DUMPSBOSS.

# Implementing Secure Solutions with Virtual Private Networks (SVPN)

## Cisco 300-730

## Version Demo

**Total Demo Questions: 22**

**Total Premium Questions: 225**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Secure Communications Architecture | 46 |
| Topic 2, Secure Communications Implementation | 110 |
| Topic 3, Secure Communications Troubleshooting | 68 |
| Topic 4, Secure Communications Monitoring | 1 |
| Total | 225 |

QUESTION NO: 1

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.

**ANSWER: B**

**Explanation:**

The certificate is regenerated at each reboot. This behavior makes the ASA's default self-signed identity certificate unsuitable for a production clientless SSL VPN deployment because the certificate presented to users can change after an ASA restart. Browsers and VPN portal users rely on a consistent server identity to validate that they are connecting to the intended gateway. When the certificate changes unexpectedly, users receive certificate warnings and can no longer reliably recognize the ASA by its prior certificate or certificate fingerprint. This creates an operational burden and can train users to bypass browser security warnings, which is undesirable for a remote-access security service.

A production ASA should instead use a persistent identity certificate, typically issued by a public certificate authority for Internet-facing remote access or by an enterprise PKI when all clients trust the internal CA. The certificate should contain the fully qualified domain name that users enter for the clientless SSL VPN portal and be configured on the appropriate ASA interface. Cisco's SSL VPN guidance discusses configuring a trusted identity certificate for WebVPN/clientless SSL VPN, rather than relying on the default self-signed certificate. See Cisco: Configure an Identity Certificate for SSL VPN on ASA and Cisco ASA Command Reference.

**QUESTION NO: 2**

Refer to the exhibit.

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.

**ANSWER: C E**

**Explanation:**

Changing the ISAKMP policy authentication on the spoke to pre-shared resolves the Phase 1 IKE authentication mismatch. For a conventional DMVPN deployment using an ISAKMP pre-shared key, both peers must negotiate a compatible IKE policy, including the same authentication method. Once the spoke uses `authentication pre-share`, it can authenticate using the configured ISAKMP key and establish the IPsec security association required to protect GRE/NHRP traffic.

Changing the NHRP authentication key on the spoke to `cisco123` resolves the NHRP authentication mismatch. DMVPN relies on NHRP between the spoke and NHS hub so that the spoke can register its tunnel-to-NBMA mapping and obtain NHRP information. When NHRP authentication is configured, the authentication string must match on NHRP peers participating in the same DMVPN cloud. With the matching key, the hub accepts the spoke's NHRP registration after the IKE/IPsec protection is available, allowing the spoke-to-hub DMVPN session to come up.

Cisco's DMVPN documentation describes the dependency on NHRP registration and the IPsec-protected DMVPN tunnel: Cisco DMVPN Overview. Cisco also documents IKE policy authentication configuration in the Cisco IKE Configuration Guide.

## QUESTION NO: 3

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

**A.** Verify that the ISAKMP proposals match.

**B.** Ensure that UDP 500 is not being blocked between the devices.

**C.** Correct the peer's IP address on the crypto map.

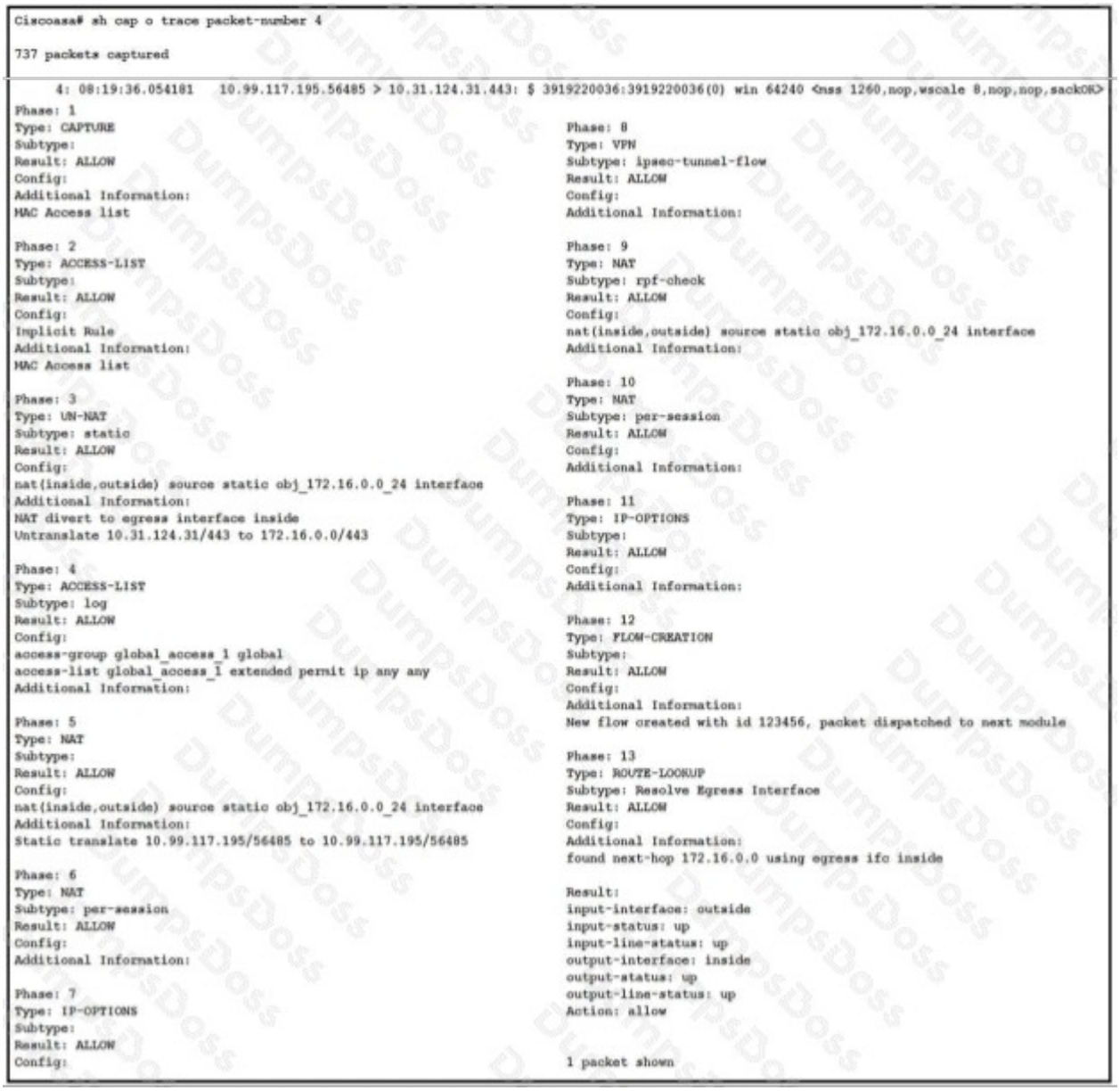
**D.** Confirm that the pre-shared keys match on both devices.

