cisco Live!

#CiscoLive

cisco The bridge to possible

Enabling Collaboration for Your Remote Workforce with Cisco Expressway

Part I

Luis Garcia

BRKCOL-2060a

Agenda

- Introduction
- Cisco Expressway
- Mobile and Remote Access
- MRA Setup
- Conclusion

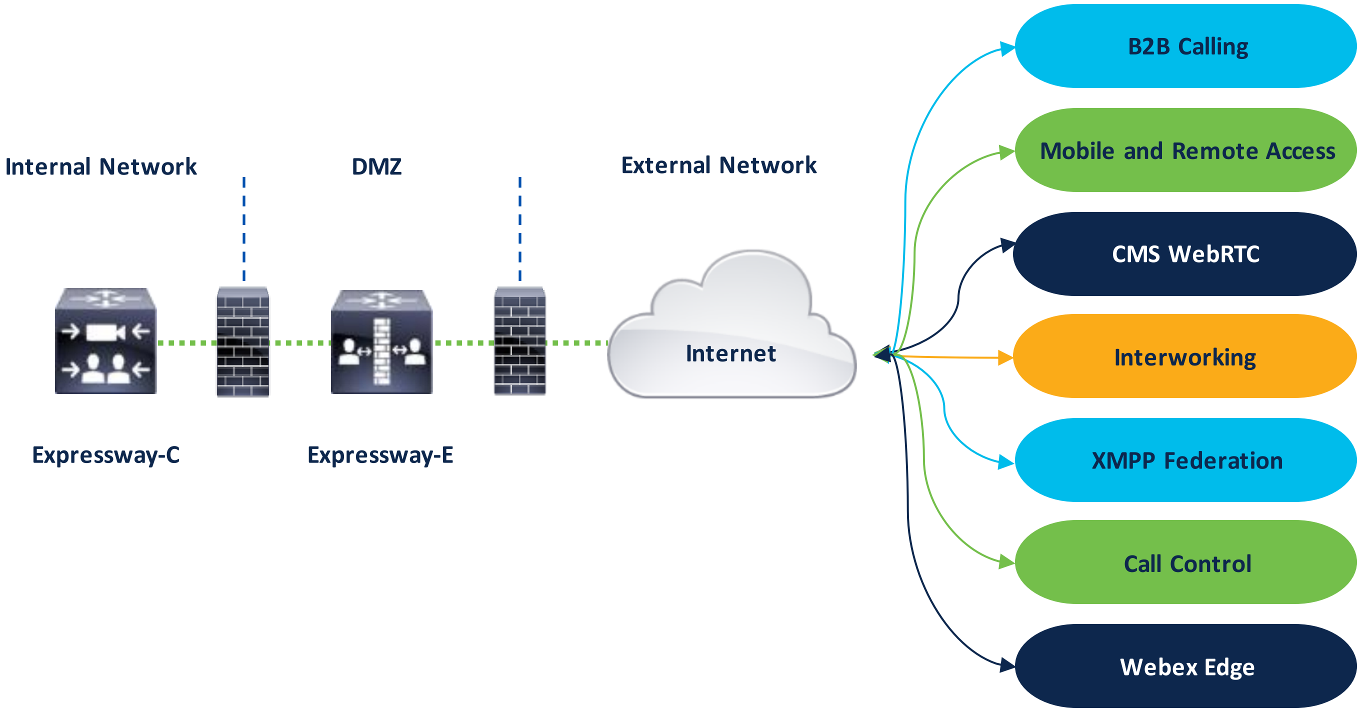
Introduction

Remote Workforce

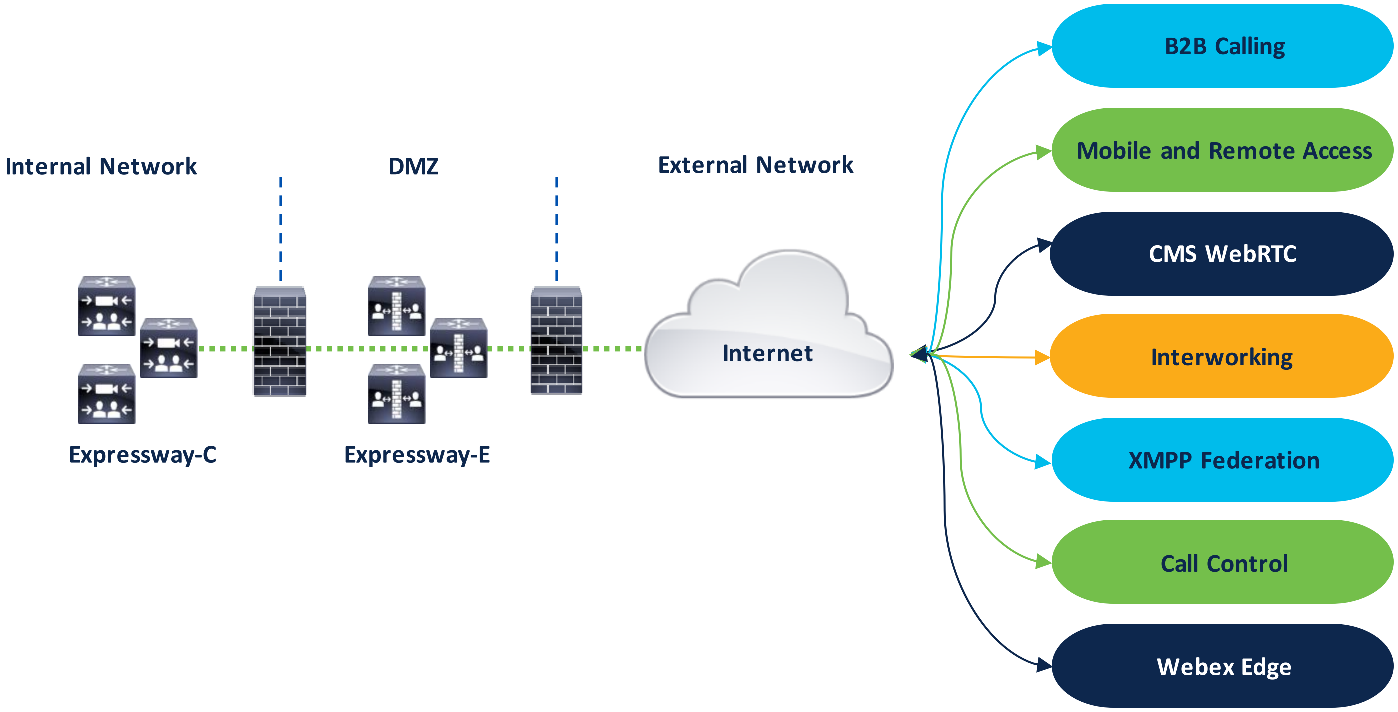
- Since COVID the number of employees working remotely grew exponentially.
- Companies with On-Premises deployments required a reliable and secure way to connect remote workers.
- Most companies will continue to adopt a hybrid work model, allowing employees to work from home or the office.

Cisco Expressway

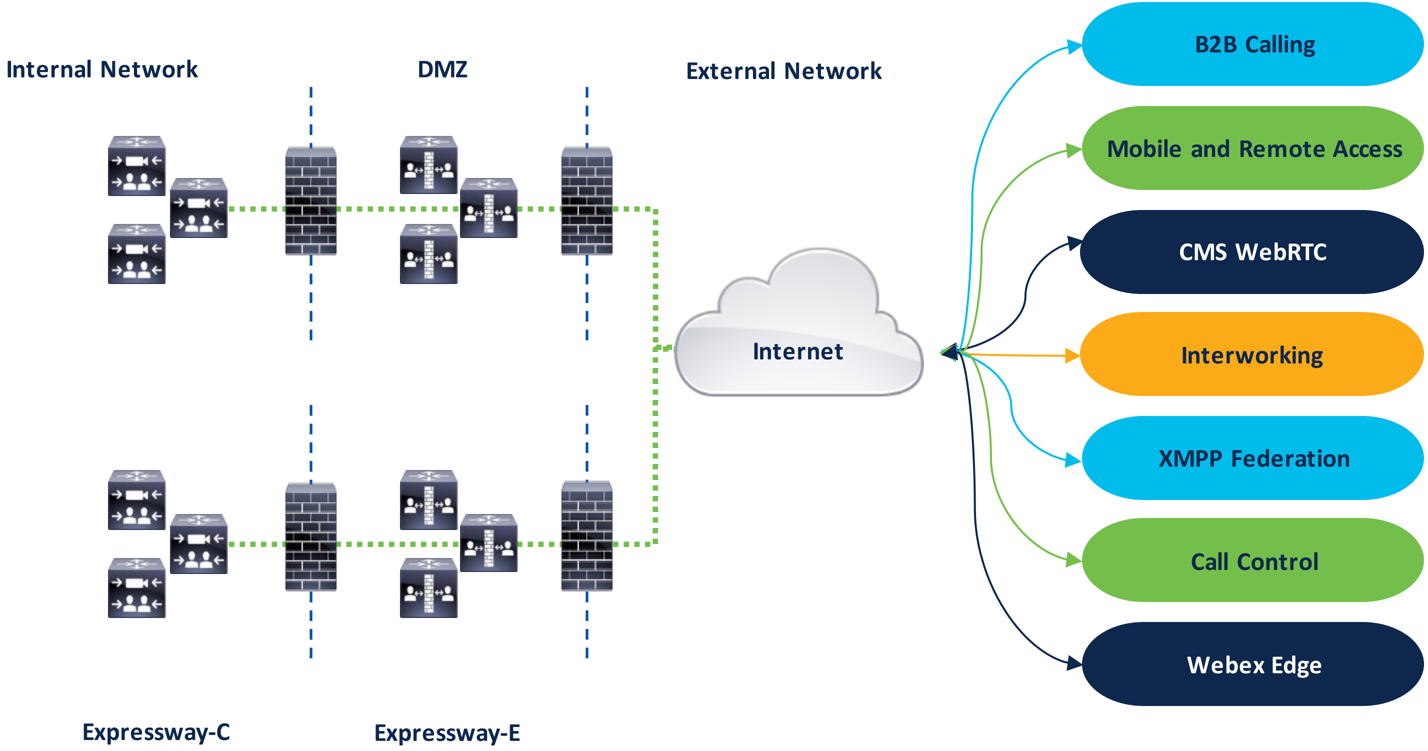
Expressway Deployments



Expressway Deployments



Expressway Deployments



Why Expressways?

