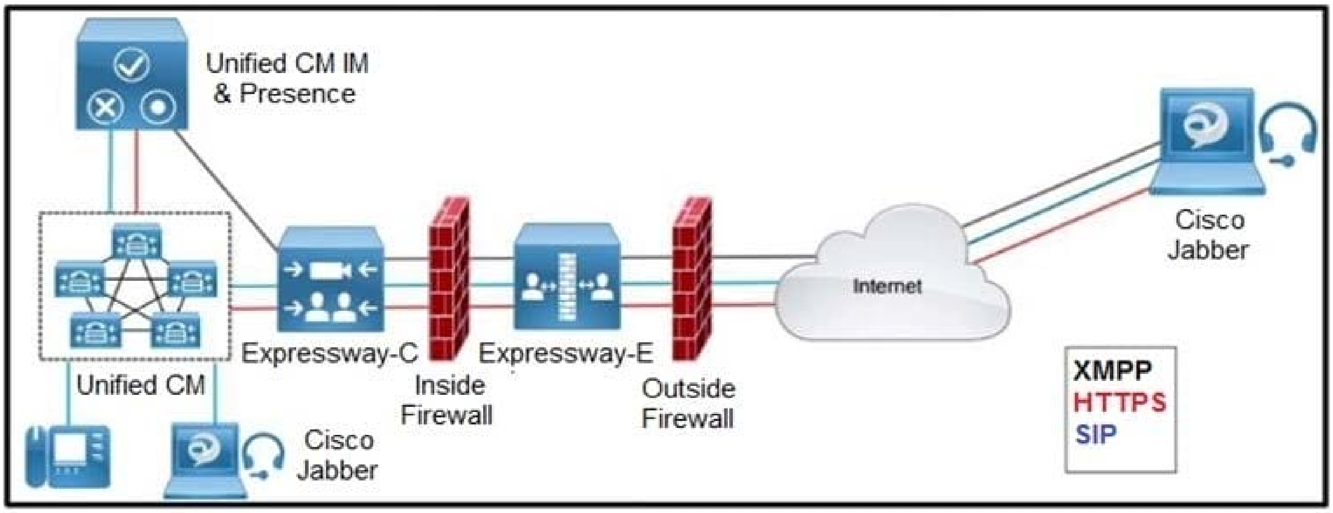
300-820Q&As

Implementing Cisco Collaboration Cloud and Edge Solutions (CLCEI)

