QUESTION 95
An administrator is designing a VPN with a partner's non-Cisco VPN solution. The partner's VPN device will negotiate an IKEv2 tunnel that will only encrypt subnets 192.168.0.0/24 going to 10.0.0.0/24. Which technology must be used to meet these requirements?

A. VTI
B. crypto map
C. GETVPN
D. DMVPN

Answer: B

QUESTION 96
A company's remote locations connect to the data centers via MPLS. A new request requires that unicast and multicast traffic that exits in the remote locations be encrypted. Which non-tunneled technology should be used to satisfy this requirement?

A. SSL
B. FlexVPN
C. DMVPN
D. GETVPN

Answer: D

QUESTION 97
While troubleshooting, an engineer finds that the show crypto isakmp sa command indicates that the last state of the tunnel is MM_KEY_EXCH. What is the next step that should be taken to resolve this issue?

A. Verify that the ISAKMP proposals match.
B. Ensure that UDP 500 is not being blocked between the devices.
C. Correct the peer's IP address on the crypto map.
D. Confirm that the pre-shared keys match on both devices.

Answer: C

QUESTION 98
Which VPN technology must be used to ensure that routers are able to dynamically form connections with each other rather than sending traffic through a hub and be able to advertise routes without the use of a dynamic routing protocol?

A. FlexVPN
B. DMVPN Phase 3
C. DMVPN Phase 2
D. GETVPN

Answer: B

QUESTION 99
An administrator is setting up AnyConnect for the first time for a few users. Currently, the router does not have access to a RADIUS server. Which AnyConnect protocol must be used to allow users to authenticate?

A. EAP-GTC
B. EAP-MSCHAPv2
C. EAP-MD5
D. EAP-AnyConnect

Answer: D

QUESTION 100
Refer to the exhibit. DMVPN spoke-to-spoke traffic works, but it passes through the hub, and never sends direct spoke-to-spoke traffic. Based on the tunnel interface configuration shown, what must be configured on the hub to solve the issue?

```
interface Tunnel0
 ip address 192.168.1.1 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 no ip split-horizon eigrp 90
 ip next-hop-self eigrp 90
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco
```

A. Enable NHRP redirect.
B. Enable split horizon.
C. Enable IP redirects.
D. Enable NHRP shortcut.

Answer: D

QUESTION 101
Refer to the exhibit. A user is connecting from behind a PC with a private IP Address. Their ISP provider is blocking TCP port 443. Which AnyConnect XML configuration will allow the user to establish a connection with the ASA?
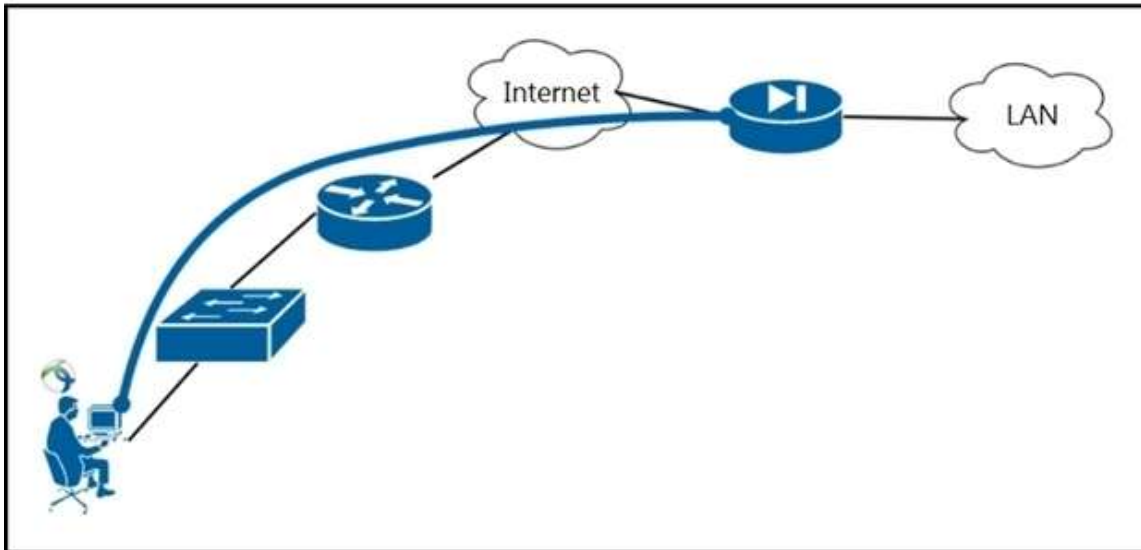
A.
```
<HostEntry>
    <HostName>RAVPN</HostName>
    <HostAddress>209.165.202.129</HostAddress>
    <PrimaryProtocol>IPsec
        <StandardAuthenticationOnly>false</StandardAuthenticationOnly>
    </PrimaryProtocol>
</HostEntry>
```

