Number: 300-730
Passing Score: 800
Time Limit: 120
File Version: 13.0

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

Exam A

QUESTION 1
Refer to the exhibit.

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.0.1

   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 192.168.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.0.1, remote crypto endpt.: 192.168.0.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0x3D05D003(1023791107)
     PFS (Y/N): N, DH group: none
```

Which two tunnel types produce the show crypto ipsec sa output seen in the exhibit? (Choose two.)

A. crypto map
B. DMVPN
C. GRE
D. FlexVPN
E. VTI

Correct Answer: B, E
Section:

QUESTION 2
Which two changes must be made in order to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two.)

A. Add NHRP shortcuts on the hub.
B. Add NHRP redirects on the spoke.
C. Disable EIGRP next-hop-self on the hub.
D. Enable EIGRP next-hop-self on the hub.
E. Add NHRP redirects on the hub.

Correct Answer: D, E
Section:
Explanation:
DMVPN disables the EIRGP next-hop-self with "no ip next-hop-self eigrp xxx" in DMVPN phase 2, and to go from Phase 2 to 3 you need use the NHRP protocol, and again enable EIRGP next-hop-self with "ip next-hop-self eigrp 134" under the tunnel interface https://www.cisco.com/c/en/us/td/docs/iosxml/ ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpndmvpn. html#GUID-BF561439-BCC0-4AAF-80D9-1F7876CB7B81

QUESTION 3
Refer to the exhibit.

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

A customer cannot establish an IKEv2 site-to-site VPN tunnel between two Cisco ASA devices. Based on the syslog message, which action brings up the VPN tunnel?

A. Reduce the maximum SA limit on the local Cisco ASA.
B. Increase the maximum in-negotiation SA limit on the local Cisco ASA.
C. Remove the maximum SA limit on the remote Cisco ASA.
D. Correct the crypto access list on both Cisco ASA devices.

Correct Answer: B
Section:

QUESTION 4
Which two parameters help to map a VPN session to a tunnel group without using the tunnel-group list? (Choose two.)

A. group-alias
B. certificate map
C. optimal gateway selection
D. group-url
E. AnyConnect client version

Correct Answer: A, D
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generationfirewalls/98580-enable-group-dropdown.html

QUESTION 5
Which method dynamically installs the network routes for remote tunnel endpoints?

A. policy-based routing
B. CEF
C. reverse route injection
D. route filtering

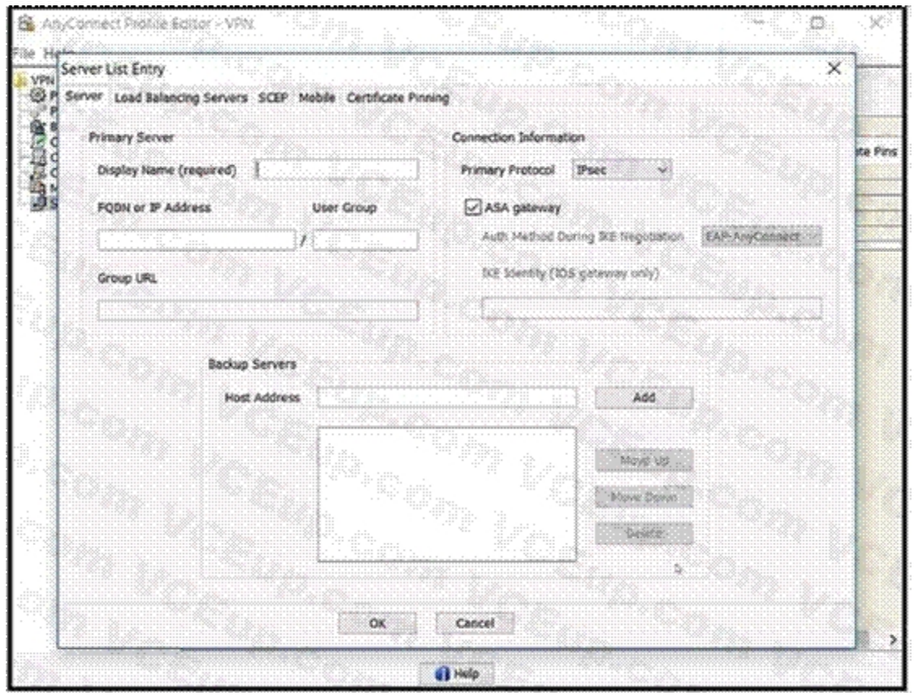
Correct Answer: C
Section:
Explanation:
Reverse route injection (RRI) is a method that dynamically installs the network routes for remote tunnel endpoints. The RRI feature allows the router to automatically learn the routes for the remote networks and automatically install these routes into the routing table. This eliminates the need for the administrator to manually configure and maintain the routes for the remote networks. This feature is commonly used in VPN environments, where the router at the VPN endpoint needs to learn the routes for the remote networks behind the other VPN endpoint. The other options such as policy-based routing, CEF, and route filtering are not used to dynamically install the network routes for remote tunnel endpoints
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-4t/sec-vpn- availability-12-4t-book/sec-rev-rte-inject.html
Topic 2, Remote access VPNs

QUESTION 6
Which command identifies a Cisco AnyConnect profile that was uploaded to the flash of an IOS router?

A. svc import profile SSL_profile flash:simos-profile.xml
B. anyconnect profile SSL_profile flash:simos-profile.xml
C. crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml
D. webvpn import profile SSL_profile flash:simos-profile.xml

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

QUESTION 7
Refer to the exhibit.



Which value must be configured in the User Group field when the Cisco AnyConnect Profile is created to connect to an ASA headend with IPsec as the primary protocol?

A. address-pool
B. group-alias
C. group-policy
D. tunnel-group

Correct Answer: D
Section:
Explanation:
The user group is used in conjunction with Host Address to form a group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url of the connection profile.
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/anyconnect-profile-editor.html#ID-1430-0000026c
Reference: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect41/administration/guide/b_AnyConnect_Administrator_Guide_4-1/configure-vpn.html

QUESTION 8
Refer to the exhibit.

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list
author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
```

