



Cisco

Exam Questions 300-209

Implementing Cisco Secure Mobility Solutions (SIMOS)

NEW QUESTION 1

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

Answer: AB

NEW QUESTION 2

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.

Which mode is needed to support an active/active solution?

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

Answer: D

NEW QUESTION 3

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.

Answer: DE

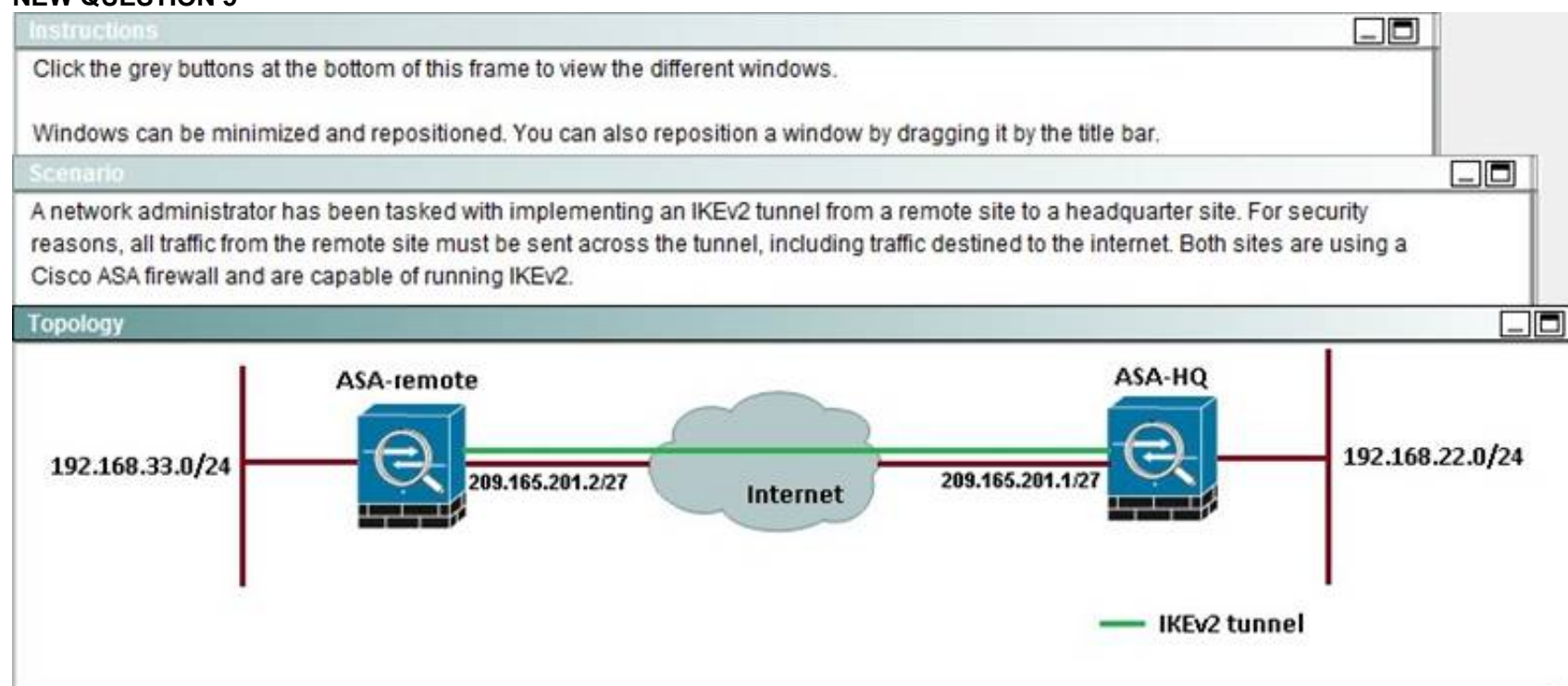
NEW QUESTION 4

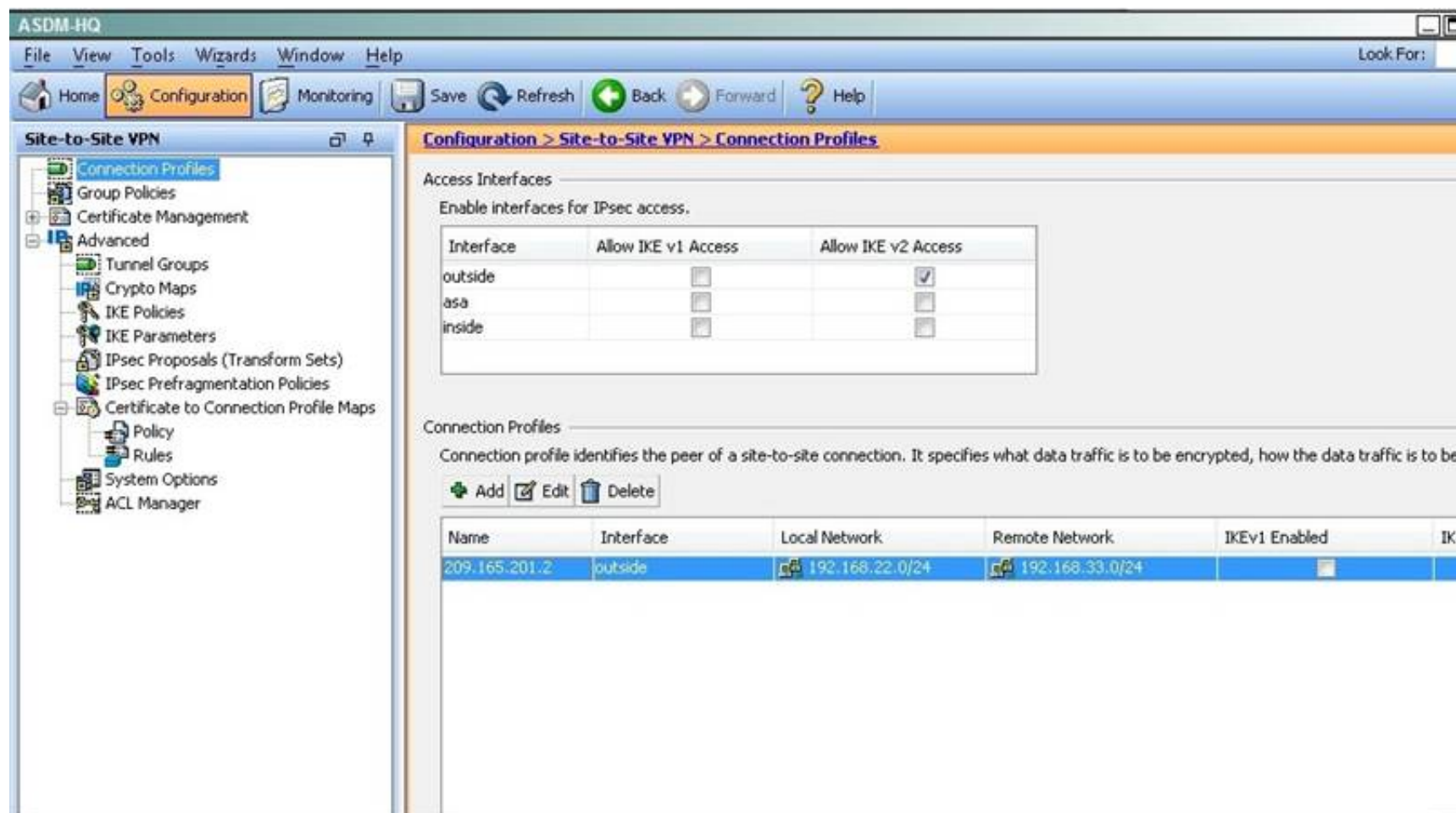
In a spoke-to-spoke DMVPN topology, which type of interface does a branch router require?

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

Answer: B

NEW QUESTION 5





ASDM-HQ Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

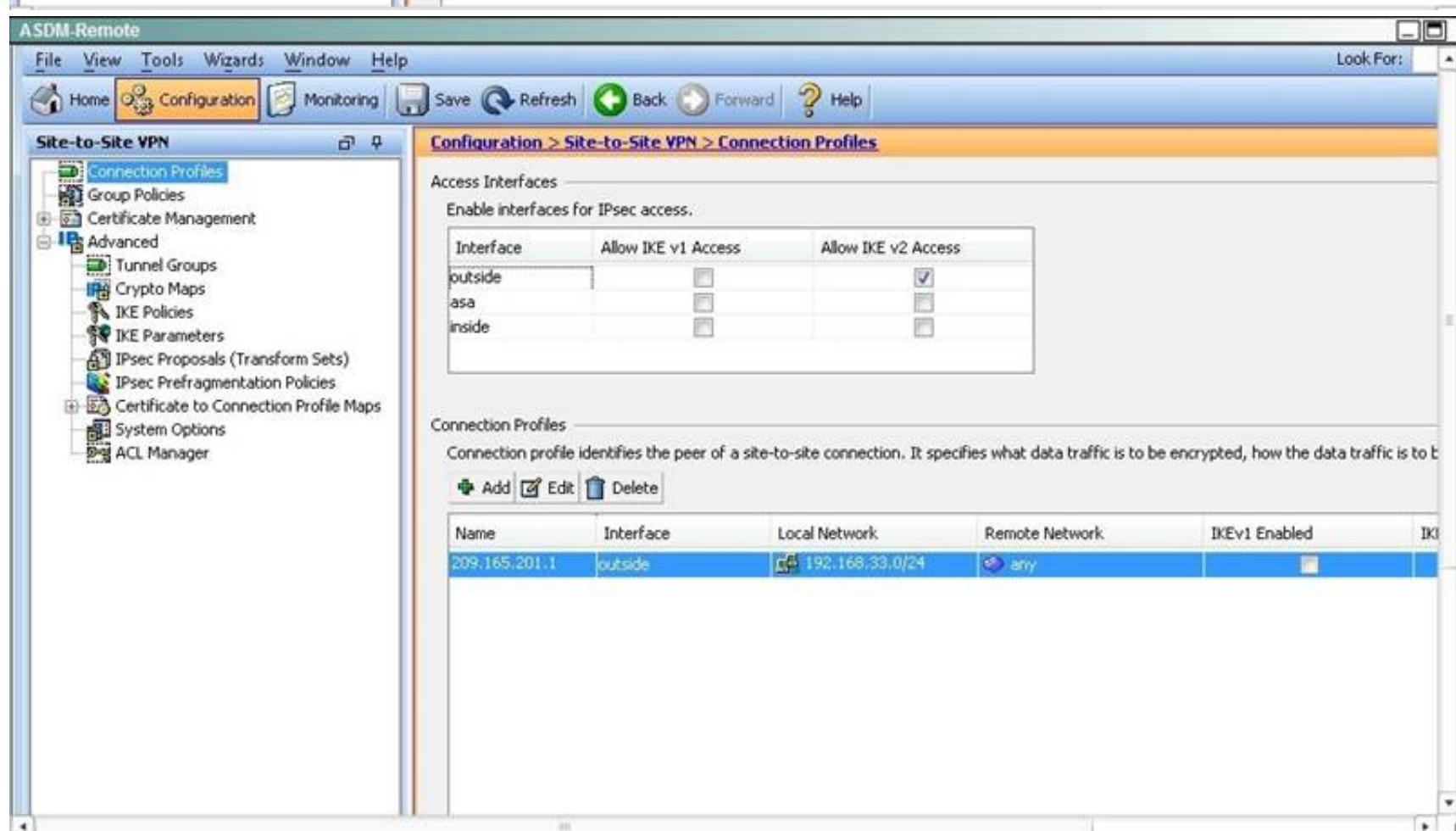
Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

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, and the peer's IP address.

Buttons: Add, Edit, Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled
209.165.201.2	outside	192.168.22.0/24	192.168.33.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>



ASDM-Remote 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, and the peer's IP address.

Buttons: 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"/>

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

- 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 192.168.33.0/0-192.168.33.255/65535 Remote selector 0.0.0.0/0 - 0.0.0.0/65535
- E. Local selector 0.0.0.0/0 - 0.0.0.0/65535 Remote selector 192.168.22.0/0 -192.168.22.255/65535

Answer: B

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).

NEW QUESTION 6

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 7

An engineer is troubleshooting network issues and wants to check the Layer 2 connectivity between routers. Which command must be run?

- A. show ip eigrp neighbors
- B. show cdp neighbor
- C. show crypto isakmp sa.
- D. show crypto issec sa.

Answer: B

NEW QUESTION 8

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

Answer: A

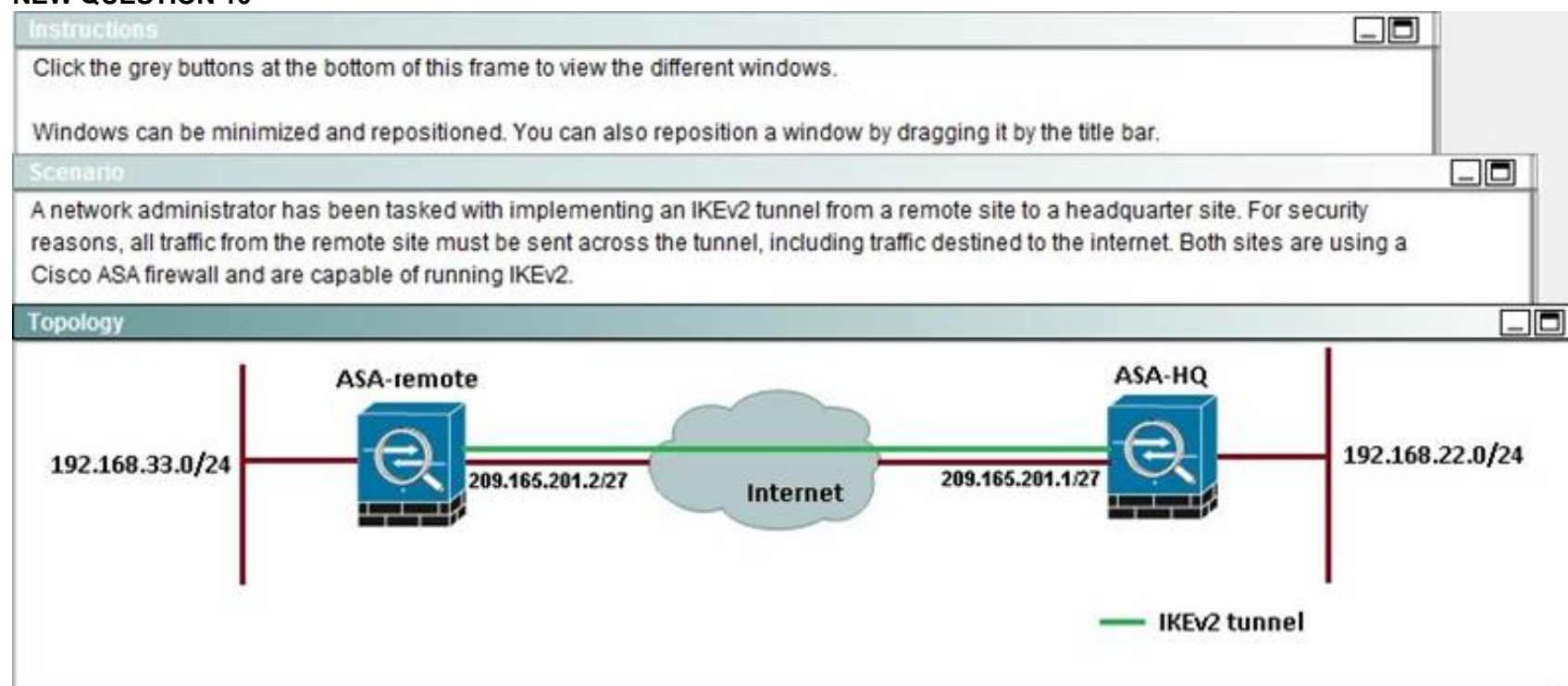
NEW QUESTION 9

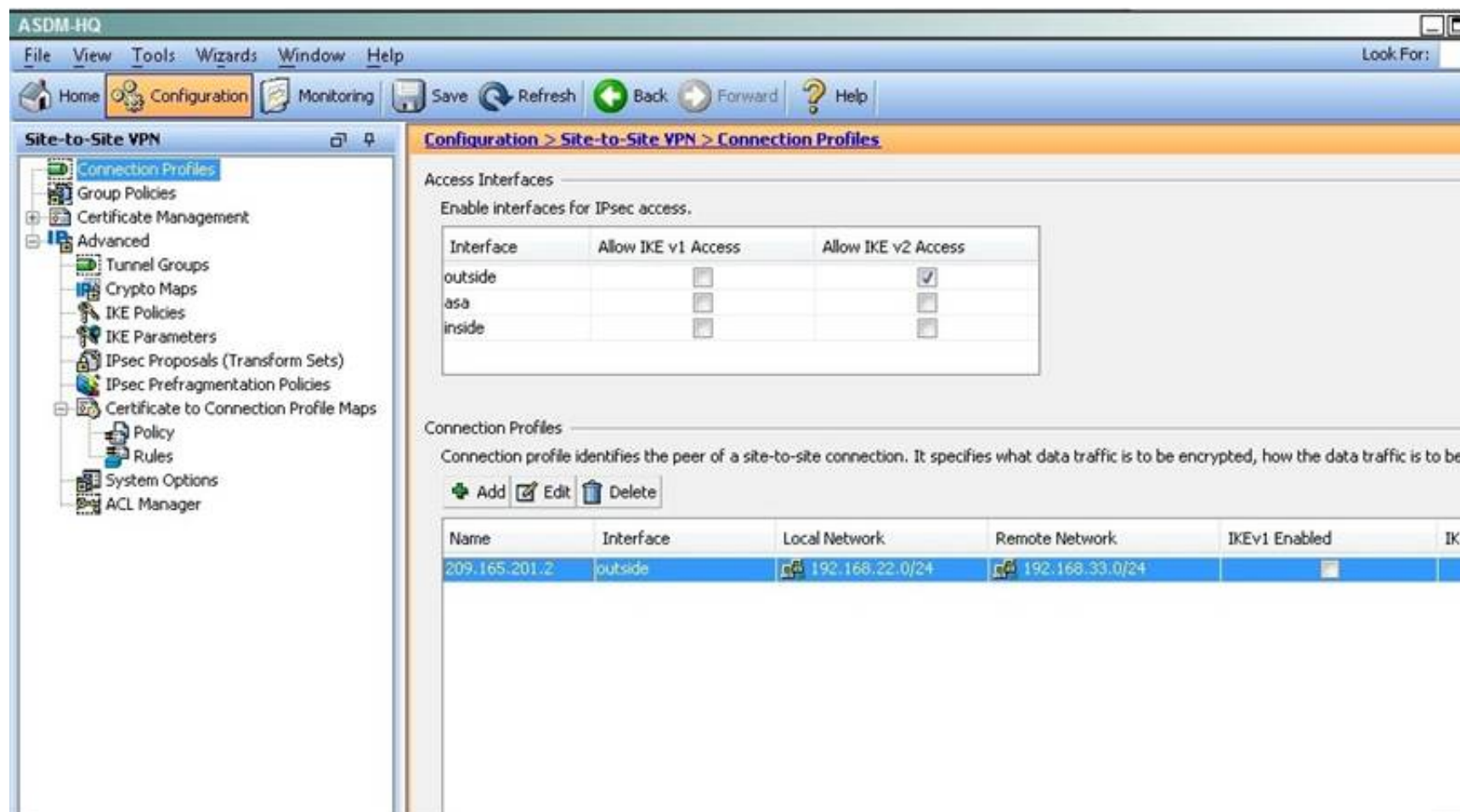
Which are two main use cases for Clientless SSL VPN? (Choose two.)

- 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

Answer: AB

NEW QUESTION 10





ASDM-HQ Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

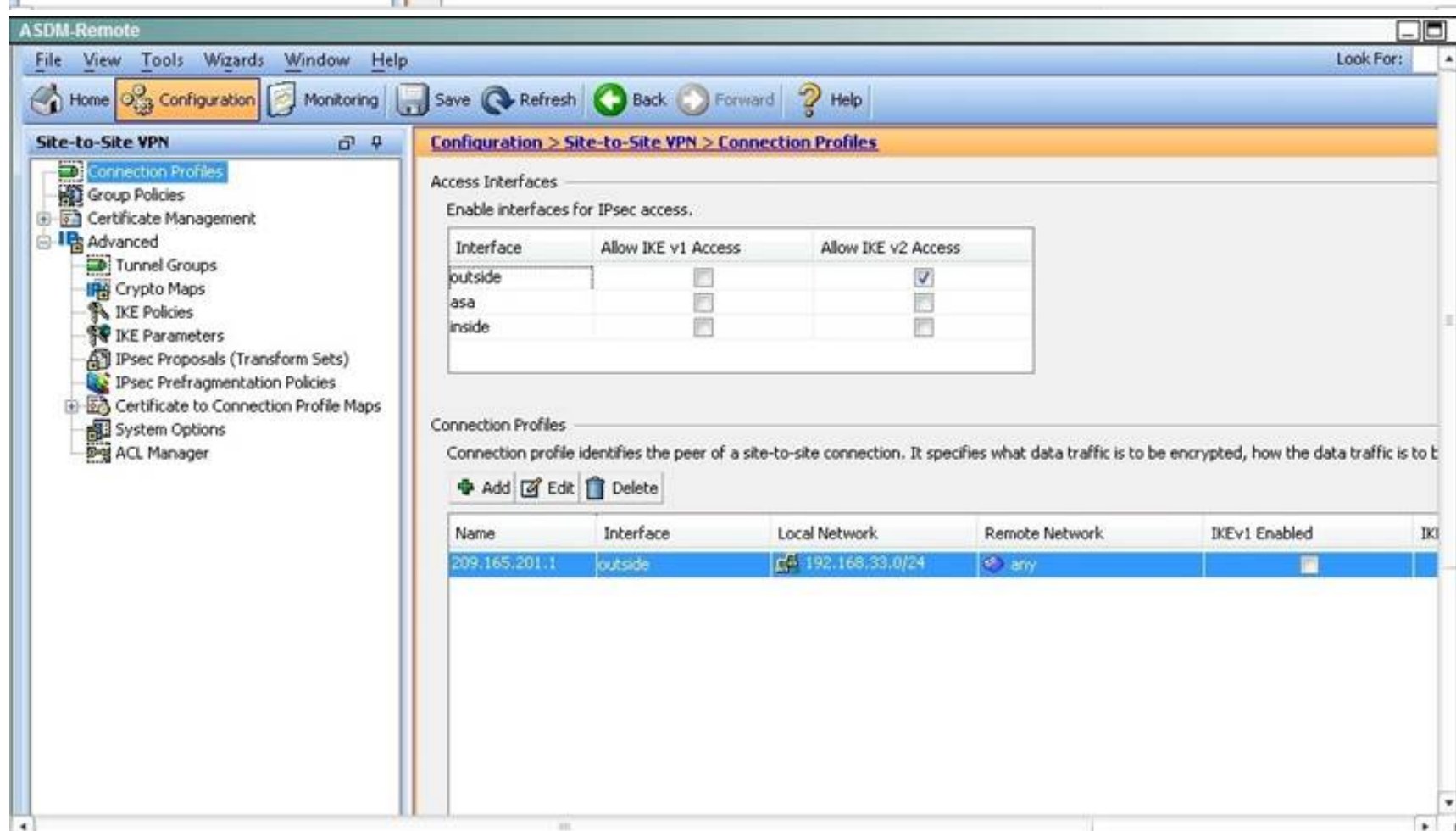
Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input type="checkbox"/>	<input checked="" type="checkbox"/>
asa	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

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, and the peer's IP address.

Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled
209.165.201.2	outside	192.168.22.0/24	192.168.33.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>



ASDM-Remote 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, and the peer's IP address.

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?

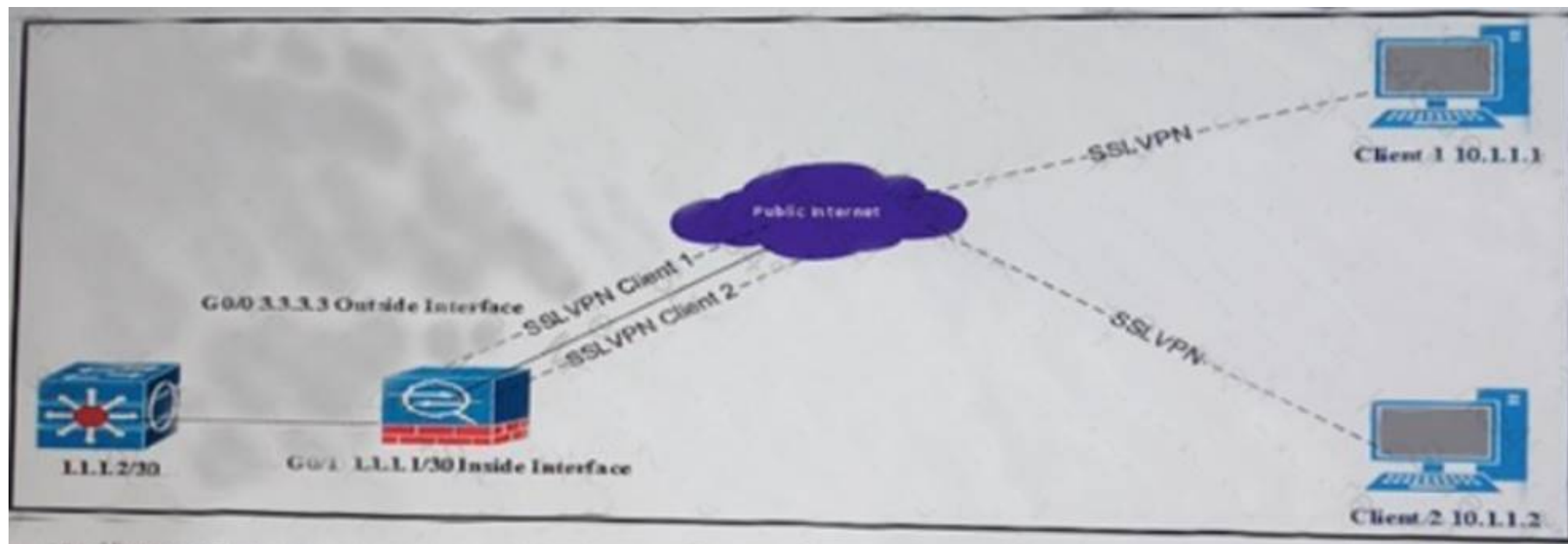
- A. DES
- B. 3DES
- C. AES
- D. AES192
- E. AES256

Answer: E

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.

NEW QUESTION 10

Refer to the Exhibit:



All internal clients behind the ASA are port address translated to the public outside interface, which has an IP address of 3.3.3.3. Client 1 and Client 2 have established successful SSL VPN connections to the ASA. However, when either client performs a browser search on their IP address, it shows up as 3.3.3.3. Why is the happening when both clients have a direct connection to the local internet service provider?

- A. Same-security-traffic permit inter-interface has not been configured.
- B. Tunnel All Networks is configured under Group Policy.
- C. Exclude Network List Below is configured under Group Policy.
- D. Tunnel Network List Below is configured under Group Policy.

Answer: B

NEW QUESTION 13

A rogue static route is installed in the routing table of a Cisco FlexVPN and is causing traffic to be blackholed. Which command should be used to identify the peer from which that route originated?

- A. show crypto ikev2 sa detail
- B. show crypto route
- C. show crypto ikev2 client flexvpn
- D. show ip route eigrp
- E. show crypto isakmp sa detail

Answer: B

NEW QUESTION 14

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

Answer: BC

NEW QUESTION 15

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 20

Which Cisco adaptive security appliance command can be used to view the count of all active VPN sessions?

- A. show vpn-sessiondb summary
- B. show crypto ikev1 sa
- C. show vpn-sessiondb ratio encryption
- D. show iskamp sa detail
- E. show crypto protocol statistics all

Answer: A

NEW QUESTION 21

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: BDE

NEW QUESTION 24

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}/

Answer: C

NEW QUESTION 25

An engineer is configuring clientless SSL VPN. The finance department has a database server that only they should access, but the sales department can currently access it. The finance and the sales departments are configured as separate group-policies. Which option must be added to the configuration to make sure the users in the sales department cannot access the finance department server?

- A. Web type ACL
- B. Port forwarding
- C. Tunnel group lock
- D. VPN filter ACL

Answer: C

NEW QUESTION 26

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

Answer: B

NEW QUESTION 31

A customer requests a VPN solution to support multicast traffic and connectivity with non-Cisco devices. What VPN solution would meet the customer requirements?

- A. GET VPN
- B. EZ VPN
- C. Flex VPN
- D. L2L VPN

Answer: C

NEW QUESTION 36

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

NEW QUESTION 37

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

Answer: D

NEW QUESTION 38

Which two statements about Internet Key Exchange version 1 are true? (Choose two.)

- A. Aggressive mode negotiates faster than main mode.
- B. When using aggressive mode, perfect forward secrecy is required.
- C. When using aggressive mode, the initiator and responder identities are passed in clear text.
- D. Main mode negotiates faster than aggressive mode.
- E. When using main mode, the initiator and responder identities are passed in clear text.

Answer: AC

NEW QUESTION 41

The Cisco AnyConnect client fails to connect via IKEv2 but works with SSL. The following error message is displayed: "Login Denied, unauthorized connection mechanism, contact your administrator" What is the most possible cause of this problem?

- A. DAP is terminating the connection because IKEv2 is the protocol that is being used.
- B. The client endpoint does not have the correct user profile to initiate an IKEv2 connection.
- C. The AAA server that is being used does not authorize IKEv2 as the connection mechanism.
- D. The administrator is restricting access to this specific user.
- E. The IKEv2 protocol is not enabled in the group policy of the VPN headend.

Answer: E

NEW QUESTION 42

Which must be configured for a Cisco Anyconnect client to determine the trustworthiness of a wireless network?

- A. Trusted network detection
- B. allow local proxy connections
- C. start before login
- D. allow VPN disconnect

Answer: A

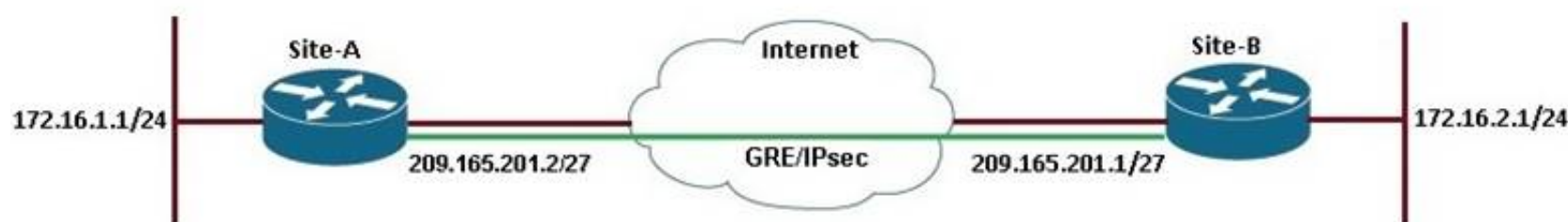
NEW QUESTION 44

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.

Topology




```
Flex-SiteA

%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>
```

Answer:

Explanation: 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 0

ip address 10.1.1.1 255.255.255.0 Tunnel source eth 0/0

Tunnel destination 209.165.201.1 tunnel protection ipsec profile default end

NEW QUESTION 47

Refer to the exhibit:

```
Router#show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA
IPv6 Crypto IKEv2 SA

Tunnel-id      fvrfl/ivrf      Status
1              none/none      READY
Local  2001:DB8:123:2::2/500
Remote 2001:DB8:123:1::2/500
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: RSA,
  Auth verify: RSA
  Life/Active Time: 86400/17811 sec
  CE id: 1024, Session-id: 4
  Status Description: Negotiation done
  Local spi: 0D26F648713C7FAB      Remote spi: 282FE0B3B5C99A2B
  Local id: 2001:DB8:123:2::2
  Remote id: 2001:DB8:123:1::2
  Local req msg id: 8              Remote req msg id: 8
  Local next msg id: 8            Remote next msg id: 8
  Local req queued: 8              Remote req queued: 8
  Local window: 5                  Remote window: 5
  DPD configured for 0 seconds, retry 0
  NAT-T is not detected
  Cisco Trust Security SGT is disabled
  Initiator of SA : No
```

Which statement about this output is true?

- A. Identity between endpoints is verified using a certificate authority
- B. The tunnel is not functional because NAT-T is not configured.
- C. This router has sent the first packet to establish the Flex VPN tunnel
- D. The remote device encrypts IKEv2 packets using key "282FE"0B3B5C99A2B".

Answer: C

NEW QUESTION 52

In a new DMVPN deployment, phase 1 completes successfully. However, phase2 experiences issues. Which troubleshooting step is valid in this situation?

- A. Temporarily remove encryption to check if the GRE tunnel is working.
- B. Verify IP routing between the external IPs of the two peers is correct.
- C. Remove NHRP configuration and reset the tunnels.
- D. Ensure that the nodes use the same authentication method.

Answer: A

NEW QUESTION 57

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

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

Answer: BC

NEW QUESTION 58

Which Cisco firewall platform supports Cisco NGE?

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

Answer: D

NEW QUESTION 60

An engineer is defining ECC variables and has set the input_mode set to B. Which statement is true?

- A. DTMF voice is accepted
- B. Get Digits are written to the CED
- C. Mixed mode input is not accepted
- D. An ASR is not being used

Answer: A

NEW QUESTION 62

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 63

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

Answer: BCD

NEW QUESTION 68

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

Answer: B

NEW QUESTION 71

A spoke has two Internet connections for failover. How can you achieve optimum failover without affecting any other router in the DMVPN cloud?

- A. Create another DMVPN cloud by configuring another tunnel interface that is sourced from the second ISP link.
- B. Use another router at the spoke site, because two ISP connections on the same router for the same hub is not allowed.
- C. Configure SLA tracking, and when the primary interface goes down, manually change the tunnel source of the tunnel interface.
- D. Create another tunnel interface with same configuration except the tunnel source, and configure the if-state nhrp and backup interface commands on the primary tunnel interface.

Answer: D

NEW QUESTION 75

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

NEW QUESTION 77

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

Answer: BC

NEW QUESTION 82

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

NEW QUESTION 83

Refer to the Exhibit:

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 150
 no ip split-horizon eigrp 100
 no ip next-hop-self eigrp 100
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco
```

An engineer must implement DMVPN phase 2 and two conclusions can be made from the configuration? (Choose two.)

- A. Spoke-to-spoke communication is allowed.
- B. Next-hop-self is required.
- C. EIGRP neighbor adjacency will fail.
- D. EIGRP route redistribution is not allowed
- E. EIGRP used as the dynamic routing protocol.

Answer: AE

NEW QUESTION 88

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

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

Answer: A

NEW QUESTION 91

Which two troubleshooting steps should be taken when Cisco AnyConnect cannot establish an IKEv2 connection, while SSL works fine? (Choose two.)

- A. Verify that the primary protocol on the client machine is set to IPsec.
- B. Verify that AnyConnect is enabled on the correct interface.

- C. Verify that the IKEv2 protocol is enabled on the group policy.
- D. Verify that ASDM and AnyConnect are not using the same port.
- E. Verify that SSL and IKEv2 certificates are not referencing the same trustpoint.

Answer: AC

NEW QUESTION 96

An engineer is configuring SSL VPN for remote access. A real-time application that is sensitive to packet delays will be used. Which feature should the engineer confirm is enabled to avoid latency and bandwidth problems associated with SSL connections?

- A. DTLS
- B. DPD
- C. SVC
- D. IKEv2

Answer: A

NEW QUESTION 100

Refer to the exhibit.

```
<ServerList>
  <HostEntry>
    <HostName>SIMOS_ASA</HostName>
    <HostAddress>simos.cisco.com</HostAddress>
    <UserGroup>simos-group</UserGroup>
    <PrimaryProtocol>IPsec</PrimaryProtocol>
  </HostEntry>
</ServerList>

tunnel-group AC general-attributes
 address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 group-alias simos-group enable
 group-url https://simos.cisco.com/simos-group enable
```

An administrator had the above configuration working with SSL protocol, but as soon as the administrator specified IPsec as the primary protocol, the Cisco AnyConnect client was not able to connect. What is the problem?

- A. IPsec will not work in conjunction with a group URL.
- B. The Cisco AnyConnect implementation does not allow the two group URLs to be the same
- C. SSL does allow this.
- D. If you specify the primary protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group).
- E. A new XML profile should be created instead of modifying the existing profile, so that the clients force the update.

Answer: C

NEW QUESTION 105

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

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

Answer: BCD

NEW QUESTION 110

You are troubleshooting a site-to-site VPN issue where the tunnel is not establishing. After issuing the debug crypto ipsec command on the headend router, you see the following output. What does this output suggest?

```
1d00h: IPSec (validate_proposal): transform proposal (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

- A. Phase 1 policy does not match on both sides.
- B. The Phase 2 transform set does not match on both sides.
- C. ISAKMP is not enabled on the remote peer.
- D. The crypto map is not applied on the remote peer.
- E. The Phase 1 transform set does not match on both sides.

Answer: B

NEW QUESTION 111

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

Answer: AD

NEW QUESTION 112

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

NEW QUESTION 116

A custom desktop application needs to access an internal server. An administrator is tasked with configuring the company's SSL VPN gateway to allow remote users to work. Which two technologies would accommodate the company's requirement? (Choose two).

- A. AnyConnect client
- B. Smart Tunnels
- C. Email Proxy
- D. Content Rewriter
- E. Portal Customizations

Answer: AB

NEW QUESTION 121

Refer to the exhibit.


```
Hub config :

crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set myset
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip nhrp authentication DMVPN01
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 ip address 209.165.200.234 255.255.255.248

Spoke 2 Config :

crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set myset
!
interface Tunnel0
 ip address 172.16.1.3 255.255.255.0
 no ip redirects
 ip nhrp authentication DMVPN1
 ip nhrp map 172.16.1.1 209.165.200.234
 ip nhrp map multicast 209.165.200.234
 ip nhrp network-id 200
 ip nhrp nh 172.16.1.1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 ip address 209.165.202.146 255.255.255.248

Hub debugs :

*Apr 25 19:32:30.867: NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 107
*Apr 25 19:32:30.868: NHRP-ATTR: Sending error indication
```

The network administrator is adding a new spoke, but the tunnel is not passing traffic. What could cause this issue?

- A. DMVPN is a point-to-point tunnel, so there can be only one spoke.
- B. There is no EIGRP configuration, and therefore the second tunnel is not working.
- C. The NHRP authentication is failing.
- D. The transform set must be in transport mode, which is a requirement for DMVPN.
- E. The NHRP network ID is incorrect.

Answer: C

Explanation:

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html#wp1055049

NEW QUESTION 122

Refer to the exhibit.

```
interface Tunnel10
 ip address 209.165.200.225 255.255.255.254
 ipv6 address 2001:DB8:100::1/64
 ipv6 enable
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 209.165.201.20
 tunnel protection ipsec profile default
end
```

An administrator is adding IPv6 addressing to an already functioning tunnel. The administrator is unable to ping 2001:DB8:100::2 but can ping 209.165.200.226. Which configuration needs to be added or changed?

- A. No configuration change is necessary
- B. Everything is working correctly.
- C. OSPFv3 needs to be configured on the interface.
- D. NHRP needs to be configured to provide NBMA mapping.
- E. Tunnel mode needs to be changed to GRE IPv4.
- F. Tunnel mode needs to be changed to GRE IPv6.

Answer: E

NEW QUESTION 125

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 129

An engineer is troubleshooting VPN connectivity issues between a PC and ASA using Cisco AnyConnect IPsec IKEv2. Which requirement must be satisfied for proper functioning?

- A. PC certificate must contain the server-auth EKU.
- B. The connection must use EAP-AnyConnect.
- C. The SAN must be used as the CN for the ASA-side certificates.
- D. profile and binary updates must be downloading over IPsec

Answer: A

NEW QUESTION 133

Which hash algorithm is required to protect classified information?