B.
```
<HostEntry>
    <HostName>RAVPN</HostName>
    <HostAddress>209.165.200.225</HostAddress>
    <PrimaryProtocol>IPsec
        <StandardAuthenticationOnly>false</StandardAuthenticationOnly>
    </PrimaryProtocol>
</HostEntry>
```

C.
```
<HostEntry>
    <HostName>RAVPN</HostName>
    <HostAddress>209.165.202.129</HostAddress>
</HostEntry>
```

D.
```
<HostEntry>
    <HostName>RAVPN</HostName>
    <HostAddress>209.165.200.225</HostAddress>
</HostEntry>
```

Answer: D

QUESTION 102
Refer to the exhibit. Which two conclusions should be drawn from the DMVPN phase 2 configuration? (Choose two.)

```
interface Tunnel0
  ip address 172.16.1.1 255.255.255.0
  no ip redirects
ip mtu 1440
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 150
no ip split-horizon eigrp 100
no ip next-hop-self eigrp 100
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
```

A. Next-hop-self is required.
B. EIGRP neighbor adjacency will fail.
C. EIGRP is used as the dynamic routing protocol.
D. EIGRP route redistribution is not allowed.
E. Spoke-to-spoke communication is allowed.

Answer: CE

QUESTION 103
Refer to the exhibit. The VPN tunnel between the FlexVPN spoke and FlexVPN hub 192.168.0.12 is failing.
What should be done to correct this issue?

```
aaa authentication login default local
aaa authorization network Flex_AAA local

crypto ikev2 authorization policy Flex_Auth
 route set remote ipv4 10.0.0.0 255.255.255.0

crypto ikev2 proposal Crypto_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy Crypto_Policy
 proposal Crypto_Proposal

crypto ikev2 keyring FlexKey
 peer any
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !

crypto ikev2 profile IKEv2_Profile
 match identity remote address 192.168.0.12 255.255.255.255
 authentication local pre-share
 authentication remote pre-share
 keyring local FlexKey
 aaa authorization group cert list Flex_AAA Flex_Auth

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel

crypto ipsec profile FlexVPN_Ipsec
 set transform-set TS
 set ikev2-profile IKEv2_Profile

interface Tunnel1
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 192.168.0.12
 tunnel protection ipsec profile FlexVPN_Ipsec
```

A. Add the address 192.168.0.12 255.255.255.255 command to the keyring configuration.
B. Add the match fvrf any command to the IKEv2 policy.
C. Add the aaa authorization group psk list Flex_AAA Flex_Auth command to the IKEv2 profile configuration.
D. Add the tunnel mode gre ip command to the tunnel configuration.