## ANSWER: B

**Explanation:**

Ensure that UDP 500 is not being blocked between the devices. The `MM_KEY_EXCH` state represents the Main Mode key-exchange portion of IKEv1 Phase 1. At this point, the peers have progressed sufficiently to exchange keying material, including the Diffie-Hellman exchange and nonce payloads, but the Main Mode negotiation has not completed. IKEv1 uses UDP port 500 for these exchanges unless NAT traversal is detected, in which case later traffic can use UDP 4500. A firewall, access-control list, security policy, or intermediate device that drops UDP 500 in either direction can therefore leave the ISAKMP security association stalled at `MM_KEY_EXCH`. Verify bidirectional UDP/500 reachability between the peer addresses, inspect filtering and NAT behavior on every transit device, and clear the incomplete ISAKMP SA before retrying the negotiation. Cisco documents that IKE establishes Phase 1 security associations through Main Mode exchanges and identifies UDP port 500 as the IKE transport port. See Cisco's IKE for IPsec VPN configuration guide and the Cisco IKE debugging guide.

## QUESTION NO: 4



```
Ciscoasa# sh cap c trace packet-number 4

737 packets captured

     4: 08:19:36.054181   10.99.117.195.56485 > 10.31.124.31.443: S 3919220036:3919220036(0) win 64240 <mss 1260,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
NAT divert to egress interface inside
Untranslate 10.31.124.31/443 to 172.16.0.0/443

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group global_access_1 global
access-list global_access_1 extended permit ip any any
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:
Static translate 10.99.117.195/56485 to 10.99.117.195/56485

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:

Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat(inside,outside) source static obj_172.16.0.0_24 interface
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 123456, packet dispatched to next module

Phase: 13
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.0.0 using egress ifc inside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow


1 packet shown
```

Refer to the exhibit. An SSL client is connecting to an ASA headend. The session fails with the message “Connection attempt has timed out. Please verify Internet connectivity.” Based on how the packet is processed, which phase is causing the failure?

**A.** phase 9: rpf-check

**B.** phase 5: NAT

**C.** phase 4: ACCESS-LIST

**D.** phase 3: UN-NAT

**ANSWER: D**

**Explanation:**

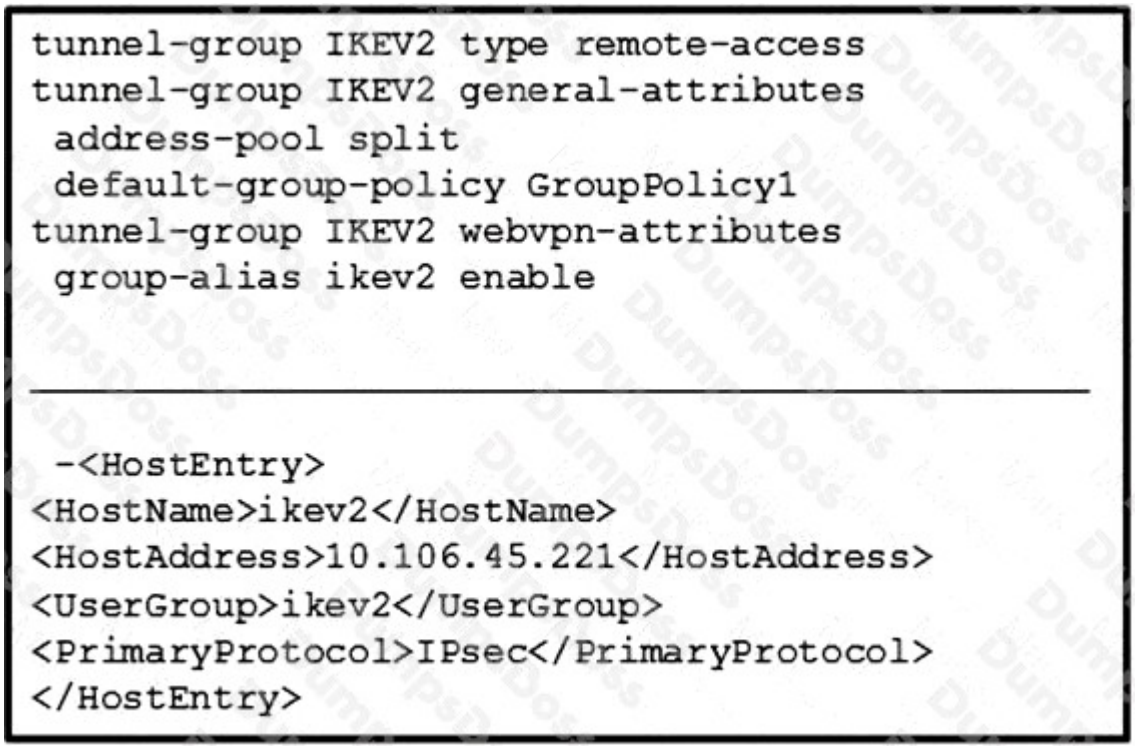
The failure occurs during **phase 3: UN-NAT**. ASA processes an arriving packet through a sequence of packet-processing checks, including reverse NAT processing before the ASA can apply the remainder of its forwarding and connection logic. UN-NAT determines whether the packet’s destination must be reverse-translated according to a configured static or identity NAT rule and identifies the effective destination information that subsequent processing uses.

