Free Questions for 300-730 by certsdeals

Shared by Rowland on 09-08-2024

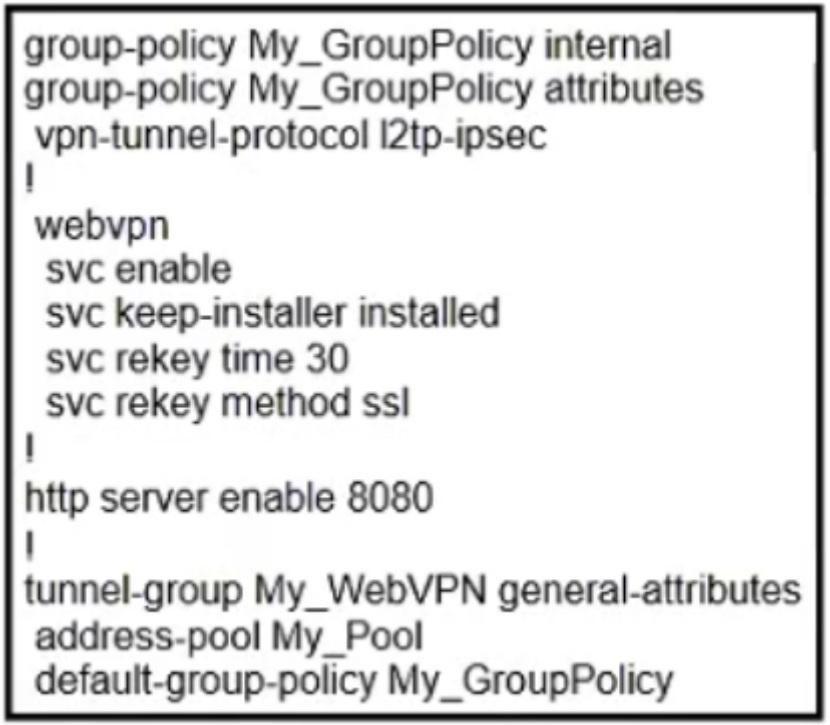
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Users cannot connect via AnyConnect SSLVPN. Which action resolves this issue?

Options:

A- Configure the ASA to act as a DHCP server.

B- Configure the HTTP server to listen on port 443.

C- Add an IPsec preshared key to the group policy.

D- Add ssl-client to the allowed list of VPN protocols.

Answer:

D

Question 2

Question Type: **MultipleChoice**

What is a characteristic of GETVPN?

Options:

A- An ACL that defines interesting traffic must be configured and applied to the crypto map.

B- Quick mode is used to create an IPsec SA.

C- The remote peer for the IPsec session is configured as part of the crypto map.

D- All peers have one IPsec SPI for inbound and outbound communication.

Answer:

D

Explanation:

In GETVPN, all group members share a common security association (SA) database and the same keys for encryption and decryption. This approach avoids the need for per-peer IPsec SAs and simplifies the configuration and management of the VPN. Instead of using multiple SAs, GETVPN uses a single SA with a unique Group Domain of Interpretation (GDOI) group key that is distributed to all group members.

Question 3

Question Type: MultipleChoice

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.)

Options:

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.

Answer:

D, E

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116000-flexvpn-config-00.html

crypto ikev2 profile CProfile

match fvrf internet // ('out vrf')

...

virtual-template 1

...

interface virtual-template 1 type tunnel

vrf forwarding internal // (internal vrf)

...

tunnel vrf internet // (out vrf)

Question 4

Question Type: **MultipleChoice**

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)


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?

Options:

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.

Answer:

A

Question 5

Question Type: MultipleChoice

An administrator is planning a VPN configuration that will encrypt traffic between multiple servers that will be passing unicast and multicast traffic. This configuration must be able to be implemented without the need to modify routing within the network. Which VPN technology must be used for this task?

Options:

A- FlexVPN

B- VTI

C- GETVPN

D- DMVPN

Answer:

C

Explanation:

The VPN technology that must be used for this task is GETVPN (Group Encrypted Transport VPN). GETVPN is designed to encrypt both unicast and multicast traffic while preserving the original source and destination IP addresses, and it does not require any changes to the existing routing infrastructure. Additionally, GETVPN provides a scalable and efficient solution for encrypting traffic within a network, making it a good choice for this scenario.

Question 6

Question Type: MultipleChoice

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?

Options:

A- clientless proxy

B- smart tunneling

C- clientless plug-in

D- clientless rewriter

Answer:

C

Question 7

Question Type: MultipleChoice

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?

Options:

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.

Answer:

D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html#anc15

Question 8

Question Type: MultipleChoice

A user is experiencing delays on audio calls over a Cisco AnyConnect VPN. Which implementation step resolves this issue?

Options:

A- Change to 3DES Encryption.

B- Shorten the encryption key lifetime.

C- Install the Cisco AnyConnect 2.3 client for the user to download.

D- Enable DTLS.

Answer:

D