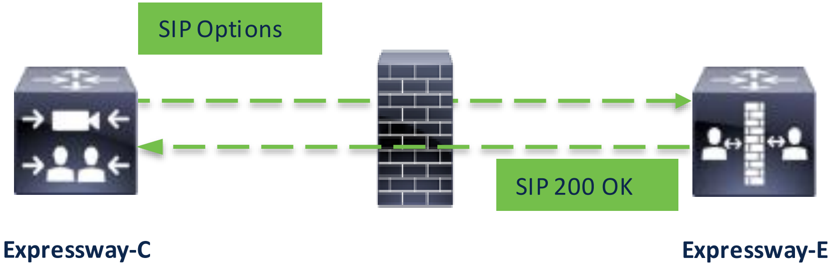
Security

- Enables encrypted communication from the corporate network to remote employees.
- Joint Interoperability Test Command (JITC) certified.
- FIPS 140-2 Level 1 compliant.
- Common Criteria (CC) accredited and Commercial Solutions for Classified (CSfC) accredited.
- Bare metal appliance (CE1200) available for secure deployments.

Why Expressways?

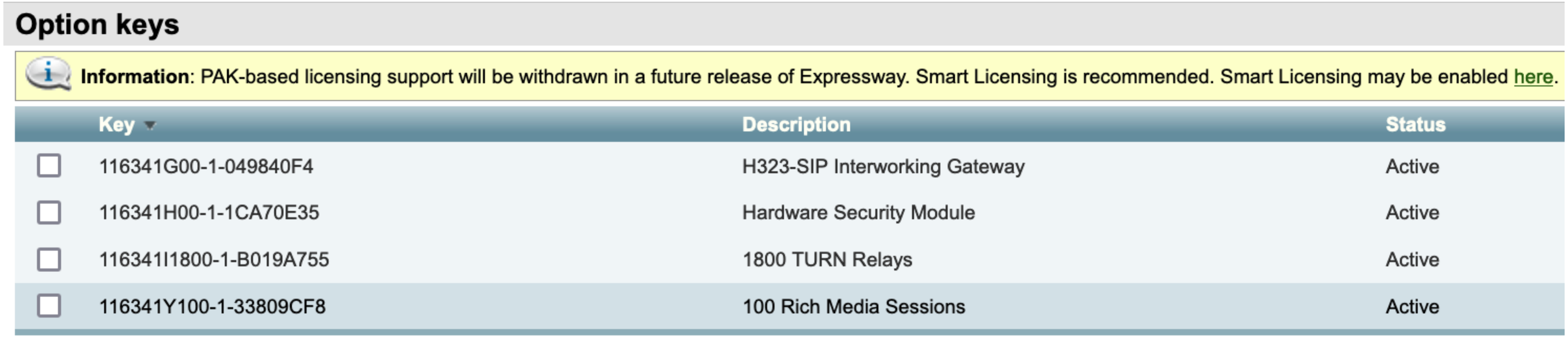
Firewall Traversal

- The traversal client constantly maintains a connection through the firewall to a designated port on the traversal server.
- There's no need to open inbound ports on the internal Firewall.



Licensing X12.6 – X14.0

- Smart Licensing was introduced in version X12.6.
- Expressway supports PAK based licensing (regular option keys) and Smart Licensing. Only one mode at any given time.

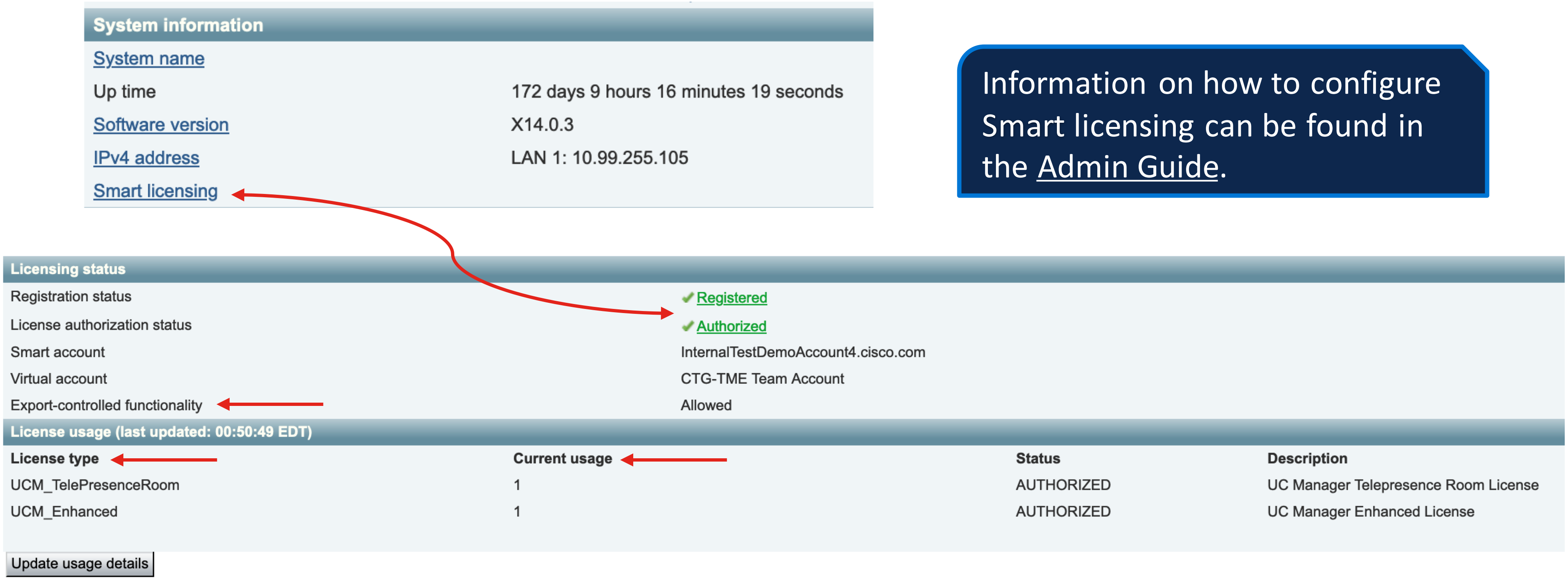


Option keys

Information: PAK-based licensing support will be withdrawn in a future release of Expressway. Smart Licensing is recommended. Smart Licensing may be enabled here.

	Key	Description	Status
□	116341G00-1-049840F4	H323-SIP Interworking Gateway	Active
□	116341H00-1-1CA70E35	Hardware Security Module	Active
□	116341I1800-1-B019A755	1800 TURN Relays	Active
□	116341Y100-1-33809CF8	100 Rich Media Sessions	Active

Licensing X12.6 – X14.0



System information

System name	
Up time	172 days 9 hours 16 minutes 19 seconds
Software version	X14.0.3
IPv4 address	LAN 1: 10.99.255.105
Smart licensing	

Licensing status

Registration status	✓ Registered
License authorization status	✓ Authorized
Smart account	InternalTestDemoAccount4.cisco.com
Virtual account	CTG-TME Team Account
Export-controlled functionality	Allowed

License usage (last updated: 00:50:49 EDT)

License type	Current usage	Status	Description
UCM_TelePresenceRoom	1	AUTHORIZED	UC Manager Telepresence Room License
UCM_Enhanced	1	AUTHORIZED	UC Manager Enhanced License

Information on how to configure Smart licensing can be found in the Admin Guide.

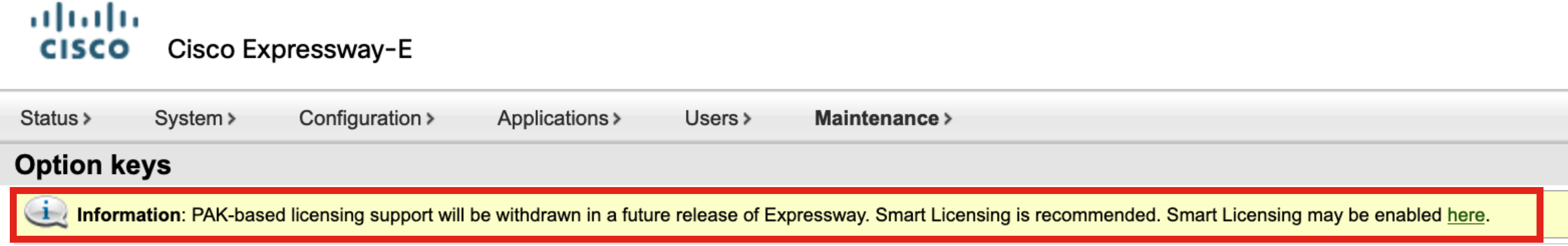
Licensing X12.6 – X14.0

Not all option keys are supported in Smart Licensing.

Smart Licensing X12.6 – X14.0	Supported	Not Supported
Rich Media Session	✓	
UC Manager Enhanced Plus (Desktop Systems)	✓	
UC Manager Telepresence (Room Systems)	✓	
Hardware Security Module (HSM) (Feature Preview)		✓
Microsoft Interoperability		✓
Advanced Account Security		✓

Licensing X14.2

- Only Smart Licensing support.
- Microsoft Interoperability will continue to work as an option key.
- Advanced Account Security option key will not be required to enable JITC. This is an export-controlled license.



Option keys

Information: PAK-based licensing support will be withdrawn in a future release of Expressway. Smart Licensing is recommended. Smart Licensing may be enabled here.

Virtual Machine Requirements

Deployment Size	vCPU	Reserved CPU Resource	Reserved RAM	NIC
Small	2 core	3600 MHz (2 x 1.8 GHz)	4 GB	1 GB
Medium	2 core	4800 MHz (2 x 2.4 GHz)	6 GB	1 GB
Large	8 core	25600 MHz (8 x 3.2 GHz)	8 GB	1 GB

No oversubscription of CPU, RAM or NIC.

Increasing or reducing the Deployment Size doesn’t happen automatically by adding or removing HW resources.

Expressway Server Capacity

Server Capacity X14.0.2+

	Registrations	B2B calls		*MRA Registrations	MRA Calls	
		Video	Audio		Video	Audio
CE1200	5,000	500	1,000	8,000	500	1,000
Large VM	5,000	500	1,000	4,000	500	1,000
Medium VM	2,500	100	200	3,500	150	300
Small VM	2,000	40	40	3,000	100	200

*Pre-Routed Route Header – Fast Path Registration enabled

Expressway Cluster Capacity

Cluster Capacity X14.0.2+

	Registrations	B2B calls		*MRA Registrations	MRA Calls	
		Video	Audio		Video	Audio
CE1200	20,000	2,000	4,000	32,000	2,000	4,000
Large VM	20,000	2,000	4,000	16,000	2,000	4,000
Medium VM	10,000	400	800	14,000	600	1,200
Small VM	2,000	40	40	3,000	100	200

Based on a 6 node cluster with a redundancy model of n+2.

*PRRH enabled.