For an SSL VPN connection addressed to the ASA headend, this stage is especially significant because the client must reach the ASA’s SSL listener using the expected outside address and TCP service. The packet-tracer result in the exhibit identifies the UN-NAT stage as the point at which processing fails. Consequently, the SSL client cannot establish the initial

TCP/SSL connection and reports a timeout rather than reaching VPN authentication or tunnel establishment. Cisco documents that ASA NAT processing includes UN-NAT handling for traffic entering an interface and that packet-tracer displays the processing phase and disposition used to isolate such failures. See Cisco's ASA NAT basics documentation and ASA packet-tracer command reference.

## QUESTION NO: 5

Refer to the exhibit.




The customer can establish a Cisco AnyConnect connection without using an XML profile. When the host " ikev2 " is selected in the AnyConnect drop down, the connection fails. What is the cause of this issue?

**A.** The HostName is incorrect.

**B.** The IP address is incorrect.

**C.** Primary protocol should be SSL.

**D.** UserGroup must match connection profile.

## ANSWER: D

**Explanation:**

**UserGroup must match connection profile.** For an AnyConnect profile that uses IPsec as its primary protocol, the UserGroup value is not merely a descriptive label displayed to the user. AnyConnect uses it with the configured host address to construct the group-based connection request, and the value must exactly match the name of the ASA or Secure Firewall connection profile (also called the tunnel group) intended for that remote-access VPN connection. When a user selects the host entry named *ikev2*, AnyConnect attempts to establish the IPsec/IKEv2 connection using the UserGroup configured in that XML host entry. If that value differs from the actual connection-profile name on the headend, the device cannot associate the request with the required tunnel-group policy, authentication settings, and IPsec parameters. The connection therefore fails even though a manually initiated connection can succeed without the XML profile. Aligning the UserGroup string, including its exact spelling and case where applicable, with the configured connection-profile name allows AnyConnect to select the correct remote-access VPN policy. Cisco documents that for IPsec primary protocol entries, User Group must be the exact connection-profile/tunnel-group name. See Cisco's AnyConnect XML Settings documentation and the Cisco ASA IKEv2 command reference.

## QUESTION NO: 6

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.** Install a machine identity certificate in the Local Computer Personal certificate store and trust its issuing CA.

**D.** Create a Cisco AnyConnect VPN profile with Always On set to true.

**E.** Create a Cisco Anyconnect VPN Management Tunnel profile.

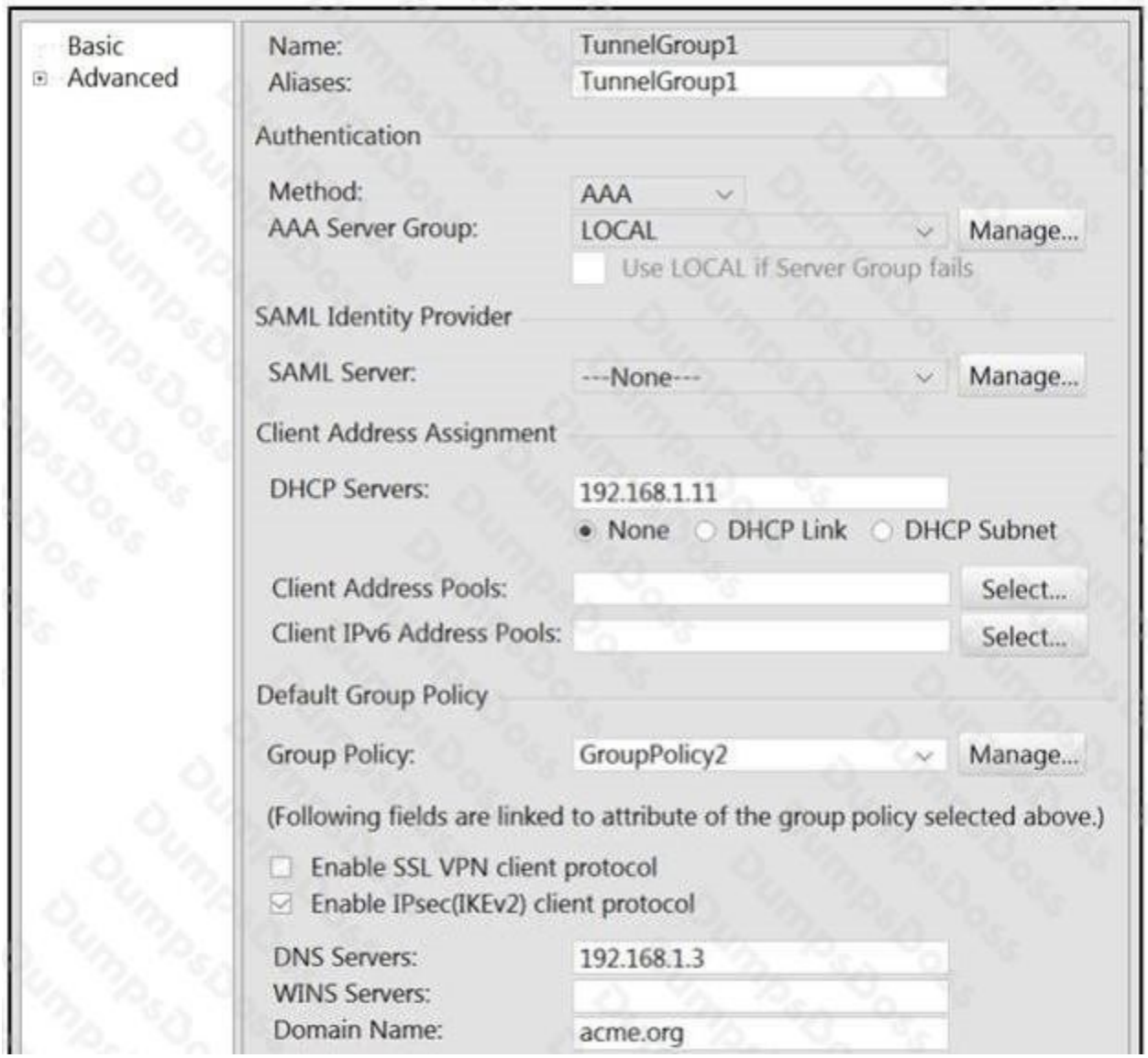
## ANSWER: B C

**Explanation:**

Start Before Logon must be enabled in the Cisco AnyConnect VPN client profile because this setting makes the AnyConnect VPN tile and connection capability available at the Windows sign-in screen, before an interactive user session begins. Establishing the tunnel at that point gives the computer reachability to domain resources, so domain processing and logon scripts can run when the user signs in. The profile is normally deployed from the ASA to the endpoint as part of the AnyConnect configuration.

