300-209.examcollection.premium.exam.234q

Number: 300-209
Passing Score: 800
Time Limit: 120 min
File Version: 8.0

300-209

Implementing Cisco Secure Mobility Solutions

Version 8.0

Exam A

QUESTION 1
Which two are characteristics of GETVPN? (Choose two.)

A. The IP header of the encrypted packet is preserved
B. A key server is elected among all configured Group Members
C. Unique encryption keys are computed for each Group Member
D. The same key encryption and traffic encryption keys are distributed to all Group Members

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A company has decided to migrate an existing IKEv1 VPN tunnel to IKEv2. Which two are valid configuration constructs on a Cisco IOS router? (Choose two.)

A.
```
crypto ikev2 keyring keyring-name
 peer peer1
  address 209.165.201.1 255.255.255.255
  pre-shared-key local key1
  pre-shared-key remote key2
```
B.
```
crypto ikev2 transform-set transform-set-name
  esp-3des esp-md5-hmac
  esp-aes esp-sha-hmac
```
C.
```
crypto ikev2 map crypto-map-name
 set crypto ikev2 tunnel-group tunnel-group-name
 set crypto ikev2 transform-set transform-set-name
```
D.
```
crypto ikev2 tunnel-group tunnel-group-name
 match identity remote address 209.165.201.1
 authentication local pre-share
 authentication remote pre-share
```
E.
```
crypto ikev2 profile profile-name
 match identity remote address 209.165.201.1
 authentication local pre-share
 authentication remote pre-share
```

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which four activities does the Key Server perform in a GETVPN deployment? (Choose four.)

A. authenticates group members
B. manages security policy
C. creates group keys
D. distributes policy/keys
E. encrypts endpoint traffic
F. receives policy/keys
G. defines group members

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Where is split-tunneling defined for remote access clients on an ASA?

A. Group-policy
B. Tunnel-group
C. Crypto-map
D. Web-VPN Portal
E. ISAKMP client

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following could be used to configure remote access VPN Host-scan and pre-login policies?

A. ASDM
B. Connection-profile CLI command
C. Host-scan CLI command under the VPN group policy
D. Pre-login-check CLI command

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
In FlexVPN, what command can an administrator use to create a virtual template interface that can be configured and applied dynamically to create virtual access interfaces?

A. interface virtual-template number type template
B. interface virtual-template number type tunnel
C. interface template number type virtual
D. interface tunnel-template number

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Here is a reference an explanation that can be included with this test.
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex-spoke.html#GUID-4A10927D-4C6A-4202-B01C-DA7E462F5D8A

Configuring the Virtual Tunnel Interface on FlexVPN Spoke

SUMMARY STEPS
1. enable
2. configure terminal
3. interface virtual-template number type tunnel
4. ip unnumbered tunnel number

5. ip nhrp network-id number
6. ip nhrp shortcut virtual-template-number
7. ip nhrp redirect [timeout seconds]
8. exit

QUESTION 7
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What are three benefits of deploying a GET VPN? (Choose three.)

A. It provides highly scalable point-to-point topologies.
B. It allows replication of packets after encryption.
C. It is suited for enterprises running over a DMVPN network.
D. It preserves original source and destination IP address information.
E. It simplifies encryption management through use of group keying.
F. It supports non-IP protocols.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
What is the default topology type for a GET VPN?

A. point-to-point
B. hub-and-spoke
C. full mesh
D. on-demand spoke-to-spoke

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which two GDOI encryption keys are used within a GET VPN network? (Choose two.)

A. key encryption key
B. group encryption key
C. user encryption key
D. traffic encryption key

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
What are the three primary components of a GET VPN network? (Choose three.)

A. Group Domain of Interpretation protocol
B. Simple Network Management Protocol
C. server load balancer
D. accounting server
E. group member
F. key server

Correct Answer: AEF
Section: (none)

Explanation

Explanation/Reference:

QUESTION 12
Which two IKEv1 policy options must match on each peer when you configure an IPsec site-to-site VPN? (Choose two.)

