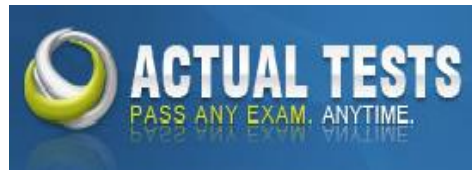


Cisco.Certkey.300-209.v2014-06-26.by.HEATHER.74q

Number: 300-209
Passing Score: 800
Time Limit: 120 min
File Version: 18.5



Exam Name: Implementing Cisco Secure Mobility Solutions (SIMOS)



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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:**

Explanation:

QUESTION 17

A network is configured to allow client less 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:**

Explanation:

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:**

Explanation:

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: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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 1234 192.168.1.3 161 to see what the firewall is doing with the user's traffic

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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 128
- F. crypto isakmp policy 10
encryption aes 64

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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
- C. tunnel mode ipsec
- D. ip unnumbered

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 52

Which protocol supports high availability in a Cisco IOS SSL VPN environment?

- A. HSRP
- B. VRRP
- C. GLBP
- D. IRDP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 53

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 54

Which hash algorithm is required to protect classified information?

- A. MD5
- B. SHA-1
- C. SHA-256
- D. SHA-384

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 55

Which cryptographic algorithms are approved to protect Top Secret information?

- A. HIPPA DES
- B. AES-128
- C. RC4-128
- D. AES-256

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 56

Which Cisco firewall platform supports Cisco NGE?

- A. FWSM
- B. Cisco ASA 5505
- C. Cisco ASA 5580
- D. Cisco ASA 5525-X

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 57

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

- A. 3DES
- B. AES
- C. DES
- D. RSA

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 58

Which encryption and authentication algorithms does Cisco recommend when deploying a Cisco NGE supported VPN solution?

- A. AES-GCM and SHA-2
- B. 3DES and DH
- C. AES-CBC and SHA-1
- D. 3DES and SHA-1

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 59

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 60

Which NGE IKE Diffie-Hellman group identifier has the strongest cryptographic properties?

- A. group 20
B. group 24
C. group 5
D. group 20

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 61

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 62

Which technology does a multipoint GRE interface require to resolve endpoints?

- A. ESP
- B. dynamic routing
- C. NHRP
- D. CEF
- E. IPSec

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 63

Which two cryptographic technologies are recommended for use with FlexVPN? (Choose two.)

- A. SHA (HMAC variant)
- B. Diffie-Hellman
- C. DES
- D. MD5 (HMAC variant)

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 64

Which command configures IKEv2 symmetric identity authentication?

- A. match identity remote address 0.0.0.0
- B. authentication local pre-share
- C. authentication pre-share
- D. authentication remote rsa-sig

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 65

Which two examples of transform sets are contained in the IKEv2 default proposal? (Choose two.)

- A. aes-cbc-192, sha256, 14
- B. 3des, md5, 5
- C. 3des, sha1, 1
- D. aes-cbc-128, sha, 5

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 66

What is the default storage location of user-level bookmarks in an IOS clientless SSL VPN?

- A. disk0:/webvpn/{context name}/
- B. disk1:/webvpn/{context name}/
- C. flash:/webvpn/{context name}/
- D. nvram:/webvpn/{context name}/

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 67

Which command will prevent a group policy from inheriting a filter ACL in a clientless SSL VPN?

- A. vpn-filter none
- B. no vpn-filter
- C. filter value none
- D. filter value ACLname

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 68

Which command specifies the path to the Host Scan package in an ASA AnyConnect VPN?

- A. csd hostscan path image
- B. csd hostscan image path
- C. csd hostscan path
- D. hostscan image path

