- Expert Verified, Online, **Free**.

Custom View Settings

## Topic 1 - Single Topic

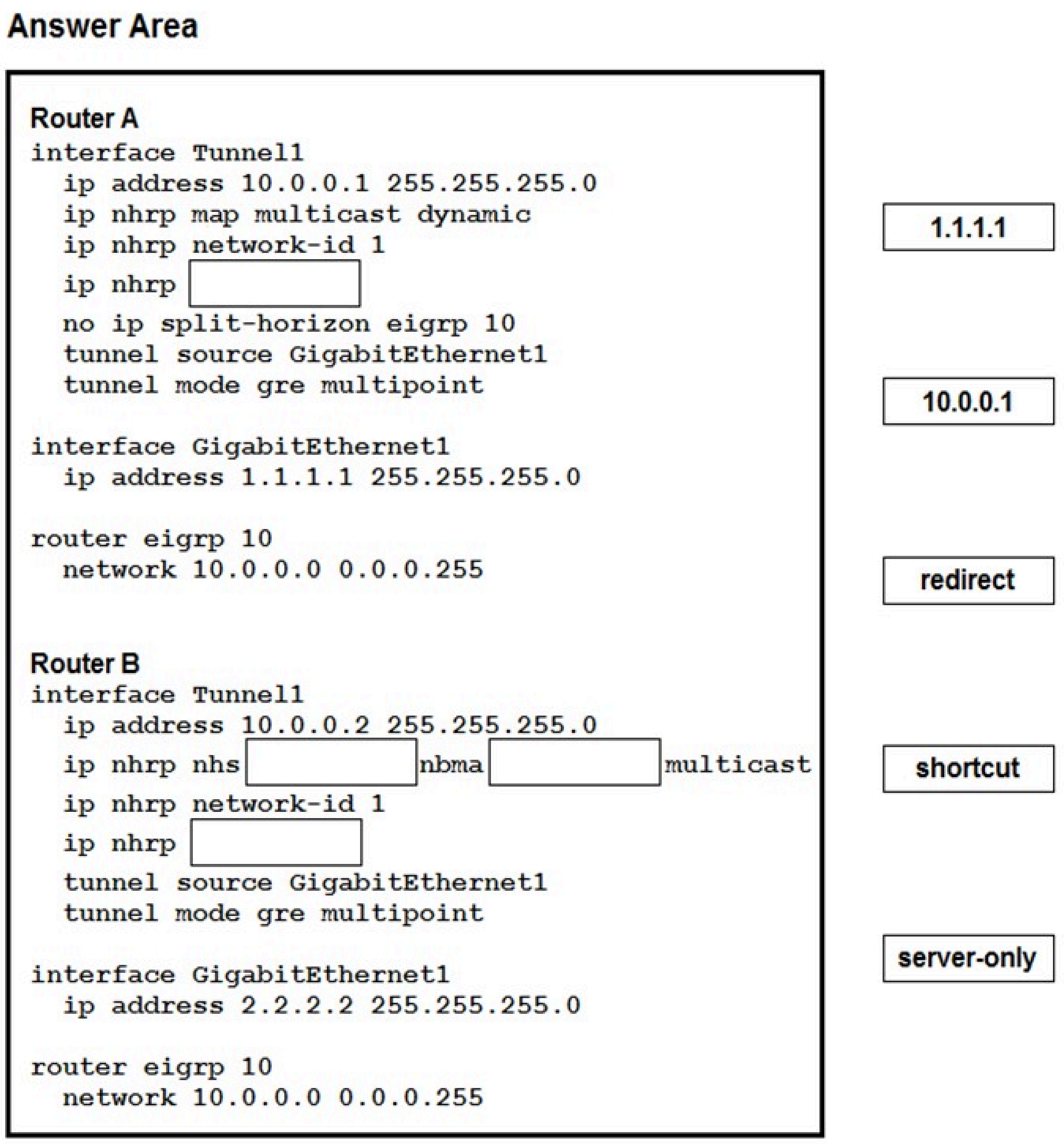
### Question #1

*Topic 1*

DRAG DROP -

Drag and drop the correct commands from the right onto the blanks within the code on the left to implement a design that allow for dynamic spoke-to-spoke communication. Not all commands are used.

Select and Place:



Answer Area

Router A

```
interface Tunnel1
  ip address 10.0.0.1 255.255.255.0
  ip nhrp map multicast dynamic
  ip nhrp network-id 1
  ip nhrp [          ]
  no ip split-horizon eigrp 10
  tunnel source GigabitEthernet1
  tunnel mode gre multipoint

interface GigabitEthernet1
  ip address 1.1.1.1 255.255.255.0

router eigrp 10
  network 10.0.0.0 0.0.0.255
```

Router B

```
interface Tunnel1
  ip address 10.0.0.2 255.255.255.0
  ip nhrp nhs [          ]nbma [          ]multicast
  ip nhrp network-id 1
  ip nhrp [          ]
  tunnel source GigabitEthernet1
  tunnel mode gre multipoint

interface GigabitEthernet1
  ip address 2.2.2.2 255.255.255.0

router eigrp 10
  network 10.0.0.0 0.0.0.255
```

## Question #2 *Topic 1*

A second set of traffic selectors is negotiated between two peers using IKEv2. Which IKEv2 packet will contain details of the exchange?

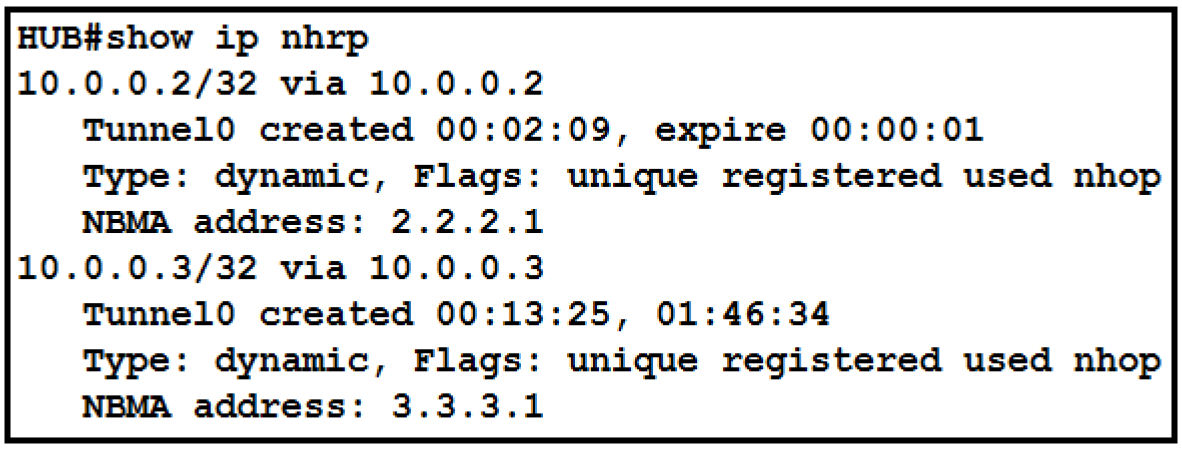
A. IKEv2 IKE_SA_INIT

B. IKEv2 INFORMATIONAL

C. IKEv2 CREATE_CHILD_SA

D. IKEv2 IKE_AUTH

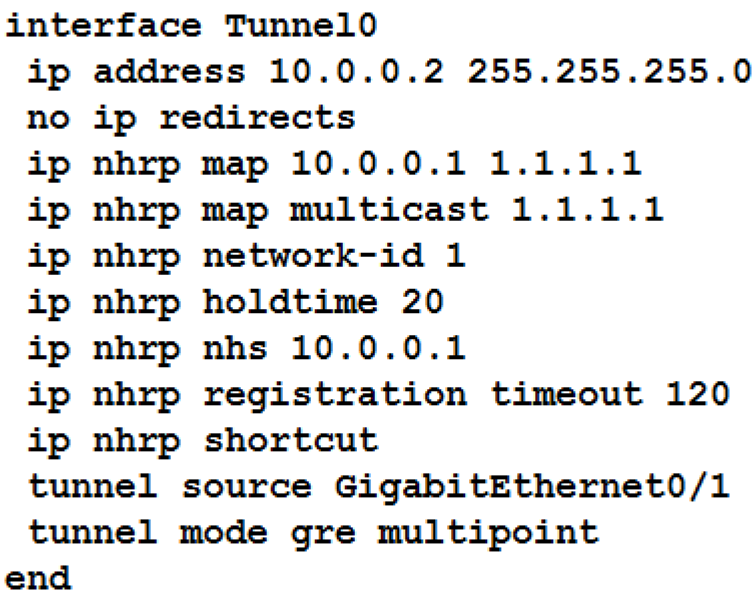
Question #3 *Topic 1*



```
HUB#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel0 created 00:02:09, expire 00:00:01
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 2.2.2.1
10.0.0.3/32 via 10.0.0.3
   Tunnel0 created 00:13:25, 01:46:34
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 3.3.3.1
```

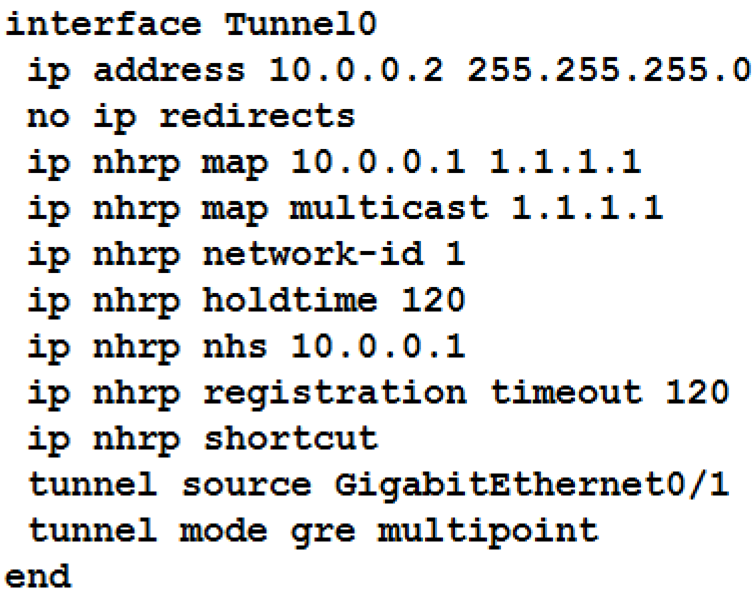
Refer to the exhibit. The DMVPN tunnel is dropping randomly and no tunnel protection is configured. Which spoke configuration mitigates tunnel drops?

A.



```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 20
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

B.



```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

C.

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 20
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

D.

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 150
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

## Question #4 *Topic 1*

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

## Question #5 *Topic 1*

Which statement about GETVPN is true?

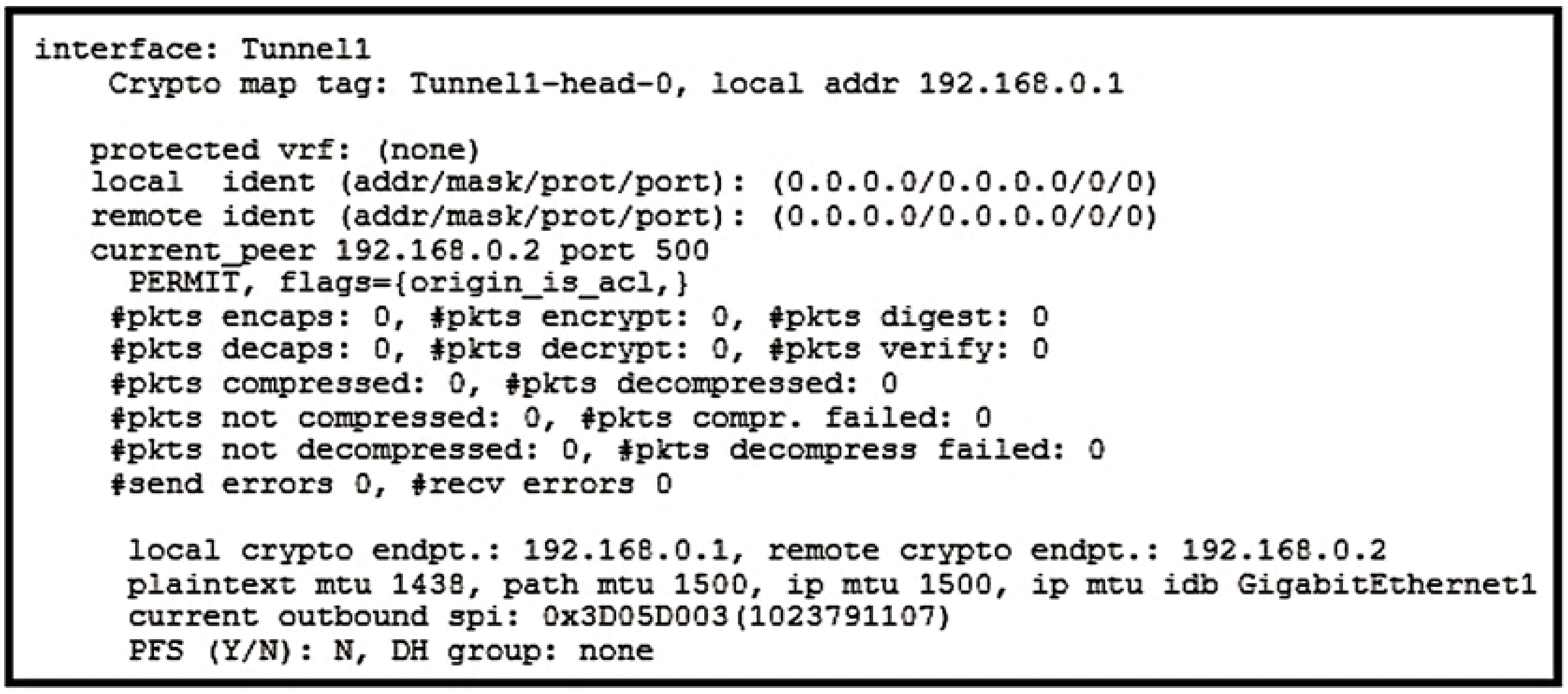
A. The configuration that defines which traffic to encrypt originates from the key server.

B. TEK rekeys can be load-balanced between two key servers operating in COOP.

C. The pseudotime that is used for replay checking is synchronized via NTP.

D. Group members must acknowledge all KEK and TEK rekeys, regardless of configuration.

## Question #6 *Topic 1*



```
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
```

Refer to the exhibit. 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

## Question #7 *Topic 1*

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.

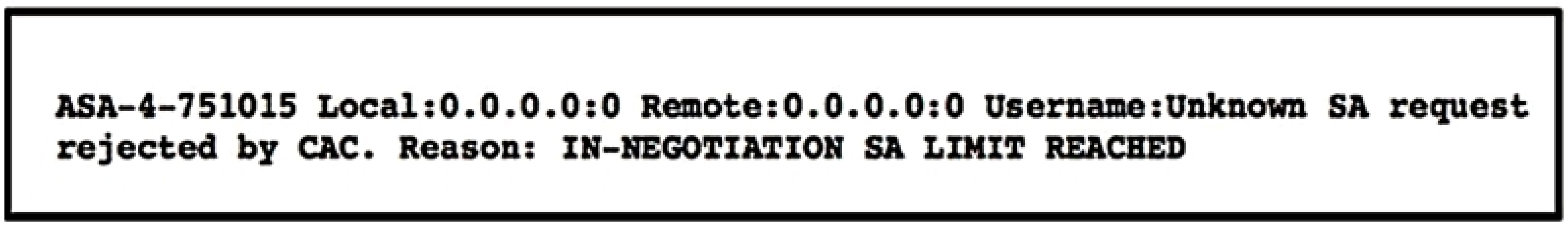
B. Add NHRP redirects on the spoke.

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.

## Question #8 *Topic 1*



```
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
```

Refer to the exhibit. 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.

## Question #9 *Topic 1*

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

## Question #10 *Topic 1*

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

A. policy-based routing

B. CEF

C. reverse route injection

D. route filtering

## Question #11 *Topic 1*

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

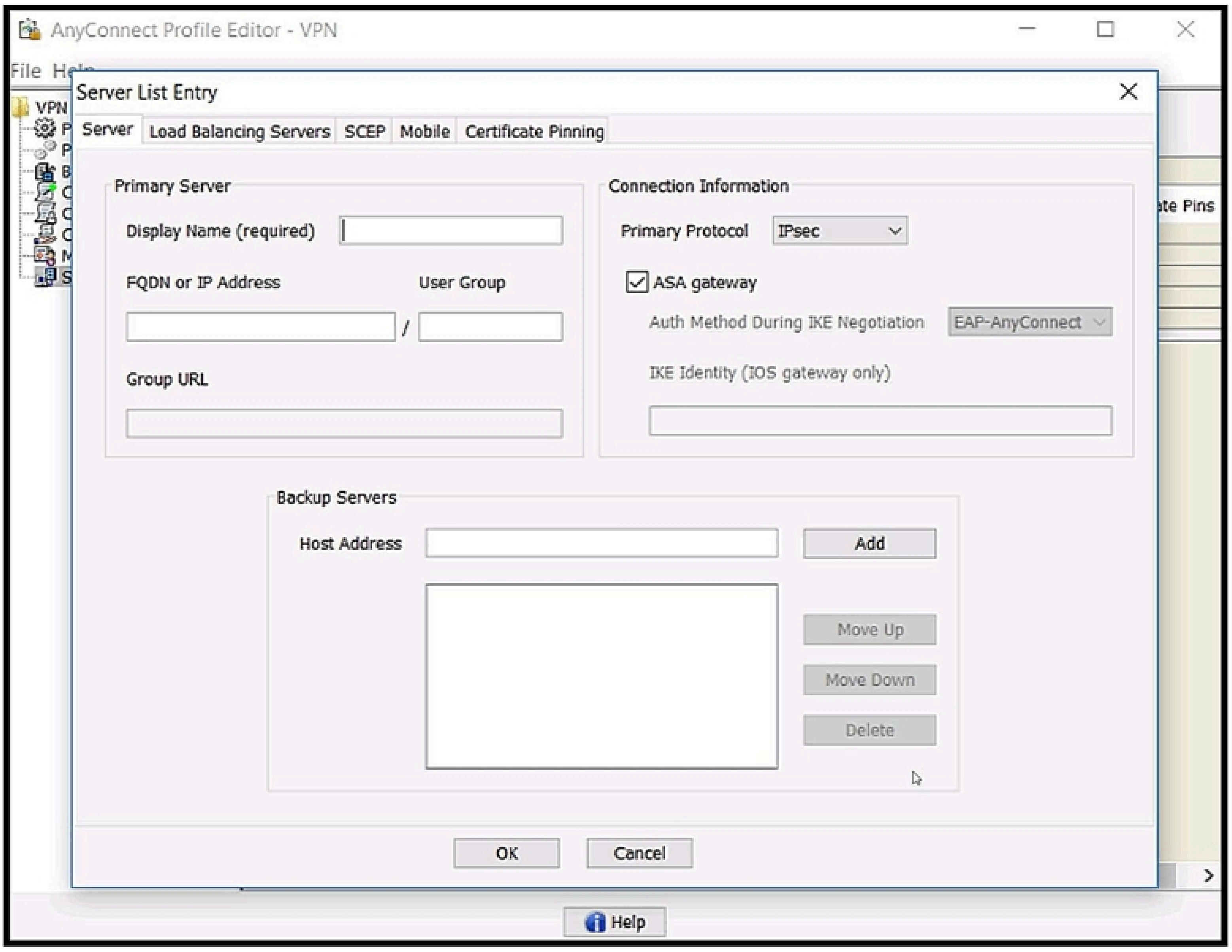
A. svc import profile SSL_profile flash:simos-profile.xml

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

Question #12 Topic 1



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?