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

Answer: D

NEW QUESTION 134

Which two parameters are specified in the isakmp (IKEv1) policy? (Choose two.)

- A. the peer
- B. the hashing algorithm
- C. the session key
- D. the authentication method
- E. the transform-set

Answer: AD

NEW QUESTION 136

Which two options are features of Cisco GET VPN? (Choose two.)

- A. Allows for optimal routing
- B. provides point to point IPsec SA
- C. Provides encryption for MPLS
- D. uses public Internet
- E. uses MORE

Answer: AC

NEW QUESTION 141

Refer to the exhibit.


```

aaa new-model
aaa authentication network FLEXVPN local

crypto ikev2 authorization policy SPOKES
 pool FlexPOOL
 route set interface
 route accept any distance 255
crypto ikev2 keyring SPOKES
 peer ALLSPOKES
  identity fqdn domain example.com
  pre-shared-key Cisco123
!
crypto ikev2 profile SPOKES
 match identity remote fqdn domain example.com
 identity local fqdn R002.example.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SPOKES
aaa authorization group psk list FLEXVPN SPOKES
virtual-template 10
 set ikev2-profile SPOKES

```

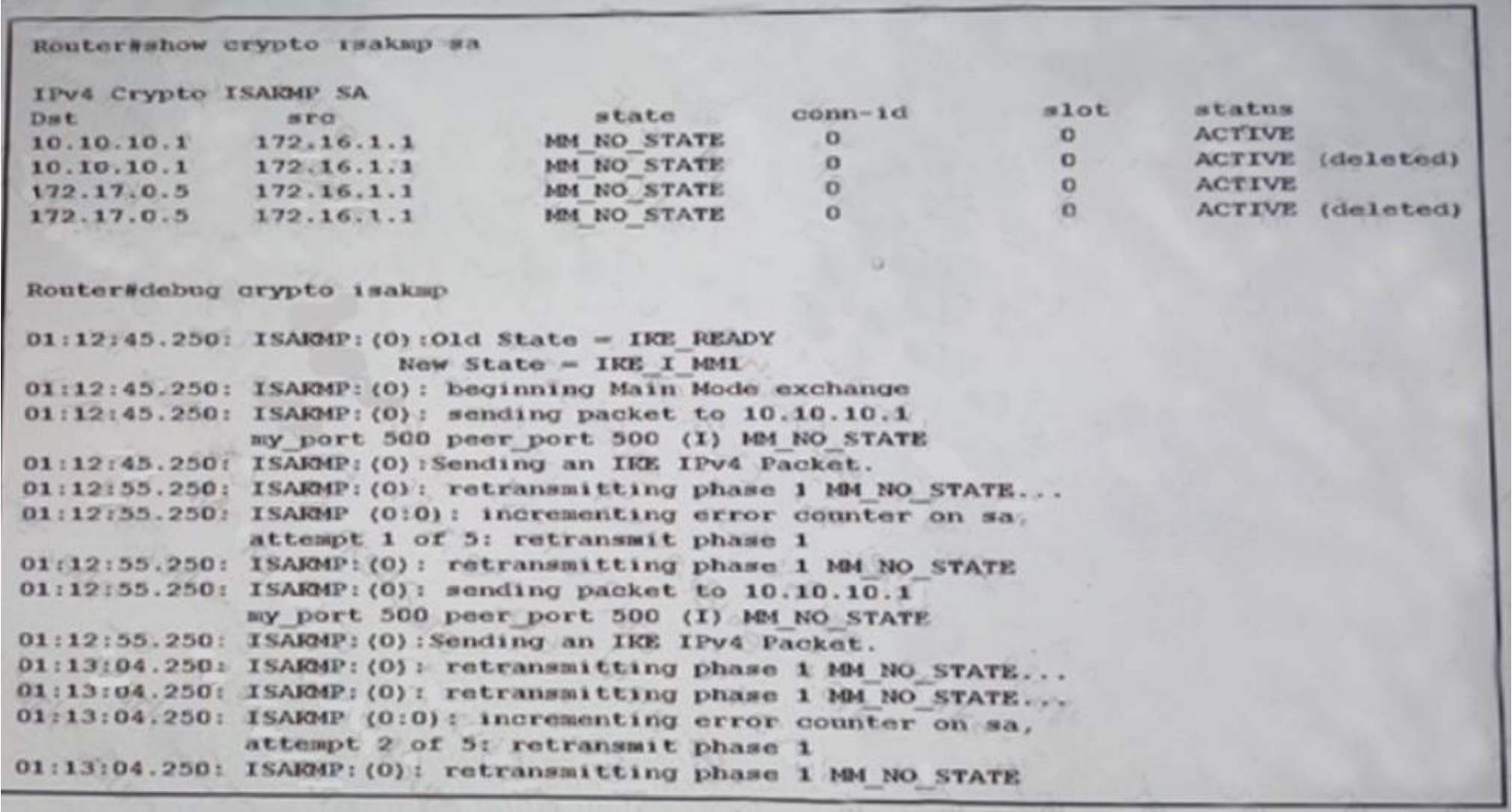
An IPsec peer is exchanging routes using IKEv2, but the routes are not installed in the RIB. Which configuration error is causing the failure?

- A. IKEv2 routing requires certificate authentication, not pre-shared keys.
- B. An invalid administrative distance value was configured.
- C. The match identity command must refer to an access list of routes.
- D. The IKEv2 authorization policy is not referenced in the IKEv2 profile.

Answer: B

NEW QUESTION 145

Refer to the Exhibit:



Why is the tunnel not establishing?

- A. Lifetimes are misconfigured.
- B. SAKMP packets are blocked.
- C. NAT statements are missing.
- D. GRE is not working correctly.

Answer: B

NEW QUESTION 148

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

NEW QUESTION 151

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

Answer: B

NEW QUESTION 155

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: ABCD

NEW QUESTION 156

A client has asked an engineer to assist in installing and upgrading to the latest version of Cisco Any Connect Secure and upgrading to the latest version of Cisco Any Connect Secure Mobility Client. Which type of deployment method requires the updated version of the client to be loaded only on the headend device such as an ASA or ISE device?

- A. Web-deploy
- B. Cloud-deploy
- C. Cloud-update
- D. Web-update

Answer: A

NEW QUESTION 159

Regarding licensing, which option will allow IKEv2 connections on the adaptive security appliance?

- A. AnyConnect Essentials can be used for Cisco AnyConnect IKEv2 connections.
- B. IKEv2 sessions are not licensed.
- C. The Advanced Endpoint Assessment license must be installed to allow Cisco AnyConnect IKEv2 sessions.
- D. Cisco AnyConnect Mobile must be installed to allow AnyConnect IKEv2 sessions.

Answer: B

NEW QUESTION 163

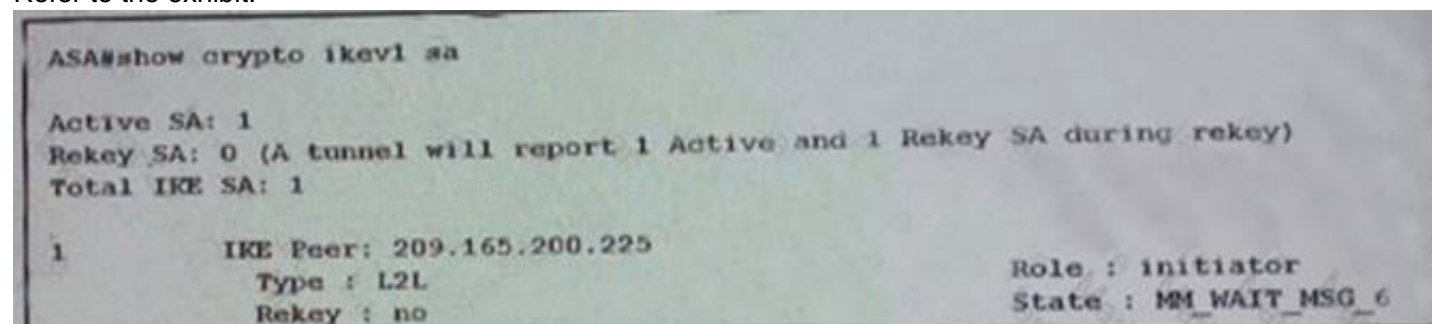
An engineer is troubleshooting DMVPN and wants to check if traffic flows in only one direction

- A. show crypto ipsec sa
- B. show crypto lkev2 sa
- C. show crypto isakmp as
- D. show crypto angina accelerator statistics

Answer: A

NEW QUESTION 165

Refer to the exhibit:



Which description of the status of this VPN tunnel is true?

- A. The pre shared key in phase 1 is mismatched between tunnel endpoints
- B. The phase 1 is complete, phase 2 status is unknown
- C. The integrity algorithm does not match between the two endpoints.
- D. The tunnel is up and waiting for traffic to flow across it

Answer: A

NEW QUESTION 166

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: AEF

NEW QUESTION 170

Which cryptographic algorithms are approved to protect Top Secret information?

- A. HIPPADES
- B. AES-128
- C. RC4-128
- D. AES-256

Answer: D

NEW QUESTION 173

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

Answer: A

NEW QUESTION 174

An engineer is configuring an IP VPN with IKEv2. Which two components are part of the IKEv2 proposal for this implementation? (Choose two.)

- A. Key ring
- B. Encryption
- C. Tunnel mode
- D. Peer name
- E. integrity

Answer: BE

NEW QUESTION 176

Which option must be enabled to allow an SSL VPN which is configured for DTLS to fall back to TLS?

- A. Svc rekey method ssl
- B. Svc dpd-interval
- C. Svc dtls enable
- D. Svc profiles value

Answer: B

NEW QUESTION 178

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

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

Answer: A

NEW QUESTION 183

Refer to the Exhibit:

```
Router#show crypto ipsec security-assoc lifetime
Security association lifetime: 4608000 kilobytes/3600 seconds

Router# show crypto ipsec sa
interface: Ethernet0/1
  Crypto map tag: vpn, local addr. 10.10.250.250
  local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (10.10.250.250/255.255.255.255/47/0)
  current_peer: 10.10.250.250:500
    PERMIT, flags=(origin_is_acl,)
  #pkts encaps: 5961, #pkts encrypt: 5961, #pkts digest 5961
  #pkts decaps: 5961, #pkts decrypt: 5961, #pkts verify 5961
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0
  local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.10.250.250
  path mtu 1500, media mtu 1500
  current outbound spi: 8E1CB77A

inbound esp sas:
  spi: 0x4579534B(1165587771)
    transform: esp-3des esp-md5-hmac ,
    in use settings = (Tunnel, )
    slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
    sa timing: remaining key lifetime (k/sec): (4506885/3581)
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
  spi: 0x8E1CB88A(2384246650)
    transform: esp-3des esp-md5-hmac ,
    in use settings = (Tunnel, )
    slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
    sa timing: remaining key lifetime (k/sec): (4506885/3581)
    IV size: 8 bytes
    replay detection support: Y
```

A network security engineer is troubleshooting intermittent connectivity issues across a tunnel. Based on the output from the show crypto ipsec sa command, which cause is most likely?

- A. ISAKMP and/or IP sec may be bouncing up and down.
- B. The security association lifetimes are set to default values.
- C. Return traffic is not coming back from the other end of the tunnel.
- D. Traffic may flow in only one direction across this tunnel.

Answer: B

NEW QUESTION 186

Which adaptive security appliance command can be used to see a generic framework of the requirements for configuring a VPN tunnel between an adaptive security appliance and a Cisco IOS router at a remote office?

- A. vpnsetup site-to-site steps
- B. show running-config crypto
- C. show vpn-sessiondb l2l
- D. vpnsetup ssl-remote-access steps

Answer: A

NEW QUESTION 191

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

Answer: C

NEW QUESTION 195

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 196

In a FlexVPN deployment, the spokes are successfully connecting to the hub. However, spoke-to-spoke tunnels do not form. Which trouble shooting step is valid for this issue?

- A. Verify the spoke configuration to check if the NHRP redirect is enabled.
- B. Verify the hub configuration to check if the NHRP shortcut is enabled.
- C. Verify the tunnel interface is contained within a VRF.
- D. Verify the spoke receives redirect messages and send resolution requests

Answer: B

NEW QUESTION 199

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 202

Which technology can provide high availability for an SSL VPN?

- A. DMVPN
- B. a multiple-tunnel configuration
- C. a Cisco ASA pair in active/passive failover configuration
- D. certificate to tunnel group maps

Answer: C

NEW QUESTION 207

Which two parameters help to map a VPN session to a tunnel group without using the tunnel-group list? (Choose two.)

- A. group-alias
- B. certificate map
- C. use gateway command
- D. group-url
- E. AnyConnect client version

Answer: BD

NEW QUESTION 211

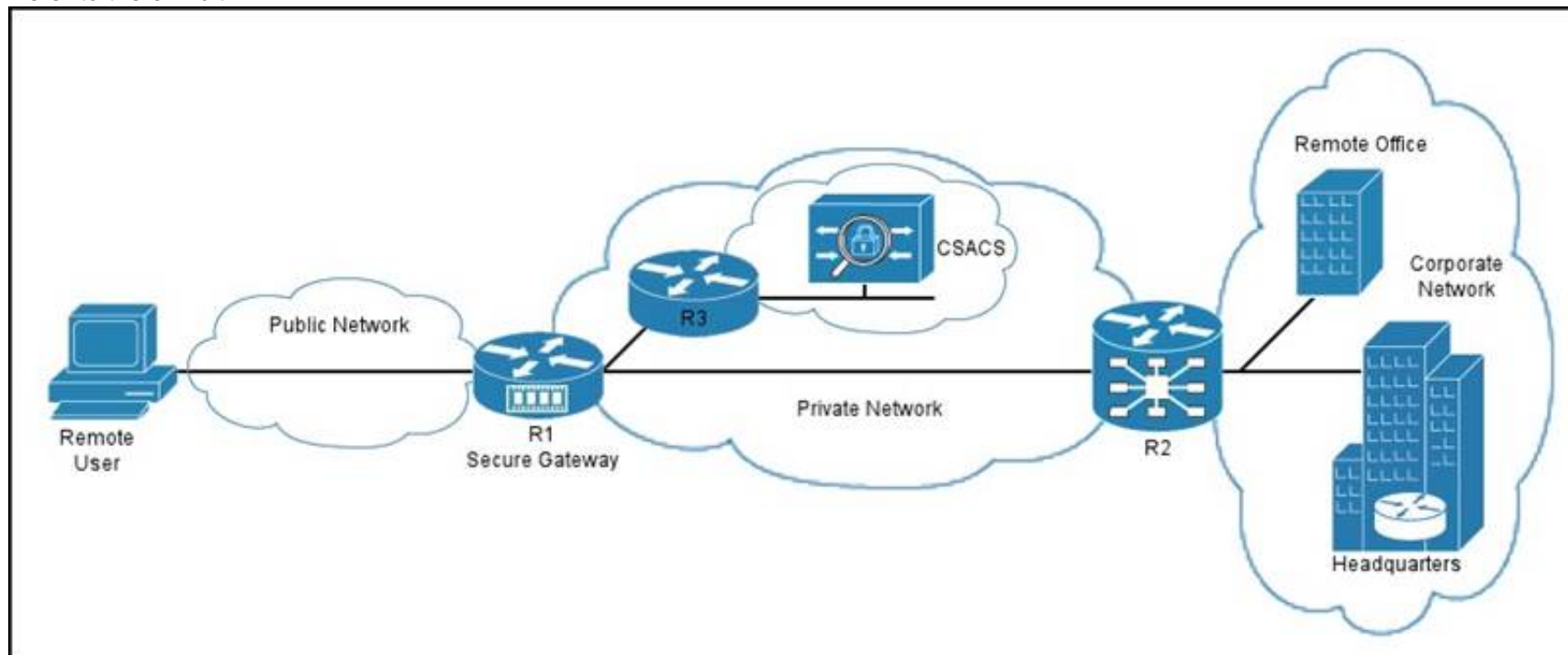
Which three changes must be made to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose three.)

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

Answer: BDE

NEW QUESTION 216

Refer to the exhibit.



You have implemented an SSL VPN as shown. Which type of communication takes place between the secure gateway R1 and the Cisco Secure ACS?

- A. HTTP proxy
- B. AAA
- C. policy
- D. port forwarding

Answer: B

NEW QUESTION 220

Which option describes the purpose of the command show derived-config interface virtual-access 1?

- A. It verifies that the virtual access interface is cloned correctly with per-user attributes.
- B. It verifies that the virtual template created the tunnel interface.
- C. It verifies that the virtual access interface is of type Ethernet.
- D. It verifies that the virtual access interface is used to create the tunnel interface.

Answer: A

NEW QUESTION 221

Which option is most effective at preventing a remote access VPN user from bypassing the corporate transparent web proxy?

- A. using the proxy-server settings of the client computer to specify a PAC file for the client computer to download
- B. instructing users to use the corporate proxy server for all web browsing
- C. disabling split tunneling

D. permitting local LAN access

Answer: C

NEW QUESTION 224

Scenario

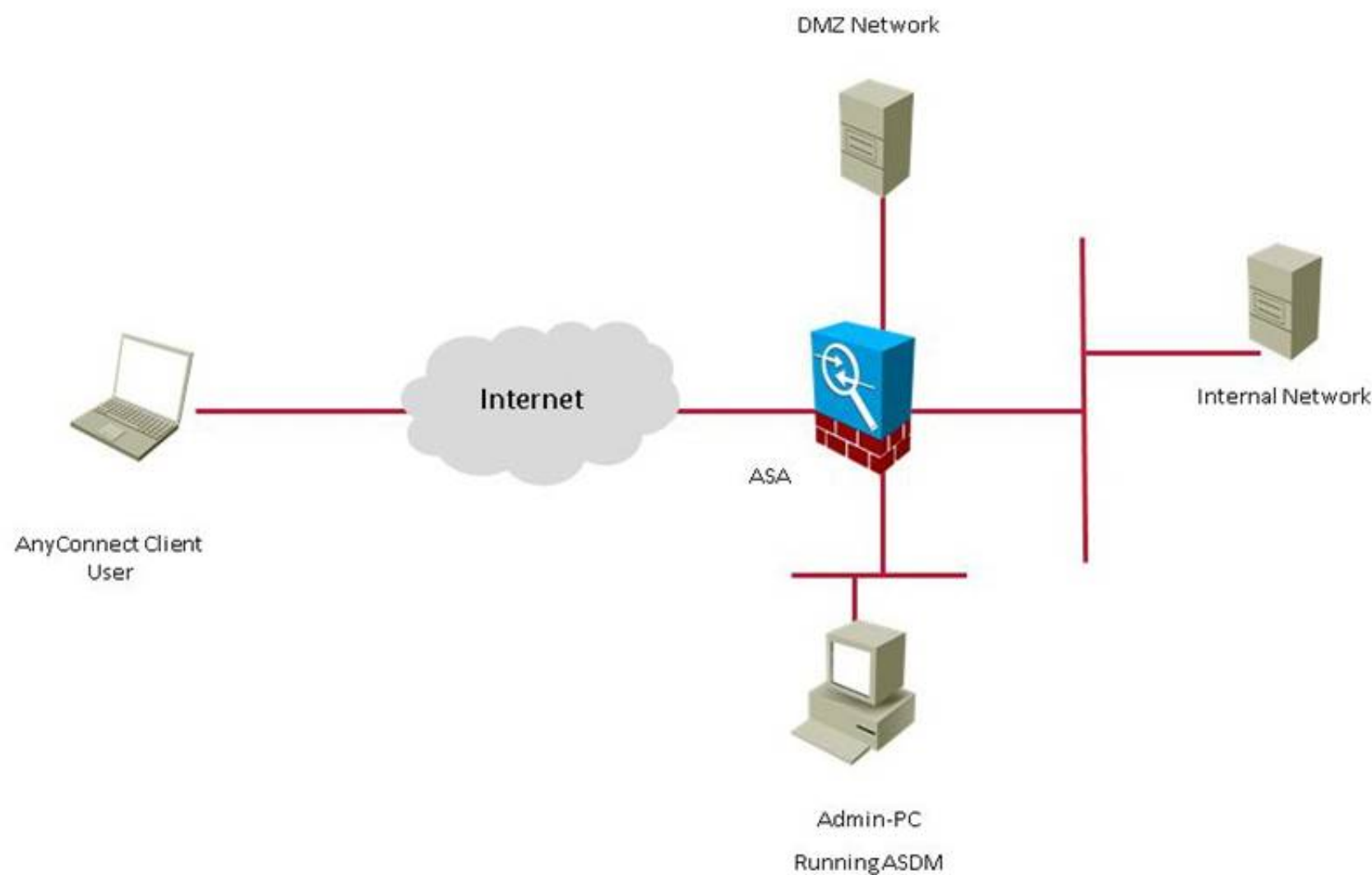
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

Note: Not all screens or option selections are active for this exercise.

Instructions

- Navigate the ASDM GUI on the device to verify network operation and answer for multiple-choice questions.
- You may have to use the scroll bars to view the entire ASDM Configuration screens.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- **NOT ALL SCREENS AND SELECTIONS ARE AVAILABLE FOR THIS EXERCISE.**
- Click on the Admin PC on the topology page to gain ASDM to the ASA. No passwords are required for this exercise.
- You may also click on the Default Home tab to access ASDM or return to the ASDM home screen at any time.
- There are **four (4)** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.
- To access the multiple-choice questions, click on the Questions tab and then numbered boxes on the left of the panel to view each question.

Topology



Default_Home



Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Group
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native	
GigabitEthernet0/1		Enabled				native	
GigabitEthernet0/1.4	inside	Enabled	100	10.10.1.1	255.255.255.0	vlan4	
GigabitEthernet0/1.250	Guest	Enabled	30	10.10.250.1	255.255.255.0	vlan250	
GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native	
GigabitEthernet0/3	Site-To...	Enabled	60	172.16.2.1	255.255.255.0	native	
GigabitEthernet0/4		Enabled				native	
GigabitEthernet0/5		Enabled				native	
Management0/0	manage...	Enabled	90	10.10.2.1	255.255.255.0	native	

Enable traffic between two or more interfaces which are configured with same security levels

Enable traffic between two or more hosts connected to the same interface

Enable jumbo frame reservation

Apply Reset

Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The **ASDM Assistant** provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts
Following are some important concepts for setting up a connection.

- 1. SSL tunnel and IPsec tunnel**
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(IKEv2) protocols, Cisco VPN Client supports only IPsec(IKEv1) protocol.
- 2. User and connection profile**
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.
You configure user account database in [AAA/Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(IKEv1\) Connection Profiles](#).
- 3. Access policy**
Access policies control how remote users can access corporate networks. An access policy includes the following:
 - Session control - how long a session can remain idle before it is closed.
 - Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [NAC](#) based endpoint security policies.

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

enables user authentication and encryption. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces
☒ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☒ Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.




Login Page Setting
☐ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.
☒ Shutdown portal login page. Shutdown notice: Service out temporarily.

Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

☒ Add ☒ Edit ☐ Delete End:

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVP...	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
AnyConnect_P...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyConnect_VPN_User	AAA(LOCAL)	GroupPolicy2

Select Address Pools

 Add
  Edit
  Delete


Pool Name	Starting Address	Ending Address/Number of Addresses	Subnet Mask/Prefix Length
AC_Addre...	10.10.15.40	10.10.15.50	255.255.255.0
Outside_A...	209.165.201.20	209.165.201.30	255.255.255.0
Remote_A...	192.168.1.100	192.168.1.150	255.255.255.0
VPN_Addr...	10.10.15.20	10.10.15.30	255.255.255.0

Assigned Address Pools

Assign-> VPN_Address_Pool

OK Cancel Help

Edit AnyConnect Connection Profile: AnyConnect_Profile

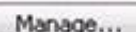
Basic
  Advanced

Name: AnyConnect_Profile

Aliases: AnyConnect_VPN_User


Authentication

Method: ☒ AAA ☐ Certificate ☐ Both

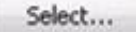
AAA Server Group: LOCAL 


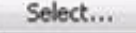
☐ Use LOCAL if Server Group fails

Client Address Assignment

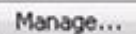
DHCP Servers: 

☒ None ☐ DHCP Link ☐ DHCP Subnet

Client Address Pools: VPN_Address_Pool 

Client IPv6 Address Pools:  

Default Group Policy


Group Policy: GroupPolicy2 

(Following field is an attribute of the group policy selected above.)



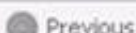
☒ Enable SSL VPN client protocol

☐ Enable IPsec(IKEv2) client protocol

DNS Servers: 10.10.3.20

WINS Servers: 

Domain Name: secure-x.local

Find:   

OK Cancel Help

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Access Rules

Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

Enabled	Source Criteria:			Destination Criteria:		Service
	Source	User	Security Group	Destination	Security Group	
DMZ (3 incoming rules)						
<input checked="" type="checkbox"/>	DMZ-server			any4		icmp
<input checked="" type="checkbox"/>	DMZ-server			HQ-srv		ftp
<input checked="" type="checkbox"/>	DMZ-server			any		domain
est (1 implicit incoming rule)						
	any			Any less secure ne...		ip
e-To-Site (1 implicit incoming rule)						
	any			Any less secure ne...		ip
ide (1 implicit incoming rule)						
	any			Any less secure ne...		ip
inagement (1 implicit incoming rule)						
	any			Any less secure ne...		ip
tside (6 incoming rules)						
<input checked="" type="checkbox"/>	any4			DMZ-server		http
<input checked="" type="checkbox"/>	any4			DMZ-server		https
<input checked="" type="checkbox"/>	any4			DMZ-server		ftp
<input checked="" type="checkbox"/>	any4			DMZ-server		icmp
<input checked="" type="checkbox"/>	any4			DMZ-server		smtp
<input checked="" type="checkbox"/>	any4			DMZ-server		domain
lobal (1 implicit rule)						
	any			any		ip

Apply Reset Advanced...

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access > Advanced > ACL Manager

Add Edit Delete Find

#	Enabled	Source	User	Security Group	Destination	Security
DMZ_access_in						
1	<input checked="" type="checkbox"/>	DMZ-server			any4	
2	<input checked="" type="checkbox"/>	DMZ-server			HQ-srv	
3	<input checked="" type="checkbox"/>	DMZ-server			any	
outside_access_in						
1	<input checked="" type="checkbox"/>	any4			DMZ-server	
2	<input checked="" type="checkbox"/>	any4			DMZ-server	
3	<input checked="" type="checkbox"/>	any4			DMZ-server	
4	<input checked="" type="checkbox"/>	any4			DMZ-server	
5	<input checked="" type="checkbox"/>	any4			DMZ-server	
6	<input checked="" type="checkbox"/>	any4			DMZ-server	
outside_cryptomap						
1	<input checked="" type="checkbox"/>	10.10.9.0/24			10.11.11.0/24	
permit-all						
1	<input checked="" type="checkbox"/>	any			any	

Collapse All Expand All

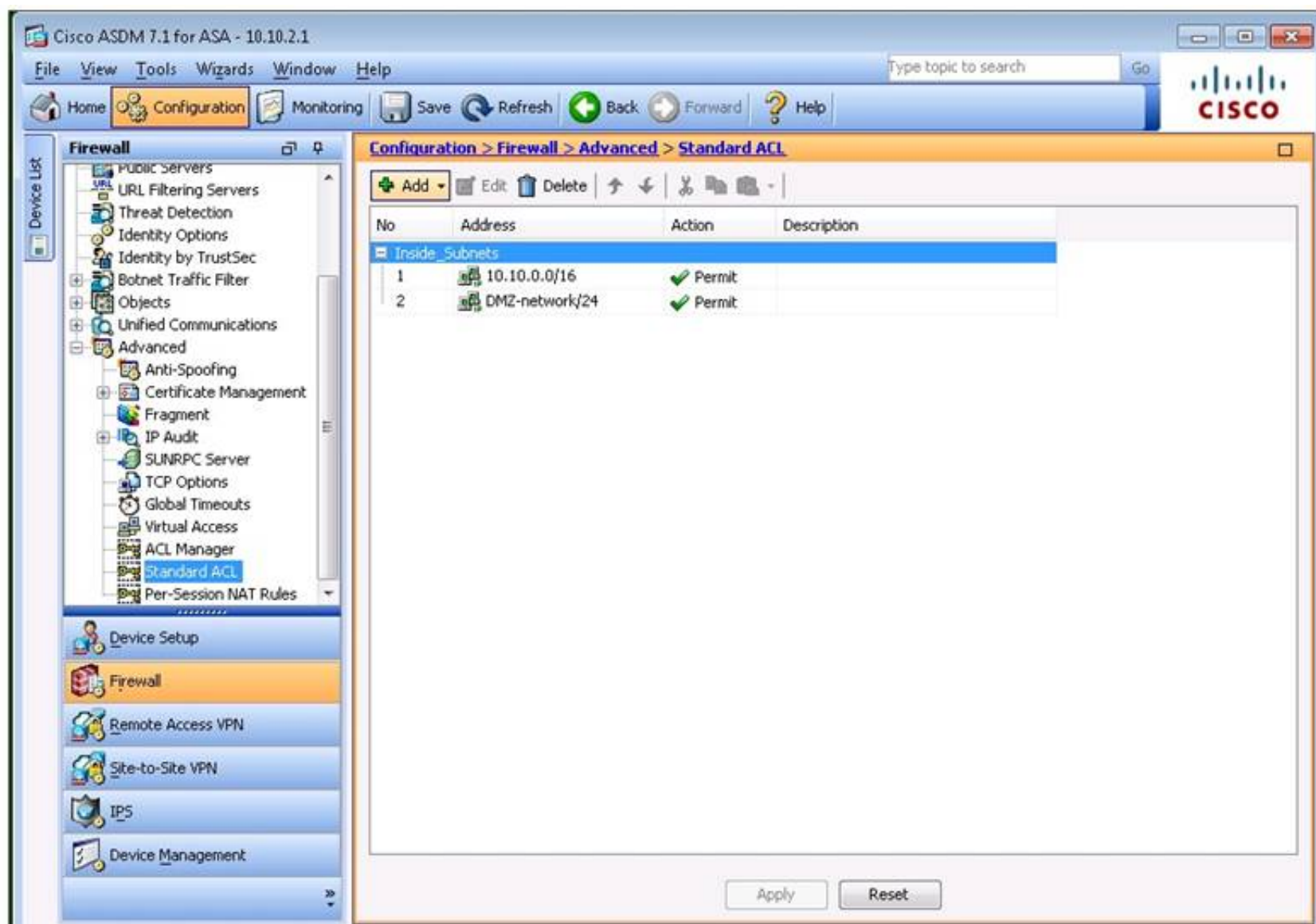
Apply Reset


The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree with 'NAT Rules' selected. The main pane shows the 'Configuration > Firewall > NAT Rules' page. It features a table with two columns: 'Match Criteria: Original Packet' and 'Action: Translated Packet'. The table lists several NAT rules, including 'outside-nat-p...', 'AnyConnect...', 'HQ-srv', 'MAIL', 'DMZ-server', 'NAT', and 'ESA'. The bottom of the pane has 'Apply' and 'Reset' buttons.


#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
1	inside	outside	any	any	any	outside-nat-p...	-- Original --	-- Original --
2	Any	outside	any	AnyConnect...	any	-- Original -- (S)	-- Original --	-- Original --
	outside	Any	AnyConnect...	any	any	-- Original -- (S)	-- Original --	-- Original --
"Network Object" NAT (Rules 3-7)								
3	Any	Any	HQ-srv	any	any	192.0.2.25 (S)	-- Original --	-- Original --
	Any	Any	any	192.0.2.25	any	-- Original -- (S)	HQ-srv	-- Original --
4	inside	outside	MAIL	any	any	192.0.2.25 (S)	-- Original --	-- Original --
	outside	inside	any	192.0.2.25	any	-- Original -- (S)	MAIL	-- Original --
5	DMZ	outside	DMZ-server	any	any	DMZ-server-g...	-- Original --	-- Original --
	outside	DMZ	any	DMZ-server...	any	-- Original -- (S)	DMZ-server	-- Original --
6	DMZ	outside	NAT	any	any	192.0.2.50 (S)	-- Original --	-- Original --
	outside	DMZ	any	192.0.2.50	any	-- Original -- (S)	NAT	-- Original --
7	Any	Any	ESA	any	any	192.0.2.55 (S)	-- Original --	-- Original --
	Any	Any	any	192.0.2.55	any	-- Original -- (S)	ESA	-- Original --

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree with 'Advanced' selected. The main pane shows the 'Configuration > Firewall > Advanced' page. It contains a list of items under the heading 'This section contains the following items:'. The items are: Anti-Spoofing, Certificate Management, Fragment, IP Audit, SUNRPC Server, TCP Options, Global Timeouts, Virtual Access, ACL Manager, Standard ACL, and Per-Session NAT Rules.

- [Anti-Spoofing](#)
- [Certificate Management](#)
- [Fragment](#)
- [IP Audit](#)
- [SUNRPC Server](#)
- [TCP Options](#)
- [Global Timeouts](#)
- [Virtual Access](#)
- [ACL Manager](#)
- [Standard ACL](#)
- [Per-Session NAT Rules](#)




Edit NAT Rule



Match Criteria: Original Packet

Source Interface:

inside

Destination Interface:

outside

Source Address:

any

Destination Address:

any

Service:

any

Action: Translated Packet

Source NAT Type:

Dynamic

Source Address:

outside-nat-pool

Destination Address:

-- Original --

☐ Use one-to-one address translation

☒ PAT Pool Translated Address:

Service:

-- Original --

☒ Round Robin

☐ Extend PAT uniqueness to per destination instead of per interface

☐ Translate TCP and UDP ports into flat range 1024-65535

☐ Include range 1-1023

☒ Fall through to interface PAT

☐ Use IPv6 for source interface PAT

☐ Use IPv6 for destination interface PAT

Options

☒ Enable rule

☒ Translate DNS replies that match this rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface

Direction:


Both

Description:

OK

Cancel

Help


Edit NAT Rule

Match Criteria: Original Packet

Source Interface: -- Any --

Destination Interface: outside

Source Address: any

Destination Address: AnyConnect_Clients

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original --

Destination Address: -- Original --

☐ Use one-to-one address translation

☐ PAT Pool Translated Address:

Service: -- Original --

☐ Round Robin
☐ Extend PAT uniqueness to per destination instead of per interface
☐ Translate TCP and UDP ports into flat range 1024-65535
☐ Include range 1-1023

☐ Fall through to interface PAT
☐ Use IPv6 for source interface PAT
☐ Use IPv6 for destination interface PAT

Options

☒ Enable rule
☐ Translate DNS replies that match this rule
☐ Disable Proxy ARP on egress interface
☐ Lookup route table to locate egress interface

Direction: Both

Description:

OK

Cancel

Help

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Network (Client) Access

- AnyConnect Connection Profiles
- AnyConnect Customization/Local
- AnyConnect Client Profile
- AnyConnect Client Software
- Dynamic Access Policies
- Group Policies
- IPsec(IKEv1) Connection Profiles
- Secure Mobility Solution
- Address Assignment
- Assignment Policy
- Address Pools
- Advanced
- AnyConnect Custom Attribut
- Endpoint Security
- IPsec
- ACL Manager
- Clientless SSL VPN Access
- AAA/Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

IPS

Device Management

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
GroupPolicy1	Internal	ikev1	203.0.113.1
GroupPolicy2	Internal	ssl-client	AnyConnect_Profile
DfltGrpPolicy (System Defa...	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultWEB...

Find: Match Case

Apply Reset

Edit Internal Group Policy: GroupPolicy2

General

Servers

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- IPsec(IKEv1) Client

Name: GroupPolicy2

Banner: ☒ Inherit

SCEP forwarding URL: ☒ Inherit

Address Pools: ☒ Inherit

IPv6 Address Pools: ☒ Inherit

More Options

Find: Next Previous

OK Cancel Help

Edit Internal Group Policy: GroupPolicy2

General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List'

DNS Names: ☒ Inherit

Send All DNS Lookups Through Tunnel: ☒ Inherit ☐ Yes ☐ No

Policy: ☒ Inherit

IPv6 Policy: ☒ Inherit

Network List: ☒ Inherit

Pressing this button to set up split exclusion for Web Security proxies.
 Set up split exclusion for Web Security...

Intercept DHCP Configuration Message from Microsoft Clients

Find: ☐ Next ☐ Previous

OK Cancel Help

Edit Internal Group Policy: DfltGrpPolicy

General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below

DNS Names:

Send All DNS Lookups Through Tunnel: ☐ Yes ☒ No

Policy: Tunnel Network List Below

IPv6 Policy: Tunnel All Networks

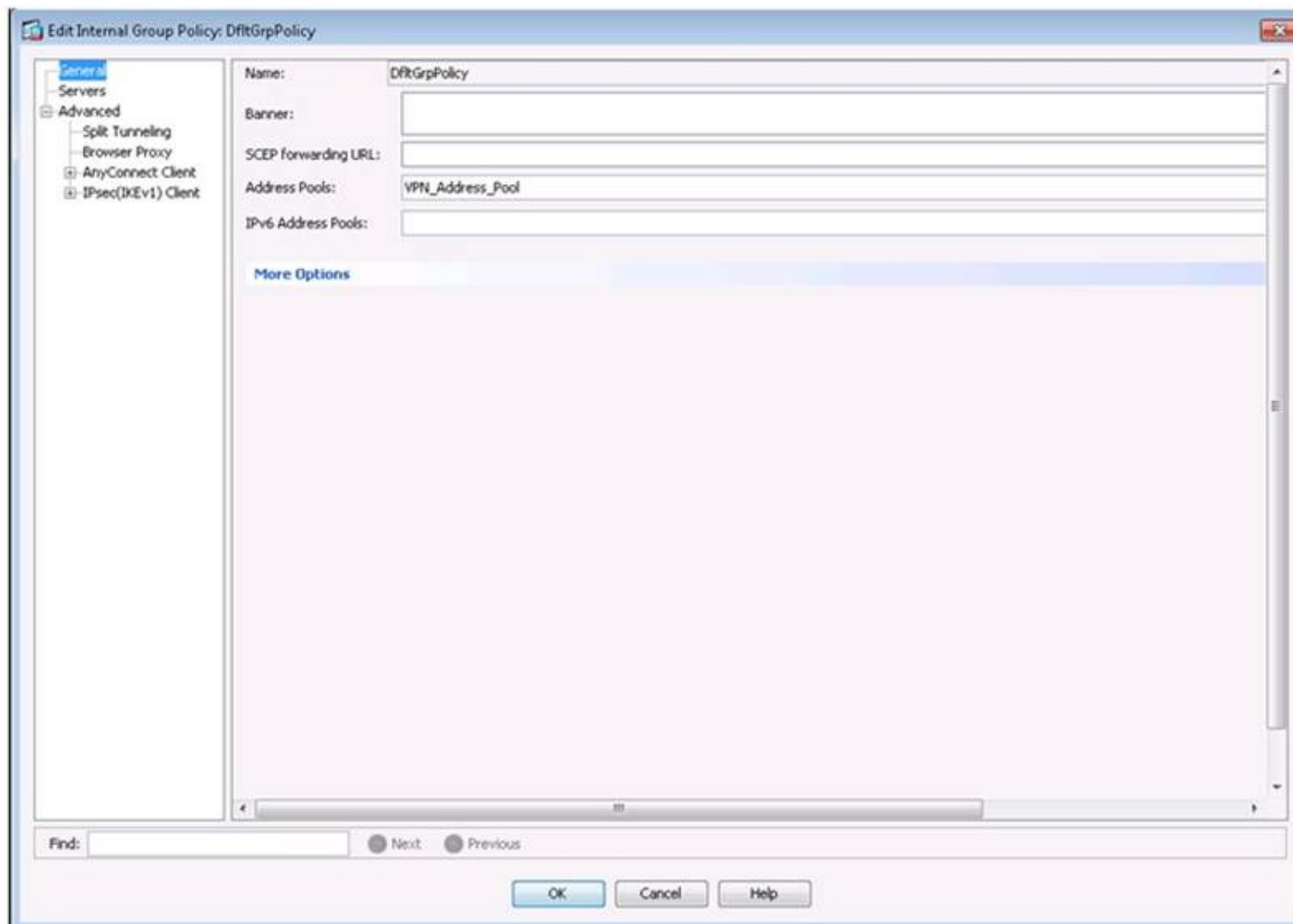
Network List: Inside_Subnets

Pressing this button to set up split exclusion for Web Security proxies.
 Set up split exclusion for Web Se...