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 69

Instructions

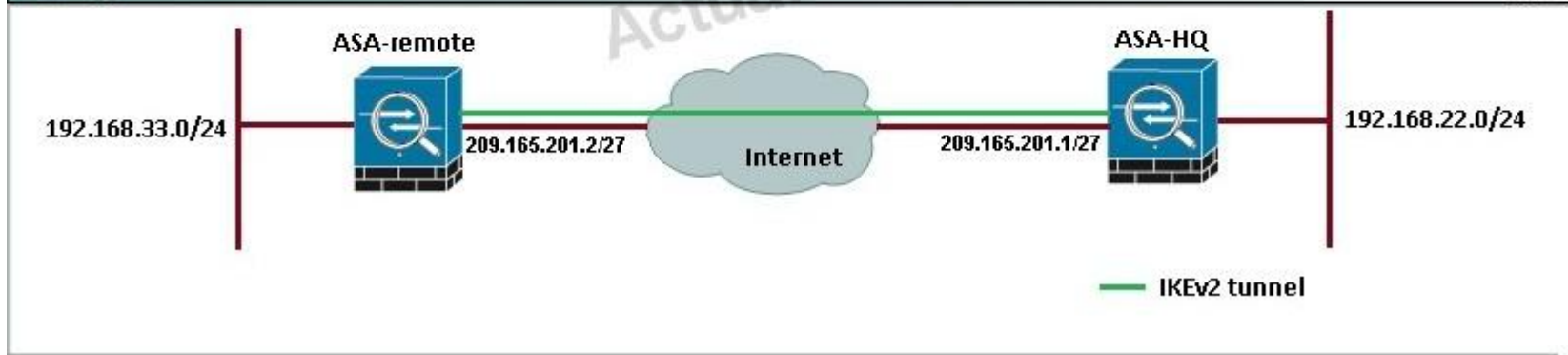
Click the grey buttons at the bottom of this frame to view the different windows.

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

Scenario

A network administrator has been tasked with implementing an IKEv2 tunnel from a remote site to a headquarter site. For security reasons, all traffic from the remote site must be sent across the tunnel, including traffic destined to the internet. Both sites are using a Cisco ASA firewall and are capable of running IKEv2.

Topology



ASDM-HQ

File View Tools Wizards Window Help Look For:

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

- Connection Profiles
- Group Policies
- Certificate Management
- Advanced
 - Tunnel Groups
 - Crypto Maps
 - IKE Policies
 - IKE Parameters
 - IPsec Proposals (Transform Sets)
 - IPsec Prefragmentation Policies
 - Certificate to Connection Profile Maps
 - Policy
 - Rules
 - System Options
 - ACL Manager

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IK
209.165.201.2	outside	192.168.22.0/24	192.168.33.0/24	<input type="checkbox"/>	

ASDM-Remote

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

- Connection Profiles
- Group Policies
- Certificate Management
- Advanced
 - Tunnel Groups
 - Crypto Maps
 - IKE Policies
 - IKE Parameters
 - IPsec Proposals (Transform Sets)
 - IPsec Prefragmentation Policies
 - Certificate to Connection Profile Maps
 - System Options
 - ACL Manager

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted.

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled
209.165.201.1	outside	192.168.33.0/24	any	<input type="checkbox"/>	<input type="checkbox"/>

When a tunnel is initiated by the headquarter ASA, which one of the following Diffie-Hellman groups is selected by the headquarter ASA during CREATE_CHILD_SA exchange?