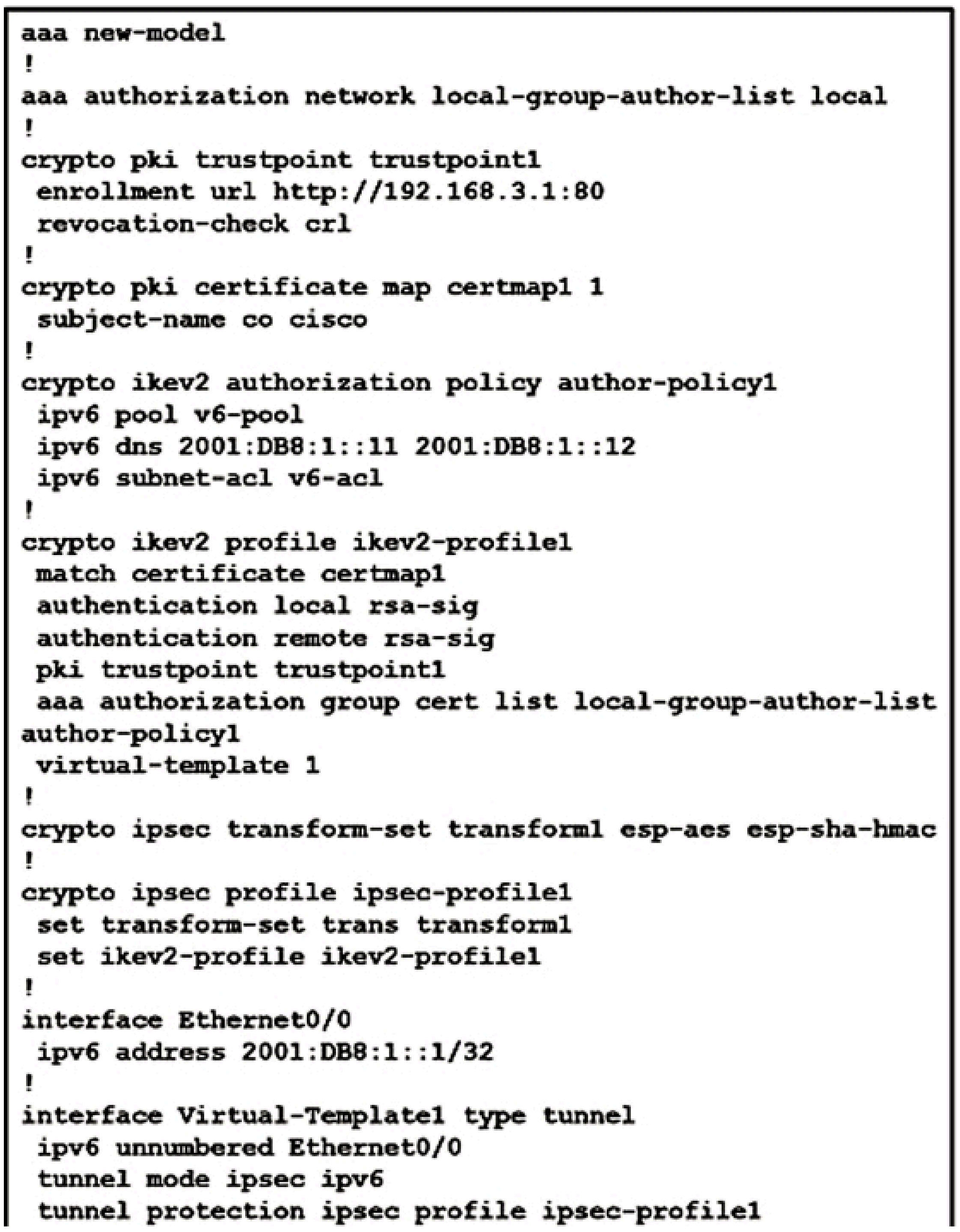
A. address-pool

B. group-alias

C. group-policy

D. tunnel-group

## Question #13 *Topic 1*



```
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
```

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

## Question #14 *Topic 1*

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

## Question #15 *Topic 1*

Which configuration construct must be used in a FlexVPN tunnel?

A. EAP configuration

B. multipoint GRE tunnel interface

C. IKEv1 policy

D. IKEv2 profile

## Question #16 *Topic 1*

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

## Question #17 *Topic 1*

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

## Question #18 *Topic 1*

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.

## Question #19 *Topic 1*

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

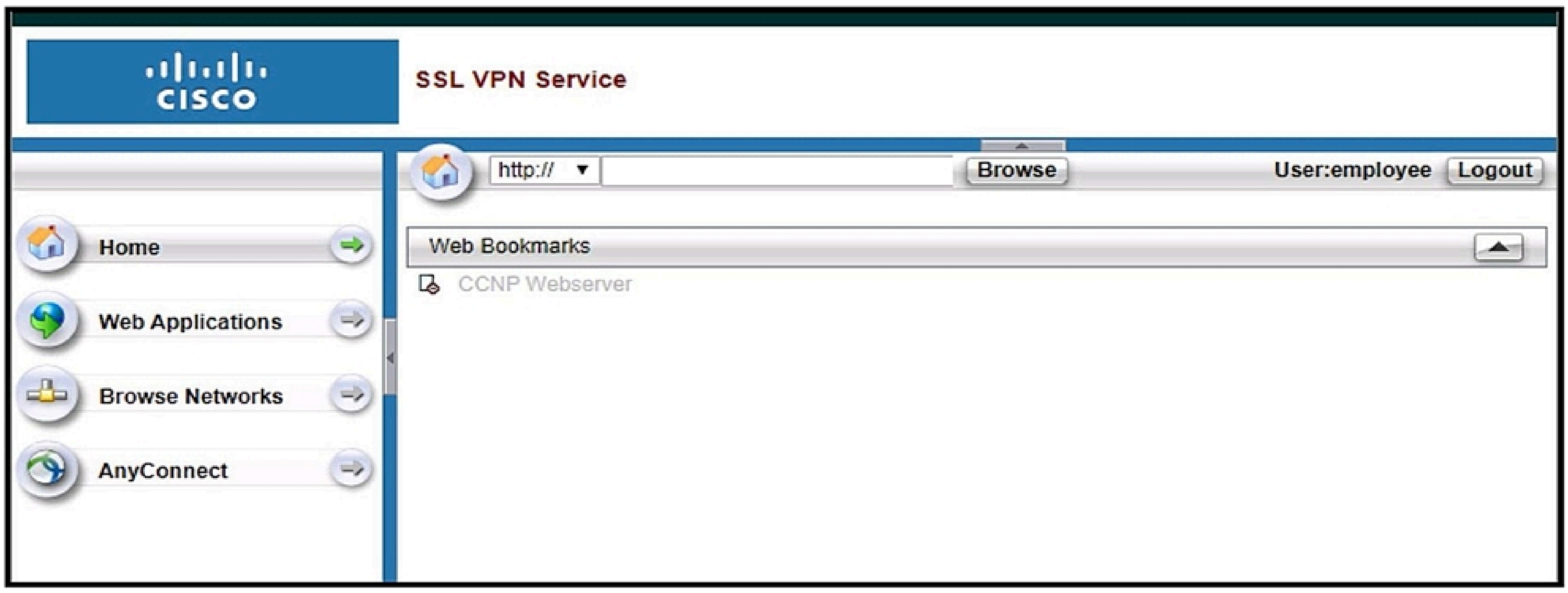
A. tunnel-group (general-attributes)

B. tunnel-group (webvpn-attributes)

C. webvpn (group-policy)

D. webvpn (global configuration)

## Question #20 *Topic 1*



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.

## Question #21 *Topic 1*

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.

Question #22 *Topic 1*

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

Question #23 *Topic 1*

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

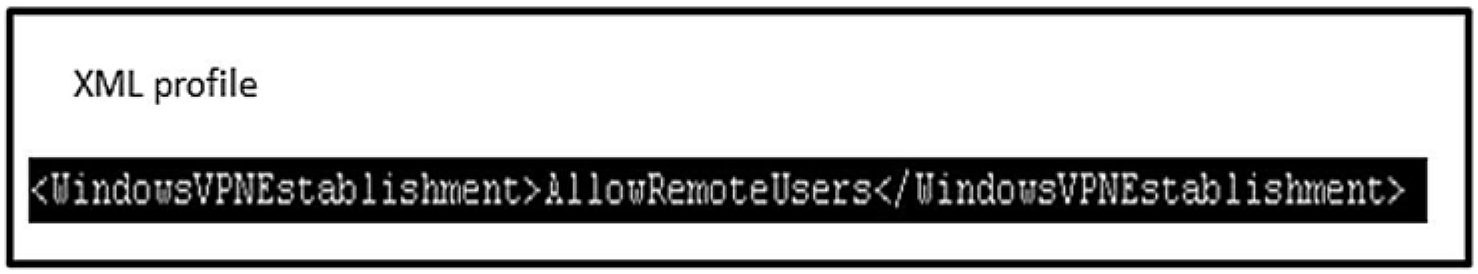
A. auto-upgrade

B. auto-connect

C. auto-start

D. auto-run

Question #24 *Topic 1*

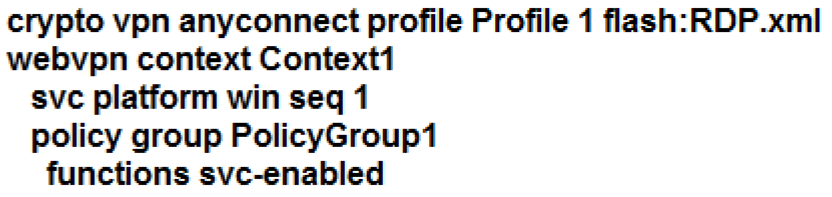


XML profile

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

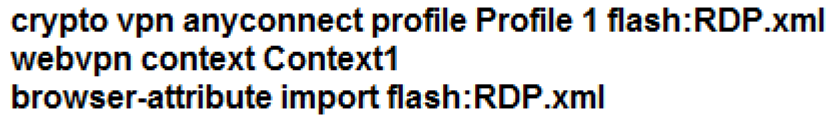
Refer to the exhibit. The customer must launch Cisco AnyConnect in the RDP machine. Which IOS configuration accomplishes this task?

A.



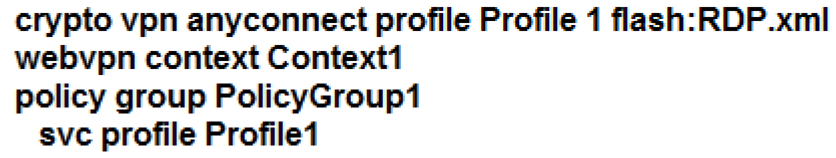
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
  svc platform win seq 1
  policy group PolicyGroup1
   functions svc-enabled
```

B.



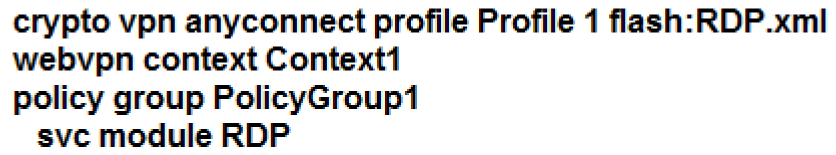
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
browser-attribute import flash:RDP.xml
```

C.



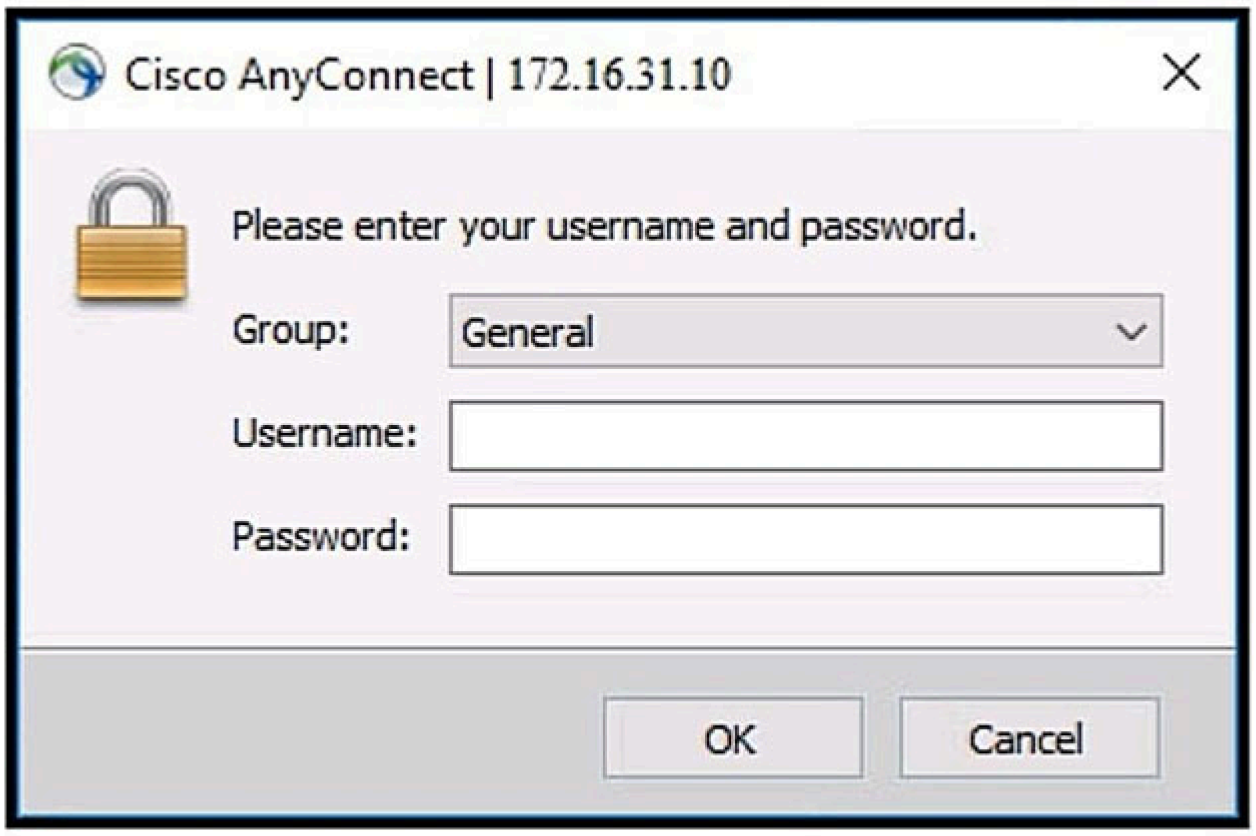
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

D.



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

Question #25 *Topic 1*



Cisco AnyConnect | 172.16.31.10

Please enter your username and password.

Group: General

Username:

Password:

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

Question #26 *Topic 1*

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

Question #27 *Topic 1*

Which IKE identity does an IOS/IOS-XE headend expect to receive if an IPsec Cisco AnyConnect client uses default settings?

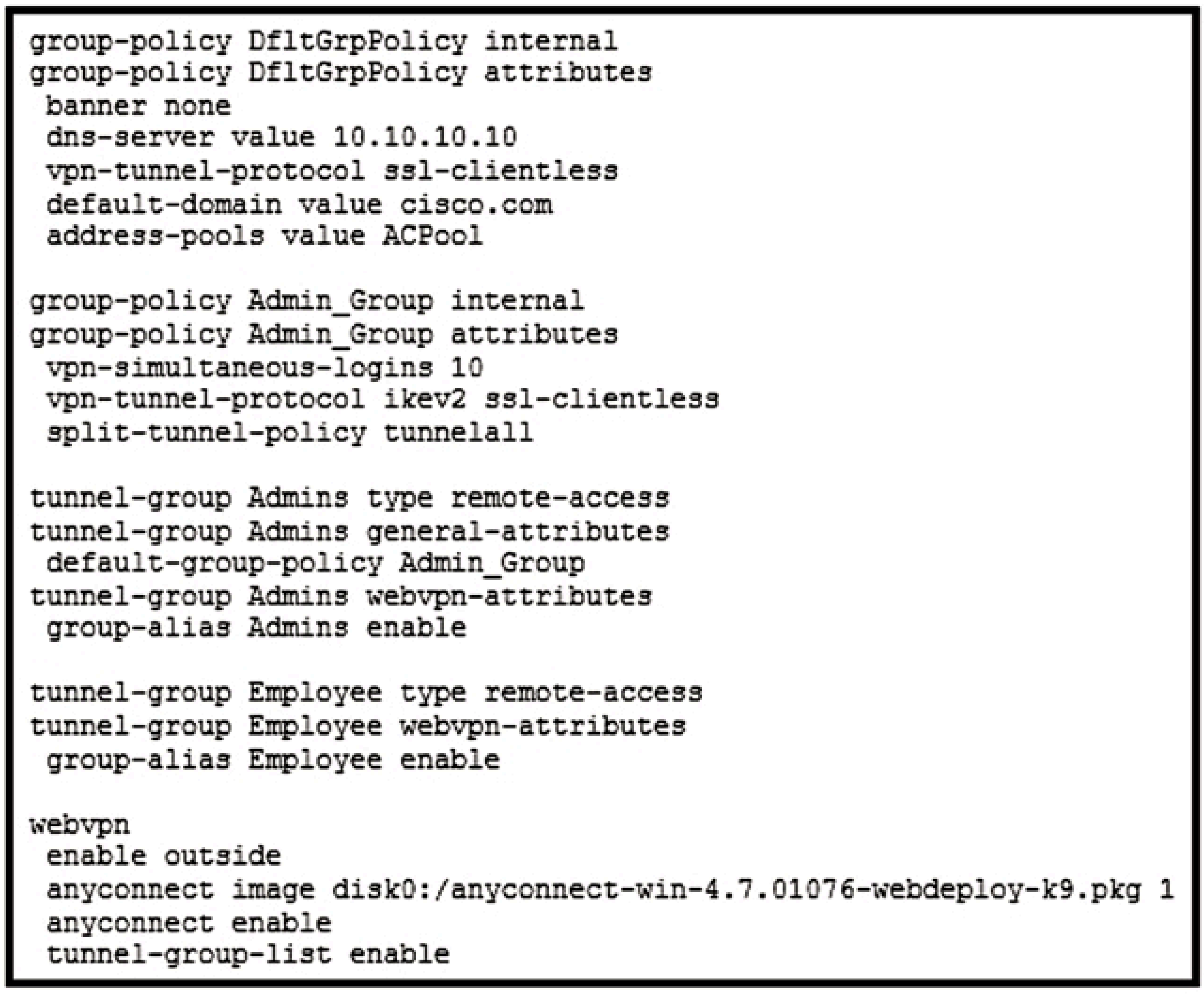
A. *$SecureMobilityClient$*

B. *$AnyConnectClient$*

C. *$RemoteAccessVpnClient$*

D. *$DfltIkeIdentityS*

## Question #28 *Topic 1*



```
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
```

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

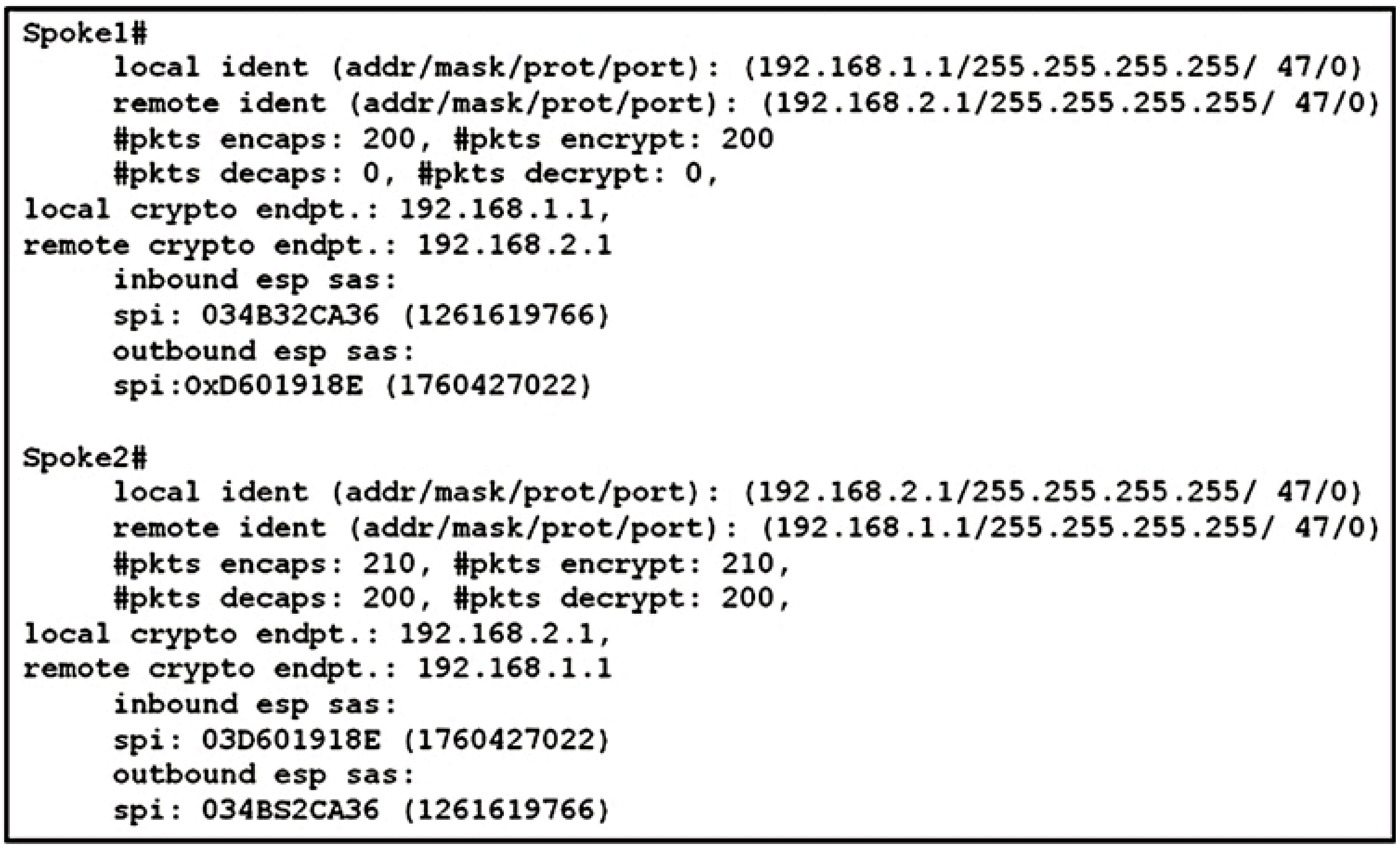
A. SSL AnyConnect

B. IKEv2 AnyConnect

C. crypto map

D. clientless

## Question #29 *Topic 1*



```
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: 034BS2CA36 (1261619766)
```

Refer to the exhibit. 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

## Question #30 *Topic 1*

Which command is used to troubleshoot an IPv6 FlexVPN spoke-to-hub connectivity failure?

