## Vendor: Cisco

## Exam Code: 300-209

## Exam Name: Implementing Cisco Secure Mobility Solutions (SIMOS)

## Version: Demo

**QUESTION 1**

Which DAP endpoint attribute checks for the matching MAC address of a client machine?

A. device

B. process

C. antispyware

D. BIA

**Correct Answer:** A

**QUESTION 2**

In FlexVPN, what is the role of a NHRP resolution request?

A. It allows these entities to directly communicate without requiring traffic to use an intermediate hop

B. It dynamically assigns VPN users to a group

C. It blocks these entities from to directly communicating with each other

D. It makes sure that each VPN spoke directly communicates with the hub

**Correct Answer:** A

**QUESTION 3**

Which two statements are true when designing a SSL VPN solution using Cisco AnyConnect? (Choose two.)

A. The VPN server must have a self-signed certificate.

B. A SSL group pre-shared key must be configured on the server.

C. Server side certificate is optional if using AAA for client authentication.

D. The VPN IP address pool can overlap with the rest of the LAN networks.

E. DTLS can be enabled for better performance.

**Correct Answer:** DE

**QUESTION 4**

Which two statements regarding IKEv2 are true per RFC 4306? (Choose two.)

A. It is compatible with IKEv1.

B. It has at minimum a nine-packet exchange.

C. It uses aggressive mode.

D. NAT traversal is included in the RFC.

E. It uses main mode.
F. DPD is defined in RFC 4309.
G. It allows for EAP authentication.

**Correct Answer:** DG

**QUESTION 5**
Which group-policy subcommand installs the Diagnostic AnyConnect Report Tool on user computers when a Cisco AnyConnect user logs in?

A. customization value dart
B. file-browsing enable
C. smart-tunnel enable dart
D. anyconnect module value dart

**Correct Answer:** D

**QUESTION 6**
When using clientless SSL VPN, you might not want some applications or web resources to go through the Cisco ASA appliance. For these application and web resources, as a Cisco ASA administrator, which configuration should you use?

A. Configure the Cisco ASA appliance for split tunneling.
B. Configure network access exceptions in the SSL VPN customization editor.
C. Configure the Cisco ASA appliance to disable content rewriting.
D. Configure the Cisco ASA appliance to enable URL Entry bypass.
E. Configure smart tunnel to bypass the Cisco ASA appliance proxy function.

**Correct Answer:** C
**Explanation:**
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/vpn_web.html
Content Rewrite
The Content Rewrite pane lists all applications for which content rewrite is enabled or disabled.
Clientless SSL VPN processes application traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript, VBScript, Java, and multi- byte characters to proxy HTTP traffic which may have different semantics and access control rules depending on whether the user is using an application within or independently of an SSL VPN device.

By default, the security appliance rewrites, or transforms, all clientless traffic. You might not want some applications and web resources (for example, public websites) to go through the security appliance. The security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without going through the security appliance. This is similar to split-tunneling in an IPSec VPN connection.

You can create multiple rewrite rules. The rule number is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

**QUESTION 7**

Which interface is managed by the VPN Access Interface field in the Cisco ASDM IPsec Site-to-Site VPN Wizard?

A. the local interface named "VPN_access"
B. the local interface configured with crypto enable
C. the local interface from which traffic originates
D. the remote interface with security level 0

**Correct Answer:** B

**QUESTION 8**

The following configuration steps have been completed.

- WebVPN was enabled on the ASA outside interface.
- SSL VPN client software was loaded to the ASA.
- A DHCP scope was configured and applied to a WebVPN Tunnel Group.

What additional step is required if the client software fails to load when connecting to the ASA SSL page?

A. The SSL client must be loaded to the client by an ASA administrator
B. The SSL client must be downloaded to the client via FTP
C. The SSL VPN client must be enabled on the ASA after loading
D. The SSL client must be enabled on the client machine before loading

**Correct Answer:** C

**QUESTION 9**

Which option describes what address preservation with IPsec Tunnel Mode allows when GETVPN is used?

A. stronger encryption methods
B. Network Address Translation of encrypted traffic
C. traffic management based on original source and destination addresses
D. Tunnel Endpoint Discovery

**Correct Answer:** C

**QUESTION 10**

A user is experiencing issues connecting to a Cisco AnyConnect VPN and receives this error message:

The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again.

Which option is the likely cause of this issue?

A. This Cisco ASA firewall has experienced a failure.
B. The user is entering an incorrect password.
C. The user's operating system is not supported with the ASA's current configuration.
D. The user laptop clock is not synchronized with NTP.

