaboration Edge

Umbrella term describing Cisco's entire collaboration architecture for edge
... features and services that help bridge islands to enable any to any collaboration...
...collaborate with anyone anywhere, on any device....

Cisco VCS

Existing product line option providing advanced video and TelePresence applications
Includes **VCS Control** and **VCS Expressway**

Cisco Expressway

New product line option for CUCM customers, providing firewall traversal & video interworking
Includes **Expressway Core** and **Expressway Edge**

Mobile and Remote Access

Feature available on **both** VCS and Expressway product lines with X8.1 s/w
Delivers VPN-less access to Jabber and Fixed Endpoints

Expressway X8.1 Product Line Options

X8.1



VCS



“VCS Control”
No Change

“VCS Expressway”
No Change



- Specialised video applications for video-only customer base and advanced video requirements
- No changes to existing licensing model



New
Offering

Expressway



“Expressway C”
Or Core

“Expressway E”
Or Edge



- Solution designed for and sold exclusively with CUCM 9.1 and above
- No additional cost for server software licenses for CUCM 9.1+ customers

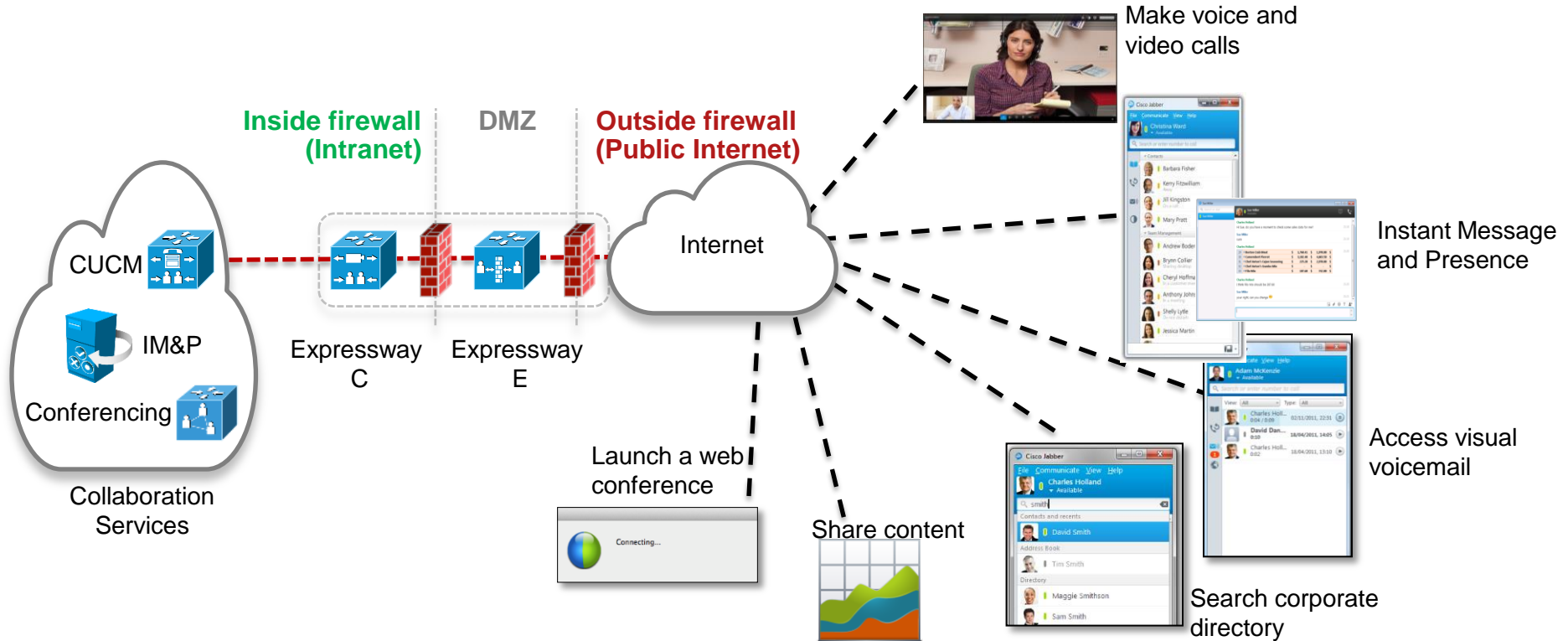
VCS and Cisco Expressway Feature Comparison

Feature Comparison	Cisco Expressway Series	Cisco VCS Family
Mobile and Remote Access	Y	Y
Business to Business Video	Y	Y
Advanced Features (Extension Mobility, voicemail, shared line, Call forward all, G729 support, ad-hoc conferencing, etc)	Y	N
Business to Consumer / Public to Enterprise Access with Jabber Guest	Y	Y
Video Interworking (IPv4 to IPv6, H.323-SIP, MS H.264 SVC-AVC, Standards-based 3rd Party Video endpoints)	Y	Y
Video / TelePresence Device Registration & Provisioning	N	Y
Video Session Management & Call Control	N	Y
WebEx Enabled TelePresence	N	Y



Expressway - Mobile & Remote Access

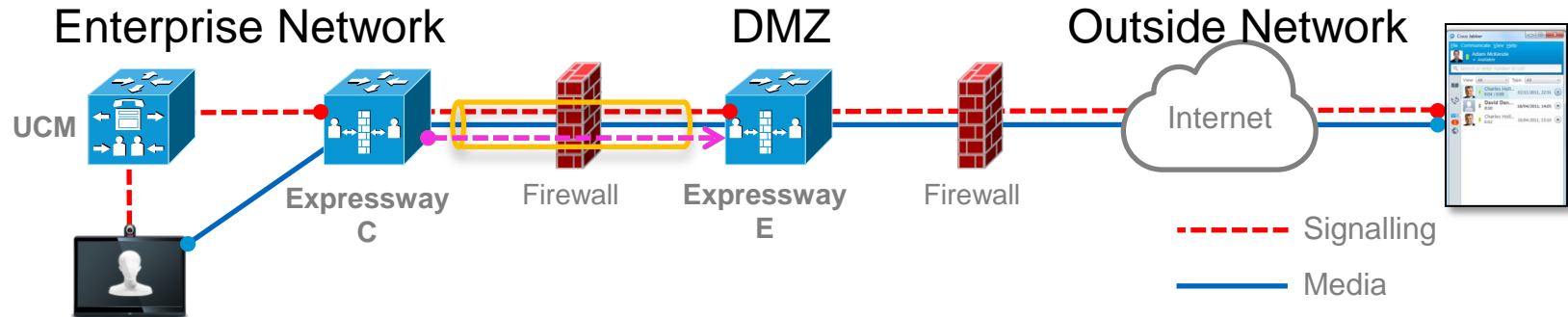
What can a Jabber Client do with Expressway?



Solution Components Software Requirements

Component	Min Software Version	Projected Availability
Cisco Expressway or Cisco VCS	X8.1	Available
Cisco Expressway or Cisco VCS	X8.1.1 (MR)	Q1CY14
CUCM	9.1(2) SU1	Available
CUCM IM&P	9.1	Available
Unity Connection	8.6(1)	Available
Jabber for Windows	9.7	Q1CY14
Jabber for iOS	9.6.1	Q1CY14
Jabber for MAC	TBD	TBD
Jabber for Android	9.6	Q1CY14
EX/MX/SX/C Series TelePresence Endpoints	TC7.0.1	Available

Expressway Firewall Traversal Basics

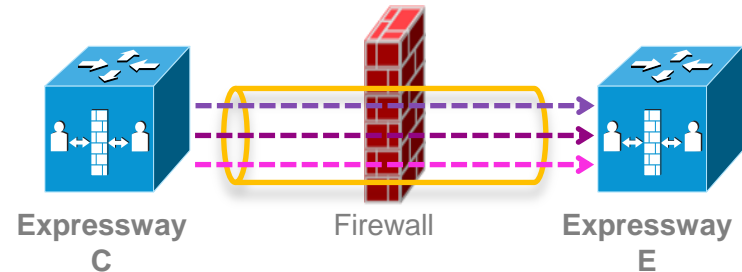


1. **Expressway E** is the traversal server installed in DMZ. **Expressway C** is the traversal client installed inside the enterprise network.
2. **Expressway C** initiates traversal connections outbound through the firewall to specific ports on **Expressway E** with secure login credentials.
3. Once the connection has been established, **Expressway C** sends keep-alive packets to **Expressway E** to maintain the connection
4. When **Expressway E** receives an incoming call, it issues an incoming call request to **Expressway C**.
5. **Expressway C** then routes the call to CUCM to reach the called user or endpoint
6. The call is established and media traverses the firewall securely over an existing traversal connection

X8.1 Firewall Traversal Capabilities Expanded

The X8.1 release delivers 3 key capabilities enabling the Expressway Mobile and Remote Access feature:

- XCP Router for XMPP traffic
- HTTPS Reverse proxy
- Proxy SIP registrations to CUCM



(details on new firewall port requirements covered later)

Mobile and Remote Access

- Enable Mobile and Remote Access on Expressway C & E
- Disabled by default in Jabber 9.6 (Windows and iOS)
- Enabled by jabber-config key

<Policies>

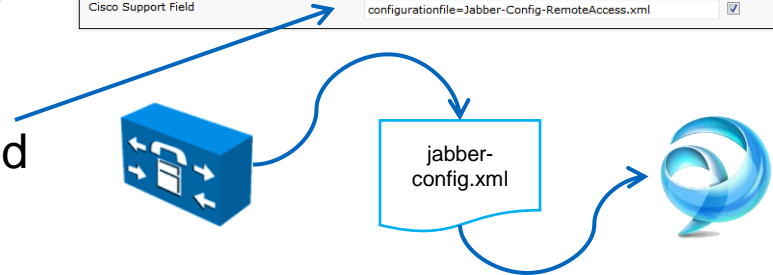
<RemoteAccess>ON</RemoteAccess>

</Policies>

- Mobile and Remote Access can be enabled for groups of users

The screenshot shows two configuration panels. The top panel, 'Unified Communications', has a 'Configuration' tab and two settings: 'Mobile and remote access' set to 'On' and 'Jabber Guest support' set to 'Off'. A 'Save' button is below. The bottom panel, 'Desktop Client Settings', lists various settings with dropdown menus and checkboxes. The 'Cisco Support Field' is set to 'configurationfile=Jabber-Config-RemoteAccess.xml' and has a checked checkbox.

Setting	Value	Checkbox
Automatically Start in Phone Control*	Disabled	<input type="checkbox"/>
Automatically Control Tethered Desk Phone*	Disabled	<input type="checkbox"/>
Extend and Connect Capability*	Enabled	<input type="checkbox"/>
Display Contact Photos*	Enabled	<input type="checkbox"/>
Number Lookups on Directory*	Enabled	<input type="checkbox"/>
Jabber For Windows Software Update Server URL		<input type="checkbox"/>
Problem Report Server URL		<input type="checkbox"/>
Analytics Collection*	Disabled	<input type="checkbox"/>
Analytics Server URL		<input type="checkbox"/>
Cisco Support Field	configurationfile=Jabber-Config-RemoteAccess.xml	<input checked="" type="checkbox"/>



Service Discovery

- Edge Detection determines whether Jabber is inside or outside the corporate firewall
 - Based on SRV records returned from DNS
 - `_collab-edge` -> outside corporate firewall
 - Transform all traffic and route through Expressway-E
 - `_cisco-uds` -> inside the company firewall
 - Do not transform traffic and route to appropriate service
- Service discovery is used to obtain login service
 - Based on highest priority SRV record returned
- Jabber Common Framework registers normally



Edge Detection

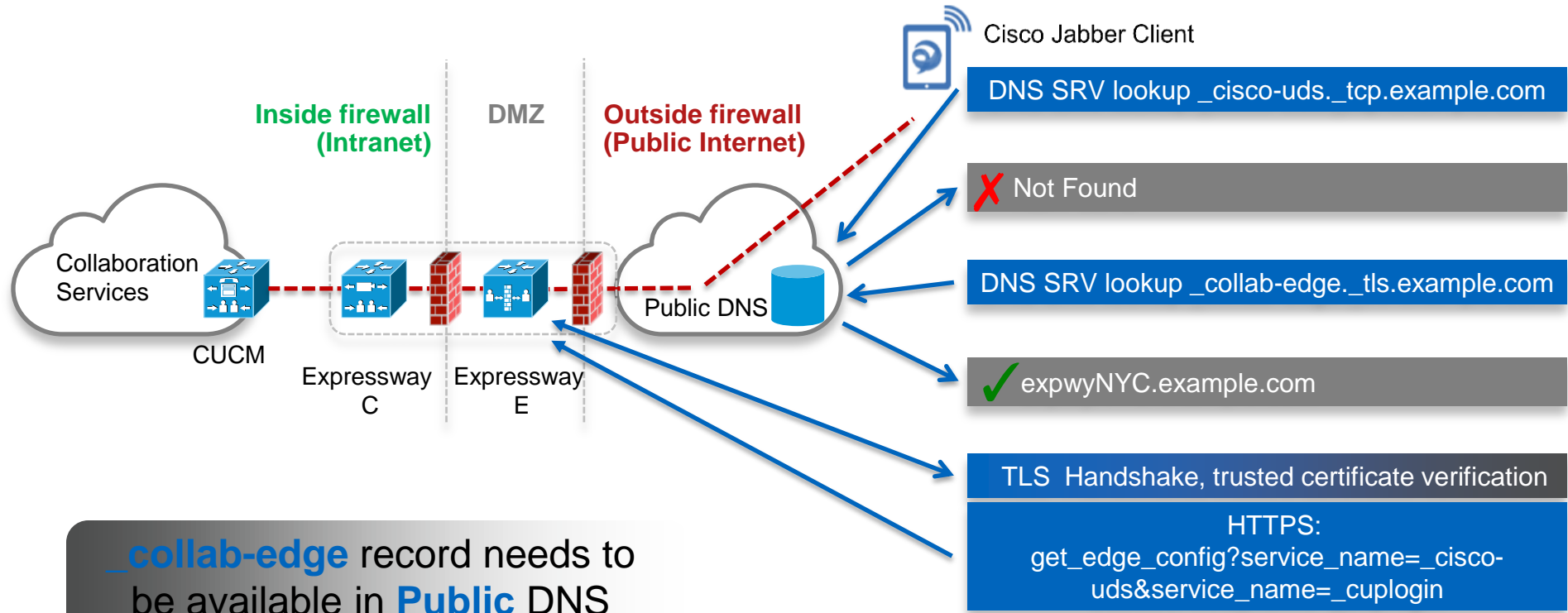


Service Discovery



Jabber Common Framework

Expressway & Jabber Service Discovery



Split DNS SRV Record Requirements

- **_collab-edge** record needs to be available in **Public** DNS
- Multiple SRV records (and Expressway E hosts) can be deployed for HA
- A GEO DNS service can be used to provide unique DNS responses by geographic region

```
_collab-edge._tls.example.com. SRV 10 10 8443 expwy1.example.com.  
_collab-edge._tls.example.com. SRV 10 10 8443 expwy2.example.com.
```

- **_cisco-uds** record needs be available only on **internal** DNS (available to Expressway C at a minimum)

```
_cisco-uds._tcp.example.com. SRV 10 10 8443 cucm1.example.com.  
_cisco-uds._tcp.example.com. SRV 10 10 8443 cucm2.example.com.
```

Jabber in Edge Mode (Transition)

When is discovery done?