Intercept DHCP Configuration Message from Microsoft Clients

Find: ☐ Next ☐ Previous

OK Cancel Help

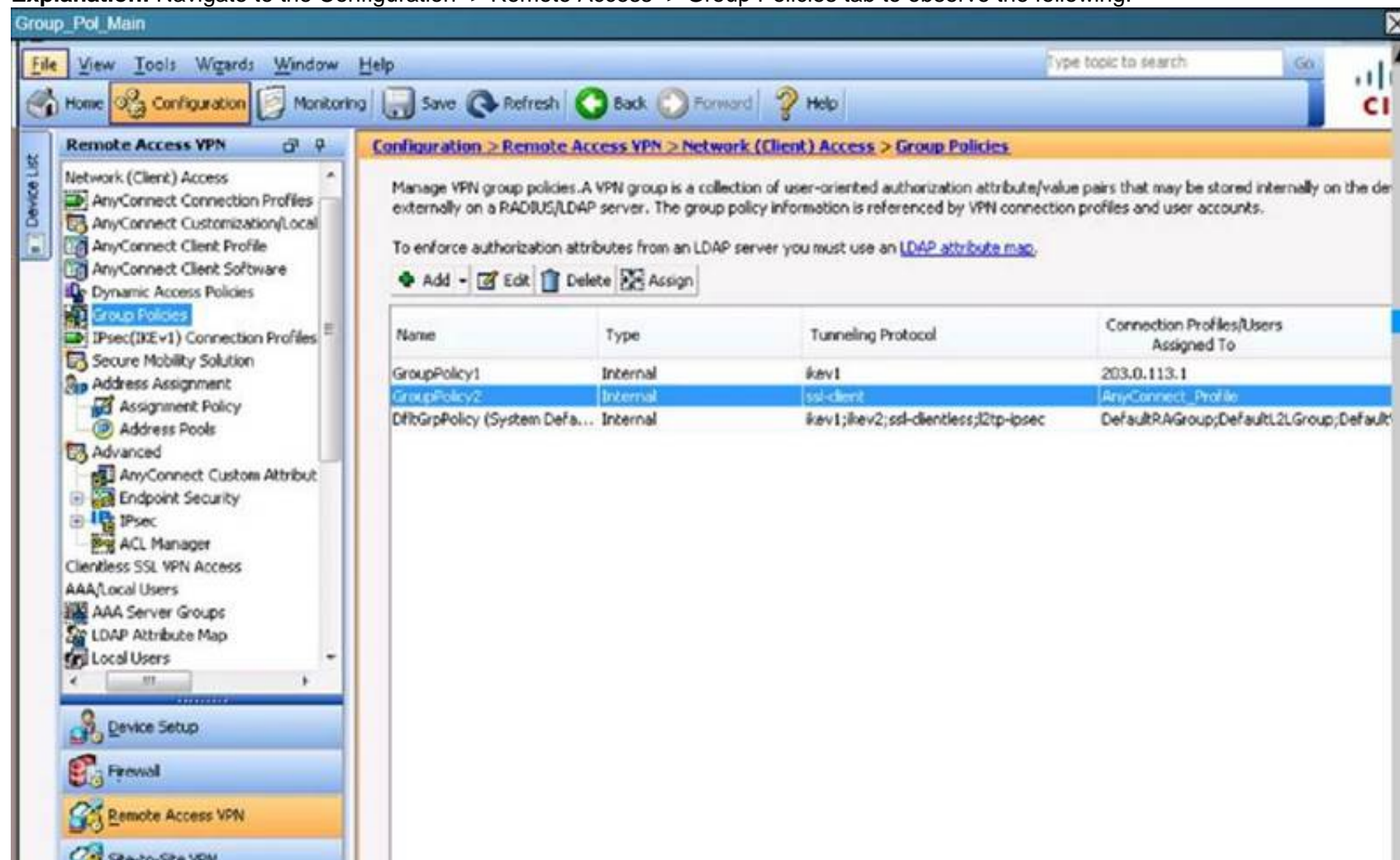


Which two networks will be included in the secured VPN tunnel? (Choose two.)

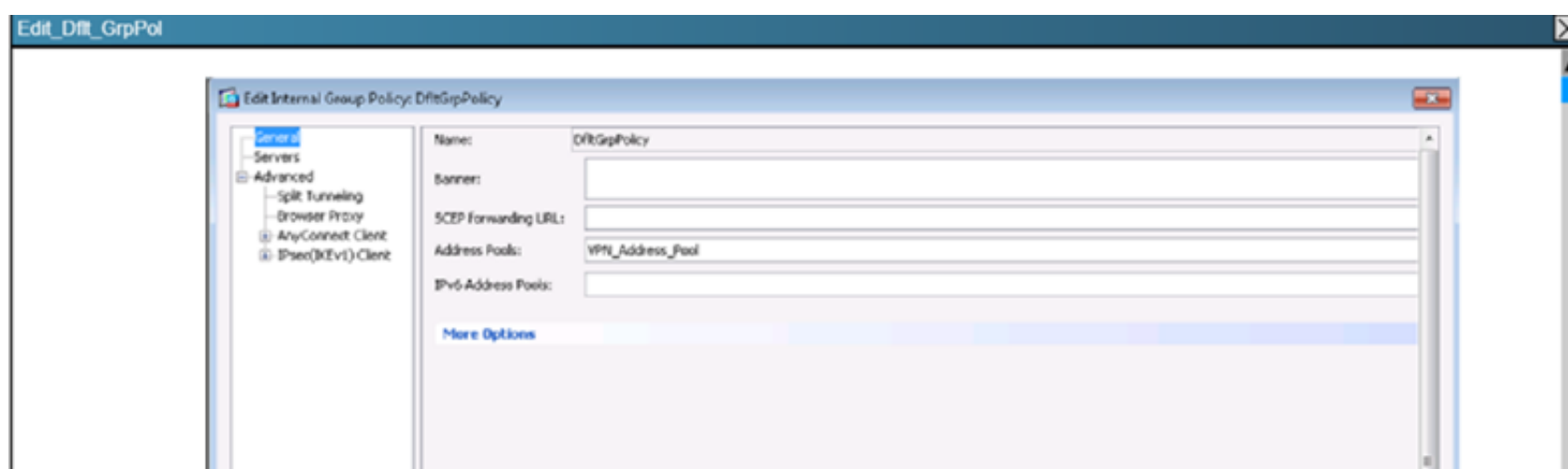
- A. 10.10.0.0/16
- B. All networks will be securely tunneled
- C. Networks with a source of any4
- D. 10.10.9.0/24
- E. DMZ network

Answer: AE

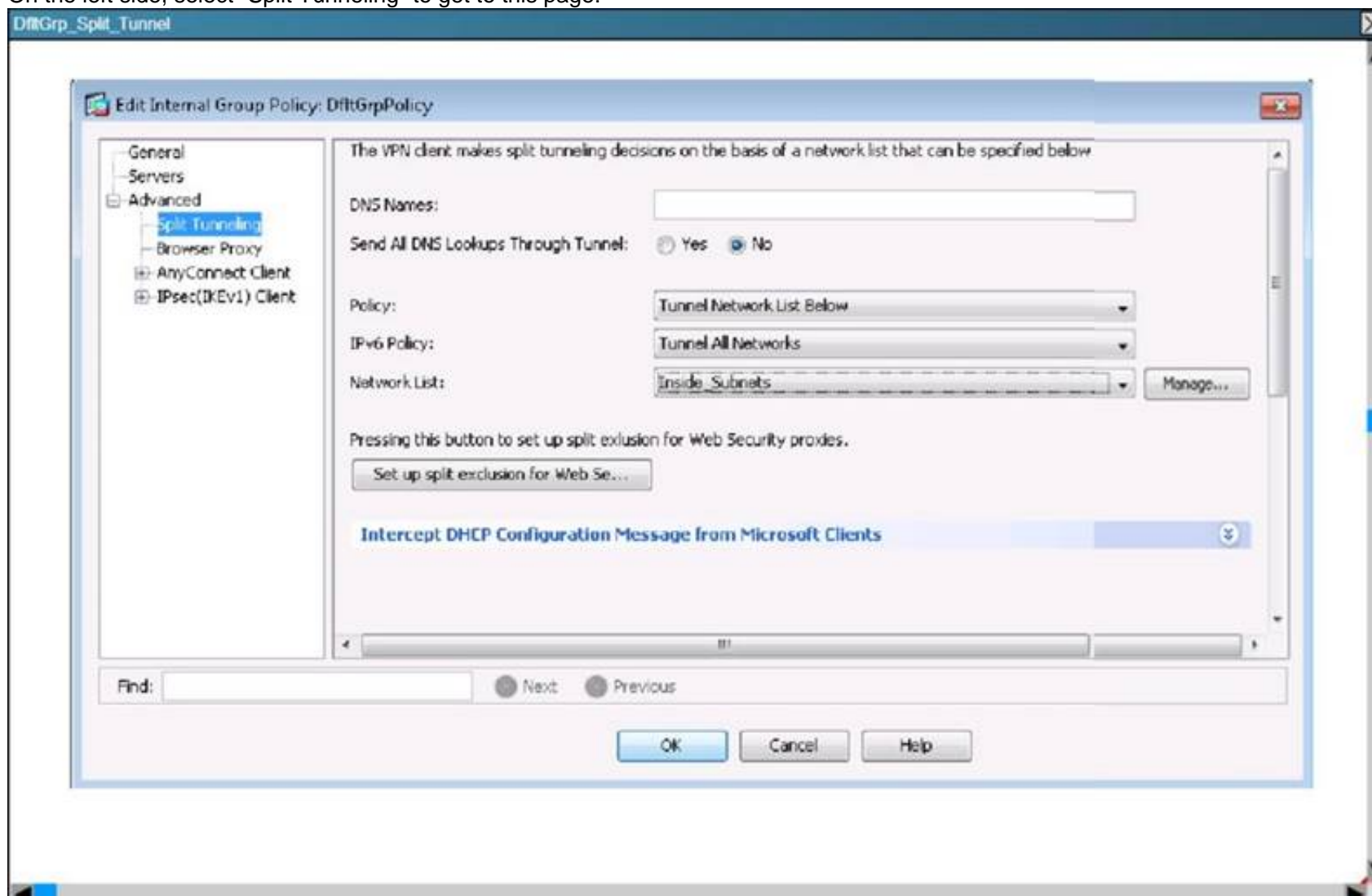
Explanation: Navigate to the Configuration -> Remote Access -> Group Policies tab to observe the following:



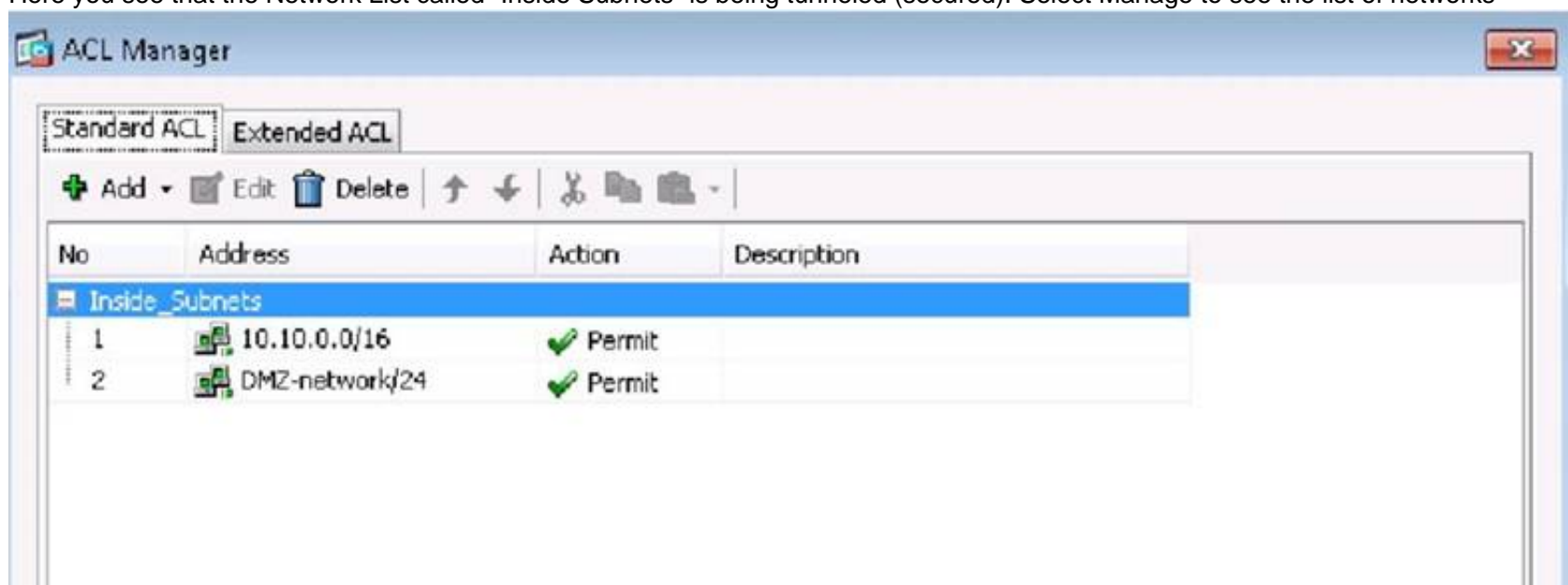
Then, click on the DfltGrpPolicy to see the following:



On the left side, select "Split Tunneling" to get to this page:



Here you see that the Network List called "Inside Subnets" is being tunneled (secured). Select Manage to see the list of networks



Here we see that the 10.10.0.0/16 and DMZ networks are being secured over the tunnel.

NEW QUESTION 229

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

NEW QUESTION 234

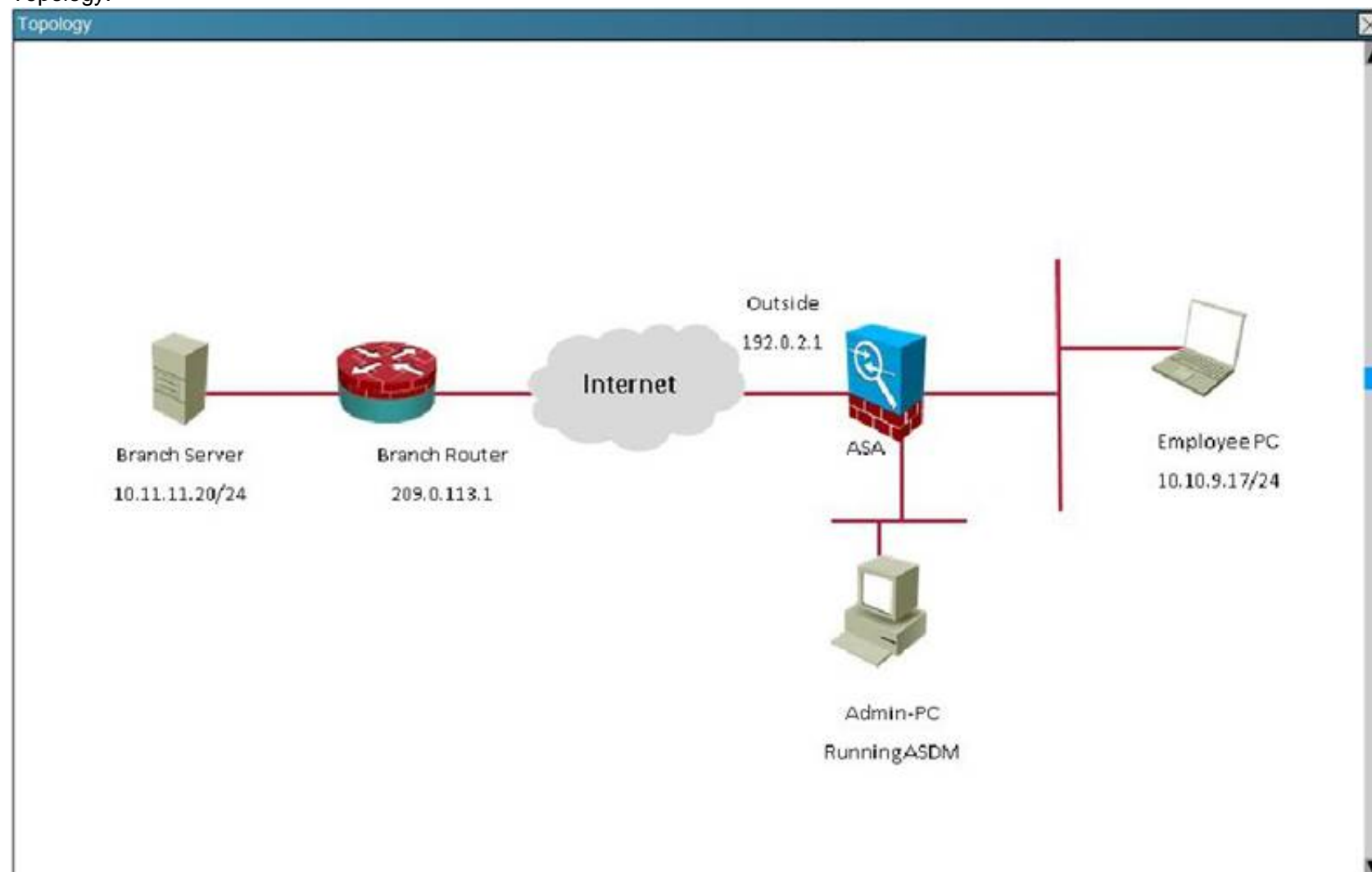
Scenario:

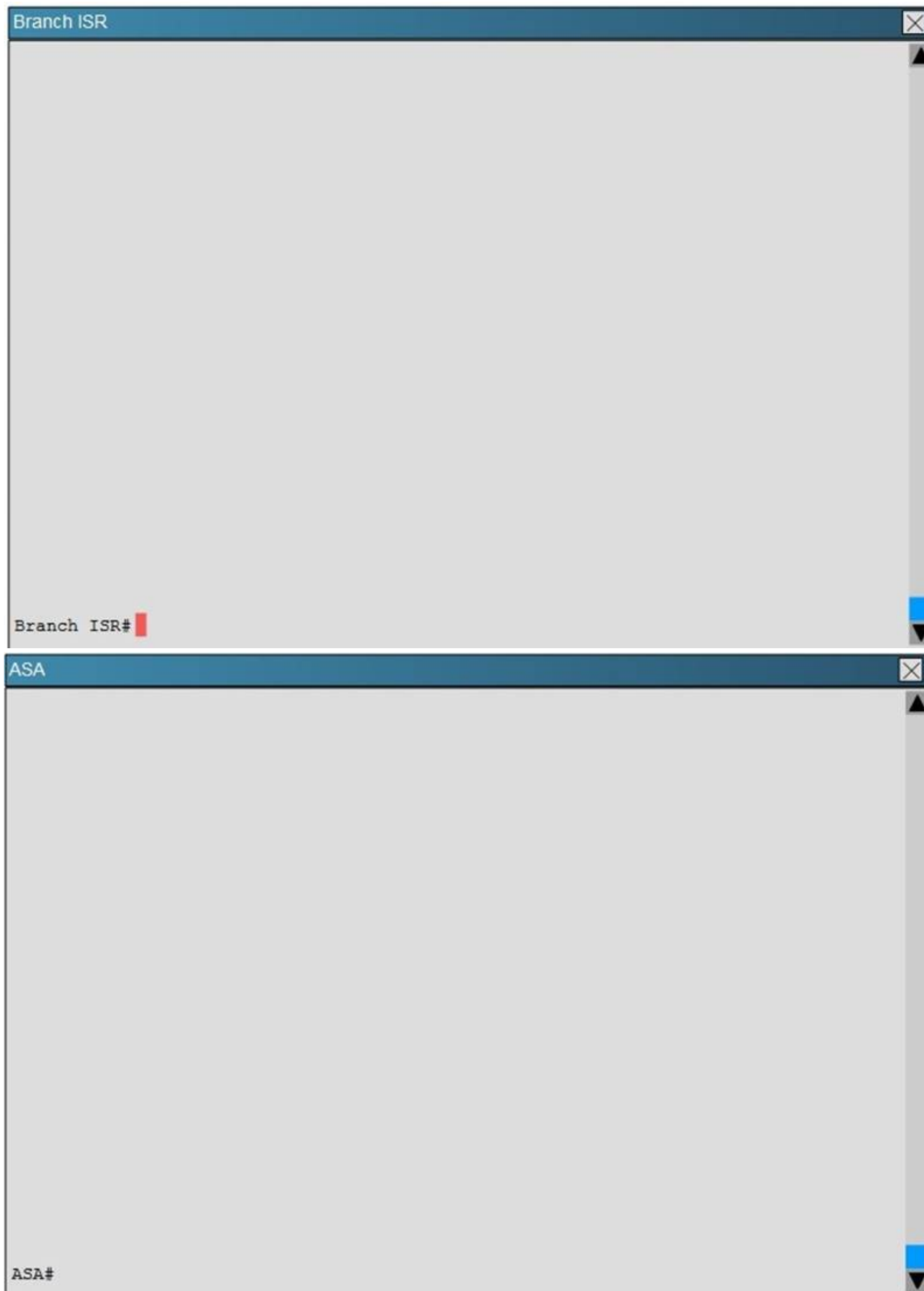
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

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 237

Which application does the Application Access feature of Clientless VPN support?

- A. TFTP
- B. VoIP
- C. Telnet
- D. active FTP

Answer: C

NEW QUESTION 238

Which VPN type can be used to provide secure remote access from public internet cafes and airport kiosks?

- A. site-to-site
- B. business-to-business
- C. Clientless SSL
- D. DMVPN

Answer: C

NEW QUESTION 243

Which option is an example of an asymmetric algorithm?

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

Answer: D

NEW QUESTION 244

Scenario:

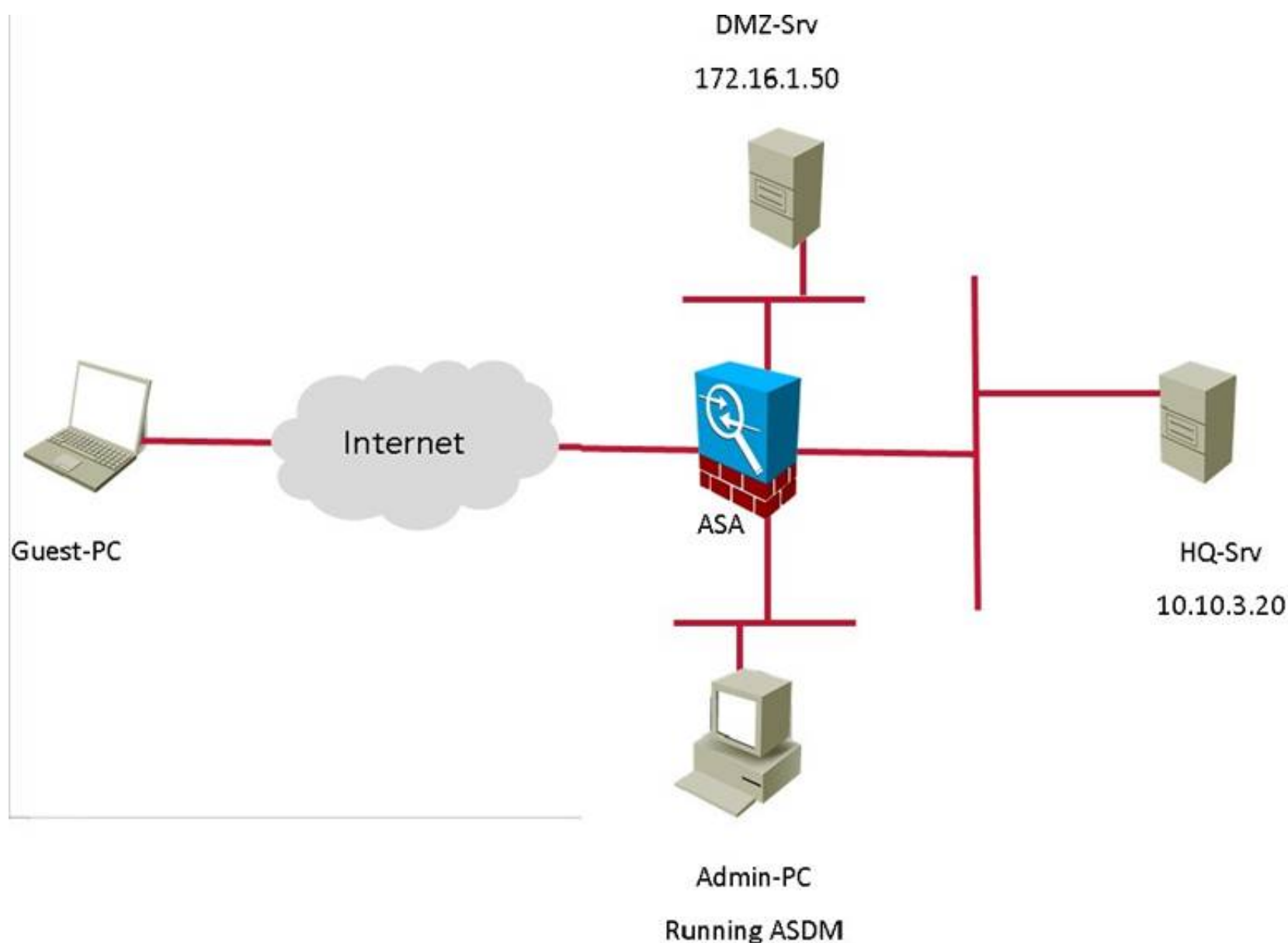
You are the network security manager for your organization. Your manager has received a request to allow an external user to access to your HQ and DM2 servers. You are given the following connection parameters for this task.

Using ASDM on the ASA, configure the parameters below and test your configuration by accessing the Guest PC. Not all ASDM screens are active for this exercise. Also, for this exercise, all changes are automatically applied to the ASA and you will not have to click APPLY to apply the changes manually.

- Enable Clientless SSL VPN on the outside interface
- Using the Guest PC, open an Internet Explorer window and test and verify the basic connection to the SSL VPN portal using address: <https://vpn-secure-x.public>
- a. You may notice a certificate error in the status bar, this can be ignored for this exercise
- b. Username: vpnuser
- c. Password: cisco123
- d. Logout of the portal once you have verified connectivity
- Configure two bookmarks with the following parameters:
- a. Bookmark List Name: MY-BOOKMARKS
- b. Use the: URL with GET or POST method
- c. Bookmark Title: HQ-Server
- i. <http://10.10.3.20>
- d. Bookmark Title: DMZ-Server-FTP
- i. <ftp://172.16.1.50>
- e. Assign the configured Bookmarks to:
- i. DfltGrpPolicy
- ii. DfltAccessPolicy
- iii. LOCAL User: vpnuser
- From the Guest PC, reconnect to the SSL VPN Portal
- Test both configured Bookmarks to ensure desired connectivity

You have completed this exercise when you have configured and successfully tested Clientless SSL VPN connectivity.

Topology:



ASDM

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard Intrusion Prevention

Device Information

General License

Host Name: HQ-ASA.secure-x.local

ASA Version: 9.1(1)4

ASDM Version: 7.1(2)

Firewall Mode: Routed

Environment Status: OK

Device Uptime: 2d 5h 26m 13s

Device Type: ASA 5515, IPS

Context Mode: Single

Total Flash: 8192 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
DMZ	172.16.1.1/24	up	up	0
Guest	10.10.250.1/24	up	up	0
Site-To-Site	172.16.2.1/24	up	up	0
inside	10.10.1.1/24	up	up	0
management	10.10.2.1/24	up	up	6
outside	192.0.2.1/24	up	up	0

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 Details

System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

4000

3500

3000

2500

2000

1500

1000

500

0

05:22 05:23 05:24 05:25 05:26

Connections Per Second Usage

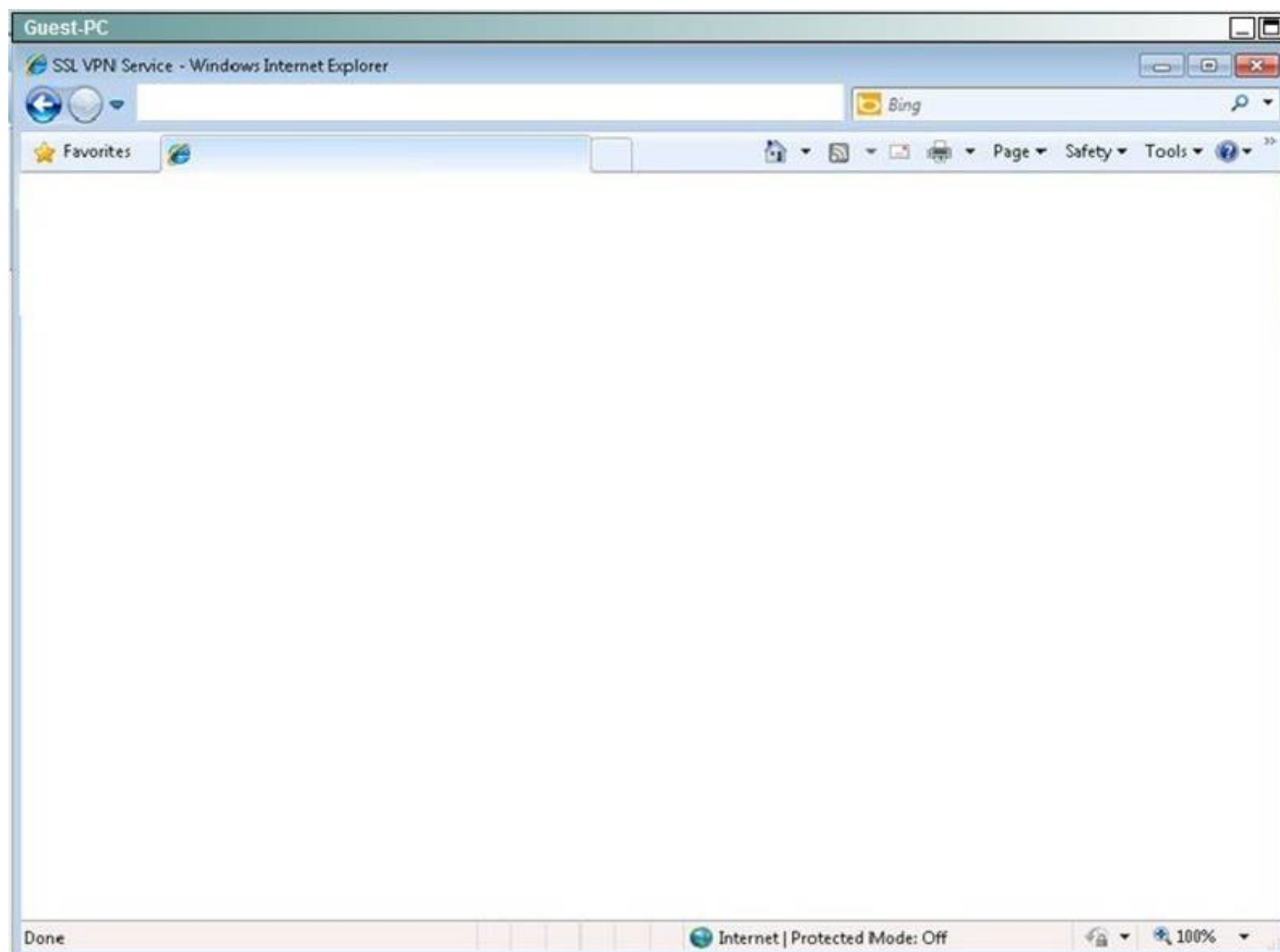
1

0

UDP: 0 TCP: 0 Total: 0

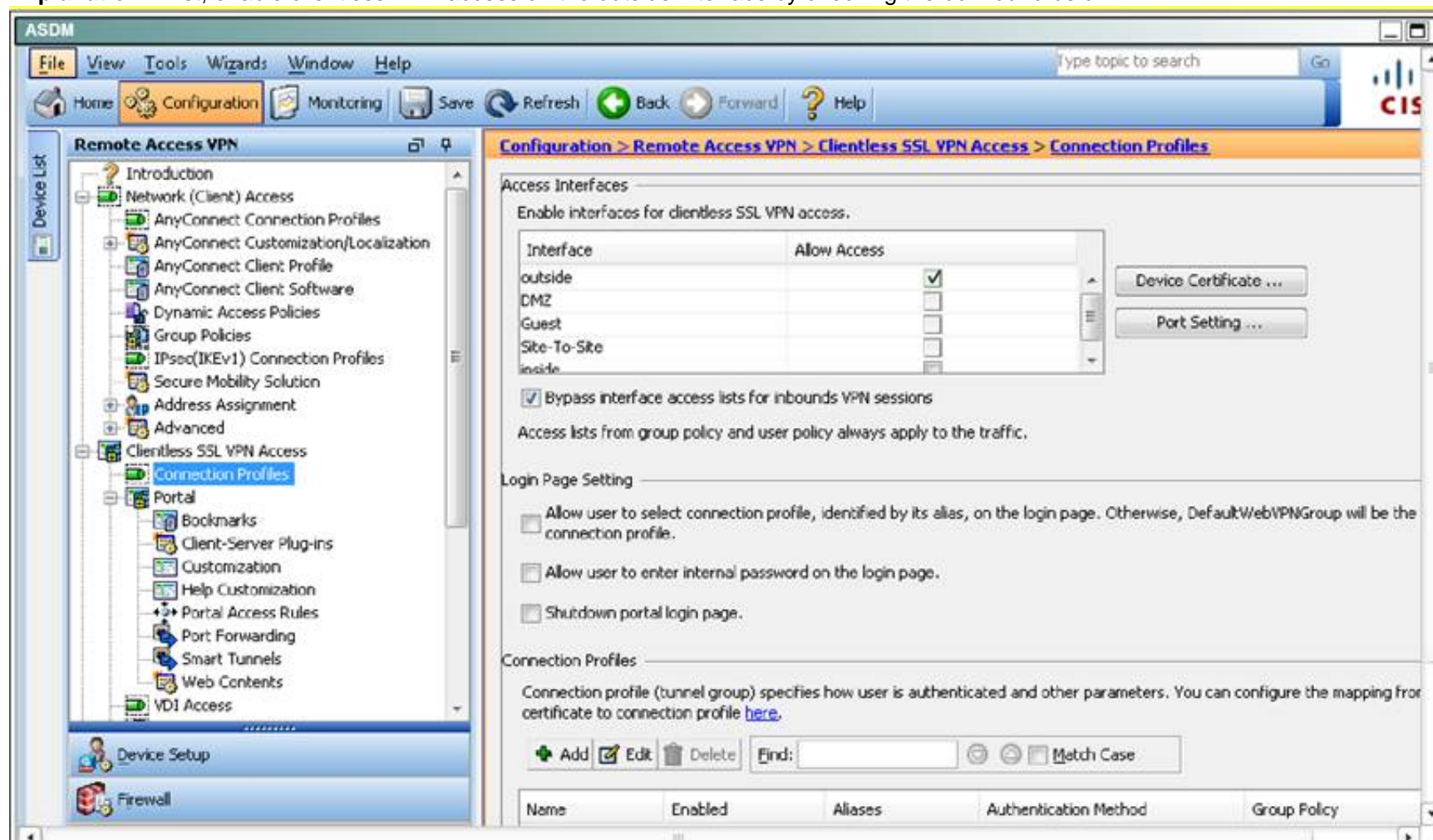
outside Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

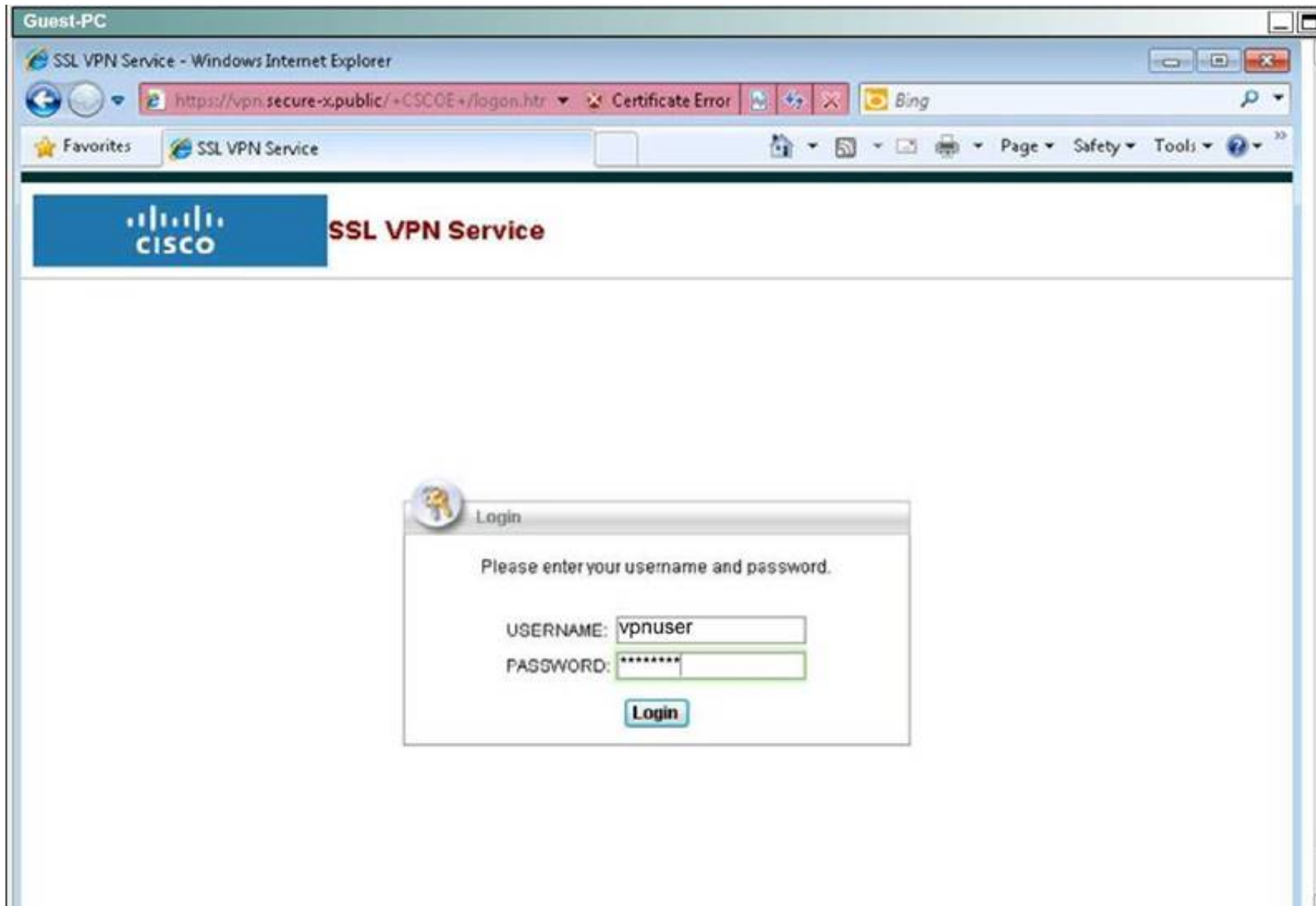


Answer:

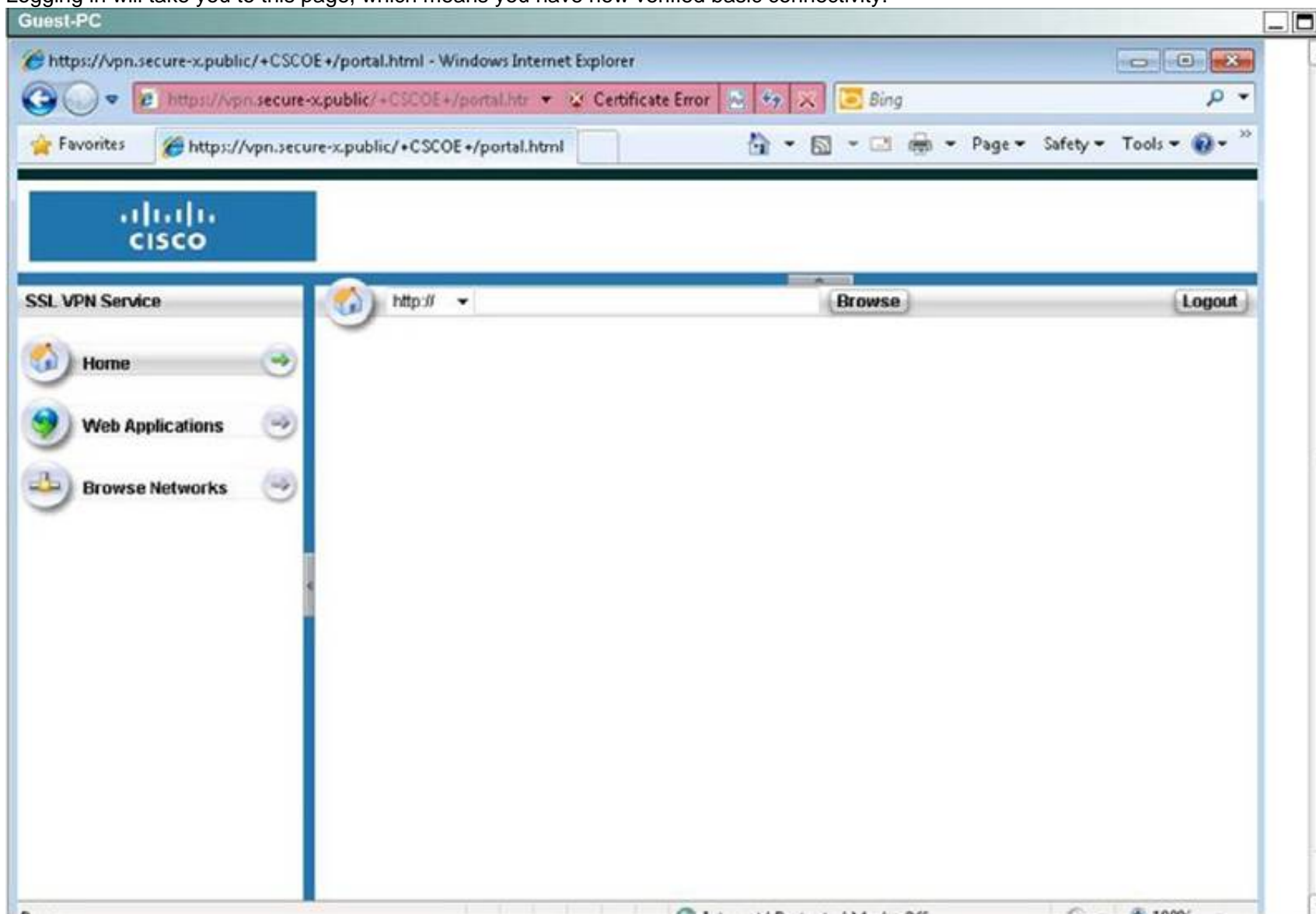
Explanation: First, enable clientless VPN access on the outside interface by checking the box found below:



Then, log in to the given URL using the vpnuser/cisco123 credentials:

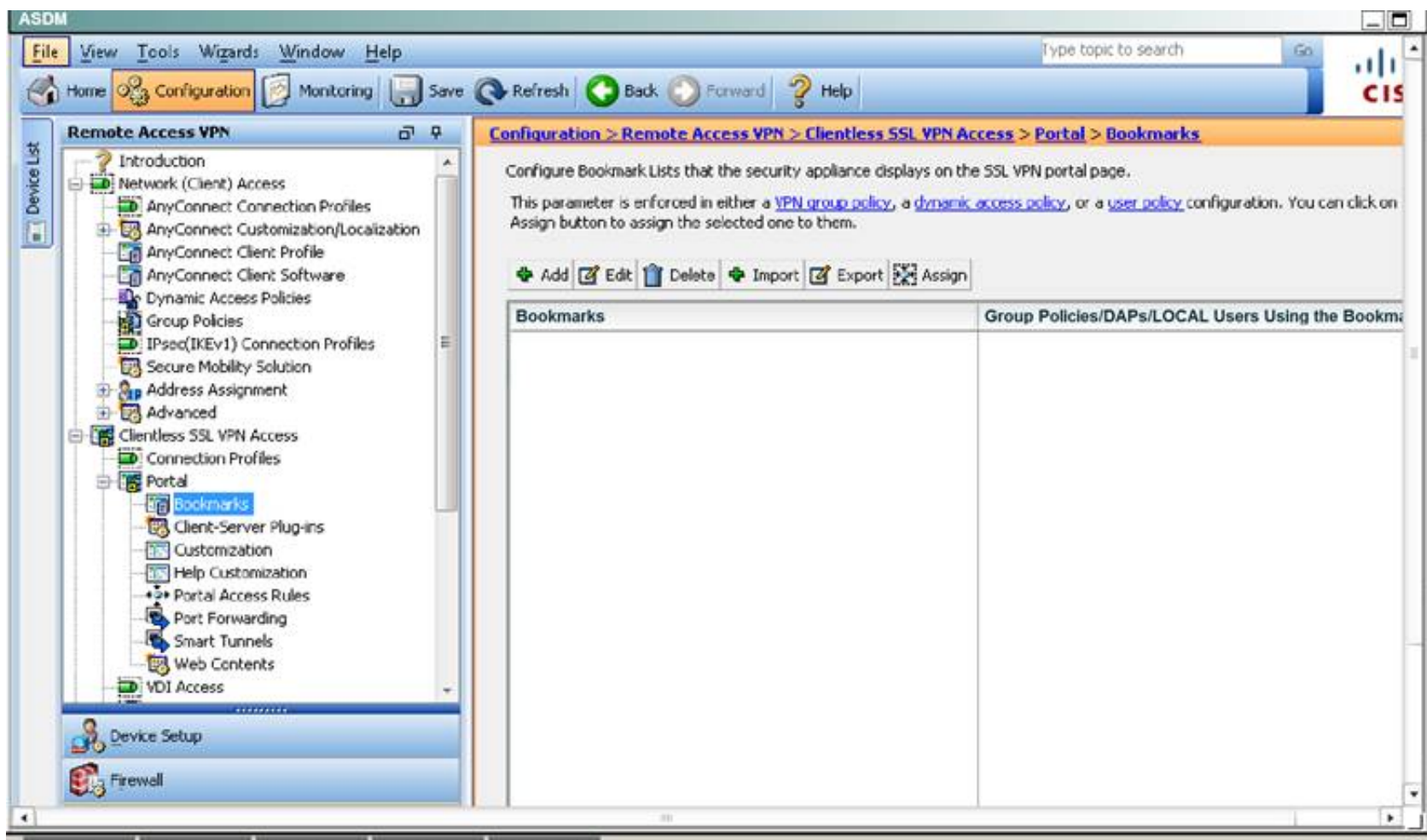


Logging in will take you to this page, which means you have now verified basic connectivity:

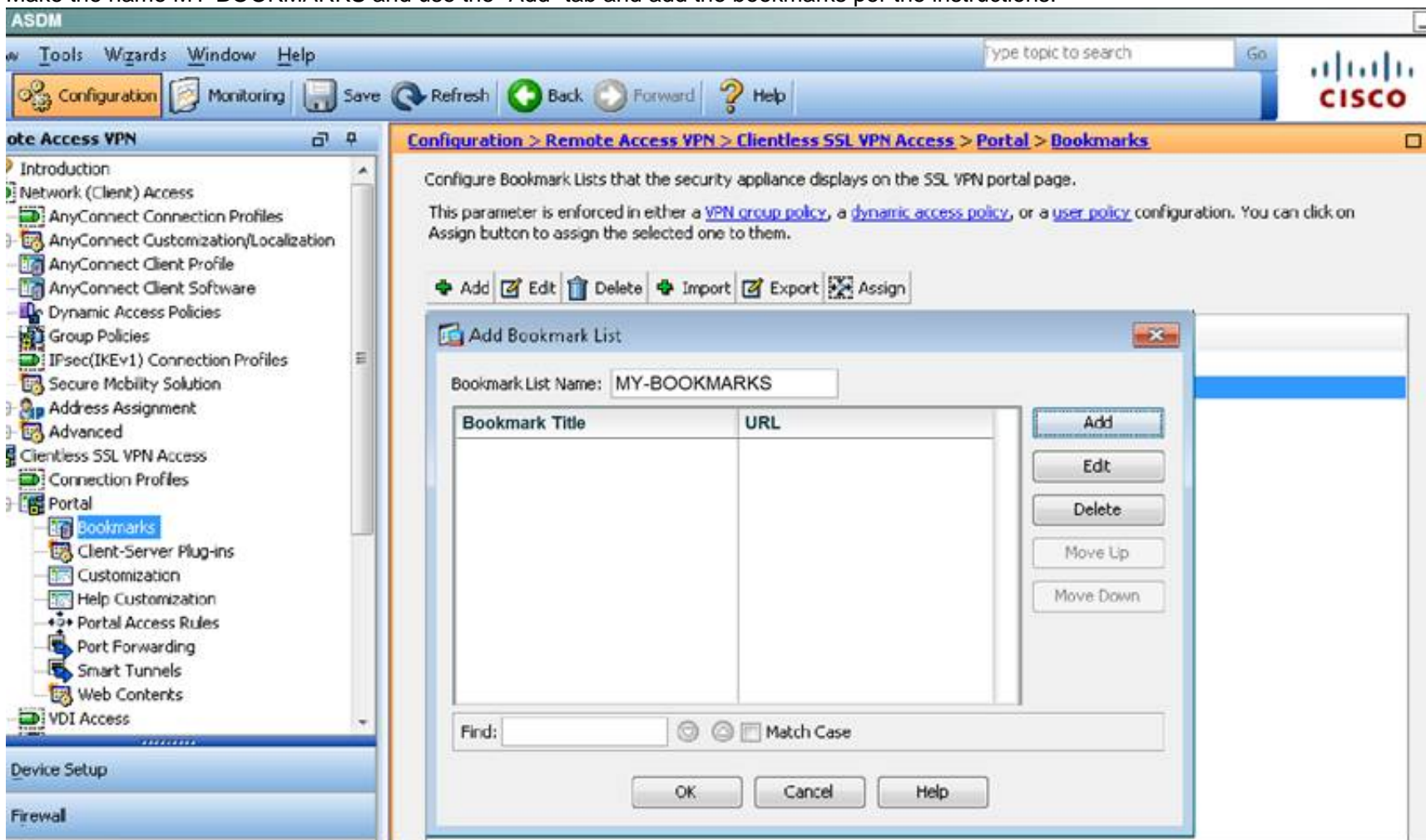


Now log out by hitting the logout button.

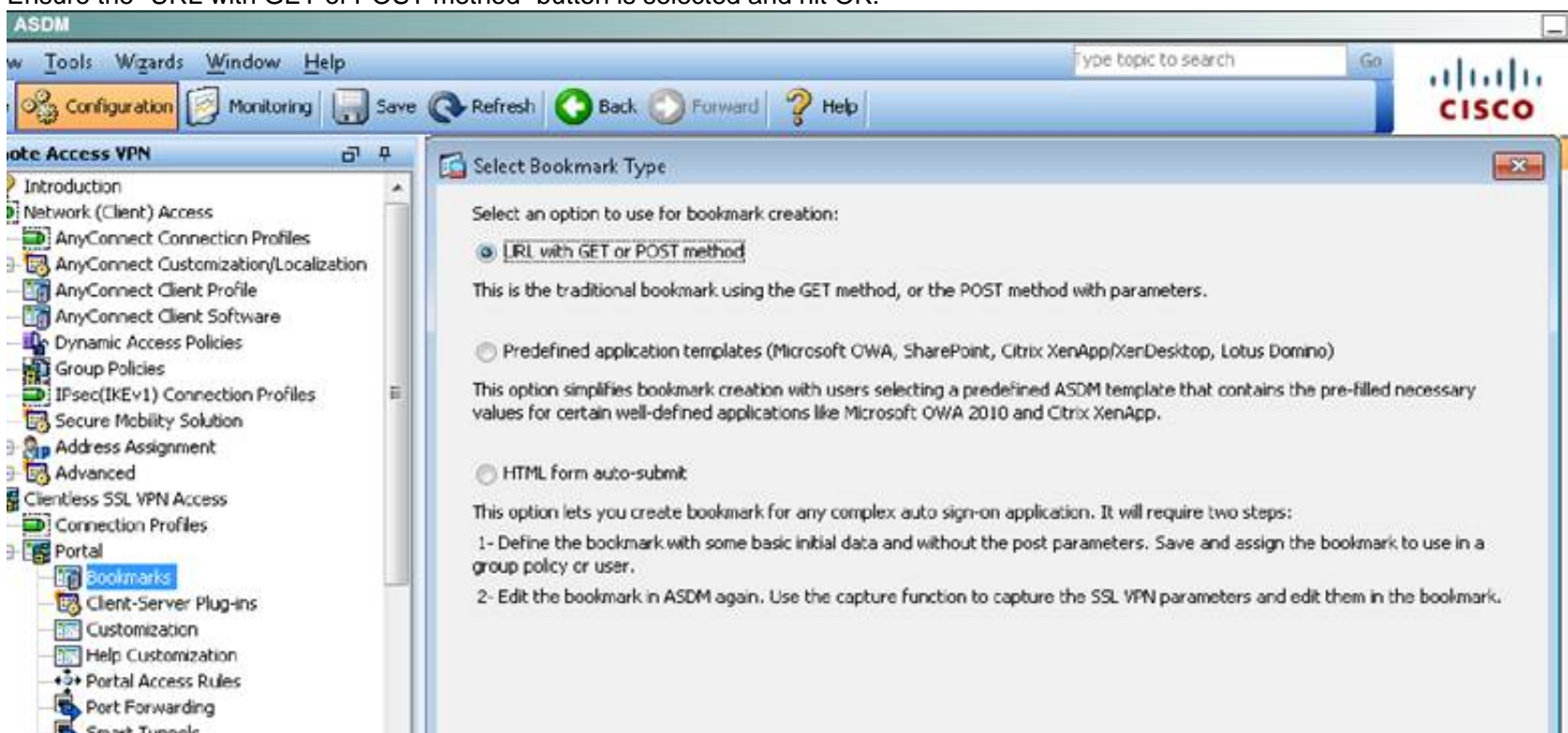
Now, go back to the ASDM and navigate to the Bookmarks portion:



Make the name MY-BOOKMARKS and use the "Add" tab and add the bookmarks per the instructions:



Ensure the "URL with GET or POST method" button is selected and hit OK:



Add the two bookmarks as given in the instructions:

Add Bookmark

Bookmark Title:

URL:

Preload Page (Optional)

Preload URL:

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

Thumbnail:

☒ Place this bookmark on the VPN home page

☐ Enable Smart Tunnel

Advanced Options

Add Bookmark

Bookmark Title:

URL:

Preload Page (Optional)

Preload URL:

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

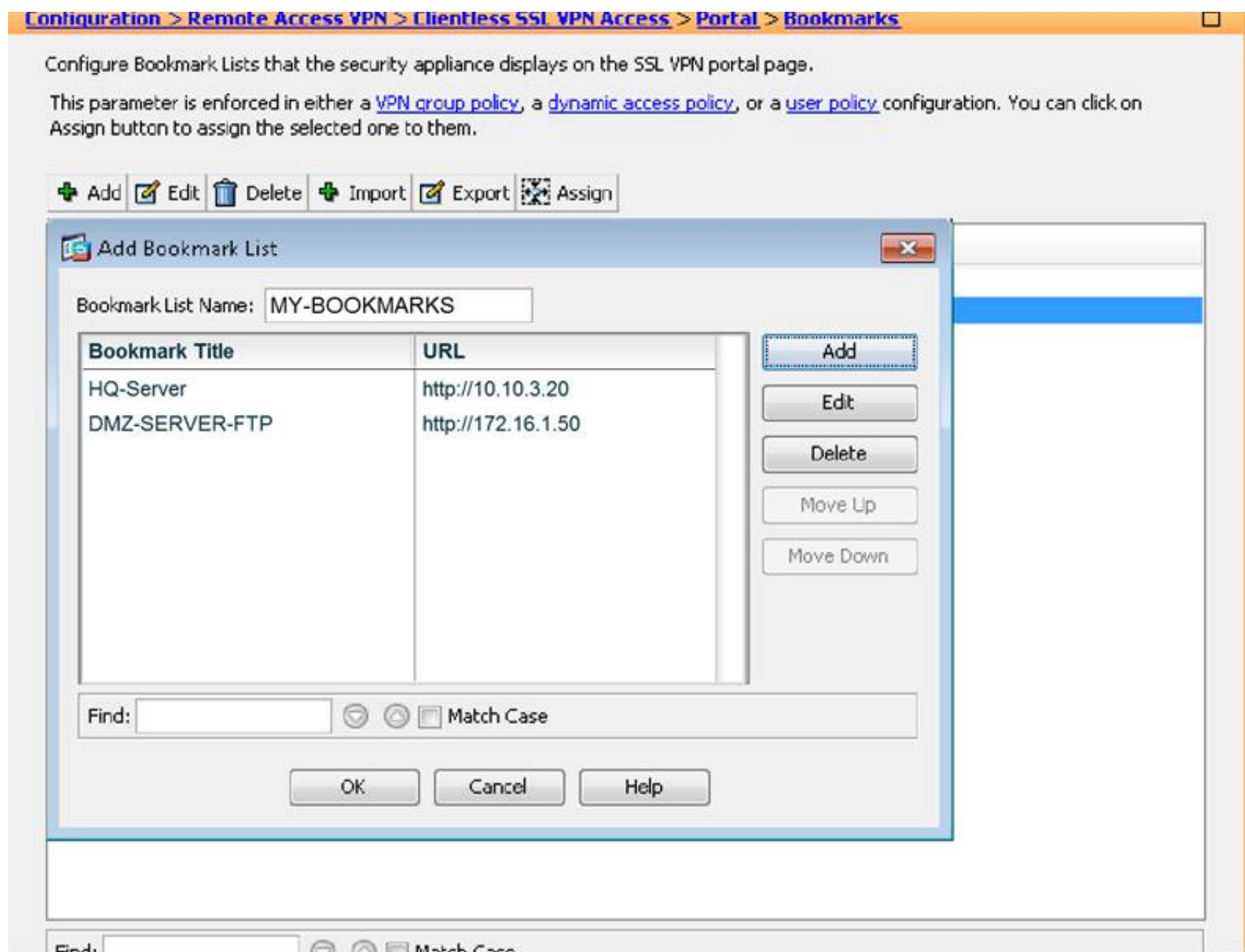
Thumbnail:

☒ Place this bookmark on the VPN home page

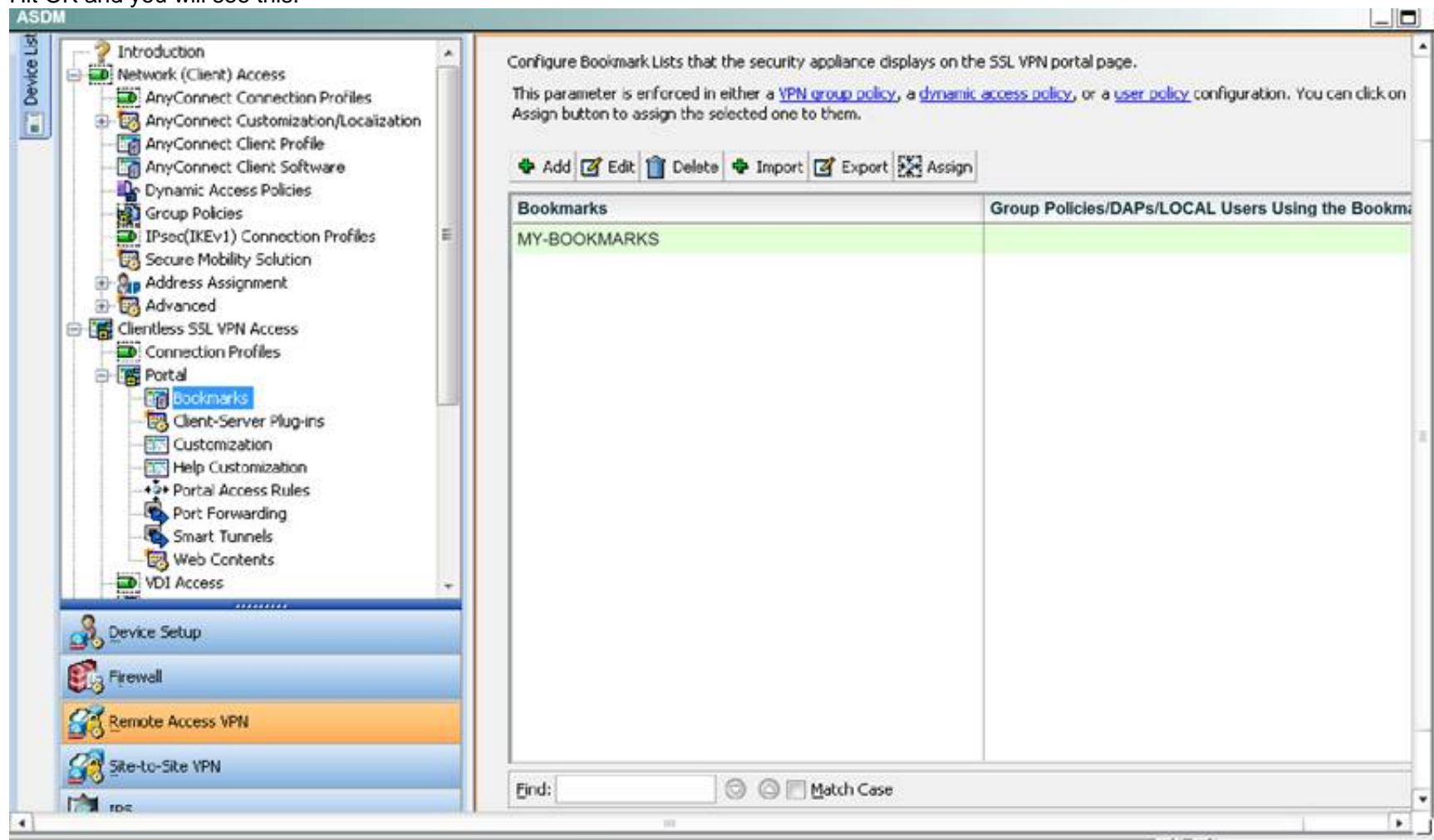
☐ Enable Smart Tunnel

Advanced Options

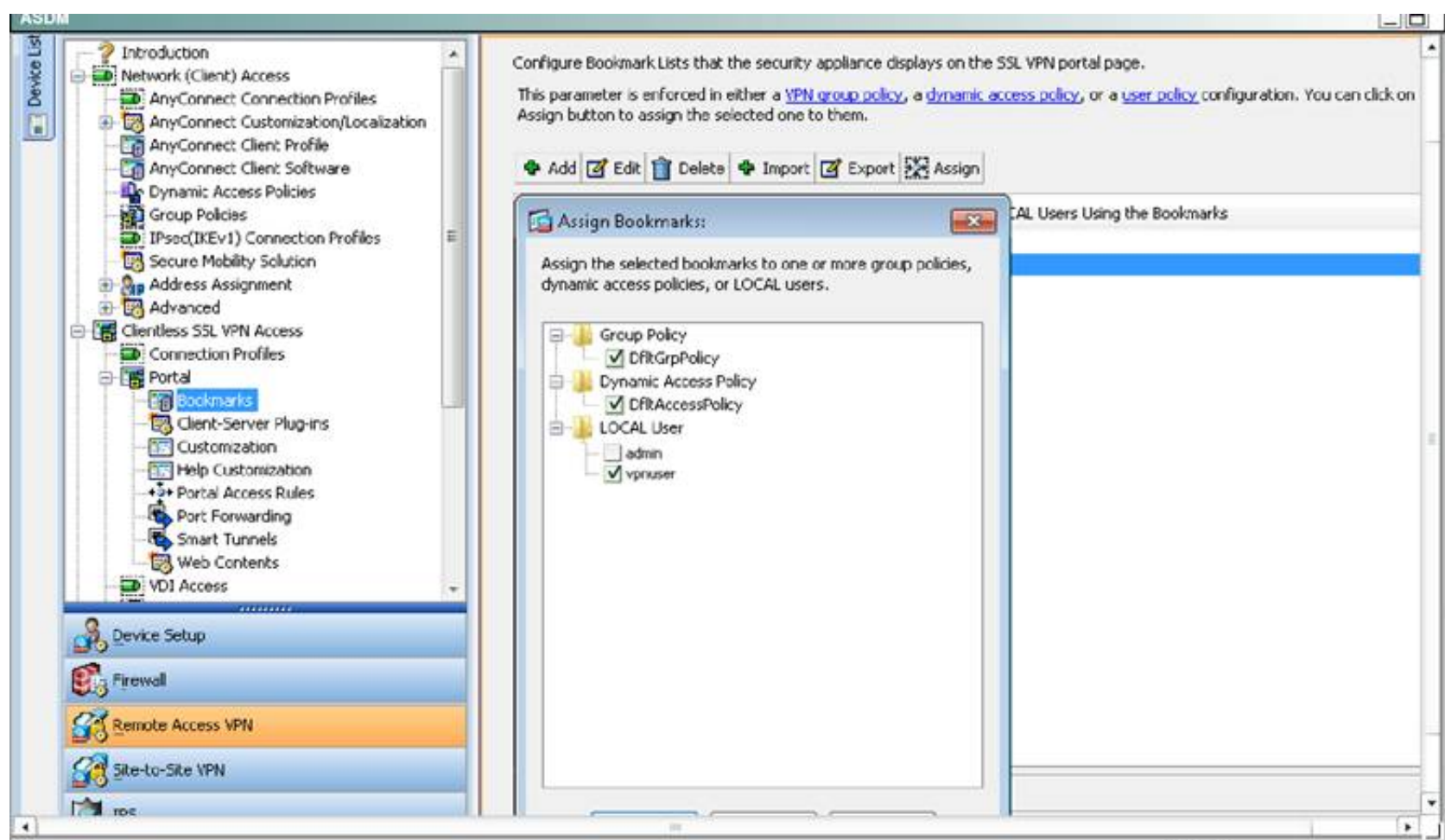
You should now see the two bookmarks listed:



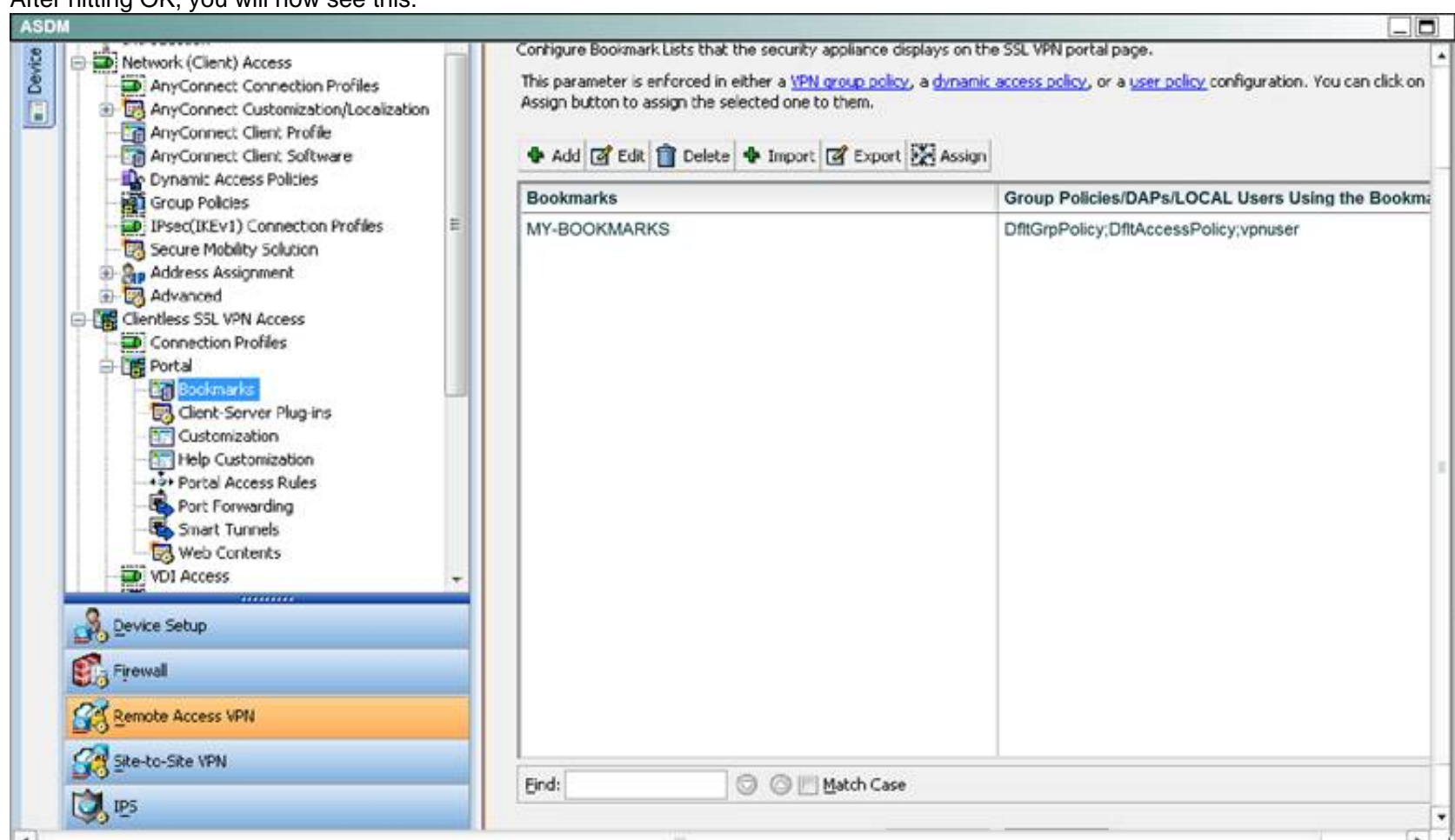
Hit OK and you will see this:



Select the MY-BOOKMARKS Bookmarks and click on the "Assign" button. Then, click on the appropriate check boxes as specified in the instructions and hit OK.



After hitting OK, you will now see this:



Then, go back to the Guest-PC, log back in and you should be able to test out the two new bookmarks.

NEW QUESTION 245

Which command enables the router to form EIGRP neighbor adjacencies with peers using a different subnet than the ingress interface?

- A. ip unnumbered interface
- B. eigrp router-id
- C. passive-interface interface name
- D. ip split-horizon eigrp as number

Answer: A

NEW QUESTION 248

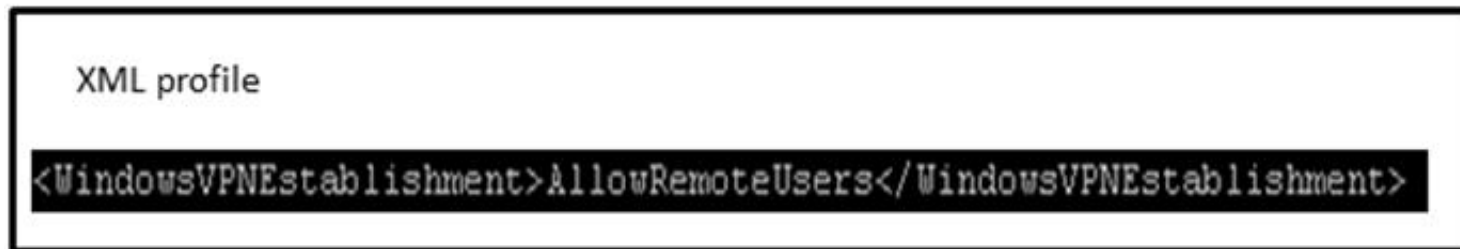
Which group-policy subcommand installs the Diagnostic AnyConnect Report Tool on user computers when a Cisco AnyConnect user logs in?

- A. customization value dart
- B. file-browsing enable
- C. smart-tunnel enable dart
- D. anyconnect module value dart

Answer: D

NEW QUESTION 251

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 defaultsvc profile test
- B. crypto vpn anyconnect profile test flash:RDP.xml webvpn context GW_1browser-attribute import flash:/swj.xml
- C. crypto vpn anyconnect profile test flash:RDP.xml policy group defaultsvc profile flash:RDP.xml
- D. crypto vpn anyconnect profile test flash:RDP.xml webvpn context GW_1browser-attribute import test

Answer: A

NEW QUESTION 252

Which type of NHRP packet is unique to Phase 3 DMVPN topologies?

- A. resolution request
- B. resolution reply
- C. redirect
- D. registration request
- E. registration reply
- F. error indication

Answer: C

NEW QUESTION 254

Which feature do you include in a highly available system to account for potential site failures?

- A. geographical separation of redundant devices
- B. hot/standby failover pairs
- C. Cisco ACE load-balancing with VIP
- D. dual power supplies

Answer: A

NEW QUESTION 256

Which two technologies are considered to be Suite B cryptography? (Choose two.)

- A. MD5
- B. SHA2
- C. Elliptical Curve Diffie-Hellman
- D. 3DES
- E. DES

Answer: BC

NEW QUESTION 258

Which two statements regarding IKEv2 are true per RFC 4306? (Choose two.)

- A. It is compatible with IKEv1.
- B. It has at minimum a nine-packet exchange.
- C. It uses aggressive mode.
- D. NAT traversal is included in the RFC.
- E. It uses main mode.
- F. DPD is defined in RFC 4309.
- G. It allows for EAP authentication.

Answer: DG

NEW QUESTION 263

Refer to the exhibit.

```
crypto isakmp policy 5
  authentication pre-share
  group 2

crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0
crypto isakmp nat keepalive 20
```

Which two statements about the given configuration are true? (Choose two.)

- A. Defined PSK can be used by any IPSec peer.
- B. Any router defined in group 2 will be allowed to connect.
- C. It can be used in a DMVPN deployment
- D. It is a LAN-to-LAN VPN ISAKMP policy.
- E. It is an AnyConnect ISAKMP policy.
- F. PSK will not work as configured

Answer: AC

NEW QUESTION 268

Scenario

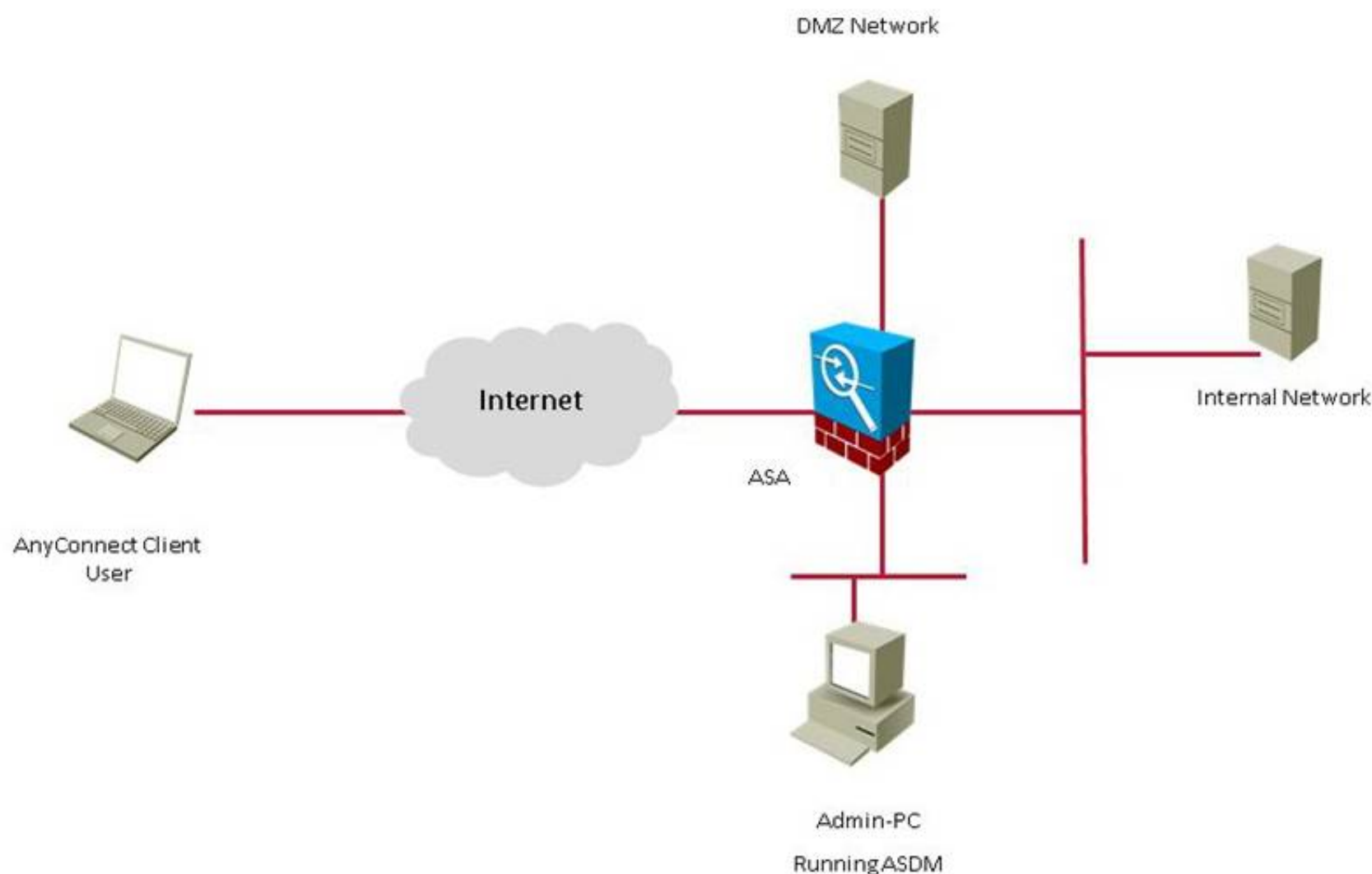
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

Note: Not all screens or option selections are active for this exercise.

Instructions

- Navigate the ASDM GUI on the device to verify network operation and answer for multiple-choice questions.
- You may have to use the scroll bars to view the entire ASDM Configuration screens.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- **NOT ALL SCREENS AND SELECTIONS ARE AVAILABLE FOR THIS EXERCISE.**
- Click on the Admin PC on the topology page to gain ASDM to the ASA. No passwords are required for this exercise.
- You may also click on the Default Home tab to access ASDM or return to the ASDM home screen at any time.
- There are **four (4)** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.
- To access the multiple-choice questions, click on the Questions tab and then numbered boxes on the left of the panel to view each question.

Topology



Default_Home



Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup

Startup Wizard

Interfaces

Routing

Device Name/Password

System Time

EtherChannel

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

IPS

Device Management

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Group
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native	
GigabitEthernet0/1		Enabled				native	
GigabitEthernet0/1.4	inside	Enabled	100	10.10.1.1	255.255.255.0	vlan4	
GigabitEthernet0/1.250	Guest	Enabled	30	10.10.250.1	255.255.255.0	vlan250	
GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native	
GigabitEthernet0/3	Site-To...	Enabled	60	172.16.2.1	255.255.255.0	native	
GigabitEthernet0/4		Enabled				native	
GigabitEthernet0/5		Enabled				native	
Management0/0	manage...	Enabled	90	10.10.2.1	255.255.255.0	native	

Enable traffic between two or more interfaces which are configured with same security levels

Enable traffic between two or more hosts connected to the same interface

Enable jumbo frame reservation

Apply Reset

Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts

Following are some important concepts for setting up a connection.