What is configured as a result of this command set?

A. FlexVPN client profile for IPv6
B. FlexVPN server to authorize groups by using an IPv6 external AAA
C. FlexVPN server for an IPv6 dVTI session
D. FlexVPN server to authenticate IPv6 peers by using EAP

Correct Answer: C
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116528-config-flexvpn-00.html

QUESTION 9

Which two types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose two.)

A. HTTP
B. ICA (Citrix)
C. VNC
D. RDP
E. CIFS

Correct Answer: A, E
Section:
Explanation:
HTTP (Hypertext Transfer Protocol) is used for transferring web resources, such as web pages andHTML documents, across the internet. CIFS (Common Internet File System) is used for sharing filesand printers between computers on a network. ICA (Citrix), VNC (Virtual Network Computing), andRDP (Remote Desktop Protocol) are not enabled by default on the Cisco ASA Clientless SSL VPNportal.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpnconfig/webvpn-configure-gateway.html

QUESTION 10
Which configuration construct must be used in a FlexVPN tunnel?

A. EAP configuration
B. multipoint GRE tunnel interface
C. IKEv1 policy
D. IKEv2 profile

Correct Answer: D
Section:
Explanation:
The correct answer is D. IKEv2 profile. A FlexVPN tunnel requires an IKEv2 profile to define theparameters for the IKEv2 negotiation and the IPsec security association. The IKEv2 profile references theIKEv2 keyring, the authentication method, the identity of the peers, and other options. The IKEv2 profileis then applied to a virtual tunnel interface (VTI) or a dynamic virtual tunnel interface (DVTI) to protectthe tunnel with IPsec12. An EAP configuration is used for authentication with Extensible AuthenticationProtocol (EAP), which is optional for FlexVPN3. A multipoint GRE tunnel interface is used for DMVPN,not FlexVPN. An IKEv1 policy is used for IKEv1, not IKEv2, which is the protocol for FlexVPN.

QUESTION 11
A Cisco AnyConnect client establishes a SSL VPN connection with an ASA at the corporate office. An engineer must ensure that the client computer meets the enterprise security policy. Which feature can update the client to meet an enterprise security policy?

A. Endpoint Assessment
B. Cisco Secure Desktop
C. Basic Host Scan
D. Advanced Endpoint Assessment

Correct Answer: D
Section:

QUESTION 12
Which two features provide headend resiliency for Cisco AnyConnect clients? (Choose two.)

A. AnyConnect Auto Reconnect
B. AnyConnect Network Access Manager
C. AnyConnect Backup Servers

D. ASA failover
E. AnyConnect Always On

Correct Answer: C, D
Section:
Explanation:
According to the Implementing Secure Solutions with Virtual Private Networks (SVPN) documents andlearning resources available at cisco.com, the two features that provide headend resiliency for CiscoAnyConnect clients are:AnyConnect Backup Servers: This feature allows the AnyConnect client to automatically connect to abackup server in case the primary server is unreachable or fails. The backup server list is configured onthe ASA or IOS headend and pushed to the client during the VPN connection establishment. The clientcan also manually select a backup server from the list if needed.This feature enhances the availabilityand reliability of the VPN service for the clients12.ASA failover: This feature enables two identical ASAs to be paired together as an active/standby oractive/active pair. The ASAs synchronize their configuration and state information and monitor eachother's health. If the active ASA fails or becomes unreachable, the standby ASA takes over the traffic andVPN sessions without any disruption for the clients.This feature provides high availability andredundancy for the VPN headend34.1: AnyConnect Backup Servers2:Redundancy options for IOS Headend for AnyConnect Clients3: ASAFailover4:AnyConnect Implementation and Performance/Scaling Reference for COVID-19 Preparation