Pass Cisco 300-820 Exam with 100% Guarantee

QUESTION 1

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

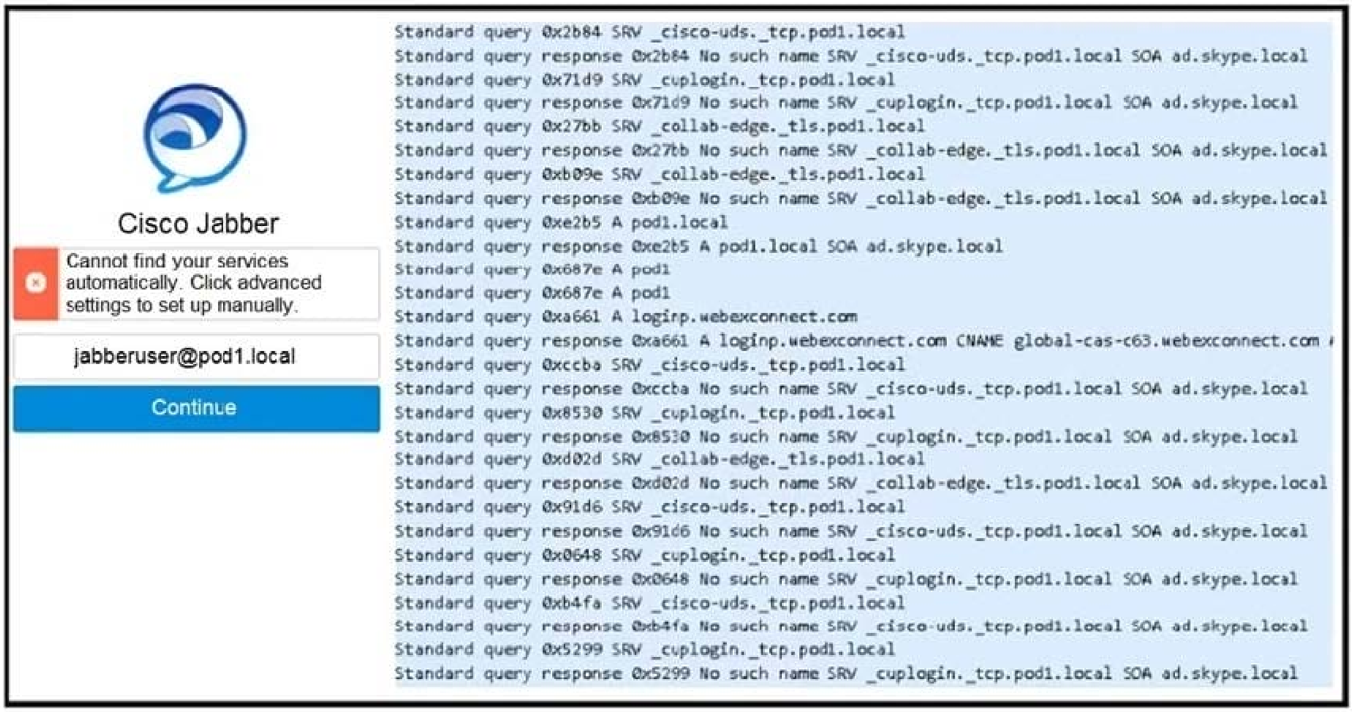
Correct Answer: AB

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

QUESTION 2

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?



Cisco Jabber

Cannot find your services automatically. Click advanced settings to set up manually.

jabberuser@pod1.local

```
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.

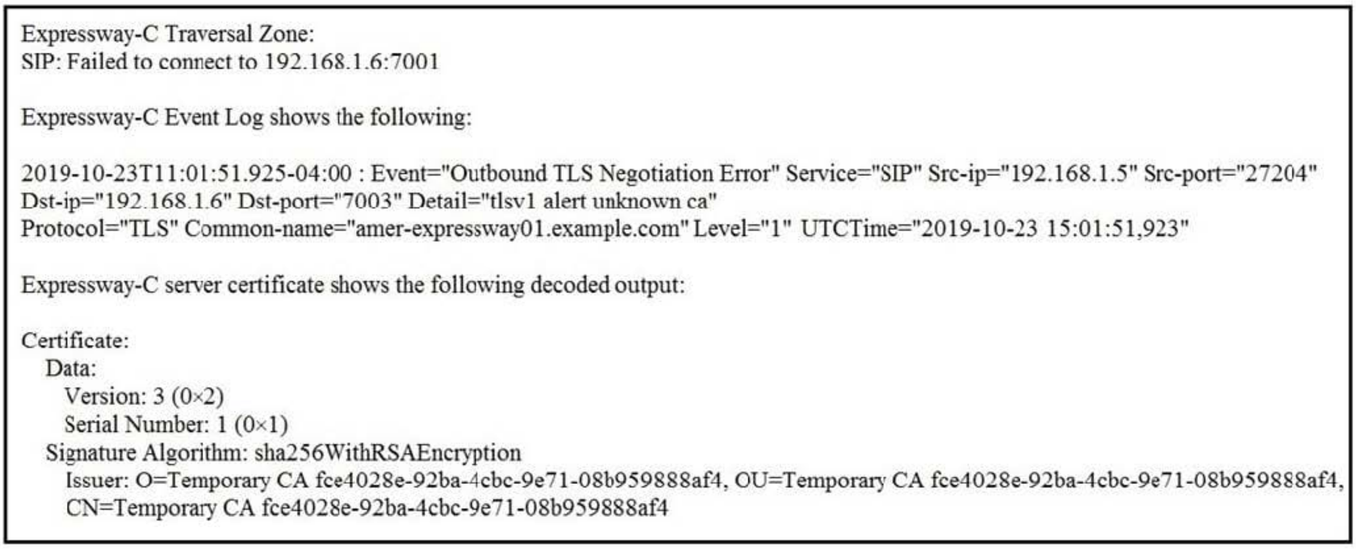
C. A DNS SRV record must be created for _collab-edge._tls.pod1.local that points to the Expressway-E.

D. The username jabberuser@pod1.local is invalid. The user should instead sign-in simply as jabberuser.

Correct Answer: C

QUESTION 3

Refer to the exhibit.



