Number: 300-730
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: 300-730
Exam Name: Implementing Secure Solutions with Virtual Private Networks

Exam A

QUESTION 1
Which Cisco AnyConnect component ensures that devices in a specific internal subnet are only accessible using port 443?

A. routing
B. WebACL
C. split tunnel
D. VPN filter

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/pix-500-series-security-appliances/99103-pix-asa-vpn-filter.html#anc6

QUESTION 2
Refer to the exhibit.

```
interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

 protected vrf: (none)
 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 current_peer 192.168.0.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 16228, #pkts encrypt: 16228, #pkts digest: 16228
  #pkts decaps: 26773, #pkts decrypt: 26773, #pkts verify: 26773
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
  #pkts invalid prot (recv) 0, #pkts verify failed: 0
  #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
  ##pkts replay failed (rcv): 23751
  #pkts tagged (send): 0, #pkts untagged (rcv): 0
  #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (recv) 0

  local crypto endpt.: 10.10.10.1, remote crypto endpt.: 192.168.0.1
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
  current outbound spi: 0x48998999(1218021785)
  PFS (Y/N): N, DH group: none
```

Upon setting up a tunnel between two sites, users are complaining that connections to applications over the VPN are not working consistently. The output of show crypto ipsec sa was collected on one of the VPN devices. Based on this output, what should be done to fix this issue?

A. Lower the tunnel MTU.
B. Enable perfect forward secrecy.
C. Specify the application networks in the remote identity.
D. Make an adjustment to IPSec replay window.

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dplane/configuration/xe-16-8/secipsec-data-plane-xe-16-8-book/sec-ipsec-antireplay.html#GUID-1FF00FBB-0746-48B2-A02A-2BB066BEDEF8

QUESTION 3
After a user configures a connection profile with a bookmark list and tests the clientless SSLVPN connection, all of the bookmarks are grayed out. What must be done to correct this behavior?

A. Apply the bookmark to the correct group policy.
B. Specify the correct port for the web server under the bookmark.
C. Configure a DNS server on the Cisco ASA and verify it has a record for the web server.
D. Verify HTTP/HTTPS connectivity between the Cisco ASA and the web server.

Correct Answer: C
Section:

QUESTION 4
Refer to the exhibit.

```
crypto gdoi group GDOI-GROUP1
server local
 address ipv4 10.0.0.1
 redundancy
  local priority 250
  peer address ipv4 10.0.6.1
```

Which type of VPN is being configured, based on the partial configuration snippet?

A. GET VPN with COOP key server
B. GET VPN with dual group member
C. FlexVPN load balancer
D. FlexVPN backup gateway

Correct Answer: A
Section:

QUESTION 5
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

Correct Answer: B
Section:

QUESTION 6
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

Correct Answer: D
Section:

QUESTION 7
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.

Correct Answer: D
Section:
Explanation:
https://www.networkworld.com/article/2288666/chapter-4--common-ipsec-vpn-issues.html

QUESTION 8
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

Correct Answer: B
Section:
Explanation:
DMVPN stands for Dynamic Multipoint VPN, which is a technology that allows routers to dynamicallyform VPN tunnels with each other without requiring a pre-configured static crypto map. DMVPN usesMultipoint GRE (mGRE) interfaces and Next Hop Resolution Protocol (NHRP) to establish directconnections between routers. DMVPN has three phases of operation, each with different features andbenefits.DMVPN Phase 1 is the basic configuration, where all spokes are configured with a single mGRE interfacethat points to the hub as the NHRP server. The spokes can only communicate with the hub, not witheach other. All traffic must go through the hub, which creates a bottleneck and increases latency.DMVPN Phase 2 improves on Phase 1 by allowing spoke-to-spoke communication without going throughthe hub. This is achieved by using NHRP to dynamically resolve the IP address of the destination spokeand create a direct GRE tunnel between the spokes. However, this still requires the use of a dynamicrouting protocol to advertise routes between the spokes, which adds overhead and complexity.DMVPN Phase 3 further enhances Phase 2 by enabling spoke-to-spoke communication without requiringa dynamic routing protocol. This is done by using NHRP shortcut switching and NHRP redirect messages.When a spoke wants to send traffic to another spoke, it sends an NHRP resolution request to the hub,which responds with an NHRP redirect message containing the IP address of the destination spoke. The

QUESTION 9
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

Correct Answer: D
Section:

QUESTION 10
Which benefit of FlexVPN is a limitation of DMVPN using IKEv1?

A. GRE encapsulation allows for forwarding of non-IP traffic.
B. IKE implementation can install routes in routing table.
C. NHRP authentication provides enhanced security.
D. Dynamic routing protocols can be configured.

Correct Answer: B
Section:

QUESTION 11
What is a requirement for smart tunnels to function properly?

