QUESTION 49
Which two statements are true when designing a SSL VPN solution using Cisco AnyConnect? (Choose two.)

A. The VPN server must have a self-signed certificate.
B. A SSL group pre-shared key must be configured on the server.
C. Server side certificate is optional if using AAA for client authentication.
D. The VPN IP address pool can overlap with the rest of the LAN networks.
E. DTLS can be enabled for better performance.

Answer: DE

QUESTION 50
An engineer is configuring IPsec VPN and wants to choose an authentication protocol that is reliable and supports ACK and sequence.
Which protocol accomplishes this goal?

A. IKEv1
B. AES-192
C. ESP
D. AES-256

Answer: C

QUESTION 51
Refer to the exhibit. What is the problem with the IKEv2 site-to-site VPN tunnel?

```
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):Failed to verify the proposed
policies
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):There was no IPSEC policy found for
received TS

*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):SM Trace-> SA:
I_SPI=527FCACA776C4724 R_SPI=EFBD7D296CCB08CA (R) MsgID = 00000001 CurState:
R_VERIFY_AUTH Event: EV_TS_UNACCEPT
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):Sending TS unacceptable notify
```

A. incorrect PSK
B. crypto access list mismatch

C. incorrect tunnel group
D. crypto policy mismatch
E. incorrect certificate

Answer: B

QUESTION 52
Which requirement is needed to use local authentication for Cisco AnyConnect Secure Mobility Clients that connect to a FlexVPN server?

A. use of certificates instead of username and password
B. EAP-AnyConnect
C. EAP query-identity
D. AnyConnect profile

Answer: D
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html

QUESTION 53
Which IKE identity does an IOS/IOS-XE headend expect to receive if an IPsec Cisco AnyConnect client uses default settings?

A. *$SecureMobilityClient$*
B. *$AnyConnectClient$*
C. *$RemoteAccessVpnClient$*
D. *$DfltIkeIdentityS*

Answer: B
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html

QUESTION 54
Refer to the exhibit. Which VPN technology is allowed for users connecting to the Employee tunnel group?

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 dns-server value 10.10.10.10
 vpn-tunnel-protocol ssl-clientless
 default-domain value cisco.com
 address-pools value ACPool

group-policy Admin_Group internal
group-policy Admin_Group attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-clientless
 split-tunnel-policy tunnelall

tunnel-group Admins type remote-access
tunnel-group Admins general-attributes
 default-group-policy Admin_Group
tunnel-group Admins webvpn-attributes
 group-alias Admins enable

tunnel-group Employee type remote-access
tunnel-group Employee webvpn-attributes
 group-alias Employee enable

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

A. SSL AnyConnect
B. IKEv2 AnyConnect
C. crypto map
D. clientless

Answer: B

QUESTION 55
Refer to the exhibit. An engineer is troubleshooting a new GRE over IPsec tunnel.
The tunnel is established but the engineer cannot ping from spoke 1 to spoke 2.
Which type of traffic is being blocked?

```
Spoke1#
     local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     #pkts encaps: 200, #pkts encrypt: 200
     #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.2.1
     inbound esp sas:
     spi: 034B32CA36 (1261619766)
     outbound esp sas:
     spi:0xD601918E (1760427022)

Spoke2#
     local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     #pkts encaps: 210, #pkts encrypt: 210,
     #pkts decaps: 200, #pkts decrypt: 200,
local crypto endpt.: 192.168.2.1,
remote crypto endpt.: 192.168.1.1
     inbound esp sas:
     spi: 03D601918E (1760427022)
     outbound esp sas:
     spi: 034BS2CA36 (1261619766)
```

A. ESP packets from spoke2 to spoke1
B. ISAKMP packets from spoke2 to spoke1
C. ESP packets from spoke1 to spoke2
D. ISAKMP packets from spoke1 to spoke2

Answer: A

QUESTION 56
Which command is used to troubleshoot an IPv6 FlexVPN spoke-to-hub connectivity failure?

A. show crypto ikev2 sa
B. show crypto isakmp sa
C. show crypto gkm
D. show crypto identity

Answer: A
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116413-configure-flexvpn-00.pdf

QUESTION 57
In a FlexVPN deployment, the spokes successfully connect to the hub, but spoke-to-spoke tunnels do not form. Which troubleshooting step solves the issue?

A. Verify the spoke configuration to check if the NHRP redirect is enabled.
B. Verify that the spoke receives redirect messages and sends resolution requests.
C. Verify the hub configuration to check if the NHRP shortcut is enabled.
D. Verify that the tunnel interface is contained within a VRF.

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-summ-maps.pdf

QUESTION 58
An engineer is troubleshooting a new DMVPN setup on a Cisco IOS router. After the show crypto isakmp sa command is issued, a response is returned of "MM_NO_STATE." Why does this failure occur?

A. The ISAKMP policy priority values are invalid.
B. ESP traffic is being dropped.
C. The Phase 1 policy does not match on both devices.
D. Tunnel protection is not applied to the DMVPN tunnel.

Answer: B

QUESTION 59
What are two variables for configuring clientless SSL VPN single sign-on? (Choose two.)

A. CSCO_WEBVPN_OTP_PASSWORD
B. CSCO_WEBVPN_INTERNAL_PASSWORD
C. CSCO_WEBVPN_USERNAME
D. CSCO_WEBVPN_RADIUS_USER

Answer: BC

QUESTION 60
Which two NHRP functions are specific to DMVPN Phase 3 implementation? (Choose two.)

A. registration request
B. registration reply
C. resolution request
D. resolution reply
E. redirect

Answer: DE