A machine identity certificate is also required for certificate-based pre-logon authentication without depending on a user certificate or interactive credential entry. The endpoint's identity certificate, including its private key, belongs in the Local Computer Personal certificate store; the issuing CA chain must be trusted by the computer, and the ASA must trust the CA that issued the machine certificate. This lets the device authenticate while no user profile is yet loaded. Cisco documents the Start Before Logon profile capability in the Cisco AnyConnect Secure Mobility Client Administrator Guide. Microsoft also documents the distinction between the local-computer personal store and trusted-root store in its Certificate Stores guidance.

## QUESTION NO: 7




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.

**ANSWER: A**

**Explanation:**

Enable the client protocol in the Cisco AnyConnect profile. A remote-access SSL VPN session using Cisco AnyConnect requires the SSL client tunnel protocol to be permitted for the applicable connection profile and its assigned group policy. This setting authorizes the ASA to negotiate an AnyConnect SSL VPN tunnel after the user supplies credentials. Local user accounts can then be used by the ASA's local authentication database, provided the connection profile is configured to use local authentication or no external AAA server group overrides it. In the exhibit's configuration, the missing client-protocol enablement prevents the AnyConnect SSL connection from progressing to a successful tunnel establishment, regardless of whether the entered local username and password are valid. Enabling the AnyConnect SSL client protocol makes the connection profile accept the intended remote-access client type and allows the local credentials to be processed for the VPN login. Cisco documents that remote-access VPN policies control the permitted tunnel protocols, including the SSL client protocol used by AnyConnect. See Cisco ASA Remote Access VPN Configuration Guide and Cisco Secure Client (AnyConnect) Administrator Guide.

## QUESTION NO: 8

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

**A.** method

**B.** profile

**C.** proposal

**D.** preference

**E.** persistence

## ANSWER: B C

**Explanation:**

FlexVPN uses IKEv2 to establish and manage the secure VPN control-plane session, so an IKEv2 proposal and an IKEv2 profile are required configuration components. The **proposal** defines the cryptographic algorithms and parameters that IKEv2 can negotiate to protect IKE security associations. This includes the encryption algorithm, integrity algorithm where applicable, Diffie-Hellman group, and pseudorandom-function settings. The peers need compatible proposal settings in order to successfully negotiate the IKEv2 security association.

The **profile** supplies the policy that IKEv2 applies when matching and authenticating a peer. In a FlexVPN deployment, the IKEv2 profile typically identifies peers through match criteria and specifies the authentication method, such as a pre-shared key or certificates. The profile also associates the applicable IKEv2 proposal with the connection policy. Together, the proposal provides the negotiable cryptographic suite and the profile provides peer matching and authentication policy, allowing FlexVPN peers to establish IKEv2-based tunnels. Cisco's FlexVPN configuration guidance shows IKEv2 proposals and profiles as core elements of the IKEv2 configuration: Cisco IOS XE FlexVPN Configuration Guide. IKEv2 proposal and profile command details are also documented in the Cisco IKEv2 Command Reference.

