PDFVCE

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **300-730**

Title : Implementing Secure Solutions with Virtual Private Networks

Vendor : Cisco

Version : DEMO

NO.1 What action does the hub take when it receives a NHRP resolution request from a spoke for a network that exists behind another spoke?
A. The hub sends back a resolution reply to the requesting spoke.
B. The hub updates its own NHRP mapping.
C. The hub forwards the request to the destination spoke.
D. The hub waits for the second spoke to send a request so that it can respond to both spokes.
Answer: C

NO.2 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
Answer: B

NO.3 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
Answer: C
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533-AnyConnect-Configure-Basic-SSLVPN-for-I.html

NO.4 Refer to the exhibit. 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?

```
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)


Router#debug crypto isakmp

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
```

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.

Answer: A

NO.5 Refer to the exhibit. Which two conclusions should be drawn from the DMVPN phase 2 configuration? (Choose two.)

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

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

NO.6 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)
Answer: C
Explanation:
The bookmark is applied under the web vpn subconfiguration mode of the group policy.

NO.7 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.

Answer: C

NO.8 A network engineer is implementing a FlexVPN tunnel between two Cisco IOS routers. The FlexVPN tunnels will terminate on encrypted traffic on an interface configured with an IP MTU of 1500, and the company has a security policy to drop fragmented traffic coming into or leaving the network. The tunnel will be used to transfer TFTP data between users and internal servers. When the TFTP traffic is not traversing a VPN, it can have a maximum IP packet size of 1500.
Assuming the encrypted payload will add 90 bytes, which configuration allows TFTP traffic to traverse the FlexVPN tunnel without being dropped?

A. Set the tunnel IP MTU to 1500.

B. Set the tunnel tcp adjust-mss to 1460.

C. Set the tunnel IP MTU to 1400.

D. Set the tunnel tcp adjust-mss to 1360.

Answer: C

Explanation:
tcp adjust-mss is for tcp traffic only. TFTP is UDP.

NO.9 Refer to the exhibit. An engineer is diagnosing an issue that occurred after a router at a branch site was assigned a new address. Based on the debugs, what must be done to resolve this issue?

```
IKEv2:(SESSION ID = 16,SA ID = 2):Received Packet [From 192.168.20.25:500/To 192.168.20.26:500/VRF i0:f0]
Initiator SPI : 334586B9AF754E5D - Responder SPI : AC90AD1EE140D901 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 VID IDr AUTH SA TSi TSr NOTIFY(USE_TRANSPORT_MODE) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

 IKEv2:(SESSION ID = 16,SA ID = 2):Process auth response notify
 IKEv2:(SESSION ID = 16,SA ID = 2):Searching policy based on peer's identity '192.168.20.25' of type 'IPv4 address'
 IKEv2-ERROR:(SESSION ID = 16,SA ID = 2):: Failed to locate an item in the database
 IKEv2:(SESSION ID = 16,SA ID = 2):Verification of peer's authentication data FAILED
 IKEv2:(SESSION ID = 16,SA ID = 2):Auth exchange failed
 IKEv2-ERROR:(SESSION ID = 16,SA ID = 2):: Auth exchange failed
 IKEv2:(SESSION ID = 16,SA ID = 2):Abort exchange
IKEv2:(SESSION ID = 16,SA ID = 2):Deleting SA
IKEv2:(SESSION ID = 10,SA ID = 1):Retransmitting packet
```

A. Add the remote peer's IP address to the server's IKEv2 keyring.

B. Ensure that the correct preshared keys are set on both sides.

C. Ensure that the UDP 500 packets between devices are not dropped.

D. Add the remote peer's identity to the server's IKEv2 profile.

Answer: D

NO.10 Which technology and VPN component allows a VPN headend to dynamically learn post NAT IP addresses of remote routers at different sites?