A. Java or ActiveX must be enabled on the client machine.
B. Applications must be UDP.
C. Stateful failover must not be configured.
D. The user on the client machine must have admin access.

Correct Answer: A
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-nextgeneration-firewalls/111007-smart-tunnel-asa-00.html

QUESTION 12
Where is split tunneling defined for IKEv2 remote access clients on a Cisco router?

A. IKEv2 authorization policy
B. Group Policy
C. virtual template
D. webvpn context

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/routers/3600-series-multiservice-platforms/91193-rtr-ipsec-internet-connect.html

QUESTION 13
Which technology is used to send multicast traffic over a site-to-site VPN?

A. GRE over IPsec on IOS router
B. GRE over IPsec on FTD
C. IPsec tunnel on FTD
D. GRE tunnel on ASA

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/216276-configure-route-based-site-to-site-vpn-t.html#anc6

QUESTION 14
Which feature of GETVPN is a limitation of DMVPN and FlexVPN?

A. sequence numbers that enable scalable replay checking
B. enabled use of ESP or AH
C. design for use over public or private WAN
D. no requirement for an overlay routing protocol

Correct Answer: D
Section:

QUESTION 15
Refer to the exhibit.

```
ip access-list extended CCNP
 permit 192.168.0.10
 permit 192.168.0.11

webvpn gateway SSL_Gateway
 ip address 172.16.0.25 port 443
 ssl trustpoint AnyConnect_Cert
 inservice

webvpn context SSL_Context
 gateway SSL_Gateway

 ssl authenticate verify all
 inservice

 policy group SSL_Policy
   functions svc-enabled
   svc address-pool "ACPool" netmask 255.255.255.0
   svc dns-server primary 192.168.0.100
   svc default-domain cisco.com
 default-group-policy SSL_Policy
```

Cisco AnyConnect must be set up on a router to allow users to access internal servers 192.168.0.10 and 192.168.0.11. All other traffic should go out of the client's local NIC. Which command accomplishes this configuration?

A. svc split include 192.168.0.0 255.255.255.0
B. svc split exclude 192.168.0.0 255.255.255.0
C. svc split include acl CCNP
D. svc split exclude acl CCNP

Correct Answer: C
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533-AnyConnect-Configure-Basic-SSLVPN-for-I.html

QUESTION 16
An engineer is configuring clientless SSL VPN. The finance department has a database server that only they should access, but the sales department can currently access it. The finance and the sales departments are configured as separate group-policies. What must be added to the configuration to make sure the users in the sales department cannot access the finance department server?

A. tunnel group lock
B. smart tunnel
C. port forwarding
D. webtype ACL

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-generalcli/acl-webtype.pdf

QUESTION 17
An engineer has integrated a new DMVPN to link remote offices across the internet using Cisco IOS routers. When connecting to remote sites, pings and voice data appear to flow properly, and all tunnel stats show that they are up.
However, when trying to connect to a remote server using RDP, the connection fails. Which action resolves this issue?

A. Adjust the MTU size within the routers.
B. Add RDP port to the extended ACL.
C. Replace certificate on the RDP server.
D. Change DMVPN timeout values.

Correct Answer: A
Section:

QUESTION 18
Where must an engineer configure a preshared key for a site-to-site VPN tunnel configured on a Cisco ASA?

A. isakmp policy
B. group policy
C. crypto map
D. tunnel group

Correct Answer: D
Section:

QUESTION 19
A network engineer has been tasked with configuring SSL VPN to provide remote users with access to the corporate network. Traffic destined to the enterprise IP range should go through the tunnel, and all other traffic should go directly to the Internet. Which feature should be configured to achieve this?

A. U-turning
B. hairpinning
C. split-tunnel
D. dual-homing

Correct Answer: C
Section:

QUESTION 20
A network engineer must design a remote access solution to allow contractors to access internal servers. These contractors do not have permissions to install applications on their computers. Which VPN solution should be used in this design?

A. IKEv2 AnyConnect
B. Clientless
C. Port forwarding
D. SSL AnyConnect

Correct Answer: B
Section:

QUESTION 21
Refer to the exhibit.

```
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 Cisc012345678 internal
group-policy Cisc012345678 attributes
 dns-server value 192.168.1.3
 vpn-tunnel-protocol ssl-client
 address-pools value vpn_pool
```

Which type of Cisco VPN is shown for group Cisc012345678?

A. Cisco AnyConnect Client VPN
B. DMVPN
C. Clientless SSLVPN
D. GETVPN

Correct Answer: A
Section:

QUESTION 22
Which command shows the smart default configuration for an IPsec profile?

