

## 300-820<sup>Q&As</sup>

Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI)

### Pass Cisco 300-820 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/300-820.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Refer to the exhibit. Logins and failing via mobile and remote access. How is this resolved?

The screenshot shows the 'Unified Communications status' page. Key sections include:

- Unified Communications status:** Enabled. Status messages for Unified CM registrations, IM and Presence Service, and OAuth token with refresh are in red, indicating they are not properly configured.
- Activity:** Shows 0 video calls, 0 audio calls, 8 current sessions, 15 total sessions, and 21 provisioning requests.
- Domains:** A table with columns Name, Services, and Associated zones. The domain 'pod1.local' is listed with services for Unified CM registrations, IM and Presence Service, and no associated zones.
- Servers:** Lists 1 IM and Presence Service node and 1 Unified CM server. A note states there are no Unity Connection servers configured.
- Zones:** A red message states: 'There are no Unified Communications traversal zones configured. Configure a secure Unified Communications traversal zone connection between this Expressway-C and the Expressway-E.'

On the right side, there is a terminal window showing 'xstatus zones zone 2' output, which details the configuration for zone 2, including SIP address, ports, and resource usage.

- A. Mobile and remote access login has not been enabled for the domain configured in the Expressway-C. The domain must be edited to allow Cisco UCM registrations.
- B. SIP is disabled on the Expressway-E. The SIP protocol must be enabled on the server.
- C. No Cisco UCM servers are configured in the Expressway-C. Servers must be added for CallManager and IM and Presence services.
- D. Although a traversal client zone exists, there is no Unified Communications traversal client zone. One must be created.

Correct Answer: D

**QUESTION 2**

What happens to the encrypted signaling traffic of a collaboration device if you place it inside a firewall with private IP addresses and try to make a call over IP without any collaboration infrastructure?

- A. The signaling makes it back to the endpoint because the firewall is an application layer gateway and provides address translation.

- B. Encrypted IP traffic for collaboration devices always is trusted by the firewall.
- C. The signaling does not make it back to the endpoint because the firewall cannot inspect encrypted traffic.
- D. The signaling makes it back to the endpoint because the endpoint sent the private address to the external endpoint.

Correct Answer: C

---

**QUESTION 3**

An engineer learns from an end user that calls from outside the company are not being received. Calls are being made to other businesses outside of the company on video using URL addresses. The change management log shows no changes in the configuration of the collaboration solutions. The engineer examines the endpoint, which seems to be registered to the Cisco UCM, and the SIP trunk between the Cisco UCM and sees that the Expressway is also up. In addition, the traversal link shows no errors between the Expressways. Which action must the engineer take to troubleshoot this issue?

- A. On the Cisco UCM, run the Real-Time Monitoring Tool to see if any incoming calls fail.
- B. On the Expressway-E, run diagnostic logging under maintenance to see if any requests reach the system.
- C. On the Expressway-E, check the NTP settings to ensure that TLS will be able to terminate. If the clock is out of sync, incoming calls from other working systems would work but not outgoing calls from the company.
- D. On the Expressway-C, run a network log under administrative tools to see if any requests reach the system.

Correct Answer: B

---

**QUESTION 4**

When an Expressway-E is configured for static NAT, which Session Description Protocol attribute is modified to reflect the NAT address?

- A. SDP b-line
- B. SIP record route
- C. SDP c-line
- D. SDP m-line

Correct Answer: C

as c-line shows the connection information, Media IP address. So if it is natted it will be reflected there.

---

**QUESTION 5**

Refer to the exhibit.

Alarms	
Alarm	Description
<input type="checkbox"/> Unified CM port conflict	There is a port conflict on Unified CM 10.0.101.111 between neighbor zone CUCM.pod1.local and Unified Communications (both are using port 5060)

**Action**

The same port on Unified CM cannot be used for line side (Unified Communications) and SIP trunk traffic. Review the port configuration on Unified CM and reconfigure the [Zone](#) if necessary

Mobile and remote access is being added to an existing B2B deployment and is failing.

When the administrator looks at the alarms on the Expressway-C, the snippets are shown. Which configuration action should the administrator take to fix this issue?