A. show crypto ikev2 sa

B. show crypto isakmp sa

C. show crypto gkm

D. show crypto identity

## Question #31 *Topic 1*

In a FlexVPN deployment, the spokes successfully connect to the hub, but spoke-to-spoke tunnels do not form. Which troubleshooting step solves the issue?

A. Verify the spoke configuration to check if the NHRP redirect is enabled.

B. Verify that the spoke receives redirect messages and sends resolution requests.

C. Verify the hub configuration to check if the NHRP shortcut is enabled.

D. Verify that the tunnel interface is contained within a VRF.

## Question #32 *Topic 1*

An engineer is troubleshooting a new DMVPN setup on a Cisco IOS router. After the show crypto isakmp sa command is issued, a response is returned of
"MM_NO_STATE." Why does this failure occur?

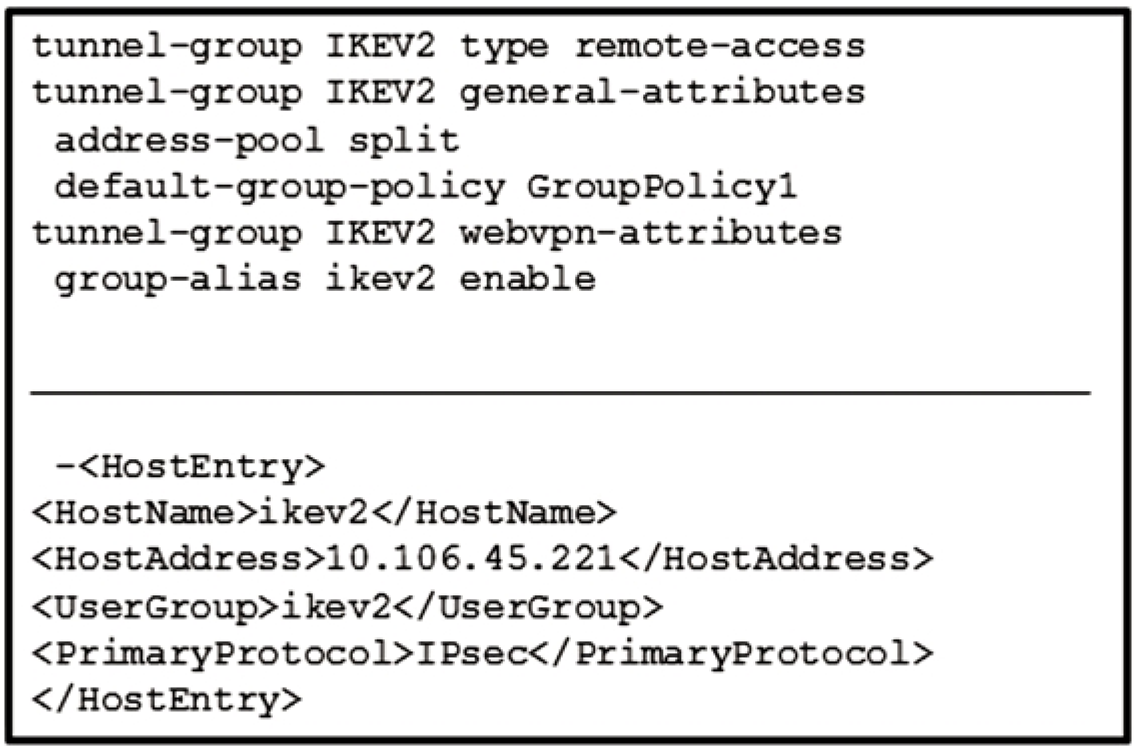
A. The ISAKMP policy priority values are invalid.

B. ESP traffic is being dropped.

C. The Phase 1 policy does not match on both devices.

D. Tunnel protection is not applied to the DMVPN tunnel.

## Question #33 *Topic 1*



```
tunnel-group IKEV2 type remote-access
tunnel-group IKEV2 general-attributes
 address-pool split
 default-group-policy GroupPolicy1
tunnel-group IKEV2 webvpn-attributes
 group-alias ikev2 enable

 -<HostEntry>
<HostName>ikev2</HostName>
<HostAddress>10.106.45.221</HostAddress>
<UserGroup>ikev2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```

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.

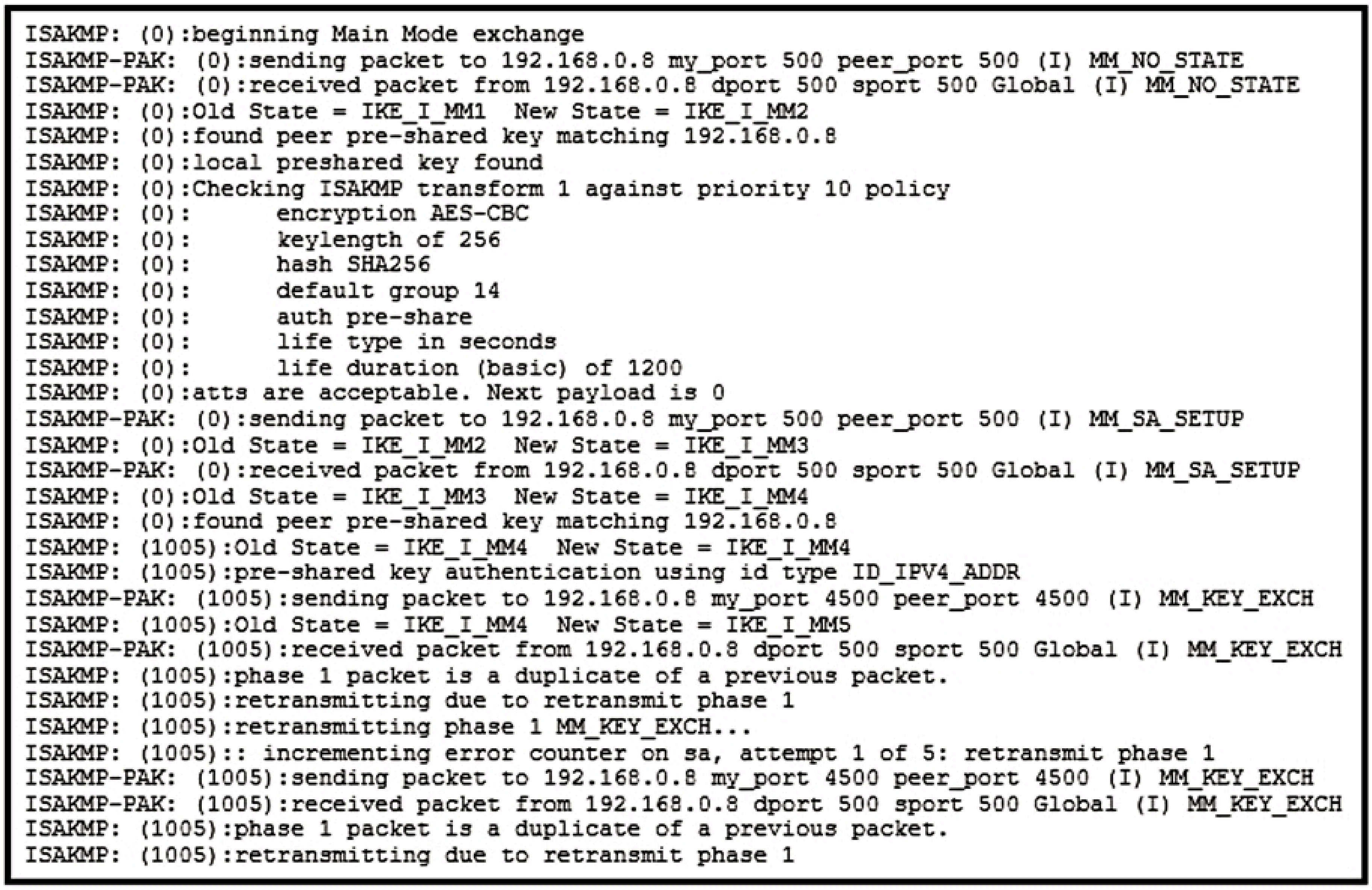
B. The IP address is incorrect.

C. Primary protocol should be SSL.

D. UserGroup must match connection profile.

## Question #34

*Topic 1*



```
ISAKMP: (0):beginning Main Mode exchange
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (0):local preshared key found
ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: (0):      encryption AES-CBC
ISAKMP: (0):      keylength of 256
ISAKMP: (0):      hash SHA256
ISAKMP: (0):      default group 14
ISAKMP: (0):      auth pre-share
ISAKMP: (0):      life type in seconds
ISAKMP: (0):      life duration (basic) of 1200
ISAKMP: (0):atts are acceptable. Next payload is 0
ISAKMP-PAK: (0):sending packet to 192.168.0.8 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP-PAK: (0):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP: (0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP: (0):found peer pre-shared key matching 192.168.0.8
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM4
ISAKMP: (1005):pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP: (1005):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
ISAKMP: (1005):retransmitting phase 1 MM_KEY_EXCH...
ISAKMP: (1005):: incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
ISAKMP-PAK: (1005):sending packet to 192.168.0.8 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
ISAKMP-PAK: (1005):received packet from 192.168.0.8 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1005):phase 1 packet is a duplicate of a previous packet.
ISAKMP: (1005):retransmitting due to retransmit phase 1
```

Refer to the exhibit. A site-to-site tunnel between two sites is not coming up. Based on the debugs, what is the cause of this issue?

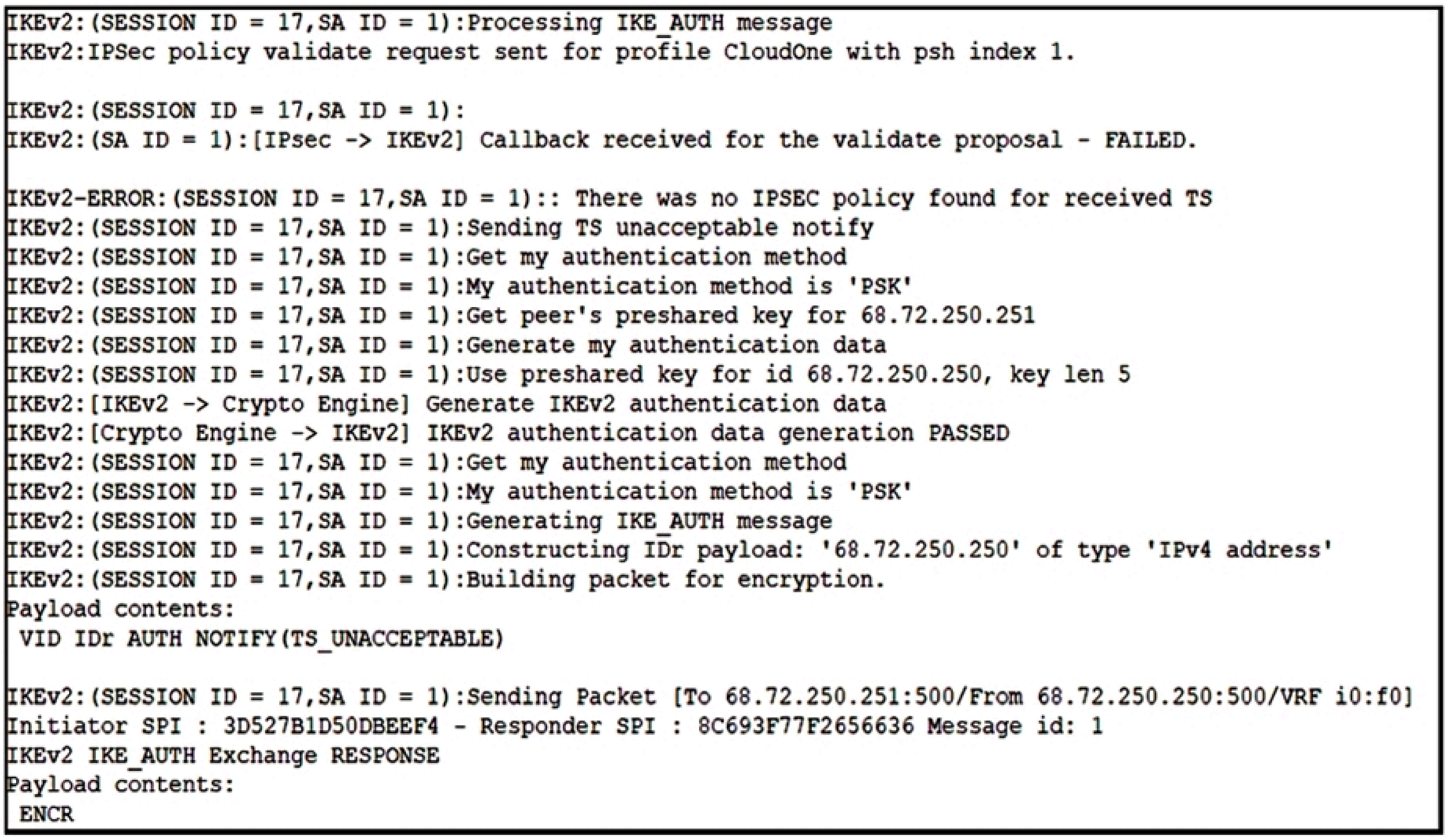
A. An authentication failure occurs on the remote peer.

B. A certificate fragmentation issue occurs between both sides.

C. UDP 4500 traffic from the peer does not reach the router.

D. An authentication failure occurs on the router.

Question #35 Topic 1



```
IKEv2:(SESSION ID = 17,SA ID = 1):Processing IKE_AUTH message
IKEv2:IPSec policy validate request sent for profile CloudOne with psh index 1.

IKEv2:(SESSION ID = 17,SA ID = 1):
IKEv2:(SA ID = 1):[IPsec -> IKEv2] Callback received for the validate proposal - FAILED.

IKEv2-ERROR:(SESSION ID = 17,SA ID = 1):: There was no IPSEC policy found for received TS
IKEv2:(SESSION ID = 17,SA ID = 1):Sending TS unacceptable notify
IKEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
IKEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
IKEv2:(SESSION ID = 17,SA ID = 1):Get peer's preshared key for 68.72.250.251
IKEv2:(SESSION ID = 17,SA ID = 1):Generate my authentication data
IKEv2:(SESSION ID = 17,SA ID = 1):Use preshared key for id 68.72.250.250, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SESSION ID = 17,SA ID = 1):Get my authentication method
IKEv2:(SESSION ID = 17,SA ID = 1):My authentication method is 'PSK'
IKEv2:(SESSION ID = 17,SA ID = 1):Generating IKE_AUTH message
IKEv2:(SESSION ID = 17,SA ID = 1):Constructing IDr payload: '68.72.250.250' of type 'IPv4 address'
IKEv2:(SESSION ID = 17,SA ID = 1):Building packet for encryption.
Payload contents:
 VID IDr AUTH NOTIFY(TS_UNACCEPTABLE)

IKEv2:(SESSION ID = 17,SA ID = 1):Sending Packet [To 68.72.250.251:500/From 68.72.250.250:500/VRF i0:f0]
Initiator SPI : 3D527B1D50DBEEF4 - Responder SPI : 8C693F77F2656636 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 ENCR
```

Refer to the exhibit. Based on the debug output, which type of mismatch is preventing the VPN from coming up?

A. interesting traffic

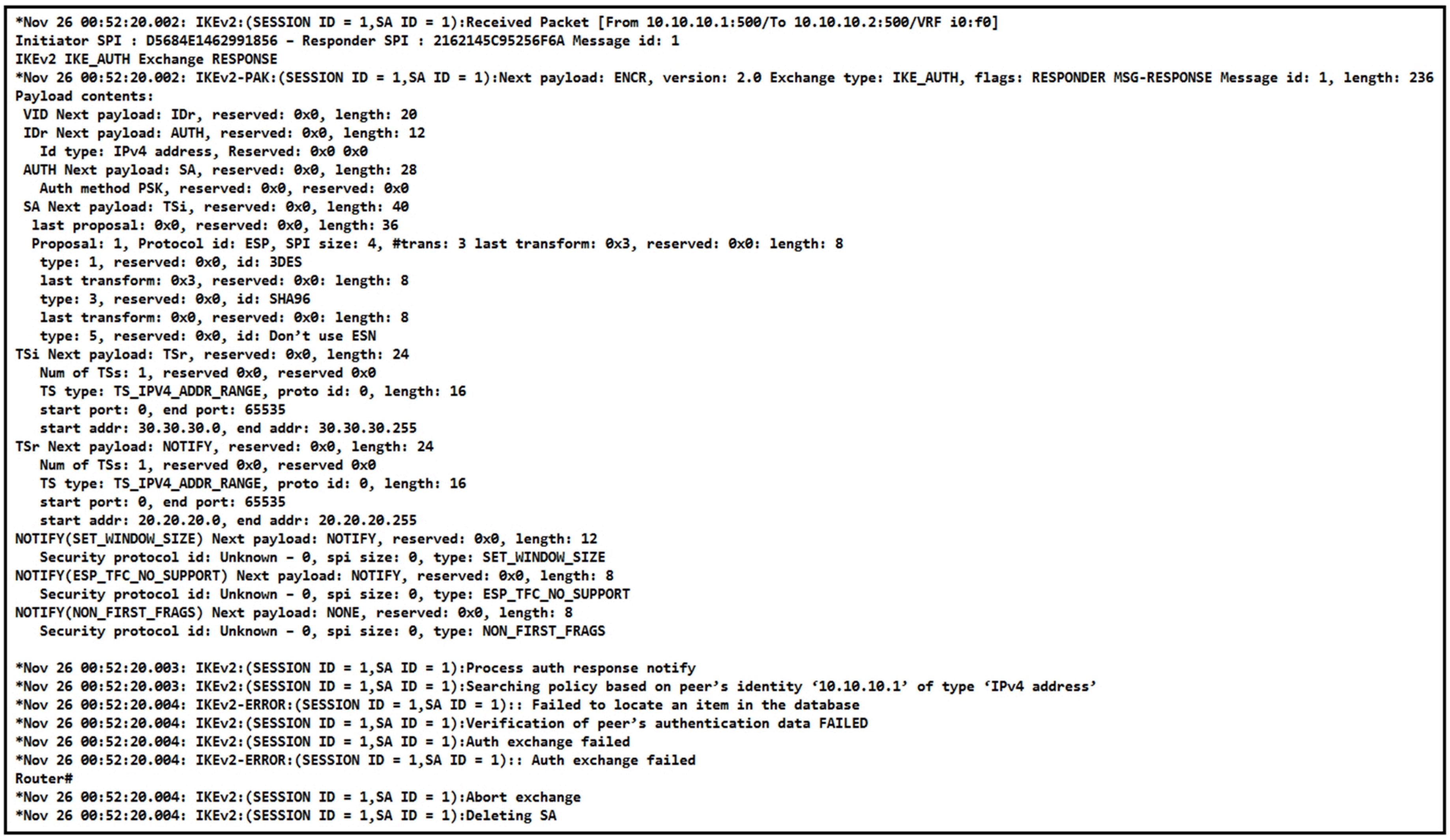
B. lifetime

C. preshared key

D. PFS

## Question #36

*Topic 1*