```
Expressway-C Traversal Zone:
SIP: Failed to connect to 192.168.1.6:7001

Expressway-C Event Log shows the following:

2019-10-23T11:01:51.925-04:00 : Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="192.168.1.5" Src-port="27204"
Dst-ip="192.168.1.6" Dst-port="7003" Detail="tlsv1 alert unknown ca"
Protocol="TLS" Common-name="amer-expressway01.example.com" Level="1" UTCTime="2019-10-23 15:01:51,923"

Expressway-C server certificate shows the following decoded output:

Certificate:
  Data:
    Version: 3 (0×2)
    Serial Number: 1 (0×1)
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: O=Temporary CA fce4028e-92ba-4cbc-9e71-08b959888af4, OU=Temporary CA fce4028e-92ba-4cbc-9e71-08b959888af4,
    CN=Temporary CA fce4028e-92ba-4cbc-9e71-08b959888af4
```

An Expressway-C and Expressway-E are configured for B2B calling and the Expressway- E zone is set to TLS Verify Currently, calls do not reach the Expressway-C. The Traversal Client zone on the Expressway-C for B2B reports the information in the exhibit for the Peer 1 address.

Which action resolves this error?

A. Configure the Expressway-C Traversal Client zone Peer 1 address with the fully qualified domain name of the Expressway-E.

B. Configure the Expressway-C Traversal Client zone transport protocol with TCP.

C. Add a server certificate to the Expressway-C that is signed by a certificate authority.

D. Add an intermediate certificate to the Expressway-C that is signed by a certificate authority.

Correct Answer: C

QUESTION 4

An engineer is supporting an existing Cisco Collaboration deployment that has internal and external home users using the solution without VPN. Business usage also includes B2B calling for voice and video. Suddenly the engineer receives a report that one of the home office users cannot use the Cisco Jabber client, and shortly after, a few more reports come in for the same error. What must the engineer check first to resolve this issue?

A. client logs of the users

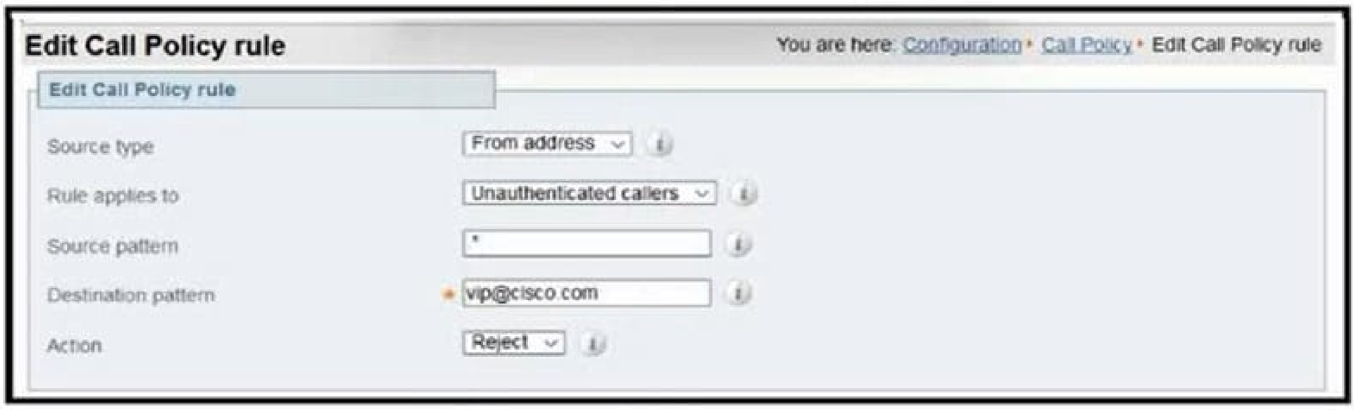
B. real-time monitoring toll logs for problems

C. alarms on the Cisco Expressways

D. alarms on the Cisco UCM Cluster

Correct Answer: C

QUESTION 5



Edit Call Policy rule

You are here: Configuration ▸ Call Policy ▸ Edit Call Policy rule

Edit Call Policy rule

Source type	From address
Rule applies to	Unauthenticated callers
Source pattern	*
Destination pattern	* vip@cisco.com
Action	Reject

Refer to the exhibit. Call policy rules on an Expressway-E prevent external callers from the internet from calling a VIP whose URI is vip@cisco.com. Which additional configuration setting is required for this call policy to function as intended?

A. The default zone on the Expressway-E must not be configured to treat as authenticated.

B. A search rule must be configured with an extract match for vip@cisco.com to pass the call to the Expressway-C.

C. The Cisco TelePresence endpoint registered with the URI vip@cisco.com must be set in "do not disturb" mode.

D. SIP TLS must be disabled on the Expressway-E.

Correct Answer: A

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-2/exwy_b_cisco-expressway-administrator-guide- x1402/exwy_m_device-authentication.html

[300-820 PDF Dumps](https://www.leads4pass.com/300-820.html) [300-820 Practice Test](https://www.leads4pass.com/300-820.html) [300-820 Braindumps](https://www.leads4pass.com/300-820.html)