A. show run all crypto ipsec profile

B. ipsec profile does not have any smart default configuration
C. show smart-defaults ipsec profile
D. show crypto ipsec profile default

Correct Answer: D
Section:
Explanation:
The following table lists the commands that are enabled with the IKEv2 Smart Defaults feature, alongwith the default values....Device# show crypto ipsec profile defaultIPSEC profile defaultSecurity association lifetime: 4608000 kilobytes/3600 secondsResponder-Only (Y/N): NPFS (Y/N): NTransform sets={default: { esp-aes esp-sha-hmac },}https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-3s/sec-flex-vpn-xe-3s-book/sec-cfg-ikev2-flex.htm

QUESTION 23
Refer to the exhibit.

Hub

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 2

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

crypto ipsec profile CCNP
 set transform-set TS

crypto isakmp key cisco address 0.0.0.0

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
 no ip split-horizon
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile CCNP

interface GigabitEthernet1
 ip address 172.16.18.1 255.255.255.0
```

Spoke

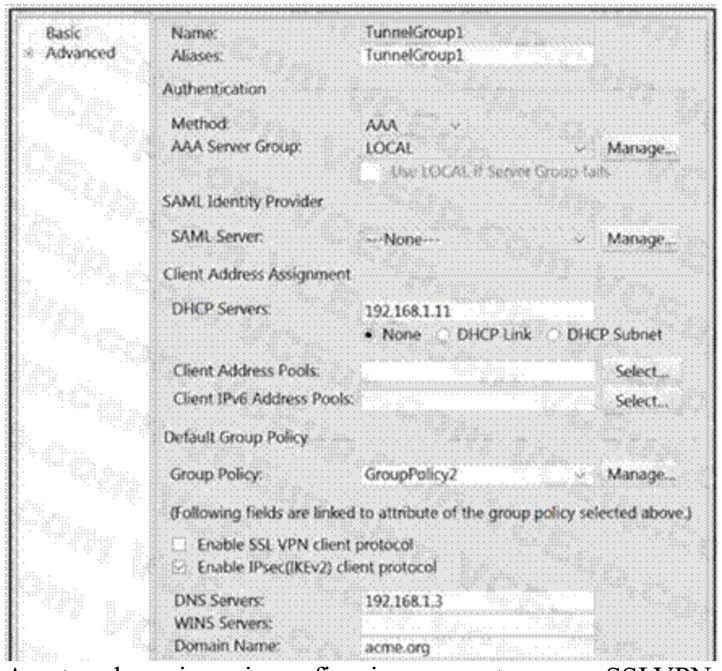
```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 2

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

crypto ipsec profile CCNP
 set transform-set TS

crypto isakmp key cisco address 172.16.18.1

interface Tunnel1
 ip address 10.0.0.2 255.255.255.0
 ip nhrp authentication cisco
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1 nbma 172.16.18.1 multicast
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile CCNP

interface GigabitEthernet1
 ip address 172.16.18.2 255.255.255.0
```

The DMVPN spoke is not establishing a session with the hub. Which two actions resolve this issue? (Choose two.)

A. Change the spoke nhs to 172.16.18.1 and the nbma to 10.0.0.1.
B. Change the transform set to mode tunnel.
C. Change the ISAKMP policy authentication on the spoke to pre-shared.
D. Change the ISAKMP key address on the spoke to 0.0.0.0.
E. Change the nhrp authentication key on the spoke to cisco123.

Correct Answer: C, E
Section:

QUESTION 24
Refer to the exhibit.



A network engineer is configuring a remote access SSLVPN and is unable to complete the connection using local credentials. What must be done to remediate this problem?

A. Enable the client protocol in the Cisco AnyConnect profile.
B. Configure a AAA server group to authenticate the client.
C. Change the authentication method to local.
D. Configure the group policy to force local authentication.

Correct Answer: A
Section:

QUESTION 25
Which two NHRP functions are specific to DMVPN Phase 3 implementation? (Choose two.)

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

Correct Answer: B, C
Section:
Explanation:
NHRP redirect is a function that allows the hub to inform the source spoke of a better path to reach thedestination spoke, by sending an NHRP redirect message containing the IP address of the destinationspoke.This triggers the source spoke to send an NHRP resolution request to the destination spoke, inorder to establish a direct spoke-to-spoke tunnel1.NHRP resolution reply is a function that allows the destination spoke to respond to the NHRP resolutionrequest from the source spoke, by sending an NHRP resolution reply containing its own IP address andthe IP address of the source spoke.This confirms the establishment of the direct spoke-to-spoke tunnel,and also allows the destination spoke to create a reciprocal tunnel to the source spoke2.These two functions are specific to DMVPN Phase 3, because they enable spoke-to-

spokecommunication without requiring a dynamic routing protocol or going through the hub.In DMVPN Phase1 and Phase 2, NHRP registration request, registration reply, and resolution request are also used, butthey have different purposes and effects3.

QUESTION 26
A network engineer must implement an SSLVPN Cisco AnyConnect solution that supports 500 concurrent users, ensures all traffic from the client passes through the ASA, and allows users to access all devices on the inside interface subnet
(192.168.0.0/24). Assuming all other configuration is set up appropriately, which configuration implements this solution?

A.
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

B.
```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.3.254 mask 255.255.252.0
```

C.
```
access-list ACSplit standard permit 192.168.0.0 255.255.255.0

group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value ACSplit
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```