## QUESTION NO: 9

**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
```

Refer to the exhibit. 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.

**ANSWER: D E**

**Explanation:**

Change the ISAKMP key address on the spoke to 0.0.0.0. This configures the spoke's pre-shared-key entry to match an IKE peer regardless of the peer's NBMA source address. In a DMVPN deployment, this is useful when the peer relationship must accept the hub through the tunnel's dynamic VPN/IPsec operation rather than relying on an overly specific address match in the key statement. The IKE Phase 1 exchange can then locate the applicable pre-shared key and establish the security association needed to protect the GRE/NHRP traffic.

Change the nhrp authentication key on the spoke to cisco123. NHRP authentication is a common key shared by members of the same DMVPN cloud. The spoke must use the same NHRP authentication string as the hub so that its NHRP registration is accepted. Once IKE/IPsec can establish and NHRP authentication matches, the spoke can register its tunnel-to-NBMA mapping with the NHS and form the operational DMVPN relationship. Cisco's DMVPN configuration guidance describes the use of NHRP authentication within an NHRP network and the supporting IPsec/IKE configuration: Cisco IOS XE DMVPN Configuration Guide. See also Cisco's IKE Configuration Guide for pre-shared-key configuration behavior.

## QUESTION NO: 10

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 resources through 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 resources through 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.

**ANSWER: C D**

**Explanation:**

A Cisco ASA can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions because the ASA remote-access VPN service supports both clientless browser-based access and AnyConnect secure-client connections at the same time. These are distinct access methods delivered through the ASA WebVPN/SSL VPN capability, and an administrator can make both available to users through the applicable connection profiles, group policies, and portal configuration. This allows browser-only access for supported web applications while also offering a full AnyConnect VPN connection where the user requires broader network access.

When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the ASA uses its configured DNS servers to perform FQDN resolution. In Clientless SSL VPN, the browser communicates with the ASA portal, and the ASA acts as the intermediary for proxied web requests. Therefore, the ASA must resolve the internal web-server name using DNS configuration available to the Clientless SSL VPN session, such as the DNS server group assigned through policy. Cisco documents DNS configuration and name-resolution behavior as part of Clientless SSL VPN setup and operation. See the Cisco ASA SSL VPN configuration guide and Cisco ASA command reference.

## QUESTION NO: 11

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.

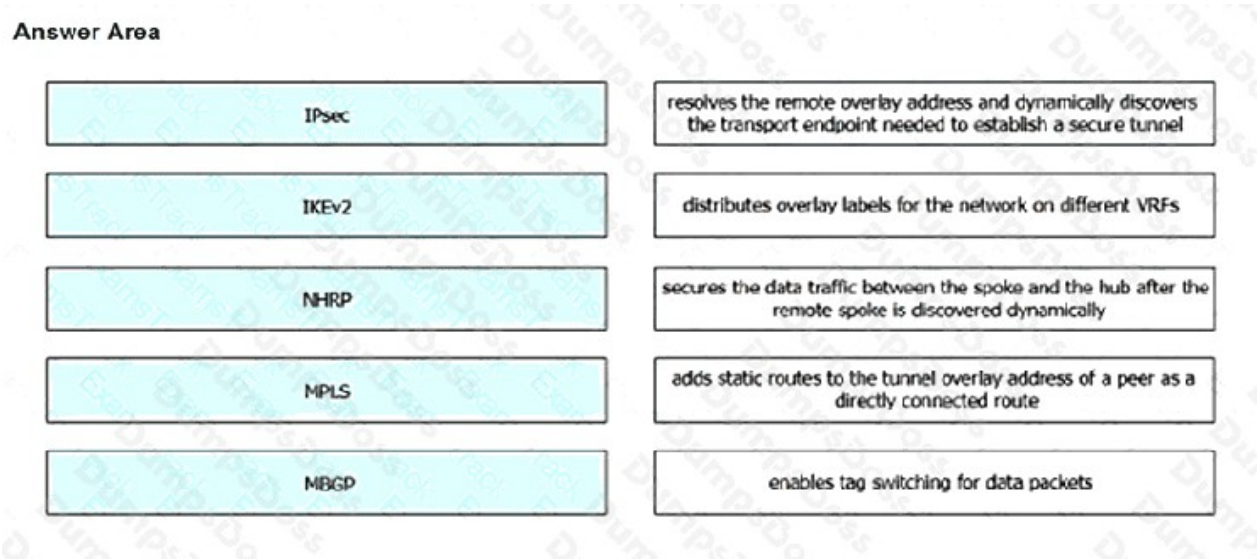
**ANSWER: B**

**Explanation:**

The ASA cannot resolve the URL. A clientless SSL VPN bookmark is accessed through the ASA, which acts as a proxy for the internal web resource. When the bookmark is configured with a hostname or fully qualified domain name rather than a directly reachable IP address, the ASA must be able to perform DNS resolution for that name before it can establish the proxied connection to the web server. The required DNS server configuration must be available to the ASA in the applicable interface, group-policy, or tunnel-group context, and the ASA must have network reachability to the DNS server. If name resolution fails, selecting the bookmark cannot produce a connection to the target web application even though the user successfully authenticated to the clientless SSL VPN portal and can see the bookmark. Cisco's clientless SSL VPN documentation describes bookmarks as links to web resources accessed through the clientless portal and documents the DNS requirements used to reach named resources. See the Cisco ASA Clientless SSL VPN configuration guide and this related Cisco Community discussion.

## QUESTION NO: 12 - (DRAG DROP)

Drag and drop the GETVPN components from the left onto the descriptions on the right.




**ANSWER:**

**Explanation:**

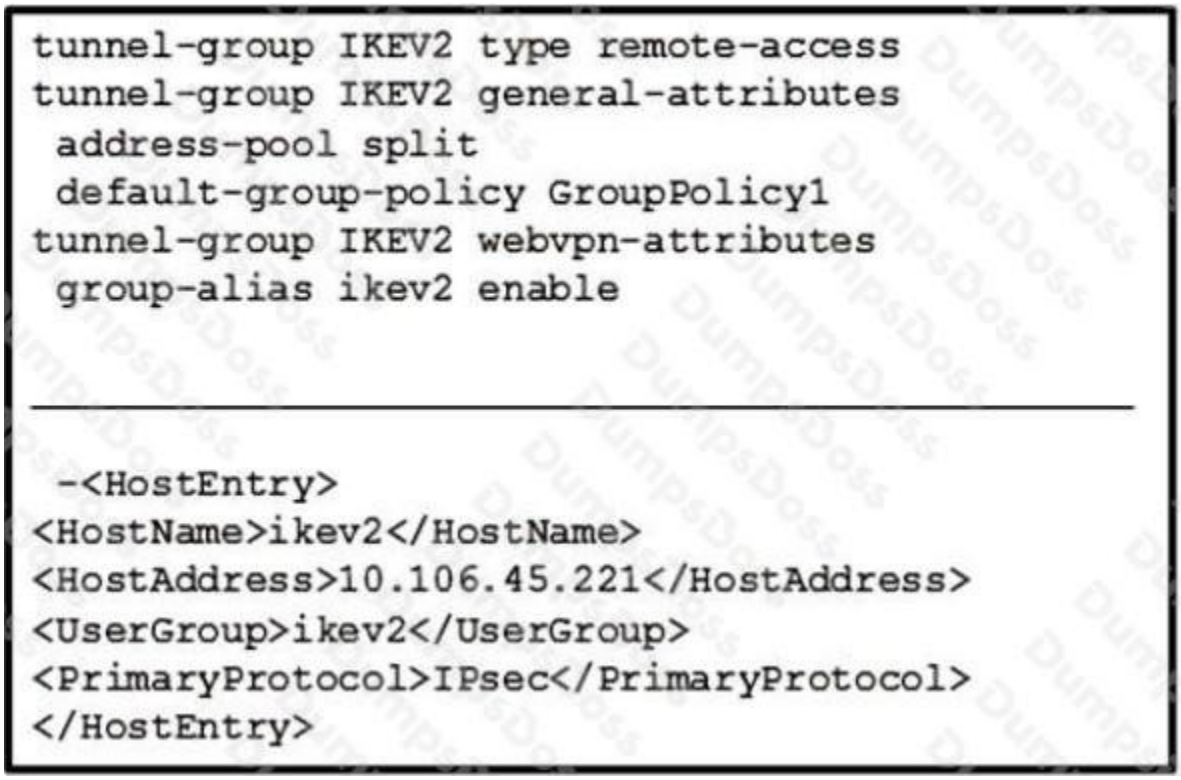
The completed mapping correctly associates each networking technology with its operational role. NHRP is responsible for resolving a remote peer's overlay address and identifying the transport endpoint that is needed to form a secure tunnel. This dynamic resolution function is what allows spoke-to-spoke communication to be established without requiring all traffic to remain on a hub path. Cisco's NHRP configuration guide describes NHRP as the mechanism used to map protocol addresses to NBMA addresses: Cisco NHRP Configuration Guide.

MPBGP distributes VPN reachability information and associated labels across different VRFs, allowing routes to be carried in a VPN-aware control plane. IPsec then provides the actual cryptographic protection for data traffic once the remote peer

has been dynamically discovered. IKEv2 supports the overlay tunnel routing behavior by adding a static route for the peer's tunnel-overlay address as a directly connected route, which enables the appropriate peer reachability used during tunnel establishment. Cisco documents IKEv2 as the key-management protocol that negotiates IPsec security associations: Cisco IKEv2 Security Configuration Guide.

Finally, MPLS enables label, commonly called tag, switching for data packets. Packets are forwarded based on labels rather than requiring a full IP route lookup at every MPLS hop. These roles align exactly with the placements shown in the answered image.

## QUESTION NO: 13




Refer to the exhibit. The customer can establish a Cisco AnyConnect connection without using an XML profile. When the host "ikev2" is selected in the AnyConnect drop down, the connection fails. What is the cause of this issue?

**A.** The HostName is incorrect.

**B.** The IP address is incorrect.

**C.** Primary protocol should be SSL.

**D.** UserGroup must match connection profile.

## ANSWER: D

**Explanation:**

UserGroup must match connection profile. An AnyConnect XML profile can define a host entry that appears in the client's server-selection drop-down list. In addition to the displayed host name and ASA address, the host entry can include a `UserGroup` value. This value tells AnyConnect which ASA connection profile (also called a tunnel group) to request when it initiates the connection. Therefore, selecting the `ikev2` host applies the configured user-group value rather than relying on the default connection behavior used when no XML profile is present.

The ASA must have a corresponding connection profile whose name matches the user-group value supplied by the XML host entry, and that profile must be enabled and configured for the intended remote-access method. When those values do not match, the client is directed to a nonexistent or unintended connection profile and the connection attempt fails. Aligning the XML `UserGroup` entry with the ASA connection-profile name ensures that selecting the host invokes the correct