A. 1

- B. 2
- C. 5
- D. 14
- E. 19

Correct Answer: C

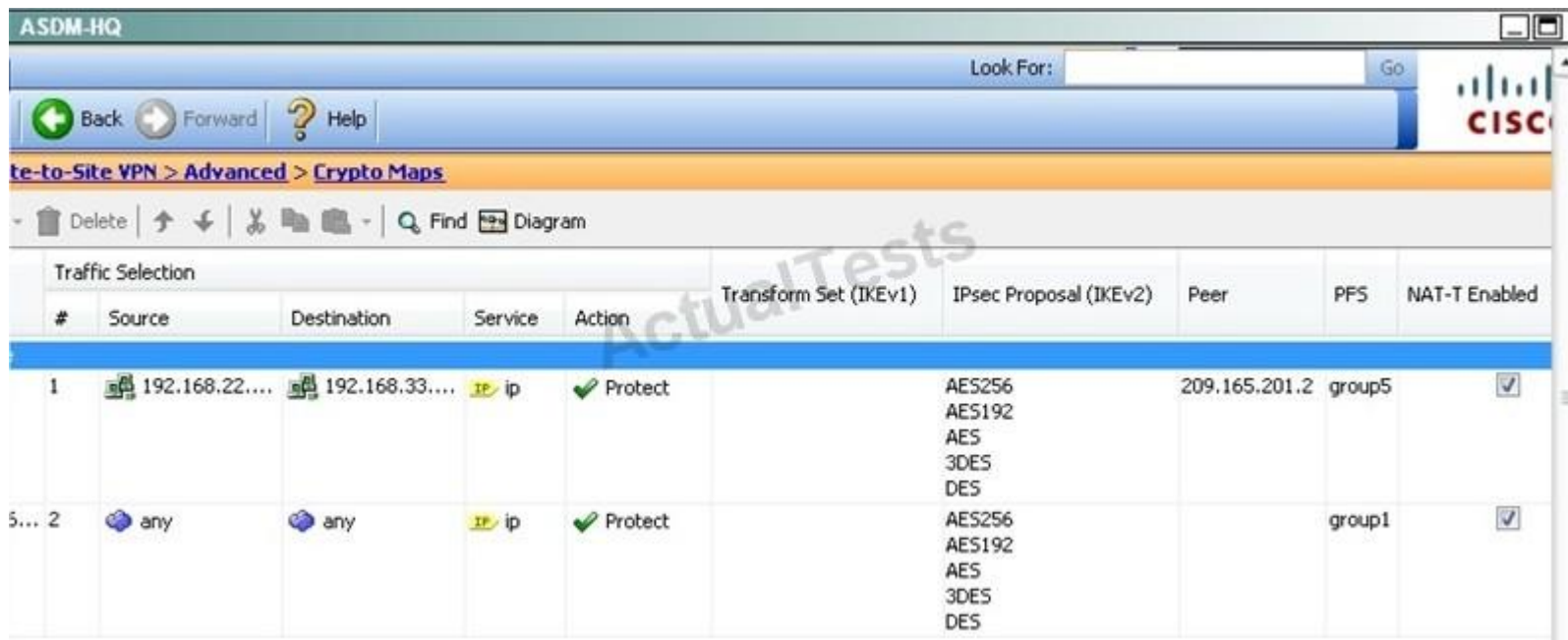
Section: (none)

Explanation

Explanation/Reference:

Explanation:

Traffic initiated by the HQ ASA is assigned to the static outside crypto map, which shown below to use DH group 5.



Traffic Selection									
#	Source	Destination	Service	Action	Transform Set (IKEv1)	IPsec Proposal (IKEv2)	Peer	PFS	NAT-T Enabled
1	192.168.22.0/24	192.168.33.0/24	IP ip	Protect		AES256 AES192 AES 3DES DES	209.165.201.2	group5	<input checked="" type="checkbox"/>
2	any	any	IP ip	Protect		AES256 AES192 AES 3DES DES		group1	<input checked="" type="checkbox"/>

QUESTION 70

Instructions

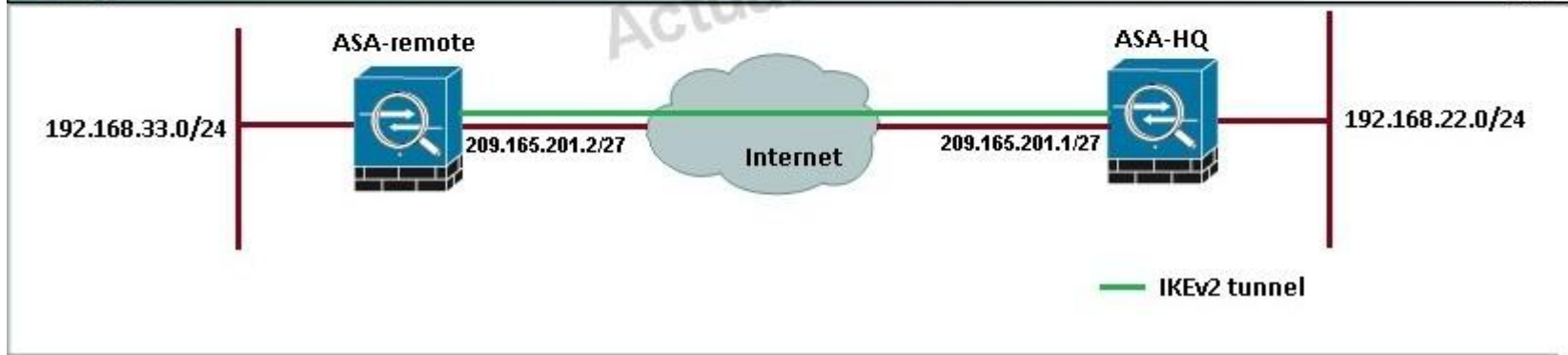
Click the grey buttons at the bottom of this frame to view the different windows.