- 1. SSL tunnel and IPsec tunnel**
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(IKEv2) protocols, Cisco VPN Client supports only IPsec(IKEv1) protocol.
- 2. User and connection profile**
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.
You configure user account database in [AAA/Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(IKEv1\) Connection Profiles](#).
- 3. Access policy**
Access policies control how remote users can access corporate networks. An access policy includes the following:
 - Session control - how long a session can remain idle before it is closed.
 - Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [NAC](#) based ending security policies.

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below.

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☒ Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☐ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.




☒ Shutdown portal login page. Shutdown notice: Service out temporarily.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVP...	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
AnyConnect_P...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyConnect_VPN_User	AAA(LOCAL)	GroupPolicy2

Select Address Pools

 Add
  Edit
  Delete

Pool Name	Starting Address	Ending Address/Number of Addresses	Subnet Mask/Prefix Length
AC_Addre...	10.10.15.40	10.10.15.50	255.255.255.0
Outside_A...	209.165.201.20	209.165.201.30	255.255.255.0
Remote_A...	192.168.1.100	192.168.1.150	255.255.255.0
VPN_Addr...	10.10.15.20	10.10.15.30	255.255.255.0

Assigned Address Pools

Assign-> VPN_Address_Pool

OK Cancel Help

Edit AnyConnect Connection Profile: AnyConnect_Profile

Basic

Advanced

Name: AnyConnect_Profile

Aliases: AnyConnect_VPN_User

Authentication

Method: ☒ AAA ☐ Certificate ☐ Both

AAA Server Group: LOCAL Manage...

☐ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

☒ None ☐ DHCP Link ☐ DHCP Subnet

Client Address Pools: VPN_Address_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: GroupPolicy2 Manage...

(Following field is an attribute of the group policy selected above.)

☒ Enable SSL VPN client protocol

☐ Enable IPsec(IKEv2) client protocol

DNS Servers: 10.10.3.20

WINS Servers:

Domain Name: secure-x.local

Find: Next Previous

OK Cancel Help

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree, with 'Access Rules' selected. The main pane shows the 'Configuration > Firewall > Access Rules' page. The table below lists the configured access rules.

Enabled	Source Criteria:	Destination Criteria:	Service			
	Source	User	Security Group	Destination	Security Group	
DMZ (3 incoming rules)						
<input checked="" type="checkbox"/>	DMZ-server			any4		icmp
<input checked="" type="checkbox"/>	DMZ-server			HQ-srv		ftp
<input checked="" type="checkbox"/>	DMZ-server			any		domain
DMZ (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ-to-Site (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ (6 incoming rules)						
<input checked="" type="checkbox"/>	any4			DMZ-server		http
<input checked="" type="checkbox"/>	any4			DMZ-server		https
<input checked="" type="checkbox"/>	any4			DMZ-server		ftp
<input checked="" type="checkbox"/>	any4			DMZ-server		icmp
<input checked="" type="checkbox"/>	any4			DMZ-server		snmp
<input checked="" type="checkbox"/>	any4			DMZ-server		domain
DMZ (1 implicit rule)						
	any			any		ip

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Remote Access VPN' configuration tree, with 'ACL Manager' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access > Advanced > ACL Manager' page. The table below lists the configured ACL rules.

#	Enabled	Source	User	Security Group	Destination	Security
DMZ_access_in						
1	<input checked="" type="checkbox"/>	DMZ-server			any4	
2	<input checked="" type="checkbox"/>	DMZ-server			HQ-srv	
3	<input checked="" type="checkbox"/>	DMZ-server			any	
outside_access_in						
1	<input checked="" type="checkbox"/>	any4			DMZ-server	
2	<input checked="" type="checkbox"/>	any4			DMZ-server	
3	<input checked="" type="checkbox"/>	any4			DMZ-server	
4	<input checked="" type="checkbox"/>	any4			DMZ-server	
5	<input checked="" type="checkbox"/>	any4			DMZ-server	
6	<input checked="" type="checkbox"/>	any4			DMZ-server	
outside_cryptomap						
1	<input checked="" type="checkbox"/>	10.10.9.0/24			10.11.11.0/24	
permit-all						
1	<input checked="" type="checkbox"/>	any			any	

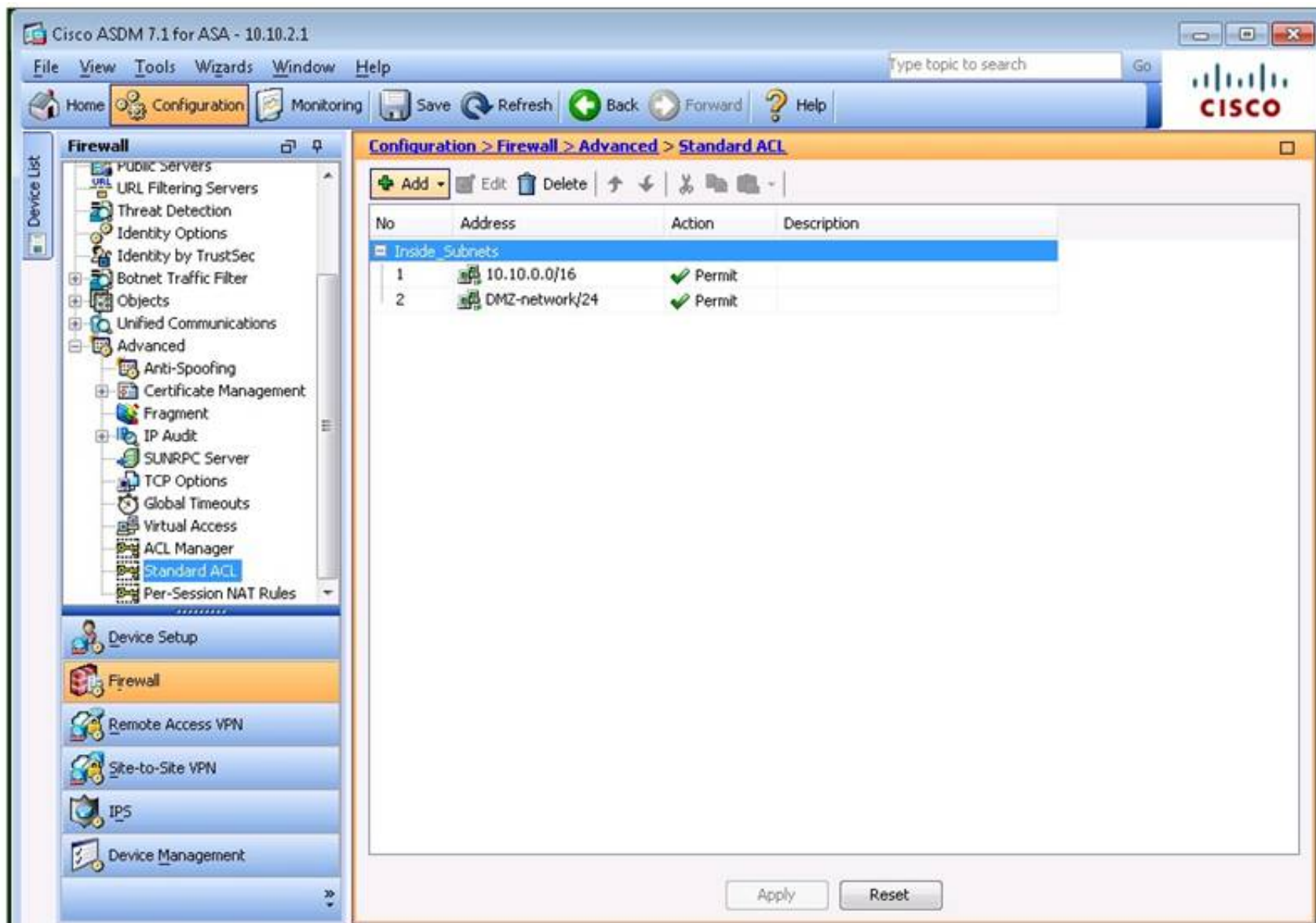
The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree with 'NAT Rules' selected. The main pane shows the 'Configuration > Firewall > NAT Rules' page. It features a table with 'Match Criteria: Original Packet' and 'Action: Translated Packet' columns. The table lists several NAT rules, including 'Network Object' NAT (Rules 3-7) and 'Any' NAT rules. The 'Match Criteria' columns include Source Intf, Dest Intf, Source, Destination, and Service. The 'Action' columns include Source, Destination, and Service. The table is as follows:

#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
1	inside	outside	any	any	any	outside-nat-p...	-- Original --	-- Original --
2	Any	outside	any	AnyConnect...	any	-- Original -- (S)	-- Original --	-- Original --
	outside	Any	AnyConnect...	any	any	-- Original -- (S)	-- Original --	-- Original --
"Network Object" NAT (Rules 3-7)								
3	Any	Any	HQ-srv	any	any	192.0.2.25 (S)	-- Original --	-- Original --
	Any	Any	any	192.0.2.25	any	-- Original -- (S)	HQ-srv	-- Original --
4	inside	outside	MAIL	any	any	192.0.2.25 (S)	-- Original --	-- Original --
	outside	inside	any	192.0.2.25	any	-- Original -- (S)	MAIL	-- Original --
5	DMZ	outside	DMZ-server	any	any	DMZ-server-g...	-- Original --	-- Original --
	outside	DMZ	any	DMZ-server...	any	-- Original -- (S)	DMZ-server	-- Original --
6	DMZ	outside	NAT	any	any	192.0.2.50 (S)	-- Original --	-- Original --
	outside	DMZ	any	192.0.2.50	any	-- Original -- (S)	NAT	-- Original --
7	Any	Any	ESA	any	any	192.0.2.55 (S)	-- Original --	-- Original --
	Any	Any	any	192.0.2.55	any	-- Original -- (S)	ESA	-- Original --

At the bottom of the main pane, there are 'Apply' and 'Reset' buttons.

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree with 'Advanced' selected. The main pane shows the 'Configuration > Firewall > Advanced' page. It contains a list of items that this section contains:


- [Anti-Spoofing](#)
- [Certificate Management](#)
- [Fragment](#)
- [IP Audit](#)
- [SUNRPC Server](#)
- [TCP Options](#)
- [Global Timeouts](#)
- [Virtual Access](#)
- [ACL Manager](#)
- [Standard ACL](#)
- [Per-Session NAT Rules](#)



The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree, with 'Standard ACL' selected under the 'Advanced' section. The main pane shows the 'Configuration > Firewall > Advanced > Standard ACL' configuration window. It contains a table with two entries under the 'Inside Subnets' group:

No	Address	Action	Description
1	10.10.0.0/16	✓ Permit	
2	DMZ-network/24	✓ Permit	

At the bottom of the configuration window are 'Apply' and 'Reset' buttons.


Edit NAT Rule

Match Criteria: Original Packet

Source Interface: inside

Destination Interface: outside

Source Address: any

Destination Address: any

Service: any

Action: Translated Packet

Source NAT Type: Dynamic

Source Address: outside-nat-pool

Destination Address: -- Original --

☐ Use one-to-one address translation

☒ PAT Pool Translated Address:

Service: -- Original --

☒ Round Robin

☐ Extend PAT uniqueness to per destination instead of per interface

☐ Translate TCP and UDP ports into flat range 1024-65535

☐ Include range 1-1023

☒ Fall through to interface PAT

☐ Use IPv6 for source interface PAT

☐ Use IPv6 for destination interface PAT

Options

☒ Enable rule

☒ Translate DNS replies that match this rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface


Direction: Both

Description:

OK

Cancel

Help

 Edit NAT Rule

Match Criteria: Original Packet

Source Interface: -- Any -- Destination Interface: outside

Source Address: any Destination Address: AnyConnect_Clients

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original -- Destination Address: -- Original --

☐ Use one-to-one address translation

☐ PAT Pool Translated Address: Service: -- Original --

☐ Round Robin

☐ Extend PAT uniqueness to per destination instead of per interface

☐ Translate TCP and UDP ports into flat range 1024-65535 ☐ Include range 1-1023

☐ Fall through to interface PAT

☐ Use IPv6 for source interface PAT ☐ Use IPv6 for destination interface PAT

Options

☒ Enable rule

☐ Translate DNS replies that match this rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface

Direction: Both

Description:

OK

Cancel

Help

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access > Group Policies' page. It includes a description of VPN group policies and a table listing existing policies.

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Buttons: Add, Edit, Delete, Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
GroupPolicy1	Internal	ikev1	203.0.113.1
GroupPolicy2	Internal	ssl-client	AnyConnect_Profile
DfltGrpPolicy (System Defa...	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultWEB...

Find: [] Match Case

Buttons: Apply, Reset

The screenshot shows the 'Edit Internal Group Policy: GroupPolicy2' dialog box. The left sidebar shows the configuration tree with 'Advanced' selected. The main pane shows the configuration fields for the policy.

Name: GroupPolicy2

Banner: ☒ Inherit

SCEP forwarding URL: ☒ Inherit

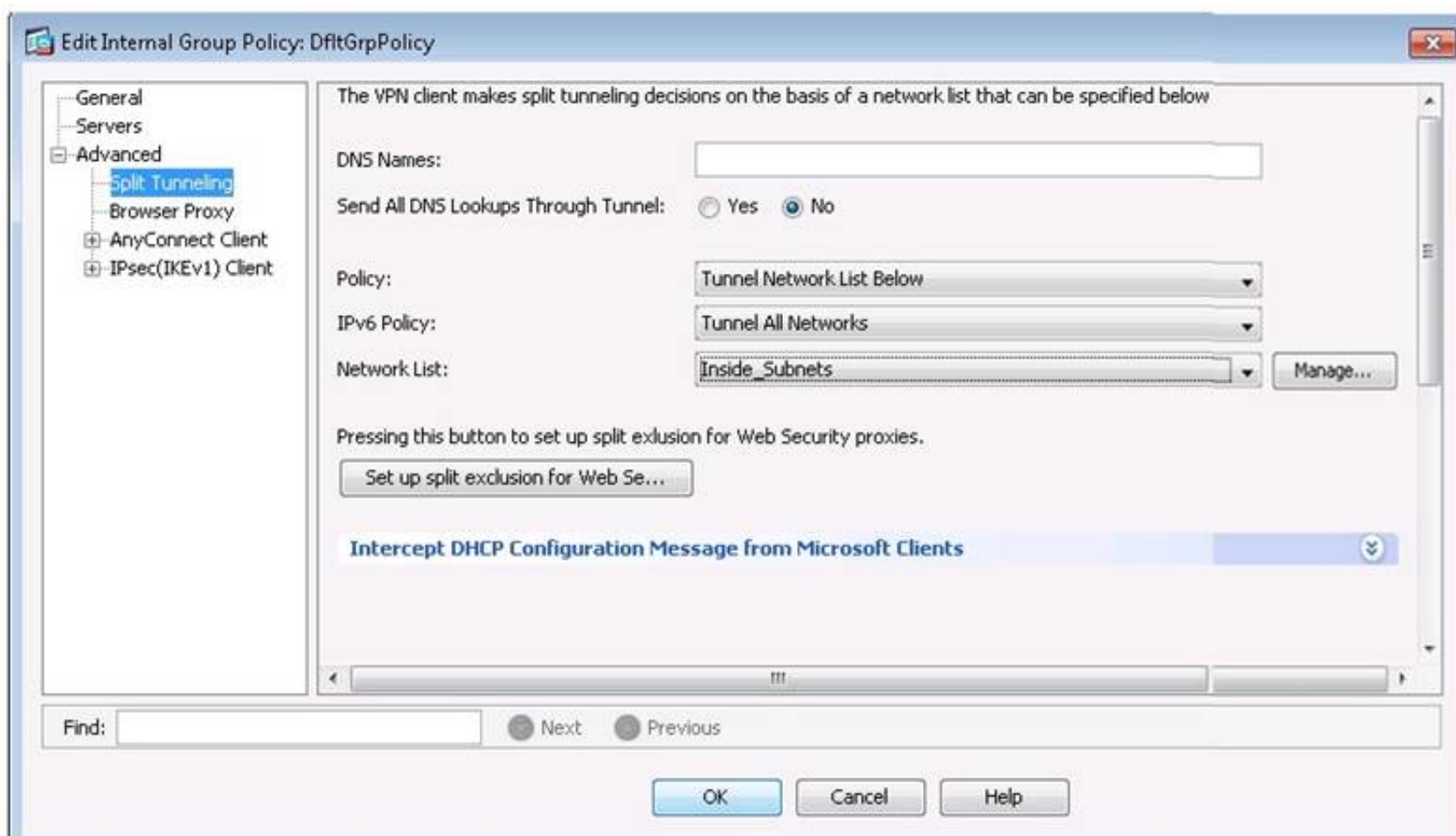
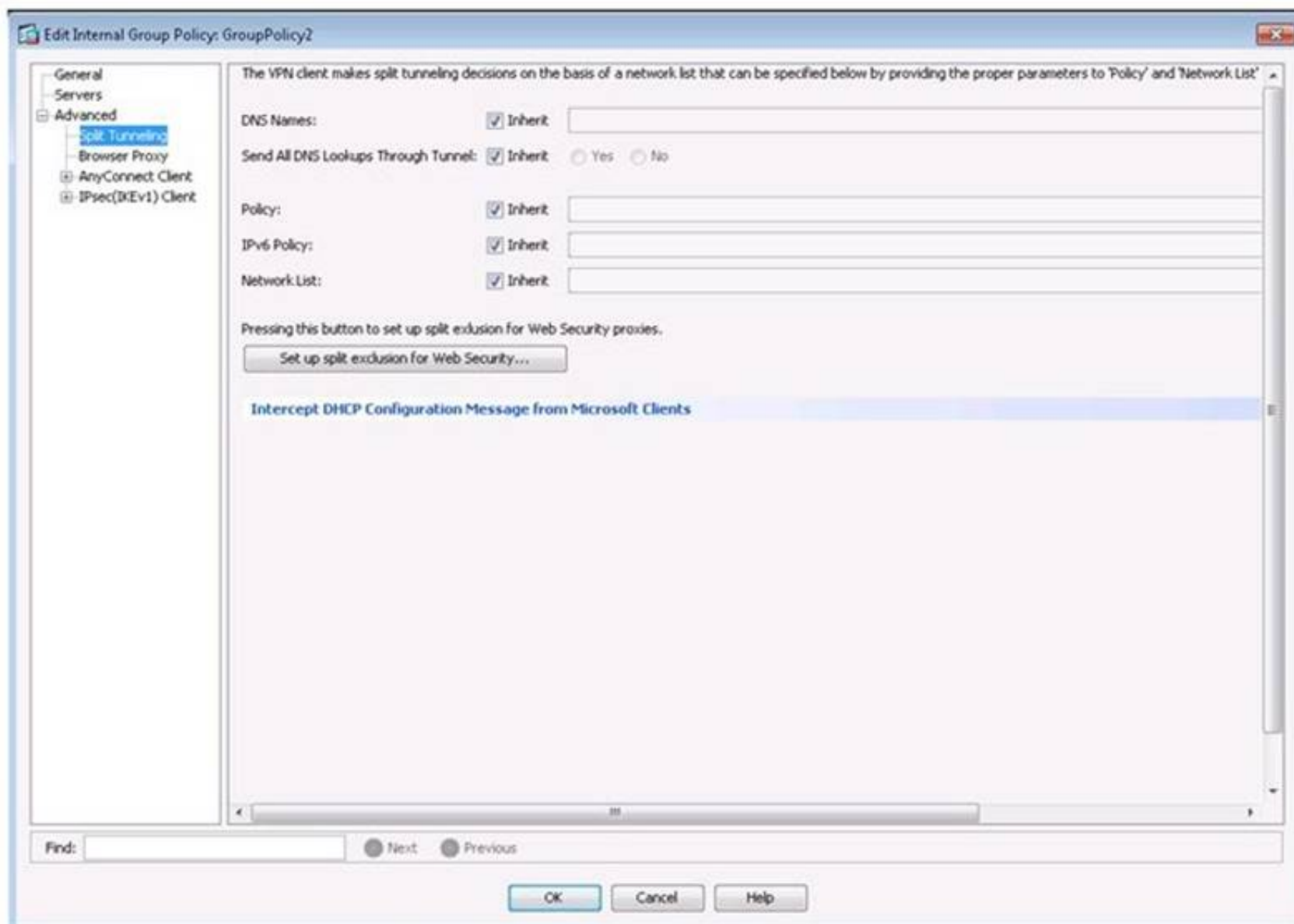
Address Pools: ☒ Inherit

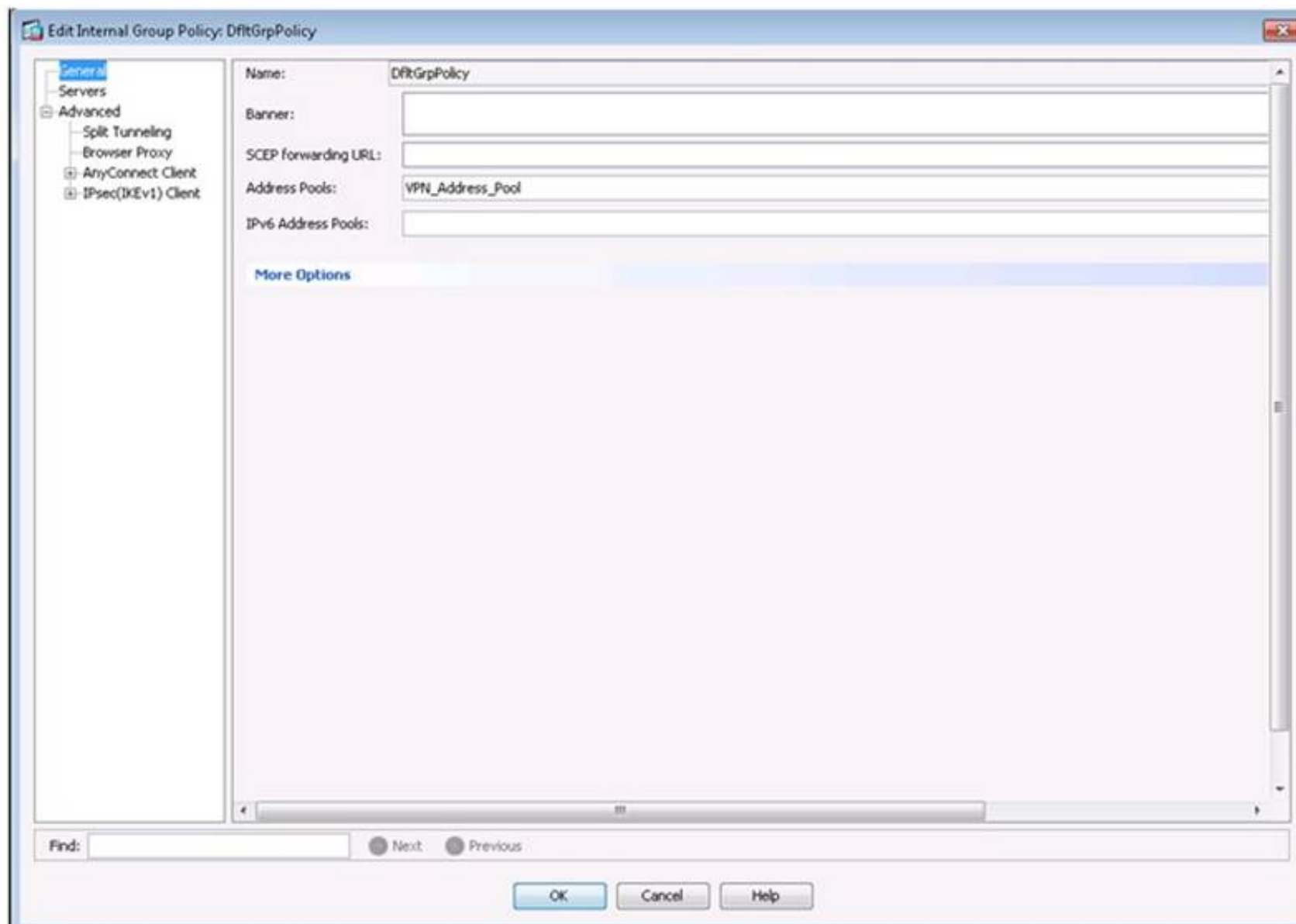
IPv6 Address Pools: ☒ Inherit

More Options

Find: [] Next Previous

Buttons: OK, Cancel, Help



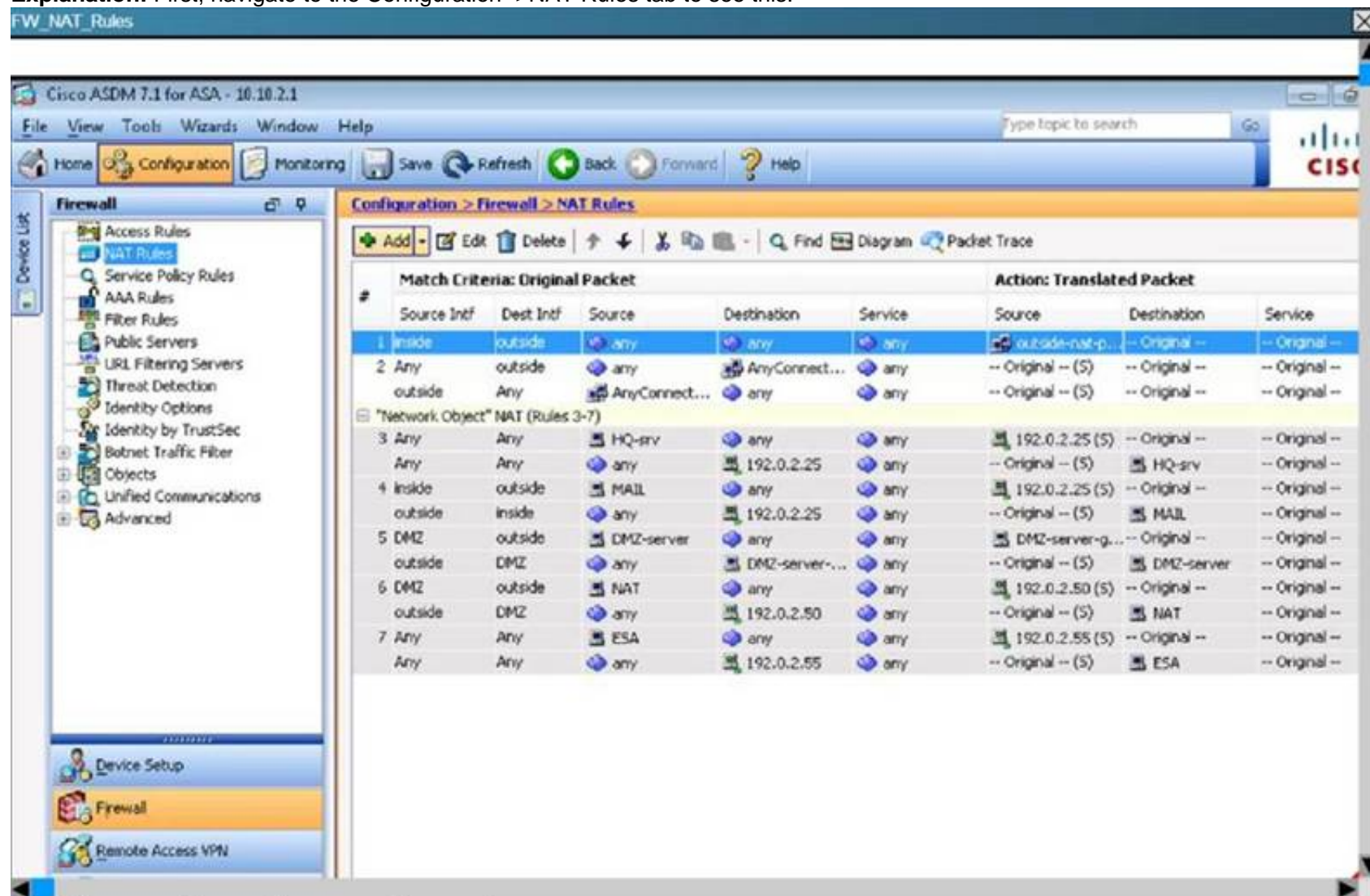


What two actions will be taken on translated packets when the AnyConnect users connect to the ASA? (Choose two.)

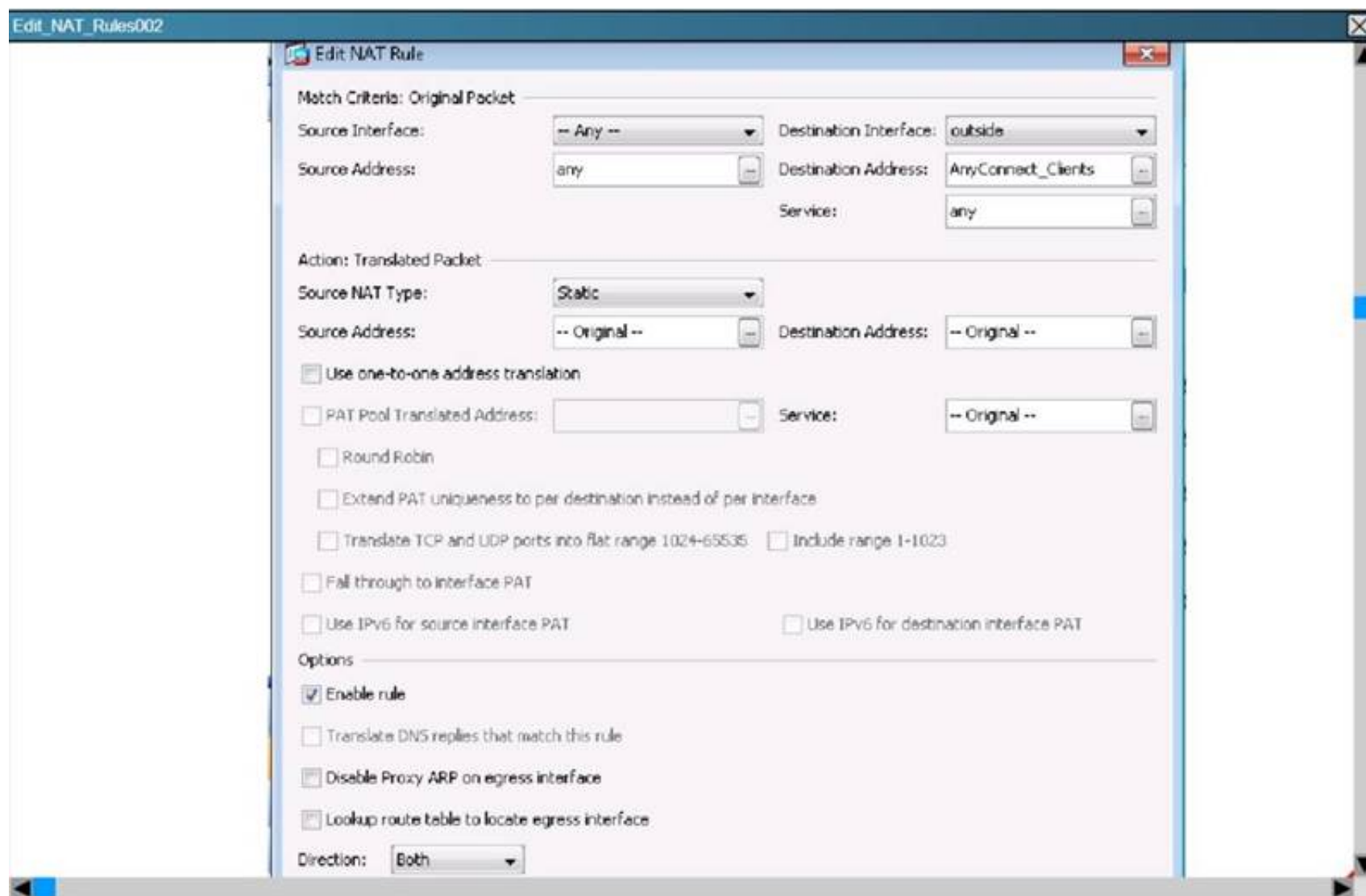
- A. No action will be taken, they will keep their original assigned addresses
- B. The source address will use the outside-nat-pool
- C. The source NAT type will be a static translation
- D. The source NAT type will be a dynamic translation
- E. DNS will be translated on rule matches

Answer: AC

Explanation: First, navigate to the Configuration -> NAT Rules tab to see this:



Here we see that NAT rule 2 applies to the AnyConnect clients, click on this rule for more details to see the following:



Here we see that it is a static source NAT entry, but that the Source and Destination addresses remain the original IP address so they are not translated.

NEW QUESTION 271

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

NEW QUESTION 276

Which technology is FlexVPN based on?

- A. OER
- B. VRF
- C. IKEv2
- D. an RSA nonce

Answer: C

NEW QUESTION 280

Refer to the exhibit.


```
Apr  2 12:03:55.391: ISAKMP (14): beginning Main Mode exchange
Apr  2 12:03:57.199: ISAKMP (14): processing SA payload. message ID = 0
Apr  2 12:03:57.203: ISAKMP (14): Checking ISAKMP transform 1 against priority 1 policy
Apr  2 12:03:57.203: ISAKMP:      encryption DES-CBC
Apr  2 12:03:57.207: ISAKMP:      hash MD5
Apr  2 12:03:57.207: ISAKMP:      default group 1
Apr  2 12:03:57.207: ISAKMP:      auth pre-share
Apr  2 12:03:57.211: ISAKMP (14): atts are acceptable. Next payload is 0
Apr  2 12:03:57.215: Crypto engine 0: generate alg param
```

Which exchange does this debug output represent?

- A. IKE Phase 1
- B. IKE Phase 2
- C. symmetric key exchange
- D. certificate exchange

Answer: A

NEW QUESTION 283

Which protocols does the Cisco AnyConnect client use to build multiple connections to the security appliance?

- A. TLS and DTLS
- B. IKEv1
- C. L2TP over IPsec
- D. SSH over TCP

Answer: A

NEW QUESTION 285

You are troubleshooting a DMVPN NHRP registration failure. Which command can you use to view request counters?

- A. show ip nhrp nhs detail
- B. show ip nhrp tunnel
- C. show ip nhrp incomplete
- D. show ip nhrp incomplete tunnel tunnel_interface_number

Answer: A

NEW QUESTION 286

Which benefit of FlexVPN is not offered by DMVPN using IKEv1?

- A. Dynamic routing protocols can be configured.
- B. IKE implementation can install routes in routing table.
- C. GRE encapsulation allows for forwarding of non-IP traffic.
- D. NHRP authentication provides enhanced security.

Answer: B

NEW QUESTION 290

Scenario:

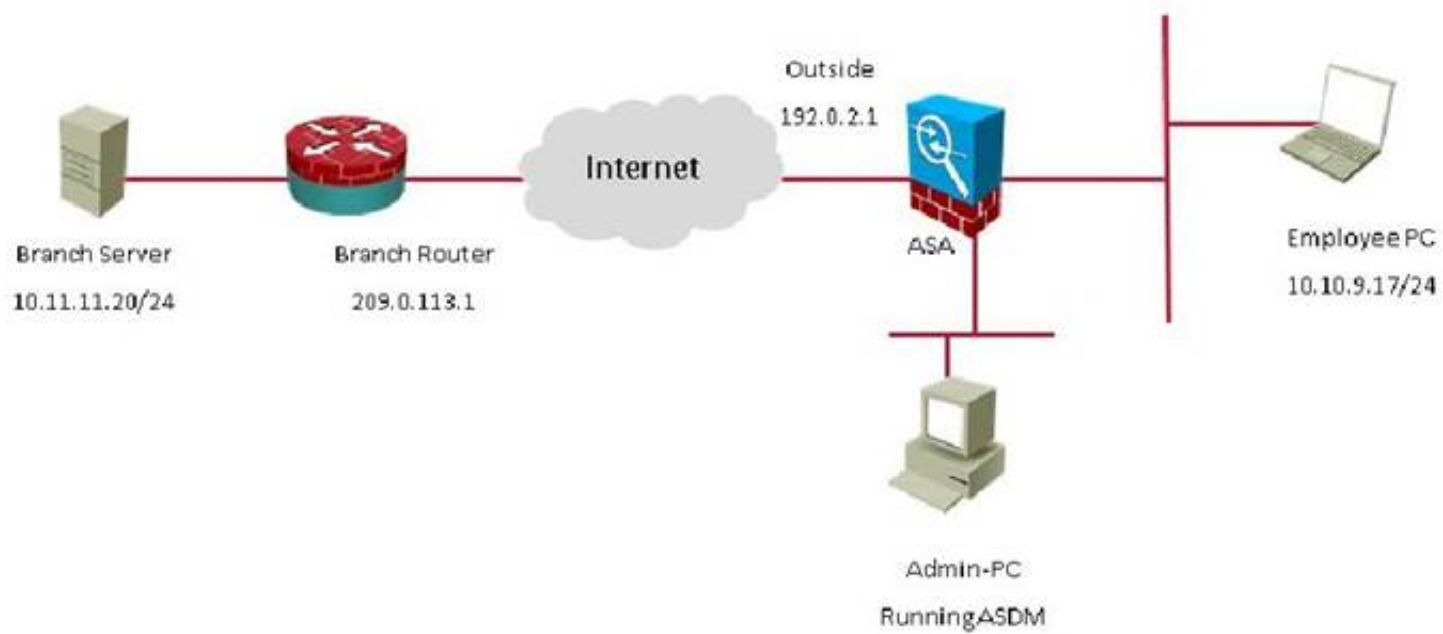
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

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.

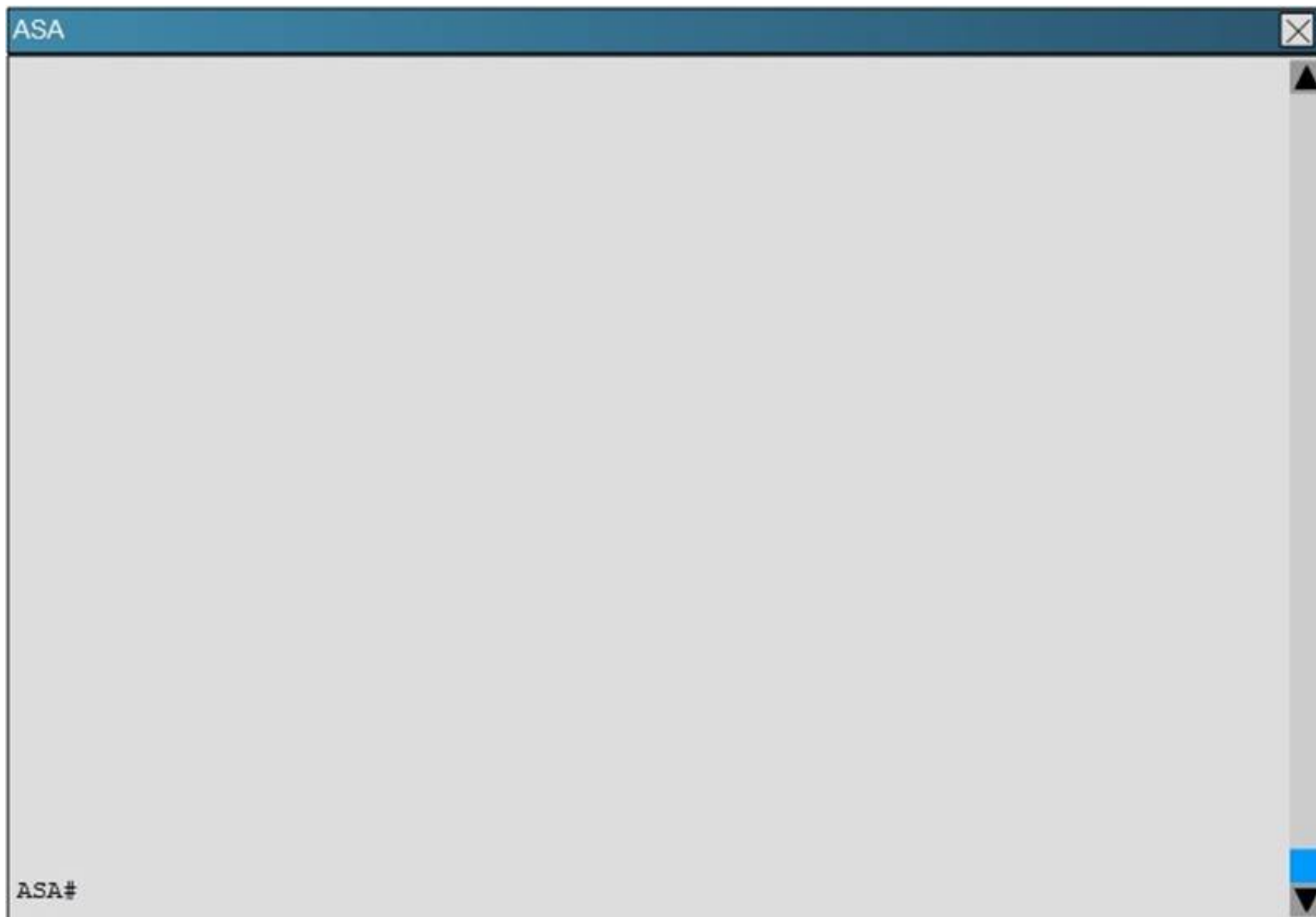
Topology:

Topology



Branch ISR

Branch ISR#



What is being used as the authentication method on the branch ISR?