authentication, group-policy, and tunnel settings. Cisco documents the XML host-entry fields, including `UserGroup`, in its AnyConnect XML Settings reference. Related Secure Client profile and connection behavior is covered in the Cisco Secure Client Administration Guide.

## QUESTION NO: 14

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

**A.** FlexVPN

**B.** clientless

**C.** EZVPN

**D.** L2TP

**E.** Cisco AnyConnect

## ANSWER: B E

**Explanation:**

Clientless and Cisco AnyConnect are the remote-access VPN solutions that support SSL/TLS. Clientless SSL VPN provides browser-based access to selected internal web applications and other supported resources without requiring a VPN client installation on the endpoint. The user connects to the secure gateway over HTTPS, authenticates, and accesses resources through the portal or URL-list mechanisms. This model is useful when endpoints cannot be managed or when installing a client is impractical.

Cisco AnyConnect supports SSL/TLS remote access VPN connections between the AnyConnect Secure Mobility Client and the security gateway. SSL/TLS provides the initial secure transport over TCP/443, which is particularly valuable when restrictive networks permit HTTPS but may block other VPN protocols. Depending on the gateway configuration and network conditions, AnyConnect can also use DTLS to provide a UDP-based data channel, but its SSL/TLS capability is the relevant feature here. Cisco documents both clientless SSL VPN access and AnyConnect SSL VPN connectivity as remote-access capabilities of Cisco Secure Firewall/ASA platforms. See Cisco's SSL VPN configuration guide and the Cisco AnyConnect Secure Mobility Client support documentation.

## QUESTION NO: 15

A network engineer is troubleshooting a route-based IPsec VPN using virtual tunnel interfaces on two Cisco IOS XE routers. The IKEv2 security association is established, but no protected user traffic crosses the tunnel. Which two items must be verified? (Choose two.)

**A.** Verify that a route to the remote protected network points to the tunnel interface.

**B.** Verify that the tunnel interface has a tunnel protection IPsec profile.

**C.** Verify that matching crypto ACLs are applied to both physical interfaces.

**D.** Verify that NHRP static mappings exist for the remote peer.

**E.** Verify that the VTI is configured as a clientless SSL VPN resource.

## ANSWER: A B

**Explanation:**

The tunnel interface must be operational and have valid routing for the protected destinations. Route-based VPNs use the routing table to select the VTI as the forwarding path for protected traffic. Even when IKEv2 is established, user traffic cannot use the VPN unless a route points the remote protected network toward the tunnel interface.

The tunnel interface must also have the appropriate tunnel protection IPsec profile applied. The profile associates IPsec protection with traffic forwarded through the VTI. A functioning IKEv2 security association alone does not ensure that packets routed into the tunnel are protected by an IPsec security association. Cisco documents VTI routing and tunnel-protection configuration in the Cisco IOS XE IPsec VPN Configuration Guide.

## QUESTION NO: 16

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

## ANSWER: B C

**Explanation:**

DNS-based hub resolution and reactivate primary peer are valid IOS FlexVPN client backup capabilities. A FlexVPN client can be configured with hub peers identified by fully qualified domain names, allowing DNS resolution to provide reachable hub addresses. This approach supports resiliency where a DNS name can resolve to an available hub address rather than binding the client permanently to one static IP address. Cisco's FlexVPN documentation describes peer selection and client connection behavior as part of the IKEv2 FlexVPN client configuration model.

The `reactivate primary-peer` behavior is also specifically intended for backup-peer operation. After the client has moved to a backup peer because the preferred peer was unavailable, this setting enables the client to attempt to return to the primary peer when that peer becomes reachable again. This preserves primary/backup preference while maintaining connectivity during a hub failure or outage. These features are configured in the IKEv2 FlexVPN client context and provide client-side hub redundancy and recovery behavior. See Cisco's FlexVPN configuration guide and the Cisco IKEv2 command reference.

## QUESTION NO: 17

Which two locations can assign a group policy to a Cisco ASA remote-access VPN user? (Choose two.)

**A.** the connection-profile general-attributes configuration

**B.** the user attributes configuration

**C.** the crypto map sequence configuration

**D.** the interface access-group configuration

**E.** the SSL trustpoint configuration

## ANSWER: A B

**Explanation:**

A group policy can be assigned as the default group policy under a connection profile, also called a tunnel group. The ASA applies this policy to users who connect through that profile unless a more specific user policy is returned or configured. The group policy can define settings such as permitted tunnel protocols, address pools, DNS servers, split-tunneling rules, and clientless portal permissions.

A group policy can also be assigned in the user attributes. A locally configured user can have a group-policy attribute, and external AAA authorization can return the applicable group-policy value. A user-level assignment takes precedence over the

default group policy configured for the connection profile. Cisco documents group-policy inheritance and user-level policy assignment in the Cisco ASA Remote-Access VPN Configuration Guide.

## QUESTION NO: 18

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

## ANSWER: D

**Explanation:**

GETVPN has no requirement for an overlay routing protocol because it encrypts traffic using tunnel-less IPsec in the original, or "native," routing domain. Group members receive a common security policy and group security association information from the key server, then apply IPsec protection directly to qualifying packets. The original source and destination IP addresses remain available for routing, so the existing WAN routing infrastructure determines the forwarding path. This is particularly useful for private MPLS or other routed WANs, where enterprises can retain their normal routing design and still apply group-based encryption across many sites.

DMVPN and FlexVPN are overlay VPN technologies: they establish IPsec-protected tunnels over an underlay network. Their VPN reachability and tunnel forwarding design commonly require routing information to be exchanged or configured across that overlay. GETVPN avoids that additional overlay-routing requirement, which simplifies deployment where the WAN already provides any-to-any connectivity and native multicast and routing behavior must be preserved. Cisco describes GETVPN as a tunnel-less VPN solution that preserves the original packet header and supports the use of native routing. See Cisco's GETVPN configuration guide and the Cisco GETVPN overview.

## QUESTION NO: 19

Refer to the exhibit.

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

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

crypto ikev2 redirect gateway init
```