```
*Nov 26 00:52:20.002: IKEv2:(SESSION ID = 1,SA ID = 1):Received Packet [From 10.10.10.1:500/To 10.10.10.2:500/VRF i0:f0]
Initiator SPI : D5684E1462991856 - Responder SPI : 2162145C95256F6A Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
*Nov 26 00:52:20.002: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 236
Payload contents:
 VID Next payload: IDr, reserved: 0x0, length: 20
 IDr Next payload: AUTH, reserved: 0x0, length: 12
   Id type: IPv4 address, Reserved: 0x0 0x0
 AUTH Next payload: SA, reserved: 0x0, length: 28
   Auth method PSK, reserved: 0x0, reserved: 0x0
 SA Next payload: TSi, reserved: 0x0, length: 40
  last proposal: 0x0, reserved: 0x0, length: 36
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8
   type: 1, reserved: 0x0, id: 3DES
   last transform: 0x3, reserved: 0x0: length: 8
   type: 3, reserved: 0x0, id: SHA96
   last transform: 0x0, reserved: 0x0: length: 8
   type: 5, reserved: 0x0, id: Don't use ESN
TSi Next payload: TSr, reserved: 0x0, length: 24
   Num of TSs: 1, reserved 0x0, reserved 0x0
   TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
   start port: 0, end port: 65535
   start addr: 30.30.30.0, end addr: 30.30.30.255
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
   Num of TSs: 1, reserved 0x0, reserved 0x0
   TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
   start port: 0, end port: 65535
   start addr: 20.20.20.0, end addr: 20.20.20.255
NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
   Security protocol id: Unknown - 0, spi size: 0, type: SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: NON_FIRST_FRAGS

*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Process auth response notify
*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Searching policy based on peer's identity '10.10.10.1' of type 'IPv4 address'
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Failed to locate an item in the database
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Verification of peer's authentication data FAILED
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Auth exchange failed
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Router#
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Abort exchange
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA
```

Refer to the exhibit. The IKEv2 site-to-site VPN tunnel between two routers is down. Based on the debug output, which type of mismatch is the problem?

A. preshared key

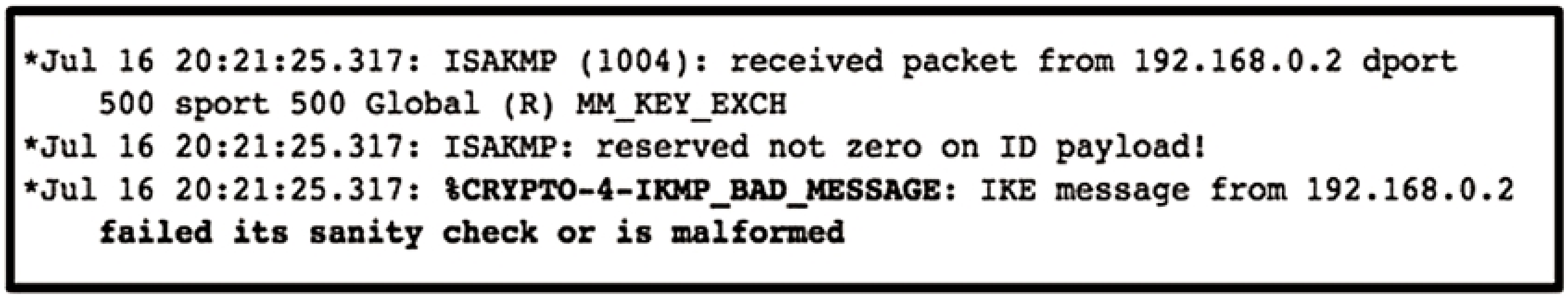
B. peer identity

C. transform set

D. ikev2 proposal

## Question #37

*Topic 1*



```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
    500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
    failed its sanity check or is malformed
```

Refer to the exhibit. Which type of mismatch is causing the problem with the IPsec VPN tunnel?

A. crypto access list

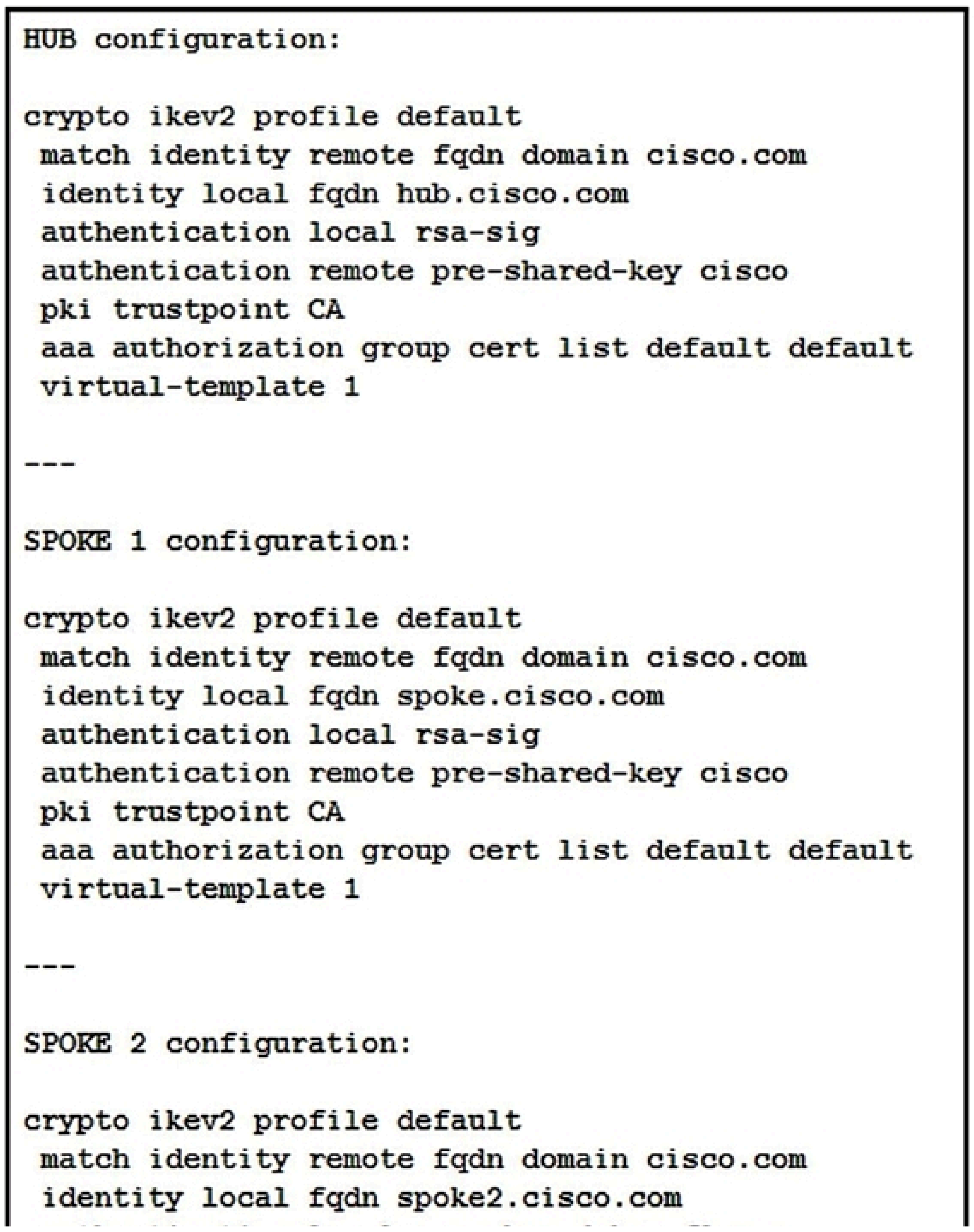
B. Phase 1 policy

C. transform set

D. preshared key

## Question #38

*Topic 1*



```
HUB configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 1 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 2 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
```

Refer to the exhibit. What is a result of this configuration?

A. Spoke 1 fails the authentication because the authentication methods are incorrect.

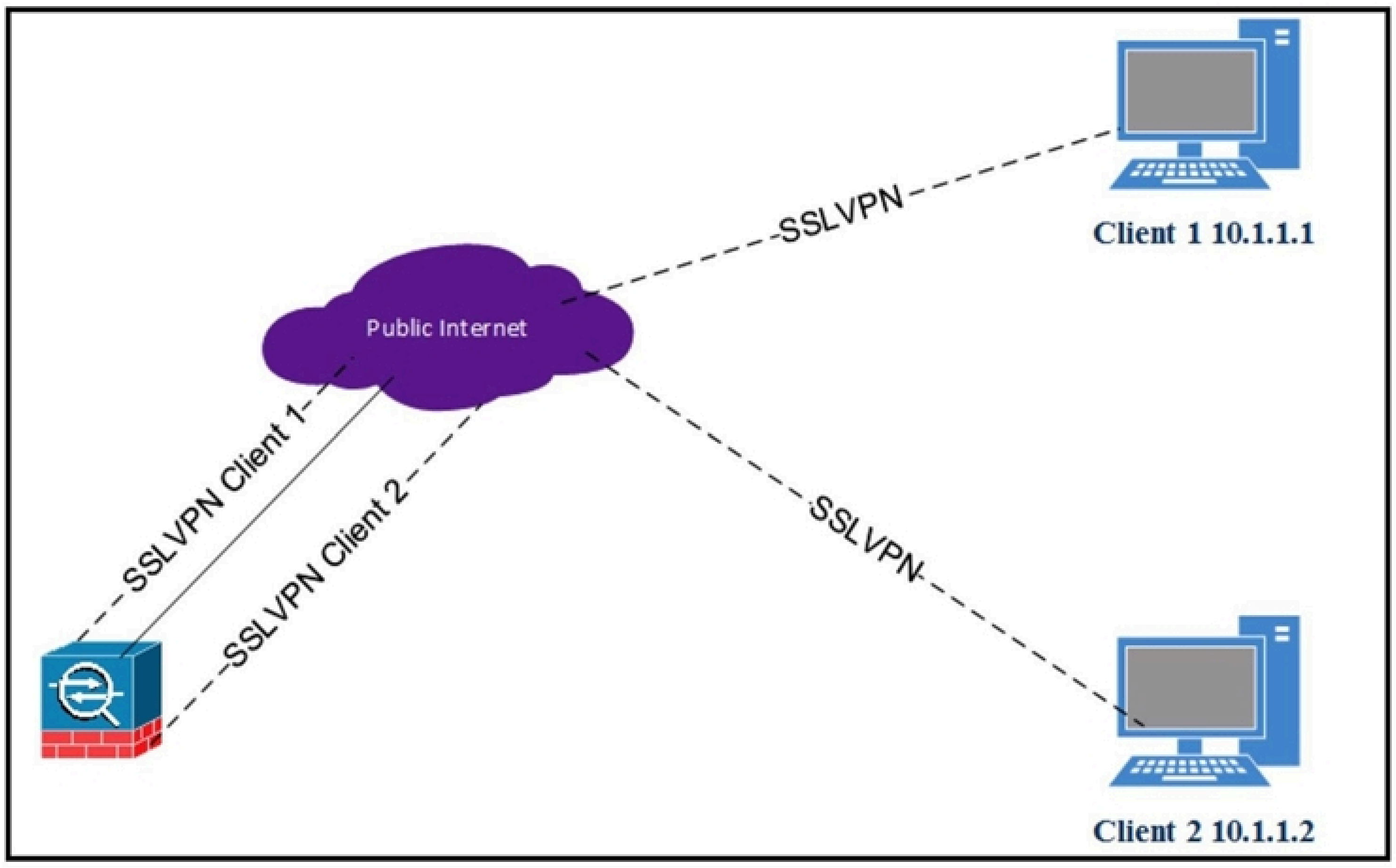
B. Spoke 2 passes the authentication to the hub and successfully proceeds to phase 2.

C. Spoke 2 fails the authentication because the remote authentication method is incorrect.

D. Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Question #39

*Topic 1*



Refer to the exhibit. Client 1 cannot communicate with client 2. Both clients are using Cisco AnyConnect and have established a successful SSL VPN connection to the hub ASA. Which command on the ASA is missing?

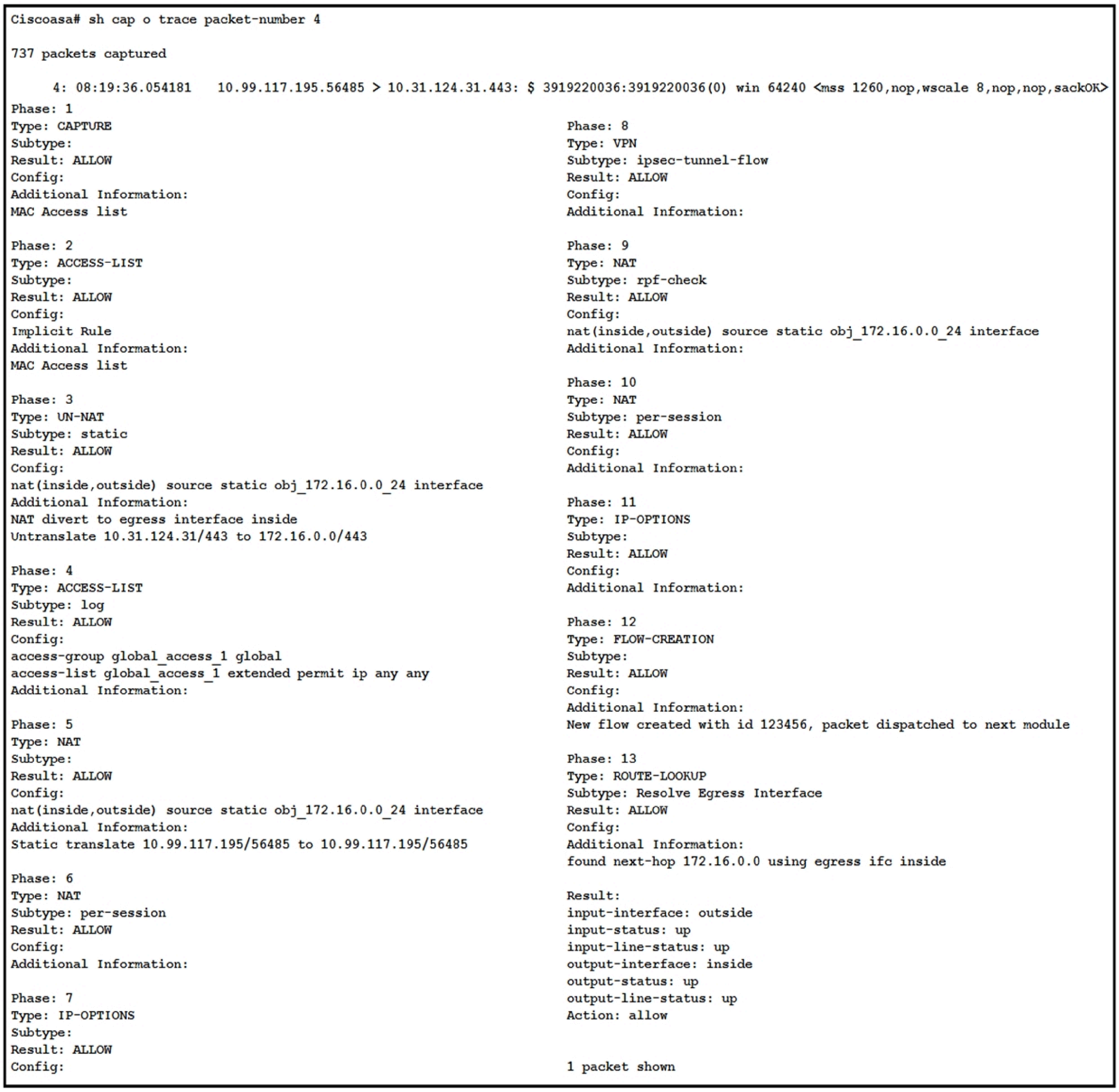
A. dns-server value 10.1.1.2

B. same-security-traffic permit intra-interface

C. same-security-traffic permit inter-interface

D. dns-server value 10.1.1.3

Question #40 *Topic 1*



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

737 packets captured

     4: 08:19:36.054181   10.99.117.195.56485 > 10.31.124.31.443: $ 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

## Question #41 *Topic 1*

Which redundancy protocol must be implemented for IPsec stateless failover to work?

A. SSO

B. GLBP

C. HSRP

D. VRRP

## Question #42 *Topic 1*

Which technology works with IPsec stateful failover?

A. GLBP

B. HSRP

C. GRE

D. VRRP

## Question #43 *Topic 1*

What are two functions of ECDH and ECDSA? (Choose two.)

A. nonrepudiation

B. revocation

C. digital signature

D. key exchange

E. encryption

## Question #44 *Topic 1*

What uses an Elliptic Curve key exchange algorithm?

A. ECDSA

B. ECDHE

C. AES-GCM

D. SHA

## Question #45 *Topic 1*

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

A. FlexVPN

B. clientless

C. EZVPN

D. L2TP

E. Cisco AnyConnect

## Question #46 *Topic 1*

Which VPN solution uses TBAR?

A. GETVPN

B. VTI

C. DMVPN

D. Cisco AnyConnect

## Question #47 *Topic 1*

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

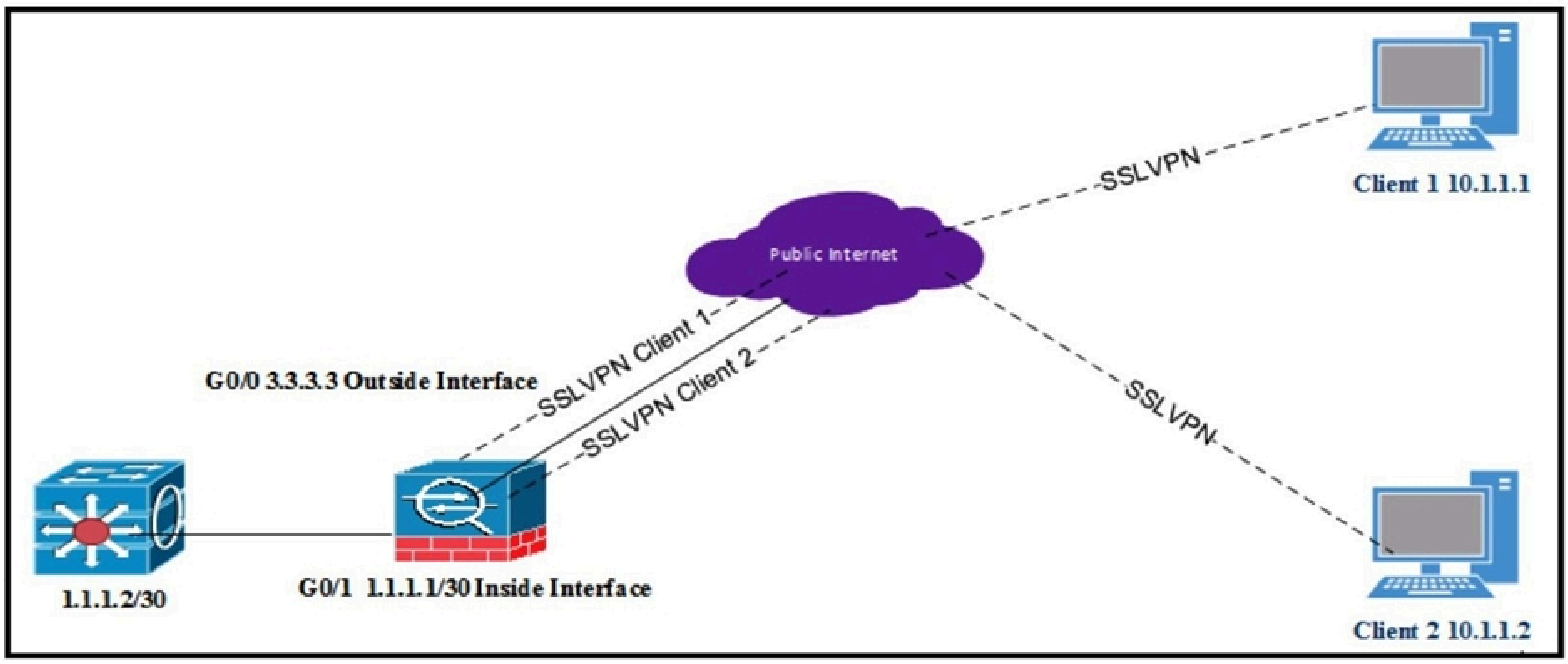
B. show ip traffic

C. show crypto ipsec sa

D. show ip nhrp traffic

E. show dmvpn detail

## Question #48 *Topic 1*



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

## Question #49 *Topic 1*

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

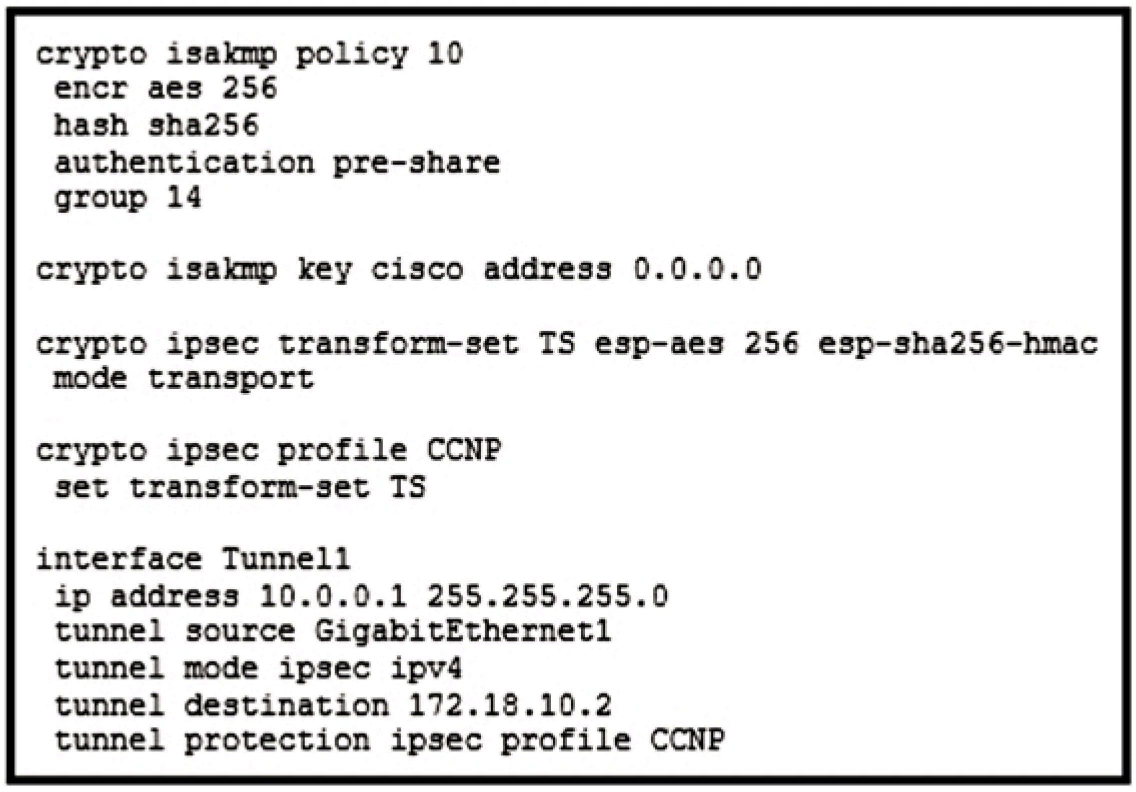
A. SSL/TLS

B. L2TP

C. DTLS

D. IPsec IKEv1

## Question #50 *Topic 1*