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

Scenario

A network administrator has been tasked with implementing an IKEv2 tunnel from a remote site to a headquarter site. For security reasons, all traffic from the remote site must be sent across the tunnel, including traffic destined to the internet. Both sites are using a Cisco ASA firewall and are capable of running IKEv2.

Topology



ASDM-HQ

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IK
209.165.201.2	outside	192.168.22.0/24	192.168.33.0/24	<input type="checkbox"/>	

ASDM-Remote

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

- Connection Profiles
- Group Policies
- Certificate Management
- Advanced
 - Tunnel Groups
 - Crypto Maps
 - IKE Policies
 - IKE Parameters
 - IPsec Proposals (Transform Sets)
 - IPsec Prefragmentation Policies
 - Certificate to Connection Profile Maps
 - System Options
 - ACL Manager

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted.

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled
209.165.201.1	outside	192.168.33.0/24	any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Based on the provided ASDM configuration for the remote ASA, which one of the following is correct?

- A. An access-list must be configured on the outside interface to permit inbound VPN traffic
- B. A route to 192.168.22.0/24 will not be automatically installed in the routing table

- C. The ASA will use a window of 128 packets (64x2) to perform the anti-replay check _
- D. The tunnel can also be established on TCP port 10000

Correct Answer: C

Section: (none)

Explanation

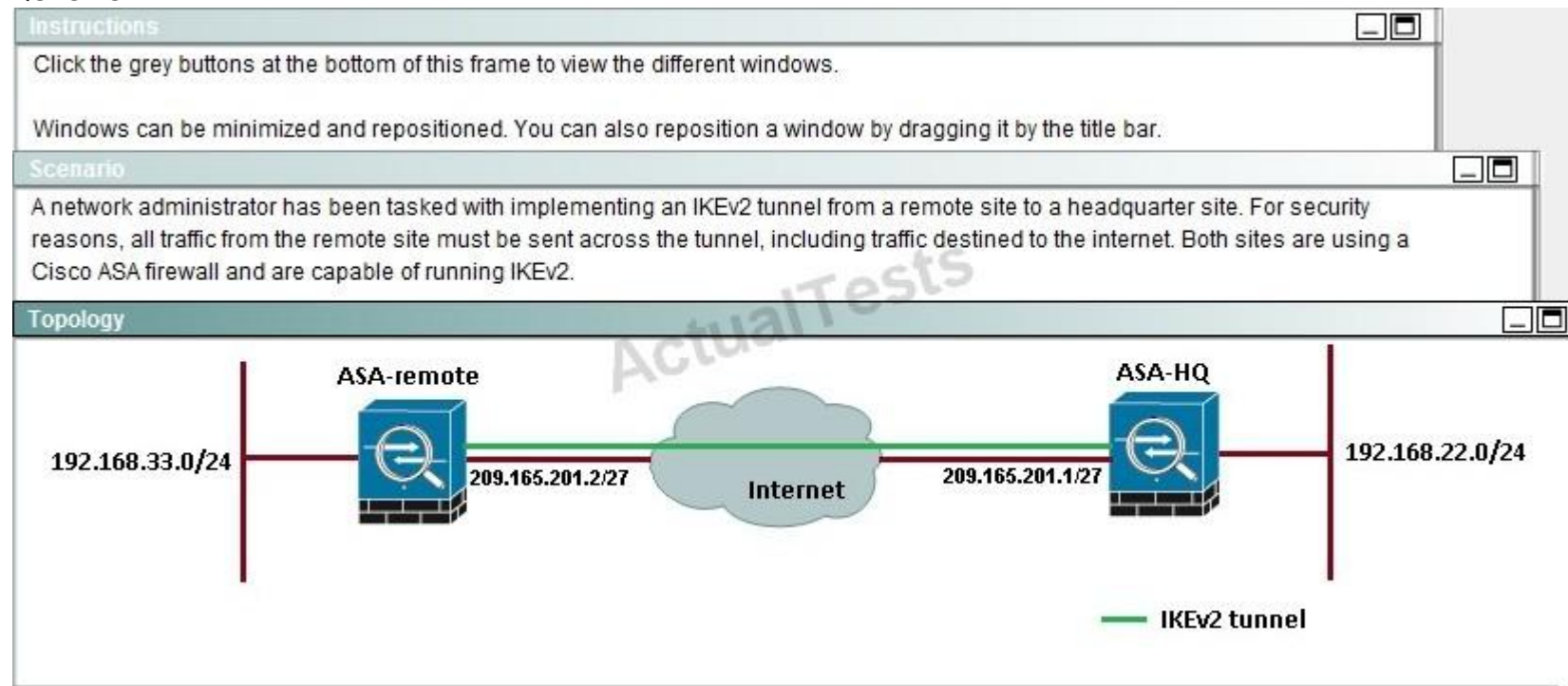
Explanation/Reference:

Explanation:

Cisco IP security (IPsec) authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. Currently, the default window size is 64 packets. Generally, this number (window size) is sufficient, but there are times when you may want to expand this window size. The IPsec Anti-Replay Window:

Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

QUESTION 71



ASDM-HQ

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IK
209.165.201.2	outside	192.168.22.0/24	192.168.33.0/24	<input type="checkbox"/>	

ASDM-Remote

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

- Connection Profiles
- Group Policies
- Certificate Management
- Advanced
 - Tunnel Groups
 - Crypto Maps
 - IKE Policies
 - IKE Parameters
 - IPsec Proposals (Transform Sets)
 - IPsec Prefragmentation Policies
 - Certificate to Connection Profile Maps
 - System Options
 - ACL Manager

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted.

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled
209.165.201.1	outside	192.168.33.0/24	any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

If the IKEv2 tunnel were to establish successfully, which encryption algorithm would be used to encrypt traffic?

- A. DES
- B. 3DES

- C. AES
- D. AES192
- E. AES256

Correct Answer: E

Section: (none)

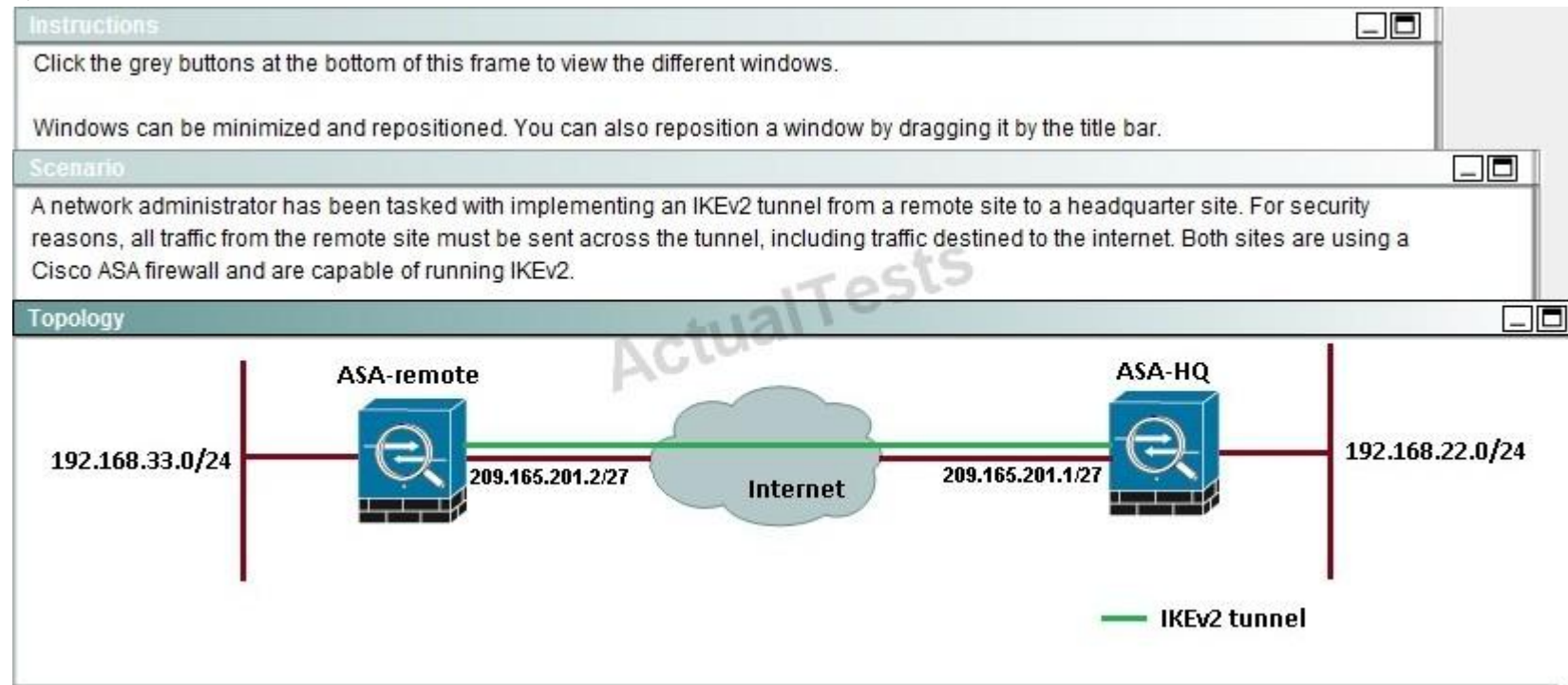
Explanation

Explanation/Reference:

Explanation:

Both ASA's are configured to support AES 256, so during the IPsec negotiation they will use the strongest algorithm that is supported by each peer.

QUESTION 72



ASDM-HQ

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IK
209.165.201.2	outside	192.168.22.0/24	192.168.33.0/24	<input type="checkbox"/>	

ASDM-Remote

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

- Connection Profiles
- Group Policies
- Certificate Management
- Advanced
 - Tunnel Groups
 - Crypto Maps
 - IKE Policies
 - IKE Parameters
 - IPsec Proposals (Transform Sets)
 - IPsec Prefragmentation Policies
 - Certificate to Connection Profile Maps
 - System Options
 - ACL Manager

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted.

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled
209.165.201.1	outside	192.168.33.0/24	any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

After implementing the IKEv2 tunnel, it was observed that remote users on the 192.168.33.0/24 network are unable to access the internet. Which of the following can be done to resolve this problem?

- A. Change the Diffie-Hellman group on the headquarter ASA to group5forthe dynamic crypto map

- B. Change the remote traffic selector on the remote ASA to 192.168.22.0/24
- C. Change to an IKEv1 configuration since IKEv2 does not support a full tunnel with static peers
- D. Change the local traffic selector on the headquarter ASA to 0.0.0.0/0
- E. Change the remote traffic selector on the headquarter ASA to 0.0.0.0/0

Correct Answer: B

Section: (none)