- A. Certificates
- B. Pre-shared keys
- C. RSA public keys
- D. Diffie-Hellman Group 2

Answer: B

Explanation: The show crypto isakmp key command shows the preshared key of “cisco”.

```
Branch ISR#show crypto isakmp key
Keyring      Hostname/Address      Preshared Key
default      192.0.2.1      cisco
Branch ISR#
Branch ISR#
Branch ISR#
```

NEW QUESTION 291

Which transform set is contained in the IKEv2 default proposal?

- A. aes-cbc-192, sha256, group 14
- B. 3des, md5, group 7
- C. 3des, sha1, group 1
- D. aes-cbc-128, sha, group 5

Answer: D

NEW QUESTION 294

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 298

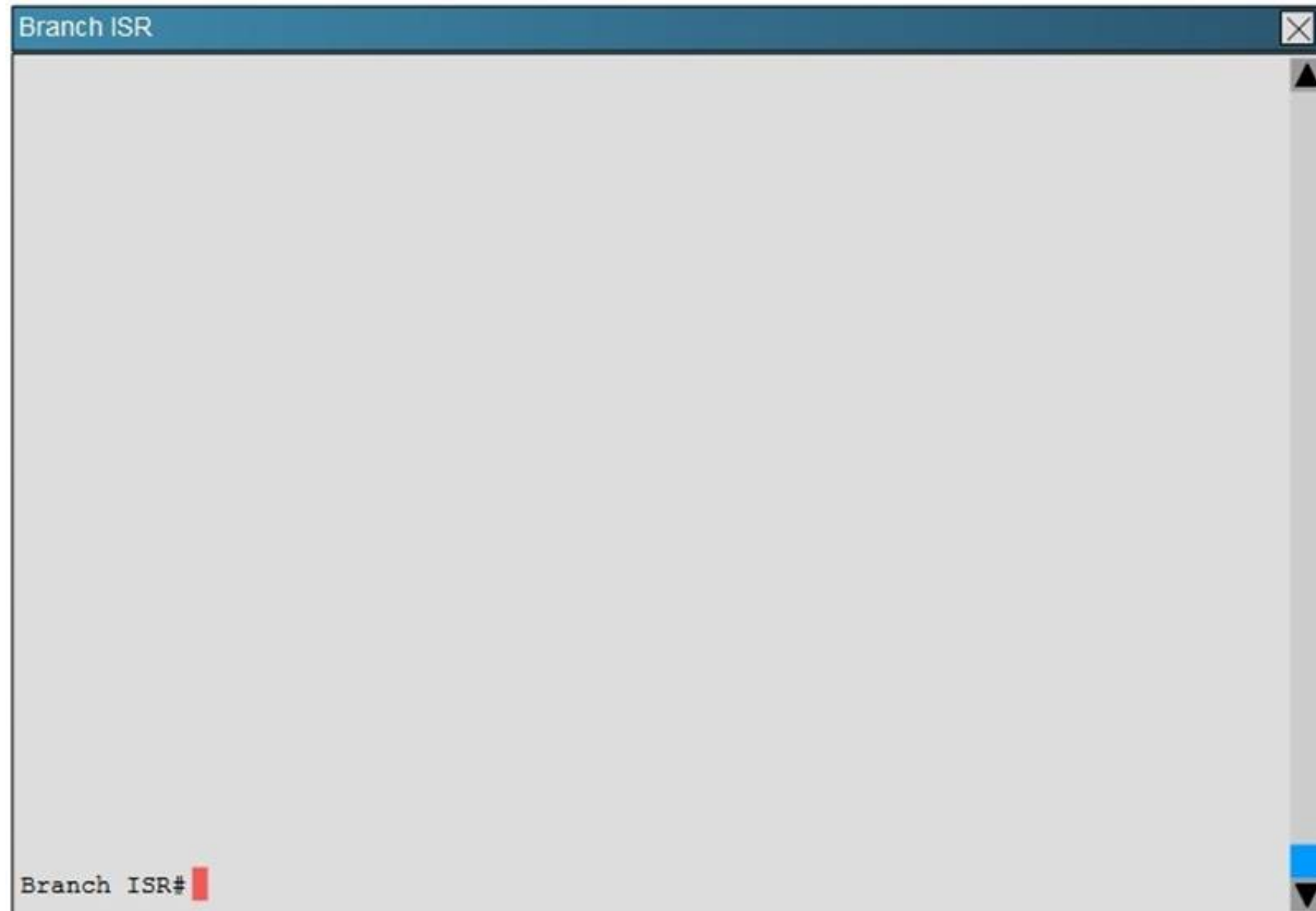
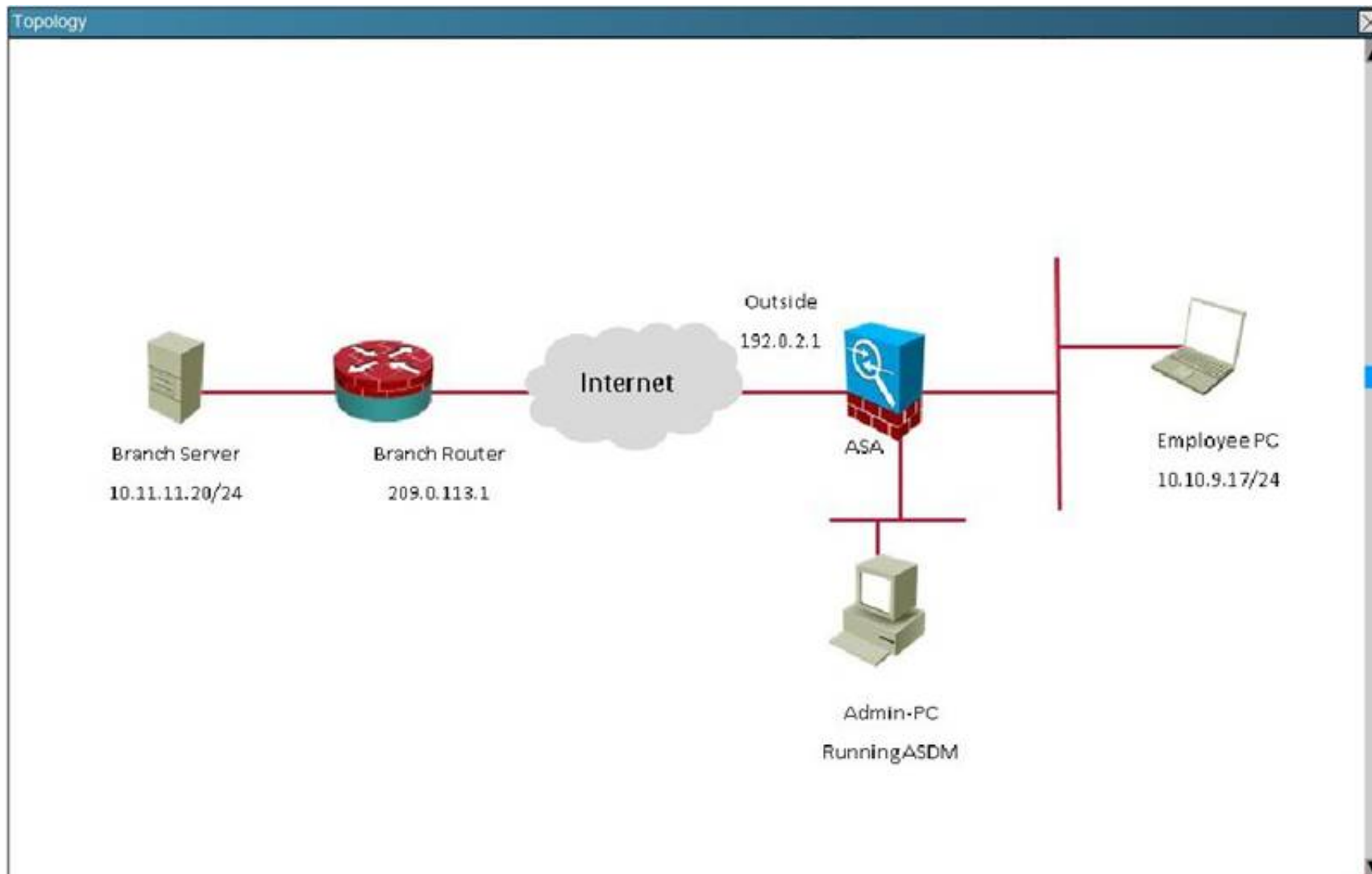
Scenario:

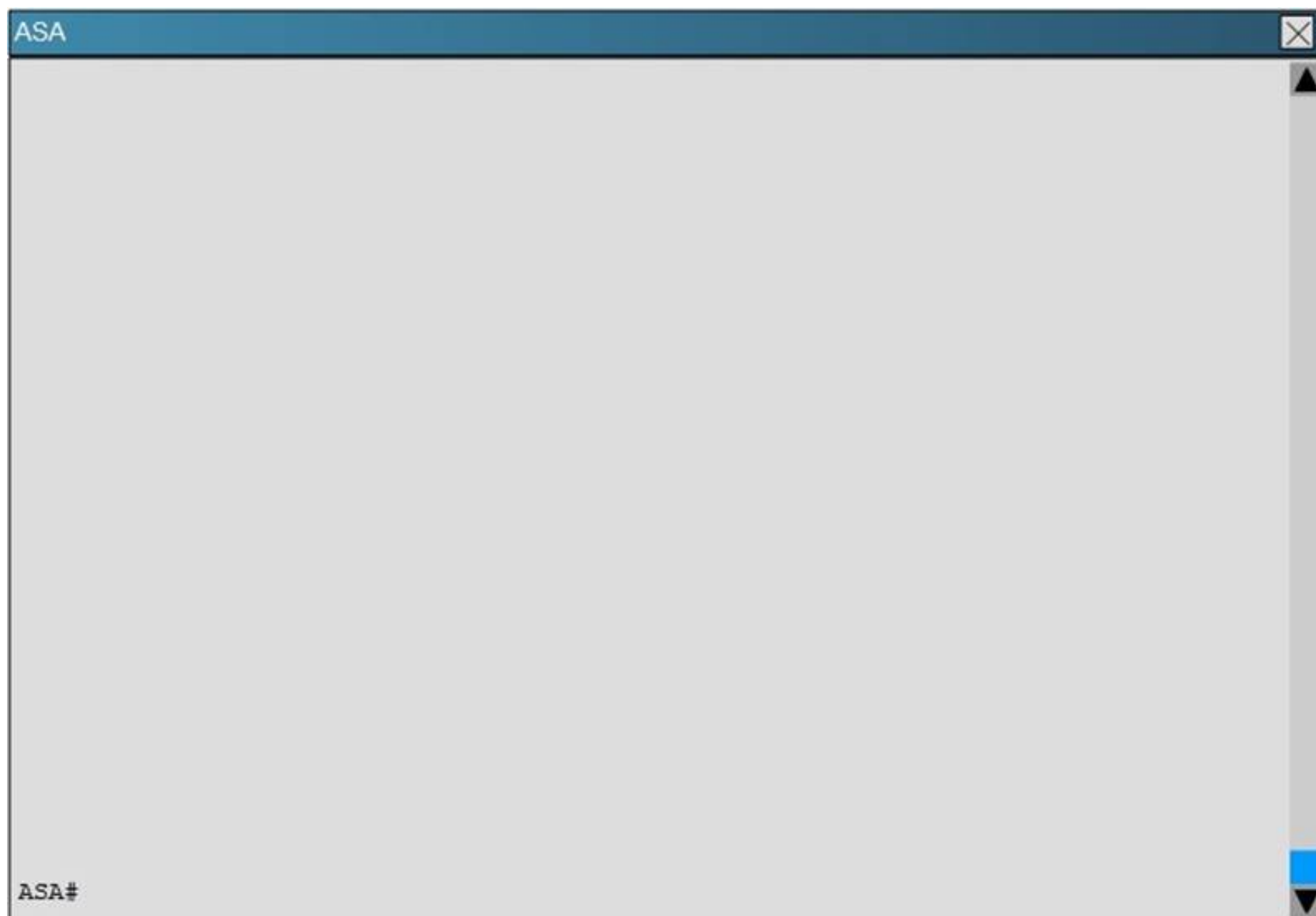
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

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:



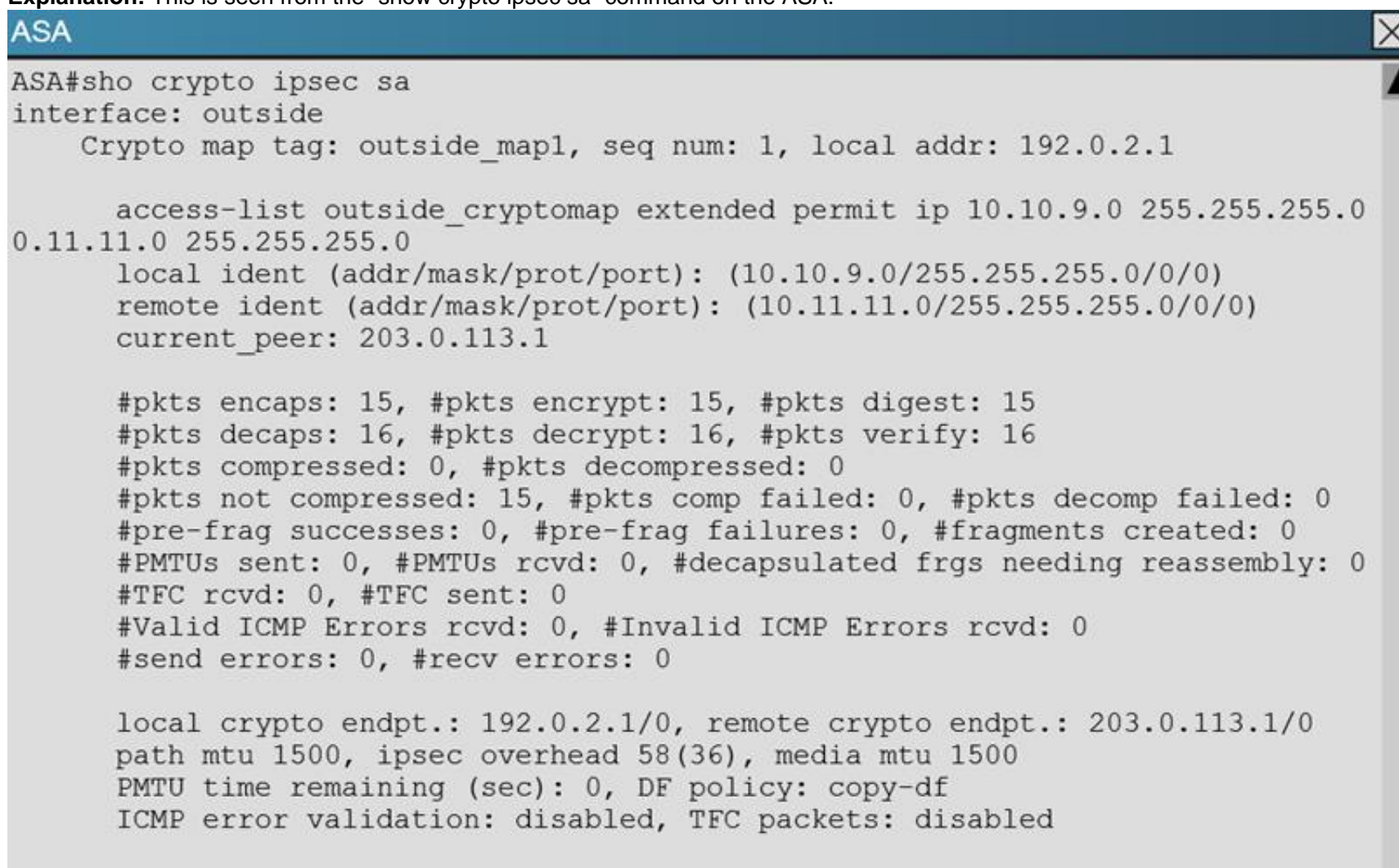


Which crypto map tag is being used on the Cisco ASA?

- A. outside_cryptomap
- B. VPN-to-ASA
- C. L2L_Tunnel
- D. outside_map1

Answer: D

Explanation: This is seen from the “show crypto ipsec sa” command on the ASA.



NEW QUESTION 303

In the Diffie-Hellman protocol, which type of key is the shared secret?

- A. a symmetric key
- B. an asymmetric key

- C. a decryption key
- D. an encryption key

Answer: A

NEW QUESTION 306

Scenario

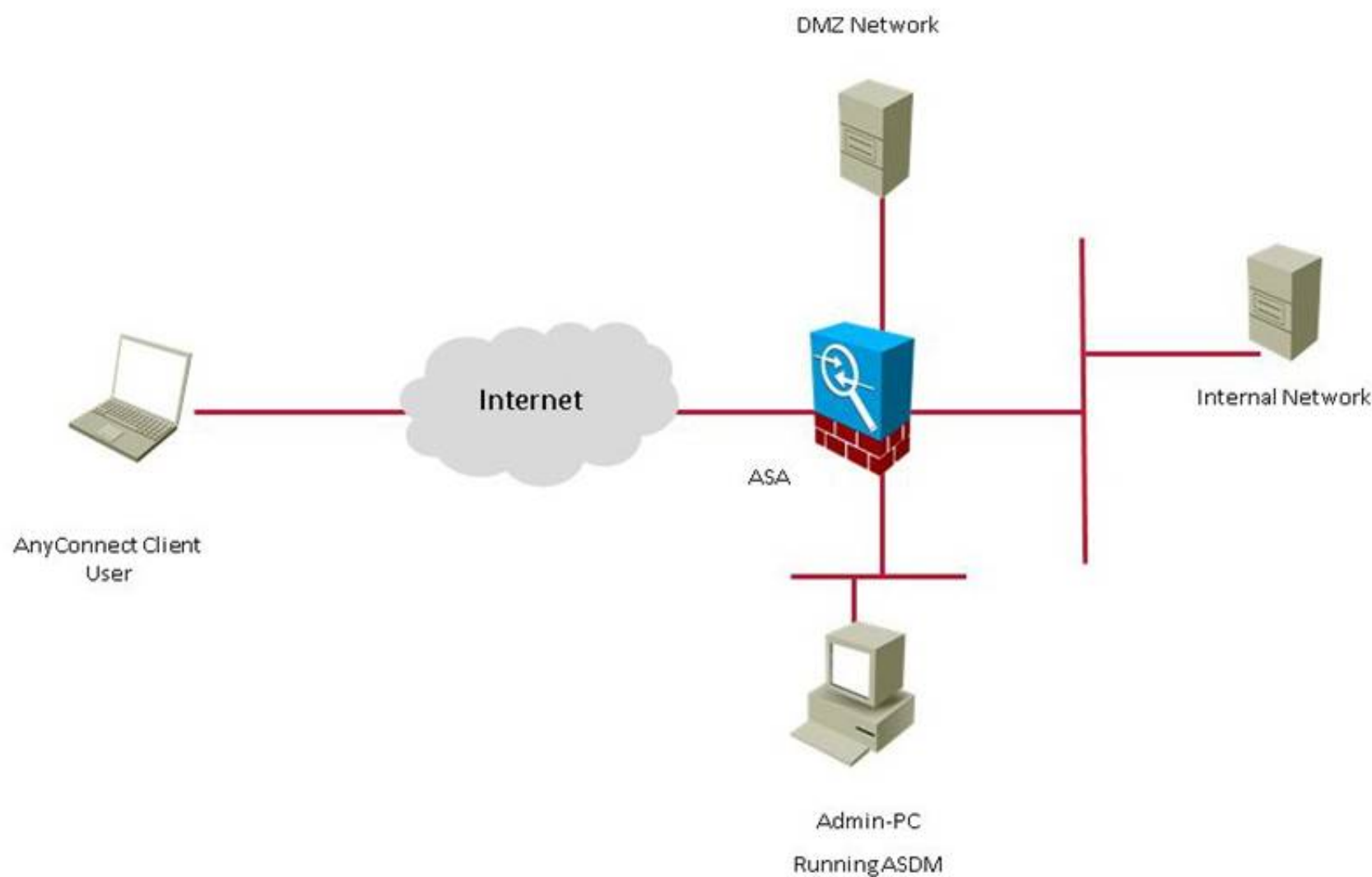
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

Note: Not all screens or option selections are active for this exercise.

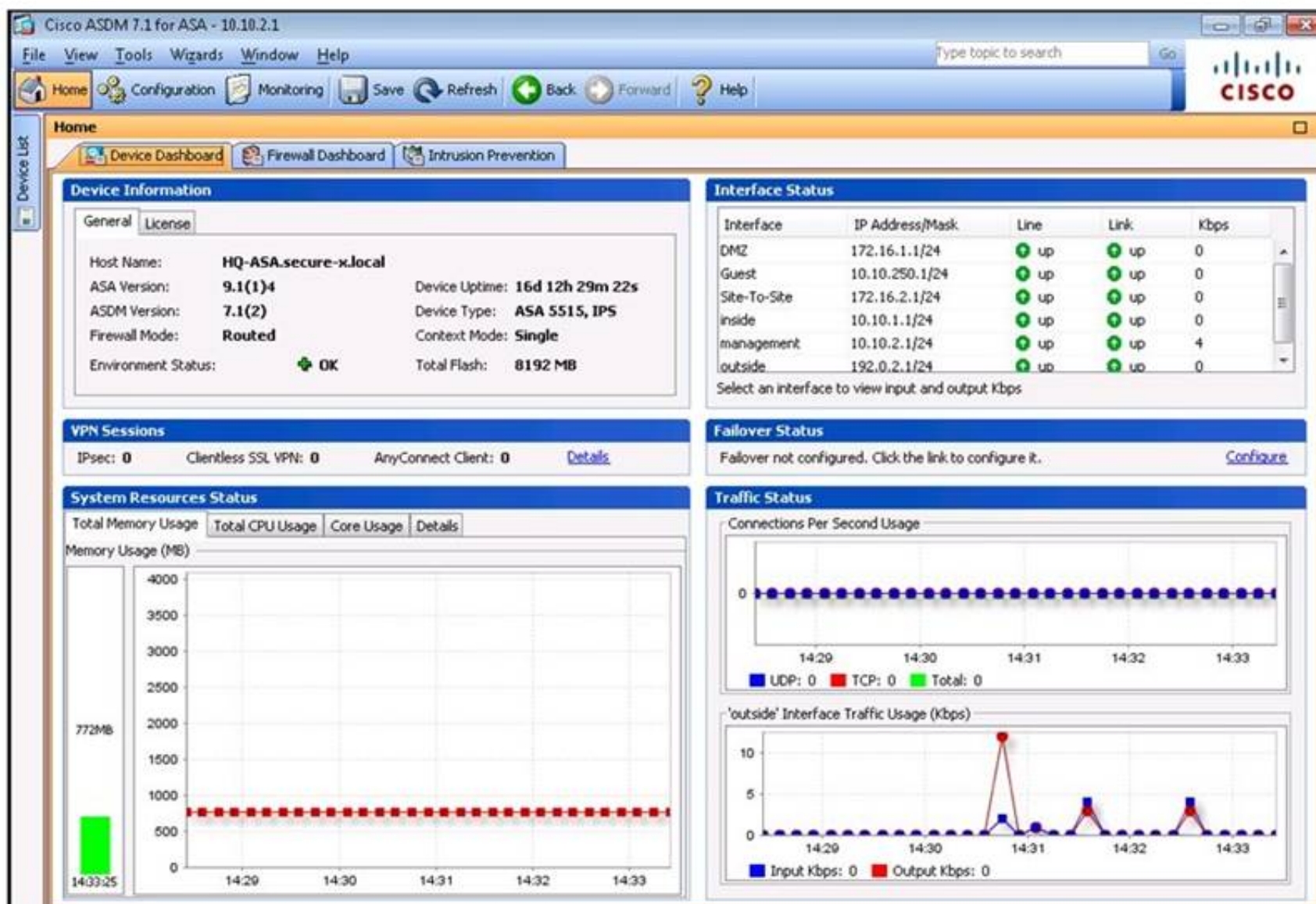
Instructions

- Navigate the ASDM GUI on the device to verify network operation and answer for multiple-choice questions.
- You may have to use the scroll bars to view the entire ASDM Configuration screens.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- NOT ALL SCREENS AND SELECTIONS ARE AVAILABLE FOR THIS EXERCISE.**
- Click on the Admin PC on the topology page to gain ASDM to the ASA. No passwords are required for this exercise.
- You may also click on the Default Home tab to access ASDM or return to the ASDM home screen at any time.
- There are **four (4)** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.
- To access the multiple-choice questions, click on the Questions tab and then numbered boxes on the left of the panel to view each question.

Topology



Default_Home



Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup

Startup Wizard

Interfaces

Routing

Device Name/Password

System Time

EtherChannel

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

IPS

Device Management

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Group
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native	
GigabitEthernet0/1		Enabled				native	
GigabitEthernet0/1.4	inside	Enabled	100	10.10.1.1	255.255.255.0	vlan4	
GigabitEthernet0/1.250	Guest	Enabled	30	10.10.250.1	255.255.255.0	vlan250	
GigabitEthernet0/2	DMZ	Enabled	50	172.16.1.1	255.255.255.0	native	
GigabitEthernet0/3	Site-To...	Enabled	60	172.16.2.1	255.255.255.0	native	
GigabitEthernet0/4		Enabled				native	
GigabitEthernet0/5		Enabled				native	
Management0/0	manage...	Enabled	90	10.10.2.1	255.255.255.0	native	

Enable traffic between two or more interfaces which are configured with same security levels

Enable traffic between two or more hosts connected to the same interface

Enable jumbo frame reservation

Apply Reset

Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(IKEv2) protocols, Cisco VPN Client supports only IPsec(IKEv1) protocol.

2. User and connection profile

To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

You configure user account database in [AAA/Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(IKEv1\) Connection Profiles](#).

3. Access policy

Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control - how long a session can remain idle before it is closed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [NAC](#) based ending security policies.

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below.

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☒ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☐ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☒ Shutdown portal login page. Shutdown notice: Service out temporarily.




Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

☒ Add
 ☒ Edit
 ☐ Delete
 Find:

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVP...	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
AnyConnect_P...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyConnect_VPN_User	AAA(LOCAL)	GroupPolicy2

Select Address Pools

 Add
  Edit
  Delete


Pool Name	Starting Address	Ending Address/Number of Addresses	Subnet Mask/Prefix Length
AC_Addre...	10.10.15.40	10.10.15.50	255.255.255.0
Outside_A...	209.165.201.20	209.165.201.30	255.255.255.0
Remote_A...	192.168.1.100	192.168.1.150	255.255.255.0
VPN_Addr...	10.10.15.20	10.10.15.30	255.255.255.0

Assigned Address Pools

Assign-> VPN_Address_Pool

OK Cancel Help

Edit AnyConnect Connection Profile: AnyConnect_Profile

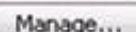
Basic
  Advanced

Name: AnyConnect_Profile

Aliases: AnyConnect_VPN_User


Authentication

Method: ☒ AAA ☐ Certificate ☐ Both

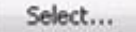
AAA Server Group: LOCAL 


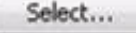
☐ Use LOCAL if Server Group fails

Client Address Assignment

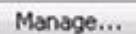
DHCP Servers: 

☒ None ☐ DHCP Link ☐ DHCP Subnet

Client Address Pools: VPN_Address_Pool 

Client IPv6 Address Pools:  

Default Group Policy


Group Policy: GroupPolicy2 

(Following field is an attribute of the group policy selected above.)



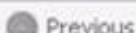
☒ Enable SSL VPN client protocol

☐ Enable IPsec(IKEv2) client protocol

DNS Servers: 10.10.3.20

WINS Servers: 

Domain Name: secure-x.local

Find:   

OK Cancel Help

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree, with 'Access Rules' selected. The main pane shows the 'Configuration > Firewall > Access Rules' page. The table below lists the configured access rules.

Enabled	Source Criteria:	Destination Criteria:	Service			
	Source	User	Security Group	Destination	Security Group	
DMZ (3 incoming rules)						
<input checked="" type="checkbox"/>	DMZ-server			any4		icmp
<input checked="" type="checkbox"/>	DMZ-server			HQ-srv		ftp
<input checked="" type="checkbox"/>	DMZ-server			any		domain
DMZ (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ-to-Site (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ (1 implicit incoming rule)						
	any			Any less secure ne...		ip
DMZ (6 incoming rules)						
<input checked="" type="checkbox"/>	any4			DMZ-server		http
<input checked="" type="checkbox"/>	any4			DMZ-server		https
<input checked="" type="checkbox"/>	any4			DMZ-server		ftp
<input checked="" type="checkbox"/>	any4			DMZ-server		icmp
<input checked="" type="checkbox"/>	any4			DMZ-server		snmp
<input checked="" type="checkbox"/>	any4			DMZ-server		domain
DMZ (1 implicit rule)						
	any			any		ip

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Remote Access VPN' configuration tree, with 'ACL Manager' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access > Advanced > ACL Manager' page. The table below lists the configured ACLs.

#	Enabled	Source	User	Security Group	Destination	Security
DMZ_access_in						
1	<input checked="" type="checkbox"/>	DMZ-server			any4	
2	<input checked="" type="checkbox"/>	DMZ-server			HQ-srv	
3	<input checked="" type="checkbox"/>	DMZ-server			any	
outside_access_in						
1	<input checked="" type="checkbox"/>	any4			DMZ-server	
2	<input checked="" type="checkbox"/>	any4			DMZ-server	
3	<input checked="" type="checkbox"/>	any4			DMZ-server	
4	<input checked="" type="checkbox"/>	any4			DMZ-server	
5	<input checked="" type="checkbox"/>	any4			DMZ-server	
6	<input checked="" type="checkbox"/>	any4			DMZ-server	
outside_cryptomap						
1	<input checked="" type="checkbox"/>	10.10.9.0/24			10.11.11.0/24	
permit-all						
1	<input checked="" type="checkbox"/>	any			any	

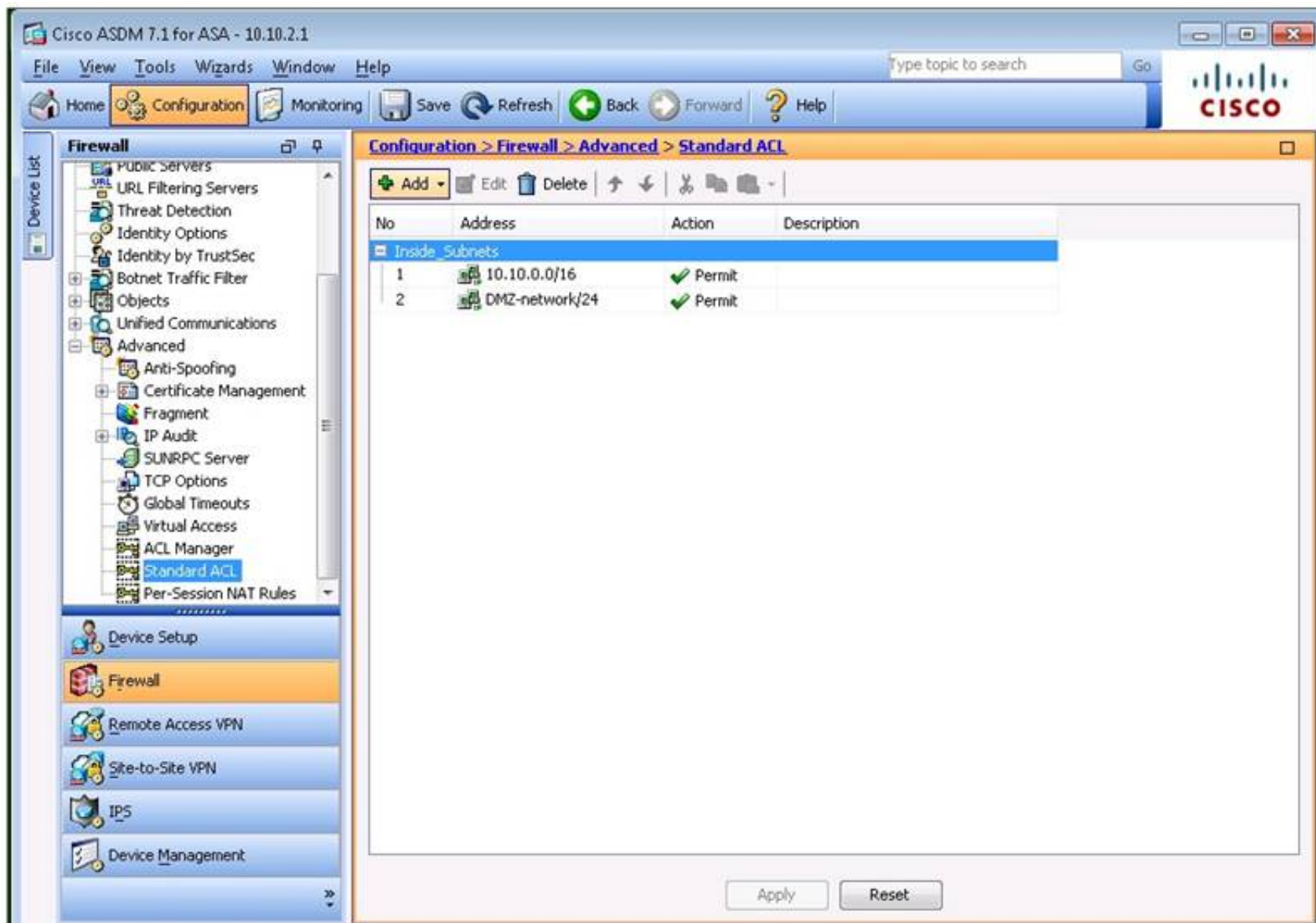
The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree with 'NAT Rules' selected. The main pane shows the 'Configuration > Firewall > NAT Rules' page. It features a table with 'Match Criteria: Original Packet' and 'Action: Translated Packet' columns. The table lists several NAT rules, including 'Network Object' NAT (Rules 3-7) and 'Any' NAT rules. The 'Match Criteria' columns include Source Intf, Dest Intf, Source, Destination, and Service. The 'Action' columns include Source, Destination, and Service. The table is scrollable, and the bottom of the pane has 'Apply' and 'Reset' buttons.

Match Criteria: Original Packet					Action: Translated Packet			
#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
1	inside	outside	any	any	any	outside-nat-p...	-- Original --	-- Original --
2	Any	outside	any	AnyConnect...	any	-- Original -- (S)	-- Original --	-- Original --
	outside	Any	AnyConnect...	any	any	-- Original -- (S)	-- Original --	-- Original --
"Network Object" NAT (Rules 3-7)								
3	Any	Any	HQ-srv	any	any	192.0.2.25 (S)	-- Original --	-- Original --
	Any	Any	any	192.0.2.25	any	-- Original -- (S)	HQ-srv	-- Original --
4	inside	outside	MAIL	any	any	192.0.2.25 (S)	-- Original --	-- Original --
	outside	inside	any	192.0.2.25	any	-- Original -- (S)	MAIL	-- Original --
5	DMZ	outside	DMZ-server	any	any	DMZ-server-g...	-- Original --	-- Original --
	outside	DMZ	any	DMZ-server...	any	-- Original -- (S)	DMZ-server	-- Original --
6	DMZ	outside	NAT	any	any	192.0.2.50 (S)	-- Original --	-- Original --
	outside	DMZ	any	192.0.2.50	any	-- Original -- (S)	NAT	-- Original --
7	Any	Any	ESA	any	any	192.0.2.55 (S)	-- Original --	-- Original --
	Any	Any	any	192.0.2.55	any	-- Original -- (S)	ESA	-- Original --

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Firewall' configuration tree with 'Advanced' selected. The main pane shows the 'Configuration > Firewall > Advanced' page. It contains a list of items that this section contains, including Anti-Spoofing, Certificate Management, Fragment, IP Audit, SUNRPC Server, TCP Options, Global Timeouts, Virtual Access, ACL Manager, Standard ACL, and Per-Session NAT Rules.

This section contains the following items:


- [Anti-Spoofing](#)
- [Certificate Management](#)
- [Fragment](#)
- [IP Audit](#)
- [SUNRPC Server](#)
- [TCP Options](#)
- [Global Timeouts](#)
- [Virtual Access](#)
- [ACL Manager](#)
- [Standard ACL](#)
- [Per-Session NAT Rules](#)



The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar contains a 'Device List' and a 'Firewall' section with various sub-items. The main pane displays the 'Configuration > Firewall > Advanced > Standard ACL' configuration page. A table lists two ACL entries under the 'Inside Subnets' section.

No	Address	Action	Description
1	10.10.0.0/16	✓ Permit	
2	DMZ-network/24	✓ Permit	

At the bottom of the main pane, there are 'Apply' and 'Reset' buttons.


Edit NAT Rule

Match Criteria: Original Packet

Source Interface: inside

Destination Interface: outside

Source Address: any

Destination Address: any

Service: any

Action: Translated Packet

Source NAT Type: Dynamic

Source Address: outside-nat-pool

Destination Address: -- Original --

☐ Use one-to-one address translation

☐ PAT Pool Translated Address:

Service: -- Original --

☐ Round Robin

☐ Extend PAT uniqueness to per destination instead of per interface

☐ Translate TCP and UDP ports into flat range 1024-65535

☐ Include range 1-1023

☐ Fall through to interface PAT

☐ Use IPv6 for source interface PAT

☐ Use IPv6 for destination interface PAT

Options

☒ Enable rule

☒ Translate DNS replies that match this rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface


Direction: Both

Description:

OK

Cancel

Help


Edit NAT Rule

Match Criteria: Original Packet

Source Interface: -- Any --

Destination Interface: outside

Source Address: any

Destination Address: AnyConnect_Clients

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original --

Destination Address: -- Original --

☐ Use one-to-one address translation

☐ PAT Pool Translated Address:

Service: -- Original --

☐ Round Robin
☐ Extend PAT uniqueness to per destination instead of per interface
☐ Translate TCP and UDP ports into flat range 1024-65535
☐ Include range 1-1023

☐ Fall through to interface PAT
☐ Use IPv6 for source interface PAT
☐ Use IPv6 for destination interface PAT

Options

☒ Enable rule
☐ Translate DNS replies that match this rule
☐ Disable Proxy ARP on egress interface
☐ Lookup route table to locate egress interface

Direction: Both

Description:

OK

Cancel

Help

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access > Group Policies' page. It includes a description of VPN group policies and a table listing existing policies.

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Buttons: Add, Edit, Delete, Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
GroupPolicy1	Internal	ikev1	203.0.113.1
GroupPolicy2	Internal	ssl-client	AnyConnect_Profile
DfltGrpPolicy (System Defa...	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultWEB...

