

Exam Questions 300-209

SIMOS Implementing Cisco Secure Mobility Solutions (SIMOS)

<https://www.2passeasy.com/dumps/300-209/>



NEW QUESTION 1

- (Exam Topic 1)

A customer requires site-to-site VPNs to connect to third party business partners and has purchased two ASAs. The customer requests an active/active configuration.

Winch mode is needed to support and active/active solution?

- A. single context
- B. NAT context
- C. PAT context
- D. multiple context

Answer: D

NEW QUESTION 2

- (Exam Topic 1)

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

Answer: AB

NEW QUESTION 3

- (Exam Topic 1)

What is the Cisco recommended TCP maximum segment on a DMVPN tunnel interface when the MTU is set to 1400 bytes?

- A. 1160 bytes
- B. 1260 bytes
- C. 1360 bytes
- D. 1240 bytes

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

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

- A. to distributed static routing information
- B. to authenticate group members
- C. to define and distribute security policies
- D. to distribute dynamic routing information
- E. to encrypt transit data traffic.

Answer: BE

NEW QUESTION 5

- (Exam Topic 1)

In DMVPN phase 2, which two EIGRP features need to be disabled on the hub to allow spoke-to-spoke communication? (Choose two.)

- A. autosummary
- B. split horizon
- C. metric calculation using bandwidth
- D. EIGRP address family
- E. next-hop-self
- F. default administrative distance

Answer: BE

NEW QUESTION 6

- (Exam Topic 1)

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
- C. tunnel mode ipsec
- D. ip unnumbered

Answer: D

NEW QUESTION 7

- (Exam Topic 1)

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: BC

NEW QUESTION 8

- (Exam Topic 1)

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

Answer: A

Explanation:

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-11>

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.

NEW QUESTION 9

- (Exam Topic 1)

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

Answer: AB

NEW QUESTION 10

- (Exam Topic 1)

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 tunnelspecifiedsplit-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 tunnelallsplit-tunnel-network-list value splitlist
- C. group-policy GroupPolicy1 internal group-policy GroupPolicy1 attributes split-tunnel-policy tunnelspecifiedsplit-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224split-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 tunnelspecifiedcrypto anyconnect split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224crypto anyconnect split-tunnel-network-list ipv4 2 209.165.202.128 255.255.255.224

Answer: A

NEW QUESTION 11

- (Exam Topic 1)

When you configure IPsec VPN High Availability Enhancements, which technology does Cisco recommend that you enable to make reconvergence faster?

- A. EOT
- B. IP SLAs
- C. periodic IKE keepalives
- D. VPN fast detection

Answer: C

NEW QUESTION 12

- (Exam Topic 1)

Refer to the Exhibit:

```
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
 authentication local pre-shared-key flexvpn
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
```

Which statement is accurate based on 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 1 passes the authentication to the hub and successfully proceeds to phase 2.
- D. Spoke 2 fails the authentication because the remote authentication method is incorrect.

Answer: C

NEW QUESTION 13

- (Exam Topic 2)

What does NHRP stand for?

- A. Next Hop Resolution Protocol
- B. Next Hop Registration Protocol
- C. Next Hub Routing Protocol
- D. Next Hop Routing Protocol

Answer: A

NEW QUESTION 14

- (Exam Topic 2)