- On start up
- Network change events will trigger SRV lookup which may transition you from external to internal
- When you get transport errors (SIP, XMPP & HTTP) will trigger SRV lookup which may transition you from internal to external
 - Only doing SRV lookup when there is network activity happening anyway and this saves battery life on mobile platforms
- During the transition period you will remain logged into the Jabber client, but you will get disconnected temporarily from the IM&P server, your presence will appear as offline, and once connected via Edge you will get reconnected to IM&P automatically and become online again.



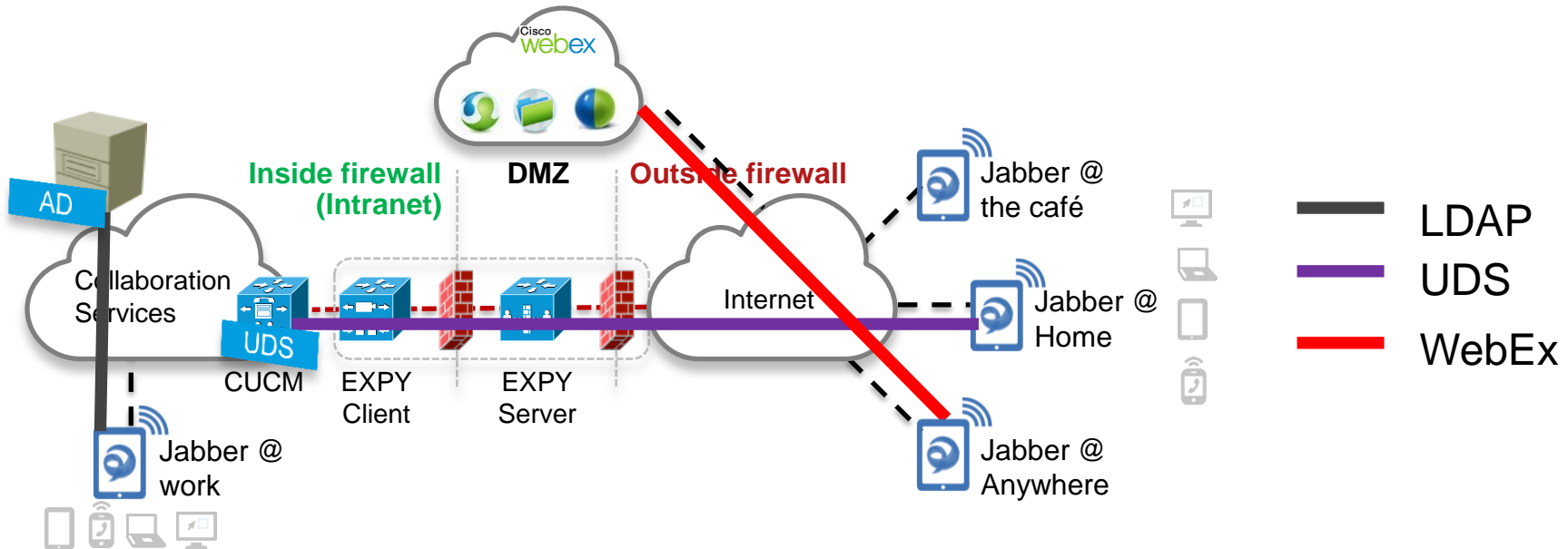
Mobile and Remote Access – Directory Integration



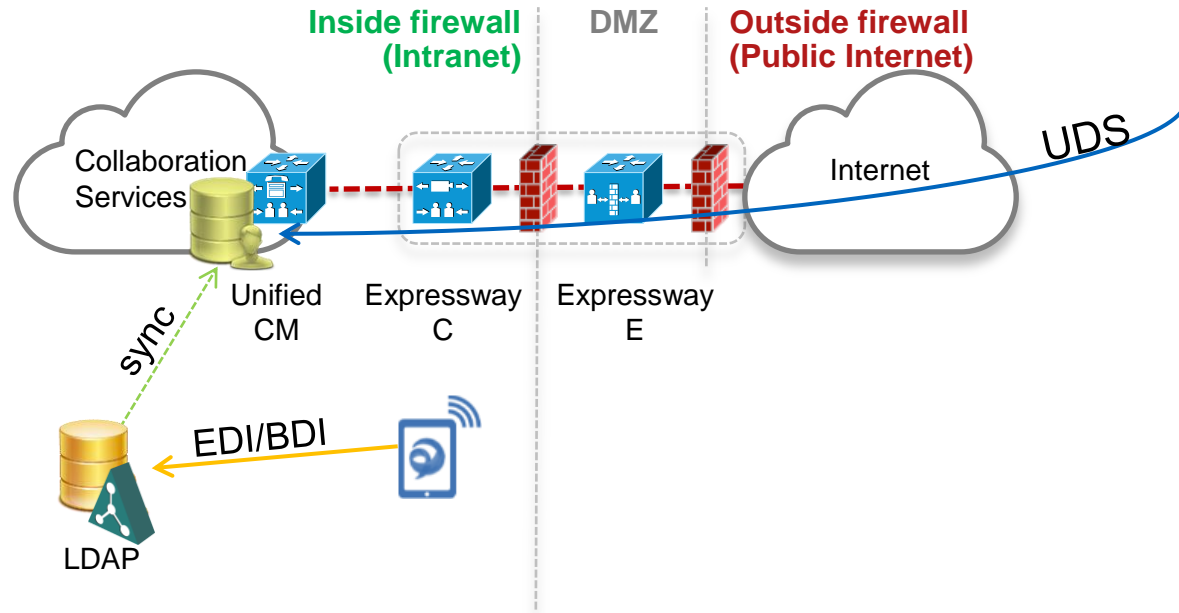
- LDAP traffic does not traverse the Collaboration Edge
- When in “edge” mode, UDS directory service provides directory integration for Jabber. UDS service runs on CUCM by default (Cisco Tomcat Service)
- When inside the firewall, Jabber will connect to a LDAP server to provide directory integration
 - Jabber for Windows supports Enhanced Directory Integration (EDI).
 - Jabber for Mac, Android and iOS, support Basic Directory Integration (BDI). BDI uses a common username and password to connect to a LDAP server for directory integration. BDI configuration is specified in the jabber-config.xml file.
- WebEx Messenger provides directory integration for Jabber/Cloud integrations

Mobile and Remote Access

- LDAP directory integration to be used in on premise mode
- UDS integration to be used in edge mode [for on-premise deployments]
- WebEx Messenger directory search to be used for cloud based deployments



Contact Search Considerations (on-premise IM&P)



- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to CUCM
- User Data Services (UDS) is a CUCM RESTful API allowing for contact search, among other things
- All Jabber clients connecting via Expressway will use UDS for contact search
- **Jabber clients deployed on-premise** will use **LDAP** for directory search
- Jabber clients will automatically use UDS for directory search when connecting via Expressway
- The entire corporate directory needs to be sync'd on every CUCM cluster for best contact search experience

Mobile and Remote Access

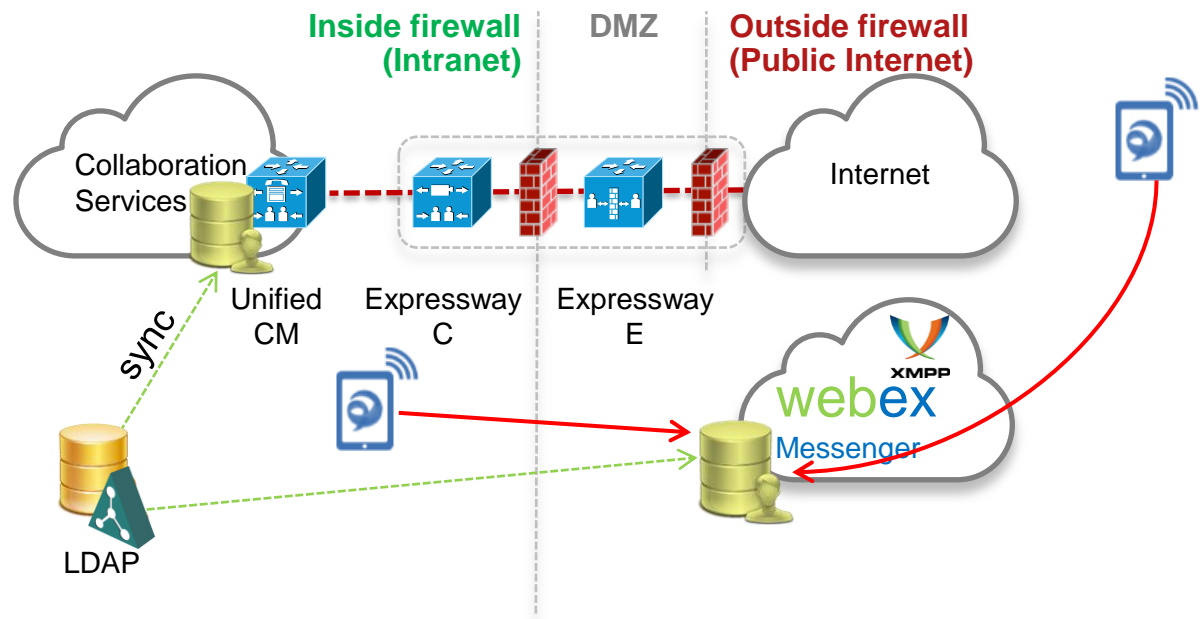
- Directory integration configured in jabber-config.xml (except for cloud mode)

```
<Directory>
  <!-- EDI Settings -->
  <SearchBase1>OU=Employees,OU=AllUsers,DC=example,DC=com</SearchBase1>
  <PhotoURISubstitutionEnabled>True</PhotoURISubstitutionEnabled>
  <PhotoURISubstitutionToken>sAMAccountName</PhotoURISubstitutionToken>
  <PhotoURIWithToken>http://photos.example.com/photo/sAMAccountName.jpg</PhotoURIWithToken>

  <!-- BDI Settings -->
  <BDIPrimaryServerName>ds.example.com</BDIPrimaryServerName>
  <BDIConnectionUsername>readonly@example.com</BDIConnectionUsername>
  <BDIConnectionPassword>readonly</BDIConnectionPassword>
  <BDISearchBase1>OU=Employees,OU=AllUsers,DC=example,DC=com</BDISearchBase1>
  <BDIPhotoURISubstitutionEnabled>True</BDIPhotoURISubstitutionEnabled>
  <BDIPhotoURISubstitutionToken>sAMAccountName</BDIPhotoURISubstitutionToken>
  <BDIPhotoURIWithToken>http://photos.example.com/photo/sAMAccountName.jpg</BDIPhotoURIWithToken>
  <EnableLocalAddressBookSearch>true</EnableLocalAddressBookSearch>

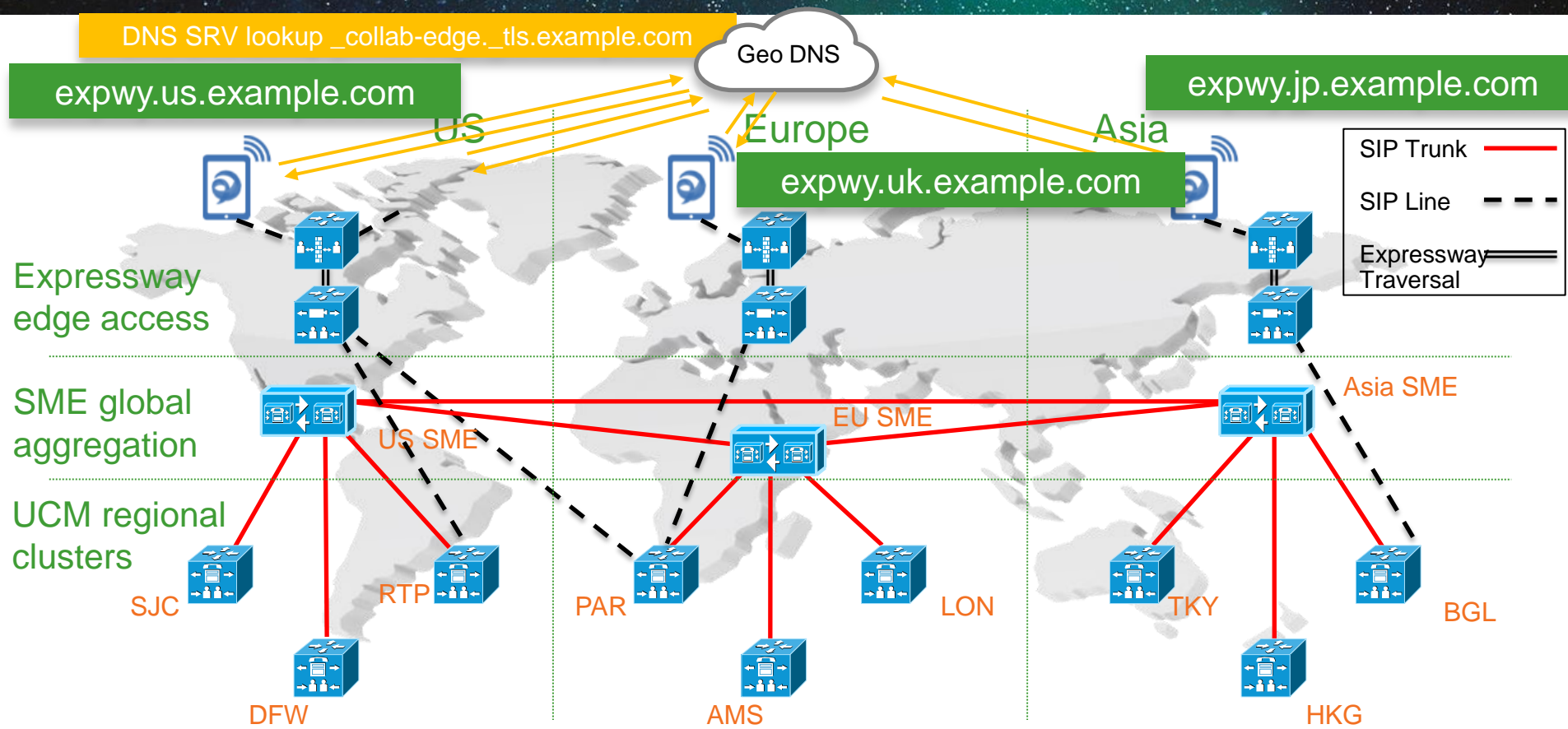
  <!-- UDS Settings for Edge users only -->
  <UDSPhotoURIWithToken>http://photos.example.com/photo/%%uid%%.jpg</UDSPhotoURIWithToken>
</Directory>
```

