Free Questions for 300-730 by dumpshq

Shared by Fox on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

```
Flex-spoke#crypto ikev2 authorization policy default
  route set interface
  route set remote ipv4 192.168.200.0 255.255.255.0

Flex-spoke#crypto ikev2 profile default
 aaa authorization group psk list default default

!--- Output is truncated ---!

Flex-spoke#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local              Remote             fvrf/ivrf         Status
1       10.0.20.41/500       172.18.3.143/500       none/none          READY
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: RSA
     Life/Active Time: 86400/6845 sec
     CE id: 1043, Session-id: 22
     Status Description: Negotiation done
     Local spi: 3413E984EC151E8D      Remote spi: 92479BD873F59132
     Local id: 10.0.20.41
     Remote id: hostname=flex-hub.cisco.com,cn=flex-hub.cisco.com
     Local req msg id:  0           Remote req msg id:  4
     Local next msg id: 0           Remote next msg id: 4
     Local req queued:  0           Remote req queued:  4
     Local window:      5           Remote window:      5
     DPD configured for 60 seconds, retry 2
     NAT-T is not detected
     Cisco Trust Security SGT is disabled      Initiator of SA : No

     Remote subnets:
     10.0.0.1 255.255.255.255
     192.168.100.0 255.255.255.0

 IPv6 Crypto IKEv2  SA
```

An engineer has configured a spoke to connect to a FlexVPN hub. The tunnel is up, but pings fail when the engineer attempts to reach host 192.168.200.10 behind the spoke, and traffic is sourced from host 192.168.100.3, which is behind the FlexVPN server. Based on packet captures, the engineer discovers that host 192.168.200.10 receives the icmp echo and sends an icmp reply that makes it to the inside interface of the spoke. Based on the output in the exhibit captured on the spoke by the engineer, which action resolves this issue?

Options:

A- Add the aaa authorization group cert list default default command to the spoke ikev2 profile.

B- Add the route set remote ipv4 192.168.200.0 255.255.255.0 command to the hub authorization policy.

C- Add the aaa authorization group cert list default default command to the hub ikev2 profile.

D- Add the route set remote ipv4 192.168.100.0 255.255.255.0 command to the spoke authorization policy.

Answer:

D

Explanation:

The problem is that the spoke does not have a route to the host 192.168.100.3, which is behind the FlexVPN server. The spoke only has a default route to the tunnel interface, which points to the FlexVPN hub. Therefore, when the spoke receives the icmp reply from host 192.168.200.10, it does not know how to forward it to host 192.168.100.3.

One way to solve this problem is to add a route to the host 192.168.100.3 on the spoke using the route set remote ipv4 command in the authorization policy on the spoke. This command allows the FlexVPN server to push a route to the FlexVPN client during IKEv2 authorization. For example:

crypto ikev2 authorization policy default route set remote ipv4 192.168.100.0 255.255.255.0

This way, the spoke will have a more specific route to host 192.168.100.3 via the tunnel interface, and will be able to forward the icmp reply correctly.

Question 2

Question Type: MultipleChoice

What must be configured in a FlexVPN deployment to allow for direct communication between spokes connected to different hubs?

Options:

A- EIGRP must be used as routing protocol.

B- Hub routers must be on same Layer 2 network.

C- Load balancing must be disabled.

D- A GRE tunnel must exist between hub routers.

Answer:

D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/118888-configure-flexvpn-00.html

Question 3

Question Type: MultipleChoice

A network engineer has almost finished setting up a clientless VPN that allows remote users to access internal HTTP servers. Users must enter their username and password twice: once on the clientless VPN web portal and again to log in to internal HTTP servers. The Cisco ASA and the HTTP servers use the same Active Directory server to authenticate users. Which next step must be taken to allow users to enter their password only once?

Options:

A- Use LDAPS and add password management to the clientless tunnel group.

B- Configure auto-sign-on using NTLM authentication.

C- Set up the Cisco ASA to authenticate users via a SAML 2.0 IDP.