- A. The listening port on the Expressway-C for SIP TCP must be changed to a value other than 5060
- B. The listening port on the Expressway-C for SIP TLS must be changed to a value other than 5061
- C. The listening port on the Cisco UCM for the Expressway-C SIP trunk must be changed to something other than 5060 or 5061
- D. The listening port on the Cisco UCM for the Expressway-C SIP trunk is set to something other than 5060 or 5061. It must be set to 5060 for insecure and 5061 for secure SIP

Correct Answer: C

## QUESTION 6

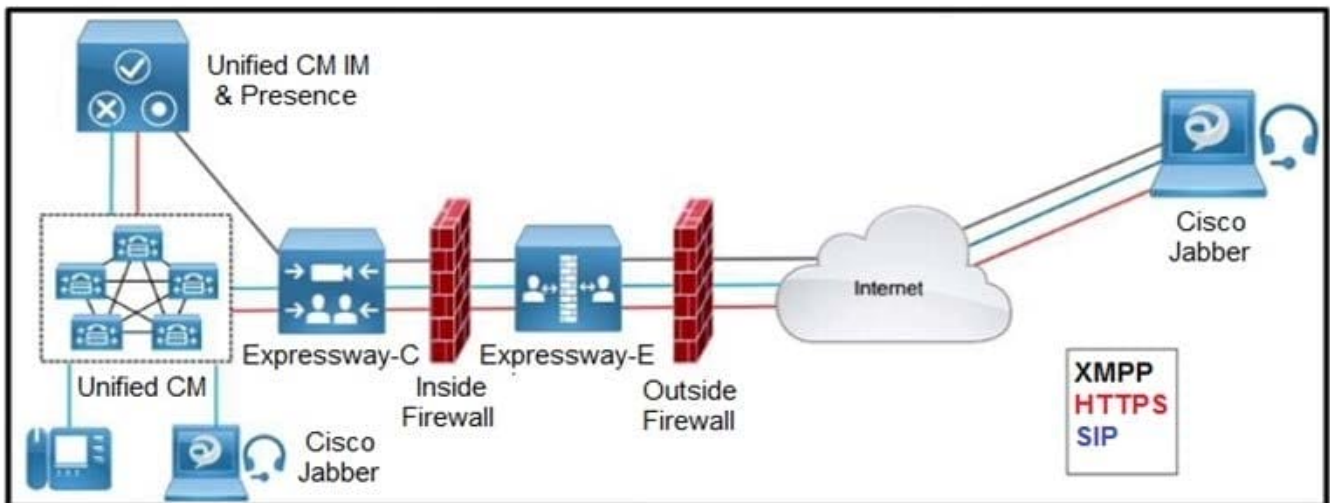
How does an administrator configure an Expressway to make sure an external caller cannot reach a specific internal address?

- A. add the specific URI in the firewall section of the Expressway and block it
- B. block the call with a call policy rule in the Expressway-E
- C. add a search rule route all calls to the Cisco UCM
- D. configure FAC for the destination alias on the Expressway

Correct Answer: B

## QUESTION 7

Refer to the exhibit.



Which two outbound connections should an administrator configure on the internal firewall? (Choose two.)

- A. XMPP: TCP 7400
- B. SIP: TCP 7001
- C. SIP TCP 5061
- D. Media: UDP 36012 to 59999
- E. HTTPS: TCP 8443

Correct Answer: AB

The internal firewall must allow the following outbound connections from the Expressway-C to the Expressway-E: SIP: TCP 7001 Traversal media: UDP 2776 to 2777 (or 36000 to 36011 for large VM/appliance) XMPP: TCP 7400 HTTPS (tunneled over SSH between C and E): TCP 2222 Source: Official Cert Guide

Reference: [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf)

## QUESTION 8

In a Mobile and Remote Access deployment, where must communications be encrypted with TLS?

- A. Cisco Expressway-E and endpoints outside the enterprise
- B. Cisco Expressway-C, Cisco Unified Communications Manager, and IMandP
- C. Cisco Expressway-C, Cisco Expressway-E, and Cisco Unified Communications Manager
- D. Cisco Expressway-C, Cisco Expressway-E, and endpoints outside the enterprise

Correct Answer: D

**QUESTION 9**

Refer to the exhibit.

Transforms							
Priority	State	Description	Pattern	Type	Behavior	Replace	
<input type="checkbox"/>	1	Enabled	Strip Domain from all calls	(.*)@(.*)	Regex	Replace	\1
<input type="checkbox"/>	2	Enabled	add pod1.local domain to all requests	(.*)	Regex	Replace	\1@pod1.local

Search rules											
Priority	Rule name	Protocol	Source	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	SIP variant	Enabled
1	Route all Calls to Local Zone	Any	Any	Any alias				Continue	LocalZone	Any	<input checked="" type="checkbox"/>

Search history				
Search type	Source	Destination	SIP variant	Status
SIP (INVITE)	jabberuser@pod1.local	sip.endpointc@pod1.local	Standards-based	Not found
SIP (INVITE)	jabberuser@pod1.local	sip.endpointb@pod1.local	Standards-based	Not found
SIP (INVITE)	jabberuser@pod1.local	sip.endpointa@pod1.local	Standards-based	Not found

Calls to locally registered endpoints are failing. At present, there are two endpoints registered locally to this Expressway. An H.323 endpoint with an alias of "EndpointA" is registered, and a SIP endpoint with an alias of "EndpointB@pod1.local" is also registered.