A. priority number
B. hash algorithm
C. encryption algorithm
D. session lifetime
E. PRF algorithm

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which two parameters are configured within an IKEv2 proposal on an IOS router? (Choose two.)

A. authentication
B. encryption
C. integrity
D. lifetime

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
In a spoke-to-spoke DMVPN topology, which type of interface does a branch router require?

A. Virtual tunnel interface

B. Multipoint GRE interface
C. Point-to-point GRE interface
D. Loopback interface

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Refer to the exhibit.

```
crypto pki certificate map CERTMAP
subject-name co cn=cisco.com
crypto ikev2 profile IKEPROFILE
authentication local pre-share
authentication remote rsa-sig
keyring local KEYRING1
match identity remote address 209.165.200.225 255.255.255.255
match identity remote address 209.165.202.155 255.255.255.255
match certificate CERTMAP
pki trustpoint TRUSTPOINT1
```

After the configuration is performed, which combination of devices can connect?

A. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name of "cisco.com"
B. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 or a certificate with subject name containing "cisco.com'
C. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 and a certificate with subject name containing "cisco.com"
D. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name containing "cisco.com"

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 16
Which three settings are required for crypto map configuration? (Choose three.)

A. match address
B. set peer
C. set transform-set
D. set security-association lifetime
E. set security-association level per-host
F. set pfs

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Consider this scenario. When users attempt to connect via a Cisco AnyConnect VPN session, the certificate has changed and the connection fails.

What is a possible cause of the connection failure?

A. An invalid modulus was used to generate the initial key.
B. The VPN is using an expired certificate.
C. The Cisco ASA appliance was reloaded.
D. The Trusted Root Store is configured incorrectly.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
In the Cisco ASDM interface, where do you enable the DTLS protocol setting?

A. Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy
B. Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit
C. Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
D. Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/admin/admin5.html

Shows where DTLS can be configured as:
• Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client

• Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

•Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

QUESTION 20
What are two forms of SSL VPN? (Choose two.)

A. port forwarding
B. Full Tunnel Mode
C. Cisco IOS WebVPN
D. Cisco AnyConnect

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
When Cisco ASA applies VPN permissions, what is the first set of attributes that it applies?

A. dynamic access policy attributes
B. group policy attributes
C. connection profile attributes
D. user attributes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
What are two variables for configuring clientless SSL VPN single sign-on? (Choose two.)

A. CSCO_WEBVPN_OTP_PASSWORD
B. CSCO_WEBVPN_INTERNAL_PASSWORD
C. CSCO_WEBVPN_USERNAME
D. CSCO_WEBVPN_RADIUS_USER

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
To change the title panel on the logon page of the Cisco IOS WebVPN portal, which file must you configure?

A. Cisco IOS WebVPN customization template
B. Cisco IOS WebVPN customization general
C. web-access-hlp.inc
D. app-access-hlp.inc

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which three plugins are available for clientless SSL VPN? (Choose three.)

A. CIFS
B. RDP2
C. SSH
D. VNC
E. SQLNET
F. ICMP

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which command simplifies the task of converting an SSL VPN to an IKEv2 VPN on a Cisco ASA appliance that has an invalid IKEv2 configuration?

A. migrate remote-access ssl overwrite
B. migrate remote-access ikev2

C. migrate l2l
D. migrate remote-access ssl

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Below is a reference for this question:
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113597-ptn-113597.html

If your IKEv1, or even SSL, configuration already exists, the ASA makes the migration process simple. On the command line, enter the migrate command:

migrate {l2l | remote-access {ikev2 | ssl} | overwrite}
Things of note:

Keyword definitions:

l2l - This converts current IKEv1 l2l tunnels to IKEv2.

remote access - This converts the remote access configuration. You can convert either the IKEv1 or the SSL tunnel groups to IKEv2.

overwrite - If you have a IKEv2 configuration that you wish to overwrite, then this keyword converts the current IKEv1 configuration and removes the superfluous IKEv2 configuration.

QUESTION 26
Which statement describes a prerequisite for single-sign-on Netegrity Cookie Support in an IOC SSL VPN?