Contact Search Considerations (Cloud based IM&P)



- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to CUCM
- Corporate directory is also exported to WebEx Messenger cloud
- All Jabber clients will use WebEx Messenger cloud as a contact source for contact search

Global Deployment Topology & Geo DNS



DNS SRV lookup _collab-edge._tls.example.com

expwy.us.example.com

Geo DNS

Europe

expwy.jp.example.com

Asia

expwy.uk.example.com

SIP Trunk ———

SIP Line - - -

Expressway Traversal ==

Expressway edge access

SME global aggregation

UCM regional clusters

US SME

EU SME

Asia SME

SJC

RTP

DFW

PAR

AMS

LON

TKY

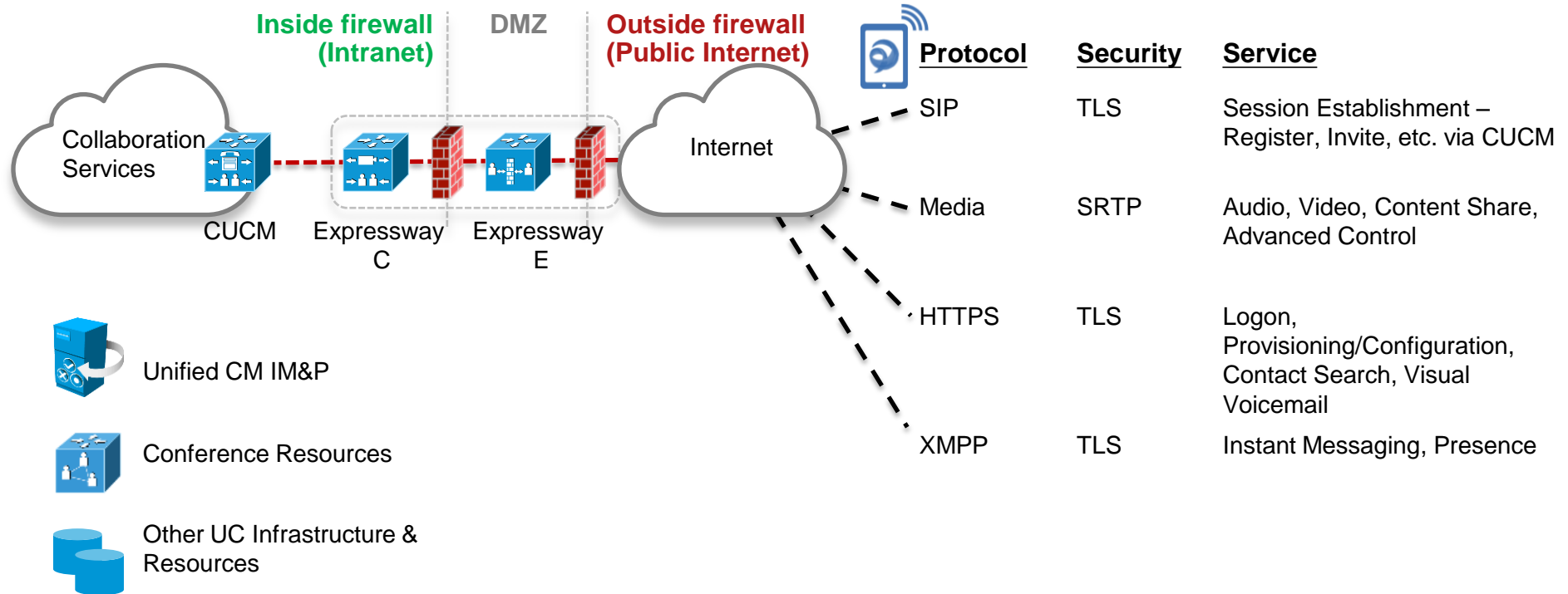
HKG

BGL



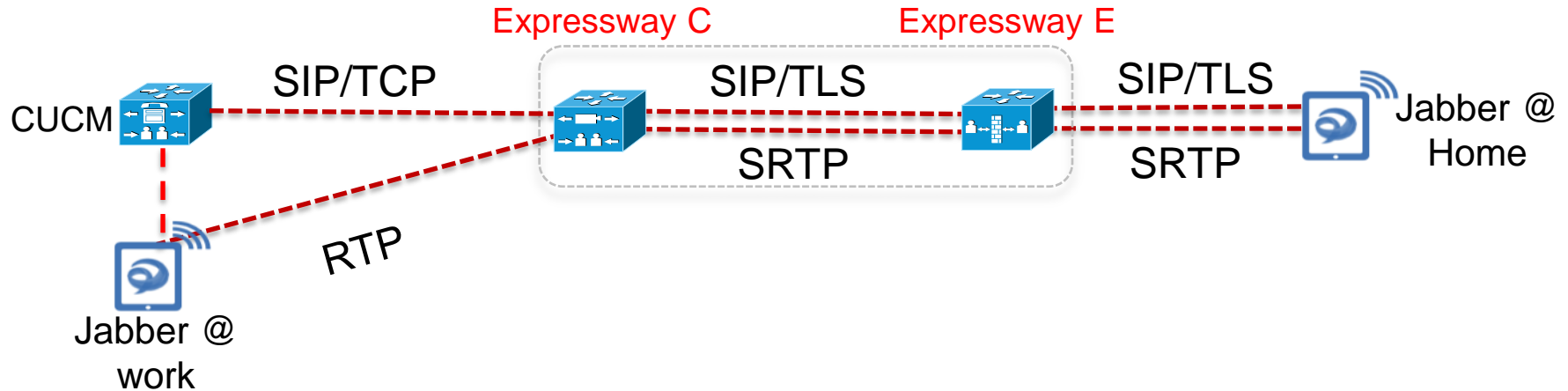
Design and Deployment Considerations

Protocol Workload Summary

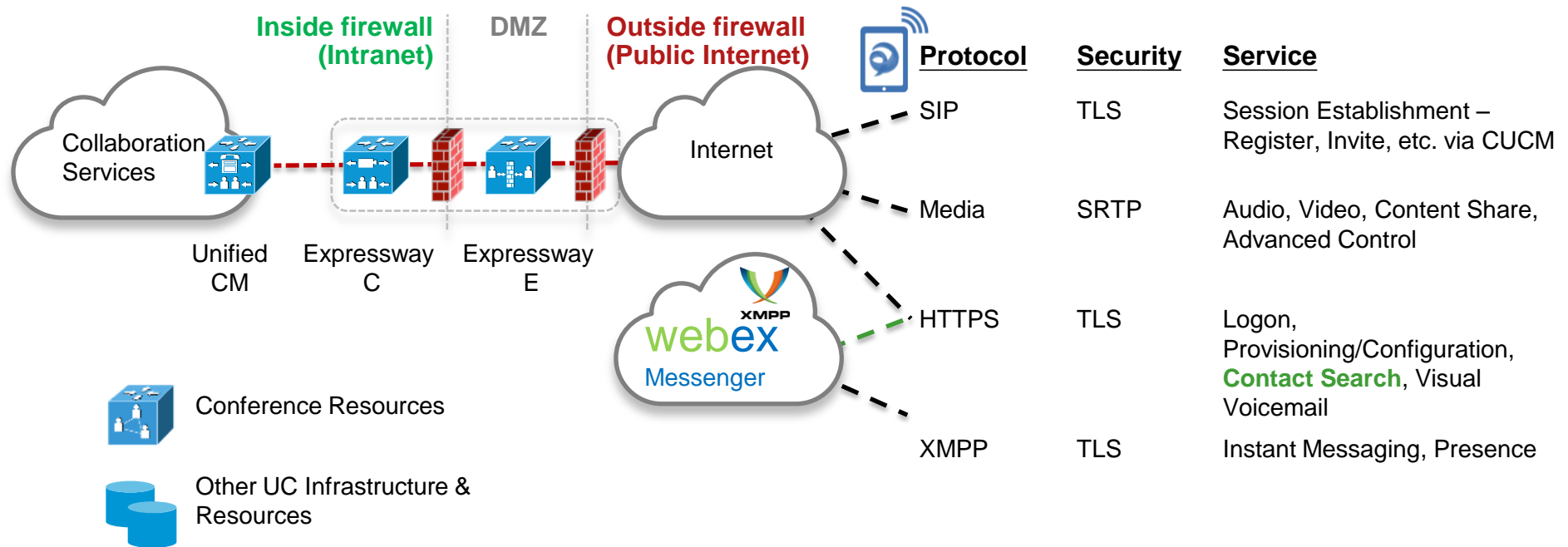


Jabber in Edge Mode

All communication from the client to Expressway Edge is secured using TLS (even if CSF device has not been CAPF enrolled)

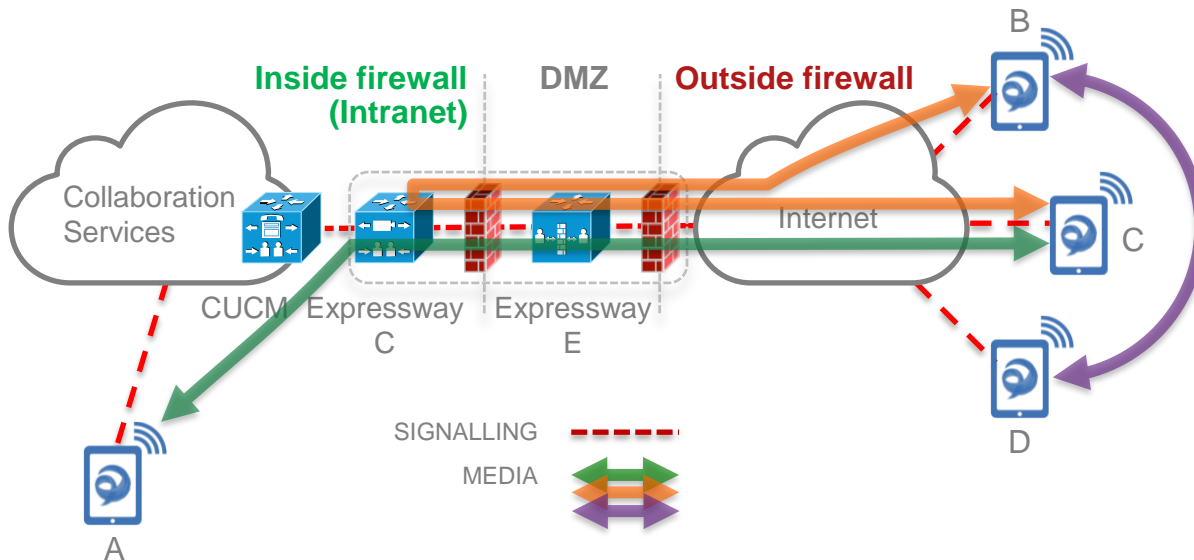


Hybrid Deployment - Cloud Based IM&P



Media Path Summary

CUCM provides call control for both mobile and on-premise endpoints



Media Traversal

- “C” calls “A” on-premise
- Expressway solution provides firewall traversal for media
- Expressway C de-multiplexes media and forwards toward “A”

Media Relay

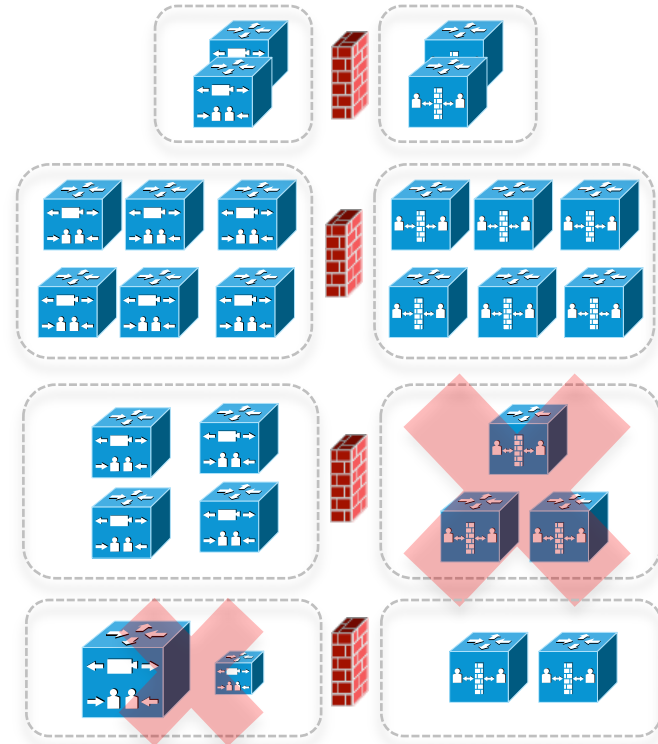
- “C” calls “B” off-premise
- Media is relayed via Expressway C

