300-730$^{\text{Q\&As}}$

Implementing Secure Solutions with Virtual Private Networks (SVPN)

QUESTION 1

A network engineer is configuring a server. The router will terminate encrypted VPN connections on g0/0, which is in the VRF "Internet". The clear-text traffic that must be encrypted before being sent out traverses g0/1, which is in the VRF "Internal". Which two VRF-specific configurations allow VPN traffic to traverse the VRF-aware interfaces? (Choose two.)

A. Under the IKEv2 profile, add the ivrf Internal command.

B. Under the virtual-template interface, add the ip vrf forwarding Internet command.

C. Under the IKEv2 profile, add the match fvrf Internal command.

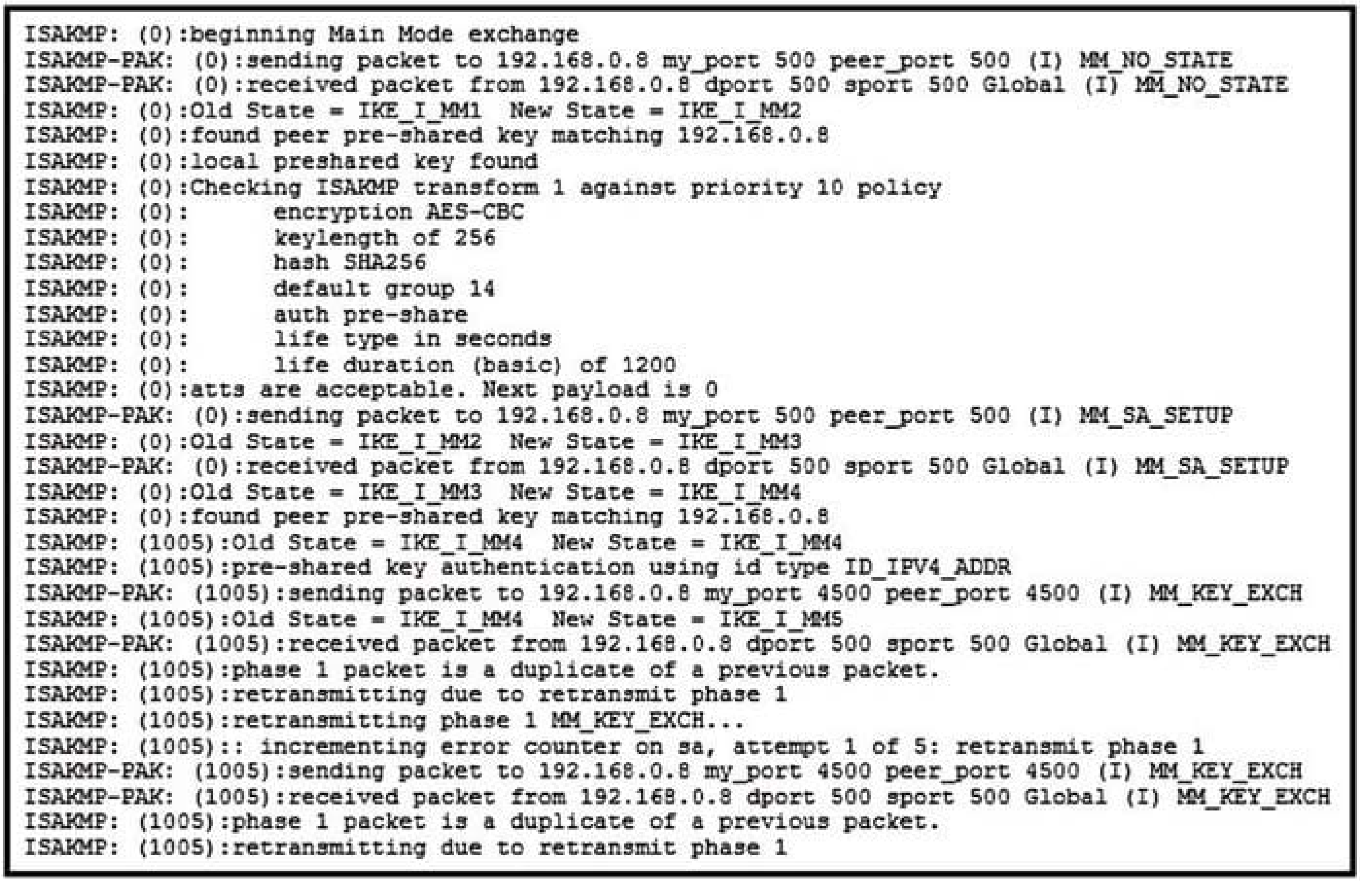
D. Under the IKEv2 profile, add the match fvrf Internet command.

E. Under the virtual-template interface, add the tunnel vrf Internet command.

Correct Answer: DE

QUESTION 2

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 3

Which configuration construct must be used in a FlexVPN tunnel?

A. EAP configuration

B. multipoint GRE tunnel interface

C. IKEv1 policy

D. IKEv2 profile

Correct Answer: D

QUESTION 4

Which two statements about the Cisco ASA Clientless SSL VPN solution are true? (Choose two.)

A. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the client uses the local DNS to perform FQDN resolution.

B. The rewriter enable command under the global webvpn configuration enables the rewriter functionality because that feature is disabled by default.

C. A Cisco ASA can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions.

D. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the ASA uses its configured DNS servers to perform FQDN resolution.

E. Clientless SSLVPN provides Layer 3 connectivity into the secured network.

Correct Answer: CD

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