A. DMVPN with ISAKMP

B. GETVPN with ISAKMP

C. DMVPN with NHRP

D. GETVPN with NHRP

Answer: C

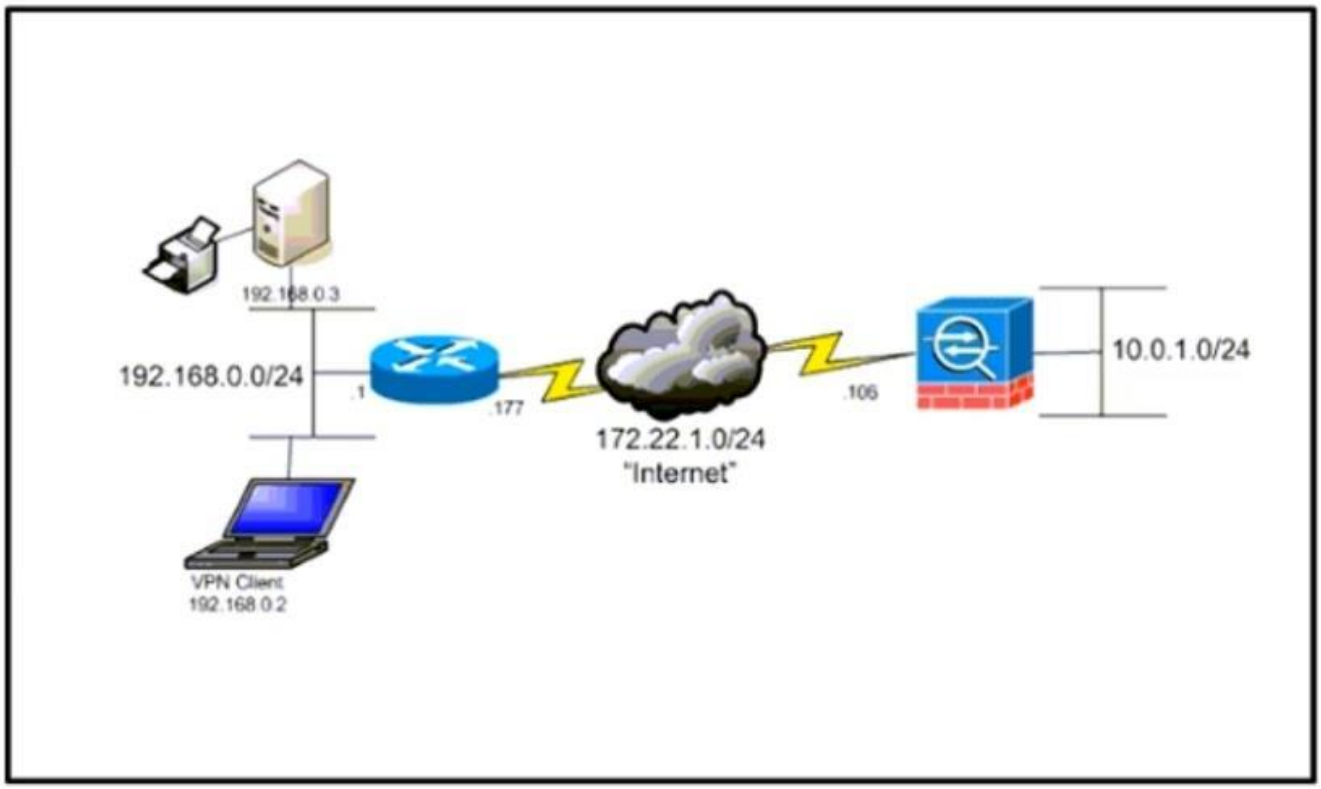
NO.11 Refer to the exhibit. Which type of VPN is used in the configuration?

```
!
interface Tunnel0
 vrf forwarding GREEN
 no ip address
 no ip redirects
 ipv6 address FE80::2001 link-local
 ipv6 address 2001:DB8:1:1::1/64
 ipv6 nhrp authentication cisco123
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 100
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf RED
!
```

A. GETVPN
B. FlexVPN
C. DMVPN
D. IPSec
Answer: C

NO.12 An engineer is requesting an SSL certificate for a VPN load-balancing cluster in which two Cisco ASAs provide clientless SSLVPN access. The FQDN that users will enter to access the clientless VPN is asa.example.com, and users will be redirected to either asa1.example.com or asa2.example.com. The cluster FQDN and individual Cisco ASAs FQDNs resolve to IP addresses 192.168.0.1, 192.168.0.2, and 192.168.0.3 respectively. The issued certificate must be able to be used to validate the identity of either ASA in the cluster without returning any certificate validation errors. Which fields must be included in the certificate to meet these requirements?
A. CN=*.example.com, SAN=asa.example.com
B. CN=192.168.0.1, SAN=asa1.example.com, asa2.example.com
C. CN=asa.example.com, SAN=asa.example.com, asa1.example.com, asa2.example.com
D. CN=192.168.0.1, SAN=192.168.0.1, 192.168.0.2, 192.168.0.3
Answer: C
Explanation:
https://integratingit.wordpress.com/2020/03/14/asa-vpn-load-balancing/

NO.13 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 ASA. Which configuration does the administrator use to accomplish this goal?