MRA New Redundancy Models – X14.2

	MRA Registrations		MRA Calls	
	PRRH Off	PRRH On	PRRH Off	PRRH On
4+2	10,000	14,000	400	600
4+1	10,000	14,000	400	600
5+1	12,500	17,500	500	750

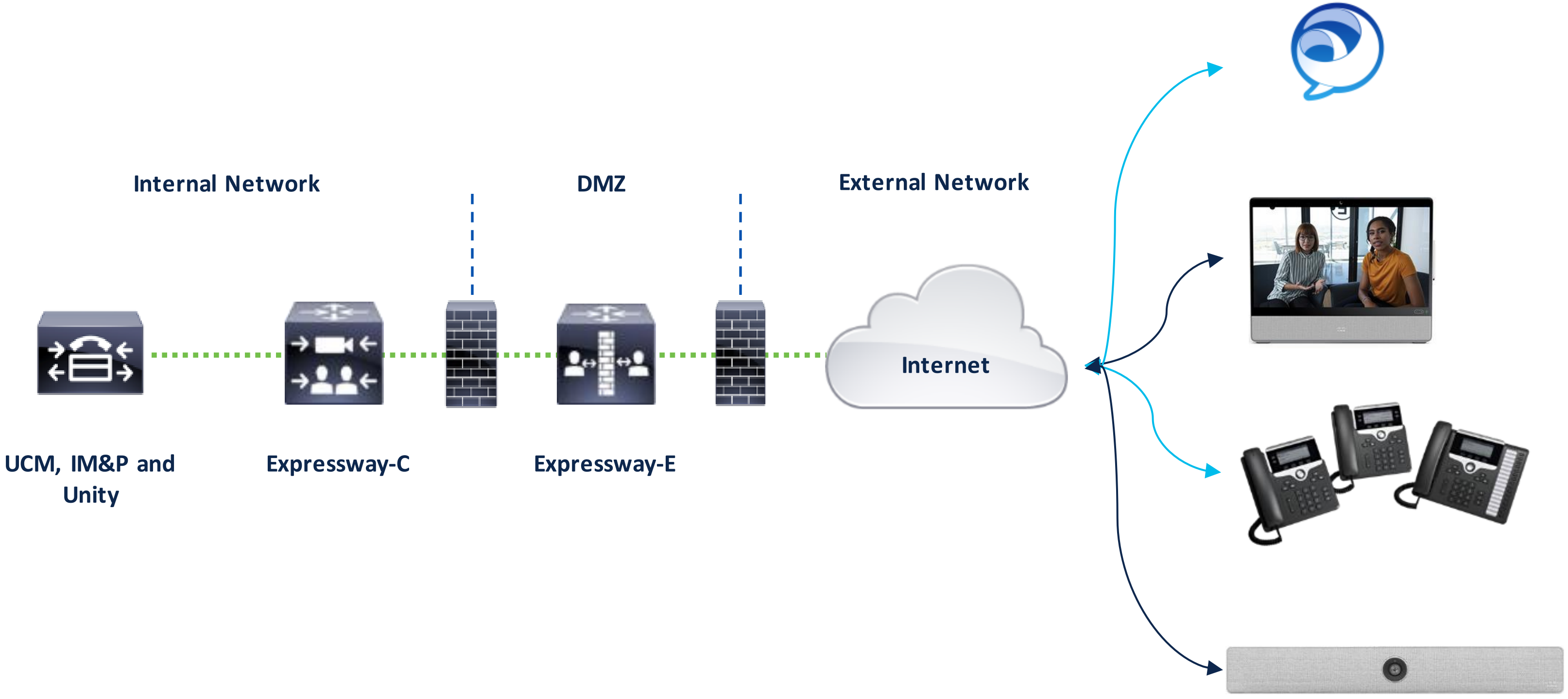
Medium OVA used as an example.

New Features in Version X14.0.x

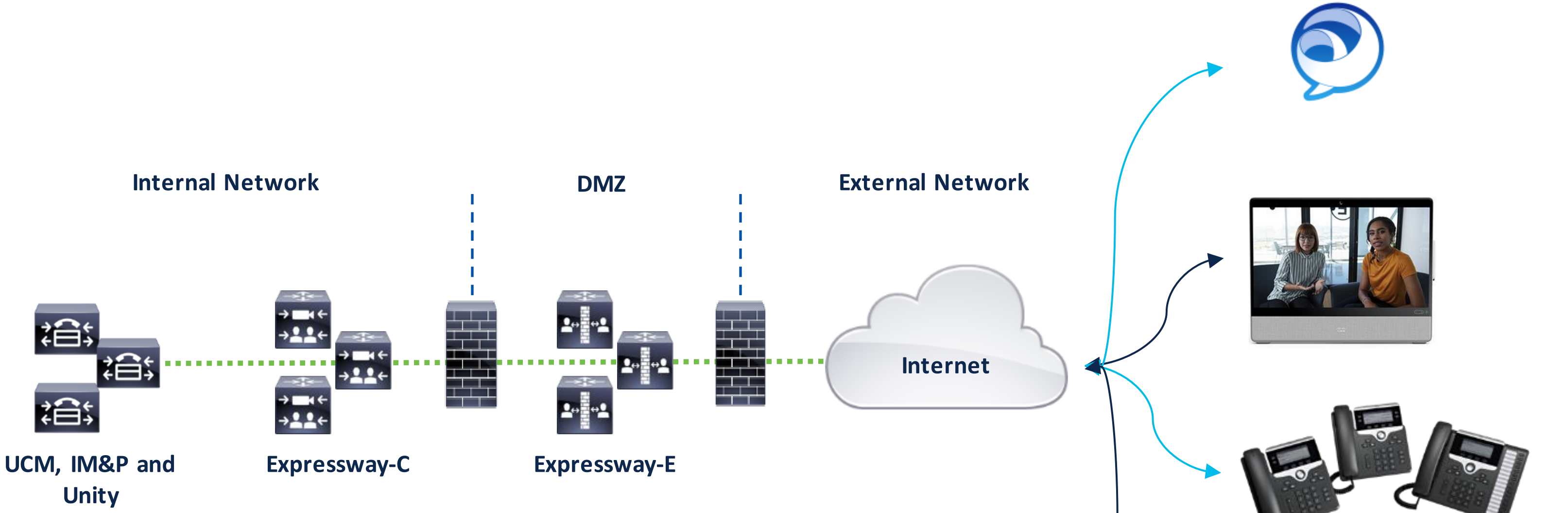
- SIP-Base DoS Attack Protection
- SIP Registration Failure Detection
- Rate Limits for SIP
- MRA Registration Failover
- Redirect URI for SSO/OAuth
- System Key Recovery
- IP/Port Filter for tcpdump on Diagnostic logs.
- Support for AV1 Codec
- Webex UCM Calling – Escalate P2P to Meeting
- API Updates
- RedSky E911 Location Services