**Correct Answer:** A

**QUESTION 11**

A private wan connection is suspected of intermittently corrupting data. Which technology can a network administrator use to detect and drop the altered data traffic?

A. AES-128
B. RSA Certificates
C. SHA2-HMAC
D. 3DES
E. Diffie-Helman Key Generation

**Correct Answer:** C

**QUESTION 12**

Which protocols does the Cisco AnyConnect client use to build multiple connections to the security appliance?

A. TLS and DTLS
B. IKEv1
C. L2TP over IPsec
D. SSH over TCP

**Correct Answer:** A

**QUESTION 13**

Which configuration construct must be used in a FlexVPN tunnel?

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

**Correct Answer:** C

**QUESTION 14**

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

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

**Correct Answer:** C

**QUESTION 15**

A network is configured to allow clientless access to resources inside the network. Which feature must be enabled and configured to allow SSH applications to respond on the specified port 8889?

A. auto applet download
B. port forwarding

C. web-type ACL

D. HTTP proxy

**Correct Answer:** B

**QUESTION 16**

Which three configurations are required for both IPsec VTI and crypto map-based VPNs? (Choose three.)

A. transform set

B. ISAKMP policy

C. ACL that defines traffic to encrypt

D. dynamic routing protocol

E. tunnel interface

F. IPsec profile

G. PSK or PKI trustpoint with certificate

**Correct Answer:** ABG

**QUESTION 17**

Which algorithm is replaced by elliptic curve cryptography in Cisco NGE?