D.
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  split-tunnel-policy tunnelall
  address-pools value ACPool

ip local pool ACPool 10.0.0.1-10.0.0.254 mask 255.255.255.0
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: A
Section:
Explanation:
ensures all traffic from the client passes through the ASA' that is one of the requirements. Meaning alltraffic should pass through the tunnel, I know they mention 192.168.0.0 network but that is just toconfuse

QUESTION 27
Which two features are valid backup options for an IOS FlexVPN client? (Choose two.)

A. HSRP stateless failover
B. DNS-based hub resolution
C. reactivate primary peer
D. tunnel pivot
E. need distractor

Correct Answer: B, C
Section:

QUESTION 28
Refer to the exhibit.

```
tunnel-group client general-attributes
address-pool MYPOOL
authentication-server-group RADIUS
tunnel-group client ipsec-attributes
pre-shared-key test123
```

Which type of VPN is used?

A. GETVPN
B. clientless SSL VPN
C. Cisco Easy VPN
D. Cisco AnyConnect SSL VPN

Correct Answer: C
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/vpn-easyvpn.html

QUESTION 29
An engineer would like Cisco AnyConnect users to be able to reach servers within the 10.10.0.0/16 subnet while all other traffic is sent out to the Internet. Which IPsec configuration accomplishes this task?

A.
```
crypto ikev2 authorization policy Local_Authz_01
 route set local ipv4 10.10.0.0 0.0.255.255
```

B.
```
crypto ikev2 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

C.
```
crypto ikev1 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

D.
```
crypto ikev2 authorization policy Local_Authz_01
 route set remote ipv4 10.10.0.0 0.0.255.255
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: B
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-3s/sec-flex-vpn-xe-3s-book/sec-cfg-flex-serv.htm

QUESTION 30
Refer to the exhibit.

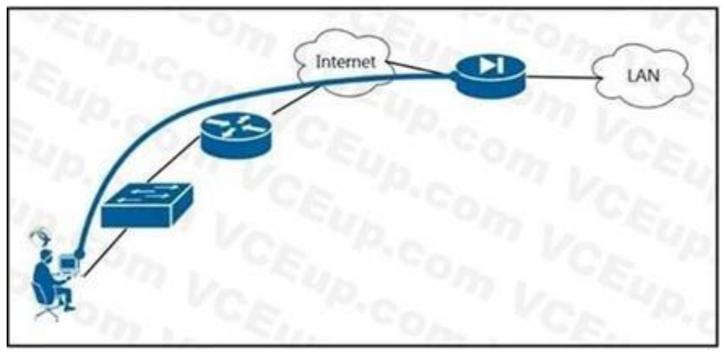
```
interface Tunnel0
ip address 192.168.1.1 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp map multicast dynamic
ip nhrp network-id 1
no ip split-horizon eigrp 90
ip next-hop-self eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco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

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

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

Correct Answer: A
Section:

QUESTION 31
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>
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: D
Section:

QUESTION 32
Refer to the exhibit.

```
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
```

Which two conclusions should be drawn from the DMVPN phase 2 configuration? (Choose two.)

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.

Correct Answer: C, E
Section:

QUESTION 33
Refer to the exhibit.

```
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
```

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

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.

Correct Answer: C
Section:

QUESTION 34
Refer to the exhibit.

```
*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
```

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?

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.

Correct Answer: C
Section:
Explanation:
DMVPN stands for Dynamic Multipoint VPN, which is a technology that allows routers to dynamicallyform VPN tunnels with each other without requiring a pre-configured static crypto map. DMVPN usesMultipoint GRE (mGRE) interfaces and Next Hop Resolution Protocol (NHRP) to establish directconnections between routers. DMVPN has three phases of operation, each with different features andbenefits.DMVPN Phase 1 is the basic configuration, where all spokes are configured with a single mGRE interfacethat points to the hub as the NHRP server. The spokes can only communicate with the hub, not witheach other. All traffic must go through the hub, which creates a bottleneck and increases latency.DMVPN Phase 2 improves on Phase 1 by allowing spoke-to-spoke communication without going throughthe hub. This is achieved by using NHRP to dynamically resolve the IP address of the destination spokeand create a direct GRE tunnel between the spokes. However, this still requires the use of a dynamicrouting protocol to advertise routes between the spokes, which adds overhead and complexity.DMVPN Phase 3 further enhances Phase 2 by enabling spoke-to-spoke communication without requiringa dynamic routing protocol. This is done by using NHRP shortcut switching and NHRP redirect messages.When a spoke wants to send traffic to another spoke, it sends an NHRP resolution request to the hub,which responds with an NHRP redirect message containing the IP address of the destination spoke. The source spoke then creates a direct GRE tunnel with the destination spoke and switches the traffic to thenew tunnel. The hub also sends an NHRP resolution reply to the destination spoke, informing it of thesource spoke's IP address. The destination spoke then creates a direct GRE tunnel with the source spokeand switches the traffic to the new tunnel. This way, the spokes can communicate directly without usinga dynamic routing protocol or going through the hub