A. Split exclude policy with a deny for 192.168.0.3/32.
B. Split exclude policy with a permit for 0.0.0.0/32.
C. Tunnel all policy.
D. Split include policy with a permit for 192.168.0.0/24.
Answer: B
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/70847-local-lan-pix-asa.html

NO.14 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?

```
IKEv2-ERROR:(SESSION ID = 20,SA ID = 1):: The peer's KE payload contained the wrong DH group
IKEv2-PAK:(SESSION ID = 20,SA ID = 1):Next payload: NOTIFY, version: 2.0 Exchange type: IKE_SA_INIT, flags: RESPONDER MSG-RESPONSE Message id: 0, length: 38
Payload contents:
 NOTIFY(INVALID_KE_PAYLOAD)  Next payload: NONE, reserved: 0x0, length: 10
    Security protocol id: Unknown - 0, spi size: 0, type: INVALID_KE_PAYLOAD

IKEv2-ERROR:(SESSION ID = 20,SA ID = 1):Initial exchange failed: Initial exchange failed
```

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

NO.15 Refer to the exhibit. A network security administrator receives this error message after configuring a site-to-site IPsec VPN between two sites What is the solution to this problem?

```
IPSEC(validate_proposal): invalid local address 192.168.10.1
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

A. Transport set must match between sites.
B. IPsec policy must match between sites.
C. ISAKMP policy must match between sites.
D. Crypto map must be applied to correct interface.
Answer: D
Explanation:
The error message "IPSEC(validate_proposal): invalid local address 192.168.10.1" indicates that the IPsec tunnel cannot establish because the specified local address is incorrect or not reachable. One common cause of this issue is that the crypto map is not applied to the correct interface or is missing entirely.

NO.16 Which technology works with IPsec stateful failover?
A. GLBR
B. HSRP
C. GRE
D. VRRP
Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html#wp
1122512

NO.17 Which two tasks must be performed to implement a clientless VPN on the Cisco ASA? (Choose two.)
A. Configure a connection profile
B. Upload an AnyConnect Package.
C. Install an enrolled X.509 Certificate.
D. Configure a language translation file.
E. Configure a portal customization.
Answer: AC

NO.18 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

Answer: AB

NO.19 On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, which command is needed for the hub to be able to terminate FlexVPN tunnels?

A. interface virtual-access

B. ip nhrp redirect

C. interface tunnel

D. interface virtual-template

Answer: D

Explanation:

Spoke-to-Spoke traffic is not allowed and wanted, therefore redirect is not needed. But FlexVPN uses Virtual Templates to create Virtual Access interfaces for each connected Spoke.

NO.20 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.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111007-smart-tunnel-asa-00.html

NO.21 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.

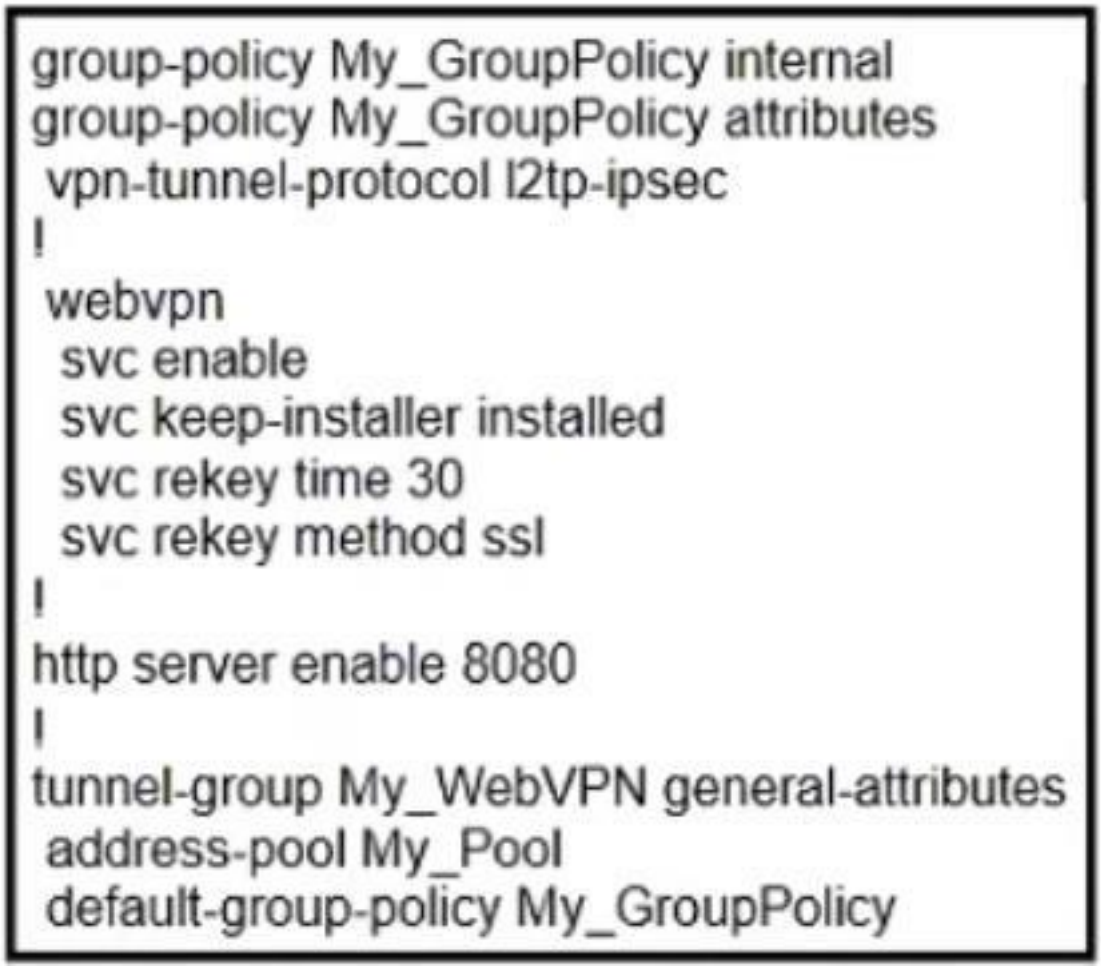
B. Adjust the preshared key on the remote peer to allow traffic to flow over the tunnel.

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.

Answer: A

NO.22 Refer to the exhibit. 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.
Answer: D

NO.23 Which two cryptographic technologies are recommended for use with FlexVPN? (Choose two.)
A. SHA (HMAC variant)
B. Diffie-Hellman
C. DES
D. MD5 (HMAC variant)
Answer: AB

NO.24 Refer to the exhibit. A network engineer is configuring remote access VPN on a Cisco IOS router but cannot establish a connection from the Cisco Secure Client client. Which action resolves the issue?