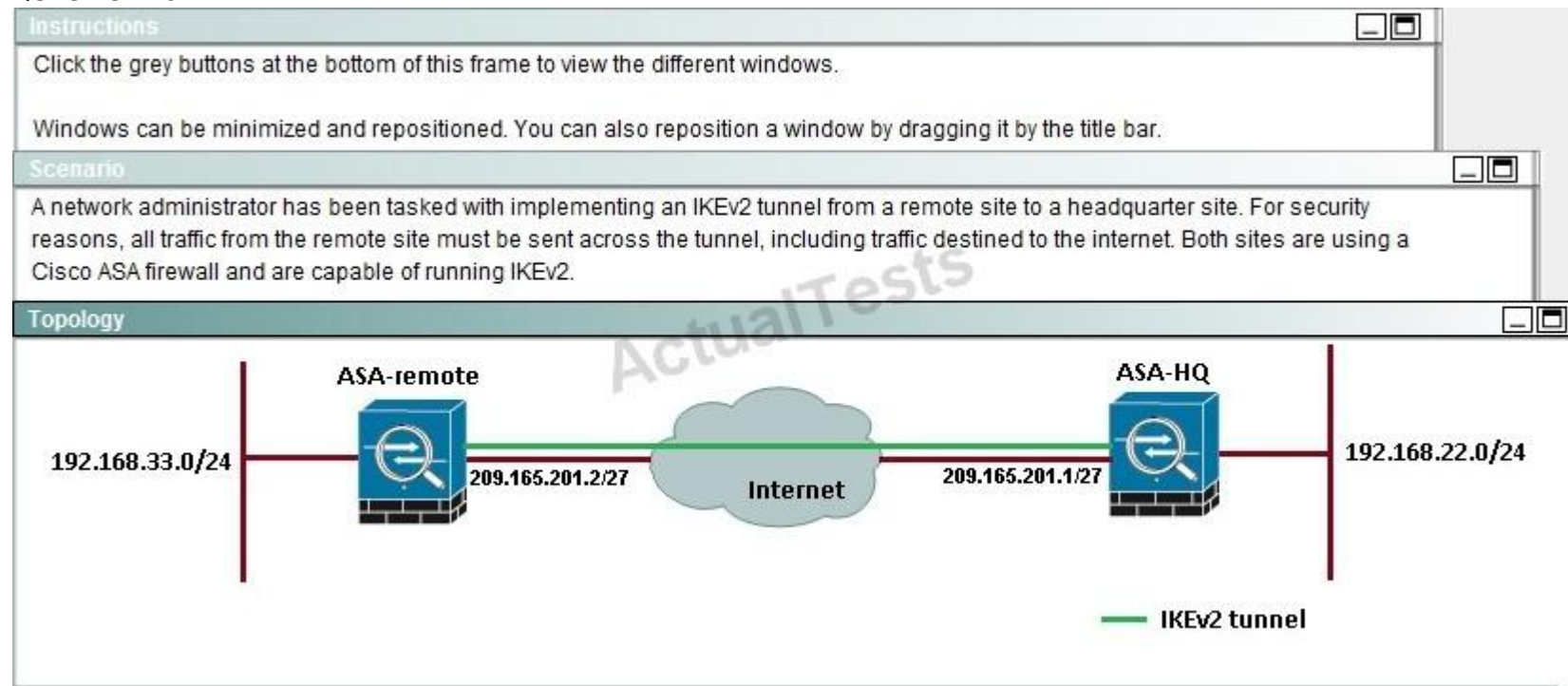
Explanation

Explanation/Reference:

Explanation:

The traffic selector is used to determine which traffic should be protected (encrypted over the IPSec tunnel). We want this to be specific, otherwise Internet traffic will also be sent over the tunnel and most likely dropped on the remote side. Here, we just want to protect traffic from 192.168.33.0/24 to 192.168.22.0/24.

QUESTION 73



ASDM-HQ

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IK
209.165.201.2	outside	192.168.22.0/24	192.168.33.0/24	<input type="checkbox"/>	

ASDM-Remote

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted.

+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled
209.165.201.1	outside	192.168.33.0/24	any	<input type="checkbox"/>	<input type="checkbox"/>

Which option shows the correct traffic selectors for the child SA on the remote ASA, when the headquarter ASA initiates the tunnel?

- Local selector 192.168.33.0/0-192.168.33.255/65535 Remote selector 192.168.20.0/0- 192.168.20.255/65535
- Local selector 192.168.33.0/0-192.168.33.255/65535 Remote selector 192.168.22.0/0- 192.168.22.255/65535

- Local selector 192.168.22.0/0-192.168.22.255/65535 Remote selector 192.168.33.0/0- 192.168.33.255/65535

- Local selector 0.0.0.0/0 - 0.0.0.0/65535 Remote selector 192.168.22.0/0 -192.168.22.255/65535

- A. Local selector 192.168.33.0/0-192.168.33.255/65535
Remote selector 192.168.20.0/0- 192.168.20.255/65535
- B. Local selector 192.168.33.0/0-192.168.33.255/65535
Remote selector 192.168.22.0/0- 192.168.22.255/65535
- C. Local selector 192.168.22.0/0-192.168.22.255/65535
Remote selector 192.168.33.0/0- 192.168.33.255/65535
- D. Local selector 0.0.0.0/0 - 0.0.0.0/65535
Remote selector 192.168.22.0/0 -192.168.22.255/65535

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: The traffic selector is used to determine which traffic should be protected (encrypted over the IPSec tunnel). We want this to be specific, otherwise Internet traffic will also be sent over the tunnel and most likely dropped on the remote side. Here, we just want to protect traffic from 192.168.33.0/24 (THE LOCAL SIDE) to 192.168.22.0/24 (THE REMOTE SIDE).