```
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
```

Refer to the exhibit. Which VPN technology is used in the exhibit?

A. DVTI

B. VTI

C. DMVPN

D. GRE

## Question #51 *Topic 1*

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

## Question #52 *Topic 1*

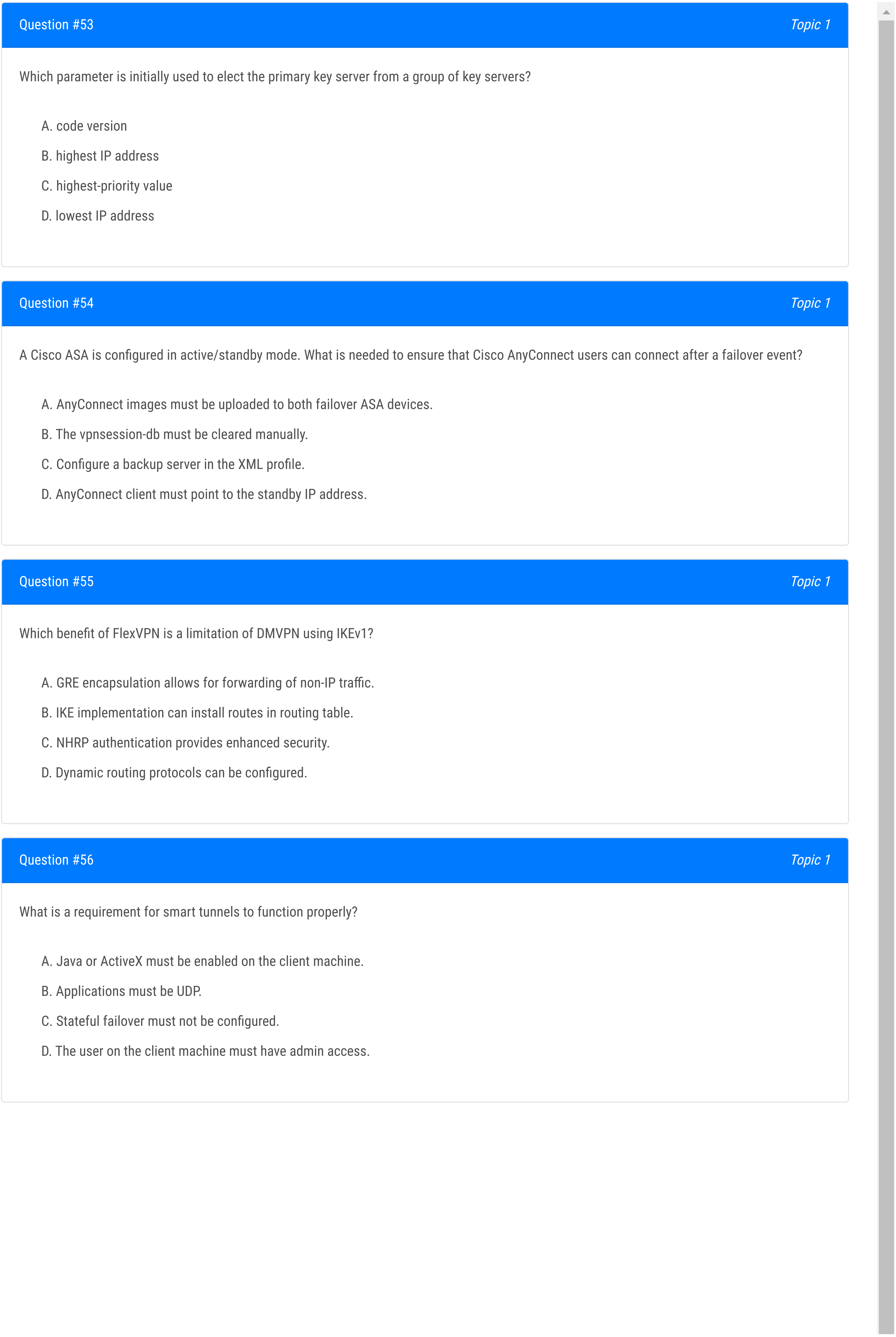
Which parameter must match on all routers in a DMVPN Phase 3 cloud?

A. GRE tunnel key

B. NHRP network ID

C. tunnel VRF

D. EIGRP split-horizon setting



Question #53 *Topic 1*

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

Question #54 *Topic 1*

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.

Question #55 *Topic 1*

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.

Question #56 *Topic 1*

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.

## Question #57 *Topic 1*

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

## Question #58 *Topic 1*

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

## Question #59 *Topic 1*

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

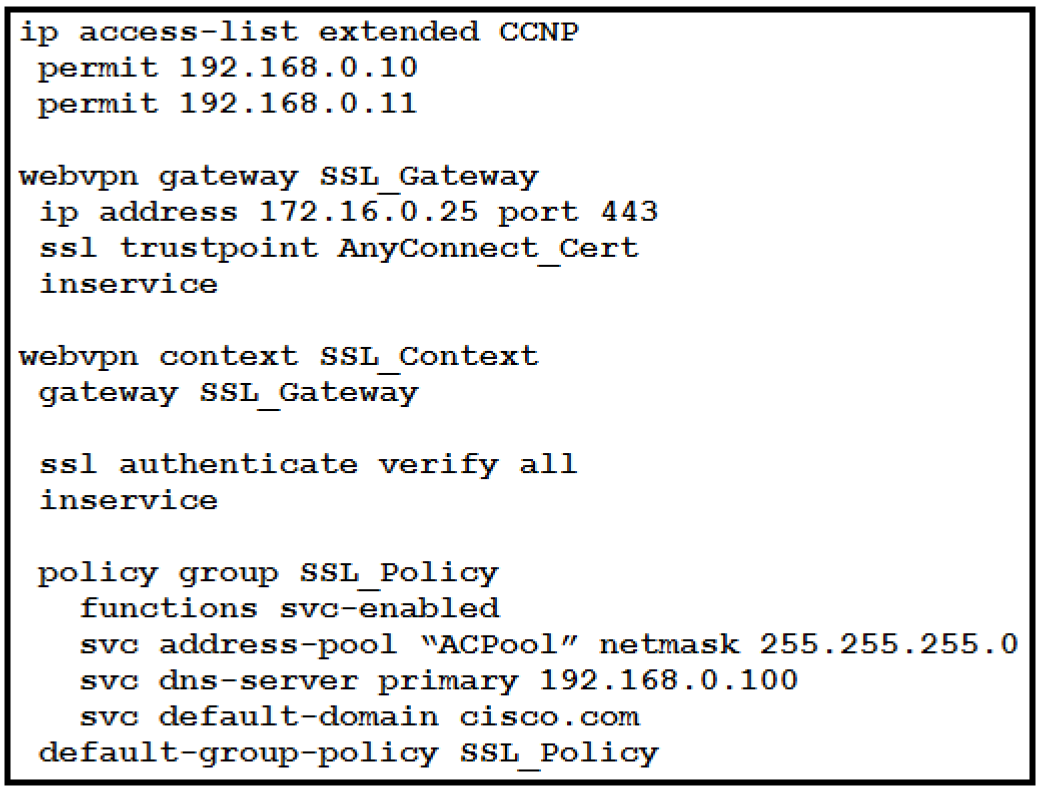
A. sequence numbers that enable scalable replay checking

B. enabled use of ESP or AH

C. design for use over public or private WAN

D. no requirement for an overlay routing protocol

## Question #60 *Topic 1*



```
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
```

Refer to the exhibit. 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

## Question #61 *Topic 1*

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

## Question #62 *Topic 1*

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.

## Question #63 *Topic 1*

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

## Question #64 *Topic 1*

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

## Question #65 *Topic 1*

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?

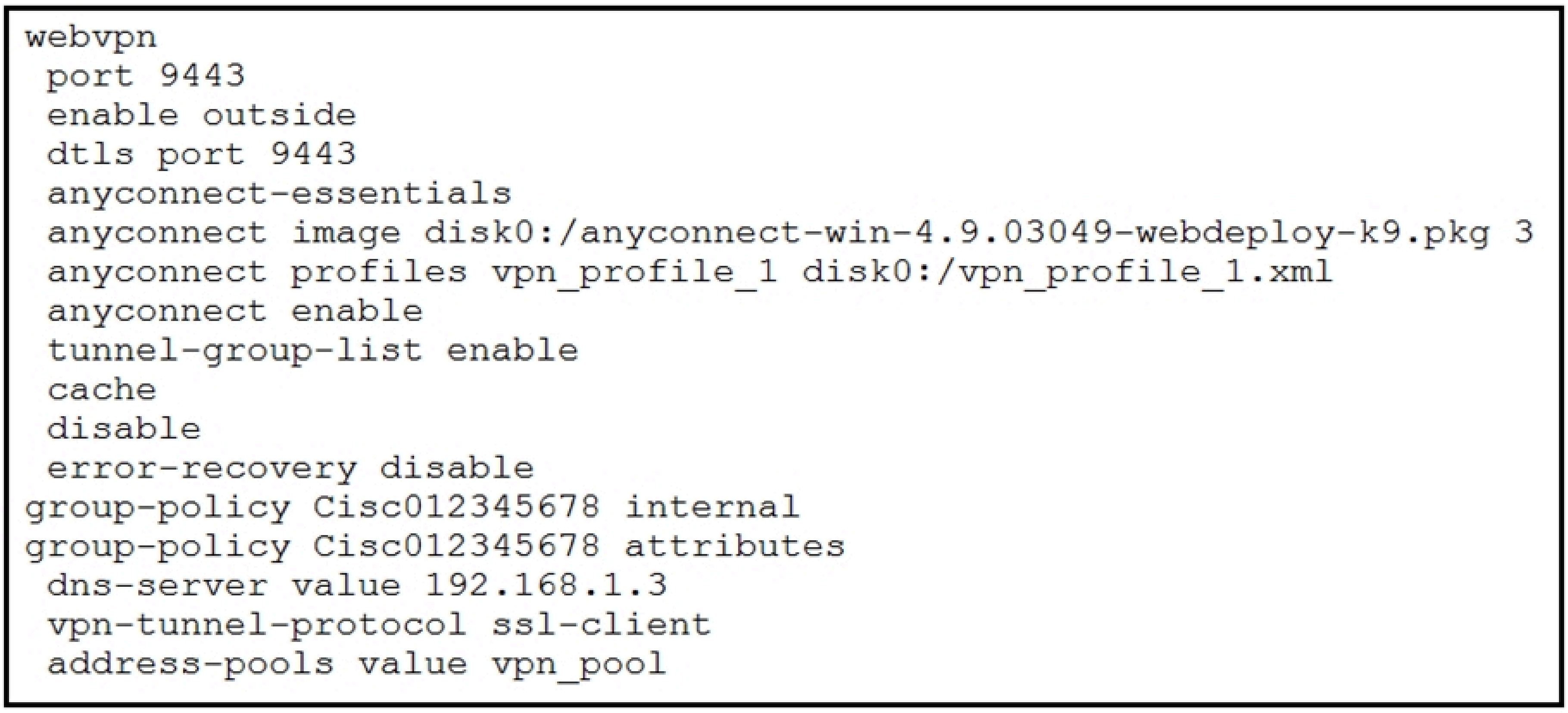
A. IKEv2 AnyConnect

B. Clientless

C. Port forwarding

D. SSL AnyConnect

## Question #66 *Topic 1*



```
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
```

Refer to the exhibit. Which type of Cisco VPN is shown for group Cisc012345678?

A. Cisco AnyConnect Client VPN

B. DMVPN

C. Clientless SSLVPN

D. GETVPN

## Question #67 *Topic 1*

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

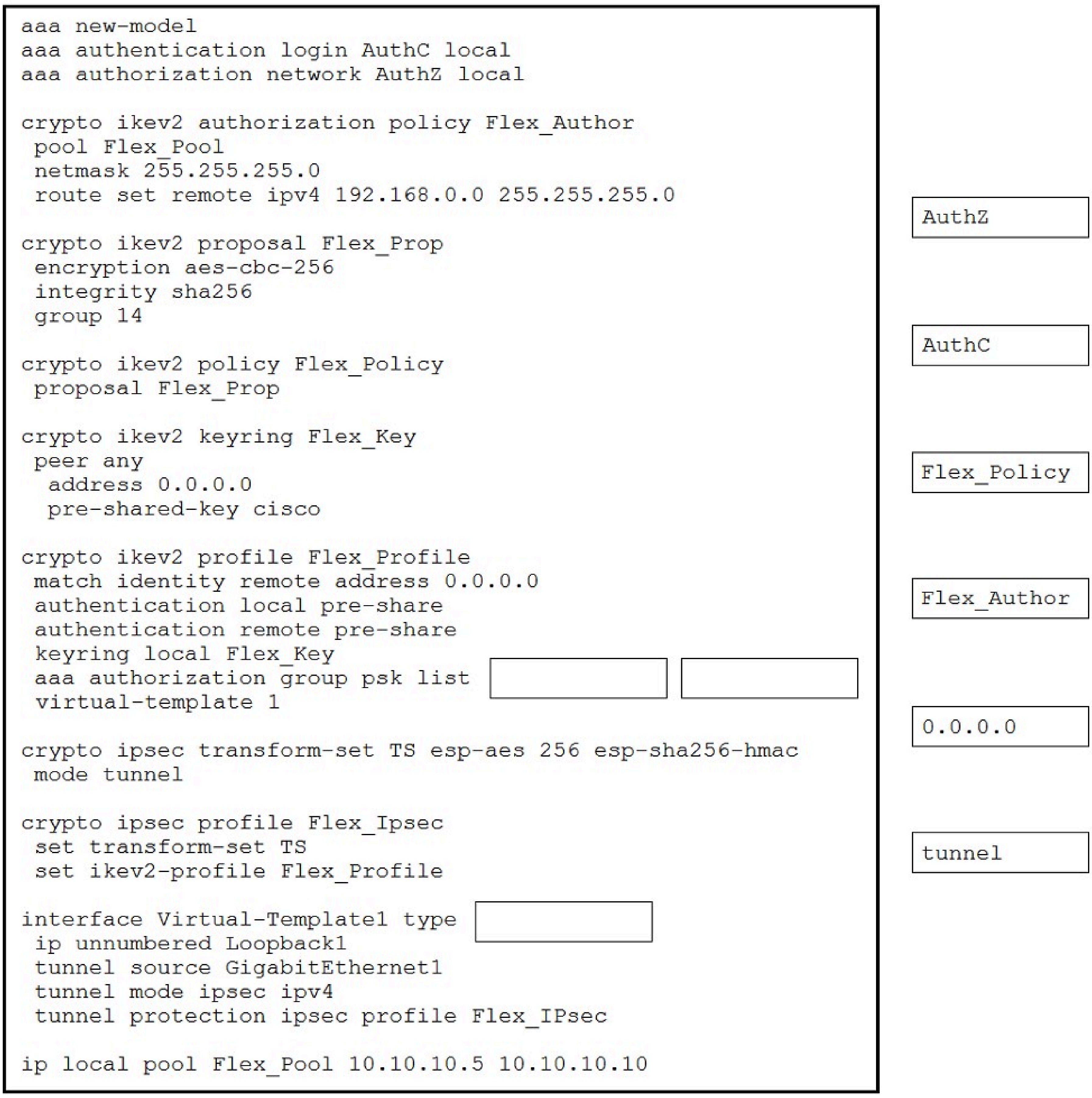
D. show crypto ipsec profile default

Question #68 *Topic 1*

DRAG DROP -

Drag and drop the code snippets from the right onto the blanks in the configuration to implement FlexVPN. Not all snippets are used.

Select and Place:



```
aaa new-model
aaa authentication login AuthC local
aaa authorization network AuthZ local

crypto ikev2 authorization policy Flex_Author
 pool Flex_Pool
 netmask 255.255.255.0
 route set remote ipv4 192.168.0.0 255.255.255.0

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

crypto ikev2 policy Flex_Policy
 proposal Flex_Prop

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

crypto ikev2 profile Flex_Profile
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local Flex_Key
 aaa authorization group psk list
 virtual-template 1

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

crypto ipsec profile Flex_Ipsec
 set transform-set TS
 set ikev2-profile Flex_Profile

interface Virtual-Template1 type
 ip unnumbered Loopback1
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flex_IPsec

ip local pool Flex_Pool 10.10.10.5 10.10.10.10
```

AuthZ

AuthC

Flex_Policy

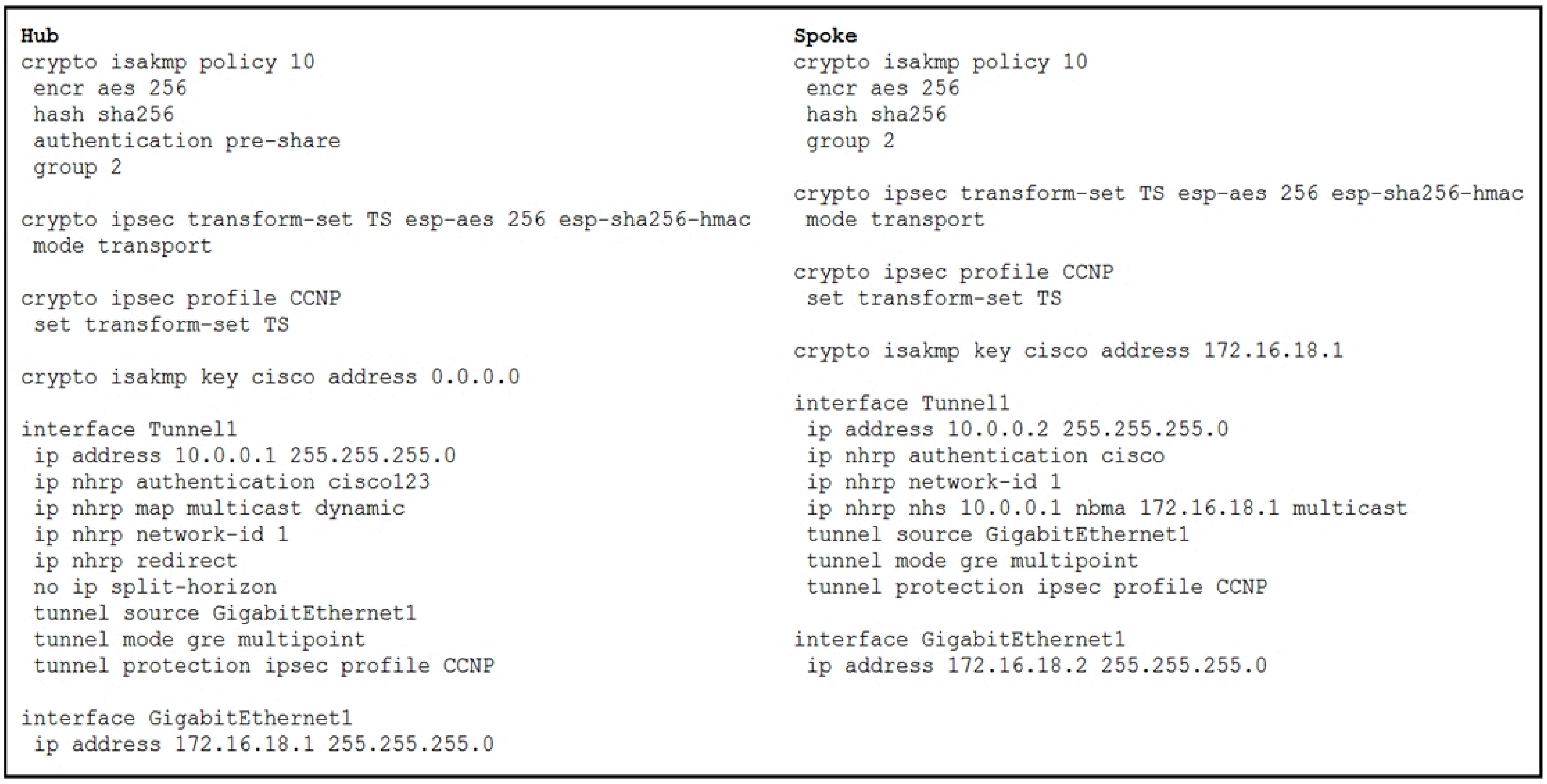
Flex_Author

0.0.0.0

tunnel

## Question #69

*Topic 1*



```
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.

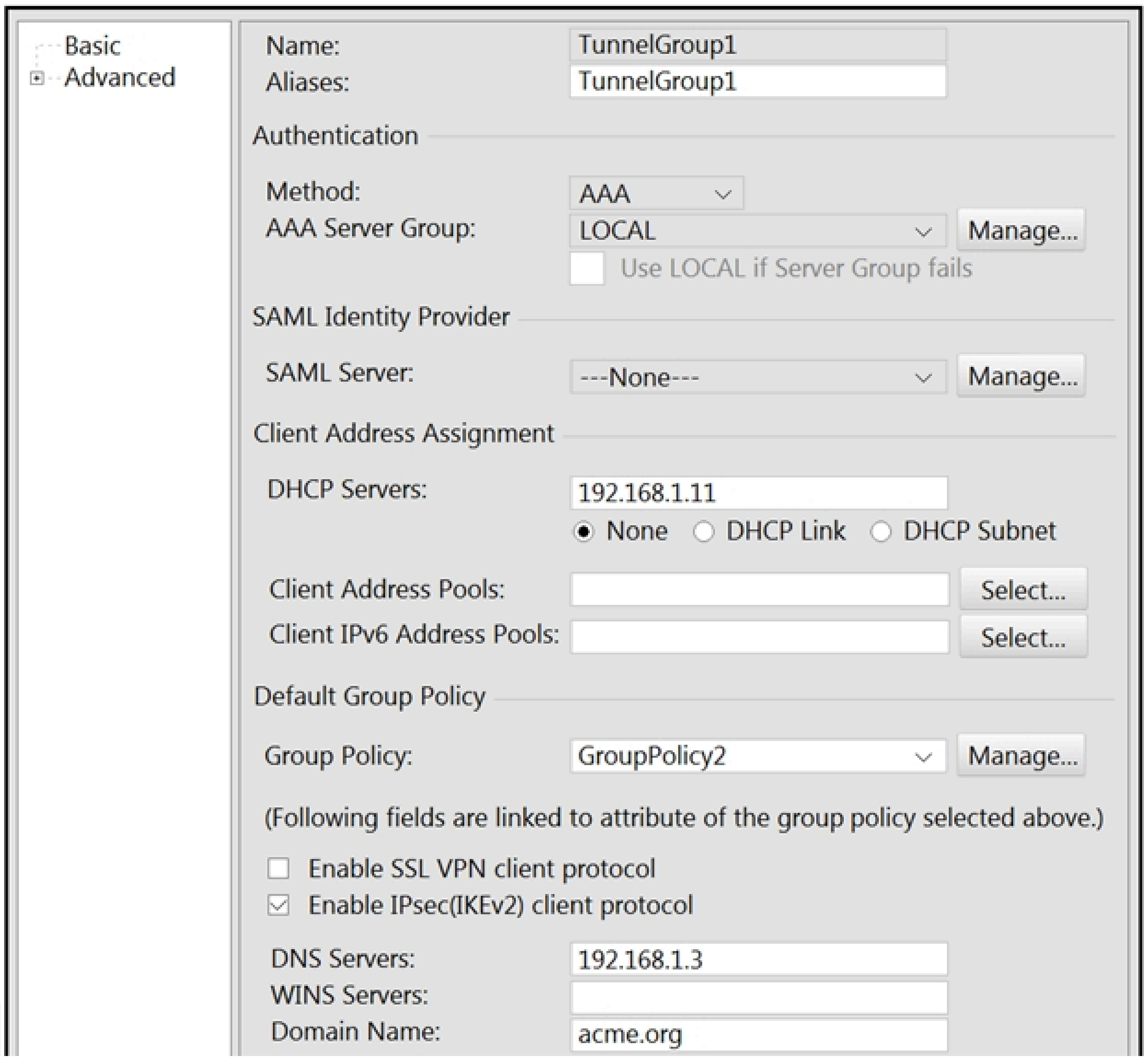
B. Change the transform set to mode tunnel.

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.

Question #70 Topic 1



Name: TunnelGroup1
Aliases: TunnelGroup1

Authentication

Method: AAA
AAA Server Group: LOCAL Manage...
□ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server: ---None--- Manage...

Client Address Assignment

DHCP Servers: 192.168.1.11
● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: Select...
Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: GroupPolicy2 Manage...

(Following fields are linked to attribute of the group policy selected above.)

□ Enable SSL VPN client protocol
☑ Enable IPsec(IKEv2) client protocol

DNS Servers: 192.168.1.3
WINS Servers:
Domain Name: acme.org

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.

Question #71 Topic 1

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

## Question #72 *Topic 1*

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
```

## Question #73 *Topic 1*

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

A. HSRP stateless failover

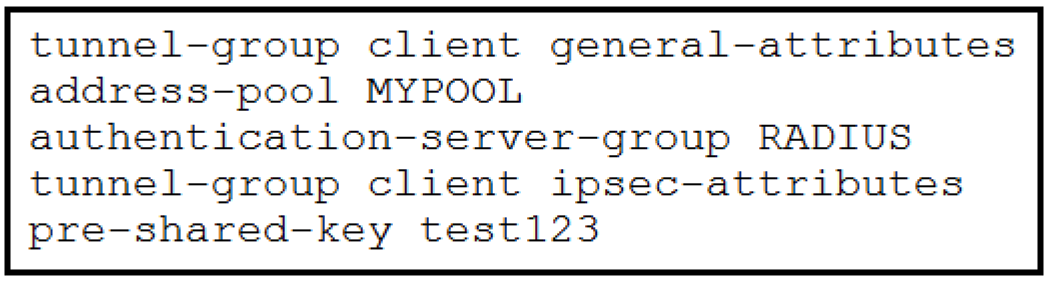
B. DNS-based hub resolution

C. reactivate primary peer

D. tunnel pivot

E. need distractor

## Question #74 *Topic 1*



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

Refer to the exhibit. Which type of VPN is used?

A. GETVPN

B. clientless SSL VPN

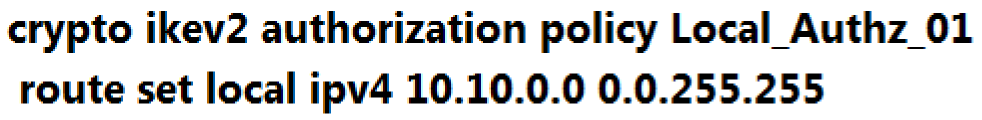
C. Cisco Easy VPN

D. Cisco AnyConnect SSL VPN

## Question #75 *Topic 1*

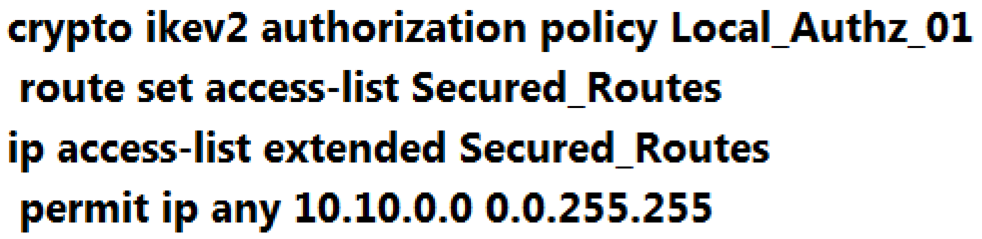
An engineer would like Cisco AnyConnect users to be able to reach servers within the 10.10.0.0/16 subnet while all other traffic is sent out to the Internet. Which
IPsec configuration accomplishes this task?

A.



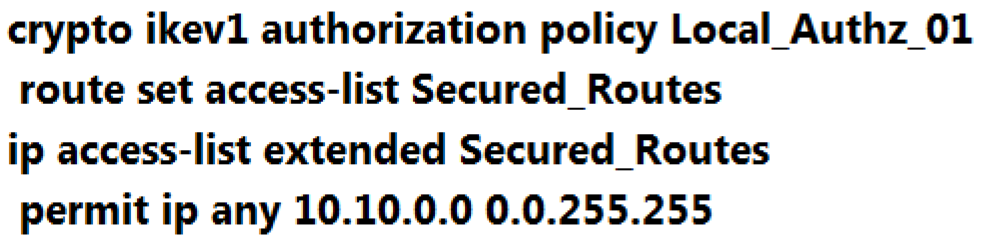
```
crypto ikev2 authorization policy Local_Authz_01
 route set local ipv4 10.10.0.0 0.0.255.255
```

B.



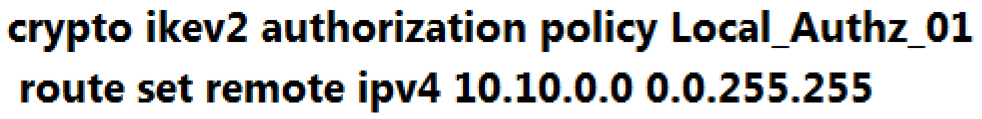
```
crypto ikev2 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```

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
```

## Question #76 *Topic 1*

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

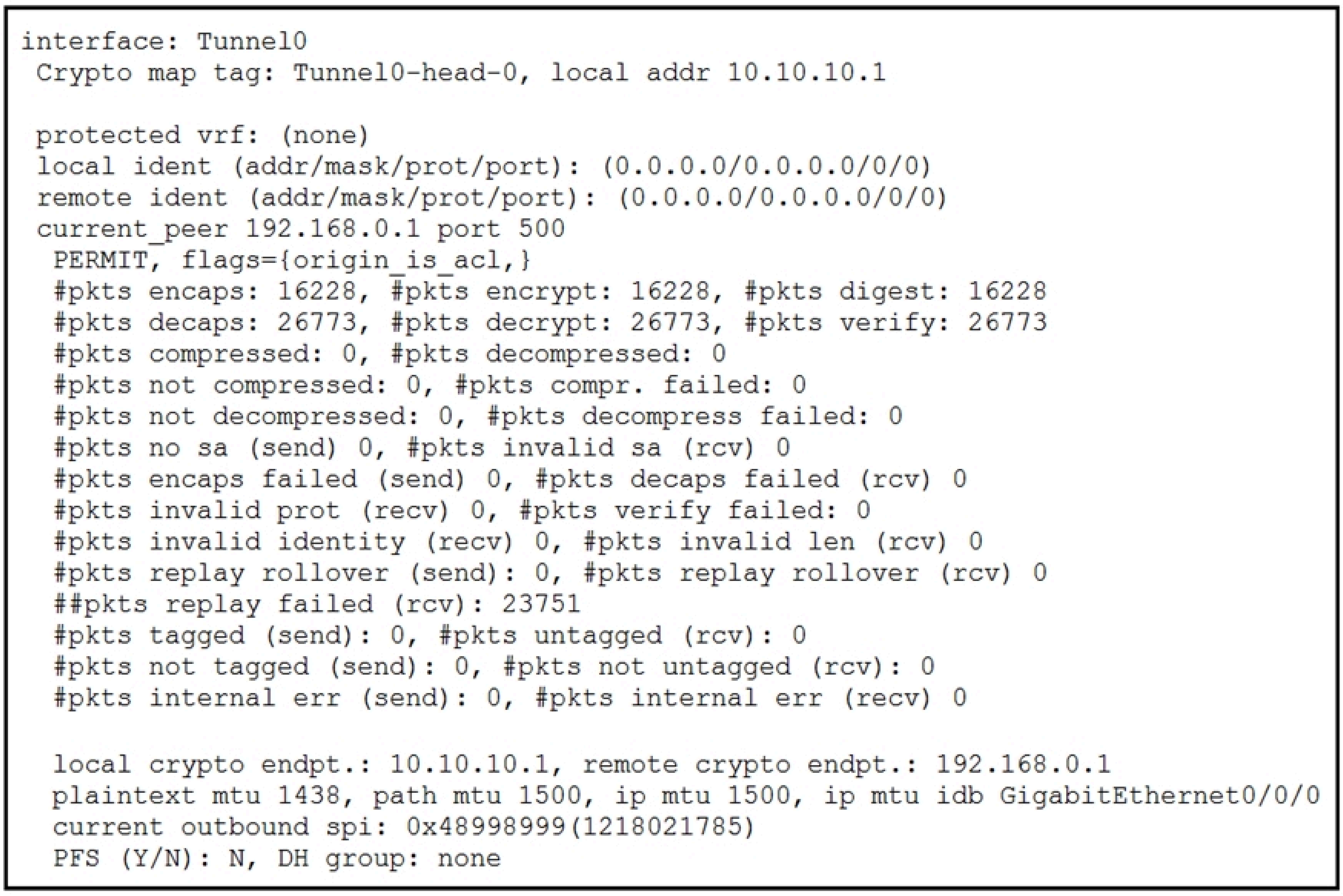
A. routing

B. WebACL

C. split tunnel

D. VPN filter

## Question #77 *Topic 1*