A. The Cisco AnyConnect Secure Mobility Client must be installed in flash.
B. A SiteMinder plug-in must be installed on the Cisco SSL VPN gateway.
C. A Cisco plug-in must be installed on a SiteMinder server.
D. The Cisco Secure Desktop software package must be installed in flash.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

Which two statements describe effects of the DoNothing option within the untrusted network policy on a Cisco AnyConnect profile? (Choose two.)

A. The client initiates a VPN connection upon detection of an untrusted network.
B. The client initiates a VPN connection upon detection of a trusted network.
C. The always-on feature is enabled.
D. The always-on feature is disabled.
E. The client does not automatically initiate any VPN connection.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which command enables IOS SSL VPN Smart Tunnel support for PuTTY?

A. appl ssh putty.exe win
B. appl ssh putty.exe windows
C. appl ssh putty
D. appl ssh putty.exe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which three remote access VPN methods in an ASA appliance provide support for Cisco Secure Desktop? (Choose three.)

A. IKEv1
B. IKEv2
C. SSL client
D. SSL clientless
E. ESP
F. L2TP

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
A user is unable to establish an AnyConnect VPN connection to an ASA. When using the Real-Time Log viewer within ASDM to troubleshoot the issue, which two filter options would the administrator choose to show only syslog messages relevant to the VPN connection? (Choose two.)

A. Client's public IP address
B. Client's operating system
C. Client's default gateway IP address
D. Client's username
E. ASA's public IP address

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which Cisco ASDM option configures forwarding syslog messages to email?

A. Configuration > Device Management > Logging > E-Mail Setup
B. Configuration > Device Management > E-Mail Setup > Logging Enable
C. Select the syslogs to email, click Edit, and select the Forward Messages option.
D. Select the syslogs to email, click Settings, and specify the Destination Email Address option.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

Which Cisco ASDM option configures WebVPN access on a Cisco ASA?

A. Configuration > WebVPN > WebVPN Access
B. Configuration > Remote Access VPN > Clientless SSL VPN Access
C. Configuration > WebVPN > WebVPN Config
D. Configuration > VPN > WebVPN Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A user with IP address 10.10.10.10 is unable to access a HTTP website at IP address 209.165.200.225 through a Cisco ASA. Which two features and commands will help troubleshoot the issue? (Choose two.)

A. Capture user traffic using command capture capin interface inside match ip host 10.10.10.10 any
B. After verifying that user traffic reaches the firewall using syslogs or captures, use packet tracer command packet-tracer input inside tcp 10.10.10.10 1234 209.165.200.225 80
C. Enable logging at level 1 and check the syslogs using commands logging enable, logging buffered 1 and show logging | include 10.10.10.10
D. Check if an access-list on the firewall is blocking the user by using command show running-config access-list | include 10.10.10.10
E. Use packet tracer command packet-tracer input inside udp 0.10.10.10 1234192.168.1.3 161 to see what the firewall is doing with the user's traffic

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A Cisco router may have a fan issue that could increase its temperature and trigger a failure. What troubleshooting steps would verify the issue without causing additional risks?

A. Configure logging using commands "logging on", "logging buffered 4", and check for fan failure logs using "show logging"
B. Configure logging using commands "logging on", "logging buffered 6", and check for fan failure logs using "show logging"
C. Configure logging using commands "logging on", "logging discriminator msglog1 console 7", and check for fan failure logs using "show logging"
D. Configure logging using commands "logging host 10.11.10.11", "logging trap 2", and check for fan failure logs at the syslog server 10.11.10.11

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
An internet-based VPN solution is being considered to replace an existing private WAN connecting remote offices. A multimedia application is used that relies on multicast for communication. Which two VPN solutions meet the application's network requirement? (Choose two.)

A. FlexVPN
B. DMVPN
C. Group Encrypted Transport VPN
D. Crypto-map based Site-to-Site IPsec VPNs
E. AnyConnect VPN

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A company needs to provide secure access to its remote workforce. The end users use public kiosk computers and a wide range of devices. They will be accessing only an internal web application. Which VPN solution satisfies these requirements?