QUESTION 13
Cisco AnyConnect Secure Mobility Client has been configured to use IKEv2 for one group of users and SSL for another group. When the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect. What might be the problem?

A. The XML profile is not configured correctly for the affected users.
B. The new client image does not use the same major release as the current one.
C. Client services are not enabled.
D. Client software updates are not supported with IKEv2.

Correct Answer: C
Section:
Explanation:
https://community.cisco.com/t5/vpn/anyconnect-service-port-not-enabled/td-p/2968124

QUESTION 14
Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?

A. tunnel-group (general-attributes)
B. tunnel-group (webvpn-attributes)
C. webvpn (group-policy)
D. webvpn (global configuration)

Correct Answer: C
Section:

QUESTION 15
Refer to the exhibit.

Based on the exhibit, why are users unable to access CCNP Webserver bookmark?

A. The URL is being blocked by a WebACL.
B. The ASA cannot resolve the URL.
C. The bookmark has been disabled.
D. The user cannot access the URL.

Correct Answer: B
Section:
Explanation:
https://community.cisco.com/t5/network-security/missing-ssl-vpn-bookmarks/td-p/1597023

QUESTION 16
Which two statements about the Cisco ASA Clientless SSL VPN solution are true? (Choose two.)

A. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resourcesthrough the URL bar, the client uses the local DNS to perform FQDN resolution.
B. The rewriter enable command under the global webvpn configuration enables the rewriter functionality because that feature is disabled by default.
C. A Cisco ASA can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions.
D. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resourcesthrough the URL bar, the ASA uses its configured DNS servers to perform FQDN resolution.
E. Clientless SSLVPN provides Layer 3 connectivity into the secured network.

Correct Answer: C, D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/webvpn.html

QUESTION 17
Which feature allows the ASA to handle nonstandard applications and web resources so that they display correctly over a clientless SSL VPN connection?

A. single sign-on
B. Smart Tunnel
C. WebType ACL
D. plug-ins

Correct Answer: D
Section:
Explanation:

Plug-ins are extensions to the Clientless SSL VPN feature that enable the ASA to handle non-standardapplications and Web resources so that they display correctly over a Clientless SSL VPN connection.Plug-ins are software components that the ASA downloads to the remote user's browser. The plug-insprovide support for applications and protocols that are not natively supported by Clientless SSL VPN,such as Java, ActiveX, SSH, Telnet, and RDP. Plug-ins can also provide enhanced functionality andsecurity for Web applications, such as Outlook Web Access and Lotus iNotes.You can read more about plug-ins and how to configure them in the document [ASDM Book 3: Cisco ASASeries VPN ASDM Configuration Guide, 7.7]1

QUESTION 18
Which command automatically initiates a smart tunnel when a user logs in to the WebVPN portal page?

A. auto-upgrade
B. auto-connect
C. auto-start
D. auto-run

Correct Answer: C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/webvpn-configure-policy-group.html

QUESTION 19
Refer to the exhibit.

XML profile

```
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
```

The customer must launch Cisco AnyConnect in the RDP machine. Which IOS configuration accomplishes this task?

A.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
  svc platform win seq 1
  policy group PolicyGroup1
   functions svc-enabled
```

B.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
browser-attribute import flash:RDP.xml
```

C.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

D.
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc module RDP
```

A. Option A
B. Option B

C. Option C
D. Option D

Correct Answer: C
Section:
Explanation:
Reference: https://community.cisco.com/t5/vpn/starting-anyconnect-vpn-through-rdp-session-oncisco-891/td- p/2128284

QUESTION 20
Refer to the exhibit.

Which two commands under the tunnel-group webvpn-attributes result in a Cisco AnyConnect user receiving the AnyConnect prompt in the exhibit? (Choose two.)

A. group-url https://172.16.31.10/General enable
B. group-policy General internal
C. authentication aaa
D. authentication certificate
E. group-alias General enable

Correct Answer: C, E
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generationfirewalls/98580-enable-group-dropdown.html

QUESTION 21
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

Correct Answer: B
Section:

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

QUESTION 22
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. *$DfltlkeldentityS*

Correct Answer: B
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPNAnyConnect-IKEv2- Remote-Access.html

QUESTION 23
Refer to the exhibit.