QUESTION 35
Refer to the exhibit.

```
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 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?

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.

Correct Answer: B
Section:

QUESTION 36
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

Correct Answer: B, E
Section:

QUESTION 37
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

Correct Answer: C
Section:

QUESTION 38
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.

Correct Answer: B, D
Section:

QUESTION 39
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

Correct Answer: C
Section:

QUESTION 40
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

Correct Answer: B, C
Section:

QUESTION 41
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 AS

A. What is a potential solution for this issue while still allowing it to be a clientless VPN setup?
B. Set up a smart tunnel with the IP address of the web server.
C. Set up a NAT rule that translates the ASA public address to the web server private address on port 80.
D. Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.
E. Set up a WebACL to permit the IP address of the web server.

Correct Answer: B
Section:

QUESTION 42
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

Correct Answer: B, E
Section:
Explanation:
The auto-signon command is a single sign-on method for users of clientless SSL VPN sessions. It passesthe login credentials (username and password) to internal servers for authentication using NTLMauthentication, basic authentication, or both. Multiple auto-signon commands can be entered and areprocessed according to the input order (early commands take precedence)
https://www.cisco.com/c/en/us/td/docs/security/asa/asa916/configuration/vpn/asa-916-vpn-config/webvpn-configure-policy-groups.html#ID-2439-00001438

QUESTION 43
Refer to the exhibit.