Answer: C

QUESTION 104
Refer to the exhibit. An IKEv2 site-to-site tunnel between an ASA and a remote peer is not building successfully. What will fix the problem based on the debug output?

```
*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. Ensure crypto IPsec policy matches on both VPN devices.
B. Install the correct certificate to validate the peer.
C. Correct crypto access list on both VPN devices.
D. Specify the peer IP address in the tunnel group name.

Answer: A

QUESTION 105
Refer to the exhibit. A network engineer is reconfiguring clientless SSLVPN during a maintenance window, and after testing the new configuration, is unable to establish the connection. What must be done to remediate this problem?

```
webvpn
 port 9443
 enable outside
 dtls port 9443
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.9.03049-webdeploy-k9.pkg 3
 anyconnect profiles vpn_profile_1 disk0:/vpn_profile_1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
group-policy vpn_policy internal
group-policy vpn_policy attributes
 dns-server value 192.168.1.3
 vpn-tunnel-protocol ssl-client
 address-pools value vpn_pool
```

A. Enable client services on the outside interface.
B. Enable clientless protocol under the group policy.
C. Enable DTLS under the group policy.
D. Enable auto sign-on for the user's IP address.

Answer: B

QUESTION 106
What are two purposes of the key server in Cisco IOS GETVPN? (Choose two.)

A. to download encryption keys
B. to maintain encryption policies
C. to distribute routing information

D. to encrypt data traffic
E. to authenticate group members

Answer: BE

QUESTION 107
An engineer notices that while an employee is connected remotely, all traffic is being routed to the corporate network. Which split-tunnel policy allows a remote client to use their local provider for Internet access when working from home?

A. tunnelall
B. excludeall
C. tunnelspecified
D. excludespecified

Answer: C

QUESTION 108
In order to enable FlexVPN to use a AAA attribute list, which two tasks must be performed? (Choose two.)

A. Define the RADIUS server.
B. Verify that clients are using the correct authorization policy.
C. Define the AAA server.
D. Assign the list to an authorization policy.
E. Set the maximum segment size.

Answer: BD

QUESTION 109
Which technology and VPN component allows a VPN headend to dynamically learn post NAT IP addresses of remote routers at different sites?

A. DMVPN with ISAKMP
B. GETVPN with ISAKMP
C. DMVPN with NHRP
D. GETVPN with NHRP

Answer: C

QUESTION 110
An engineer must configure remote desktop connectivity for offsite admins via clientless SSL VPN, configured on a Cisco ASA to Windows Vista workstations. Which two configurations provide the requested access? (Choose two.)

A. Telnet bookmark via the Telnet plugin
B. RDP2 bookmark via the RDP2 plugin
C. VNC bookmark via the VNC plugin
D. Citrix bookmark via the ICA plugin
E. SSH bookmark via the SSH plugin

Answer: BE

QUESTION 111
A network engineer must design a clientless VPN solution for a company. VPN users must be able to access several internal web servers. When reachability to those web servers was tested, it was found that one website is not being rewritten correctly by the ASA. What is a potential solution for this issue while still allowing it to be a clientless VPN setup?

A. Set up a smart tunnel with the IP address of the web server.
B. Set up a NAT rule that translates the ASA public address to the web server private address on port 80.
C. Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.
D. Set up a WebACL to permit the IP address of the web server.

Answer: A

QUESTION 112
Which two types of SSO functionality are available on the Cisco ASA without any external SSO servers? (Choose two.)

A. SAML
B. NTLM
C. Kerberos
D. OAuth 2.0
E. HTTP Basic

Answer: BE

QUESTION 113
Refer to the exhibit. Which type of VPN implementation is displayed?

```
hostname RouterA
interface GigabitEthernet 0/0/0
ip address 10.0.0.1 255.255.255.0
standby 1 priority 110
standby ikev1-cluster
end

crypto ikev2 cluster
  standby-group ikev1-cluster
  slave max-session 500
  port 2000
  no shutdown

crypto ikev2 redirect gateway init
```

A. IKEv1 cluster
B. IKEv2 backup gateway
C. IKEv2 load balancer
D. IKEv2 reconnect

Answer: C