Free Questions for 300-730 by certsinside

Shared by Ramsey on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An engineer is using DMVPN to provide secure connectivity between a data center and remote sites. Which two routing protocols should be used between the routers? (Choose two.)

Options:

A- IS-IS

B- BGP

C- RIPv2

D- OSPF

E- EIGRP

Answer:

B, E

Question 2

Question Type: MultipleChoice

Which feature allows a DMVPN Phase 3 spoke to switch to an alternate hub when the primary hub is unreachable?

Options:

A- multicast PIM

B- backup NHS

C- per-tunnel jitter probes

D- NHRP shortcut

Answer:

B

Explanation:

The DMVPN-Tunnel Health Monitoring and Recovery (Backup NHS) feature allows you to control the number of connections to the Dynamic Multipoint Virtual Private Network (DMVPN) hub and allows you to switch to alternate hubs in case of a connection failure to the primary hubs. https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-2mt/sec-conn-dmvpn-backup-nhs.html#:~:text=The%20DMVPN%2DTunnel%20Health%20Monitoring%20and%20Recovery%20(Backup%20NHS),failure%20to%20the%20prima

Backup NHS, or Next Hop Server, is a feature of DMVPN Phase 3 that allows a spoke router to switch to an alternate hub when the primary hub is unreachable. This is accomplished by using a secondary IP address for the hub router, which is used as the next hop for any traffic sent by the spoke router to the hub.

Question 3

Question Type: MultipleChoice

A user is trying to log in to a Cisco ASA using the clientless SSLVPN feature and receives the error message "clientless (browser) SSLVPN access is not allowed". Which step should the Cisco ASA administrator take to resolve this issue?

Options:

A- Enable the clientless VPN protocol on the group policy.

B- Validate that the correct license is in use on the ASA for WebVPN.

C- Increase the number of simultaneous logins allowed on the group policy.

D- Verify that a user account exists in the local AAA database for the user.

Answer:

B

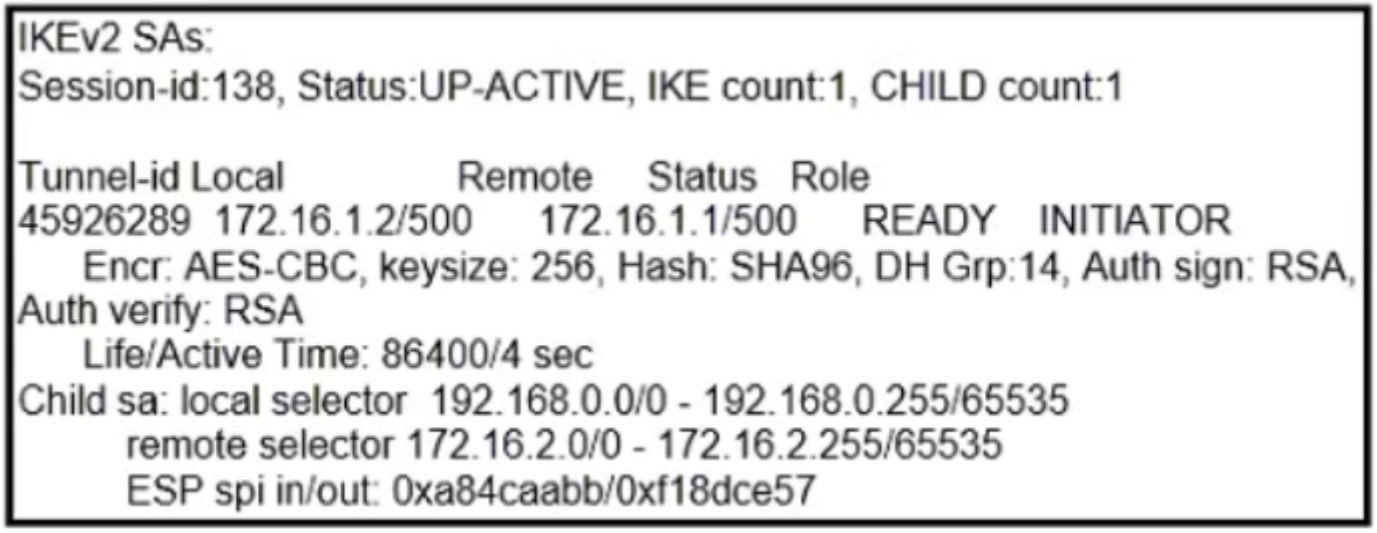
Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html#anc12
https://community.cisco.com/t5/vpn/clientless-vpn-clientless-browser-ssl-vpn-access-is-not-allowed/td-p/1569690

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



A Cisco ASA is configured as a client to a router running as a FlexVPN server. The router is configured with a virtual template to terminate FlexVPN clients. Traffic between networks 192.168.0.0/24 and 172.16.20.0/24 does not work as expected. Based on the show crypto ikev2 sa output collected from the Cisco ASA in the exhibit, what is the solution to this issue?

Options:

A- Modify the crypto ACL on the router to permit network 192.168.0.0/24 to network 172.16.20.0/24.

B- Modify the crypto ACL on the ASA to permit network 192.168.0.0/24 to network 172.16.20.0/24.

C- Modify the crypto ACL on the ASA to permit network 172.16.20.0/24 to network 192.168.0.0/24.

D- Modify the crypto ACL on the router to permit network 172.16.20.0/24 to network 192.168.0.0/24.

Answer:

B

Explanation:

the show crypto ukev2 sa output from the ASA, the local selector is 192.168.0.0/24 the remote selector is 172.16.2.0/24 (which is wrong , should be .20.0/24) . so , the ACL in the ASA should be to permit 192.168.0.0/24 to 172.16.20.0/24

Question 5

Question Type: MultipleChoice

An engineer has successfully established a Phase 1 and Phase 2 tunnel between two sites. Site A has internal subnet 192.168.0.0/24 and Site B has internal subnet 10.0.0.0/24. The engineer notices that no packets are decrypted at Site B. Pings to 192.168.0.1 from internal Site B devices make it to the Site B router, and the Site A router has incrementing encrypt and decrypt counters. What must be done to ensure bidirectional communication between both sites?

Options:

A- Modify the routing at Site B so that traffic is sent to Site A.

B- Configure the correct DH group on both devices.

C- Allow protocol ESP or AH on the firewall in front of the Site B router.

D- Enable PFS on the headend device.

Answer:

C

Question 6

Question Type: **MultipleChoice**

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-level100
 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?

Options:

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.

Answer:

B

Question 7

Question Type: **MultipleChoice**

Which DMVPN feature allows spokes to be deployed with dynamically assigned public IP addresses?

Options:

A- 2547oDMVPN

B- NHRP

C- OSPF

D- NAT Traversal

Answer:

B