Optimised Media (roadmap ICE support)

- “B” calls “D” off-premise
- Both “B” and “D” are ICE-enabled
- STUN binding success
- Media flows are optimised between endpoints

Expressway Clustering, 4+2

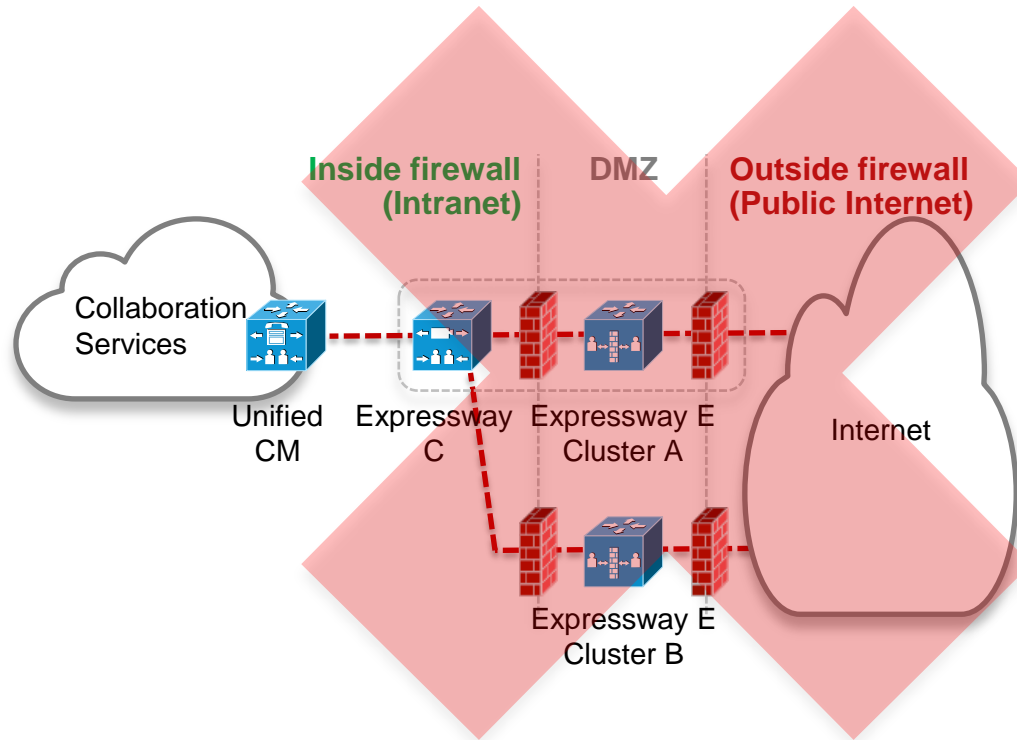
- Cluster Expressways for scale and redundancy
- Expressway Clusters support up to 6 peers
- Expressway E and C node types cannot be mixed in the same cluster
- Deploy equal number of peers in Expressway C and E clusters
- Deploy same OVA sizes throughout cluster
- Expressway remote access is limited to one customer domain per cluster
- However customers can deploy multiple clusters for the same customer domain



Mobile & Remote Access Deployment Options

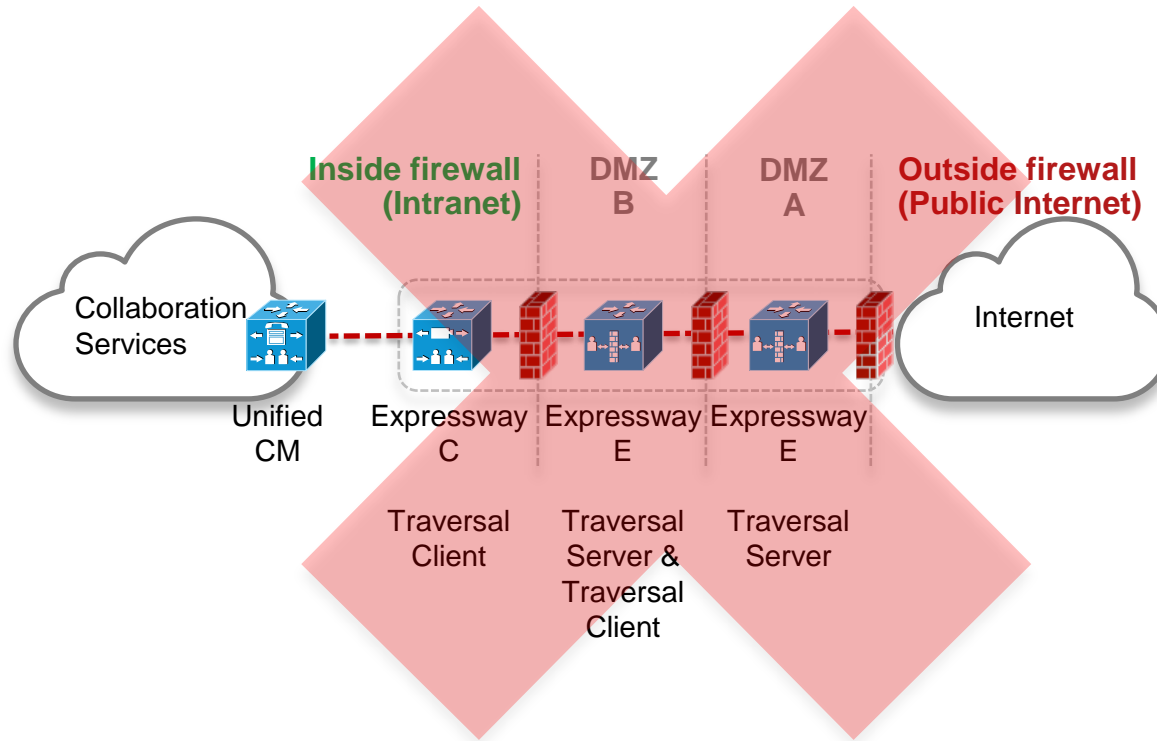
CUCM Clusters	Expressway C Clusters	Expressway E Clusters	Comments
1	1	1	Single Expressway deployment providing remote access to a central CUCM cluster
1	2+	2+	Regional Expressway deployments providing remote access to a central CUCM cluster
2+	1	1	Single Expressway deployment providing remote access to a multiple CUCM clusters
2+	2+	2+	Regional Expressway deployments providing remote access to multiple CUCM Clusters

Unsupported: Unbalanced Expressway Deployments



- This model is still supported for traditional VCS Expressway deployments
- But this is **not supported for the new mobile and remote access** functionality introduced in X8.1
- Expressway X8.1 remote access requires a Expressway C cluster for each Expressway E cluster
- **Only one “Mobile & Remote Access” enabled Traversal zone per cluster**

Unsupported: Expressway Chained Traversal



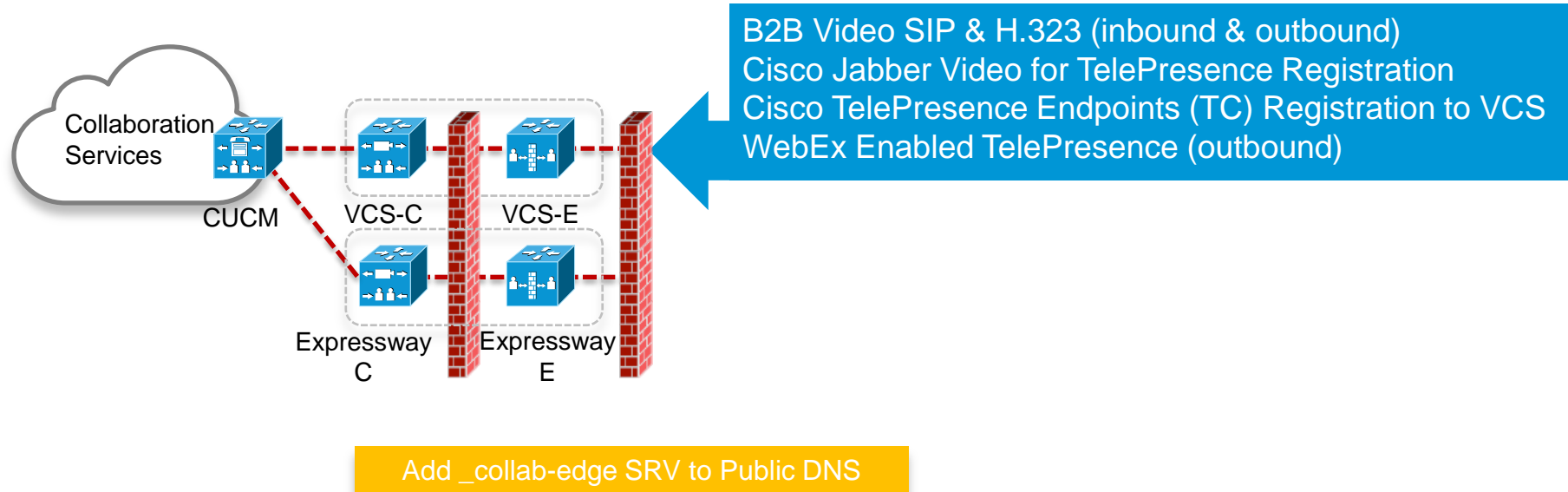
- Chained traversal is often used in environments with heightened security policies
- This option is still supported for traditional VCS deployments, or Expressway deployments that do not require the remote and mobile access feature
- Not supported for the new mobile and remote access functionality introduced in X8.1
- **Only one “Mobile & Remote Access” enabled Traversal zone per cluster**

Existing VCS Customers

- Customers with VCS-C and VCS-E can add Mobile and Remote Access to an existing deployment
- Simply add a parallel traversal zone on existing VCSs to support mobile and remote access
- Ideal for mid-market customers, POCs, or pilot programs
- Concurrent session scale is the primary reason for adding Expressways dedicated to Mobile & Remote access
 - Will the number of remote Jabber users making calls over Expressway crush my existing TelePresence deployment?
- The difference in security posture between B2B video and remote access solutions is another consideration
 - Does it make sense for the customer to combine these solutions on the same VMs?

Parallel Deployments of VCS & Expressway

- `_collab-edge` SRV records don't conflict with existing VCS SRV record usage



AnyConnect & Expressway Coexistence

- Customers that have deployed AnyConnect can also deploy Expressway Mobile & Remote Access feature
- For the best end user experience, prevent all Jabber traffic from using the AnyConnect tunnel
 - ☹ Active calls going through Expressway will be dropped if AnyConnect tunnel is established mid-call
- 😊 Expressway can provide Jabber client access to on-premise collaboration services even with an active AnyConnect tunnel established
- Requirements to keep Jabber traffic going through Expressway
 - AnyConnect split tunnel providing connectivity to internal enterprise \ network **only** (not including Expressway E)
 - Deny access (ASA DNS inspection) to the internal DNS SRV records (_cisco-uds & _cuplogin) to AnyConnect clients





Expressway Configuration

Expressway Configuration Summary

- Enable Mobile & Remote Access feature, Configuration > Unified Communications
- Provide IM&P Publisher address and supply admin credentials for each IM&P cluster (not required for hybrid deployments)
- Provide CUCM Publisher address and supply admin credentials for each CUCM cluster
 - Expressway C connects to each Publisher and discovers all cluster nodes
 - Neighbour Zone auto-generated for each CUCM node
 - Search Rules auto-generated for each CUCM node
- Add the customer domain and select services
- Generate certificate signing requests and procure CA signed certs
- Configure Traversal Zone with Mobile & Remote Access feature enabled


Unified Communications Configuration


- Expressway C

Unified Communications

You are here: [Configuration](#) ▶ [Unified Communications](#) ▶ Configurati

Configuration

Mobile and remote access On 

Jabber Guest support On 

IM and Presence servers and Unified CM servers

IM and Presence servers 2 [Discover IM and Presence servers](#)

Unified CM servers 3 [Configure Unified CM servers](#)

Advanced

HTTP server allow list [Configure HTTP server allow list](#)

Jabber Guest servers [Configure Jabber Guest servers](#)

Advanced settings [Show advanced settings](#)

Unified Communications Configuration

- Expressway C

The screenshot shows the Cisco Expressway-E configuration page. At the top left is the Cisco logo and the text "Cisco Expressway-E". Below this is a navigation bar with tabs for "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "Configuration" tab is selected. To the right of the navigation bar are help and refresh icons. Below the navigation bar is a breadcrumb trail: "You are here: Configuration > Unified Communications > Configuration". The main content area is titled "Unified Communications" and contains a "Configuration" section with two settings: "Mobile and remote access" and "Jabber Guest support". Both settings are currently set to "On" and have an information icon to their right. At the bottom left of the configuration area is a "Save" button.