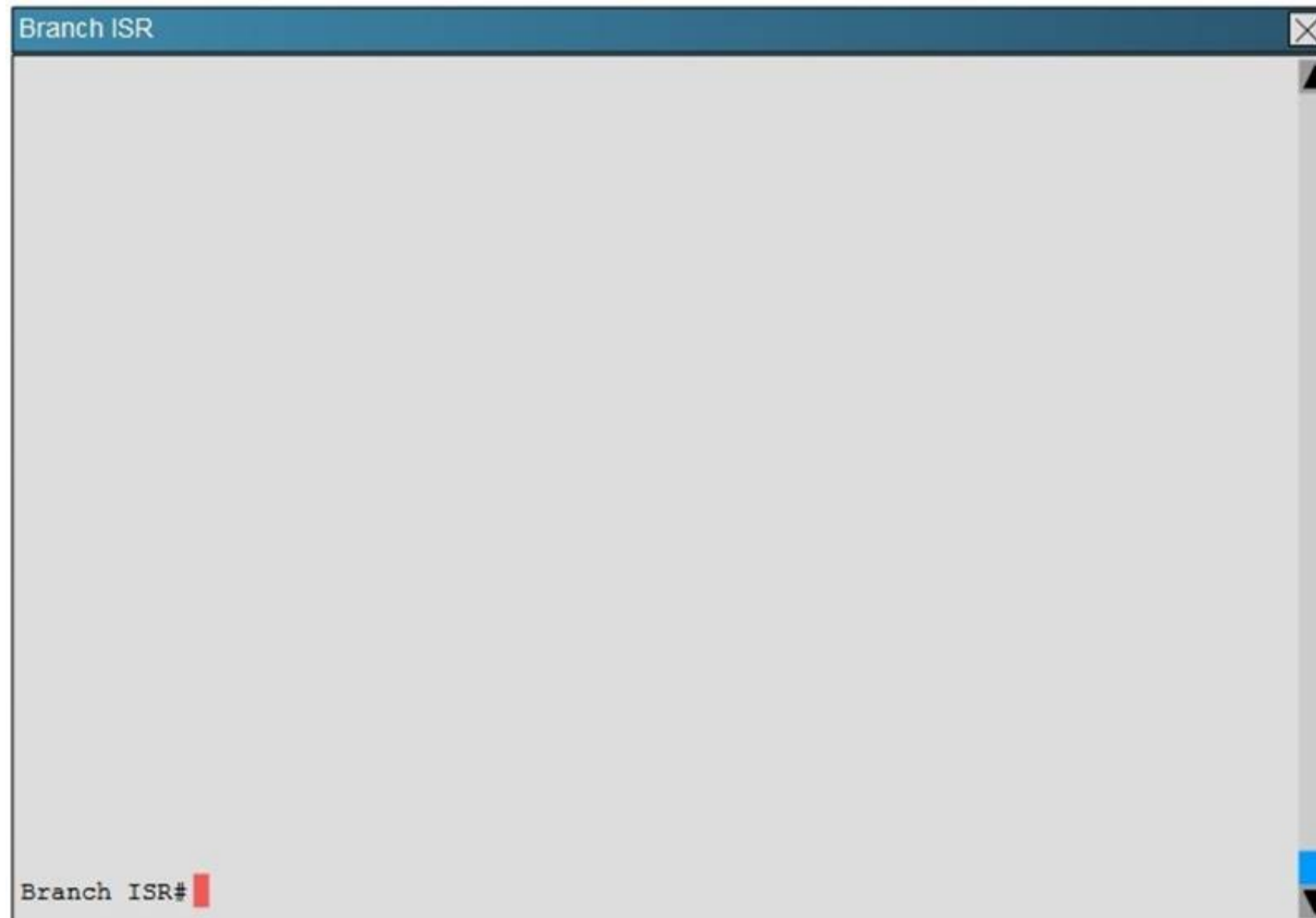
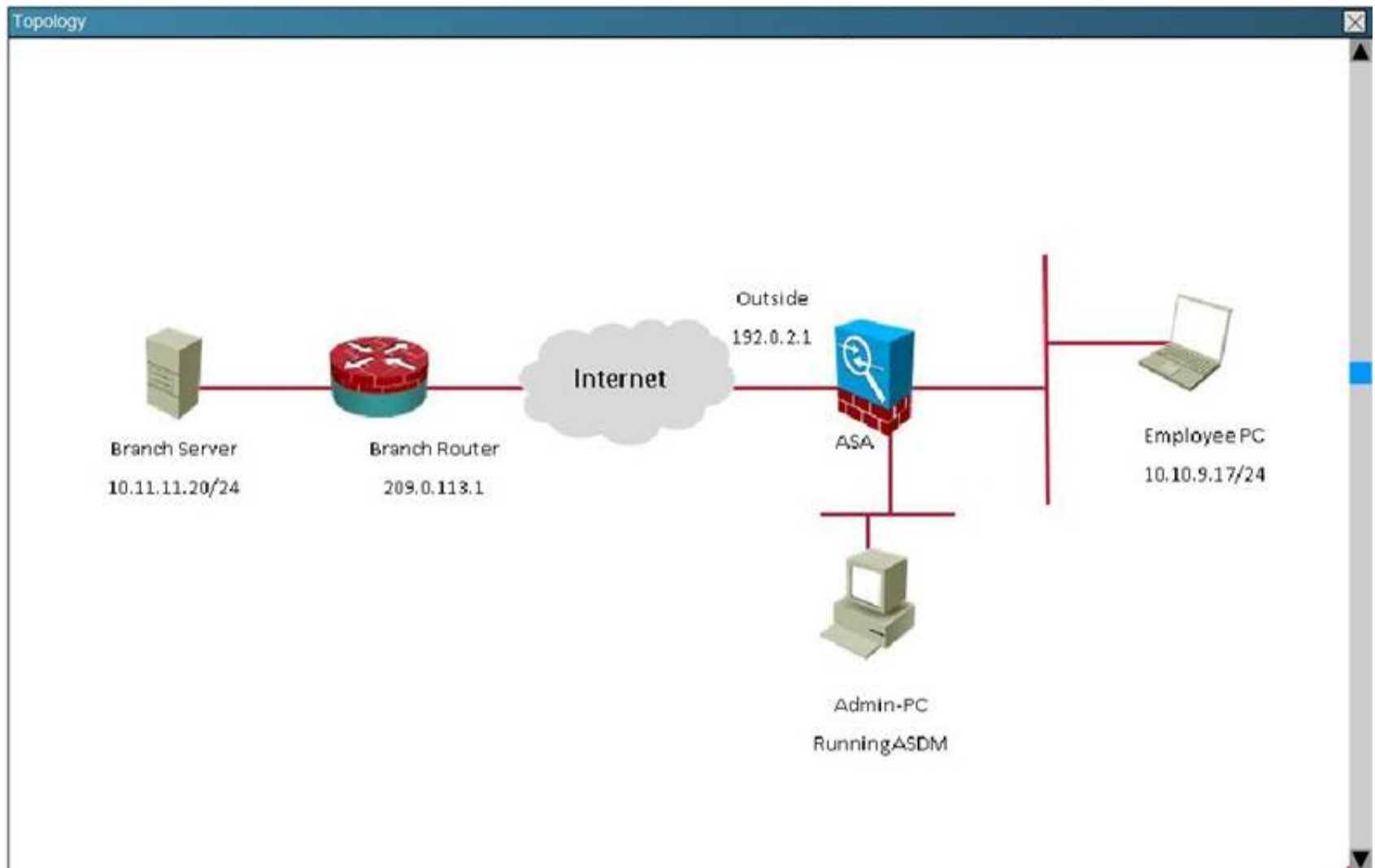
Scenario:

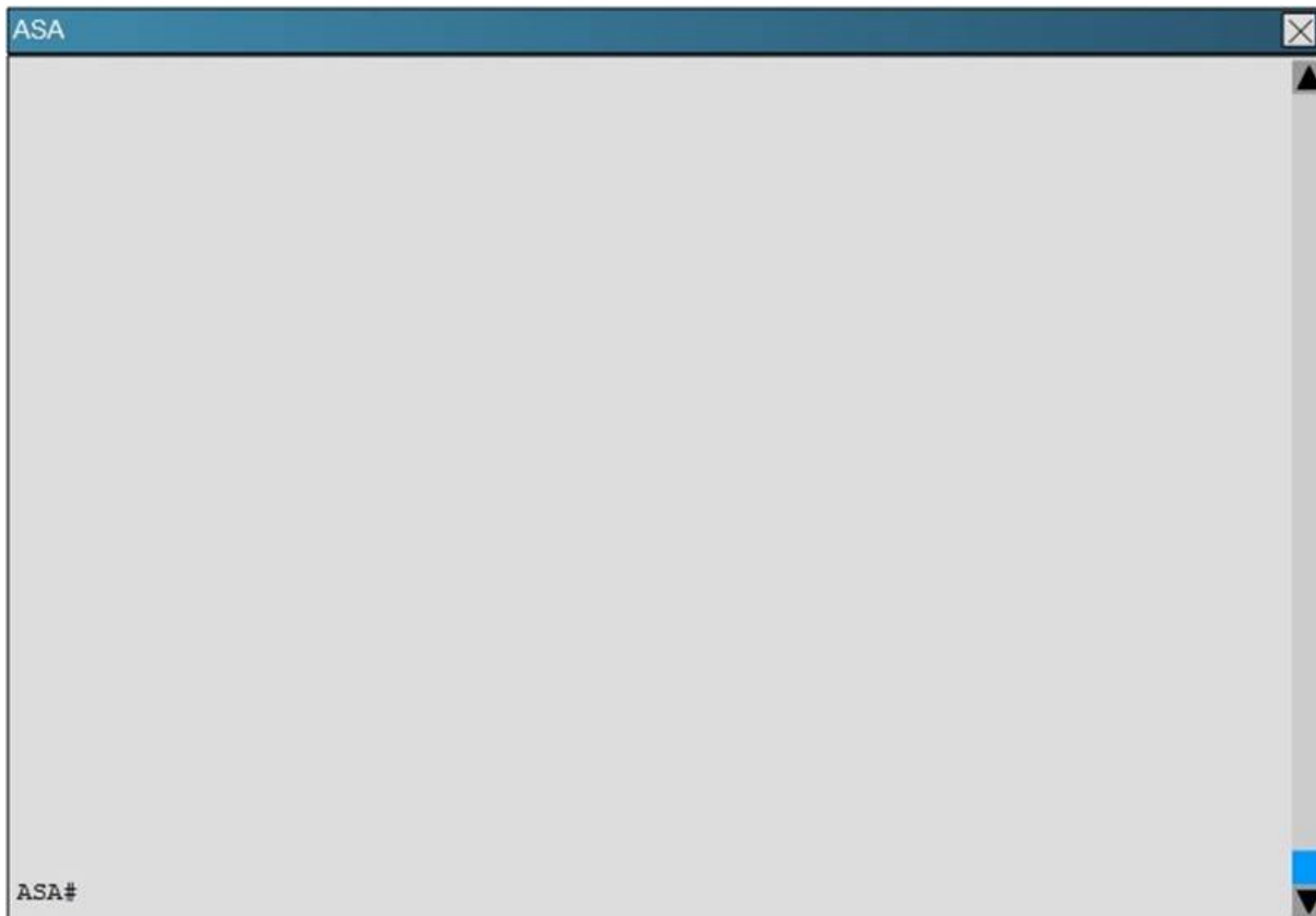
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

