Question 1

Question Type: MultipleChoice

D18912E1457D5D1DDCBD40AB3BF70D5D

```
Module="network.tcp" Level="DEBUG":  Dst-ip="10.0.101.119" Dst-port="7002" Detail="TCP Connecting"
Module="network.tcp" Level="DEBUG":  Dst-ip="10.0.101.119" Dst-port="7002" Detail="TCP Connection Established"
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.0.101.115" Src-port="27161" Dst-ip="10.0.101.119"
    Dst-port="7002" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-name="10.0.101.119"
```

📄 Valid from	Friday, October 18, 2019 ...
📄 Valid to	Sunday, October 17, 202...
📄 Subject	expe.pod1.local, Systems...
📄 Public key	RSA (4096 Bits)
📄 Public key parameters	05 00
🔧 Enhanced Key Usage	Server Authentication (1....
🔧 Subject Alternative Name	DNS Name=expe.pod1.local
🔧 Subject Key Identifier	c7b28ee75e675005198f9...

Location

Peer 1 address	10.0.101.119	ⓘ	SIP: Failed to connect to 10.0.101.119:7002 : TLS negotiation failure Check the certificates for the traversal connection
Peer 2 address		ⓘ	
Peer 3 address		ⓘ	
Peer 4 address		ⓘ	
Peer 5 address		ⓘ	
Peer 6 address		ⓘ	

Refer to the exhibit showing logs from the Expressway-C, a copy of the Expressway-E certificate, and the UC traversal zone configuration for the Expressway-C. An office administrator is deploying mobile and remote access and sees an issue with the UC traversal zone. The zone is showing "TLS negotiation failure". What is causing this issue?

Options:

A) The Expressway-E certificate includes the Expressway-C FQDN as a SAN entry

B) The Expressway-C is missing the FQDN of Cisco UCM in the Common Name of its certificate

C) In the UC Traversal Zone on the Expressway-C, the peer address is set to the IP of the Expressway-E, which is not a SAN entry in the Expressway-E certificate

D) The Expressway-E does not have the FQDN of Cisco UCM listed as a SAN in its certificate

Answer:

D

Question 2

Question Type: MultipleChoice

D18912E1457D5D1DDCBD40AB3BF70D5D

```
Module="network.tcp" Level="DEBUG":  Dst-ip="10.0.101.119" Dst-port="7002" Detail="TCP Connecting"
Module="network.tcp" Level="DEBUG":  Dst-ip="10.0.101.119" Dst-port="7002" Detail="TCP Connection Established"
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.0.101.115" Src-port="27161" Dst-ip="10.0.101.119"
    Dst-port="7002" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-name="10.0.101.119"
```

📄	Valid from	Friday, October 18, 2019 ...
📄	Valid to	Sunday, October 17, 202...
📄	Subject	expe.pod1.local, Systems...
📄	Public key	RSA (4096 Bits)
📄	Public key parameters	05 00
📄	Enhanced Key Usage	Server Authentication (1....
📄	Subject Alternative Name	DNS Name=expe.pod1.local
📄	Subject Key Identifier	c7b28ee75e675005198f9...

Location

Peer 1 address	10.0.101.119	ⓘ SIP: Failed to connect to 10.0.101.119:7002 : TLS negotiation failure
		Check the certificates for the traversal connection
Peer 2 address		ⓘ
Peer 3 address		ⓘ
Peer 4 address		ⓘ
Peer 5 address		ⓘ
Peer 6 address		ⓘ

Refer to the exhibit showing logs from the Expressway-C, a copy of the Expressway-E certificate, and the UC traversal zone configuration for the Expressway-C. An office administrator is deploying mobile and remote access and sees an issue with the UC traversal zone. The zone is showing "TLS negotiation failure". What is causing this issue?

Options:

A) The Expressway-E certificate includes the Expressway-C FQDN as a SAN entry

B) The Expressway-C is missing the FQDN of Cisco UCM in the Common Name of its certificate

C) In the UC Traversal Zone on the Expressway-C, the peer address is set to the IP of the Expressway-E, which is not a SAN entry in the Expressway-E certificate

D) The Expressway-E does not have the FQDN of Cisco UCM listed as a SAN in its certificate

Answer:
D