Find: [] Match Case

Buttons: Apply, Reset

The screenshot shows the 'Edit Internal Group Policy: GroupPolicy2' dialog box. The left sidebar shows the configuration tree with 'Advanced' selected. The main pane shows the configuration fields for GroupPolicy2.

Name: GroupPolicy2

Banner: ☒ Inherit

SCEP forwarding URL: ☒ Inherit

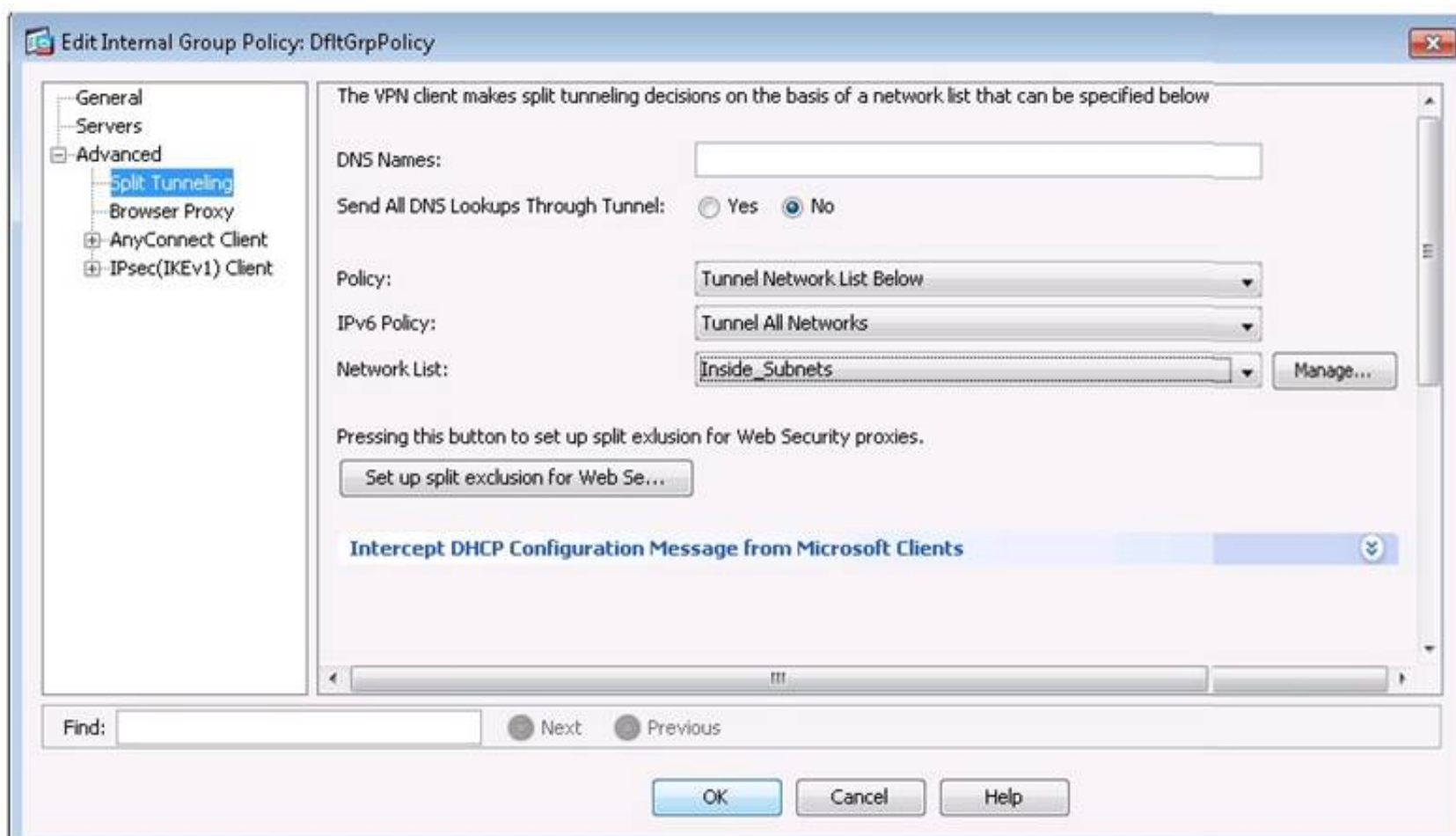
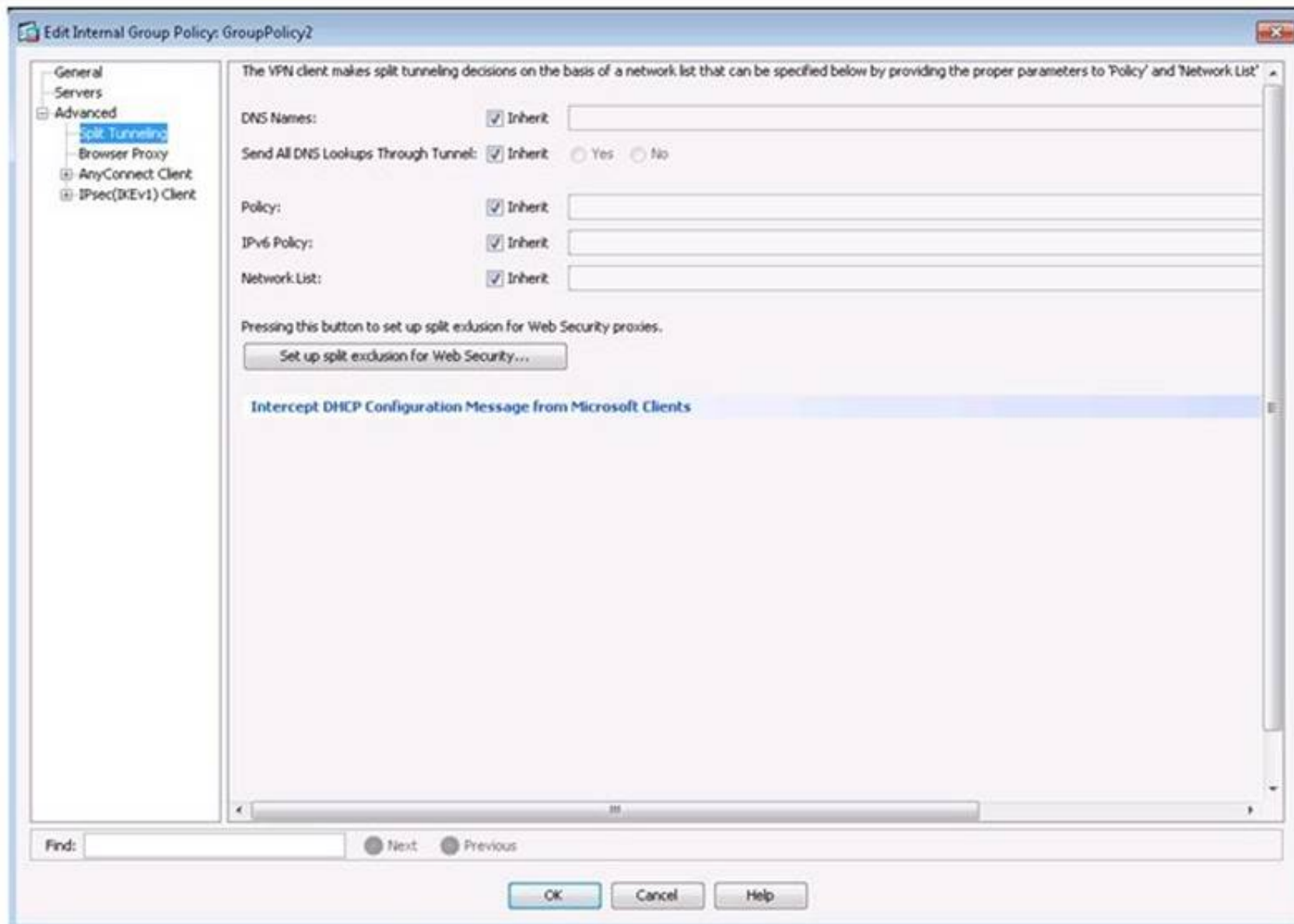
Address Pools: ☒ Inherit

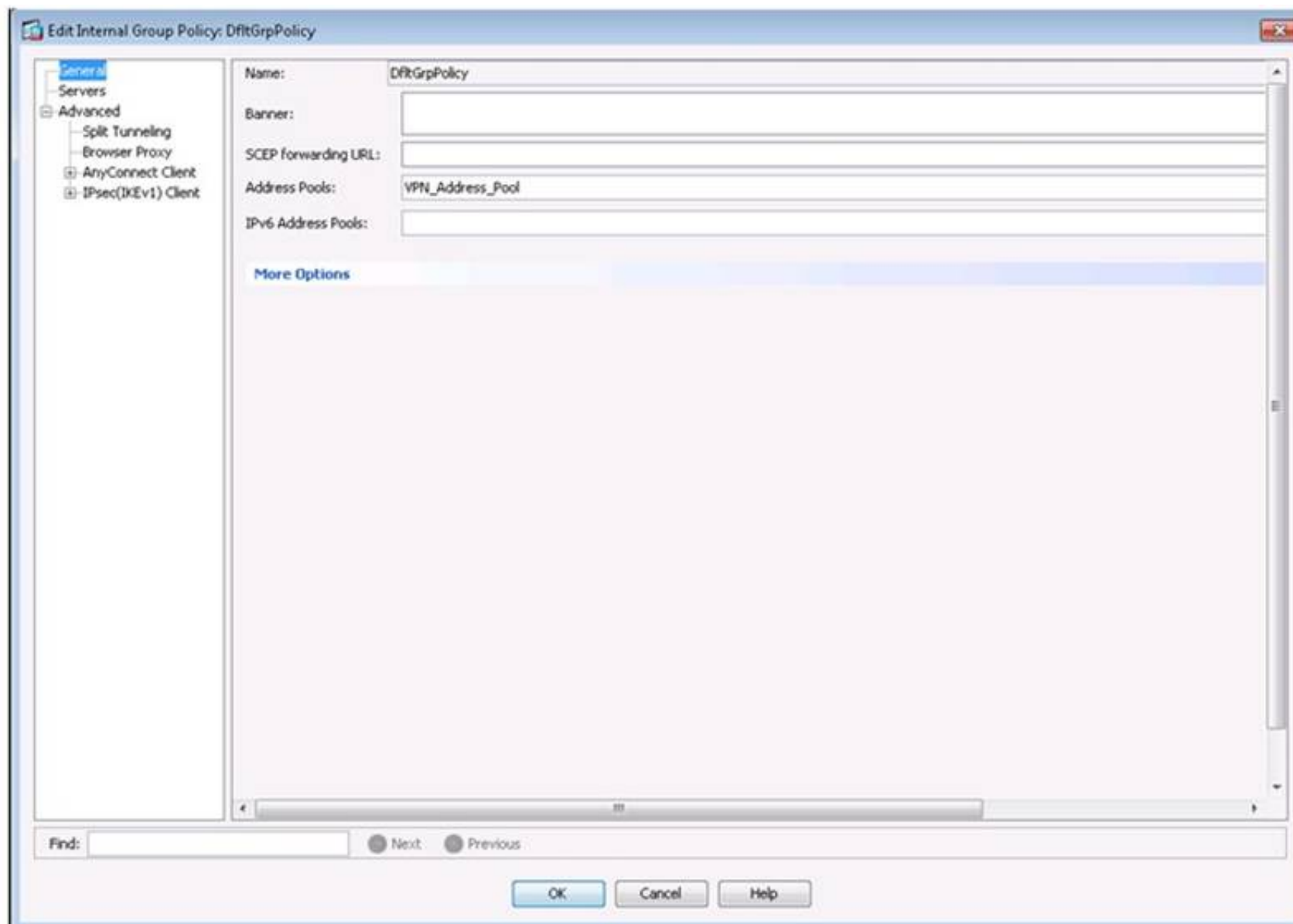
IPv6 Address Pools: ☒ Inherit

More Options

Find: [] Next Previous

Buttons: OK, Cancel, Help



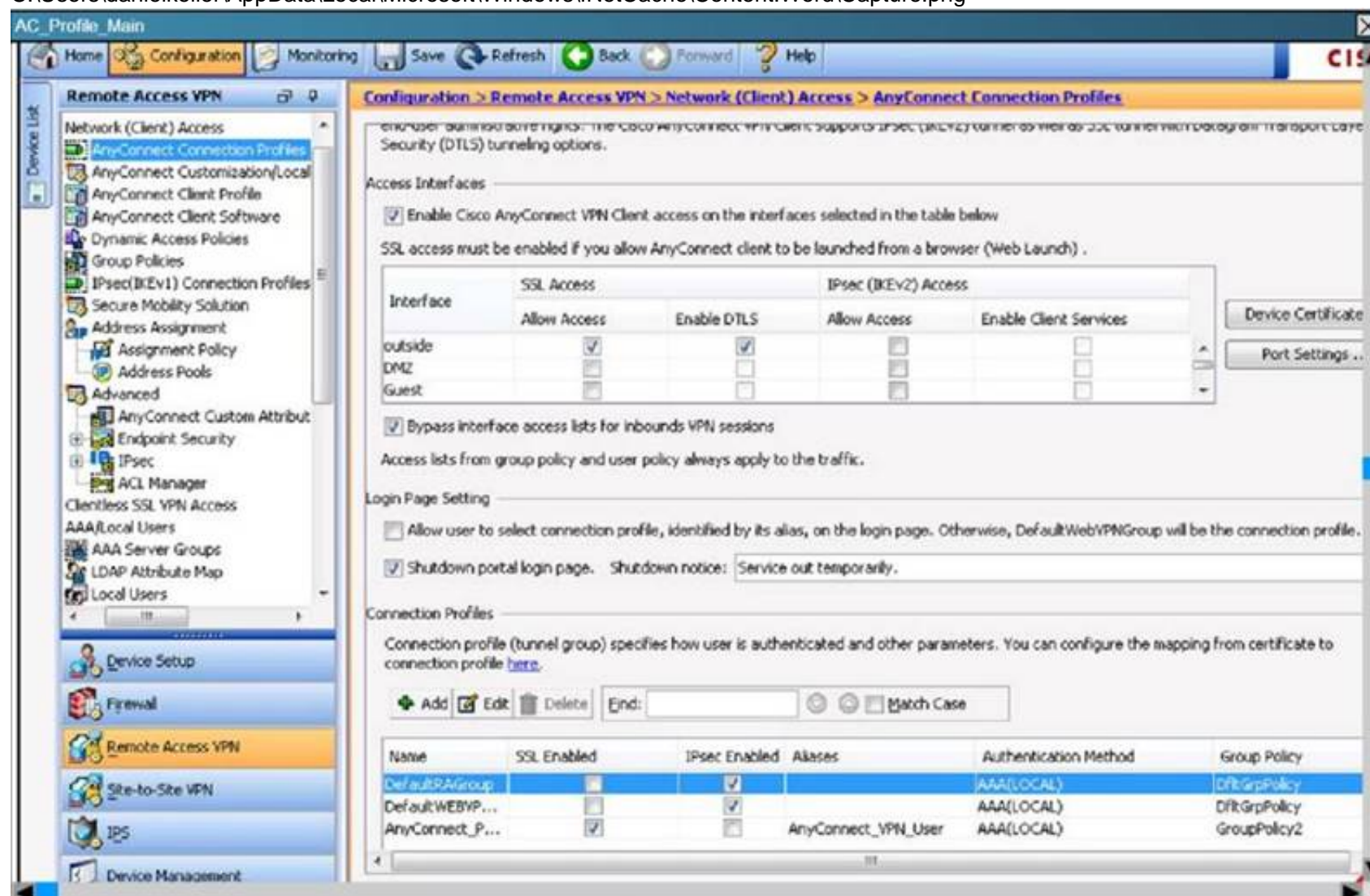


Which address range will be assigned to the AnyConnect users?

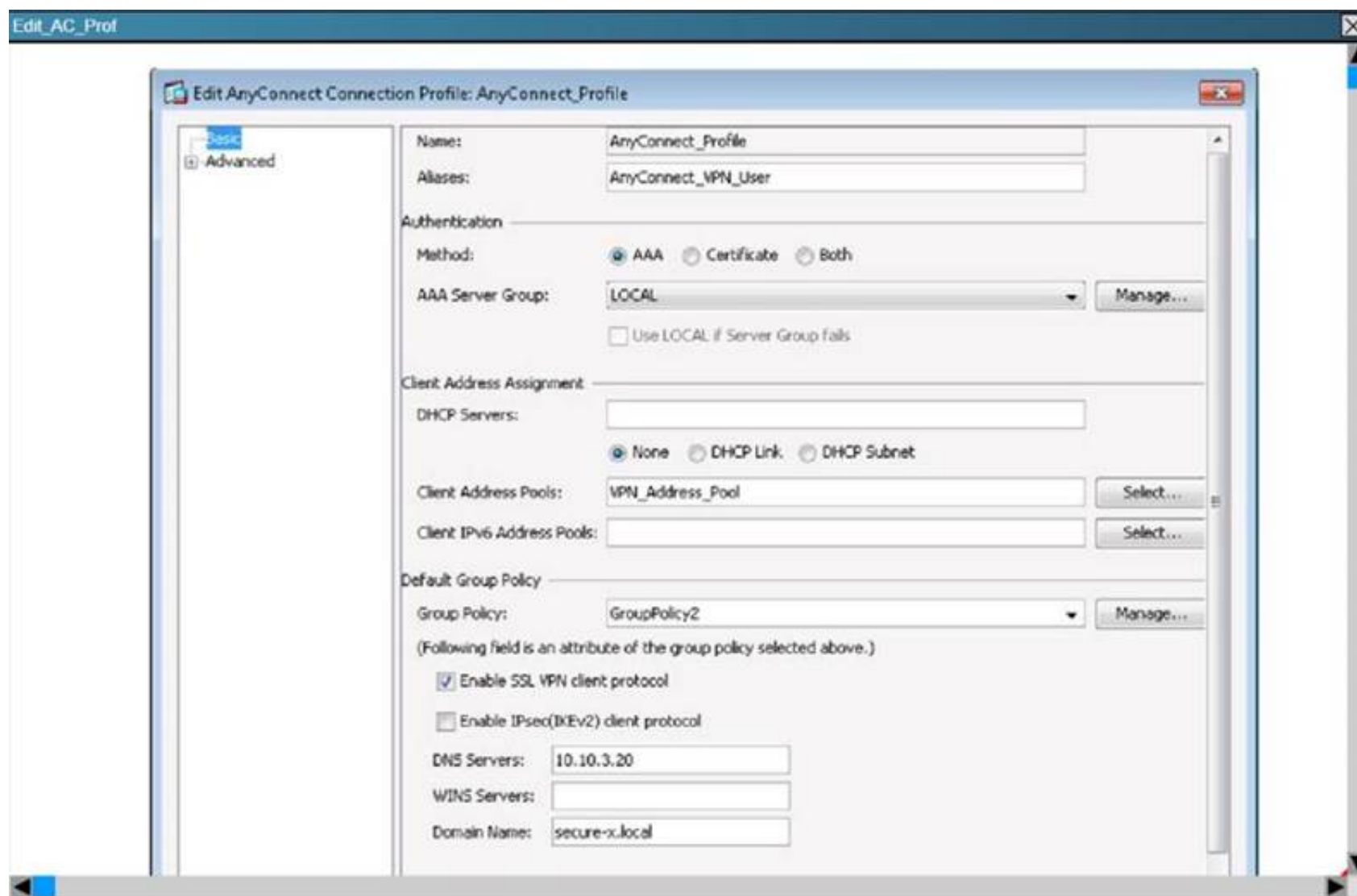
- A. 10.10.15.40-50/24
- B. 209.165.201.20-30/24
- C. 192.168.1.100-150/24
- D. 10.10.15.20-30/24

Answer: D

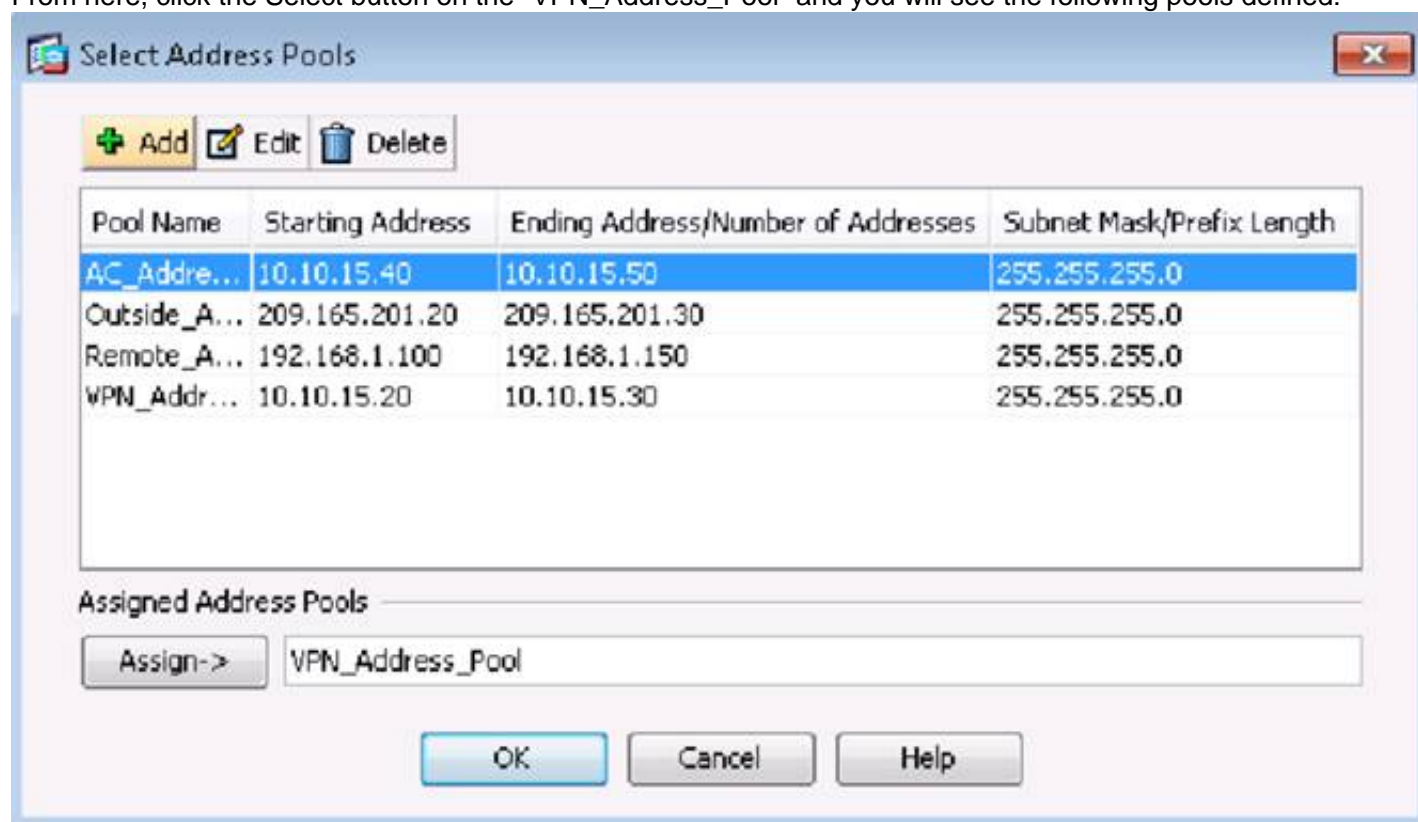
Explanation: First Navigate to the Configuration -> Remote Access VPN tab and then choose the "AnyConnect Connection Profile as shown below:
C:\Users\danielkeller\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Capture.png



Then, clicking on the AnyConnect Profile at the bottom will bring you to the edit page shown below:
C:\Users\danielkeller\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Capture.png



From here, click the Select button on the "VPN_Address_Pool" and you will see the following pools defined:



Here we see that the VPN_Address_Pool contains the IP address range of 10.10.15.20-10.10.15.30/24.

NEW QUESTION 311

Which statement about the hub in a DMVPN configuration with iBGP is true?

- A. It must be a route reflector client.
- B. It must redistribute EIGRP from the spokes.
- C. It must be in a different AS.
- D. It must be a route reflector.

Answer: D

NEW QUESTION 312

Which type of communication in a FlexVPN implementation uses an NHRP shortcut?

- A. spoke to hub
- B. spoke to spoke
- C. hub to spoke
- D. hub to hub

Answer: B

NEW QUESTION 315

Which cryptographic algorithms are a part of the Cisco NGE suite?

- A. HIPPADES
- B. AES-CBC-128
- C. RC4-128
- D. AES-GCM-256

Answer: D

Explanation:

Reference: https://www.cisco.com/web/learning/le21/le39/docs/tdw166_prezo.pdf

NEW QUESTION 320

Refer to the exhibit.

```
crypto ipsec transform-set gdoi-trans-group1 esp-aes esp-sha-hmac

crypto ipsec profile gdoi-profile-group1
  set security-association lifetime seconds 1800
  set transform-set gdoi-trans-group1

crypto gdoi group group1
  identity number 1
  server local
    rekey lifetime seconds 86400
    rekey retransmit 10 number 2
    rekey authentication mypubkey rsa group1-export-general
    rekey transport unicast
  sa ipsec 1
    profile gdoi-profile-group1
    match address ipv4 101
    replay counter window-size 64
  address ipv4 209.165.200.225
  redundancy
    local priority 10
    peer address ipv4 209.165.200.225
```

Which VPN solution does this configuration represent?

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

Answer: B

NEW QUESTION 325

Which Cisco adaptive security appliance command can be used to view the IPsec PSK of a tunnel group in cleartext?

- A. more system:running-config
- B. show running-config crypto
- C. show running-config tunnel-group
- D. show running-config tunnel-group-map
- E. clear config tunnel-group
- F. show ipsec policy

Answer: A

NEW QUESTION 327

An administrator desires that when work laptops are not connected to the corporate network, they should automatically initiate an AnyConnect VPN tunnel back to headquarters. Where does the administrator configure this?

- A. Via the svc trusted-network command under the group-policy sub-configuration mode on the ASA
- B. Under the "Automatic VPN Policy" section inside the Anyconnect Profile Editor within ASDM
- C. Under the TNDPolicy XML section within the Local Preferences file on the client computer
- D. Via the svc trusted-network command under the global webvpn sub-configuration mode on the ASA

Answer: B

NEW QUESTION 332

Refer to the exhibit.

```
%LINK-3-UPDOWN: Interface Tunnel0, changed state to up
NHRP: if_up: Tunnel0 proto 0
NHRP: Tunnel0: Cache update for target 10.1.1.254/32 next-hop 10.1.1.254 172.16.10.1
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220
NHRP: Attempting to send packet via DEST 10.1.1.25
```

Which action is demonstrated by this debug output?

- A. NHRP initial registration by a spoke.
- B. NHRP registration acknowledgement by the hub.
- C. Disabling of the DMVPN tunnel interface.
- D. IPsec ISAKMP phase 1 negotiation.

Answer: A

NEW QUESTION 335

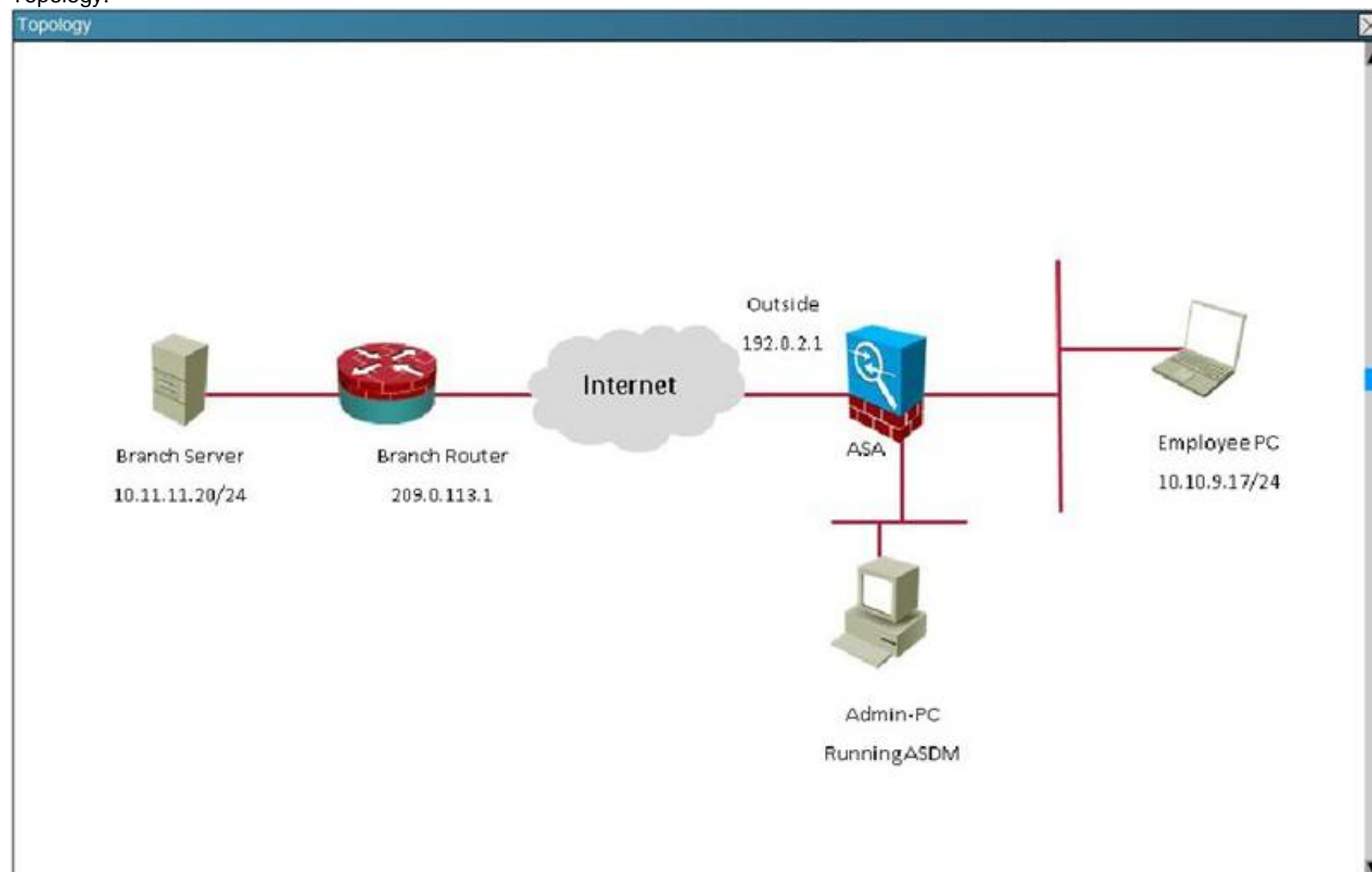
Scenario:

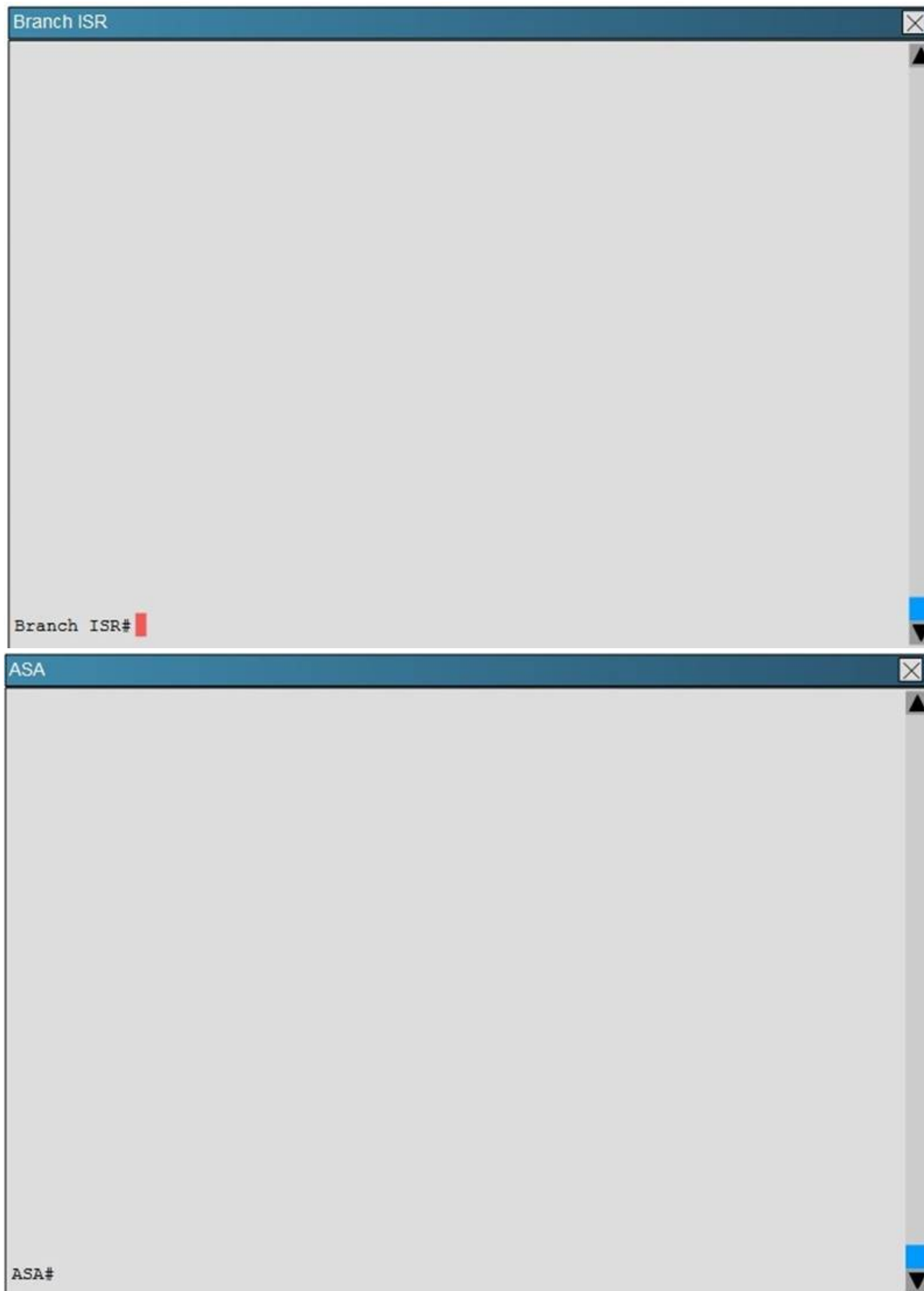
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

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:





Which transform set is being used on the branch ISR?

- A. Default
- B. ESP-3DES ESP-SHA-HMAC
- C. ESP-AES-256-MD5-TRANS mode transport
- D. TSET

Answer: B

Explanation: This can be seen from the “show crypto ipsec sa” command as shown below:

Branch ISR

```
Branch ISR#show crypto ipsec sa
interface: GigabitEthernet0/1
  Crypto map tag: VPN-to-ASA, local addr 203.0.113.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
current_peer 192.0.2.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 569, #pkts encrypt: 569, #pkts digest: 569
  #pkts decaps: 681, #pkts decrypt: 681, #pkts verify: 681
  #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

local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x8E47598C(2387040652)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xCE89192A(3465091370)
  transform: esp-3des esp-sha-hmac ,
```

Branch ISR

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
current_peer 192.0.2.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 569, #pkts encrypt: 569, #pkts digest: 569
  #pkts decaps: 681, #pkts decrypt: 681, #pkts verify: 681
  #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

local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x8E47598C(2387040652)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xCE89192A(3465091370)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
Branch ISR#
Branch ISR#
```

NEW QUESTION 336

Which three types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose three.)

- A. HTTP
- B. VNC
- C. CIFS
- D. RDP
- E. HTTPS
- F. ICA (Citrix)

Answer: ACE

NEW QUESTION 340

A customer requires all traffic to go through a VPN. However, access to the local network is also required. Which two options can enable this configuration? (Choose two.)

- A. split exclude
- B. use of an XML profile
- C. full tunnel by default

- D. split tunnel
- E. split include

Answer: AB

NEW QUESTION 342

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

- A. enrollment profile
- B. enrollment terminal
- C. enrollment url
- D. enrollment selfsigned

Answer: A

NEW QUESTION 343

Refer to the exhibit.

