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.geekcert.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.

```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: (0):      encryption AES-CBC
ISAKMP: (0):      keylength of 256
ISAKMP: (0):      hash SHA256
ISAKMP: (0):      default group 14
ISAKMP: (0):      auth pre-share
ISAKMP: (0):      life type in seconds
ISAKMP: (0):      life duration (basic) of 1200
ISAKMP: (0):atts are acceptable. Next payload is 0
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM4
ISAKMP: (1005):pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH...
ISAKMP: (1005):: incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
```

A site-to-site tunnel between two sites is not coming up. Based on the debugs, what is the cause of this issue?

A. An authentication failure occurs on the remote peer.

B. A certificate fragmentation issue occurs between both sides.

C. UDP 4500 traffic from the peer does not reach the router.

D. An authentication failure occurs on the router.

Correct Answer: C

QUESTION 2

A Cisco IOS router is reconfigured to connect to an additional DMVPN hub that is a part of a different DMVPN phase 3 cloud. After this change was made, users begin to experience problems accessing corporate resources over both tunnels. Before the additional tunnel was created, users could access resources over the first tunnel without any issues. Both tunnels terminate on the same interface of the router and use the same IPsec proposals. Which two actions

resolve the issue without affecting spoke-to-spoke traffic in either DMVPN cloud? (Choose two.)

A. Enable dead peer detection for both tunnels.

B. Use the same shared IPsec profile for both tunnels.

C. Configure the same NHRP network IDs for both tunnels.

D. Specify the tunnel destination in each tunnel.

E. Assign a unique tunnel key to each tunnel.

Correct Answer: DE

QUESTION 3

A network engineer has set up a FlexVPN server to terminate multiple FlexVPN clients. The VPN tunnels are established without issue. However, when a Change of Authorization is issued by the RADIUS server, the FlexVPN server does not update the authorization of connected FlexVPN clients. Which action resolves this issue?

A. Add the aaa server radius dynamic-author command on the FlexVPN clients.

B. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN server.

C. Add the aaa server radius dynamic-author command on the FlexVPN server.

D. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN clients.

Correct Answer: C

QUESTION 4

Users cannot log in to a Cisco ASA using clientless SSLVPN. Troubleshooting reveals the error message "WebVPN session terminated: Client type not supported". Which step does the administrator take to resolve this issue?

A. Enable the Cisco AnyConnect premium license on the Cisco ASA.

B. Have the user upgrade to a supported browser.

C. Increase the simultaneous logins on the group policy.

D. Enable the clientless VPN protocol on the group policy.

Correct Answer: D

QUESTION 5

An administrator is setting up a VPN on an ASA for users who need to access an internal RDP server. Due to security restrictions, the Microsoft RDP client is blocked from running on client workstations via Group Policy. Which VPN feature should be implemented by the administrator to allow these users to have access to the RDP server?

A. clientless proxy

B. smart tunnelcing

C. clientless plug-in

D. clientless rewriter

Correct Answer: C