Cisco Expressway-E

Status System **Configuration** Applications Users Maintenance

Unified Communications You are here: [Configuration](#) > [Unified Communications](#) > Configuration

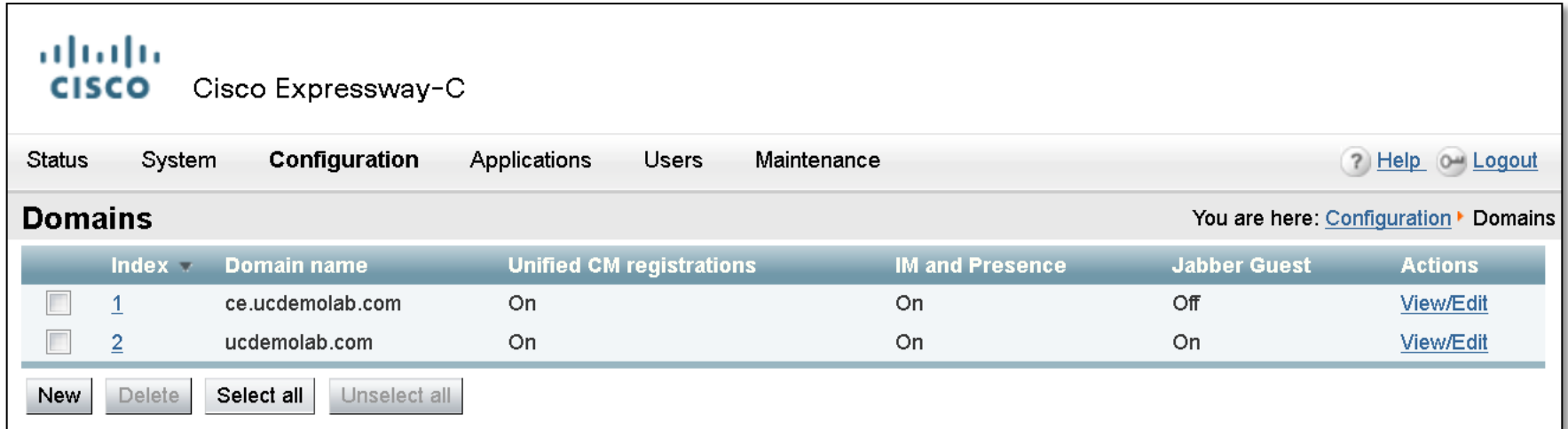
Configuration

Mobile and remote access On

Jabber Guest support On

Save

Expressway C Domain Configuration



The screenshot displays the Cisco Expressway-C configuration interface. At the top left is the Cisco logo and the text "Cisco Expressway-C". Below this is a navigation menu with tabs for "Status", "System", "Configuration" (which is selected), "Applications", "Users", and "Maintenance". To the right of the navigation menu are links for "Help" and "Logout".

The main content area is titled "Domains" and includes a breadcrumb trail: "You are here: Configuration > Domains". Below the title is a table with the following columns: "Index", "Domain name", "Unified CM registrations", "IM and Presence", "Jabber Guest", and "Actions".

Index	Domain name	Unified CM registrations	IM and Presence	Jabber Guest	Actions
<input type="checkbox"/> 1	ce.ucdemolab.com	On	On	Off	View/Edit
<input type="checkbox"/> 2	ucdemolab.com	On	On	On	View/Edit

Below the table are four buttons: "New", "Delete", "Select all", and "Unselect all".

- Note: No domain configuration required on Expressway E

Expressway C Traversal Client Zone

Edit zone

Configuration

Name ⓘ

Type

Hop count ⓘ

Connection credentials

Username ⓘ

Password ⓘ

H.323

Mode ⓘ

Protocol ⓘ

SIP

Mode ⓘ

Port ⓘ

Transport ⓘ

Mobile and remote access ⓘ

TLS verify mode ⓘ

Media encryption mode ⓘ

ICE support ⓘ

Poison mode ⓘ

Authentication

Authentication policy ⓘ

Client settings

Retry interval ⓘ

Location

Peer 1 address

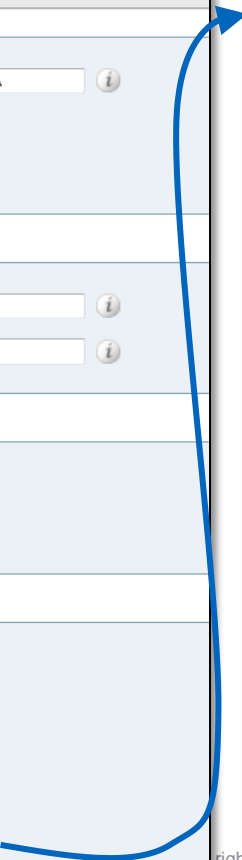
Peer 2 address

Peer 3 address

Peer 4 address

Peer 5 address

Peer 6 address



Expressway E Traversal Server Zone

Edit zone

Configuration

Name ⓘ

Type Traversal server

Hop count ⓘ

Connection credentials

Username ⓘ

Password [Add/Edit local authentication database](#)

H.323

Mode ⓘ

Protocol ⓘ

H.460.19 demultiplexing mode ⓘ

SIP

Mode ⓘ

Port ⓘ

Transport ⓘ

Mobile and remote access ⓘ

TLS

TLS verify mode ⓘ

TLS verify subject name ⓘ

Media encryption mode ⓘ

ICE support ⓘ [Configure TURN servers](#)

Poison mode ⓘ

Authentication

Authentication policy ⓘ

UDP / TCP probes

UDP retry interval ⓘ

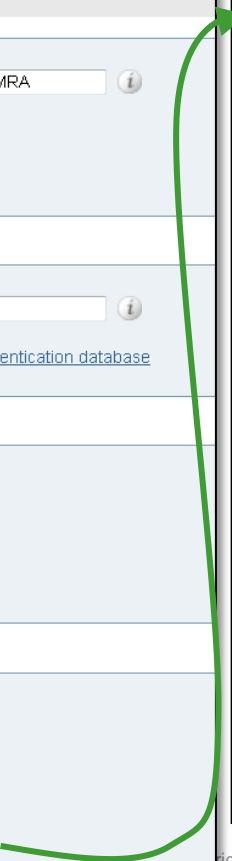
UDP retry count ⓘ

UDP keep alive interval ⓘ

TCP retry interval ⓘ

TCP retry count ⓘ

TCP keep alive interval ⓘ



Allowed Reverse Proxy Traffic

- Expressway E server will be listening on TCP 8443 for HTTPS traffic
- Basic mobile & remote access configuration allows inbound authenticated HTTPS requests to the following destinations on the enterprise network
 - All discovered CUCM nodes TCP 6970 (TFTP file requests) & TCP 8443 (UDS API)
 - All discovered IM&P nodes TCP 7400 (XCP Router) & TCP 8443 (SOAP API)
- HTTPS traffic to any additional hosts need to be added to the Exp-C allow list

Server hostname	Description	Actions
<input type="checkbox"/> cuc2.ucdemolab.com	CUC2 FQDN	View/Edit
<input type="checkbox"/> cuc1.ucdemolab.com	CUC1 FQDN	View/Edit

- Provides a mechanism to support Visual Voice Mail access, contact photo retrieval, Jabber custom tabs, etc.

Expressway C Unified Communications Status

- Status > Unified Communications

Unified Communications (last updated: 03:06:32 EST)

Unified Communications status	Enabled
Jabber Guest support	Enabled
Unified Communications services	Active
IM and Presence servers	2
Unified CM servers	3
Current provisioned sessions	0
Total provisioning requests since last restart	0
Total provisioned sessions since last restart	0
Unified CM calls	Current video: 0, Current audio (SIP): 0

Domains

Name	Services	Associated zones
ce.ucdemolab.com	Unified CM registrations, IM and Presence	Traversal Client MRA
ucdemolab.com	Unified CM registrations, IM and Presence, Jabber Guest	Traversal Client MRA

Zones

Name	Sip status
Traversal Client MRA	Active

Advanced status information

[View provisioning sessions](#)

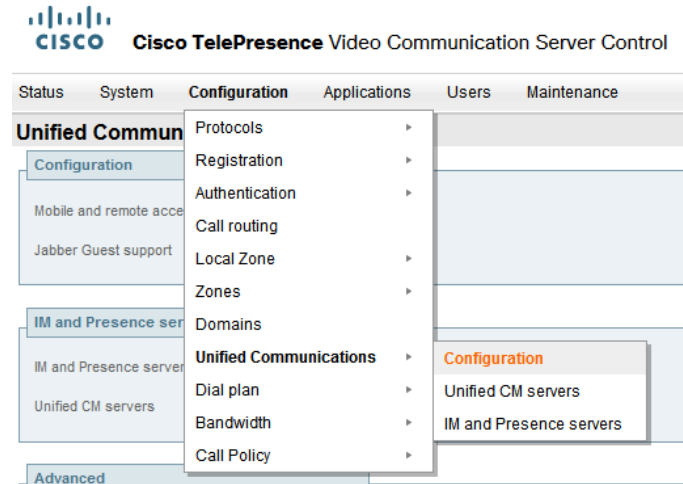
[View ssh tunnel status](#)

Supported Services with Collab Edge

- Instant Messaging and Presence – [Cloud & On Premise](#)
- Softphone Voice and Video Calls – [CUCM 9.0 +](#)
- Conferencing – [Audio and Video](#)
- Video Desktop Share – [BFCP](#)
- WebEx Desktop Share
- Visual Voicemail – [Using HTTP Whitelisting on Expressway-C](#)
- Installer Update - [Using HTTP Whitelisting on Expressway-C](#)
- Custom HTML Tabs - [Using HTTP Whitelisting on Expressway-C](#)
- Directory Search [UDS] – [Dictated by Edge Detection Service](#)
- Directory Photo Resolution - [Using HTTP Whitelisting on Expressway-C](#)

Mobile and Remote Access - Voicemail

- Jabber connects to Unity Connection over a REST interface to gather voicemail data to display in the visual voicemail tab
 - This is a HTTP connection and will not be allowed through the collaboration edge architecture by default.
- On the Expressway-C, we can create a HTTP whitelist which allows Jabber to send HTTP requests to specified internal hosts



Mobile and Remote Access

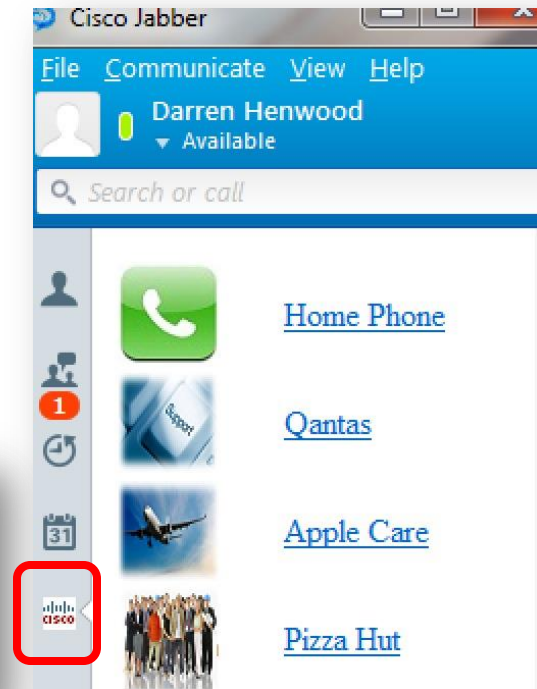
- What should we whitelist?
 - Unity Connection Server for Visual Voicemail
 - Directory photo server if using http server to deliver photos
 - HTML tab host e.g. company intranet html tab
 - HTML tab icon host
 - Jabber update host

HTTP server allow list

Success: Saved

Server hostname	Description
<input type="checkbox"/> ucxn1.example.com	Unity Connection Server
<input type="checkbox"/> icons.example.com	HTML Tab Icon Server
<input type="checkbox"/> companyintranet.example.com	HTML Tab Access to Intranet homepage
<input type="checkbox"/> photos.example.com	Photo Server

New Delete Select all Unselect all



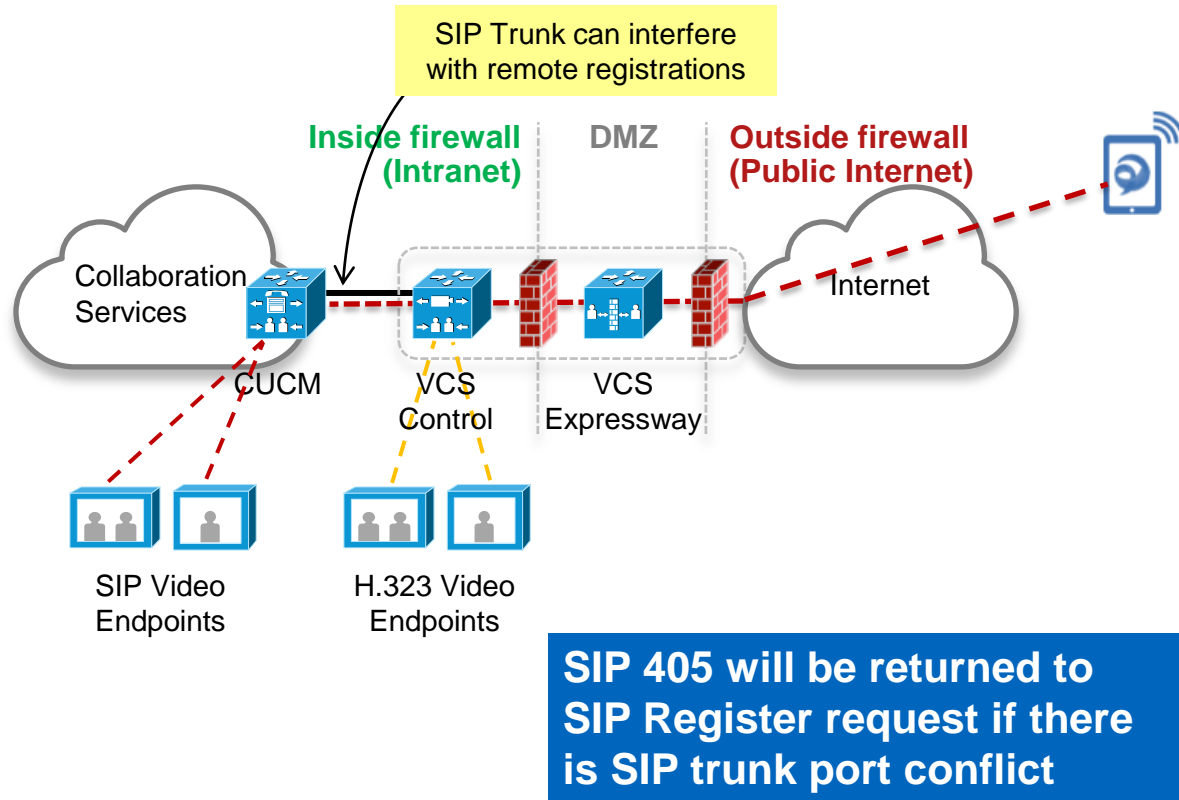


CUCM Requirements

Expressway Remote Access from CUCM Perspective

- Remote access provided by Expressway is, for the most part, **transparent** to CUCM
- Think SIP line integration, versus SIP trunk
- No requirement to build a SIP trunk on CUCM to Expressway C or E
- No requirement to make dial plan changes
- No remote access policy mechanism to limit edge access to certain Jabber users or devices
- Remote Jabber clients or TelePresence Endpoints registering to CUCM through Expressway will appear to CUCM as Expressway-C IP address (opportunity for CUCM Device Mobility feature usage)