```
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
```

Refer to the exhibit. 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.

## Question #78 *Topic 1*

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?

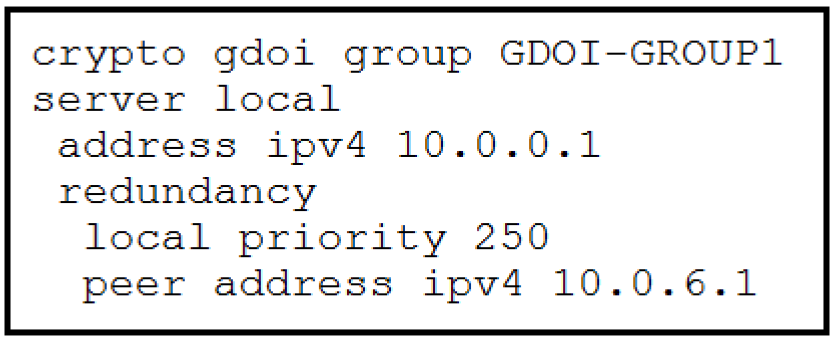
A. Apply the bookmark to the correct group policy.

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.

## Question #79 *Topic 1*



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

Refer to the exhibit. 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

## Question #80 *Topic 1*

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

## Question #81 *Topic 1*

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

## Question #82 *Topic 1*

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.

## Question #83 *Topic 1*

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

## Question #84 *Topic 1*

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?

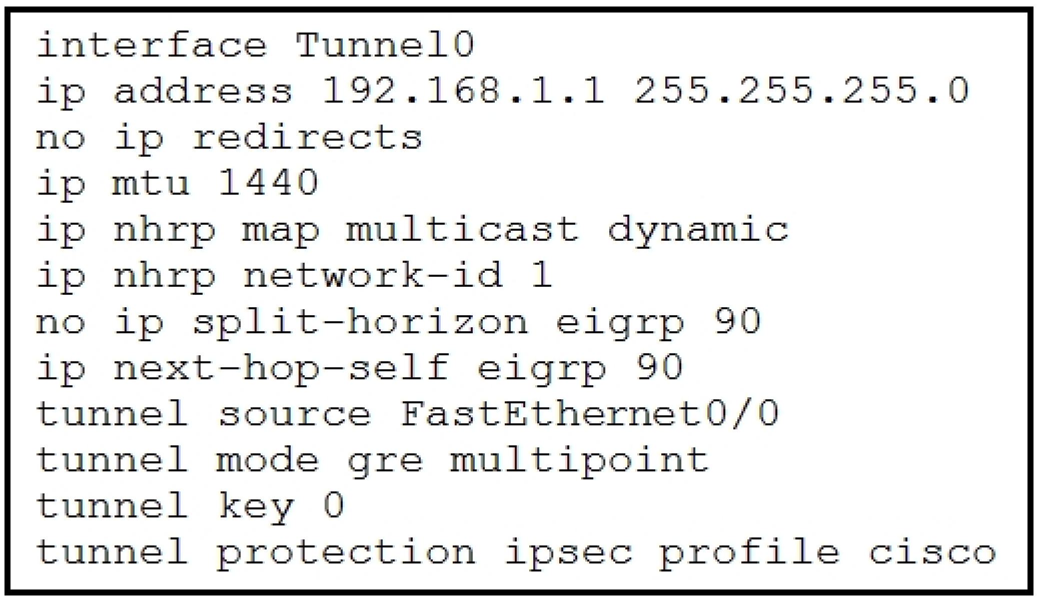
A. EAP-GTC

B. EAP-MSCHAPv2

C. EAP-MD5

D. EAP-AnyConnect

## Question #85 *Topic 1*



```
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
```

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

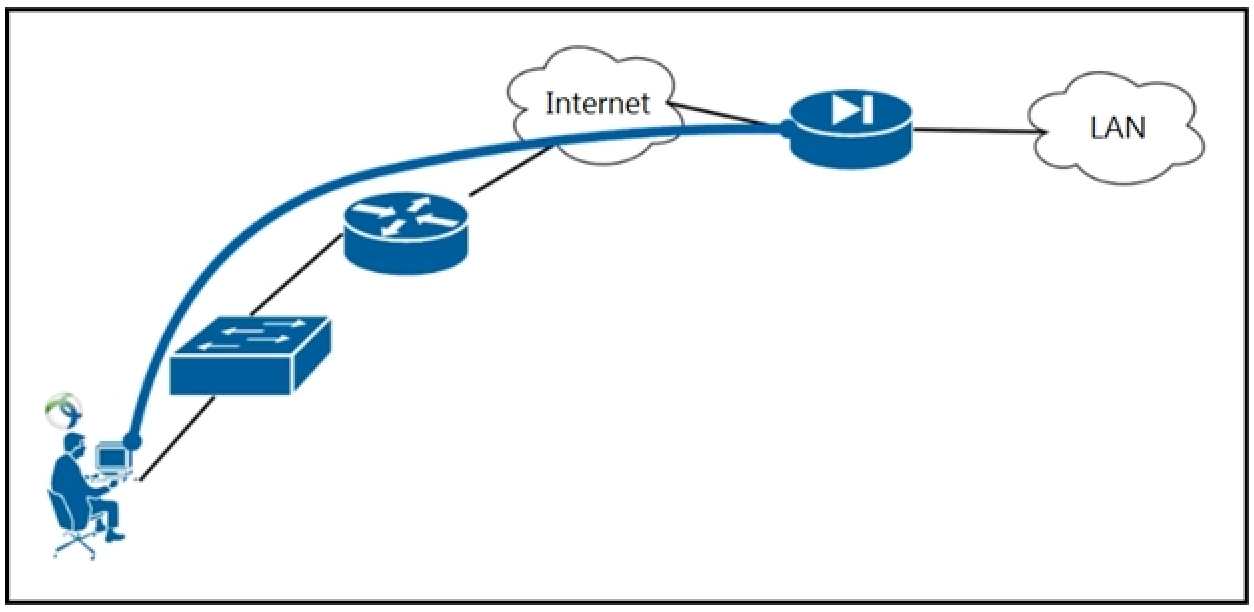
A. Enable NHRP redirect.

B. Enable split horizon.

C. Enable IP redirects.

D. Enable NHRP shortcut.

## Question #86 *Topic 1*



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>
```

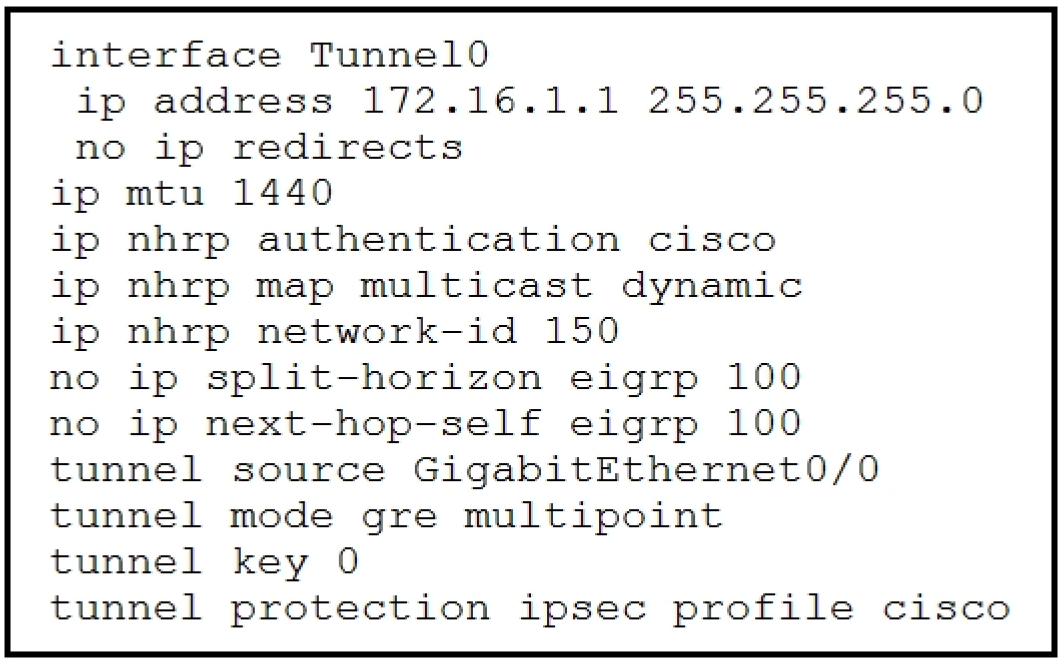
C.

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

D.

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

Question #87 *Topic 1*



```
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
```

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

A. Next-hop-self is required.

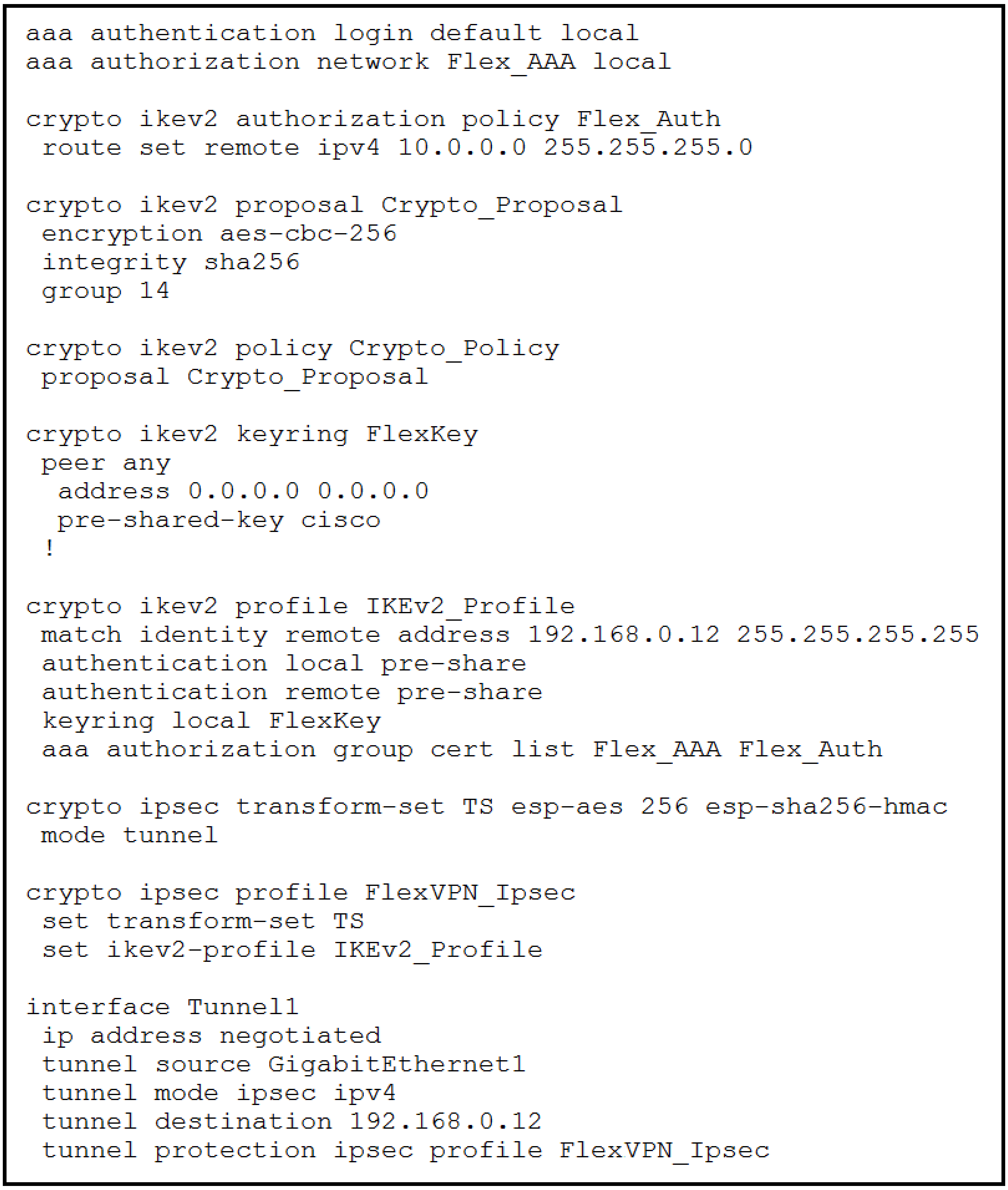
B. EIGRP neighbor adjacency will fail.

C. EIGRP is used as the dynamic routing protocol.

D. EIGRP route redistribution is not allowed.

E. Spoke-to-spoke communication is allowed.

Question #88 *Topic 1*



```
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
```

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

A. Add the address 192.168.0.12 255.255.255.255 command to the keyring configuration.

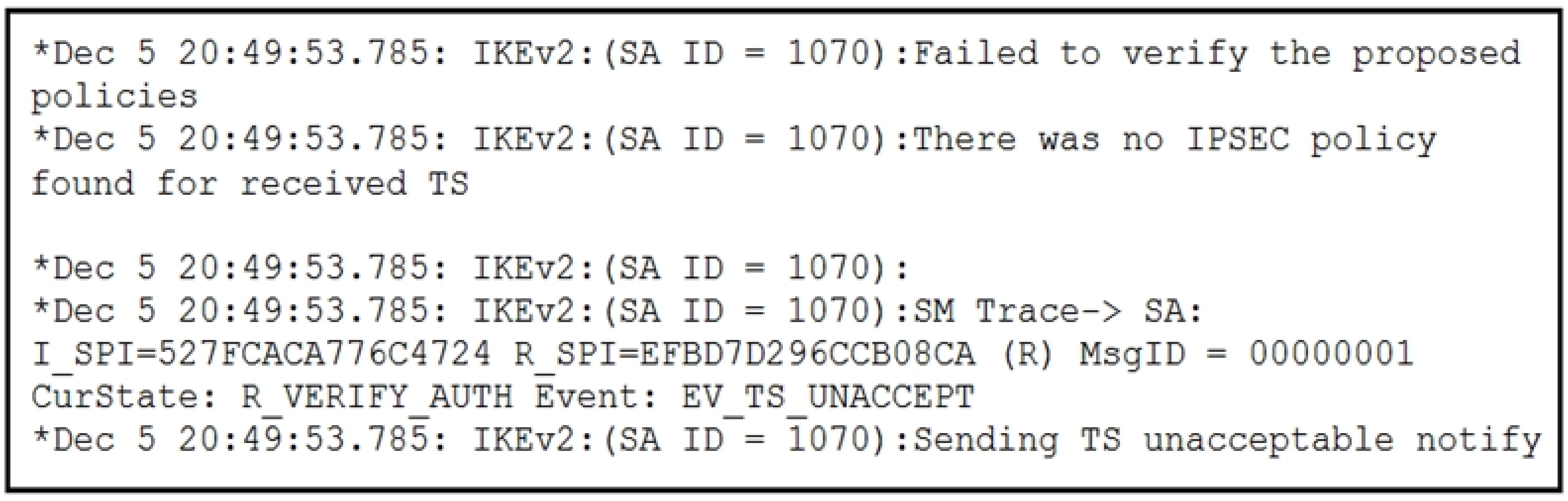
B. Add the match fvrf any command to the IKEv2 policy.

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.

## Question #89

*Topic 1*



```
*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
```

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

A. Ensure crypto IPsec policy matches on both VPN devices.

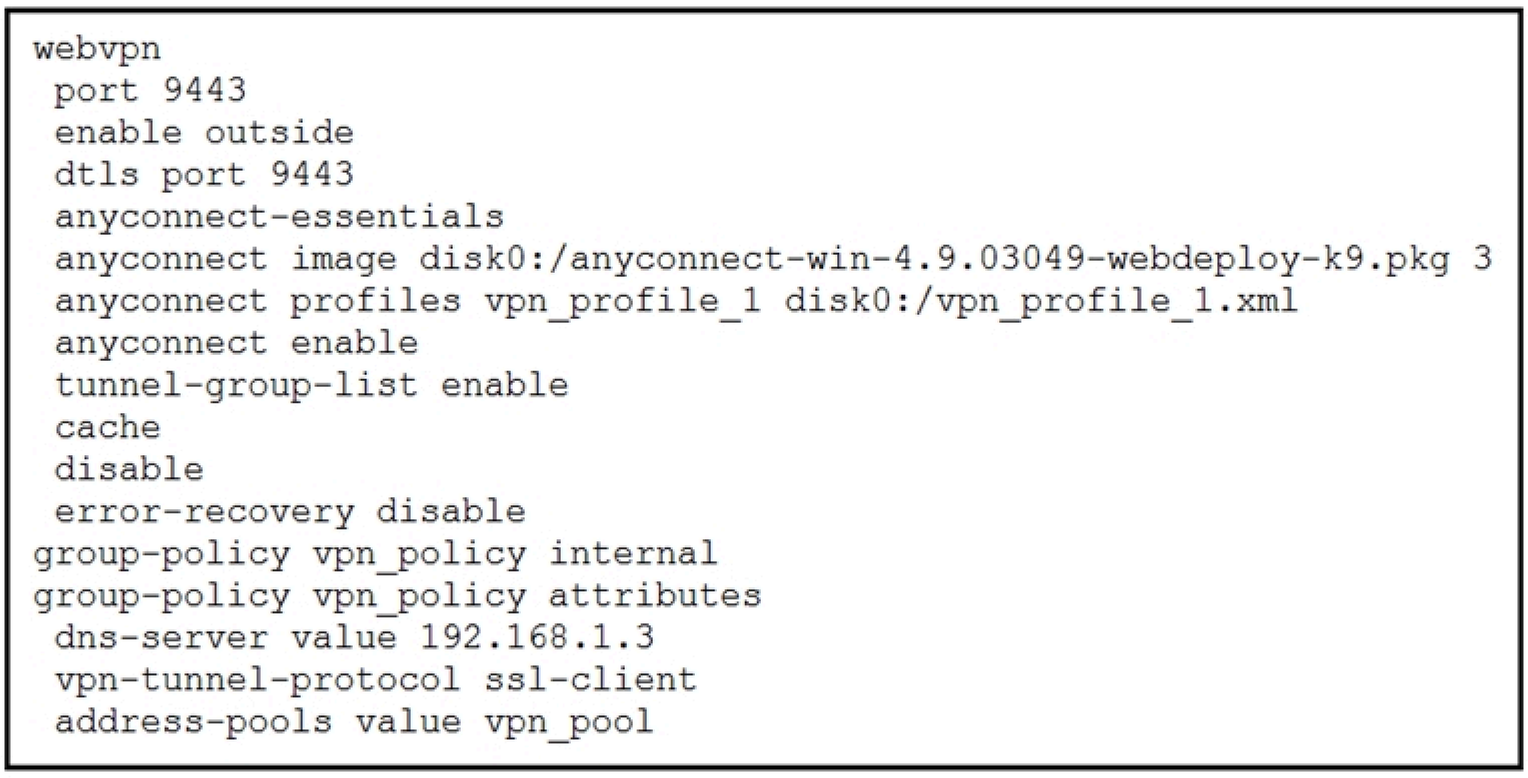
B. Install the correct certificate to validate the peer.