Mobile and Remote Access

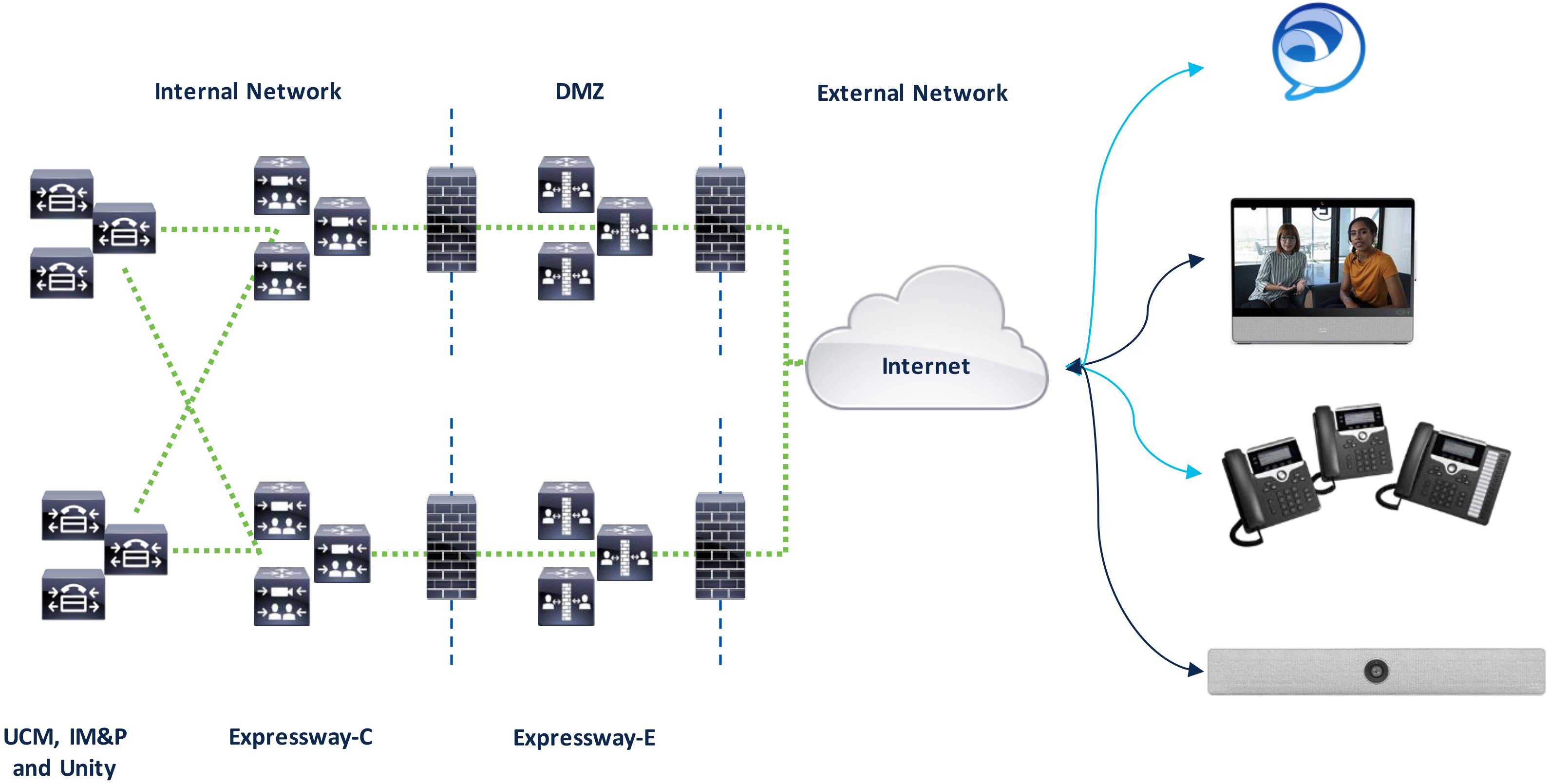
Mobile and Remote Access



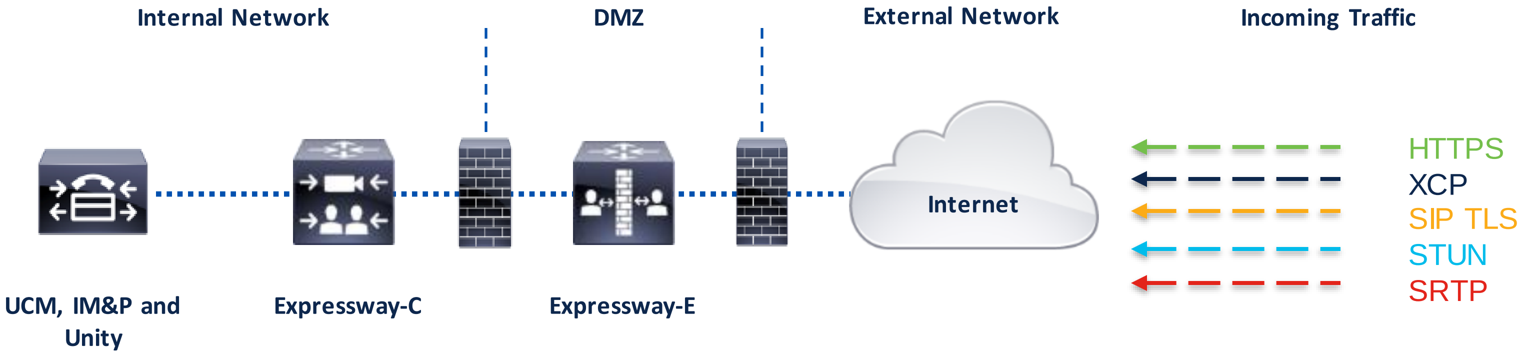
Mobile and Remote Access



Mobile and Remote Access

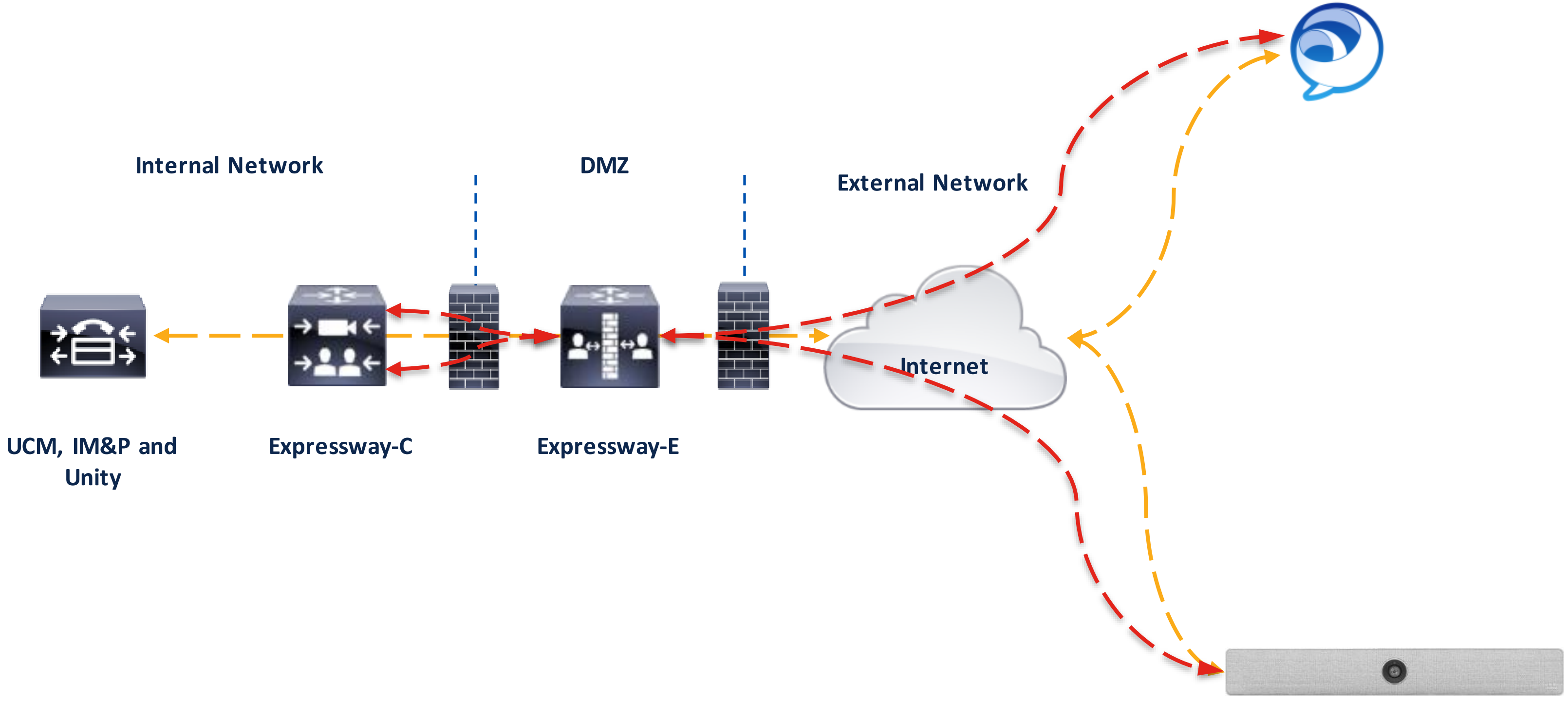


Mobile and Remote Access



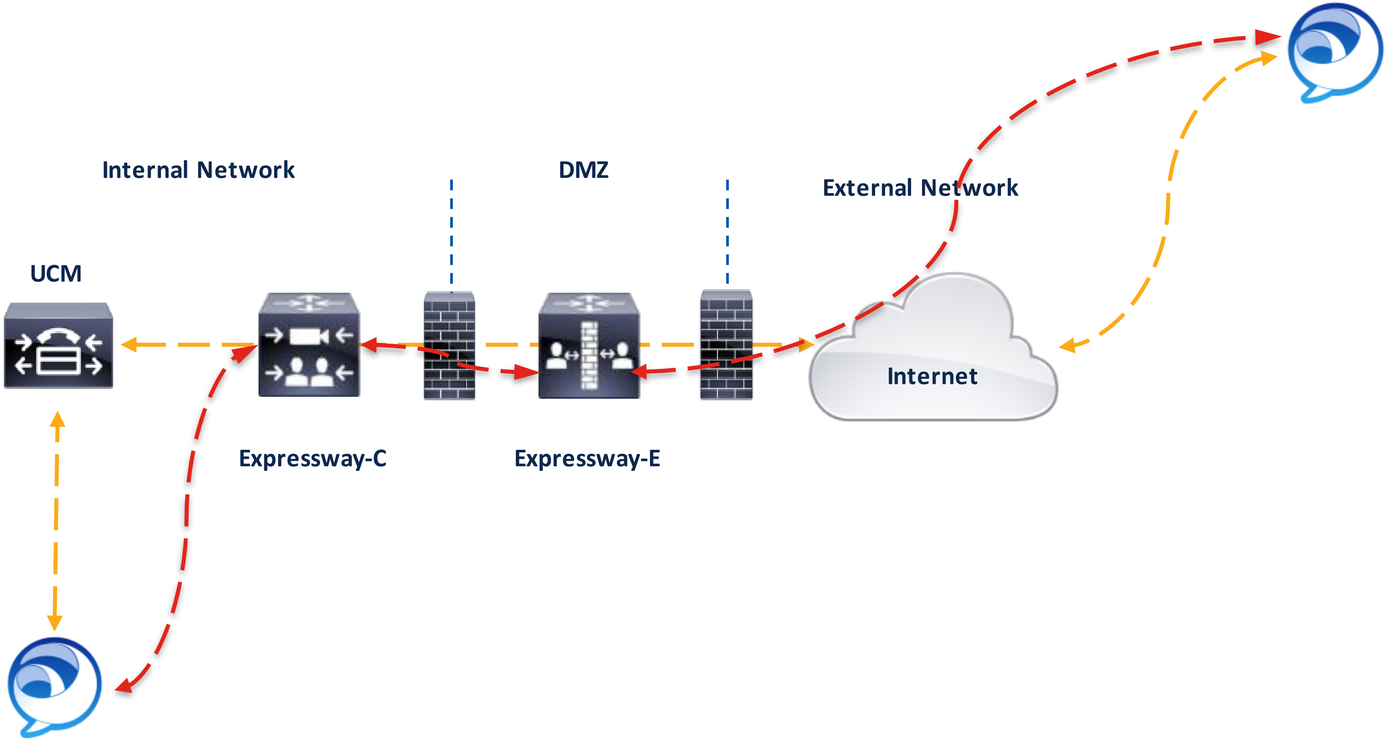
SIP TLS
SRTP

Media Path – MRA

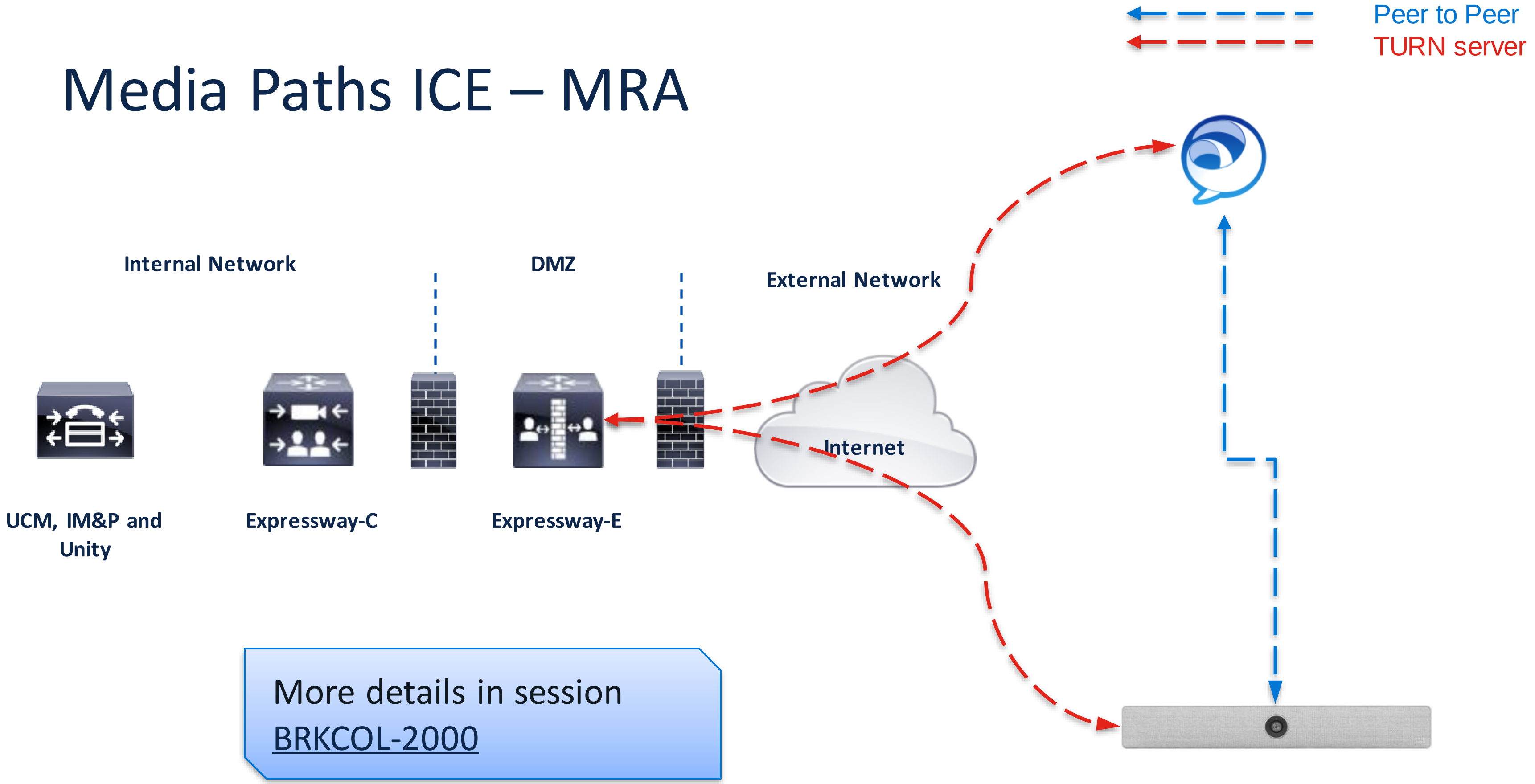


SIP TLS
SRTP

Media Path – MRA

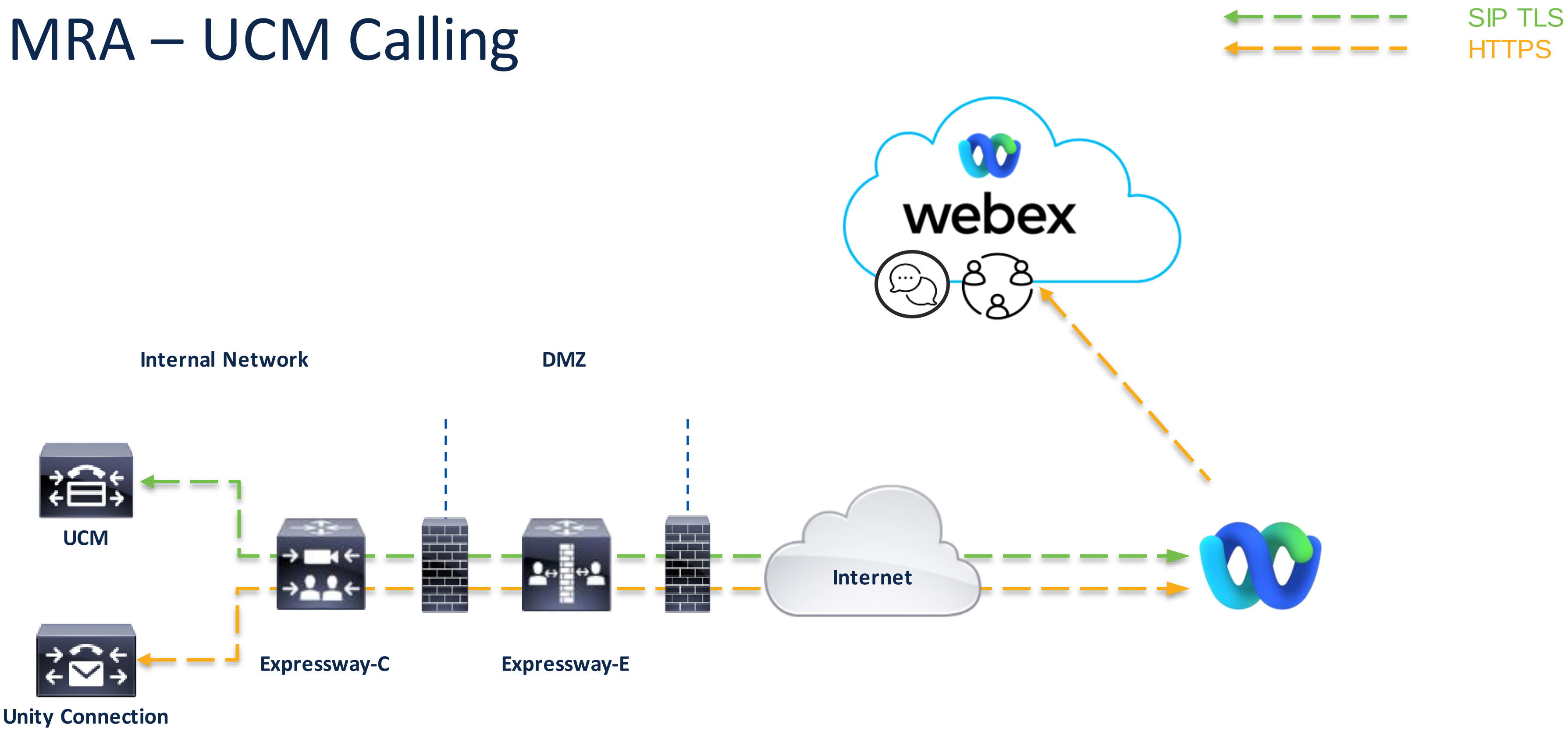


Media Paths ICE – MRA



More details in session BRKCOL-2000

MRA – UCM Calling



MRA Configuration – Prerequisites

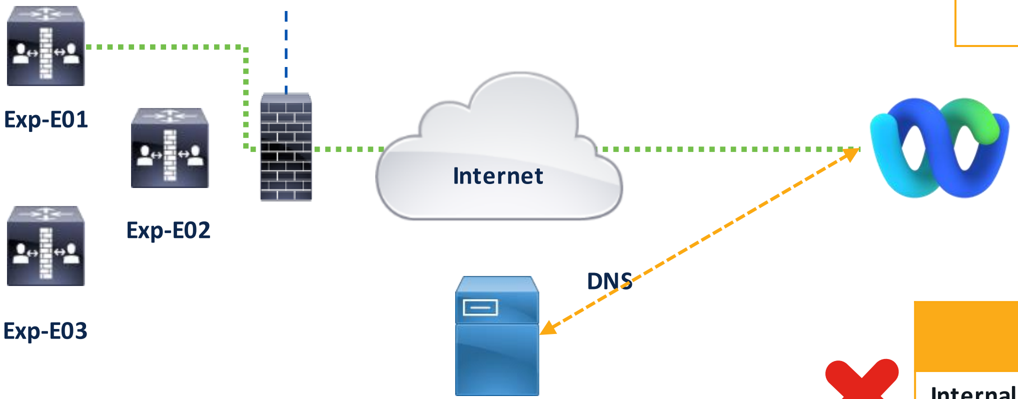