Interaction with SIP Trunk



- SIP trunk is **not required** between Expressway C (or VCS-C) and CUCM for Mobile & Remote Access
- However, if CUCM includes a SIP trunk for other integrations, **CUCM will reject any SIP registration attempts from remote Jabber or TP endpoints**, as the register method is not accepted on CUCM SIP trunk interface
- **Update CUCM SIP trunk security profile to listen on ports other than TCP 5060 or 5061 (you could use 5560, 5561, etc.)**
- Port change allows SIP trunk integration + mobile & remote access

Debugging (Logs)

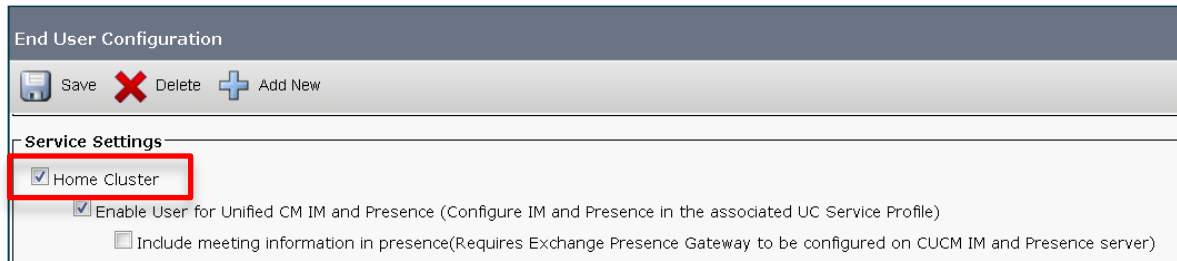
- Check lossy network connection
 - Search string “RTP STATS”

```
[media::rtp::SessionImpl::logRtpStatsWithLock] - RTP STATS,session_id=6,session_type=audio-main,rx_bytes_rcv=3920,rx_pkts_rcv=49,rx_pkts_lost=0,rx_curr_loss=0.00%,rx_cum_loss=0.00%,rx_bitrate=1,rx_jitter=2,rx_fec_pkts_rcv=49,rx_fec_pkts_lost=0,rx_fec_curr_loss=0.00%,rx_fec_cum_loss=0.00%,tx_bytes_sent=3920,tx_pkts_sent=49,tx_pkts_rcv=9,tx_pkts_lost=0,tx_curr_loss=0.00%,tx_cum_loss=0.00%,tx_bitrate=1,tx_jitter=2,tx_round_trip=113,tx_last_ssrc=7547D352,tx_last_ext_high_seq=4321,tx_received_rb=1,tx_active_sources=1,tx_total_sources=1
```

- Search string “steady_state_adaption”
 - [steady_state_adaption, Sender_side] Network IS_CONSISTENTLY_LOSSY. New sending bitrate will be hard reduction to 302kbps.

UDS Directory Search

- All Jabber clients connecting via Expressway will use UDS for directory search (assuming CUCM IM&P deployment)
- TelePresence endpoints always use UDS for directory search
- For the best contact search experience, all Enterprise Users should be imported into every CUCM cluster's end user table
- Home cluster check box needs to be selected on only one cluster for each user



- CUCM clusters support 80K end users, and can scale as high as 160K with BU megacluster approval



Security

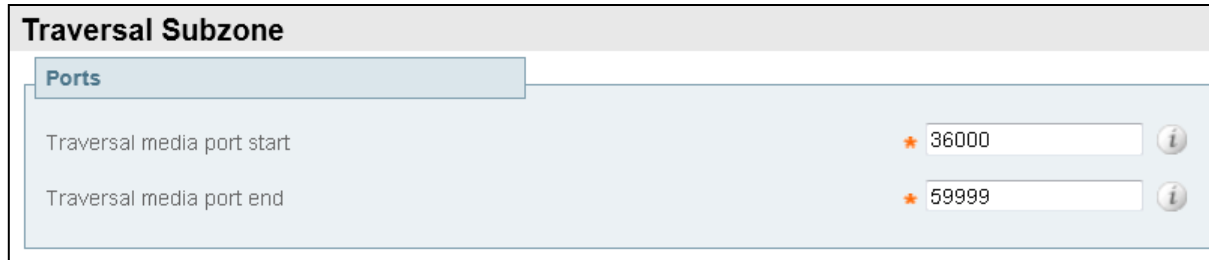
Firewall Port Details

- **No inbound ports required to be opened on the internal firewall**
- Internal firewall needs to allow the following outbound connections from Expressway C to Expressway E
 - SIP: TCP 7001
 - Traversal Media: UDP 36000 to 36011
 - XMPP: TCP 7400
 - HTTPS (tunneled over SSH between C and E): TCP 2222
- External firewall needs to allow the following inbound connections to Expressway
 - SIP: TCP 5061
 - HTTPS: TCP 8443
 - XMPP: TCP 5222
 - Media: UDP 36002 to 59999
 - TURN server control: UDP 3478 – 3483
 - TURN server media : UDP 24000 – 24999

Jabber Guest, not required for Mobile & Remote Access

Media Port Range Expansion

- X8.1 scalability improvements require a media port range expansion
- X8.1 default media Port Range is now UDP 36000 – 59999
- VCS systems upgraded from X7 to X8.1 will need to manually update port range, Configuration > Local Zone > Traversal Subzone



The screenshot shows a configuration window titled "Traversal Subzone". Inside, there is a "Ports" section with two input fields. The first field is labeled "Traversal media port start" and contains the value "36000". The second field is labeled "Traversal media port end" and contains the value "59999". Both fields have a red asterisk icon to their left and an information icon to their right.

Field Label	Value
Traversal media port start	36000
Traversal media port end	59999

Traversal Media Port Changes

Important change for existing VCS customers to understand

- X7 release included the ability to configure the Expressway Media demultiplexing RTP port and RTCP port

Ports	
Configuration	
Media demultiplexing RTP port	★ 2776 ⓘ
Media demultiplexing RTCP port	★ 2777 ⓘ
H.323 Assent call signaling port	★ 2776 ⓘ
H.323 H.460.18 call signaling port	★ 2777 ⓘ

Configuration Removed
in X8.1

- Upon upgrading to X8.1 the traversal media ports are automatically migrated to the first 2 ports in the current media port range (details on previous slide)
- Customers will need to coordinate X8.1 upgrade with firewall port change
- New X8.1 installs on the Large OVA will use UDP 36000 – 36011, the expanded port range is required to support scalability improvements

Edge Server Authentication

- No matter which client authentication model is deployed, server authentication is always performed by the remote device
- i.e. remote Jabber clients and remote endpoints will always validate the Expressway E Server Certificate presented in the TLS handshake
- Jabber Clients will rely on the underlying platform trusted CA list
- TelePresence Endpoints will rely on a trusted CA list included in firmware
- No CTL requirement for Edge Server authentication



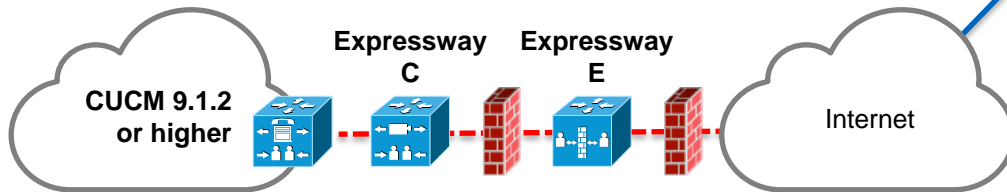
High Level Deployment Guidance

- Start on solid ground
 - Jabber service discovery needs to work on-premise
 - Start on-premise and then add edge access
 - Verify end user home cluster discovery in multi CUCM cluster deployments
- Don't forget about DNS
 - Understand split DNS SRV requirements, get DNS change requests in the queue
 - A common DNS domain simplifies matters
- Review TCP and UDP port requirements with firewall team
- Verify Expressway CA signed certs
 - Confirm SANs returned in CA signed cert match what was requested in the CSR
 - Verify cert includes both TLS Web **Server & Client** Authentication Extended Key Usage

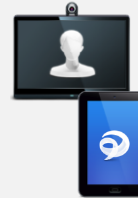


Licensing and Scalability

Cisco Expressway Licensing

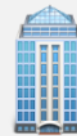


Fixed and Mobile Users at no additional cost



- Mobile and Fixed Endpoint registration
- IM & Presence
- Video and Audio Media Sessions
- Includes Virtual Edition Expressway Server Software
- **No Cost with CUCM 9.1.2 or later**

Business to Business, Jabber Guest, 3rd party interworking – Concurrent Sessions



- Business to Business Video and Audio Media Sessions
- Includes Virtual Edition Expressway Server Software
- **Expressway Rich Media Session licenses available a la carte**

Expressway: Unified CM Calls

- Calls from endpoints using the Mobile and Remote Access feature are classified as **Unified CM calls**
- Unified CM calls do not consume Rich Media Sessions (Expressway) or Traversal Licenses (VCS)
- But Unified CM Calls do count against the overall system capacity

Resource usage (last updated: 21:08:20 PST)		
		Total
Unified CM calls	Current video	0
	Current audio (SIP)	0
	Peak video	4
	Peak audio (SIP)	1
Rich media session traversal calls	Current video	0
	Current audio (SIP)	0
	Peak video	0
	Peak audio (SIP)	0
Rich media session non-traversal calls	Current	0
	Peak	0
Monitored resource usage	Current	0
Rich media sessions	License usage current	0%
	License usage peak	0%