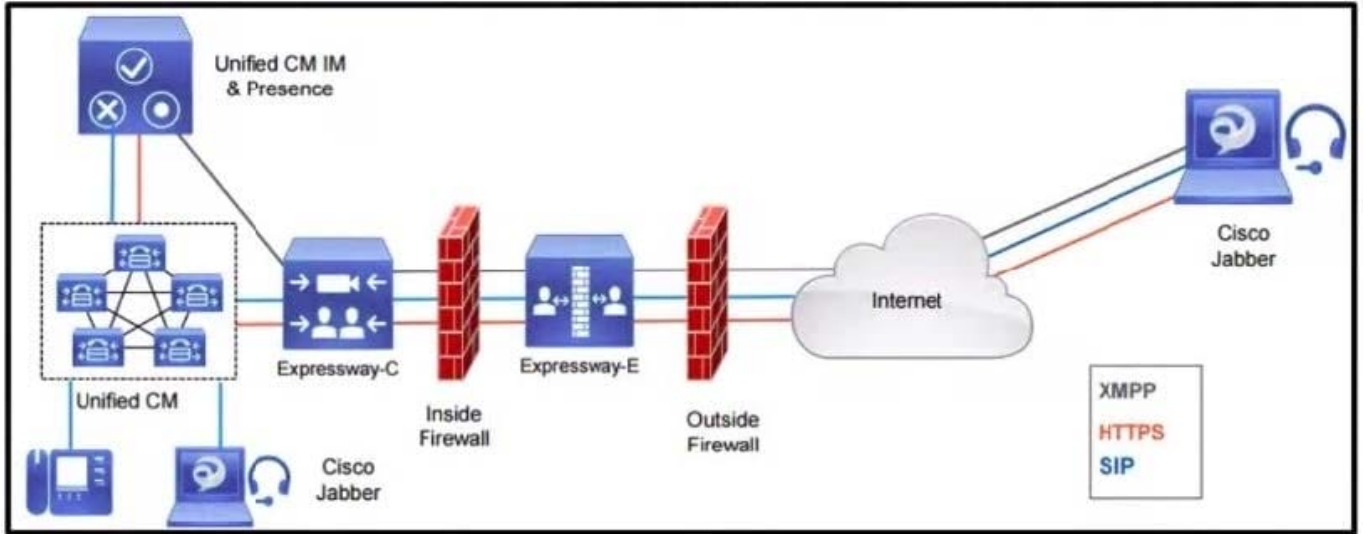
How is this issue resolved?

- A. The dialplan must be redesigned to use the transforms to convert the alias into SIP URI format and then use separate search rules for each format that needs to be dialed within the local zone.
- B. The calls are failing because there are insufficient licenses. Additional licenses must be installed for the Expressway to route these calls.
- C. The current search rule does not match the call, so the search rule must be modified to include a SIP Variant of "Standards-Based".
- D. Calling parties are placing calls with the wrong domain. End-users must be instructed not to use the pod1.local domain as that is owned by the local system. Calls to any other domain would work.

Correct Answer: A

**QUESTION 10**

Refer to the exhibit.



Which inbound connection should an administrator configure on the outside firewall?

- A. Media: UDP 36000 to 36011
- B. HTTPS (tunneled over SSH between C and E): TCP 2222
- C. SIP TCP 5061
- D. XMPP TCP 5222

Correct Answer: D

Based on following LINK and page 18(SIP Calls) + 29 (MRA Connections): [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf)

SIP UDP: 5060 SIP TCP: 5060 SIP TLS: 5061 XMPP TCP: 5222 RTP/RTCP: 36000-59999

## QUESTION 11

An engineer must configure Mobile and Remote Access. One of the requirements is to expect Cisco Jabber users to enter `username@cisco.com` as the login userid. Which DNS record must the engineer modify to start implementing this requirement?