Which type of VPN implementation is displayed?

**A.** IKEv1 cluster

**B.** IKEv2 backup gateway

**C.** IKEv2 load balancer

**D.** IKEv2 reconnect

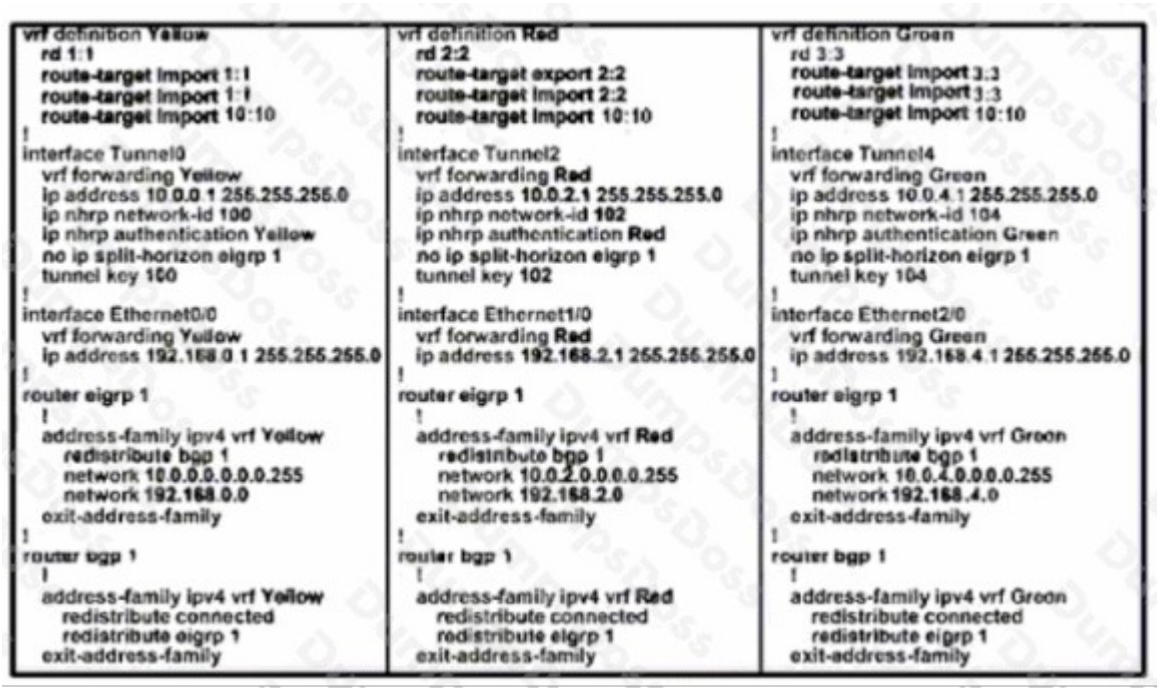
**ANSWER: C**

**Explanation:**

IKEv2 load balancer is correct. Cisco FlexVPN supports IKEv2 server load balancing to distribute remote-access VPN connection requests across multiple VPN gateways. In this design, a load-balancing device or designated load-balancing function receives the initial IKEv2 connection request and directs the client toward an appropriate VPN gateway, based on the configured policy and the availability or load of the gateways. The client then establishes its VPN security association with the selected gateway. This approach lets an organization scale remote-access VPN capacity while presenting a consistent entry point to users and avoiding concentration of new sessions on one headend. Cisco documents this capability as FlexVPN Server Load Balancing and describes its use with IKEv2 to redirect clients to an available server in a server group. The topology shown therefore represents an IKEv2 load-balancing implementation. See Cisco's FlexVPN Server Load Balancing configuration guide and the Cisco IOS XE IKEv2 and FlexVPN configuration guide.