A. 3DES

B. AES

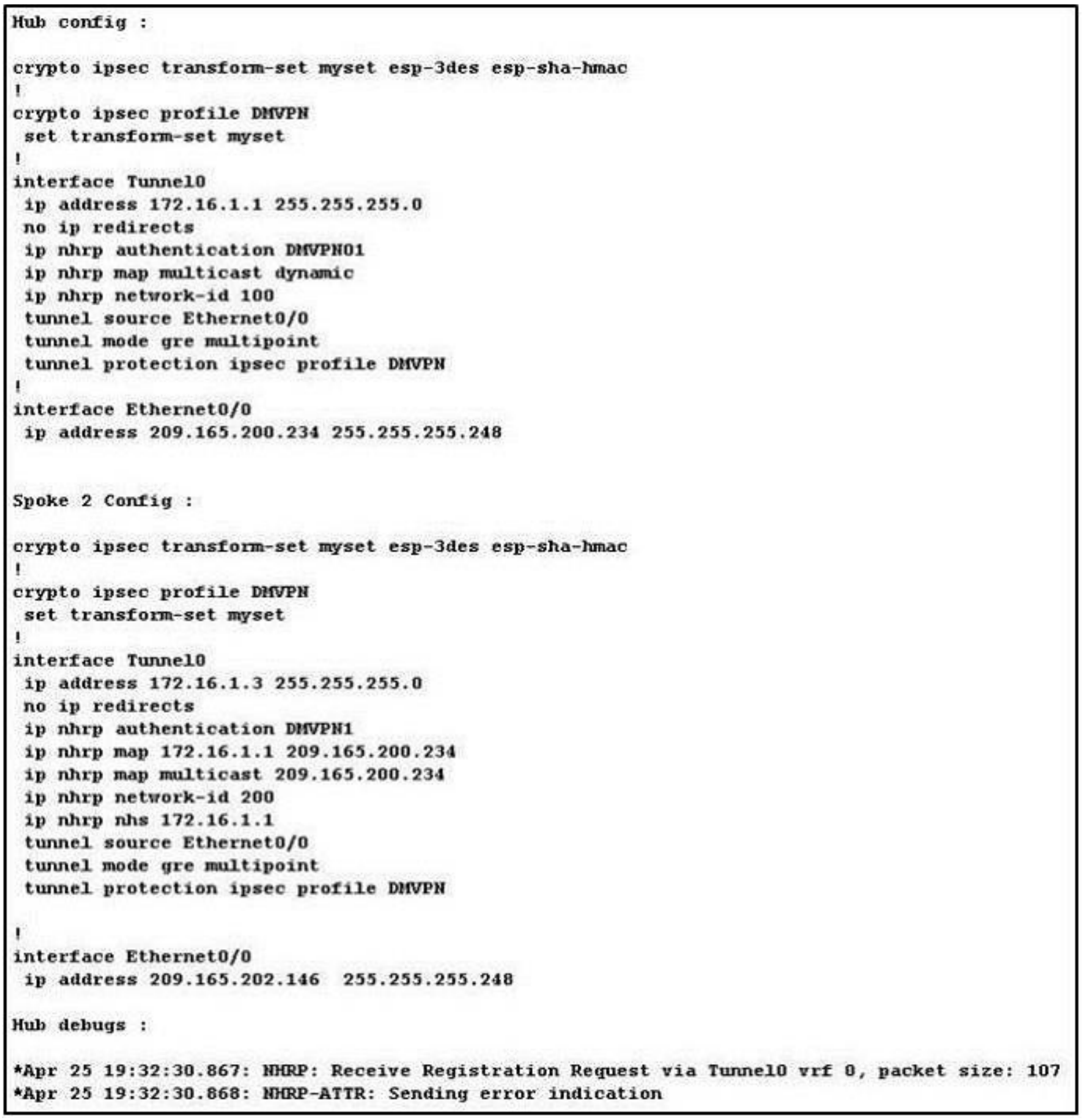
C. DES

D. RSA

**Correct Answer:** D

**QUESTION 18**

Refer to the exhibit. The network administrator is adding a new spoke, but the tunnel is not passing traffic. What could cause this issue?



```
Hub config :

crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set myset
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip nhrp authentication DMVPN01
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 ip address 209.165.200.234 255.255.255.248


Spoke 2 Config :

crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set myset
!
interface Tunnel0
 ip address 172.16.1.3 255.255.255.0
 no ip redirects
 ip nhrp authentication DMVPN1
 ip nhrp map 172.16.1.1 209.165.200.234
 ip nhrp map multicast 209.165.200.234
 ip nhrp network-id 200
 ip nhrp nhs 172.16.1.1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN

!
interface Ethernet0/0
 ip address 209.165.202.146  255.255.255.248

Hub debugs :

*Apr 25 19:32:30.867: NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 107
*Apr 25 19:32:30.868: NHRP-ATTR: Sending error indication
```

