

## 300-730<sup>Q&As</sup>

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.lead4pass.com/300-730.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.

```
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

A network administrator is troubleshooting a FlexVPN tunnel. The hub router is unable to ping the spoke router's tunnel interface IP address of 192.168.1.2, even though the tunnel is showing up. The output of the debug ip packet CLI

command on the hub router shows the following entry.

IP: tableid=0123456789 s=192.168.1.1 (local), d=192.168.1.2 (loopback2), routed via FIB.

What must be configured to fix this issue?

- A. A matching IKEv2 pre-shared key on the hub and spoke routers in the crypto keyring configuration.
- B. An outbound ACL on the dynamic VTI of the hub router that allows ICMP traffic to 192.168.1.2.
- C. An IKEv2 authorization policy must be configured on the spoke router to advertise the interface route.
- D. A route map must be configured on hub router to set the next hop for 192.168.1.2 to the dynamic VTI.

Correct Answer: C

---

### QUESTION 3

Cisco AnyConnect Secure Mobility Client has been configured to use IKEv2 for one group of users and SSL for another group.

When the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect. What might be the problem?

- A. The XML profile is not configured correctly for the affected users.
- B. The new client image does not use the same major release as the current one.
- C. Client services are not enabled.
- D. Client software updates are not supported with IKEv2.

Correct Answer: C

On ASDM, under connection profile -> access interfaces -> IPSEC (IKEv2) Access : you can check or uncheck the boxes for "allow access" and "enable client access"

---

### QUESTION 4

Which feature of GETVPN is a limitation of DMVPN and FlexVPN?

- A. sequence numbers that enable scalable replay checking
- B. enabled use of ESP or AH
- C. design for use over public or private WAN
- D. no requirement for an overlay routing protocol

Correct Answer: D

---

## QUESTION 5

An administrator is setting up AnyConnect for the first time for a few users. Currently, the router does not have access to a RADIUS server. Which AnyConnect protocol must be used to allow users to authenticate?

- A. EAP-GTC
- B. EAP-MSCHAPv2
- C. EAP-MD5
- D. EAP-AnyConnect

Correct Answer: D

[Latest 300-730 Dumps](#)

[300-730 Study Guide](#)

[300-730 Braindumps](#)