- MRA it's only one feature running in Expressway, before you configure it, you should follow the Basic Configuration and Administrator guides. Here are some recommendations before setting up MRA:

1. Single NIC with Static NAT is supported but not recommended.
2. All alarms should be cleared out.
3. Internal logins should work before you implement MRA.
4. Static routes might be needed when using a Dual NIC deployment.
5. Cluster should be built before you setup MRA.

MRA DNS Records

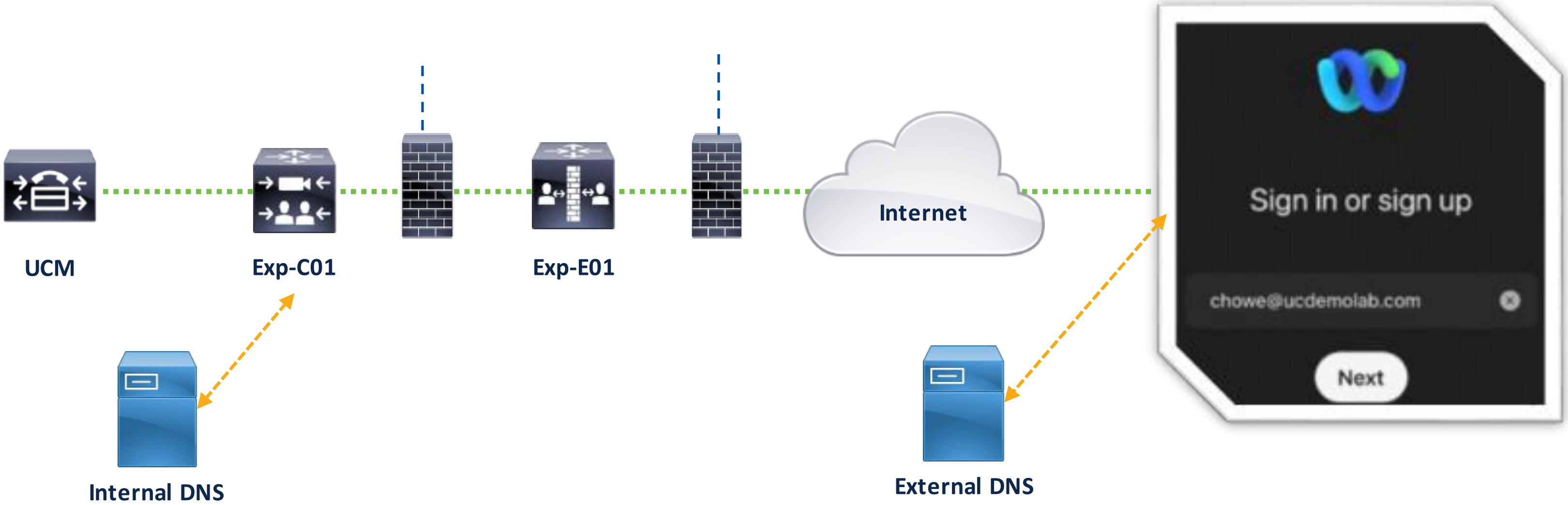
GET https:///.../get_edge_config?service_name=_cisco-uds

	FQDN	Priority	Weight
_collab-edge	Exp-E01	10	10
	Exp-E02	10	10
	Exp-E03	10	10



	Service	Protocol	Port	Host FQDN
✗ **Internal**	_cisco-uds	TCP	8443	UCM FQDN
✓ **External**	_collab-edge	TCP	8443	Exp-E FQDN