- A. `_cuplogin._tcp.cisco.com`
- B. `_collab-edge._tls.cisco.com`
- C. `_cisco-uds._tls.cisco.com`
- D. `_cisco-uds._tcp.cisco.com`

Correct Answer: B

## QUESTION 12

When the network requirements are configured for a new Video Mesh deployment, which firewall ports are required so that Video Mesh cascade signaling succeeds?

- A. TCP 443 and 444
- B. TCP 443 and 8443
- C. UDP 5004 and 5005
- D. UDP 33432 through 33433

Correct Answer: A

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html)

---

### QUESTION 13

What is a benefit of Cisco Webex Messenger Cloud deployment?

- A. Cloud deployment is more secure than an on-premises deployment.
- B. There is no additional cost to use a cloud deployment.
- C. Cloud deployment allows interoperability between Cisco Jabber and Webex Teams users.
- D. Cloud deployment is faster than using an on-premises deployment.

Correct Answer: C

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/spark/hybrid-services/messageservice/cmgt\\_b\\_spark-hybrid-message-deployment-guide/cmgt\\_b\\_spark-hybrid-message-deployment-guide\\_chapter\\_00.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybrid-services/messageservice/cmgt_b_spark-hybrid-message-deployment-guide/cmgt_b_spark-hybrid-message-deployment-guide_chapter_00.html)

---

### QUESTION 14

An engineer reviews the configuration of a pair of Expressway servers for a company with the domain example.com. The company allows toll fraud calls to reach the Cisco UCM only when it expects externally registered devices to call internal 5-digit extensions. The search history shows that the fraudulent calls have a destination URI of 8 or more digits and several domains. What must the engineer configure to prevent all toll fraud calls from going past the Expressway-E to the internal network?

- A. search rules to only route calls with a destination URI of 5 to 8 digits long on the Expressway-E
- B. CPL that blocks calls with a destination domain other than example.com on the Expressway-C.
- C. search rules to only route calls with a destination domain of example.com on the Expressway-E
- D. CPL to block calls with a destination URI with 8 or more digits on the Expressway-E

Correct Answer: D

---



## QUESTION 15

Refer to the exhibit. The administrator attempted to log in, but Jabber clients cannot log in via mobile and remote access. How is this issue resolved?

The screenshot shows a Cisco Jabber login interface with an error message: "Cannot find your services automatically. Click advanced settings to set up manually." The username field is populated with "jabberuser@pod1.local" and a "Continue" button is present. To the right, a network log displays the following entries:

```

Standard query 0x2b84 SRV _cisco-uds._tcp.pod1.local
Standard query response 0x2b84 No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x71d9 SRV _cuplogin._tcp.pod1.local
Standard query response 0x71d9 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
Standard query 0x27bb SRV _collab-edge._tls.pod1.local
Standard query response 0x27bb No such name SRV _collab-edge._tls.pod1.local SOA ad.skype.local
Standard query 0xb09e SRV _collab-edge._tls.pod1.local
Standard query response 0xb09e No such name SRV _collab-edge._tls.pod1.local SOA ad.skype.local
Standard query 0xe2b5 A pod1.local
Standard query response 0xe2b5 A pod1.local SOA ad.skype.local
Standard query 0x687e A pod1
Standard query 0x687e A pod1
Standard query 0xa661 A loginp.webexconnect.com
Standard query response 0xa661 A loginp.webexconnect.com CNAME global-cas-c63.webexconnect.com /
Standard query 0xccba SRV _cisco-uds._tcp.pod1.local
Standard query response 0xccba No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x8530 SRV _cuplogin._tcp.pod1.local
Standard query response 0x8530 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
Standard query 0xd02d SRV _collab-edge._tls.pod1.local
Standard query response 0xd02d No such name SRV _collab-edge._tls.pod1.local SOA ad.skype.local
Standard query 0x91d6 SRV _cisco-uds._tcp.pod1.local
Standard query response 0x91d6 No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x0648 SRV _cuplogin._tcp.pod1.local
Standard query response 0x0648 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
Standard query 0xb4fa SRV _cisco-uds._tcp.pod1.local
Standard query response 0xb4fa No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x5299 SRV _cuplogin._tcp.pod1.local
Standard query response 0x5299 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
    
```

- A. Skype for Business mode must be disabled on the DNS server because it conflicts with Jabber login requirements.
- B. The domain pod1.local must be deprovisioned from the Webex cloud for Jabber logins.
- C. A DNS SRV record must be created for \_collab-edge.\_tls.pod1.local that points to the Expressway-E.
- D. The username jabberuser@pod1.local is invalid. The user should instead sign-in simply as jabberuser.

Correct Answer: C