

Cisco VPN Security Specialist 300-209

Implementing Cisco Secure Mobility Solutions (SIMOS)

Thank You for Downloading 300-209 Updated Exam Questions

<https://certs4sale.com/cisco/300-209-pdf-exam-dumps>

Version: 16.0

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

Answer: A, D

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

Answer: A, E

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

Answer: A, B, C, D

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

Answer: A

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

Answer: A

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

Answer: B

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

Answer: A

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.

Answer: B, D, E

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

Answer: C

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

Answer: A, D

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

Answer: A, E, F

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

Answer: B, C

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

Answer: B, C

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

Answer: B

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"

Answer: D

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

Answer: A, B, C

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

Answer: B

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.

Answer: C

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

Answer: C

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

Answer: CD

THANK YOU FOR DOWNLOADING 300-209 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our 300-209 Exam Product

Visit Our Site to Purchase the Full Set of Actual 300-209 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/cisco/300-209-pdf-exam-dumps>