```
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
```

Which VPN technology is allowed for users connecting to the Employee tunnel group?

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

Correct Answer: D
Section:
Explanation:
When you configure other group policies, any attribute that you do not explicitly specify takes its value from the default group policy. To view the default group policy.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/vpngrp.html

QUESTION 24
Refer to the exhibit.

```
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: 034B32CA36 (1261619766)
```

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?

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

Correct Answer: A
Section:

QUESTION 25
What uses an Elliptic Curve key exchange algorithm?

A. ECDSA
B. ECDHE
C. AES-GCM
D. SHA

Correct Answer: B
Section:
Explanation:
Reference: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curvecryptography/

QUESTION 26
Which two remote access VPN solutions support SSL? (Choose two.)

A. FlexVPN
B. clientless
C. EZVPN
D. L2TP

E. Cisco AnyConnect

Correct Answer: B, E
Section:

QUESTION 27
Which VPN solution uses TBAR?

A. GETVPN
B. VTI
C. DMVPN
D. Cisco AnyConnect

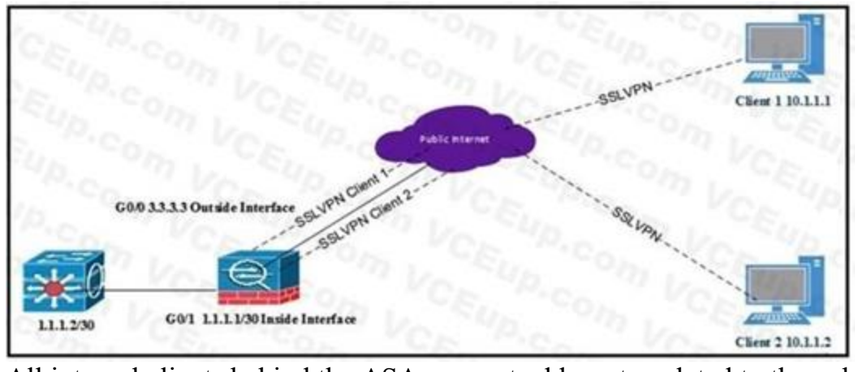
Correct Answer: A
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get- vpn-xe-3s-book/sec-get-vpn.html

QUESTION 28
Which two commands help determine why the NHRP registration process is not being completed even after the IPsec tunnel is up? (Choose two.)

A. show crypto isakmp sa
B. show ip traffic
C. show crypto ipsec sa
D. show ip nhrp traffic
E. show dmvpn detail

Correct Answer: A, D
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

QUESTION 29
Refer to the exhibit.



All internal clients behind the ASA are port address translated to the public outside interface that has an IP address of 3.3.3.3. Client 1 and client 2 have established successful SSL VPN connections to the ASA. What must be implemented so that "3.3.3.3" is returned from a browser search on the IP address?

A. Same-security-traffic permit inter-interface under Group Policy

B. Exclude Network List Below under Group Policy

C. Tunnel All Networks under Group Policy

D. Tunnel Network List Below under Group Policy

Correct Answer: C
Section:
Explanation:
The reason is that by default, the SSL VPN clients use split tunneling, which means they only send trafficdestined for the corporate network through the VPN tunnel, and use their local gateway for other traffic, such as browsing the internet. This means that when they search for their IP address on abrowser, they will see their local IP address, not the IP address of the ASA.To change this behavior, you need to configure the Group Policy on the ASA to tunnel all networks,which means that all traffic from the SSL VPN clients will go through the VPN tunnel, regardless of thedestination. This way, when they search for their IP address on a browser, they will see the IP address ofthe ASA, which is 3.3.3.3.To configure tunnel all networks under Group Policy, you can use either ASDM or CLI.For example, usingASDM, you can follow these steps1:Choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies.Select the group policy that you want to modify and click Edit.In the Edit Internal Group Policy window, choose Advanced > Split Tunneling.In the Policy drop-down list, choose Tunnel All Networks.Click OK and then Apply.Using CLI, you can enter these commands:ciscoasa(config)# group-policy <group_policy_name> attributes ciscoasa(config-group-policy)# split-tunnel-policy tunnelall

QUESTION 30
Cisco AnyConnect clients need to transfer large files over the VPN sessions. Which protocol provides the best throughput?

A. SSL/TLS
B. L2TP
C. DTLS
D. IPsec IKEv1

Correct Answer: C
Section:

QUESTION 31
Refer to the exhibit.

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14

crypto isakmp key cisco address 0.0.0.0

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

crypto ipsec profile CCNP
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 172.18.10.2
 tunnel protection ipsec profile CCNP
```

Which VPN technology is used in the exhibit?

