Exam Questions 300-209

SIMOS Implementing Cisco Secure Mobility Solutions (SIMOS)

http://www.2passeasy.com/dumps/300-209/

1. Refer to the exhibit.

```
interface Loopback 10
   ip address 192.0.2.1 255.255.255.0

interface GigabitEthernet 0/0
   description WAN interface
   ip address 10.1.1.1 255.0.0.0

ip nat inside source static 192.0.2.1 10.1.1.2 !
webvpn gateway GATEWAY
   ip address 192.0.2.1 port 443
```

Which VPN solution does this configuration represent?

A. Cisco AnyConnect (IKEv2)

B. site-to-site

C. DMVPN

D. SSL VPN

Answer: D

2. Which technology can you implement to reduce latency issues associated with a Cisco AnyConnect VPN?

A. DTLS

B. SCTP

C. DCCP

D. SRTP

Answer: A

3. Refer to the exhibit.

```
Tunnel-id   Local                 Remote                fvrf/ivrf            Status
1           209.165.202.130/500   209.165.200.230/500   none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/7141 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: C156F9DB2F08AE06       Remote spi: B383BC5A6A805430
      Local id: R002.example.com
      Remote id: R005.example.com
      Local req msg id:  4              Remote req msg id:  3
      Local next msg id: 4              Remote next msg id: 3
      Local req queued:  4              Remote req queued:  3
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not configured.
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Assigned host addr: 10.2.2.10
      Initiator of SA : No
      Remote subnets:
      10.2.2.10 255.255.255.255
```

Which authentication method was used by the remote peer to prove its identity?

A. Extensible Authentication Protocol

B. certificate authentication

C. pre-shared key

D. XAUTH

Answer: C

4. Which three parameters must match on all routers in a DMVPN Phase 3 cloud? (Choose three.)

A. NHRP network ID

B. GRE tunnel key

C. NHRP authentication string

D. tunnel VRF

E. EIGRP process name

F. EIGRP split-horizon setting

Answer: A,B,C

5. Refer to the exhibit.

The customer needs to launch AnyConnect in the RDP machine. Which configuration is correct?

A. crypto vpn anyconnect profile test flash:RDP.xml

policy group default

svc profile test

B. crypto vpn anyconnect profile test flash:RDP.xml

webvpn context GW_1

browser-attribute import flash:/swj.xml

C. crypto vpn anyconnect profile test flash:RDP.xml

policy group default

svc profile flash:RDP.xml

D. crypto vpn anyconnect profile test flash:RDP.xml

webvpn context GW_1

browser-attribute import test

Answer: A

6. Which command clears all crypto configuration from a Cisco Adaptive Security Appliance?

A. clear configure crypto

B. clear configure crypto ipsec

C. clear crypto map

D. clear crypto ikev2 sa

Answer: A

7. 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 with an AnyConnect Premium Peers license can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions.

D. Content rewriter functionality in the Clientless SSL VPN portal is not supported on Apple mobile devices.

E. Clientless SSLVPN provides Layer 3 connectivity into the secured network.

Answer: C,D

8. Which protocol does DTLS use for its transport?

A. TCP

B. UDP

C. IMAP

D. DDE

Answer: B

9. 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

10. 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

11. Remote users want to access internal servers behind an ASA using Microsoft terminal services. Which option outlines the steps required to allow users access via the ASA clientless VPN portal?

A. 1. Configure a static pat rule for TCP port 3389

2. Configure an inbound access-list to allow traffic from remote users to the servers

3. Assign this access-list rule to the group policy

B. 1. Configure a bookmark of the type http:// server-IP :3389

2. Enable Smart tunnel on this bookmark

3. Assign the bookmark to the desired group policy

C. 1. Configure a Smart Tunnel application list

2. Add the rdp.exe process to this list

3. Assign the Smart Tunnel application list to the desired group policy

D. 1. Upload an RDP plugin to the ASA

2. Configure a bookmark of the type rdp:// server-IP

3. Assign the bookmark list to the desired group policy

Answer: D

12. Which technology is FlexVPN based on?

A. OER

B. VRF

C. IKEv2

D. an RSA nonce

Answer: C

13. Refer to the exhibit.

```
crypto ikev2 keyring KR1
 peer ALL
  address ::/0
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
```

What technology does the given configuration demonstrate?

