

Pre Requisites

Jabber MRA

The Firewall needs to be supported Nat Traversal.

DMZ zone is mandatory for the terminating the edge servers.

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

Expressway Server Certificates Requirements

- 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

- 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

Subject Alternative Name (SAN) Requirements

Expressway-E Server Certificate

- Customer's service discovery domain is required to be included as a DNS SAN in all Expressway-E server certificates
- Service discovery domain in this case is collab10x.cisco.com
- This domain is used for SRV lookups, extracted from here
- This is a security measure that allows clients to verify connections to edge servers authoritative for their domain (RFC 6125)

For Example

DNS X509v3 Subject Alternative Name: DNS:collab10x.cisco.com



Cisco Meeting Server Requirements

BRKCOL-2803.pdf - Adobe Reader

File Edit View Window Help

33 / 138 105%

Tools Sign Comment

Cisco Meeting Server Certificate Requirements

Component	Certificate Type	Comments
WebAdmin	self-signed Public CA Signed	
WebBridge	self-signed Public CA Signed	Public CA signed certificate required only if CMA WebRTC is used
CallBridge	self-signed Public CA Signed	Self-signed certificates cannot be used in a Skype/Lync deployment. Deployments with TLS SIP Trunks cannot use self signed certificates.
Trunk	self-signed Public CA Signed	
LoadBalancer	self-signed Public CA Signed	
Database Cluster	Public CA Signed	Self-signed certificates cannot be used in a clustered deployment
Recorder Server	self-signed	Applications that interface to external devices require Public CA certificates. Applications that interface internally in the Cisco Meeting Server only require certificates signed by an Internal CA. Self-signed certificates can be created via the MMP interface on Cisco Meeting however it is strongly recommended that self-signed certificates only be used for test environments.
Streaming Server	self-signed	

Cisco *live!*

BRKCOL-2803 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 35

3:27 PM


BRKEVT-2665.pdf - Adobe Reader

File Edit View Window Help

Tools Sign Comment

Cisco Meeting Server

DNS Requirements



Record Type	Example	Description
A	xmpp.example.com	Used by Meeting Apps to login
A	join.example.com	IP address of WebBridge
A	cms.example.com	IP address of the CallBridge (For Lync FE)
A	cmsadmin.example.com	IP address of the WebAdmin Interface
A	fe.lync-domain.com	IP address for each SfB/Lync FE server
SRV	_xmpp-client._tcp.example.com	The A record xmpp.example.com above
SRV	_xmpp-server._tcp.example.com	The A record xmpp.example.com above
SRV	_sipinternatls._tcp.fe.lyncdomain.com	The A record of the Lync FE server or FE Pool
SRV	_xmpp-component._tcp.example.com	The A record xmpp.example.com above, Required if you plan to use DNS to connect between CallBridges and XMPP servers
SRV	_xmpp-client._tcp.example.com	The A record xmpp.example.com above

Cisco live!

BRKEVT-2665 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 28

6:07 PM

BRKEVT-2665.pdf - Adobe Reader

File Edit View Window Help

29 / 71 105%

Tools Sign Comment

Cisco Meeting Server

General Considerations

- The WebBridge and CallBridge are configured using a DNS A records
- The XMPP server has associated XMPP SRV records
- Connections between the **Core** (CallBridge) and the **Edge** (WebBridges/TURN) use:
 - 443 and 3478 respectively
- **Edge** server has generally requires **two** public IP address
 - i.e. if **WebBridge** server is running on port 443, **TURN** server is running port 443
 - The Load Balancer / SIP Edge listens on either one of the external interfaces
 - MMP (WebAdmin) listens on an internal private network
- Interfaces on same server, **MUST** have separate subnets

Cisco live!

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

6:07 PM