A. DVTI
B. VTI
C. DMVPN
D. GRE

Correct Answer: B
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/zZArchive/IPsec_Virtual_Tunnel_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91

QUESTION 32
Which VPN does VPN load balancing on the ASA support?

A. VTI
B. IPsec site-to-site tunnels
C. L2TP over IPsec
D. Cisco AnyConnect

Correct Answer: D
Section:

QUESTION 33
Which parameter must match on all routers in a DMVPN Phase 3 cloud?

A. GRE tunnel key
B. NHRP network ID
C. tunnel VRF

D. EIGRP split-horizon setting

Correct Answer: A
Section:
Explanation:
NHRP network IDs are locally significant and can be different. It makes sense from a deployment andmaintenance perspective to use unique network ID numbers (using the ip nhrp network-id command)across all routers in a DMVPN network, but it is not necessary that they be the same.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-dmvpn.html

QUESTION 34
Which parameter is initially used to elect the primary key server from a group of key servers?

A. code version
B. highest IP address
C. highest-priority value
D. lowest IP address

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transportvpn/deployment_guide_c07_554713.html

QUESTION 35
A Cisco ASA is configured in active/standby mode. What is needed to ensure that Cisco AnyConnect users can connect after a failover event?

A. AnyConnect images must be uploaded to both failover ASA devices.
B. The vpnsession-db must be cleared manually.
C. Configure a backup server in the XML profile.
D. AnyConnect client must point to the standby IP address.

Correct Answer: A
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_active_standby.html

QUESTION 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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
```

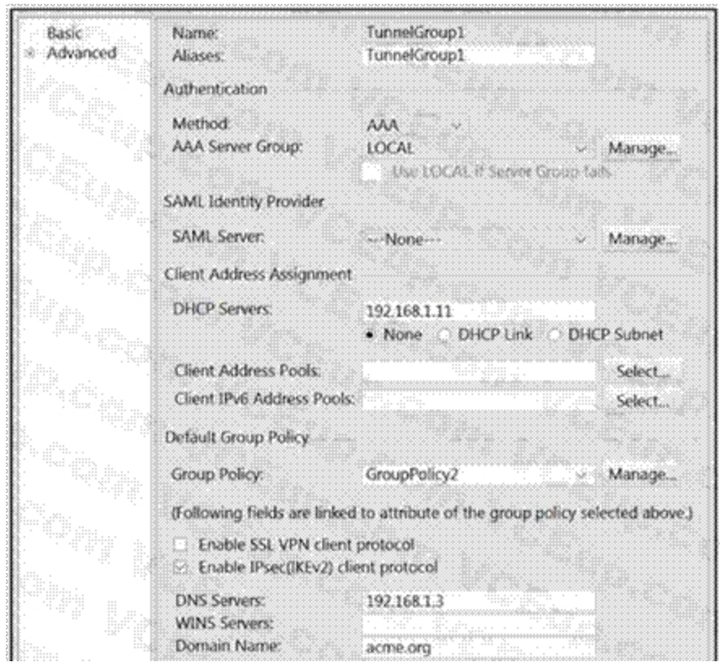
```
Spoke
crypto isakmp policy 10
 encr aes 256
 hash sha256
 group 2

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 50
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 51
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 52
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 53
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 54
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 55
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 56
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 57
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 58
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 59
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 60
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 61
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 62
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 63
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 64
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 65
Refer to the exhibit.