A. Keyring used to encrypt IPSec traffic

B. FlexVPN with IPV6

C. FlexVPN with AnyConnect

D. Crypto Policy to enable IKEv2

Answer: B

14. An administrator wishes to limit the networks reachable over the Anyconnect VPN tunnels. Which configuration on the ASA will correctly limit the networks reachable to 209.165.201.0/27 and 209.165.202.128/27?

A. access-list splitlist standard permit 209.165.201.0 255.255.255.224

access-list splitlist standard permit 209.165.202.128 255.255.255.224

!

group-policy GroupPolicy1 internal

group-policy GroupPolicy1 attributes

split-tunnel-policy tunnelspecified

split-tunnel-network-list value splitlist

B. access-list splitlist standard permit 209.165.201.0 255.255.255.224

access-list splitlist standard permit 209.165.202.128 255.255.255.224

!

group-policy GroupPolicy1 internal

group-policy GroupPolicy1 attributes

split-tunnel-policy tunnelall

split-tunnel-network-list value splitlist

C. group-policy GroupPolicy1 internal

group-policy GroupPolicy1 attributes

split-tunnel-policy tunnelspecified

split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224

split-tunnel-network-list ipv4 2 209.165.202.128 255.255.255.224

D. access-list splitlist standard permit 209.165.201.0 255.255.255.224

access-list splitlist standard permit 209.165.202.128 255.255.255.224

!

crypto anyconnect vpn-tunnel-policy tunnelspecified

crypto anyconnect vpn-tunnel-network-list splitlist

E. crypto anyconnect vpn-tunnel-policy tunnelspecified

crypto anyconnect split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224

crypto anyconnect split-tunnel-network-list ipv4 2 209.165.202.128 255.255.255.224

Answer: A

15. Refer to the exhibit.

```
interface Tunnel12
 ip address 172.16.16.5 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast 10.10.10.1
 ip nhrp map multicast 20.20.20.1
 ip nhrp map 172.16.16.1 10.10.10.1
 ip nhrp map 172.16.16.3 20.20.20.1
 ip nhrp network-id 12
 ip nhrp nhs 172.16.16.1
 ip nhrp nhs 172.16.16.3
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 ip ospf dead-interval 9
 ip ospf hello-interval 3
 ip ospf cost 1100
 load-interval 30
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 12
 tunnel protection ipsec profile TUNNEL-12
end
```

Which two characteristics of the VPN implementation are evident? (Choose two.)

A. dual DMVPN cloud setup with dual hub

B. DMVPN Phase 3 implementation

C. single DMVPN cloud setup with dual hub

D. DMVPN Phase 1 implementation

E. quad DMVPN cloud with quadra hub

F. DMVPN Phase 2 implementation

Answer: B,C

16. 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

Answer: B

17. 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

Answer: C

18. 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.

Answer: B

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.

19. 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

Answer: A

20. Refer to the exhibit.

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 14463, #pkts decrypt: 14463, #pkts verify: 14463
#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
```

You executed the show crypto ipsec sa command to troubleshoot an IPSec issue. What problem does the given output indicate?

A. IKEv2 failed to establish a phase 2 negotiation.

B. The Crypto ACL is different on the peer device.

C. ISAKMP was unable to find a matching SA.

D. IKEv2 was used in aggressive mode.

Answer: B

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-209 Product From:

http://www.2passeasy.com/dumps/300-209/

Money Back Guarantee

300-209 Practice Exam Features:

* 300-209 Questions and Answers Updated Frequently

* 300-209 Practice Questions Verified by Expert Senior Certified Staff

* 300-209 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-209 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year