Flexible Call Licensing

- X8.1 introduces audio-only classification for SIP traversal or Unified CM calls
- Calls with only one m= line in the SDP will be classified as Audio calls
- 1 Expressway Rich Media Session license allows either 1 video call or 2 audio-only SIP calls
- 1 VCS Traversal license allows either 1 video call or 2 audio-only SIP calls
- Example:
 - 100 VCS Traversal licenses allows for
 - 90 video and 20 audio-only simultaneous calls

```
Session-Expires: 1800
Allow-Events: dialog Recv-Info: x-cisco-conference
Content-Type: application/sdp
Content-Length: 237
v=0
o=tandberg 7 3 IN IP4 182.16.1.115
s=-
c=IN IP4 182.16.1.115
b=AS:64
t=0 0
m=audio 2336 RTP/AVP 8 0 101
b=TIAS:64000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

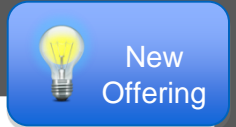
New Compute Platforms for X8

Specs Based Virtual Machine Support

OVA Size	vCPU	Reserved RAM	Disk Space	vNIC(s)
Small	2 x 1.8 GHz	4GB	132GB	1Gb
Medium	2 x 2.4 GHz	6GB	132GB	1Gb
Large	8 x 3.3 GHz	8GB	132GB	10Gb

Appliance Support

Existing VCS Appliance



CE 500



CE 1000



- New appliances based on UCS C220 M3
- Bare metal – no hypervisor
- Fixed configurations for high and low end deployment
- Solution for customers with security policies that do not allow VMware in the DMZ
- CE500 Single components, 1Gbps interfaces
- CE1000 Redundant components, 1 or 10Gbps

Expressway X8.1 Scalability

	Server			Cluster		
Platform	Proxied Registrations	Video Calls	Audio Only Calls	Proxied Registrations	Video Calls	Audio Only Calls
Large OVA	5,000	500	1,000	20,000	2,000	4,000
Medium OVA	2,500	100	200	10,000	400	800
Small OVA (BE6K)	2,500	100	200	2,500	100	200
VCS Appliance	2,500	100	200	10,000	400	800

Note: Expressway C&E or VCS-C can be clustered across multiple BE6000s for redundancy purposes, but with no additional scale benefit

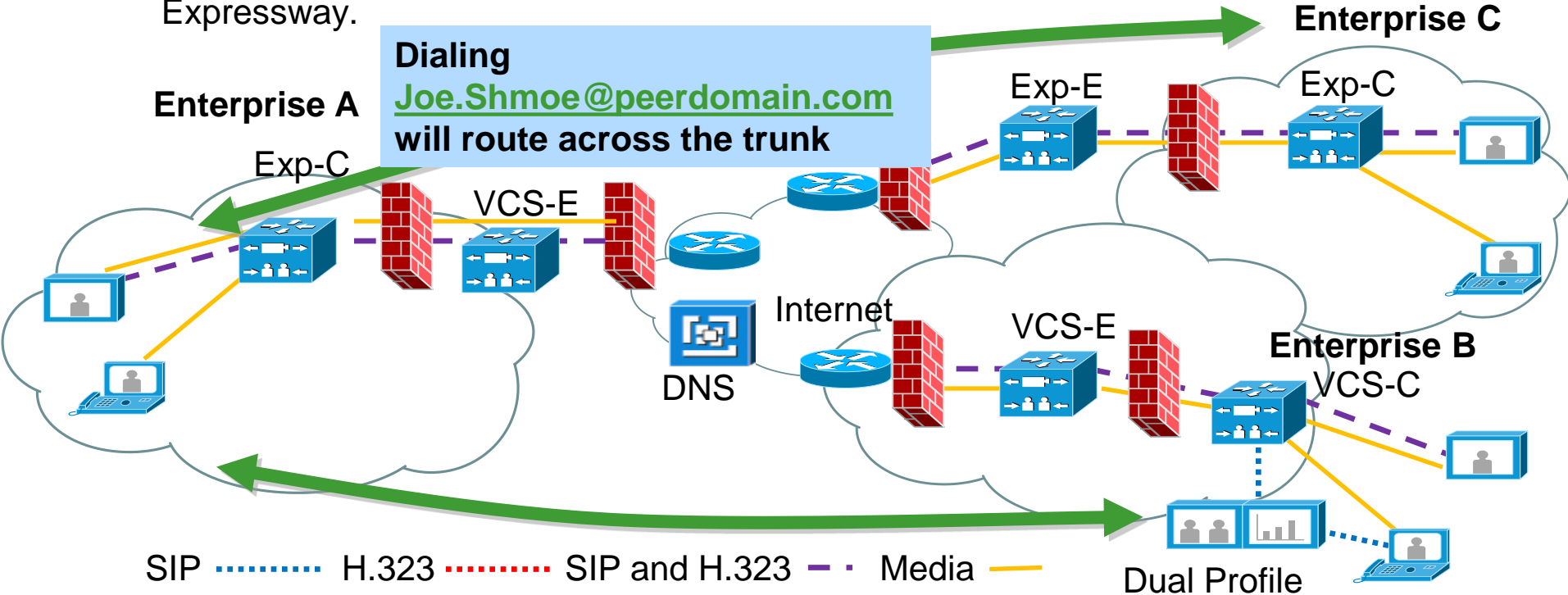
Expressway Rich Media Session Licenses

- Rich Media Session is the only session license type sold with Expressway (simple!)
- Rich Media Session licenses are consumed for either traversal or non-traversal call types
- A traversal call will require a Rich Media Sessions license on both the Expressway E and Expressway C
- Mobile and Remote Access Feature has **no requirements** for Rich Media Sessions licenses
- Rich Media Sessions should be purchased for Expressways deployed for
 - B2B Video
 - Jabber Guest
 - 3rd party video interworking

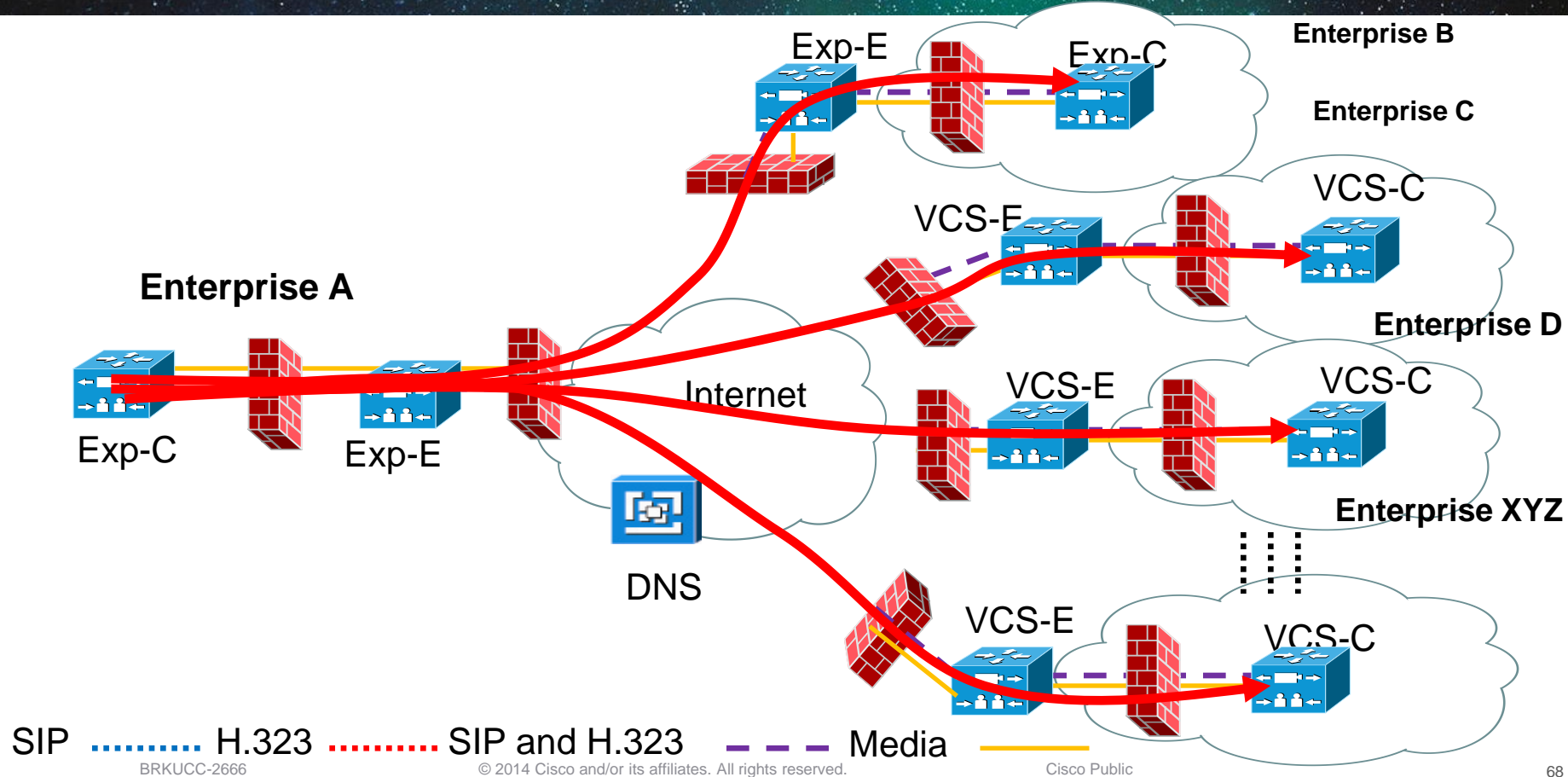


Direct Peering Model – B2B Communications

The relationship (trunk) between the companies is configured using the domain of the peer, i.e. calls to *@peerdomain.com will be routed over the trunk to the peer VCS Expressway.



Open Internet Model – B2B Communications



Expressway License Keys

License Description	PID	Expressway C (EXPWY-VE-C-K9)	Expressway E (EXPWY-VE-E-K9)
X8 Release Key	LIC-SW-EXP-K9	Included	Included
Expressway Series	LIC-EXP-SERIES	Included	Included
H323-SIP interworking Gateway	LIC-EXP-GW	Included	Included
Traversal Server Feature Set	LIC-EXP-E	N/A	Included
Advanced Networking Option	LIC-EXP-AN	N/A	Included
TURN Relay Option	LIC-EXP-TURN	N/A	Included
Expressway Rich Media Session	LIC-EXP-RMS	Optional	Optional
Microsoft Interoperability Option	LIC-EXP-MSFT	Optional	N/A

Expressway Series Roadmap

Subject to change
Roadmap

X7.2 (Shipping)

Edge Features:

- SRTP-to-RTP Conversion
- Enhanced certificate management
- Access Control Lists
- Controlled TLS
- Scale (AES-NI support)

Available Now Remote and Mobile Collaboration:

- Simple, secure, scalable collaboration
- Connect remotely with Jabber and TC endpoints
- Register directly to CUCM 9.1.2 (or better)
- Voice, Video, IM&P, Directory, Visual Voicemail outside the network without a VPN
- AVC-SVC gateway: Lync 2013 Interop

1HCY14 (to be committed)

Remote and Mobile Collaboration:

- Additional endpoint support: DX Series
- Enhanced Mobility Support incl. DVO
- Single Sign-On Support
- Media Path Optimisation (ICE)
- Inter-domain XMPP Federation
- Inter-company AVC-SVC gateway

2HCY14 (under investigation)

Remote and Mobile Collaboration:

- Streamlined provisioning, management, and alarm handling
- Granular Policy Control
- RDP interop



Q&A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

www.CiscoLiveAPAC.com



CISCO™

Unsupported Features

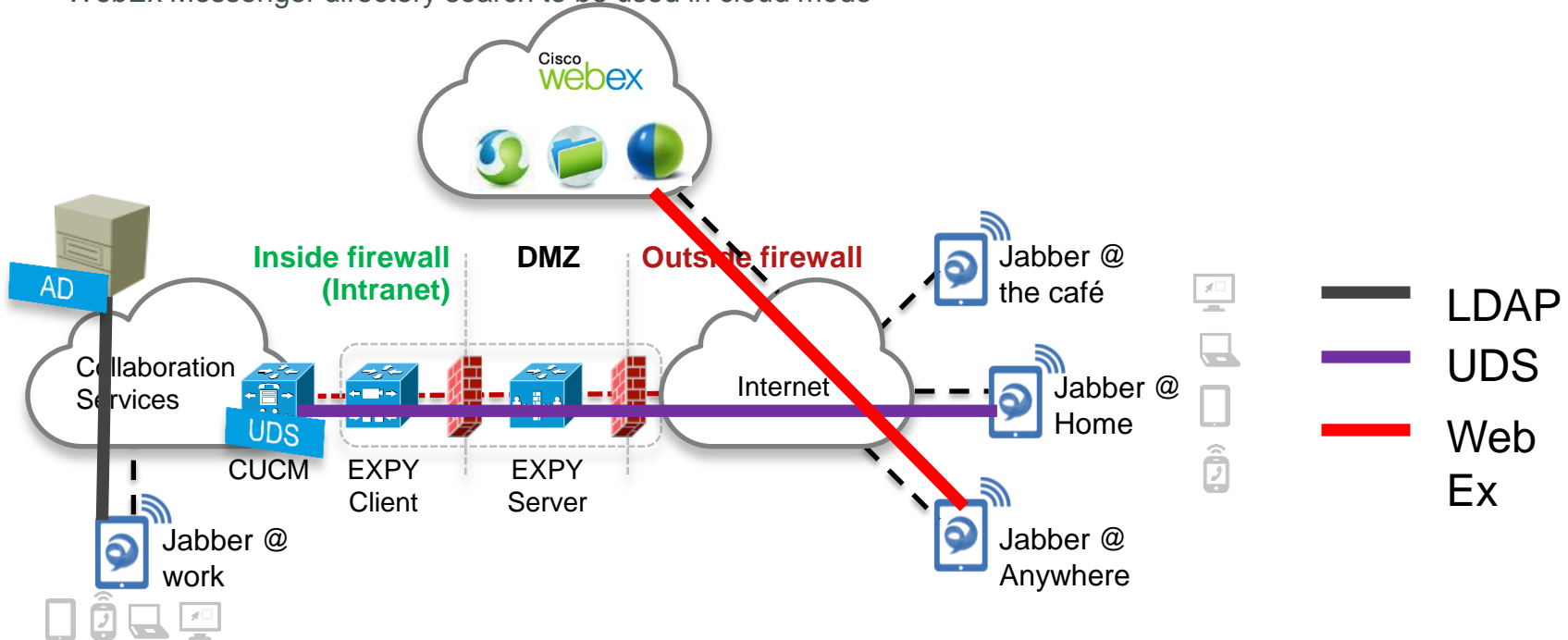
- CTI phone control
- CAPF client certificate provisioning
- Jabber file transfer (supported only in hybrid IM&P deployment)
- Jabber Mobile features include DVO-R, GSM handoff, session persistency
- TC Endpoint OBTP
- TC Endpoint management (SNMP, SSH/HTTP access)
- Media Path Optimisation (ICE)

Directory Integration Update

- Cisco recommends Enhanced Directory Integration for deployments of Jabber for Windows
- Recommendation is in order to ensure scalability of the solution for our Enterprise customers.
- Existing Jabber 9.2 UDS deployments will continue to receive TAC support
 - Jabber 9.6 will only use UDS in edge mode
- 9.2 UDS deployments should not exceed 200 users per cluster.
- Additional UDS capacity will be available in upcoming Jabber and CUCM releases
 - Batch API
 - Distributed Caching Refresh

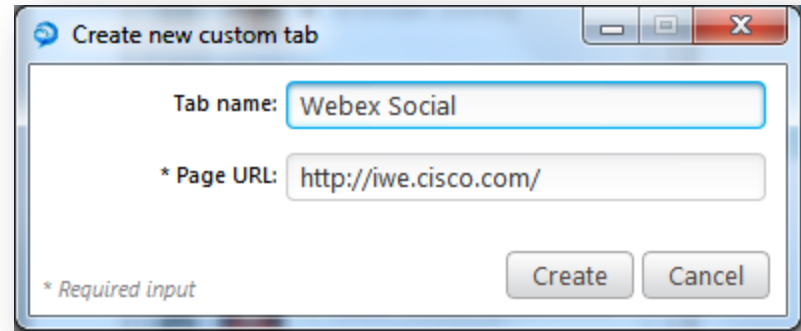
Directory Search in 9.6/9.7

- LDAP directory integration to be used in on premise mode
- UDS integration to be used in edge mode [for on-premise deployments]
- WebEx Messenger directory search to be used in cloud mode

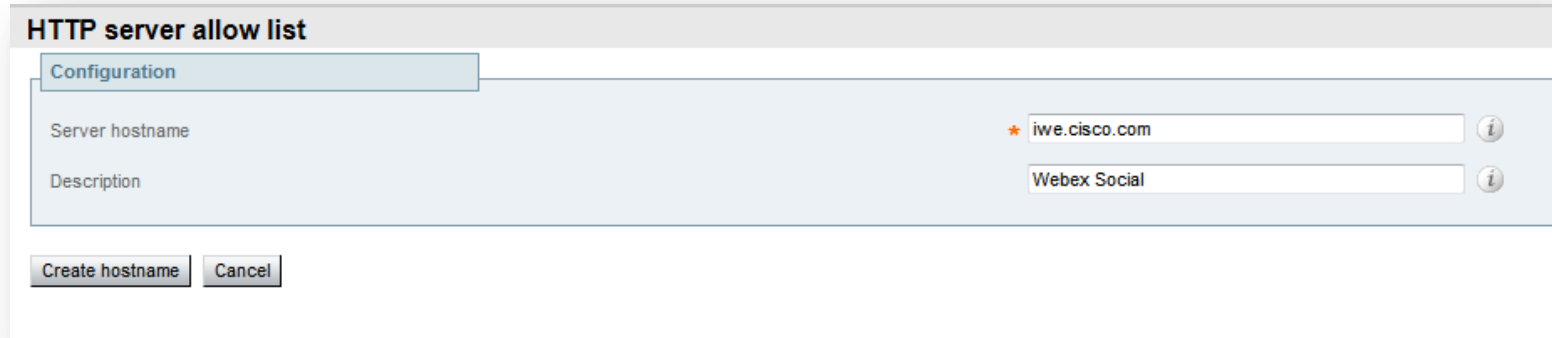


HTML Tabs White List

- HTML Tabs are supported through Collaboration Edge
- Create whitelist on Expressway-C
 - Specify host



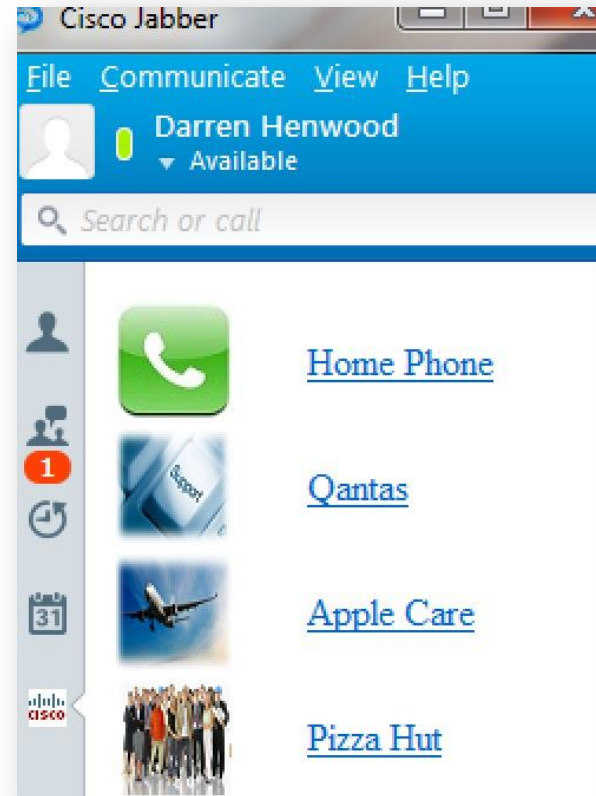
A screenshot of a dialog box titled "Create new custom tab". It contains two input fields: "Tab name:" with the value "Webex Social" and "* Page URL:" with the value "http://iwe.cisco.com/". The asterisk indicates that the Page URL is a required input. At the bottom right, there are "Create" and "Cancel" buttons. A small asterisk and the text "* Required input" are located at the bottom left of the dialog box.



A screenshot of a configuration window titled "HTTP server allow list". It has a "Configuration" tab selected. The window contains two input fields: "Server hostname" with the value "iwe.cisco.com" and "Description" with the value "Webex Social". Both fields have an information icon (i) to their right. At the bottom left, there are "Create hostname" and "Cancel" buttons.

What to Whitelist?

- Visual Voicemail
- Directory Photo Host
- Jabber Update Server
- HTML Tabs
- HTML Tab Icons
- Webmail



Reverse Proxy Usage

Initial get_edge_config and internal SRV record request (decrypted)