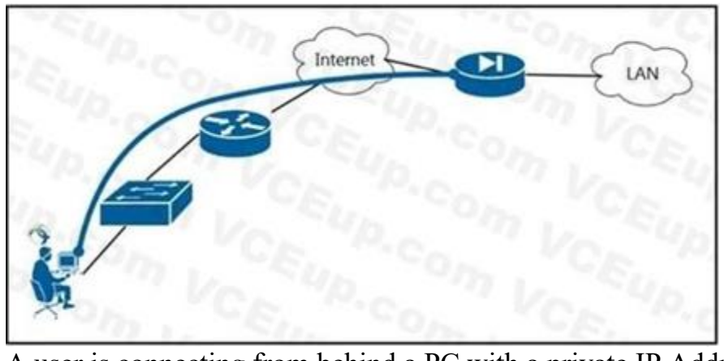
```
interface Tunnel0
ip address 192.168.1.1 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp map multicast dynamic
ip nhrp network-id 1
no ip split-horizon eigrp 90
ip next-hop-self eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco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

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 66
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 67
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 68
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 69

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 70
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 71
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 72
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 73
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 74
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 75
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 76
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 77
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 78
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 79

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 80
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 81
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 82
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 83
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.

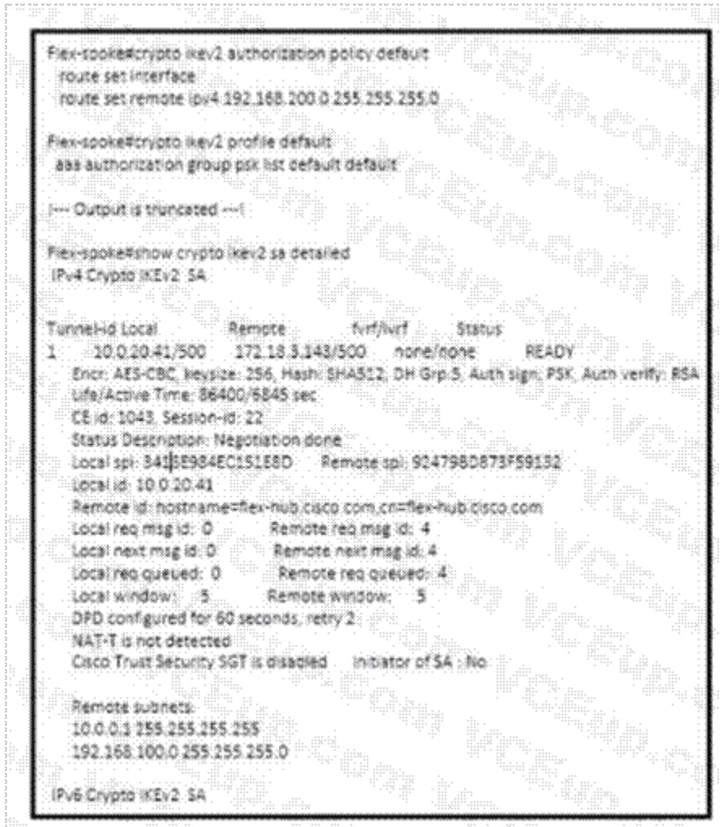
Correct Answer: B
Section:

QUESTION 84
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 85
Refer to the exhibit.



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 86

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

A. 2547oDMVPN
B. NHRP
C. OSPF
D. NAT Traversal

Correct Answer: B
Section:

QUESTION 87
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?

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.

Correct Answer: B
Section:

QUESTION 88
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?

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.

Correct Answer: C
Section:

QUESTION 89
Refer to the exhibit.