```
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
```

Which type of VPN implementation is displayed?

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

Correct Answer: C
Section:

QUESTION 44
A network engineer is setting up a clientless SSLVPN on a Cisco AS

A. Remote users must be able to access an internal webserver via the URL example.com. Which two steps accomplish this task? (Choose two.)
B. Configure a bookmark for the webserver.
C. Configure routing so that the user's computer can reach the webserver.
D. Configure a DNS server that can resolve the webserver URL.
E. Configure a browser plugin on the Cisco ASA.
F. Configure routing so that the Cisco ASA can reach the webserver.

Correct Answer: A, C
Section:

QUESTION 45
A network engineer has set up a FlexVPN server to terminate multiple FlexVPN clients. The VPN tunnels are established without issue. However, when a Change of Authorization is issued by the RADIUS server, the FlexVPN server does not update the authorization of connected FlexVPN clients.
Which action resolves this issue?

A. Add the aaa server radius dynamic-author command on the FlexVPN clients.
B. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN server.
C. Add the aaa server radius dynamic-author command on the FlexVPN server.
D. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN clients.

Correct Answer: C
Section:

QUESTION 46
A company needs to ensure only corporate issued laptops and devices are allowed to connect with the Cisco AnyConnect client. The solution should be applicable to multiple operating systems, including Windows, MacOS, and Linux, and should allow for remote remediation if a corporate issued device is stolen. Which solution should be used to accomplish these goals?

A. Use a DAP registry check on the system to determine the relationship with the corporate domain.
B. Use a DAP file check on the system to determine the relationship with the corporate domain.
C. Install and authenticate user certificates on the corporate devices.
D. Install and authenticate machine certificates on the corporate devices

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/vpn/asdm-78-vpn-config/vpnasdm-dap.html#ID-2184-00000017

QUESTION 47
When a FlexVPN is configured, which two components must be configured for IKEv2? (Choose two.)

A. method
B. profile
C. proposal
D. preference
E. persistence

Correct Answer: B, C
Section:

QUESTION 48
A DMVPN spoke router tunnel is up and passing traffic, but it cannot establish an EIGRP neighbor relationship with the hub router. Which solution resolves this issue?

A. Enable EIGRP Split Horizon on the hub tunnel interface.
B. Remove the EIGRP stub configuration on the spoke tunnel interface.
C. Enable the EIGRP next hop self feature on the hub tunnel interface.
D. Configure the dynamic NHRP multicast map on the hub tunnel interface.

Correct Answer: D
Section:

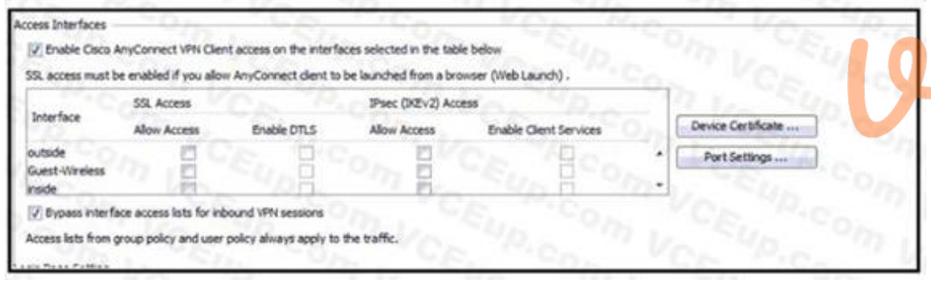
QUESTION 49
Refer to the exhibit.

An IPsec Cisco AnyConnect client is failing to connect and generates these debugs every time a connection to an IOS headend is attempted. Which action resolves this issue?

A. Correct the DH group setting.
B. Correct the PFS setting.
C. Correct the integrity setting.
D. Correct the encryption setting.

Correct Answer: A
Section:

QUESTION 50
Refer to the exhibit.

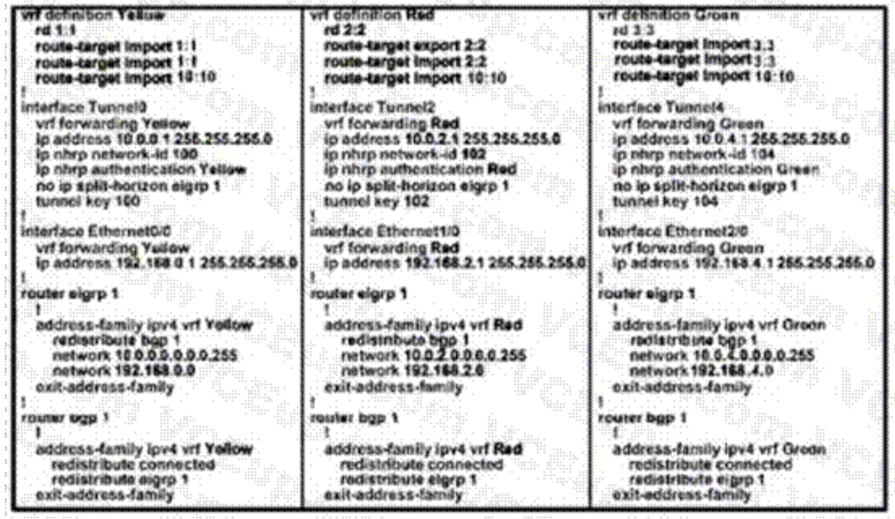


An engineer must allow Cisco AnyConnect users to access the outside interface using protocol UDP 500/4500. In addition, these clients must be able to establish an SSL connection to update Cisco AnyConnect software over the same connection. Which two actions must be taken to achieve this goal? (Choose two.)

A. IPsec (IKEv2) Allow Access must be checked on the outside interface.
B. SSL Enable DTLS must be checked on the outside interface.
C. Bypass interface access lists for inbound VPN sessions must be unchecked.
D. IPsec (IKEv2) Enable Client Services must be checked on the outside interface.
E. SSL Allow Access must be checked on the outside interface.

Correct Answer: A, D
Section:

QUESTION 51
Refer to the exhibit.



Based on the configuration output, what is the VPN technology?

A. site-to-site
B. DMVPN
C. L2VPN
D. multicast VPN

Correct Answer: B
Section:
Explanation:

QUESTION 52
A user at a company HQ is having trouble accessing a network share at a branch site that is connected with a L2L IPsec VPN. While troubleshooting, a network security engineer runs a packet tracer on the Cisco ASA to simulate the user traffic and discovers that the encryption counter is increasing but the decryption counter is not. What must be configured to correct this issue?

A. Adjust the routing on the remote peer device to direct traffic back over the tunnel.
B. Adjust the preshared key on the remote peer to allow traffic to flow over the tunnel.
C. Adjust the transform set to allow bidirectional traffic.
D. Adjust the peer IP address on the remote peer to direct traffic back to the ASA.

Correct Answer: A
Section:

QUESTION 53
A user is experiencing delays on audio calls over a Cisco AnyConnect VPN. Which implementation step resolves this issue?

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.

Correct Answer: D
Section:

QUESTION 54
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?

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.

Correct Answer: D
Section:

QUESTION 55
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?

A. clientless proxy
B. smart tunneling
C. clientless plug-in
D. clientless rewriter

Correct Answer: C
Section:

QUESTION 56
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?

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

Correct Answer: C
Section:
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 sourceand 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 57
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?

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.

Correct Answer: A
Section:

QUESTION 58
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.)

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.

Correct Answer: D, E
Section:
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 59
What is a characteristic of GETVPN?

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.

Correct Answer: D
Section:
Explanation:

QUESTION 60
Refer to the exhibit.