D- Create smart tunnels for the HTTP servers.

Answer:

B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html#anc17

Question 4

Question Type: MultipleChoice

A network engineer is setting up Cisco AnyConnect 4.9 on a Cisco ASA running ASA software 9.1. Cisco AnyConnect must connect to the Cisco ASA before the user logs on so that login scripts can work successfully. In addition, the VPN must connect without user intervention. Which two key steps accomplish this task? (Choose two.)

Options:

A- Create a Network Access Manager profile with a client policy set to connect before user logon.

B- Create a Cisco AnyConnect VPN profile with Start Before Logon set to true.

C- Issue an identity certificate to the trusted root CA folder in the machine store.

D- Create a Cisco AnyConnect VPN profile with Always On set to true.

E- Create a Cisco Anyconnect VPN Management Tunnel profile.

Answer:

B, C

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/215442-configure-anyconnect-management-vpn-tunn.html

Question 5

Question Type: MultipleChoice

A network engineer is installing Cisco AnyConnect on company laptops so that users can access corporate resources remotely. The VPN concentrator is a Cisco router running IOS-XE 16.9.1 code and configured as a FlexVPN server that uses local authentication and *$Cisc431089017$* as the key-id for the IKEv2 profile. Which two steps must be taken on the computer to allow a successful AnyConnect connection to the router? (Choose two.)

Options:

A- In the Cisco AnyConnect XML profile, set the IPsec Authentication method to EAP-AnyConnect.

B- In the Cisco AnyConnect XML profile, add the hostname and host address to the server list.

C- In the Cisco AnyConnect XML profile, set the user group field to DefaultAnyConnectClientGroup.

D- In the Cisco AnyConnect Local Policy, set the BypassDownloader option in the local to true.

E- In the Cisco AnyConnect Local Policy, add the router IP address to the Update Policy.

B) In the Cisco AnyConnect XML profile, adding the hostname and host address to the server list ensures that the AnyConnect client knows the address of the VPN concentrator (router) to connect to. E. In the Cisco AnyConnect Local Policy, adding the router IP address to the Update Policy allows the client to connect to the router for updates and configuration.

Answer:

B, E

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override


Gateway of last resort is 192.168.1.1 to network 0.0.0.0


      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
B        172.16.0.0/16 [200/0] via 172.16.1.1, 00:06:27
H        172.16.0.1/32 is directly connected, 00:06:38, Tunnel2
S  %     172.16.1.1/32 is directly connected, Tunnel7
C        172.16.1.3/32 is directly connected, Tunnel7
H        172.16.1.4/32 is directly connected, 00:01:30, Virtual-Access10
S        172.16.2.1/32 is directly connected, Tunnel2
C        172.16.2.3/32 is directly connected, Tunnel2
H        172.16.2.4/32 [250/1] via 172.16.2.3, 00:01:30, Virtual-Access10
      192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1
L        192.168.1.3/32 is directly connected, Ethernet0/1
      192.168.4.0/32 is subnetted, 1 subnets
H        192.168.4.4 [250/1] via 172.16.1.3, 00:01:30, Virtual-Access10
```

Given the output of the show ip route command, which remote access VPN technology is in use?

Options:

A- Reverse Route Injection

B- FlexVPN

C- Dynamic Crypto Map

D- DMVPN

Answer:

B

Explanation:

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex-spoke.html

Question 7

Question Type: MultipleChoice

An administrator must guarantee that remote access users are able to reach printers on their local LAN after a VPN session is established to the headquarters. All other traffic should be sent over the tunnel. Which split-tunnel policy reduces the configuration on the ASA headend?

Options:

A- include specified

B- exclude specified

C- tunnel specified

D- dynamic exclude

Answer:

B

Explanation:

You could in theory 'tunnel specified' and list every subnet aside from the local one in the split tunnel list, but that is cumbersome and clearly not the best answer from the 'reduce the configuration' requirement. Exclude only the local subnet and continue with your day.