QUESTION 74

CORRECT TEXT

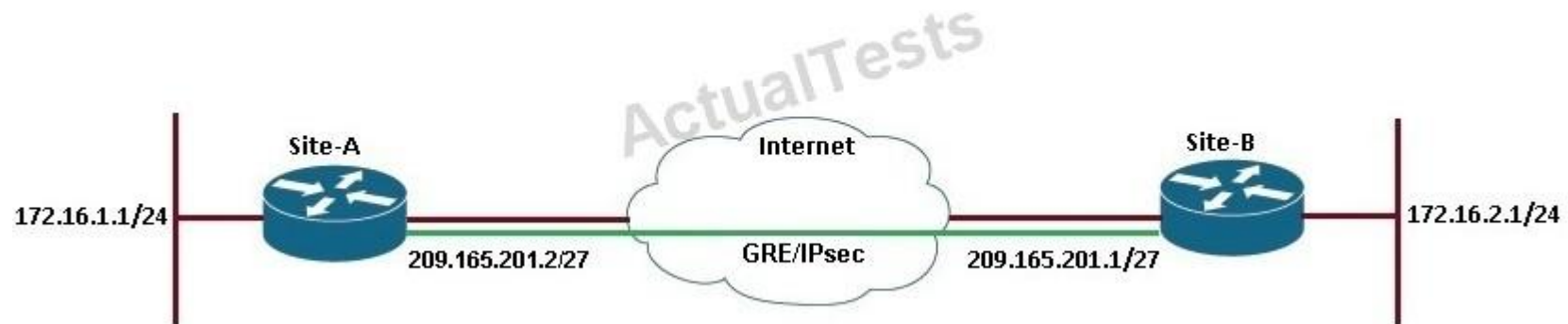
Scenario

As a network administrator you are tasked with configuring a FlexVPN site-to-site GRE/IPsec tunnel. The two sites use Cisco IOS routers and support the FlexVPN framework. The router at Site B is preconfigured. You must use the IKEv2 configuration blocks to accomplish this task.

- Configure a point-to-point GRE tunnel on the router and use interface Ethernet0/0 as the tunnel source (Use tunnel 0 for this purpose). Configure 10.1.1.1/24 as the IP address on the tunnel interface. Verify that you are able to ping across the GRE tunnel
- Configure an IKEv2 proposal, and make sure that the tunnel uses the following parameters:
 - Encryption algorithm: **AES 128**
 - Integrity algorithm: **SHA1**
 - Diffie-Hellman group: **5**
- Configure an IKEv2 key ring, with the local pre-shared key **SiteA** and remote pre-shared key **SiteB**.
- Configure an IKEv2 profile for pre-shared key authentication. Make sure that you use the FQDN **SiteA.cisco.com** as the local IKE identity of the router. The peer router is configured to send an identity of **SiteB.cisco.com**.
- Create an IPsec profile named **default**. Reference the IKEv2 profile in the IPsec profile.
- Enable encryption on the GRE tunnel, and do not use a crypto map. Verify that the IKEv2 tunnel is up and passing traffic by making sure that you can ping across the tunnel. Use show commands to verify that the tunnel is using the correct encryption and integrity algorithms and that traffic is encrypted/decrypted.

"Pass Any Exam. Any Time." - www.actualtests.com 34 Cisco 300-209 Exam

Topology




```
Flex-SiteA

ActualTests

%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
%LINK-3-UPDOWN: Interface Ethernet0/1, changed state to administratively down
%LINK-3-UPDOWN: Interface Ethernet0/2, changed state to administratively down
%LINK-3-UPDOWN: Interface Ethernet0/3, changed state to administratively down
Press RETURN to get started!
Flex-SiteA>
```

- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Answer: Here are the steps as below:

Step 1: configure key ring

crypto ikev2 keyring mykeys

peer SiteB.cisco.com

```
address 209.161.201.1
pre-shared-key local $iteA
pre-shared key remote $iteB
Step 2: Configure IKEv2 profile
Crypto ikev2 profile default
identity local fqdn SiteA.cisco.com
Match identity remote fqdn SiteB.cisco.com
Authentication local pre-share
Authentication remote pre-share
```

```
Keyring local mykeys
Step 3: Create the GRE Tunnel and apply profile
crypto ipsec profile default
set ikev2-profile default
Interface tunnel 1
ip address 10.1.1.1
Tunnel source eth 0/0
Tunnel destination 209.165.201.1
tunnel protection ipsec profile default
end
```