```
group-policy My_GroupPolicy internal
group-policy My_GroupPolicy attributes
 vpn-tunnel-protocol l2tp-ipsec
!
 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
http server enable 8080
!
tunnel-group My_WebVPN general-attributes
 address-pool My_Pool
 default-group-policy My_GroupPolicy
```

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

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.

Correct Answer: D
Section:

QUESTION 61
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?

A. include specified
B. exclude specified
C. tunnel specified
D. dynamic exclude

Correct Answer: B
Section:
Explanation:
You could in theory 'tunnel specified' and list every subnet aside from the local one in the split tunnellist, 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.

QUESTION 62
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?

A. Reverse Route Injection
B. FlexVPN

C. Dynamic Crypto Map
D. DMVPN

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

QUESTION 63
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.)

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.

Correct Answer: B, E
Section:
Explanation:
B) In the CiscoAnyConnect XML profile, adding the hostname and host address to the server list ensures that theAnyConnect client knows the address of the VPN concentrator (router) to connect to.
E. In the CiscoAnyConnect Local Policy, adding the router IP address to the Update Policy allows the client to connectto the router for updates and configuration.

QUESTION 64
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.)

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.

Correct Answer: B, C
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/215442-configure-anyconnect-management-vpn-tunn.html

QUESTION 65
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?

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.

Correct Answer: B
Section:

QUESTION 66
What must be configured in a FlexVPN deployment to allow for direct communication between spokes connected to different hubs?

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.

Correct Answer: D
Section:

QUESTION 67
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: 341BE984EC151E8D       Remote spi: 924798D873F59132
      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?

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.

Correct Answer: D
Section:

QUESTION 68
Over which two transport mediums is FlexVPN deployed? (Choose two.)

A. 5G
B. VPLS
C. internet
D. MPLS
E. DWDM

Correct Answer: C, D
Section:
Explanation:
Transport network: FlexVPN can be deployed either over a public internet or a private Multiprotocol Label Switching (MPLS) VPN network. https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

QUESTION 69
A network administrator is troubleshooting a FlexVPN tunnel. The hub router is unable to ping the spoke router's tunnel interface IP address of 192.168.1.2, even though the tunnel is showing up. The output of the debug ip packet CLI command on the hub router shows the following entry.
IP: tableid=0123456789 s=192.168.1.1 (local), d=192.168.1.2 (loopback2), routed via FIB.
What must be configured to fix this issue?

A. A matching IKEv2 pre-shared key on the hub and spoke routers in the crypto keyring configuration.
B. An outbound ACL on the dynamic VTI of the hub router that allows ICMP traffic to 192.168.1.2.
C. An IKEv2 authorization policy must be configured on the spoke router to advertise the interface route.
D. A route map must be configured on hub router to set the next hop for 192.168.1.2 to the dynamic VTI.

Correct Answer: C
Section:

QUESTION 70
A network engineer must configure the Cisco ASA so that Cisco AnyConnect clients establishing an SSL VPN connection create an additional tunnel for real-time traffic that is sensitive to packet delays. If this additional tunnel experiences any issues, it must fall back to a TLS connection. Which two Cisco AnyConnect features must be configured to accomplish this task? (Choose two.)

A. DTLS

B. DSCP Preservation
C. DPD
D. SSL Rekey
E. OMTU

Correct Answer: A, C
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpn-anyconnect.html
Configure Dead Peer Detection Dead Peer Detection (DPD) ensures that the ASA (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed. To enable dead peer detection (DPD) and set the frequency with which either the AnyConnect client or the ASA gateway performs DPD, do the following: Before you begin This feature applies to connectivity between the ASA gateway and the AnyConnect SSL VPN Client only. It does not work with IPsec since DPD is based on the standards implementation that does not allow padding, and CLientless SSL VPN is not supported. If you enable DTLS, enable Dead Peer Detection (DPD) also. DPD enables a failed DTLS connection to fallback to TLS. Otherwise, the connection terminates.

QUESTION 71
Refer to the exhibit.