MRA – Split DNS with a Single Domain



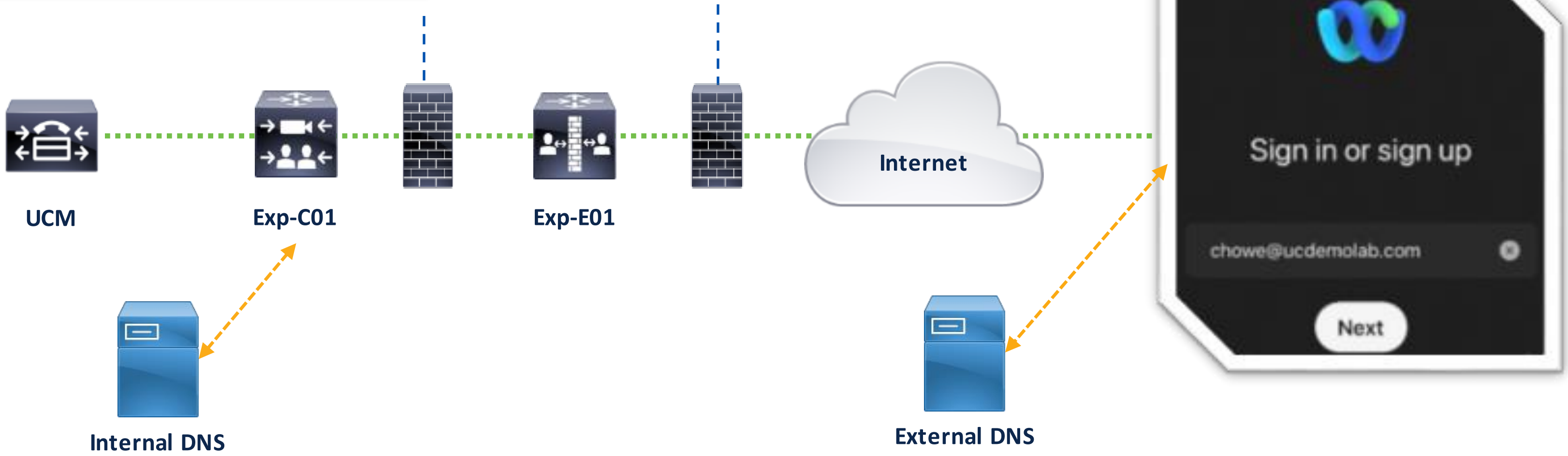
chowe@ucdemolab.com

_cisco-uds._tcp.ucdemolab.com	UCM FQDN

_collab-edge._tls.ucdemolab.com	Exp-E FQDN

MRA – Dual Domain without Split DNS

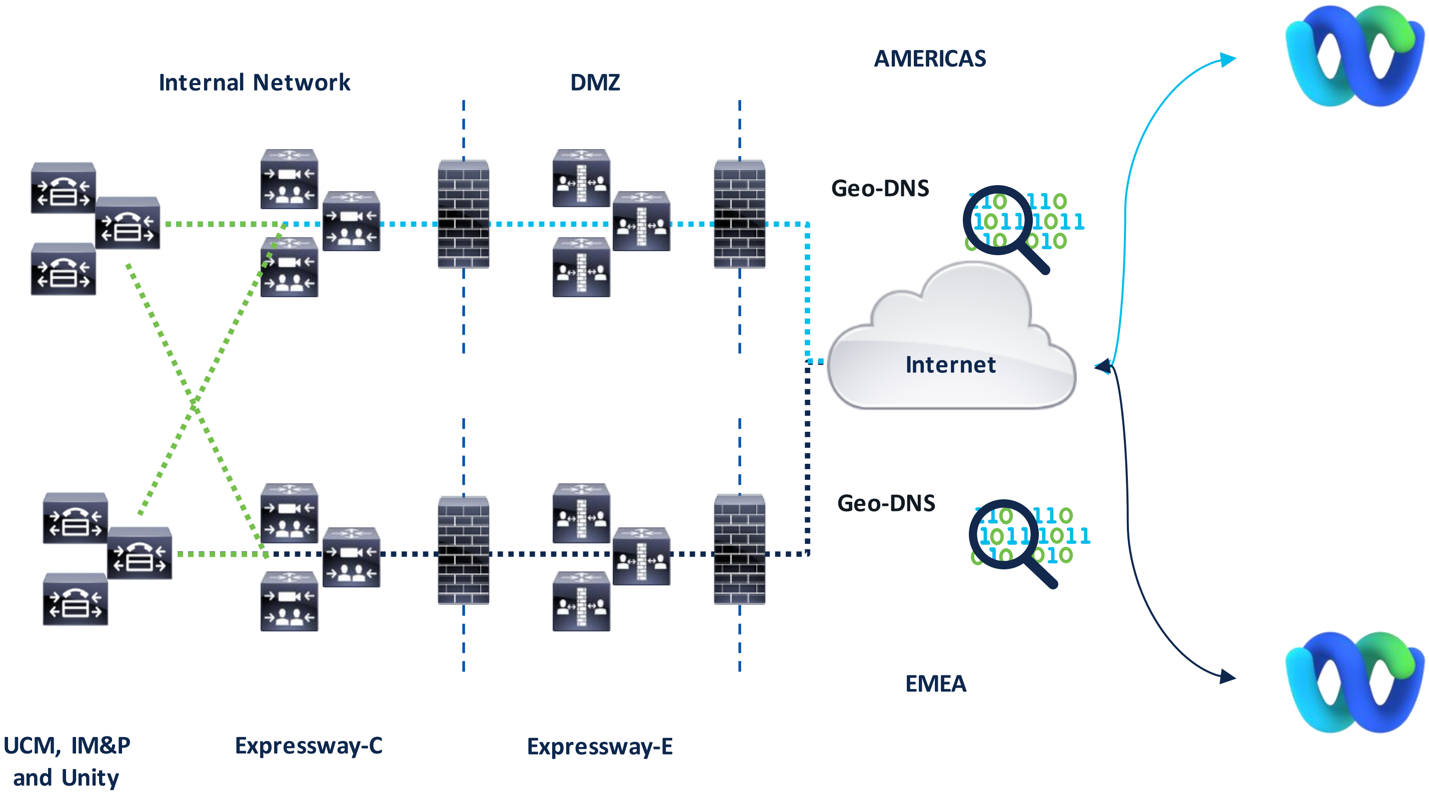
After X12.5, an internal cisco-uds record for the external domain is not required. UCM nodes need to be identified as FQDNs.



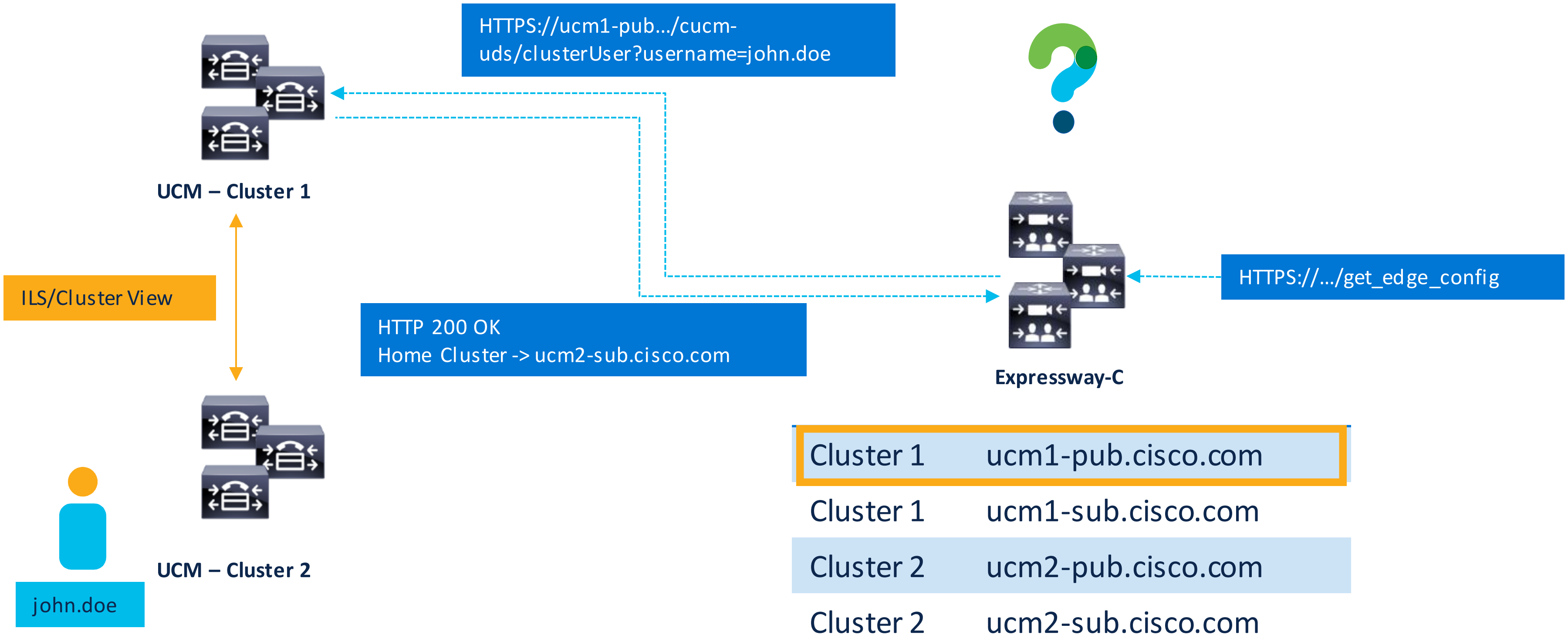
_cisco-uds._tcp.ucdemolab.com	~~UCM FQDN~~

_collab-edge._tls.ucdemolab.com	Exp-E FQDN

DNS - Multiple Regions



Multiple Cluster Setup



HTTPS://ucm1-pub…/cucm-uds/clusterUser?username=john.doe

HTTP 200 OK
Home Cluster -> ucm2-sub.cisco.com

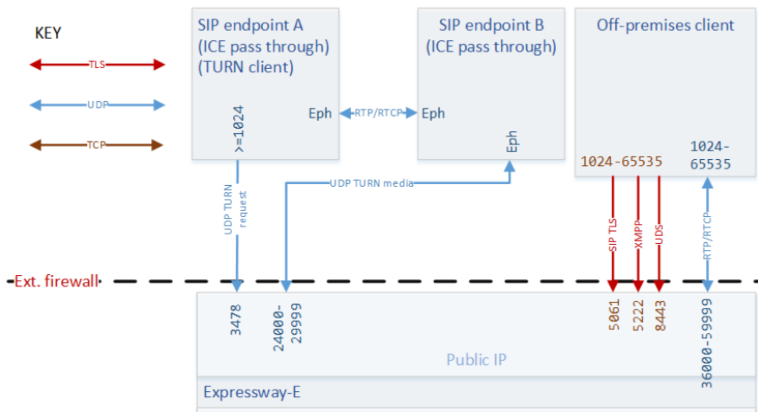
HTTPS://…/get_edge_config

Cluster 1	ucm1-pub.cisco.com
Cluster 1	ucm1-sub.cisco.com
Cluster 2	ucm2-pub.cisco.com
Cluster 2	ucm2-sub.cisco.com

MRA – Firewall

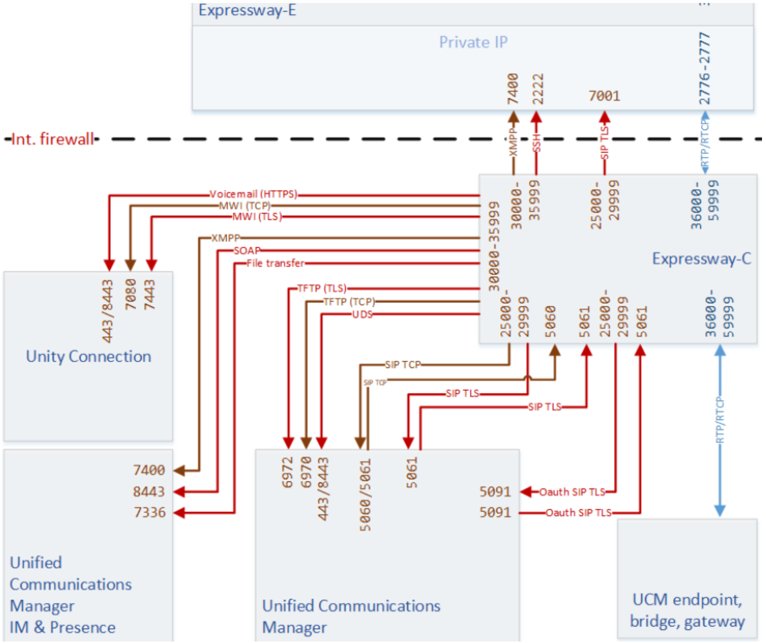
- Off Premise clients initiate the connection to the Exp-E.
- TURN media and RTP/RTCP ports are different.
- Traffic on port 5061, 8443 and 5222 uses TLS.
- Phone only deployments don’t need port 5222 open.