```
aaa authentication login EAP_AUTHC local
aaa authorization exec default local
aaa authorization network EAP_AUTHZ local
!
!
crypto pki trustpoint TP_AnyConnect
enrollment selfsigned
usage ike
serial-number none
fqdn Router.com
ip-address none
subject-name cn=r01.companyx.com
subject-alt-name r01.companyx.com
revocation-check none
rsakeypair AnyConnect
!
!
crypto ikev2 profile AC_EAP
match identify remote key-id *$AnyConnectClient$*
authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint TP-AnyConnect
aaa authentication anyconnect-eap EAP_AUTHC
aaa authorization group anyconnect-eap list EAP_AUTHZ ikev2-auth-policy
aaa authorization user anyconnect-eap cached
!
no crypto ikev2 http-url cert
!
```

A. Use symmetric keys in ikev2 profile.

B. Change Secure Client IKE identity to *$Default$*.

C. Enable crypto ikev2 http-url cert.

D. Replace self-signed certificate with a valid certificate.

Answer: D

Explanation:

In the given configuration, the trustpoint TP_AnyConnect is using a self-signed certificate (enrollment selfsigned). When using Cisco Secure Client (formerly AnyConnect) with IKEv2, the client expects a valid, trusted certificate issued by a Certificate Authority (CA).

Since self-signed certificates are not trusted by default, the client may reject the connection, causing the VPN tunnel to fail. To resolve this issue, the engineer should:

1. Obtain and install a trusted CA-signed certificate on the router.
2. Update the crypto pki trustpoint configuration to use the new certificate.
3. Ensure the certificate Common Name (CN) and Subject Alternative Name (SAN) match the VPN gateway's FQDN.