```
GET /dWNkZW1vbGFiLmNvbQ/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin HTTP/1.1
Authorization: Basic bWR1ZGU6dGhpc3Bhc3N3ZHdpbGxiZXJlc2V0
Host: collabedge1e.ucdemolab.com:8443
Accept: */*
User-Agent: Jabber-Win-472
```

Base64 encoded credentials

Base64 decode = ucdemolab.com

Subsequent home cluster discovery request (decrypted)

```
GET /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWntLXB1Yi51Y2R1bW9sYWl0Y29tLzg0NDM/cucm-uds/clusterUser?username=mdude HTTP/1.1
Host: collabedge1e.ucdemolab.com:8443
Accept: */*
Cookie: X-Auth=7f501814-e61f-483a-8620-ed0b5d3792db
User-Agent: Jabber-Win-472
```

X-Auth token

Base64 decode = ucdemolab.com/https/cucm-pub.ucdemolab.com/8443



Not a general purpose reverse proxy, intended for Cisco clients only!

Home Cluster Discovery

- Expressway C will use the following UDS API to determine a user's home cluster



<https://<CUCM>/cucm-uds/clusterUser?username=<USERNAME>>

```
- <clusterUser uri="https://cucm1-1.eft.cisco.com:8443/cucm-uds/clusterUser?username=mjackson" version="9.1.2">  
  <result version="10.0.1" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/user/mjackson" found="true"/>  
  <homeCluster>cucm2-1.eft.cisco.com</homeCluster>  
</clusterUser>
```



CUCM 9.1.2

```
- <clusterUser version="10.0.1" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/clusterUser?username=mjackson">  
  <result found="true" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/user/mjackson" version="10.0.1"/>  
  <homeCluster serversUri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/servers">cucm2-1.eft.cisco.com</homeCluster>  
  <homeClusterDetails>  
    <selfProvisioningSecureMode>true</selfProvisioningSecureMode>  
    <adminProvisionMode>>false</adminProvisionMode>  
  </homeClusterDetails>  
</clusterUser>
```



CUCM 10.0



Expressway Server Certificates

Expressway Server Certificates

- Expressway E Server certificates should be signed by 3rd party Public CA
- Expressway C server certificates can be signed by 3rd party Public CA or Enterprise CA
- Expressway server certificates need to allow for both client & server authentication

X509v3 Extended Key Usage:
TLS Web Client Authentication
TLS Web Server Authentication

X.509v3

- Public CA signed certificates allow Jabber clients and endpoints to validate the server certificate without a CTL
- Jabber clients with a CTL will not use the CTL to validate Expressway certificate - no requirement to include Expressway certs in CTL
- No support for wildcard certificates
- Don't upload stacked certificates, separate signed server cert from CA chain

Expressway Certs and Clustering

- Set a cluster name (System > Clustering) even when starting with a single node
- Generate server certificate CSR with Common Name set to “FQDN of VCS Cluster”

Status System Configuration Applications Users Maintenance

Generate CSR

Common name

Common name FQDN of VCS cluster ⓘ

Common name as it will appear cluster.collabedge1c.ucdemolab.com


- Build Expressway E Traversal Server zone with the “TLS verify subject name” set to “Cluster FQDN”

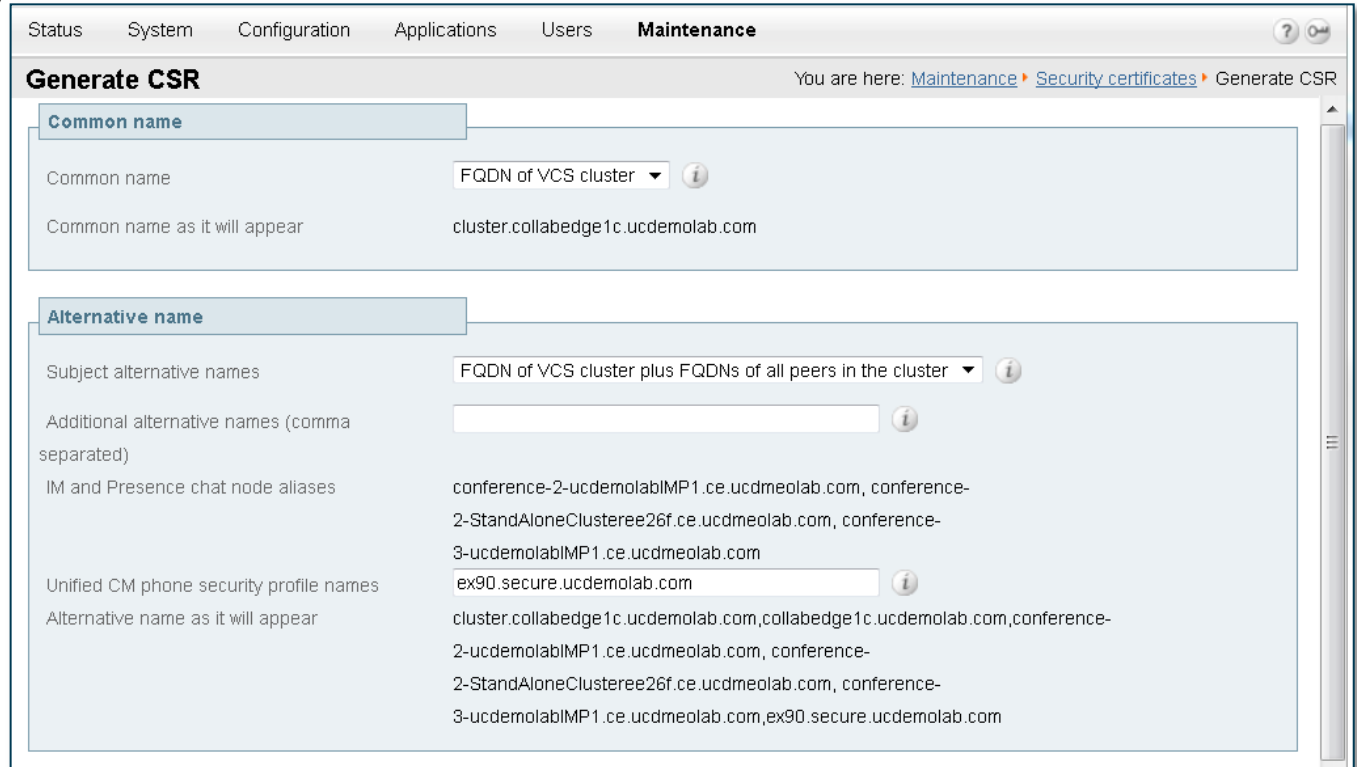
TLS verify mode On ⓘ

TLS verify subject name ★ cluster.collabedge1c.ucdemolab.com ⓘ

Expressway Certificate Signing Request (CSR)

Maintenance > Security Certificates > Server Certificate

Click  to load this page ----->



The screenshot shows the 'Generate CSR' configuration page in the Cisco Expressway interface. The breadcrumb trail is 'Maintenance > Security Certificates > Generate CSR'. The page is divided into two main sections: 'Common name' and 'Alternative name'.

Common name section:

- Common name:** FQDN of VCS cluster (dropdown menu)
- Common name as it will appear:** cluster.collabedge1c.ucdemolab.com

Alternative name section:

- Subject alternative names:** FQDN of VCS cluster plus FQDNs of all peers in the cluster (dropdown menu)
- Additional alternative names (comma separated):** (empty text field)
- IM and Presence chat node aliases:** conference-2-ucdemolabIMP1.ce.ucdmeolab.com, conference-2-StandAloneClusteree26f.ce.ucdmeolab.com, conference-3-ucdemolabIMP1.ce.ucdmeolab.com
- Unified CM phone security profile names:** ex90.secure.ucdemolab.com
- Alternative name as it will appear:** cluster.collabedge1c.ucdemolab.com,collabedge1c.ucdemolab.com,conference-2-ucdemolabIMP1.ce.ucdmeolab.com, conference-2-StandAloneClusteree26f.ce.ucdmeolab.com, conference-3-ucdemolabIMP1.ce.ucdmeolab.com,ex90.secure.ucdemolab.com

Cert Subject Alternative Name (SAN) Requirements

- Customer's primary domain required to be included as a DNS SAN in all Expressway E server certificates
- Primary domain as in **example.com** or **cisco.com** or
`DNS X509v3 Subject Alternative Name: DNS:ucdemolab.com`
- This domain is used for SRV lookups and extracted from here
- This is a security measure that allows clients to verify connections to edge servers authoritative for their domain (RFC 6125)
- Similar usage exists with CUCM IM&P XMPP certificates



CUCM Mixed Mode & Expressway SANs

- Expressway C Server Certificate Generation CSR page will also include the option to include CUCM security profile names as additional SANs

DNS X509v3 Subject Alternative Name: DNS:secure.ex90.ucdemo1ab.com

- This is **only required in deployments that include encrypted security profiles** (requires CUCM to be in mixed mode with CTL deployed)
- The Expressway C server certificate will be presented to CUCM during the TLS handshake on behalf of remote endpoints with encrypted security profiles
- UCM needs to find a match between the Expressway certificate's CN or SAN and the phone security profile name to authorise the TLS registration on TCP 5061
- CUCM phone security profile names cannot be shared across device types

Optional SANs for Future Usage

- The Expressway Server Certificate Generate CSR page will also insert “**chat node aliases**” as SANs
- These specific SANS will allow for **TLS XMPP federation**

X509v3 Subject Alternative Name: DNS:conference-2-StandAloneCluster9c265.ucdemo1ab.com

- There will be 1 chat node alias per deployed CUCM IM&P server
- Expressway XMPP federation is still a roadmap feature, but this inclusion will potentially save customers from having to get new certificates signed in the future when deploying XMPP federation

X.509v3

Expressway Trusted CA Certificates


- Trusted CA certificates can now be viewed in either a decoded human-readable format, or in base64 encoded PEM format
- X8.1 release will **not** include the default trusted CA certificate list
- VCS customers upgrading from X7 or prior should consider purging this list

Trusted CA certificate You are here: [Maintenance](#) > [Security certificates](#) > Trusted CA certificate

Type	Issuer	Subject	Expiration date	Validity	View	
<input type="checkbox"/>	Certificate	O=Digital Signature Trust Co., CN=DST Root CA X3	O=Cisco Systems, CN=Cisco SSCA2	Oct 22 2015	Valid	View (decoded)
<input type="checkbox"/>	Certificate	O=Cisco, OU=CTG-TME, CN=kroarty-lab	Matches Issuer	Jul 18 2016	Valid	View (decoded)
<input type="checkbox"/>	Certificate	O=Digital Signature Trust Co., CN=DST Root CA X3	Matches Issuer	Sep 30 2021	Valid	View (decoded)













[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)

Upload

Select the file containing trusted CA certificates [Browse...](#) No file selected. 

[Append CA certificate](#) [Reset to default CA certificate](#)

Expressway Trusted CA Certificates

Certificate Type	Expressway C	Expressway E	Comments
Public CA cert chain used to sign Expressway E certificate			Required to establish Traversal Zone connections
Public or Enterprise CA cert chain used to sign Expressway C certificate			Required to establish Traversal Zone connections
CUCM Tomcat certificates or CA chain			Only required when Expressway C configured to use TLS Verify mode on Unified CM discovery
CUCM CallManager certificates or CA chain			Only required when CUCM is in mixed mode for end to end TLS
CUCM IM&P Tomcat certificates or CA chain			Only required when Expressway C configured to use TLS Verify mode on IM&P discovery
CUCM CAPF certificate(s)			Only required when remote endpoints authenticate with LSC certificate



CISCO™