A. Clientless SSLVPN
B. AnyConnect Client using SSLVPN
C. AnyConnect Client using IKEv2
D. FlexVPN Client
E. Windows built-in PPTP client

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A network administrator is configuring AES encryption for the ISAKMP policy on an IOS router. Which two configurations are valid? (Choose two.)

A. crypto isakmp policy 10
encryption aes 254
B. crypto isakmp policy 10
encryption aes 192
C. crypto isakmp policy 10
encryption aes 256
D. crypto isakmp policy 10
encryption aes 196
E. crypto isakmp policy 10
encryption aes 199
F. crypto isakmp policy 10
encryption aes 64

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which two qualify as Next Generation Encryption integrity algorithms? (Choose two.)

A. SHA-512
B. SHA-256
C. SHA-192
D. SHA-380
E. SHA-192
F. SHA-196

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which statement is true when implementing a router with a dynamic public IP address in a crypto map based site-to-site VPN?

A. The router must be configured with a dynamic crypto map.
B. Certificates are always used for phase 1 authentication.
C. The tunnel establishment will fail if the router is configured as a responder only.
D. The router and the peer router must have NAT traversal enabled.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which two features are required when configuring a DMVPN network? (Choose two.)

A. Dynamic routing protocol
B. GRE tunnel interface
C. Next Hop Resolution Protocol
D. Dynamic crypto map
E. IPsec encryption

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
What are two benefits of DMVPN Phase 3? (Choose two.)

A. Administrators can use summarization of routing protocol updates from hub to spokes.
B. It introduces hierarchical DMVPN deployments.
C. It introduces non-hierarchical DMVPN deployments.
D. It supports L2TP over IPSec as one of the VPN protocols.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which are two main use cases for Clientless SSL VPN? (Choose two.)

A. In kiosks that are part of a shared environment
B. When the users do not have admin rights to install a new VPN client
C. When full tunneling is needed to support applications that use TCP, UDP, and ICMP
D. To create VPN site-to-site tunnels in combination with remote access

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which technology can rate-limit the number of tunnels on a DMVPN hub when system utilization is above a specified percentage?

A. NHRP Event Publisher
B. interface state control
C. CAC
D. NHRP Authentication
E. ip nhrp connect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which technology supports tunnel interfaces while remaining compatible with legacy VPN implementations?

A. FlexVPN
B. DMVPN
C. GET VPN
D. SSL VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which IKEv2 feature minimizes the configuration of a FlexVPN on Cisco IOS devices?

A. IKEv2 Suite-B
B. IKEv2 proposals
C. IKEv2 profiles
D. IKEv2 Smart Defaults

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
When an IPsec SVTI is configured, which technology processes traffic forwarding for encryption?

A. ACL
B. IP routing
C. RRI
D. front door VPN routing and forwarding

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
An IOS SSL VPN is configured to forward TCP ports. A remote user cannot access the corporate FTP site with a Web browser. What is a possible reason for the failure?

A. The user's FTP application is not supported.
B. The user is connecting to an IOS VPN gateway configured in Thin Client Mode.
C. The user is connecting to an IOS VPN gateway configured in Tunnel Mode.
D. The user's operating system is not supported.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://www.cisco.com/c/en/us/support/docs/security/ssl-vpn-client/70664-IOSthinclient.html

Thin-Client SSL VPN (Port Forwarding)

A remote client must download a small, Java-based applet for secure access of TCP applications that use static port numbers. UDP is not supported. Examples include access to POP3, SMTP, IMAP, SSH, and Telnet. The user needs local administrative privileges because changes are made to files on the local machine. This method of SSL VPN does not work with applications that use dynamic port assignments, for example, several FTP applications.

QUESTION 50
A Cisco IOS SSL VPN gateway is configured to operate in clientless mode so that users can access file shares on a Microsoft Windows 2003 server. Which protocol is used between the Cisco IOS router and the Windows server?

A. HTTPS
B. NetBIOS
C. CIFS
D. HTTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
You are configuring a Cisco IOS SSL VPN gateway to operate with DVTI support. Which command must you configure on the virtual template?

A. tunnel protection ipsec
B. ip virtual-reassembly