```
IKEv2 SAs:
Session-id:138, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local              Remote     Status  Role
45926289  172.16.1.2/500     172.16.1.1/500     READY   INITIATOR
    Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
    Life/Active Time: 86400/4 sec
Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
        remote selector 172.16.2.0/0 - 172.16.2.255/65535
        ESP spi in/out: 0xa84caabb/0xf18dce57
```

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?

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.

Correct Answer: B
Section:
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 90
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?

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.

Correct Answer: B
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html#anc12

QUESTION 91
Which feature allows a DMVPN Phase 3 spoke to switch to an alternate hub when the primary hub is unreachable?

A. multicast PIM
B. backup NHS
C. per-tunnel jitter probes
D. NHRP shortcut

Correct Answer: B
Section:
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-conndmvpn-backupnhs.html#:~:text=The%20DMVPN%2DTunnel%20Health%20Monitoring%20and%20Recovery%20(Backup%20NHS),failure%20to%20the%20primary%20hubs.
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 92
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.)

A. IS-IS
B. BGP
C. RIPv2
D. OSPF
E. EIGRP

Correct Answer: B, E
Section:

QUESTION 93
Which remote access VPN technology requires the use of the IPsec-proposal configuration option?

A. clientless SSLVPN
B. SSLVPN Full Tunnel
C. IKEv2-based VPN
D. IKEv1-based VPN

Correct Answer: C
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpnconfig/vpn-remote-access.html

QUESTION 94
Over the weekend, an administrator upgraded the Cisco ASA image on the firewalls and noticed that users cannot connect to the headquarters site using Cisco AnyConnect. What is the solution for this issue?

A. Upgrade the Cisco AnyConnect client version to be compatible with the Cisco ASA software image.

B. Upgrade the Cisco AnyConnect Network Access module to be compatible with the Cisco ASA software image.
C. Upgrade the Cisco AnyConnect client driver to be compatible with the Cisco ASA software image.
D. Upgrade the Cisco AnyConnect Start Before Logon module to be compatible with the Cisco ASA software image.

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asa-vpn-compatibility.html#Cisco_Reference.dita_60cec583-01b8-4cb2-a6e3-2fe87a6b0f82

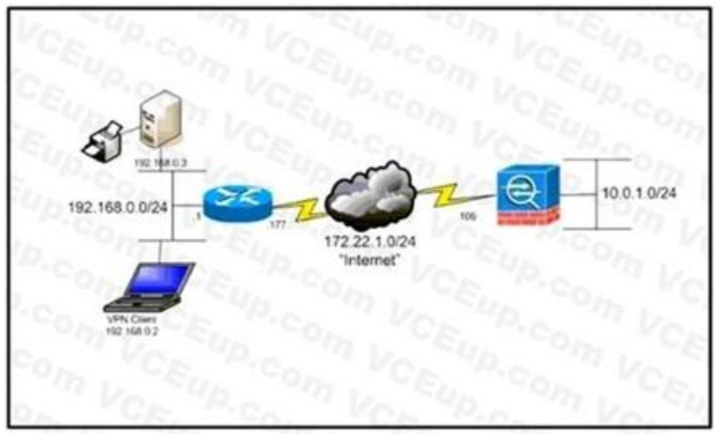
QUESTION 95

Which two components are required in a Cisco IOS GETVPN key server configuration? (Choose two.)

A. RSA key
B. IKE policy
C. SSL cipher
D. GRE tunnel
E. L2TP protocol

Correct Answer: A, B
Section:

QUESTION 96
Refer to the exhibit.



The network administrator must allow the Cisco AnyConnect Secure Mobility Client to securely access the corporate resources via IKEv2 and print locally. Traffic that is destined for the Internet must still be tunneled to the Cisco AS

A. Which configuration does the administrator use to accomplish this goal?
B. Split exclude policy with a deny for 192.168.0.3/32.
C. Split exclude policy with a permit for 0.0.0.0/32.
D. Tunnel all policy.
E. Split include policy with a permit for 192.168.0.0/24.

Correct Answer: B
Section:

QUESTION 97
An organization wants to distribute remote access VPN load across 12 VPN headend locations supporting 25,000 simultaneous users. Which load balancing method meets this requirement?

A. one VPN profile per site
B. DNS-based load balancing
C. AnyConnect native load balancing
D. equal cost, multipath load balancing

Correct Answer: B

Section:

QUESTION 98
What are two advantages of using GETVPN to traverse over the network between corporate offices?
(Choose two.)

A. It has unique session keys for improved security.
B. It supports multicast.
C. It has QoS support.
D. It is a highly scalable any to any mesh topology.
E. It supports a hub-and-spoke topology.

Correct Answer: B, D
Section:

QUESTION 99
Why must a network engineer avoid usage of the default X.509 certificate when implementing clientless SSLVPN on an ASA?

A. The certificate must be managed by the local CA.
B. The certificate is regenerated at each reboot.
C. The default X.509 certificate is not supported for SSLVPN.
D. The certificate is too weak to provide adequate security.

Correct Answer: B
Section:
Explanation:
By default, the ASA generates a self-signed X.509 certificate upon startup. This certificate is used in order to serve client connections by default. It is not recommended to use this certificate because its authenticity cannot be verified by the browser. Furthermore, this certificate is regenerated upon each reboot so it changes after each reboot. https://www.cisco.com/c/en/us/support/docs/securityvpn/ webvpn-ssl-vpn/119417-config-asa-00.html

QUESTION 100
An engineer has configured Cisco AnyConnect VPN using IKEv2 on a Cisco IOS router. The user cannot connect in the Cisco AnyConnect client, but receives an alert message "Use a browser to gain access." Which action does the engineer take to resolve this issue?

A. Reset user login credentials.
B. Correct the URL address.
C. Connect using HTTPS.
D. Disable the HTTP server.

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/115755-flexvpn-ike-eap-00.html

QUESTION 101
A router is being configured for IKEv2 AnyConnect using AnyConnect-EAP. How would the administrator separate profiles for administrators and employees so that authorization differs when they connect?

A. Define group aliases on the headend and have the user pick the appropriate alias when they connect
B. Define group-urls on the headend and create two XML profiles to match the administrator and user group urls

C. Create a certificate map and match on the appropriate certificate fields
D. Upgrade the Cisco AnyConnect Start Before Logon module to be compatible with the Cisco ASA software image.

Correct Answer: B
Section:
Explanation:
According to the documentConfigure FlexVPN: AnyConnect IKEv2 Remote Access with Local UserDatabase, one way to separate profiles for administrators and employees is to use group-urls on theheadend and create two XML profiles to match the administrator and user group urls. This allows theheadend to assign different group-policies and tunnel-groups based on the group-url that the userconnects to. For example:webvpn enable outside anyconnect image disk0:/anyconnect-win-4.6.03049-webdeploy-k9.pkg 1anyconnect enable tunnel-group-list enable group-policy Admin internal group-policy Admin attributesvpn-tunnel-protocol ikev2 ssl-client address-pools value AdminPool group-policy User internal group-policy User attributes vpn-tunnel-protocol ikev2 ssl-client address-pools value UserPool tunnel-groupAdmin type remote-access tunnel-group Admin general-attributes default-group-policy Admin tunnel-group Admin webvpn-attributes group-url https://10.0.0.1/Admin enable tunnel-group User typeremote-access tunnel-group User general-attributes default-group-policy User tunnel-group Userwebvpn-attributes group-url https://10.0.0.1/User enableThe XML profiles can be created with the AnyConnect Profile Editor and uploaded to the headend. Theprofile for administrators should have the server list entry as:<ServerList> <HostEntry> <HostName>Admin</HostName> <HostAddress>10.0.0.1</HostAddress><PrimaryProtocol>IPsec</PrimaryProtocol> <UserGroup>Admin</UserGroup> </HostEntry></ServerList>The profile for users should have the server list entry as:<ServerList> <HostEntry> <HostName>User</HostName> <HostAddress>10.0.0.1</HostAddress><PrimaryProtocol>IPsec</PrimaryProtocol> <UserGroup>User</UserGroup> </HostEntry> </ServerList>This way, when the user connects to the headend, they can choose either Admin or User from the drop-down list and get the appropriate authorization based on their group-url.

QUESTION 102
Which parameter in IPsec VPN tunnel configurations is optional?

A. hash
B. lifetime
C. encryption
D. Perfect Forward Secrecy

Correct Answer: D
Section:

QUESTION 103
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 104
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 105
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.

QUESTION 106
A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

A. failsafe
B. inline tap
C. promiscuous
D. bypass

Correct Answer: C
Section:
Explanation:
The correct answer is C. promiscuous mode. In promiscuous mode, the Cisco IPS appliance operates as a passive device that monitors a copy of the network traffic and analyzes it for malicious activity. The appliance does not affect the traffic flow, but it can generate alerts, logs, and reports based on the configured security policy. Promiscuous mode is useful for initial deployment and baseline analysis, as well as for monitoring low-risk segments of the network12.

QUESTION 107
A network administrator wants to block traffic to a known malware site at https:/www.badsite.com and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

A. Access Control policy with URL filtering
B. Prefilter policy
C. DNS policy
D. SSL policy

Correct Answer: A
Section:
Explanation:
The correct answer is A. Access Control policy with URL filtering. An Access Control policy is a type of policy that allows you to control how traffic is handled on your network based on various criteria, such as source and destination IP addresses, ports, protocols, applications, users, and URLs. URL filtering is a feature that enables you to block or allow traffic based on the URL category or reputation of the website. You can create custom URL objects to specify the exact URLs or domains that you want to block or allow. For example, you can create a URL object for https:/www.badsite.com and set it to block. This will prevent any traffic from reaching that site and any subdomains under it12.

QUESTION 108
An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

A. Specify the trace using the -T option after the capture-traffic command
B. Perform the trace within the Cisco FMC GUI instead of the Cisco FMC CLI
C. Use the verbose option as a part of the capture-traffic command
D. Use the capture command and specify the trace option to get the required information

Correct Answer: A
Section:
Explanation:
The correct answer is A. Specify the trace using the -T option after the capture-traffic command. According to the document Use Firepower Threat Defense Captures and Packet Tracer, the capture-traffic command allows you to capture packets on the Snort engine domain of the FTD device. However, by default, it only shows the packet headers and does not include the Snort detection actions. To see the Snort detection actions, you need to use the -T option, which enables tracing. For example:
capture-traffic -T
This will show the packet headers along with the Snort verdicts, such as allow, block, or replace. You can also use other options to filter or save the capture output1.
B) Performing the trace within the Cisco FMC GUI instead of the Cisco FMC CLI is not a valid option, because the FMC GUI does not support packet capture or tracing on the FTD device. You can only use the FMC GUI to view and export captures that are taken on the FTD CLI1. C) Using the verbose option as a part of the capture-traffic command is not a valid option, because there is no verbose option for this command. The verbose option is only available for the capture command, which is used to capture packets on the LINA engine domain of the FTD device1. D) Using the capture command and specifying the trace option to get the required information is not a valid option, because the capture command does not have a trace option. The capture command allows you to capture packets on the LINA engine domain of the FTD device, but it does not show the Snort detection actions. The trace option is only available for the packet-tracer command, which is used to simulate a packet going through the FTD device and show its processing steps1.