C. Correct crypto access list on both VPN devices.

D. Specify the peer IP address in the tunnel group name.

## Question #90

*Topic 1*



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

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

A. Enable client services on the outside interface.

B. Enable clientless protocol under the group policy.

C. Enable DTLS under the group policy.

D. Enable auto sign-on for the user's IP address.

## Question #91 *Topic 1*

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

A. to download encryption keys

B. to maintain encryption policies

C. to distribute routing information

D. to encrypt data traffic

E. to authenticate group members

## Question #92 *Topic 1*

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

A. tunnelall

B. excludeall

C. tunnelspecified

D. excludespecified

## Question #93 *Topic 1*

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

A. Define the RADIUS server.

B. Verify that clients are using the correct authorization policy.

C. Define the AAA server.

D. Assign the list to an authorization policy.

E. Set the maximum segment size.

## Question #94 *Topic 1*

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

## Question #95

*Topic 1*

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

## Question #96

*Topic 1*

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

A. Set up a smart tunnel with the IP address of the web server.

B. Set up a NAT rule that translates the ASA public address to the web server private address on port 80.

C. Set up Cisco AnyConnect with a split tunnel that has the IP address of the web server.

D. Set up a WebACL to permit the IP address of the web server.

## Question #97

*Topic 1*

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

A. SAML

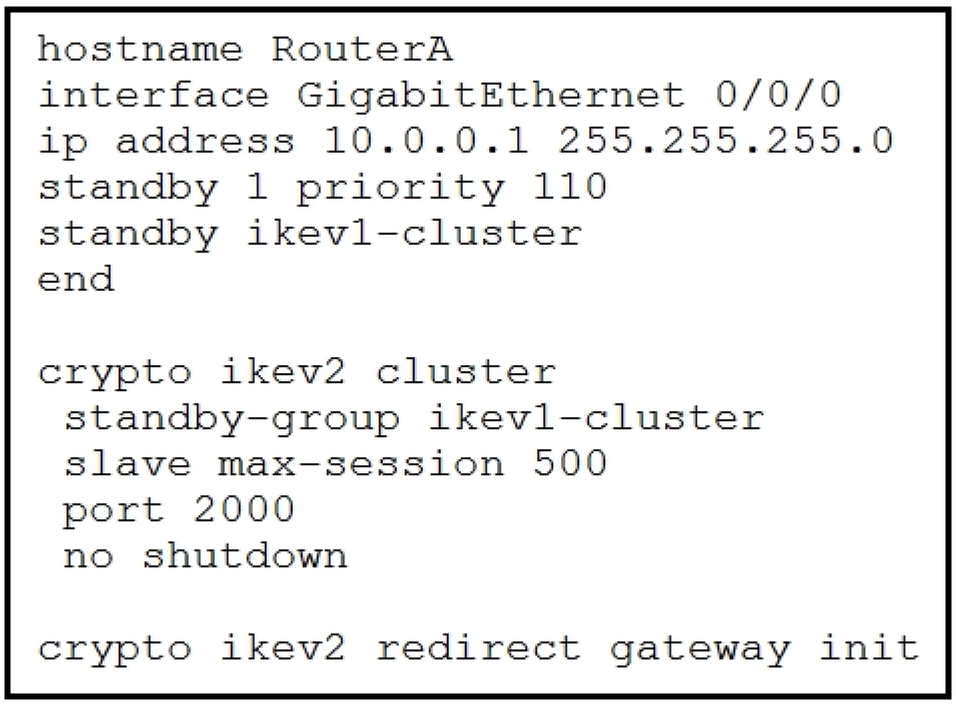
B. NTLM

C. Kerberos

D. OAuth 2.0

E. HTTP Basic

## Question #98 *Topic 1*



```
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
```

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

A. IKEv1 cluster

B. IKEv2 backup gateway

C. IKEv2 load balancer

D. IKEv2 reconnect

## Question #99 *Topic 1*

A DMVPN spoke is configured with IKEv1 to secure the tunnel. Despite having a configuration similar to other working spokes, the tunnel is not coming up. Packet captures on the spoke show packets leaving the spoke router, but not making it to the hub router. Which solution resolves this issue?

A. Configure the spoke and hub to use the same IKE version.

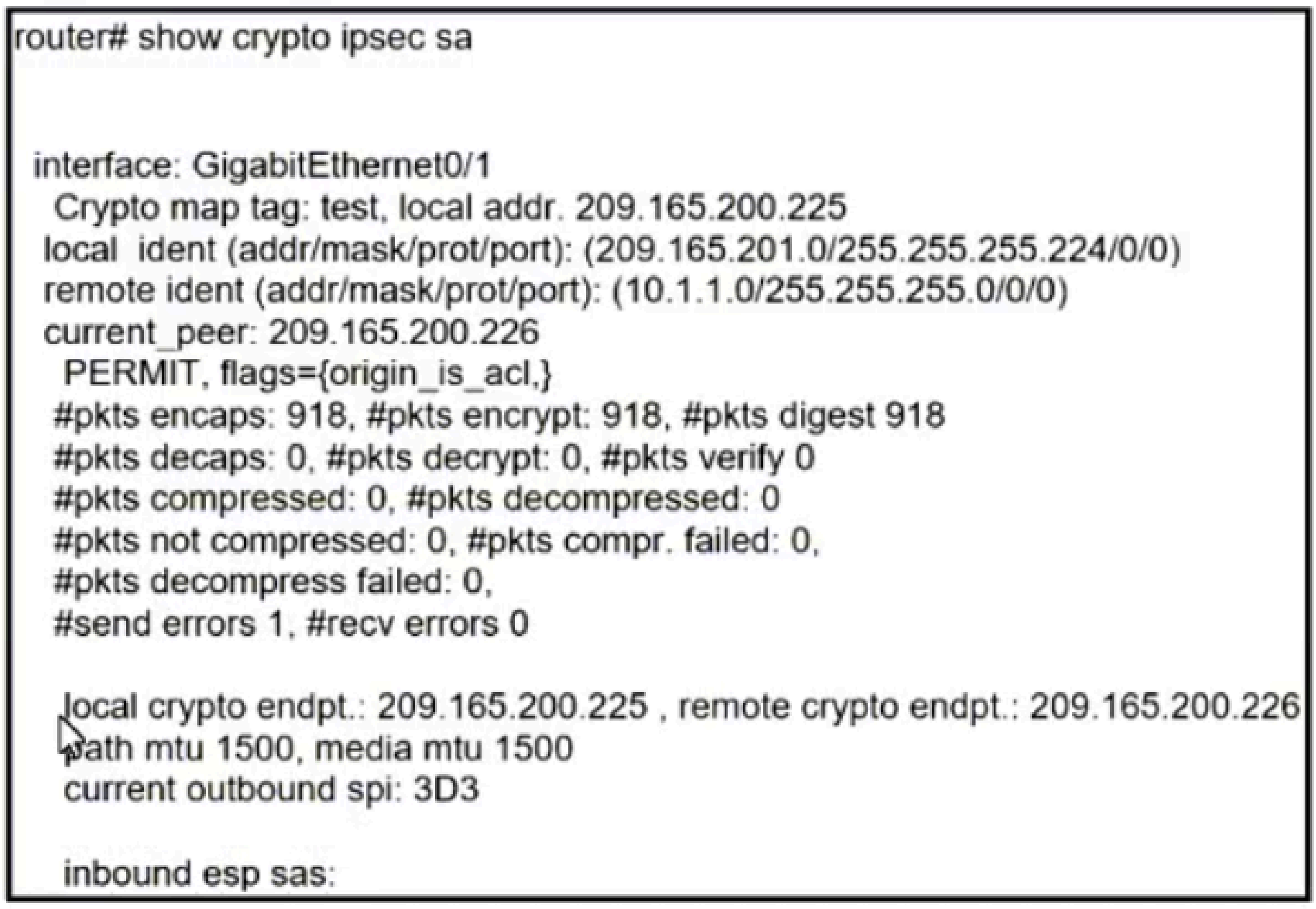
B. Ensure that devices between the hub and spoke are not blocking ESP traffic.

C. Ensure that devices between the hub and spoke are not blocking GRE traffic.

D. Enable the tunnel interface with the no shutdown command.

## Question #100 *Topic 1*

Refer to the exhibit.



```
router# show crypto ipsec sa


 interface: GigabitEthernet0/1
   Crypto map tag: test, local addr. 209.165.200.225
  local  ident (addr/mask/prot/port): (209.165.201.0/255.255.255.224/0/0)
  remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  current_peer: 209.165.200.226
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 918, #pkts encrypt: 918, #pkts digest 918
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0,
   #pkts decompress failed: 0,
   #send errors 1, #recv errors 0

    local crypto endpt.: 209.165.200.225 , remote crypto endpt.: 209.165.200.226
    path mtu 1500, media mtu 1500
    current outbound spi: 3D3

    inbound esp sas:
```

A TCP based application that should be accessible over the VPN tunnel is not working. Pings to the appropriate IP address are failing. Based on the output, what is a fix for this issue?

A. Add a route on the remote peer for 209.165.201.0/27.

B. Add a route on the local peer for 10.1.1.0/24.

C. Add a permit for TCP traffic going to 10.1.1.0/24.

D. Add a permit for TCP traffic going to 209.165.201.0/27.

## Question #101 *Topic 1*

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

## Question #102 *Topic 1*

A clientless SSLVPN is set up to allow remote users to access internal HTTPS webservers. Users can access all but one server and see the message "Connection Failed. Server 192.168.0.101 unavailable". Pings between the Cisco ASA and the webserver are successful, and users can connect to the webserver when they use their computer in the internal network. Which action resolves this issue?

A. Add an SSL cipher that can be negotiated with the webserver to the Cisco ASA.

B. Add the http 192.168.0.101 255.255.255.255 inside command to the Cisco ASA.

C. Configure routing on the Cisco ASA so it can reach the webserver.

D. Configure a DNS server that can resolve the webserver domain on the Cisco ASA.

## Question #103 *Topic 1*

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

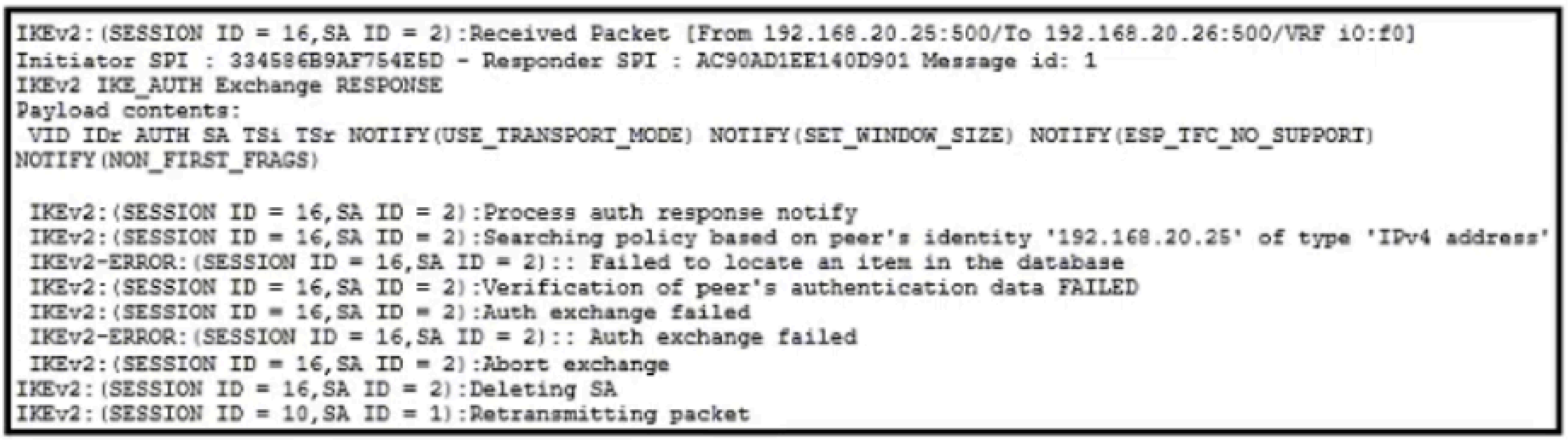
A. Citrix load balancer

B. port reflector

C. Java rewriter -
C. Java plug-ins

D. script browser

## Question #104 *Topic 1*



```
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
```

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?

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.

## Question #105 *Topic 1*

A network engineer is setting up a clientless SSLVPN on a Cisco ASA. Remote users must be able to access an internal webserver via the URL example.com. Which two steps accomplish this task? (Choose two.)

A. Configure a bookmark for the webserver.

B. Configure routing so that the user's computer can reach the webserver.

C. Configure a DNS server that can resolve the webserver URL.

D. Configure a browser plugin on the Cisco ASA.

E. Configure routing so that the Cisco ASA can reach the webserver.

## Question #106 *Topic 1*

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

A. Add the aaa server radius dynamic-author command on the FlexVPN clients.

B. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN server.

C. Add the aaa server radius dynamic-author command on the FlexVPN server.

D. Fix the RADIUS key mismatch between the RADIUS server and FlexVPN clients.

## Question #107 *Topic 1*

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

A. Use a DAP registry check on the system to determine the relationship with the corporate domain.

B. Use a DAP file check on the system to determine the relationship with the corporate domain.

C. Install and authenticate user certificates on the corporate devices.

D. Install and authenticate machine certificates on the corporate devices

## Question #108 *Topic 1*

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

## Question #109 *Topic 1*

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

A. Enable EIGRP Split Horizon on the hub tunnel interface.

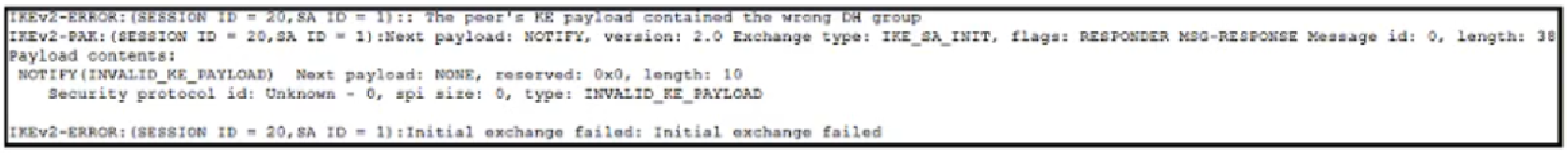
B. Remove the EIGRP stub configuration on the spoke tunnel interface.

C. Enable the EIGRP next hop self feature on the hub tunnel interface.

D. Configure the dynamic NHRP multicast map on the hub tunnel interface.

## Question #110 *Topic 1*

Refer to the exhibit.



```
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
```

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

A. Correct the DH group setting.

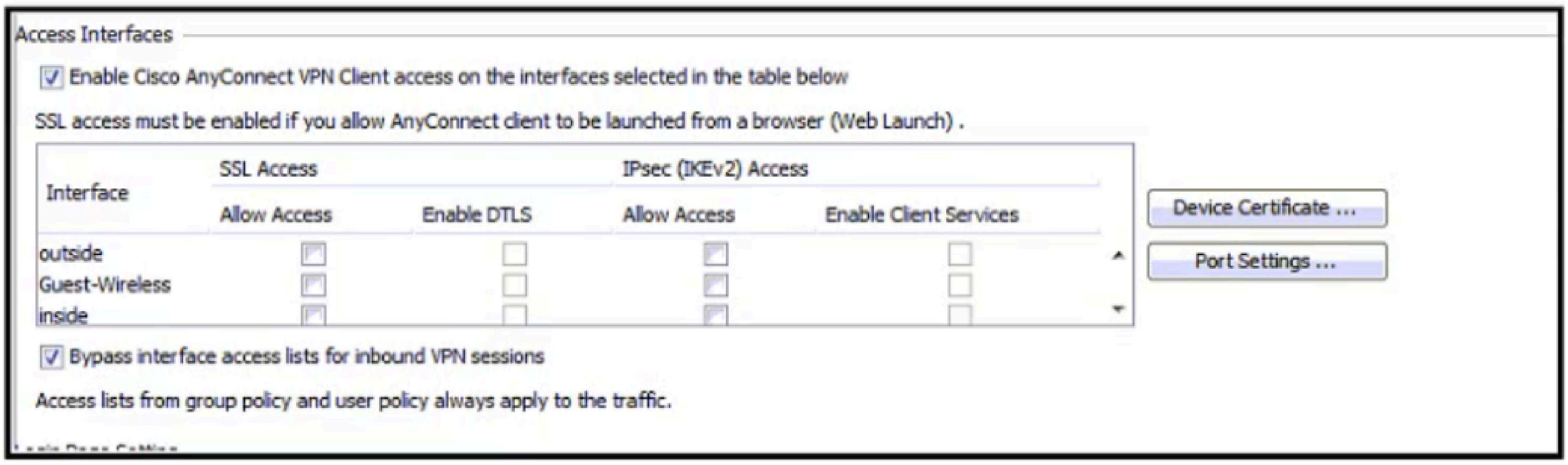
B. Correct the PFS setting.

C. Correct the integrity setting.

D. Correct the encryption setting.

## Question #111 *Topic 1*

Refer to the exhibit.



Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

| Interface | SSL Access | | IPsec (IKEv2) Access | |
|---|---|---|---|---|
| | Allow Access | Enable DTLS | Allow Access | Enable Client Services |
| outside | ☐ | ☐ | ☐ | ☐ |
| Guest-Wireless | ☐ | ☐ | ☐ | ☐ |
| inside | ☐ | ☐ | ☐ | ☐ |

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

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

A. IPsec (IKEv2) Allow Access must be checked on the outside interface.

B. SSL Enable DTLS must be checked on the outside interface.

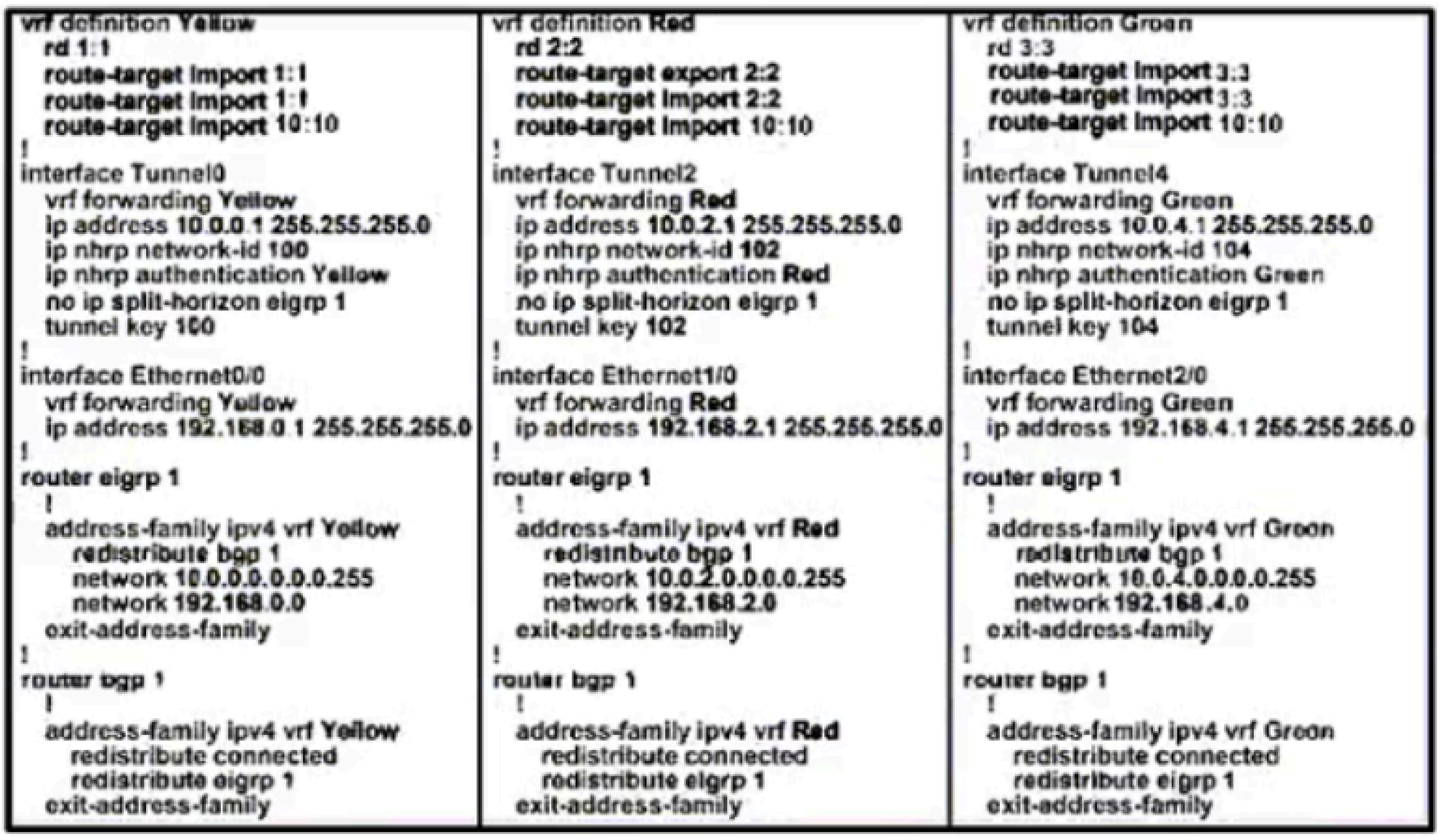
C. Bypass interface access lists for inbound VPN sessions must be unchecked.

D. IPsec (IKEv2) Enable Client Services must be checked on the outside interface.

E. SSL Allow Access must be checked on the outside interface.

Question #112 Topic 1

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

Question #113 Topic 1

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.

## Question #114 *Topic 1*

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.

## Question #115 *Topic 1*

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.

## Question #116 *Topic 1*

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

## Question #117 *Topic 1*

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