300-730 Q&As

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

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

https://www.pass2lead.com/300-730.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.

```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
Dst             src             state          conn-id        slot      status
10.10.10.1      172.16.1.1      MM_NO_STATE      0              0       ACTIVE
10.10.10.1      172.16.1.1      MM_NO_STATE      0              0       ACTIVE (deleted)
172.17.0.5      172.16.1.1      MM_NO_STATE      0              0       ACTIVE
172.17.0.5      172.16.1.1      MM_NO_STATE      0              0       ACTIVE (deleted)


Router#debug crypto isakmp

01:12:45.250: ISAKMP:(0):Old State = IKE_READY
                        New State = IKE_I_MM1
01:12:45.250: ISAKMP:(0): beginning Main Mode exchange
01:12:45.250: ISAKMP:(0): sending packet to 10.10.10.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:45.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:12:55.250: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
01:12:55.250: ISAKMP:(0): sending packet to 10.10.10.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:55.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

VPN tunnels between a spoke and two DMVPN hubs are not coming up. The network administrator has verified that the encryption, hashing, and DH group proposals for Phase 1 and Phase 2 match on both ends. What is the solution to this issue?

A. Ensure bidirectional UDP 500/4500 traffic.

B. Increase the isakmp phase 1 lifetime.

C. Add NAT statements for VPN traffic.

D. Enable shared tunnel protection.

Correct Answer: A

QUESTION 2

Refer to the exhibit.

```
interface Ethernet0
 nameif outside
 security-level0
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.0.1 255.255.255.0
!
object network InsideNet
subnet 10.7.7.0 255.255.255.0
!
object network RemoteNet
subnet 10.8.8.0 255.255.255.0
!
nat (inside,outside) source static InsideNet InsideNet destination static RemoteNet RemoteNet
!
access-list cmap10 extended permit ip object InsideNet object RemoteNet
!
route outside 0.0.0.0 0.0.0.0 172.16.1.1
!
crypto ipsec ikev1 transform-set AES256 esp-aes-256 esp-sha-hmac
!
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
!
crypto map cmap 10 match address cmap10
crypto map cmap 10 set peer 172.17.1.1
crypto map cmap 10 set ikev1 transform-set AES256
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key Cisco123
```

An engineer is building an IKEv1 tunnel to a peer Cisco ASA, but the tunnel is failing. Based on the configuration in the exhibit, which action must be taken to allow the VPN tunnel to come up?

A. Add a route for the 10.7.7.0/24 network to egress the outside interface.

B. Enable IKEv1 on the outside interface.

C. Change the IKEv1 policy number to be at least 256.

D. Change the transform set mode to transport.

Correct Answer: B

QUESTION 3

After a user configures a connection profile with a bookmark list and tests the clientless SSLVPN connection, all of the bookmarks are grayed out. What must be done to correct this behavior?

A. Apply the bookmark to the correct group policy.

B. Specify the correct port for the web server under the bookmark.

C. Configure a DNS server on the Cisco ASA and verify it has a record for the web server.

D. Verify HTTP/HTTPS connectivity between the Cisco ASA and the web server.

Correct Answer: C

QUESTION 4

Refer to the exhibit.

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

A customer cannot establish an IKEv2 site-to-site VPN tunnel between two Cisco ASA devices. Based on the syslog message, which action brings up the VPN tunnel?

A. Reduce the maximum SA limit on the local Cisco ASA.

B. Increase the maximum in-negotiation SA limit on the local Cisco ASA.

C. Remove the maximum SA limit on the remote Cisco ASA.

D. Correct the crypto access list on both Cisco ASA devices.

Correct Answer: B

QUESTION 5

What is a requirement for smart tunnels to function properly?

A. Java or ActiveX must be enabled on the client machine.

B. Applications must be UDP.

C. Stateful failover must not be configured.

D. The user on the client machine must have admin access.

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111007-smart-tunnel-asa-00.html