You are now tasked with verifying the IKEv1 IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.

NOTE: the show running-config command cannot be used for this exercise.

Topology:





In what state is the IKE security association in on the Cisco ASA?

- A. There are no security associations in place
- B. MM_ACTIVE
- C. ACTIVE(ACTIVE)
- D. QM_IDLE

Answer: B

Explanation:

This can be seen from the "show crypto isa sa" command:

```
ASA#show crypto isa sa
IKEv1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 203.0.113.1
   Type    : L2L           Role    : responder
   Rekey   : no           State   : MM_ACTIVE

There are no IKEv2 SAs
```

NEW QUESTION 15

- (Exam Topic 2)

Which VPN feature allows remote access clients to print documents to local network printers?

- A. Reverse Route Injection
- B. split tunneling
- C. loopback addressing
- D. dynamic virtual tunnels

Answer: B

NEW QUESTION 16

- (Exam Topic 2)

On which Cisco platform are dynamic virtual template interfaces available?

- A. Cisco Adaptive Security Appliance 5585-X
- B. Cisco Catalyst 3750X
- C. Cisco Integrated Services Router Generation 2

D. Cisco Nexus 7000

Answer: C

NEW QUESTION 17

- (Exam Topic 2)

Refer to the exhibit.

```
crypto ikev2 proposal PROP
  encryption aes-cbc-128
  integrity sha256
  group 20

crypto ikev2 policy IKEV2_POLICY
  match address local 10.1.1.2
  proposal PROP

crypto ikev2 keyring KEYRING
  peer spokes
  address 10.0.0.0 255.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123

crypto ikev2 profile PROFILE_IKEV2
  match identity remote address 10.0.0.0 255.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local KEYRING
  aaa authorization group psk list default default
  virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto ipsec transform-set TRANSFORM_IPSEC esp-gcm
  mode transport

crypto ipsec profile PROFILE_IPSEC
  set transform-set TRANSFORM_IPSEC
  set ikev2-profile PROFILE_IKEV2

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback100
  tunnel path-mtu-discovery
  tunnel protection ipsec profile PROFILE_IPSEC
```

Which VPN solution does this configuration represent?

- A. DMVPN
- B. GETVPN
- C. FlexVPN
- D. site-to-site

Answer: C

NEW QUESTION 18

- (Exam Topic 3)

Using the Next Generation Encryption technologies, which is the minimum acceptable encryption level to protect sensitive information?

- A. AES 92 bits
- B. AES 128 bits
- C. AES 256 bits
- D. AES 512 bits

Answer: C

NEW QUESTION 19

- (Exam Topic 3)

Which two changes must be made to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two)

- A. Disable EIGRP next-hop-self on the hub.
- B. Enable EIGRP next-hop-self on the hub.
- C. Acid NHRP shortcuts on the hub.
- D. Add NHRP redirects on the hub.
- E. Add NHRP redirects on the spoke.

Answer: BD

NEW QUESTION 20

From the CLI of a Cisco ASA 5520, which command shows specific information about current clientless and Cisco Anyconnect SSL VPN users only?

- A. show crypto ikve1 sa detail

- B. show vpn-sessiondb remote
- C. show vpn-sessiondb
- D. show von-sessiondb detail

Answer: D

NEW QUESTION 21

.....

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:

<https://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