MRA Connections



MRA – Firewall

- Expressway C (traversal client) initiates the connection to Expressway-E (traversal server).
- 2776-2777 are demuxed ports used for RTP/RTCP in small/medium deployments.
- Large deployments use the first 12 ports from the Media Traversal port range.
- XMPP port changes from 5222 to 7400.

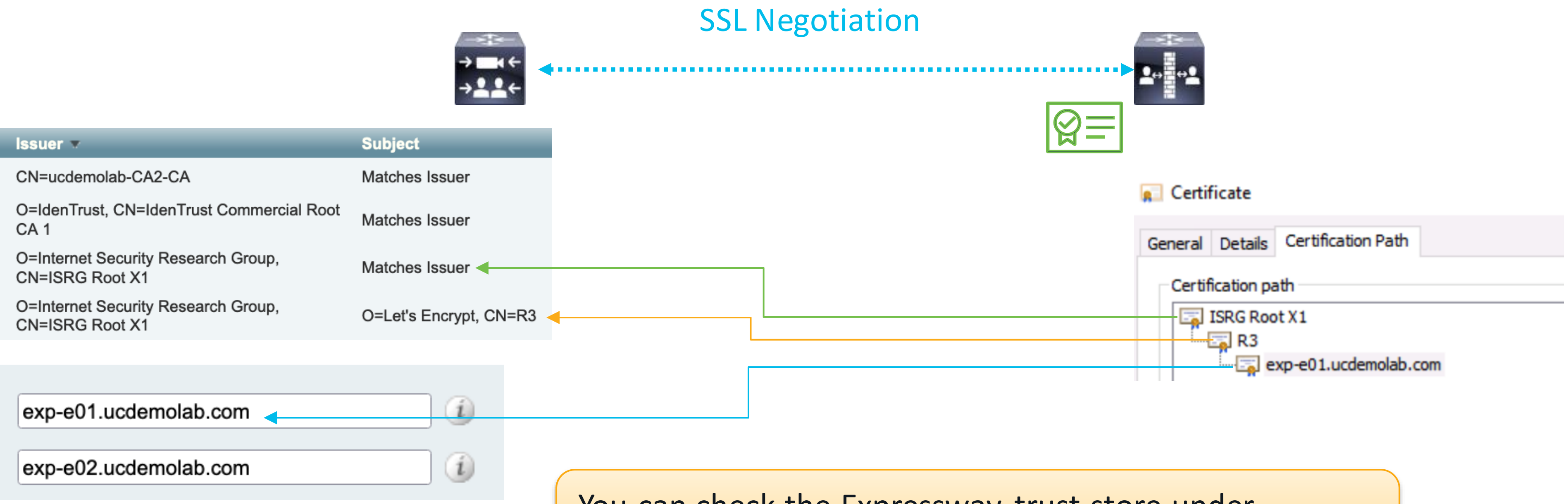


Certificates

- Signing the Exp-E certificate with an internal/private CA will result in the external client failing to connect or showing alerts to the end user.
- Webex app by default won't accept the certificate unless the UC Registration domain is added as a SAN.

	Expressway C	Expressway E
CA	Public/Private	Public
SAN	Phone Security Profile Expressway Cluster name IM&P Chat node aliases	UCM Domain XMPP Federation Domains IM&P Chat node aliases

MRA – Certificates



Issuer	Subject
CN=ucdemolab-CA2-CA	Matches Issuer
O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
O=Internet Security Research Group, CN=ISRG Root X1	Matches Issuer
O=Internet Security Research Group, CN=ISRG Root X1	O=Let's Encrypt, CN=R3

exp-e01.ucdemolab.com

exp-e02.ucdemolab.com

Certificate

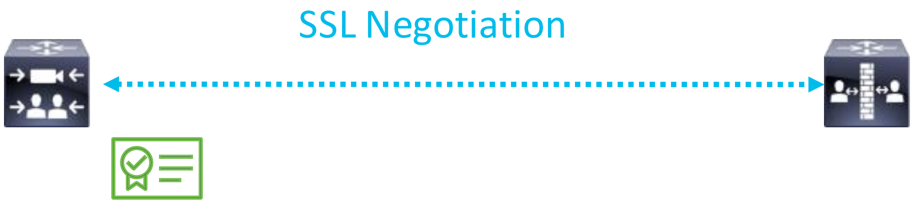
General | Details | Certification Path

Certification path

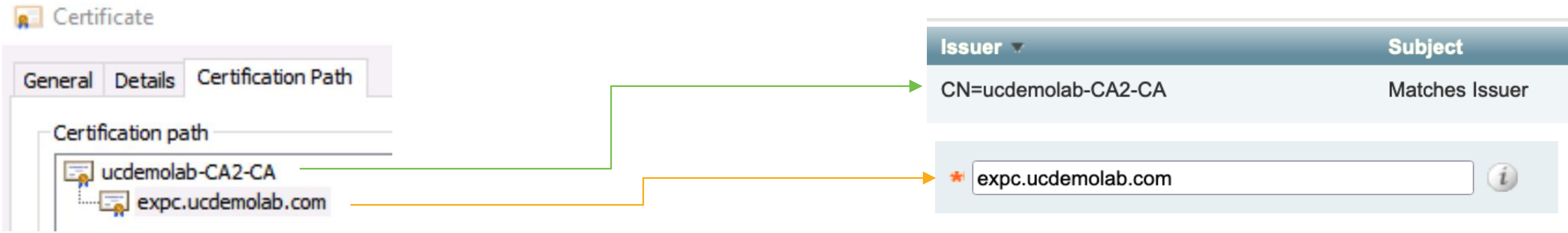
- ISRG Root X1
  - R3
    - exp-e01.ucdemolab.com

You can check the Expressway trust store under Maintenance > Security > Trusted CA certificate

MRA – Certificates



SSL Negotiation



Certification path

- ucdemolab-CA2-CA
  - expc.ucdemolab.com

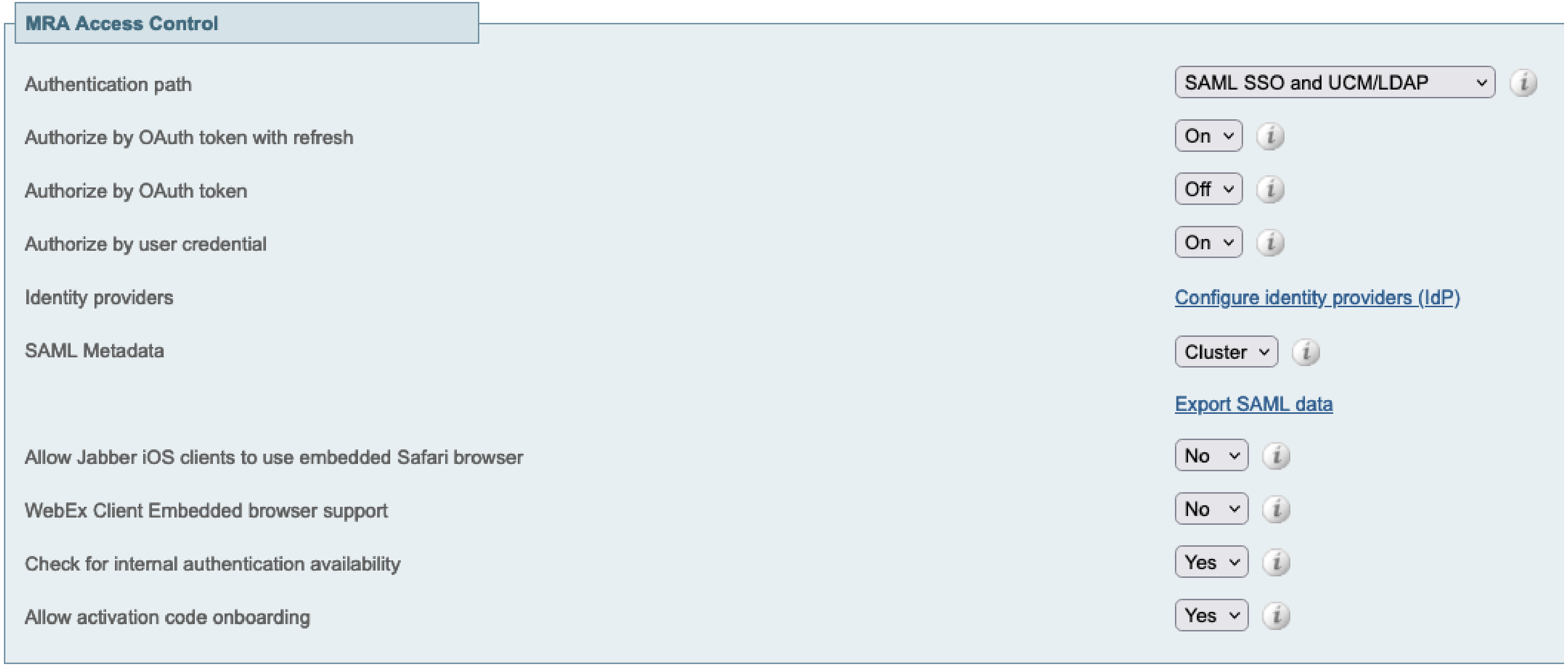
Issuer	Subject
CN=ucdemolab-CA2-CA	Matches Issuer

* expc.ucdemolab.com

Exp-C FQDN is configured in the UC Traversal Zone in the TLS verify subject name field.

MRA Authentication

What do I choose?