A. DMVPN is a point-to-point tunnel, so there can be only one spoke.

B. There is no EIGRP configuration, and therefore the second tunnel is not working.

C. The NHRP authentication is failing.

D. The transform set must be in transport mode, which is a requirement for DMVPN.

E. The NHRP network ID is incorrect.

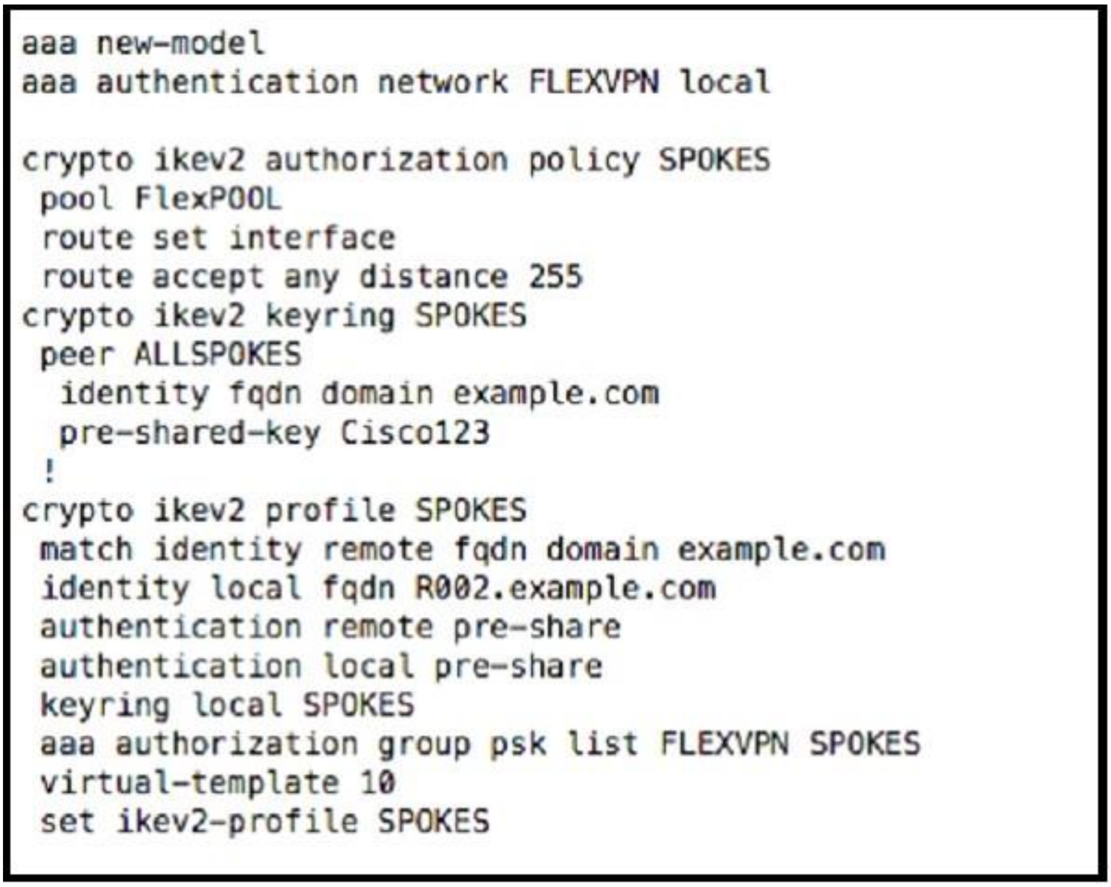
**Correct Answer:** C

**Explanation:**

http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html#wp1055049

**QUESTION 19**

Refer to the exhibit. An IPsec peer is exchanging routes using IKEv2, but the routes are not installed in the RIB. Which configuration error is causing the failure?



```
aaa new-model
aaa authentication network FLEXVPN local

crypto ikev2 authorization policy SPOKES
 pool FlexPOOL
 route set interface
 route accept any distance 255
crypto ikev2 keyring SPOKES
 peer ALLSPOKES
  identity fqdn domain example.com
  pre-shared-key Cisco123
 !
crypto ikev2 profile SPOKES
 match identity remote fqdn domain example.com
 identity local fqdn R002.example.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SPOKES
 aaa authorization group psk list FLEXVPN SPOKES
 virtual-template 10
 set ikev2-profile SPOKES
```

A. IKEv2 routing requires certificate authentication, not pre-shared keys.

B. An invalid administrative distance value was configured.

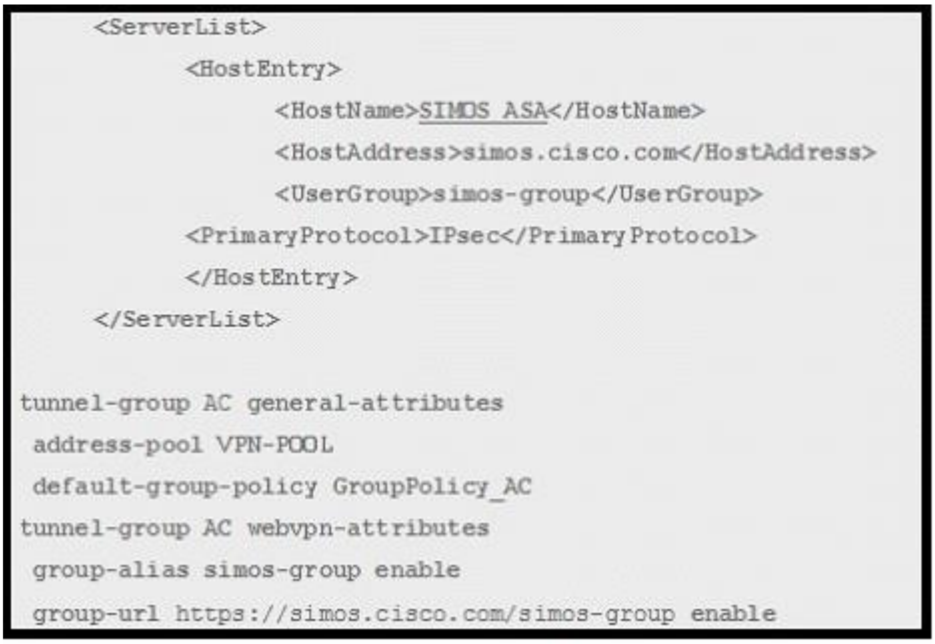
C. The match identity command must refer to an access list of routes.

D. The IKEv2 authorization policy is not referenced in the IKEv2 profile.

**Correct Answer:** B

**QUESTION 20**

Refer to the exhibit. An administrator had the above configuration working with SSL protocol, but as soon as the administrator specified IPsec as the primary protocol, the Cisco AnyConnect client was not able to connect. What is the problem?



```
      <ServerList>
            <HostEntry>
                  <HostName>SIMOS ASA</HostName>
                  <HostAddress>simos.cisco.com</HostAddress>
                  <UserGroup>simos-group</UserGroup>
            <PrimaryProtocol>IPsec</PrimaryProtocol>
            </HostEntry>
      </ServerList>

tunnel-group AC general-attributes
 address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 group-alias simos-group enable
 group-url https://simos.cisco.com/simos-group enable
```

A. IPsec will not work in conjunction with a group URL.

B. The Cisco AnyConnect implementation does not allow the two group URLs to be the same. SSL does allow this.

C. If you specify the primary protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group).

D. A new XML profile should be created instead of modifying the existing profile, so that the clients force the update.

**Correct Answer:** C