## QUESTION NO: 20

Refer to the exhibit.



```
vrf definition Yellow
 rd 1:1
 route-target import 1:1
 route-target import 1:1
 route-target import 10:10
!
interface Tunnel0
 vrf forwarding Yellow
 ip address 10.0.0.1 255.255.255.0
 ip nhrp network-id 100
 ip nhrp authentication Yellow
 no ip split-horizon eigrp 1
 tunnel key 100
!
interface Ethernet0/0
 vrf forwarding Yellow
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 !
 address-family ipv4 vrf Yellow
  redistribute bgp 1
  network 10.0.0.0.0.0.0.255
  network 192.168.0.0
 exit-address-family
!
router bgp 1
 !
 address-family ipv4 vrf Yellow
  redistribute connected
  redistribute eigrp 1
 exit-address-family
```

```
vrf definition Red
 rd 2:2
 route-target export 2:2
 route-target import 2:2
 route-target import 10:10
!
interface Tunnel2
 vrf forwarding Red
 ip address 10.0.2.1 255.255.255.0
 ip nhrp network-id 102
 ip nhrp authentication Red
 no ip split-horizon eigrp 1
 tunnel key 102
!
interface Ethernet1/0
 vrf forwarding Red
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 !
 address-family ipv4 vrf Red
  redistribute bgp 1
  network 10.0.2.0.0.0.0.255
  network 192.168.2.0
 exit-address-family
!
router bgp 1
 !
 address-family ipv4 vrf Red
  redistribute connected
  redistribute eigrp 1
 exit-address-family
```

```
vrf definition Green
 rd 3:3
 route-target import 3:3
 route-target import 3:3
 route-target import 10:10
!
interface Tunnel4
 vrf forwarding Green
 ip address 10.0.4.1 255.255.255.0
 ip nhrp network-id 104
 ip nhrp authentication Green
 no ip split-horizon eigrp 1
 tunnel key 104
!
interface Ethernet2/0
 vrf forwarding Green
 ip address 192.168.4.1 255.255.255.0
!
router eigrp 1
 !
 address-family ipv4 vrf Green
  redistribute bgp 1
  network 10.0.4.0.0.0.0.255
  network 192.168.4.0
 exit-address-family
!
router bgp 1
 !
 address-family ipv4 vrf Green
  redistribute connected
  redistribute eigrp 1
 exit-address-family
```

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

**A.** site-to-site

**B.** DMVPN

**C.** L2VPN

**D.** multicast VPN

**ANSWER: C**

**Explanation:**

L2VPN is correct because the configuration output identifies a Layer 2 VPN service, which transports Ethernet or other Layer 2 frames across an IP/MPLS provider network while preserving Layer 2 service characteristics for the attached customer endpoints. Cisco Layer 2 VPN implementations commonly use pseudowires, with commands and operational output referring to constructs such as an xconnect, a virtual circuit, attachment circuits, or a pseudowire peer. These elements indicate that the device is extending a Layer 2 service between locations rather than simply encrypting routed IP traffic.

Cisco documents L2VPN as a VPN architecture that provides Layer 2 connectivity between customer sites over a service-provider backbone. In particular, Ethernet over MPLS and pseudowire services map a local attachment circuit to a remote pseudowire, allowing the customer-facing interfaces to behave as though they are connected by a common Layer 2 service. This is the defining behavior identified by the displayed configuration. See Cisco's Layer 2 VPN configuration guide and its pseudowire configuration documentation.

## QUESTION NO: 21

Refer to the exhibit.

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

## ANSWER: C

**Explanation:**

**FlexVPN server for an IPv6 dVTI session** is configured. FlexVPN uses IKEv2 to establish dynamic, policy-based remote-access or site-to-site VPN connections, and a dynamic Virtual Tunnel Interface (dVTI) provides the per-peer virtual access interface created when an authorized IKEv2/IPsec session comes up. The server-side configuration associates IKEv2 authorization and IPsec protection with a virtual-template interface, allowing the router to instantiate a separate virtual-access interface dynamically for each connecting peer.

When IPv6 addressing and IPv6 routing attributes are supplied through the IKEv2 authorization policy and applied to the dynamic tunnel, the resulting FlexVPN connection is an IPv6 dVTI session. This design supports scalable peer connections because the hub does not require a separately preconfigured static tunnel interface for every remote peer. Cisco's FlexVPN configuration guidance describes use of IKEv2 profiles, authorization policies, virtual templates, and dynamic VTIs for this server role. See Cisco FlexVPN Configuration Guide and Cisco IOS XE FlexVPN Configuration Guide.

## QUESTION NO: 22

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

(Choose two.)

**A.** Telnet bookmark via the Telnet plugin

**B.** RDP2 bookmark via the RDP2 plugin

**C.** VNC bookmark via the VNC plugin

**D.** Citrix bookmark via the ICA plugin

**E.** SSH bookmark via the SSH plugin

**ANSWER: B C**

**Explanation:**

The correct configurations are **RDP2 bookmark via the RDP2 plugin** and **VNC bookmark via the VNC plugin**. Both provide graphical remote-desktop access through the ASA clientless SSL VPN portal. The RDP2 plug-in is designed for Microsoft Remote Desktop connections and supports access to Windows Vista systems using their Remote Desktop Services capability. An administrator can publish an RDP2 bookmark in the appropriate group policy and then initiate a remote graphical session to the Vista workstation from the clientless portal, provided the target system is configured to accept Remote Desktop connections.

A VNC bookmark via the VNC plug-in also provides a graphical remote-control session to a Windows Vista workstation. This option is appropriate when the target workstation has a compatible VNC server installed, enabled, and reachable from the ASA. The ASA presents the remote session through the clientless SSL VPN portal, allowing the offsite administrator to control the desktop without deploying the full AnyConnect VPN client. Cisco documents RDP and VNC as supported clientless SSL VPN plug-ins for remote-access applications. See Cisco's Clientless SSL VPN configuration guide and the Cisco ASA command reference.