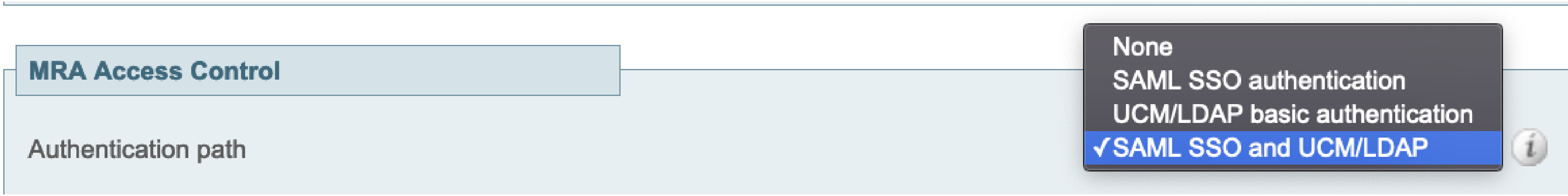


MRA Access Control

Authentication path	SAML SSO and UCM/LDAP
Authorize by OAuth token with refresh	On
Authorize by OAuth token	Off
Authorize by user credential	On
Identity providers	Configure identity providers (IdP)
SAML Metadata	Cluster Export SAML data
Allow Jabber iOS clients to use embedded Safari browser	No
WebEx Client Embedded browser support	No
Check for internal authentication availability	Yes
Allow activation code onboarding	Yes

MRA Authentication

- Jabber and Webex app can use Single Sign On or UCM/LDAP for authentication over MRA.
- Telepresence endpoints and 78XX/88XX phones can only do the UCM/LDAP authentication.
- Activation codes + Manufacturing Installed Certificates for 78XX/88XX phones.

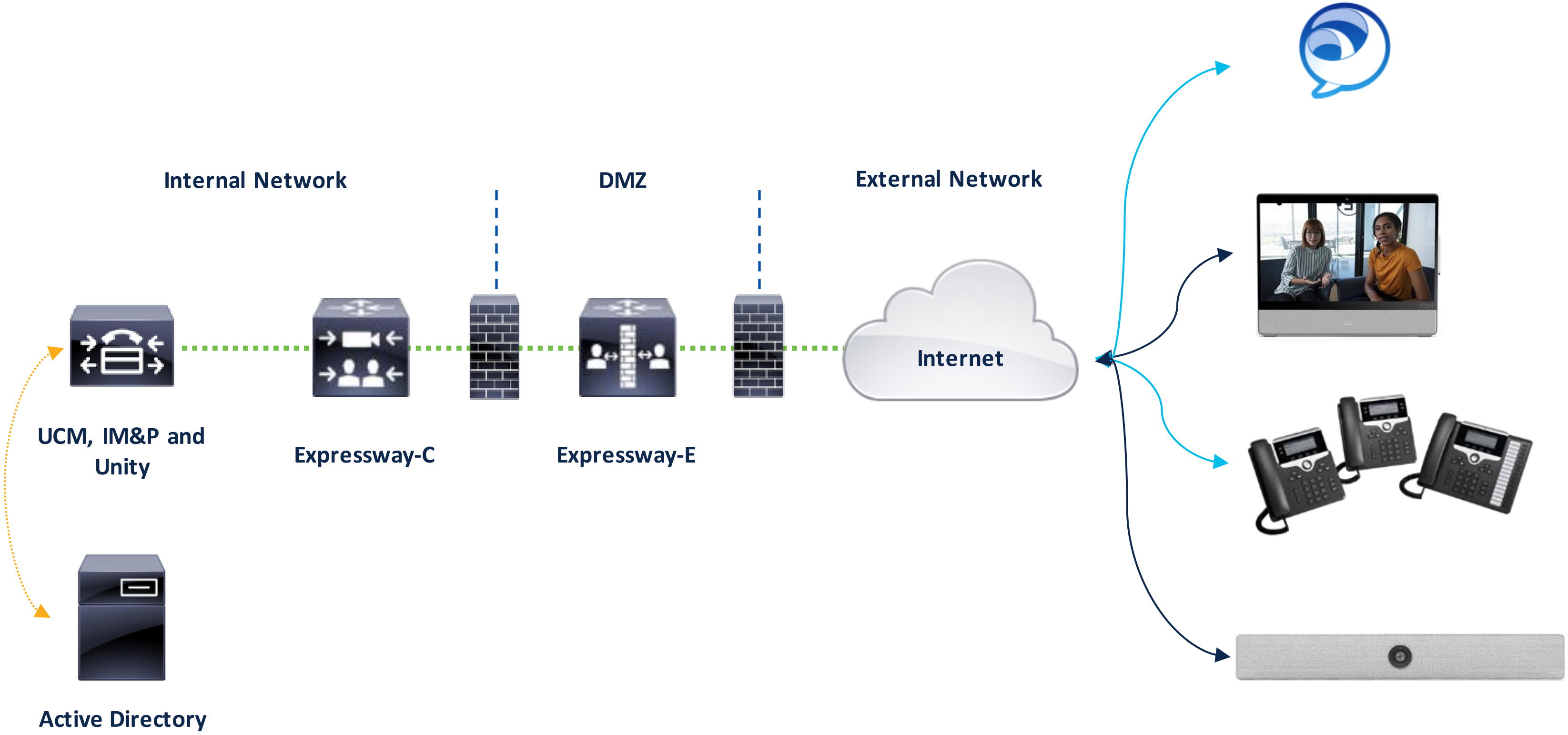


MRA Access Control

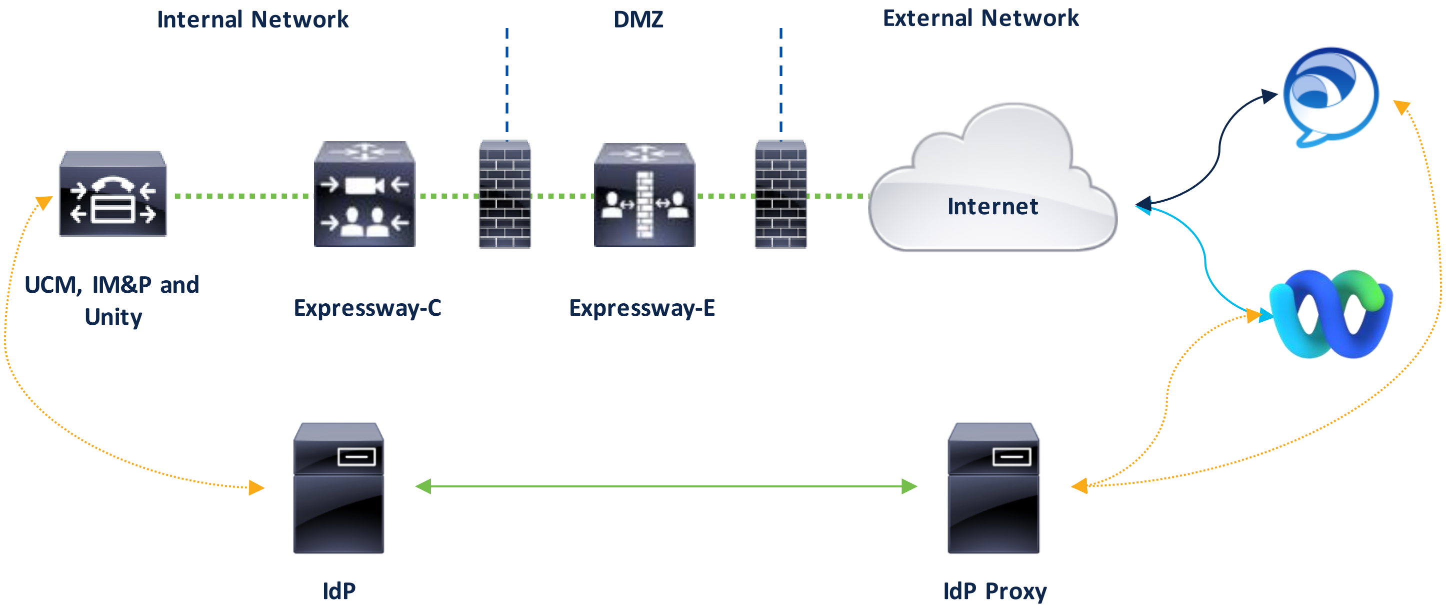
Authentication path

None
SAML SSO authentication
UCM/LDAP basic authentication
✓SAML SSO and UCM/LDAP

MRA Authentication Paths

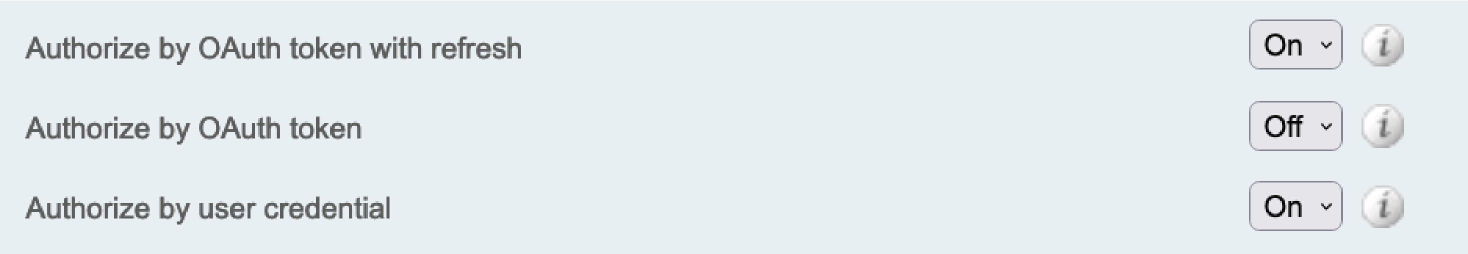


MRA Authentication Path



MRA Authentication

- OAuth token with refresh applies to both SSO and non-SSO deployments.
- User credential is required for Telepresence endpoints and IP phones.
- OAuth token (without refresh) is only needed if your UCM infrastructure doesn't support OAuth token with refresh. (11.5(1) SU3+)



Authorize by OAuth token with refresh	On
Authorize by OAuth token	Off
Authorize by user credential	On

Configuration – UCM/IM&P

- Considerations before adding UCM to Expressway C:
  1. Only Publishers are added to Expressway-C. Discovery of subscribers will occur after publisher is added.
  2. If using TLS Verify you should add the CUCM/IM&P publisher based on the Common Name (CN) value in the Tomcat certificate that is uploaded to the Expressway-C.
  3. Download Tomcat certificates from CUCM/IM&P OS Administration. Upload certificates under (Maintenance > Security certificates > Trusted CA certificates)
  4. You need an application user with the AXL API Access Role.
  5. Once CUCM is added the necessary Search Rules and Neighbor Zones are automatically configured.
  6. Secured communication between Exp-C and CUCM is not required, but recommended.

Conclusion

Highlights

- Companies with On-Prem UC need Expressway to support their hybrid work strategies.
- Expressway continues to be important in our portfolio of products.
- Webex UCM Calling over MRA allows to have some benefits of the Webex Cloud while continue to use your On-Prem solution for calls.
- X14.2 will increase the capacity of the Expressway clusters.

What’s Next!

cisco Live!

Las Vegas + Digital | June 12-16, 2022

ALL IN

#CiscoLive

Watch My Session

Enabling Collaboration for your Remote Workforce with Cisco Expressway - Part 2

Speaker: Luis Garcia

BRKCOL-2060b

Continue your education

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

The bridge to possible

Thank you

cisco Live!

#CiscoLive