```
<snip>
Tunnel Group: VPNPhone, Client Cert Auth Success.
WebVPN: CSD data not sent from client
http_remove_auth_handle(): handle 24 not found!
<snip>
```

A network administrator is setting up a phone VPN on a Cisco AS

A. The phone cannot connect and the error is presented in a debug on the Cisco ASA. Which action fixes this issue?
B. Enable web-deploy of the posture module so that the module can be downloaded from the Cisco ASA to an IP phone.
C. Configure the Cisco ASA to present an RSA certificate to the phone for authentication.
D. Disable Cisco Secure Desktop under the connection profile VPNPhone.
E. Install the posture module on the Cisco ASA.

Correct Answer: C
Section:
Explanation:
CSD and IP phones: Currently, IP phones do not support Cisco Secure Desktop (CSD) and do not connect when CSD is enabled for the tunnel group or globally in the ASA.

QUESTION 72
Which two protocols does DMVPN leverage to build dynamic VPNs to multiple destinations? (Choose two.)

A. IKEv2
B. NHRP
C. mGRE
D. mBGP
E. GDOI

Correct Answer: B, C
Section:

QUESTION 73
DRAG DROP
Drag and drop the GET VPN components from the left onto the correct descriptions on the right.

Select and Place:

Answer Area

KEK	gets the IPsec SA to encrypt data traffic within the group
TEK	provides group key and group SA management
GDOI protocol	maintains security policies and provides the session key for encrypting traffic
KS	encrypts the rekey message
GM	used by all the group members to communicate securely among each other

Correct Answer:

Answer Area

	GM
	GDOI protocol
	KS
	KEK
	TEK

Section:
Explanation:

QUESTION 74
A network administrator wants the Cisco ASA to automatically start downloading the Cisco AnyConnect client without prompting the user to select between WebVPN or AnyConnect. Which command accomplishes this task?

A. anyconnect ssl df-bit-ignore enable

B. anyconnect ask none default anyconnect
C. anyconnect ask enable default anyconnect
D. anyconnect modules value default

Correct Answer: B
Section:
Explanation:
https://networklessons.com/cisco/asa-firewall/cisco-asa-anyconnect-remote-access-vpn#:~:text=The%20anyconnect%20ask%20command%20specifies,of%20the%20anyconnect%20client%20automatically.

QUESTION 75
An administrator is deciding which authentication protocol should be implemented for their upcoming Cisco AnyConnect deployment. A list of the security requirements from upper management are: the ability to force AnyConnect users to use complex passwords such as C1$c0451035084!, warn users a few days before their password expires, and allow users to change their password during a remote access session. Which authentication protocol must be used to meet these requirements?

A. LDAPS
B. RADIUS
C. Kerberos
D. TACACS+

Correct Answer: A
Section:
Explanation:
To enforce complex passwords---for example, to require that a password contain upper- and lowercase letters, numbers, and special characters---enter the password-management command in tunnel-group general-attributes configuration mode on the ASA and perform the following steps under Active Directory. https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/vpn-groups.html

QUESTION 76
Which clientless SSLVPN supported feature works when the http-only-cookie command is enabled?

A. Citrix load balancer
B. port reflector
C. Java rewriter -
D. Java plug-ins
E. script browser

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/asdm74/vpn/asdm-74-vpn-config/webvpn-troubleshooting.html
The following Clientless SSL VPN features will not work when the http-only-cookie command is
enabled:
* Java plug-ins
* Java rewriter
* Port forwarding
* File browser
* Sharepoint features that require desktop applications (for example, MS Office applications)
* AnyConnect Web launch

* Citrix Receiver, XenDesktop, and Xenon
* Other non-browser-based and browser plugin-based applications

QUESTION 77
A network engineer must expand a company's Cisco AnyConnect solution. Currently, a Cisco ASA is set up in North America and another will be installed in Europe with a different IP address. Users should connect to the ASA that has the lowest Round Trip Time from their network location as measured by the AnyConnect client. Which solution must be implemented to meet this requirement?

A. VPN Load Balancing
B. IP SLA
C. DNS Load Balancing
D. Optimal Gateway Selection

Correct Answer: D
Section:
Explanation:
Optimal Gateway Selection (OGS). OGS is a feature that can be used in order to determine which gateway has the lowest Round Trip Time (RTT) and connect to that gateway. One can use the OGS feature in order to minimize latency for Internet traffic without user intervention. With OGS, Cisco AnyConnect Secure Mobility Client (AnyConnect) identifies and selects which secure gateway is best for connection or reconnection. OGS begins upon first connection or upon a reconnection at least four hours after the previous disconnection.

QUESTION 78
An engineer is creating an URL object on Cisco FMC. How must it be configured so that the object will match for HTTPS traffic in an access control policy?

A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website.
C. Use the subject common name from the website certificate.
D. Define the path to the individual webpage that uses HTTPS.

Correct Answer: B
Section:
Explanation:
Use the FQDN including the subdomain for the website.According to the Firepower Management Center Configuration Guide, Version 6.61, when you create a URL object, you must use the fully qualified domain name (FQDN) of the website, including any subdomains, and omit the protocol prefix (HTTP or HTTPS). For example, to match www.example.com, you must enter www.example.com as the URL object value, not http://www.example.com or https://www.example.com. The system automatically matches both HTTP and HTTPS traffic for the same FQDN. Specifying the protocol to match (HTTP or HTTPS) is not required and will result in an invalid URL object. Using the subject common name from the website certificate or defining the path to the individual webpage that uses HTTPS are not supported options for URL objects.