```
access-list temp_acl webtype permit url http://10.0.4.10
webvpn
enable outside
svc enable
tunnel-group-list enable
group-policy temp_worker internal
group-policy temp_worker attributes
banner value Welcome Temp Workers!
vpn-tunnel-protocol webvpn
vlan 100
webvpn
url-list value Corporate_Server
url-entry disable
group-policy Default attributes
vpn-tunnel-protocol IPsec svc webvpn
webvpn
url-list value Corporate_Server
filter value temp_acl
username temp1 password cisco
```

```
username temp1 attributes
vpn-group-policy temp_worker
vpn-tunnel-protocol webvpn
group-lock value temp_worker
service-type remote-access
webvpn
file-browsing disable
file-entry enable
url-entry disable
hidden-shares none
url-list value Corporate_Server
customization value temp_worker
tunnel-group temp_worker type remote-access
tunnel-group temp_worker general-attributes
default-group-policy temp_worker
tunnel-group temp_worker webvpn-attributes
customization temp_worker
group-alias temp_worker enable
group-url https://192.168.4.2/temp_worker enable
```

A junior network engineer configured the corporate Cisco ASA appliance to accommodate a new temporary worker. For security reasons, the IT department wants to restrict the internal network access of the new temporary worker to the corporate server, with an IP address of 10.0.4.10. After the junior network engineer finished the configuration, an IT security specialist tested the account of the temporary worker. The tester was able to access the URLs of additional secure servers from the WebVPN user account of the temporary worker.

What did the junior network engineer configure incorrectly?

- A. The ACL was configured incorrectly.
- B. The ACL was applied incorrectly or was not applied.
- C. Network browsing was not restricted on the temporary worker group policy.
- D. Network browsing was not restricted on the temporary worker user policy.

Answer: B

NEW QUESTION 348

Which algorithm does ISAKMP use to securely derive encryption and integrity keys?

- A. Diffie – Hellman
- B. AES
- C. ECDSA
- D. RSA
- E. 3DES

Answer: D

NEW QUESTION 350

An XYZ Corporation systems engineer, while making a sales call on the ABC Corporation headquarters, tried to access the XYZ sales demonstration folder to transfer a demonstration via FTP from an ABC conference room behind the firewall. The engineer could not reach XYZ through the remote-access VPN tunnel. From home the previous day, however, the engineer did connect to the XYZ sales demonstration folder and transferred the demonstration via IPsec over DSL. To get the connection to work and transfer the demonstration, what should the engineer do?

- A. Change the MTU size on the IPsec client to account for the change from DSL to cable transmission.
- B. Enable the local LAN access option on the IPsec client.
- C. Enable the IPsec over TCP option on the IPsec client.
- D. Enable the clientless SSL VPN option on the PC.

Answer: C

Explanation: IP Security (IPSec) over Transmission Control Protocol (TCP) enables a VPN Client to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, User Datagram Protocol (UDP) 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and it enables secure tunneling through both Network Address Translation (NAT) and Port Address Translation (PAT) devices and firewalls

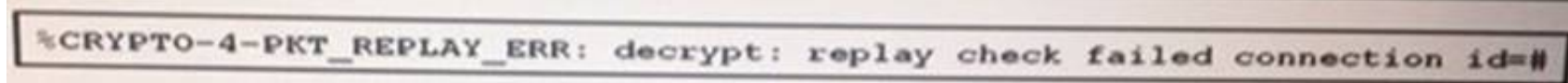
NEW QUESTION 354

What routing protocol is recommended by Cisco in DMVPN between company router and ISP router? (Choose Two)

- A. OSPF
- B. RIPv2
- C. ISIS
- D. BGP
- E. EIGRP

Answer: DE

NEW QUESTION 358



Refer to the exhibit. An engineer encounters a debug message. Which action can the engineer take to eliminate this error message?

- A. Use stronger encryption suite.
- B. Correct the VPN peer address.
- C. Make adjustment to IPSec replay window.
- D. Change the preshared key to match.

Answer: B

NEW QUESTION 361

Which DAP endpoint attribute checks for the matching MAC address of a client machine?

- A. device
- B. process
- C. antispyware
- D. BIA

Answer: A

NEW QUESTION 366

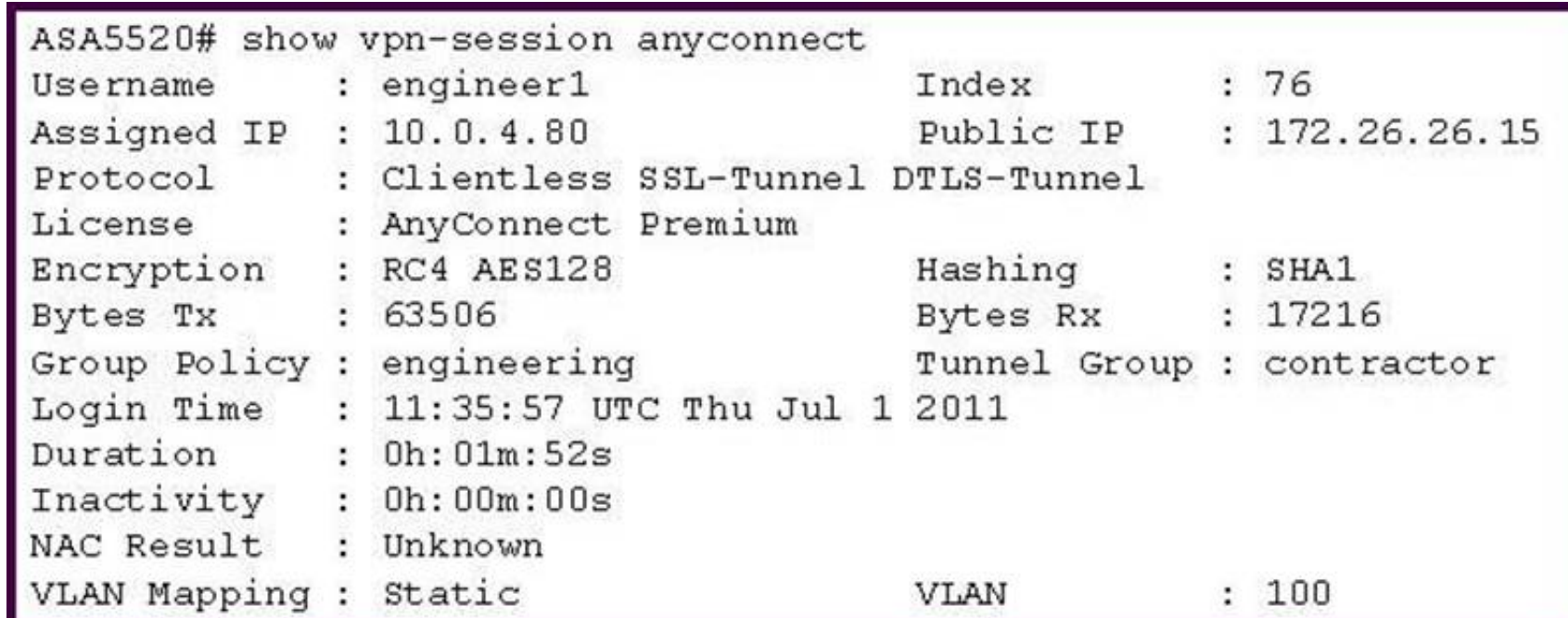
Using the Next Generation Encryption technologies, which is the minimum acceptable encryption level to protect sensitive information?

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

Answer: C

NEW QUESTION 369

Refer to the exhibit.



A NOC engineer needs to tune some prelogin parameters on an SSL VPN tunnel.

From the information that is shown, where should the engineer navigate to find the prelogin session attributes?

- A. "engineering" Group Policy
- B. "contractor" Connection Profile
- C. "engineer1" AAA/Local Users

D. DfltGrpPolicy Group Policy

Answer: B

Explanation: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac05hosts

NEW QUESTION 371

When using clientless SSL VPN, you might not want some applications or web resources to go through the Cisco ASA appliance. For these application and web resources, as a Cisco ASA administrator, which configuration should you use?

- A. Configure the Cisco ASA appliance for split tunneling.
- B. Configure network access exceptions in the SSL VPN customization editor.
- C. Configure the Cisco ASA appliance to disable content rewriting.
- D. Configure the Cisco ASA appliance to enable URL Entry bypass.
- E. Configure smart tunnel to bypass the Cisco ASA appliance proxy function.

Answer: C

Explanation: http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/vpn_web.html Content Rewrite

The Content Rewrite pane lists all applications for which content rewrite is enabled or disabled.

Clientless SSL VPN processes application traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTP traffic which may have different semantics and access control rules depending on whether the user is using an application within or independently of an SSL VPN device.

By default, the security appliance rewrites, or transforms, all clientless traffic. You might not want some applications and web resources (for example, public websites) to go through the security appliance. The security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without going through the security appliance. This is similar to split-tunneling in an IPSec VPN connection.

You can create multiple rewrite rules. The rule number is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

NEW QUESTION 374

An engineer is configuring an IPsec VPN with IKEv2. Which three components are part of the IKEv2 proposal for this implementation? (Choose three.)

- A. key ring
- B. DH group
- C. integrity
- D. tunnel name
- E. encryption

Answer: BCE

NEW QUESTION 375

When attempting to tunnel FTP traffic through a stateful firewall that might be performing NAT or PAT, which type of VPN tunneling should you use to allow the VPN traffic through the stateful firewall?

- A. clientless SSL VPN
- B. IPsec over TCP
- C. smart tunnel
- D. SSL VPN plug-ins

Answer: B

Explanation: IP Security (IPSec) over Transmission Control Protocol (TCP) enables a VPN Client to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, User Datagram Protocol (UDP) 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and it enables secure tunneling through both Network Address Translation (NAT) and Port Address Translation (PAT) devices and firewalls

NEW QUESTION 379

An employee working from home sends all traffic to company server. Is there policy for him to use his local internet provider and VPN only for company data?

- A. tunnel all
- B. No such policy exist
- C. tunnel specified
- D. tunnel exclude

Answer: C

NEW QUESTION 381

Refer to the exhibit.

```
ASA5520# show vpn-session anyconnect
Username       : engineer1           Index       : 76
Assigned IP    : 10.0.4.80           Public IP    : 172.26.26.15
Protocol       : Clientless SSL-Tunnel DTLS-Tunnel
License        : AnyConnect Premium
Encryption     : RC4 AES128           Hashing      : SHA1
Bytes Tx       : 63506               Bytes Rx     : 17216
Group Policy    : engineering         Tunnel Group : contractor
Login Time     : 11:35:57 UTC Thu Jul 1 2011
Duration       : 0h:01m:52s
Inactivity     : 0h:00m:00s
NAC Result     : Unknown
VLAN Mapping   : Static              VLAN        : 100
```

A NOC engineer needs to tune some postlogin parameters on an SSL VPN tunnel.

From the information shown, where should the engineer navigate to, in order to find all the postlogin session parameters?

- A. "engineering" Group Policy
- B. "contractor" Connection Profile
- C. DefaultWEBVPNGroup Group Policy
- D. DefaultRAGroup Group Policy
- E. "engineer1" AAA/Local Users

Answer: A

Explanation: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1054618

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of remote users.

Entering the policy group command places the router in webvpn group policy configuration mode. After it is configured, the group policy is attached to the SSL VPN context configuration by configuring the default-group-policy command.

The following tasks are accomplished in this configuration:

The presentation of the SSL VPN portal page is configured.

A NetBIOS server list is referenced.

A port-forwarding list is referenced.

The idle and session timers are configured.

A URL list is referenced.

NEW QUESTION 383

Which equation describes an elliptic curve?

- A. $y^3 = x^3 + ax + b$
- B. $x^3 = y^2 + ab + x$
- C. $y^4 = x^2 + ax + b$
- D. $y^2 = x^3 + ax + b$
- E. $y^2 = x^2 + ax + b^2$

Answer: D

NEW QUESTION 384

Refer to the exhibit.

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
failed its sanity check or is malformed
```

Which type of mismatch is causing the problem with the IPsec VPN tunnel?

- A. PSK
- B. Phase 1 policy
- C. transform set
- D. crypto access list

Answer: A

NEW QUESTION 388

A company has a Flex VPN solution for remote access and one of their Cisco any Connect remote clients is having trouble connecting properly. Which command verifies that packets are being encrypted and decrypted?

- A. show crypto session active

- B. show crypto ikev2 stats
- C. show crypto ikev1 sa
- D. show crypto ikev2 sa
- E. show crypto session detail

Answer: E

NEW QUESTION 391

Which statement about plug-ins is false?

- A. Plug-ins do not require any installation on the remote system.
- B. Plug-ins require administrator privileges on the remote system.
- C. Plug-ins support interactive terminal access.
- D. Plug-ins are not supported on the Windows Mobile platform.

Answer: B

Explanation: http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deployhtml#wp1162435

Plug-ins

The security appliance supports Java plug-ins for clientless SSL VPN connections. Plug-ins are Java programs that operate in a browser. These plug-ins include SSH/Telnet, RDP, VNC, and Citrix.

Per the GNU General Public License (GPL), Cisco redistributes plug-ins without making any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.

To use plug-ins you must install Java Runtime Environment (JRE) 1.4.2.x or greater. You must also use a compatible browser specified here:

<http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpncompatibility.html>

NEW QUESTION 396

Refer to the exhibit.



You are configuring a laptop with the Cisco VPN Client, which uses digital certificates for authentication. Which protocol does the Cisco VPN Client use to retrieve the digital certificate from the CA server?

- A. FTP
- B. LDAP
- C. HTTPS
- D. SCEP
- E. OCSP

Answer: D

Explanation: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html About CRLs

Certificate Revocation Lists provide the security appliance with one means of determining whether a certificate that is within its valid time range has been revoked by its issuing CA. CRL configuration is a part of the configuration of a trustpoint.

You can configure the security appliance to make CRL checks mandatory when authenticating a certificate (revocation-check crl command). You can also make the CRL check optional by adding the none argument (revocation-check crl none command), which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

The security appliance can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a length of time configurable for each trustpoint.

When the security appliance has cached a CRL for more than the length of time it is configured to cache CRLs, the security appliance considers the CRL too old to be reliable, or "stale". The security appliance attempts to retrieve a newer version of the CRL the next time a certificate authentication requires checking the stale CRL.

NEW QUESTION 400

Refer to the exhibit.

```
hostname RouterA
interface GigabitEthernet 0/0/0
ip address 10.0.0.1 255.255.255.0
standby 1 priority 110
standby ikev1-cluster
end

crypto ikev2 cluster
standby-group ikev1-cluster
slave max-session 500
port 2000
no shutdown

crypto ikev2 redirect gateway init
```

Which type of VPN implementation is displayed?

- A. IKEv2 reconnect
- B. IKEv1 cluster
- C. IKEv2 load balancer
- D. IKEv1 client
- E. IPsec high availability
- F. IKEv2 backup gateway

Answer: C

NEW QUESTION 401

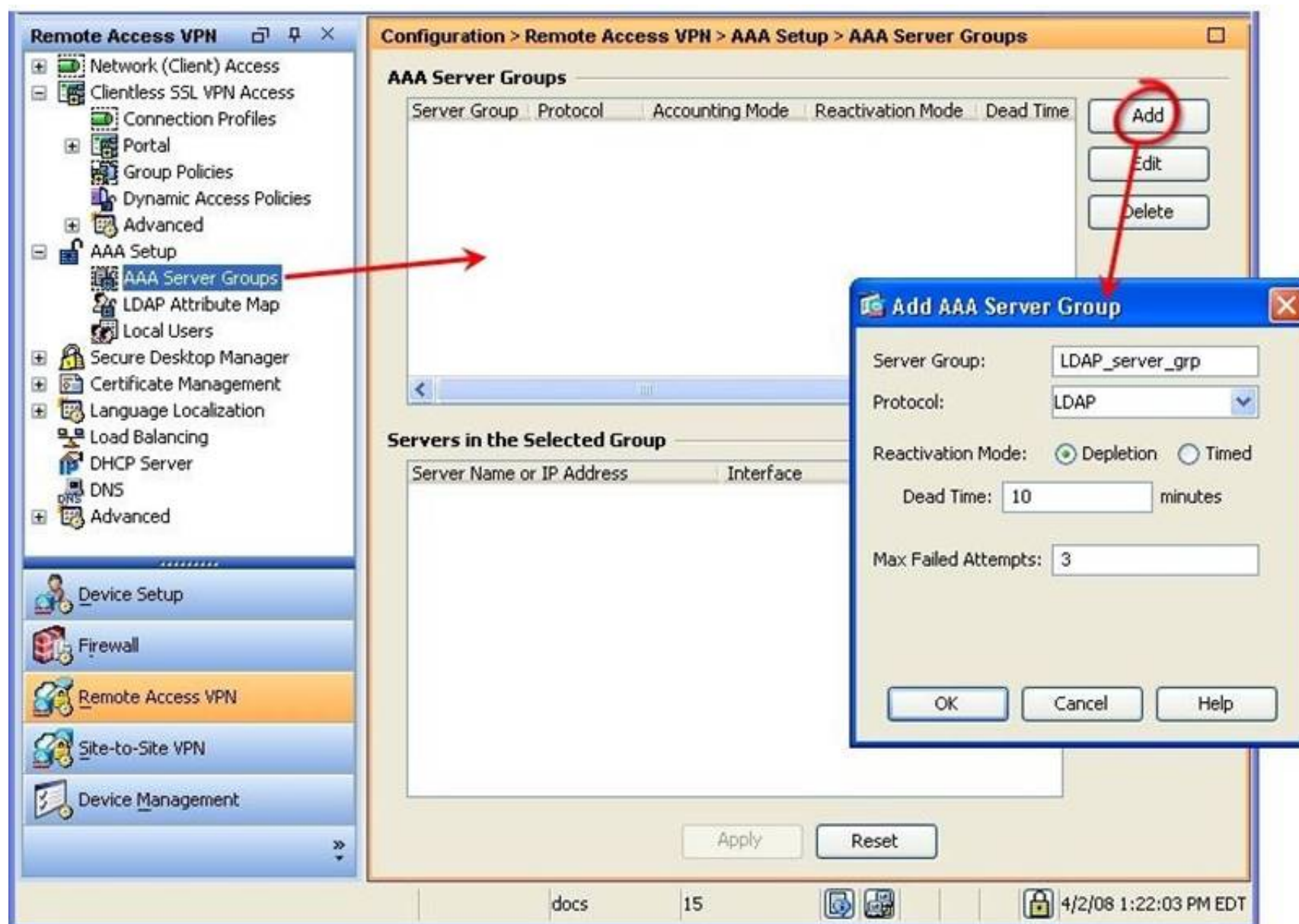
Which statement about CRL configuration is correct?

- A. CRL checking is enabled by default.
- B. The Cisco ASA relies on HTTPS access to procure the CRL list.
- C. The Cisco ASA relies on LDAP access to procure the CRL list.
- D. The Cisco Secure ACS can be configured as the CRL server.

Answer: C

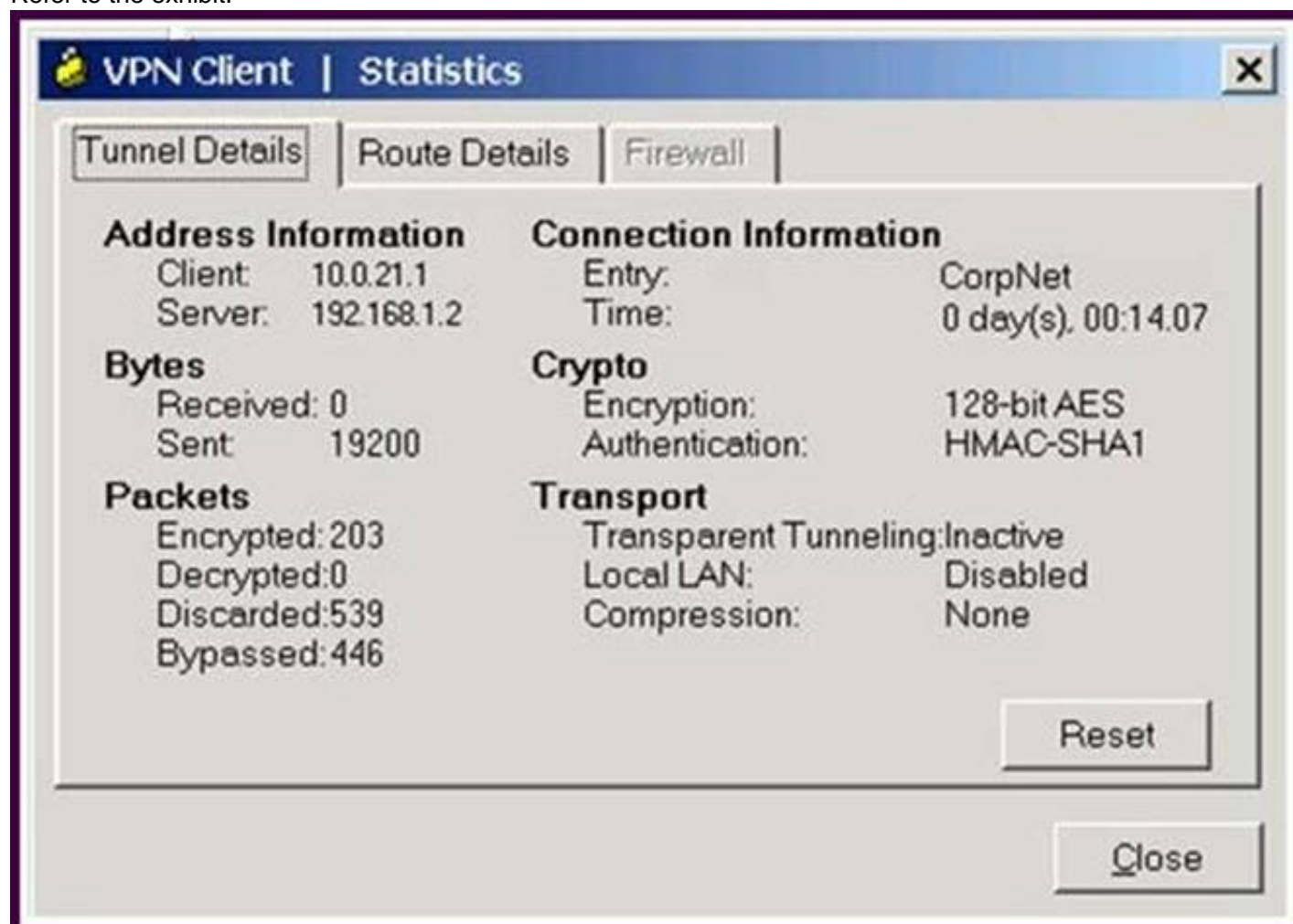
Explanation: ASA SSLVPN deployment guide:

The security appliance supports various authentication methods: RSA one-time passwords, Radius, Kerberos, LDAP, NT Domain, TACACS, Local/Internal, digital certificates, and a combination of both authentication and certificates.



NEW QUESTION 406

Refer to the exhibit.



A new NOC engineer is troubleshooting a VPN connection.

Which statement about the fields within the Cisco VPN Client Statistics screen is correct?

- A. The ISP-assigned IP address of 10.0.21.1 is assigned to the VPN adapter of the PC.
- B. The IP address of the security appliance to which the Cisco VPN Client is connected is 192.168.1.2.
- C. CorpNet is the name of the Cisco ASA group policy whose tunnel parameters the connection is using.
- D. The ability of the client to send packets transparently and unencrypted through the tunnel for test purposes is turned off.
- E. With split tunneling enabled, the Cisco VPN Client registers no decrypted packets.

Answer: B

NEW QUESTION 408

When initiating a new SSL or TLS session, the client receives the server SSL certificate and validates it. After validating the server certificate, what does the client use the certificate for?

- A. The client and server use the server public key to encrypt the SSL session data.
- B. The server creates a separate session key and sends it to the client.
- C. The client decrypts the session key by using the server public key.
- D. The client and server switch to a DH key exchange to establish a session key.
- E. The client generates a random session key, encrypts it with the server public key, and then sends it to the server.

Answer: D

NEW QUESTION 412

Refer to the exhibit.

%ASA-5-713259: Group = contractor, Username = vpnuser, IP = 172.16.1.20, Session is being torn down. Reason: Phase 2 Mismatch

While troubleshooting a remote-access application, a new NOC engineer received the logging message that is shown in the exhibit. Which configuration is most likely to be mismatched?

- A. IKE configuration
- B. extended authentication configuration
- C. IPsec configuration
- D. digital certificate configuration

Answer: C

Explanation: The termination reason for the ISAKMP session appears, which occurs when the session is torn down through session management.

- groupname—The tunnel group of the session being terminated
- username—The username of the session being terminated
- peerIP—The peer address of the session being terminated
- reason—The RADIUS termination reason of the session being terminated. Reasons include the following:
 - Port Preempted (simultaneous logins)
 - Idle Timeout
 - Max Time Exceeded
 - Administrator Reset

NEW QUESTION 415

Which command identifies an AnyConnect profile that was uploaded to the router flash?

- A. crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml
- B. svc import profile SSL_profile flash:simos-profile.xml
- C. anyconnect profile SSL_profile flash:simos-profile.xml
- D. webvpn import profile SSL_profile flash:simos-profile.xml

Answer: A

NEW QUESTION 419

Authorization of a clientless SSL VPN defines the actions that a user may perform within a clientless SSL VPN session. Which statement is correct concerning the SSL VPN authorization process?

- A. Remote clients can be authorized by applying a dynamic access policy, which is configured on an external AAA server.
- B. Remote clients can be authorized externally by applying group parameters from an external database.
- C. Remote client authorization is supported by RADIUS and TACACS+ protocols.
- D. To configure external authorization, you must configure the Cisco ASA for cut-through proxy.

Answer: B

Explanation: CISCO SSL VPN guide

The aaa authentication command is entered to specify an authentication list or server group under a SSL VPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.

The database that is configured for remote-user authentication on the SSL VPN gateway can be a local database, or the database can be accessed through any RADIUS or TACACS+ AAA server.

We recommend that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions.

NEW QUESTION 422

Which protocol can be used for better throughput performance when using Cisco AnyConnect VPN?

- A. TLSv1
- B. TLSv1.1
- C. TLSv1.2
- D. DTLSv1

Answer: D

NEW QUESTION 423

As network consultant, you are asked to suggest a VPN technology that can support a multivendor environment and secure traffic between sites. Which

technology should you recommend?

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

Answer: B

NEW QUESTION 424

Which algorithm does ISAKMP used to securely derive encryption and integrity keys?

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

Answer: C

NEW QUESTION 426

Refer to the exhibit.

```
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Failed to verify the proposed
policies
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):There was no IPSEC policy found for
received TS

*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):SM Trace-> SA:
I_SPI=527FCACA776C4724 R_SPI=EFBD7D296CCB08CA (R) MsgID = 00000001 CurState:
R_VERIFY_AUTH Event: EV_TS_UNACCEPT
*Dec 5 20:49:53.785: IKEv2:(SA ID = 1070):Sending TS unacceptable notify
```

What is the problem with the IKEv2 site-to-site VPN tunnel?

- A. incorrect PSK
- B. crypto access list mismatch
- C. incorrect tunnel group
- D. crypto policy mismatch
- E. incorrect certificate

Answer: D

NEW QUESTION 431

Which two statements comparing ECC and RSA are true? (Choose two.)

- A. ECC can have the same security as RSA but with a shorter key size.
- B. ECC lags in performance when compared with RSA.
- C. Key generation in ECC is slower and less CPU intensive.
- D. ECC cannot have the same security as RSA, even with an increased key size.
- E. Key generation in ECC is faster and less CPU intensive.

Answer: AE

NEW QUESTION 432

Which statement is correct concerning the trusted network detection (TND) feature?

- A. The Cisco AnyConnect 3.0 Client supports TND on Windows, Mac, and Linux platforms.
- B. With TND, one result of a Cisco Secure Desktop basic scan on an endpoint is to determine whether a device is a member of a trusted or an untrusted network.
- C. If enabled, and a CSD scan determines that a host is a member of an untrusted network, an administrator can configure the TND feature to prohibit an end user from launching the Cisco AnyConnect VPN Client.
- D. When the user is inside the corporate network, TND can be configured to automatically disconnect a Cisco AnyConnect session.

Answer: D

Explanation: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administration/guide/ac03featu Trusted Network Detection
Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.
If AnyConnect is also running Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the computer automatically closes.
TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office.
Because the TND feature controls the AnyConnect GUI and automatically initiates connections, the GUI should run at all times. If the user exits the GUI, TND does

not automatically start the VPN connection.
You configure TND in the AnyConnect profile. No changes are required to the ASA configuration.

NEW QUESTION 437

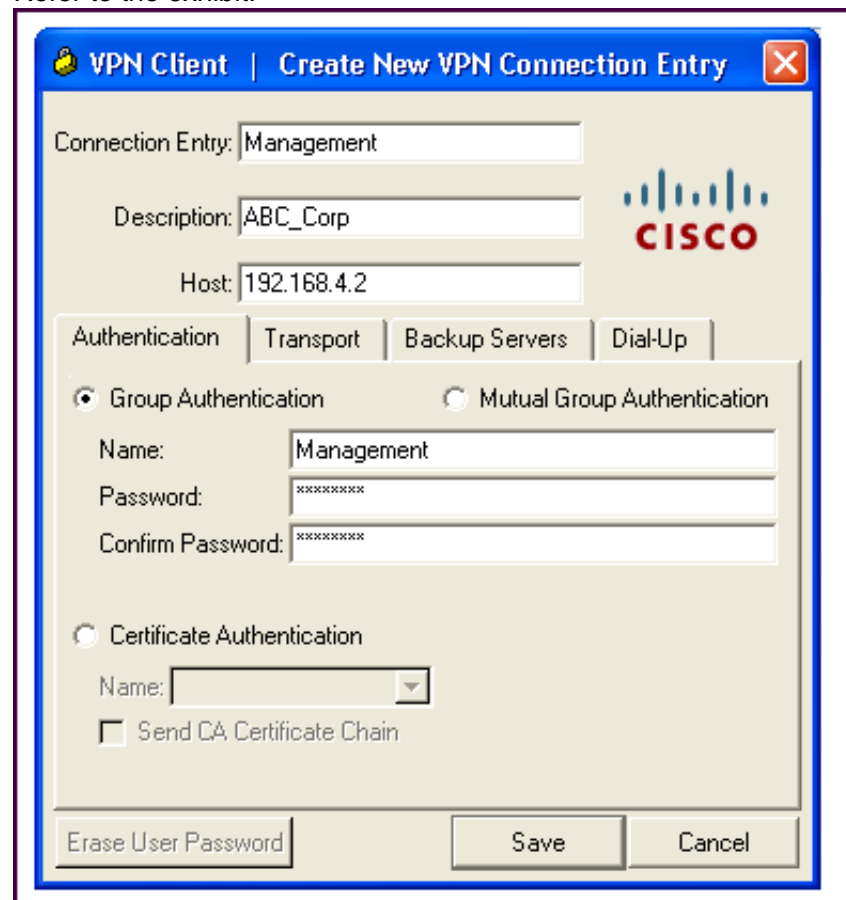
Which statement regarding hashing is correct?

- A. MD5 produces a 64-bit message digest.
- B. SHA-1 produces a 160-bit message digest.
- C. MD5 takes more CPU cycles to compute than SHA-1.
- D. Changing 1 bit of the input to SHA-1 can change up to 5 bits in the output.

Answer: B

NEW QUESTION 442

Refer to the exhibit.



A NOC engineer is in the process of entering information into the Create New VPN Connection Entry fields. Which statement correctly describes how to do this?

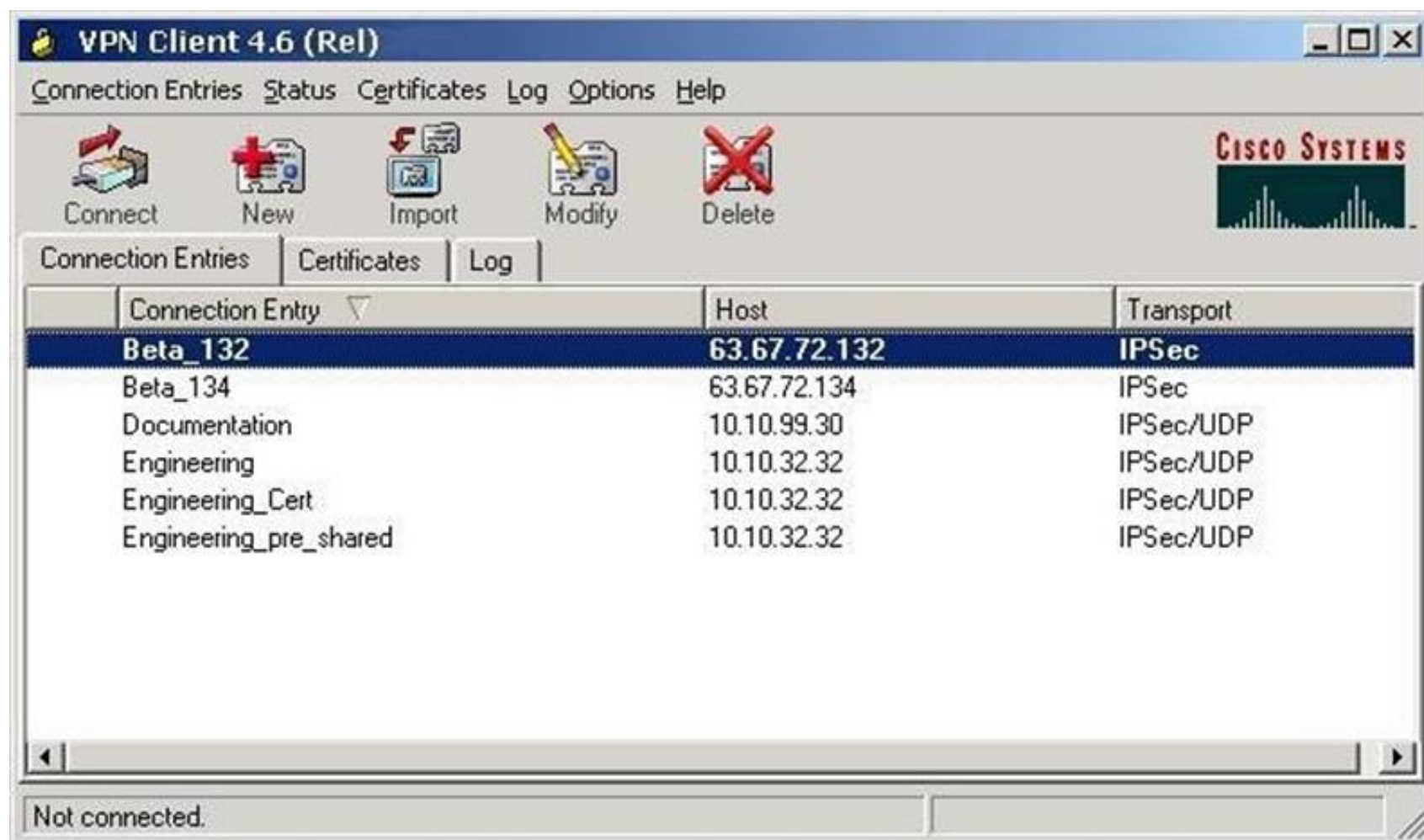
- A. In the Connection Entry field, enter the name of the connection profile as it is specified on the Cisco ASA appliance.
- B. In the Host field, enter the IP address of the remote client device.
- C. In the Authentication tab, click the Group Authentication or Mutual Group Authentication radio button to enable symmetrical pre-shared key authentication.
- D. In the Name field, enter the name of the connection profile as it is specified on the Cisco ASA appliance.

Answer: D

Explanation: http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/win/user/guide/vc4.html#

Step 1 Start the VPN Client by choosing Start > Programs > Cisco Systems VPN Client > VPN Client.

Step 2 The VPN Client application starts and displays the advanced mode main window (Figure 4-1). If you are not already there, open the Options menu in simple mode and choose Advanced Mode or press Ctrl-M.



Step 3 Select New from the toolbar or the Connection Entries menu. The VPN Client displays a form



Step 4 Enter a unique name for this new connection. You can use any name to identify this connection; for example, Engineering. This name can contain spaces, and it is not case-sensitive.

Step 5 Enter a description of this connection. This field is optional, but it helps further identify this connection. For example, Connection to Engineering remote server.

Step 6 Enter the hostname or IP address of the remote VPN device you want to access. Group Authentication

Your network administrator usually configures group authentication for you. If this is not the case, use the following procedure:

Step 1 Click the Group Authentication radio button.

Step 2 In the Name field, enter the name of the IPSec group to which you belong. This entry is case-sensitive. Step 3 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The field displays only asterisks.

Step 4 Verify your password by entering it again in the Confirm Password field.

NEW QUESTION 443

Which two operational advantages does GetVPN offer over site-to-site IPSec tunnel in a private MPLS-based core network? (Choose two.)

- A. Key servers perform encryption and decryption of all the data in the network, which allows for tight security policies.
- B. Traffic uses one VRF to encrypt data and a different one to decrypt data, which allows for multicast traffic isolation.
- C. GETVPN is tunnel-less, which allows any group member to perform decryption and routing around network failures.
- D. Packets carry original source and destination IP addresses, which allows for optimal routing of encrypted traffic.
- E. Group Domain of Interpretation protocol allows for homomorphic encryption, which allows group members to operate on messages without decrypting them

Answer: DE

NEW QUESTION 447

An engineer is attempting to establish a new site-to-site VPN connection. The tunnel terminates on an ASA 5506-X which is behind an ASA 5515-X. The engineer notices that the tunnel is not establishing. Which option is a potential cause?

- A. Certificates were not configured
- B. Diffie – Helman Group is not set
- C. Access lists were not applied
- D. NAT – traversal is not configured

Answer: D

NEW QUESTION 452

An engineer has configured Cisco AnyConnect VPN using IKEv2 on a Cisco ISO router. The user cannot connect in the Cisco AnyConnect client, but receives an alert message “Use a browser to gain access.” Which action does the engineer take to eliminate this issue?

- A. Reset user login credentials.
- B. Disable the HTTP server.
- C. Correct the URL address.
- D. Connect using HTTPS.

Answer: B

NEW QUESTION 456

Which three configurations are prerequisites for stateful failover for IPsec? (Choose three.)

- A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.
- B. Only crypto map configuration that is set up on the active device must be duplicated on the standby device.
- C. The IPsec configuration that is set up on the active device must be duplicated on the standby device.
- D. The active and standby devices can run different versions of the Cisco IOS software but need to be the same type of device.
- E. The active and standby devices must run the same version of the Cisco IOS software and should be the same type of device.
- F. Only the IPsec configuration that is set up on the active device must be duplicated on the standbydevice; the IKE configuration is copied automatically.
- G. The IKE configuration that is set up on the active device must be duplicated on the standby device.

Answer: CEG

NEW QUESTION 458

A network engineer must configure a new VPN tunnel Utilizing IKEv2 For with three reasons would a configuration use IKEv2 instead d KEv1? (Choose three.)

- A. increased hash size
- B. DOS protection
- C. Preshared keys are used for authentication.
- D. RSA-Sig used for authentication
- E. native NAT traversal
- F. asymmetric authentication

Answer: BEF

NEW QUESTION 459

Refer to the exhibit.



The screenshot shows the 'Configuration > Remote Access VPN > AAA/Local Users > Local Users' page. It contains a table with the following data:

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
employee1	15	Full	employee	-- Inherit Group Polic...
manager1	2	No ASDM/CLI	management	-- Inherit Group Polic...
contractor	15	Full	-- Inherit Group Policy --	-- Inherit Group Polic...
contractor1	2	No ASDM/CLI	new_hire	-- Inherit Group Polic...

Buttons for 'Add', 'Edit', and 'Delete' are visible on the right side of the table.

When the user "contractor" Cisco AnyConnect tunnel is established, what type of Cisco ASA user restrictions are applied to the tunnel?

- A. full restrictions (no Cisco ASDM, no CLI, no console access)
- B. full restrictions (no read, no write, no execute permissions)
- C. full restrictions (CLI show commands and Cisco ASDM monitoring permissions only)
- D. full access with no restrictions

Answer: D

NEW QUESTION 464

An administrator received a report that a user cannot connect to the headquarters site using Cisco AnyConnect and receives this error. The installer was not able to start the Cisco VPN client, clientless access is not available, Which option is a possible cause for this error?

- A. The client version of Cisco AnyConnect is not compatible with the Cisco ASA software image.
- B. The operating system of the client machine is not supported by Cisco AnyConnect.

- C. The driver for Cisco AnyConnect is outdatate.
- D. The installed version of Java is not compatible with Cisco AnyConnect.

Answer: C

NEW QUESTION 466

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

- A. to define group members.
- B. to distribute static routing information.
- C. to distribute dynamic routing information.
- D. to encrypt transit traffic.

Answer: AD

NEW QUESTION 468

Refer to the exhibit.

```
access-list outside_cryptomap_1 line 1 extended deny tcp any host 10.0.4.4 eq https
access-list outside_cryptomap_1 line 1 extended permit tcp any host 10.0.4.0 255.255.255.0 eq https
crypto map outside_map 1 match address outside_cryptomap_1
```

In the CLI snippet that is shown, what is the function of the deny option in the access list?

- A. When set in conjunction with outbound connection-type bidirectional, its function is to prevent the specified traffic from being protected by the crypto map entry.
- B. When set in conjunction with connection-type originate-only, its function is to instruct the Cisco ASA to deny specific inbound traffic if it is not encrypted.
- C. When set in conjunction with outbound connection-type answer-only, its function is to instruct the Cisco ASA to deny specific outbound traffic if it is not encrypted.
- D. When set in conjunction with connection-type originate-only, its function is to cause all IP traffic that matches the specified conditions to be protected by the crypto map.

Answer: A

NEW QUESTION 470

When troubleshooting clientless SSL VPN connections, which option can be verified on the client PC?

- A. address assignment
- B. DHCP configuration
- C. tunnel group attributes
- D. host file misconfiguration

Answer: D

NEW QUESTION 474

An engineer is configuring high availability for crypto-map-based site-to-site VPNs on Cisco devices. Which protocol must be used?

- A. VRRP
- B. BFD
- C. ESP
- D. HSRP

Answer: D

NEW QUESTION 477

An engineer notices that while an employee is connected remotely, all traffic is being routed to the corporate network. Which split-tunnel policy allows remote client to use their local provider for Internet access when working from home?

- A. No policy allows that type of configuration
- B. tunnelspecified
- C. excludespecified
- D. tunnelall

Answer: B

NEW QUESTION 482

What is the name of the transform set being used on the ISR?

- A. Default
- B. ESP-AESESP-SHA-HMAC
- C. SP-AES-256-MD5-TRANS
- D. TSET

Answer: B

NEW QUESTION 484

Why must a network engineer avoid usage of the default X509 certificate when implementing clientless SSLVPN on an ASA?

- A. The certificate is too weak to provide adequate security.
- B. The certificate is regenerated at each reboot.
- C. The certificate must be managed by the local CA.
- D. The default X.509 certificate is not supported for SSLVPN.

Answer: C

NEW QUESTION 488

Mobile work force client are using Cisco Encryption for AnyConnect for remote access to the corporate network. In a attempt to save bandwidth on the internet circuit, those working remotely are permitted use to their local connectivity for internet use while still connect to the corporate network. Which feature allows distinct destination to be encryption on the remote client?

- A. DART
- B. Split Tuning
- C. NAT Exempt
- D. Kerberos

Answer: B

NEW QUESTION 492

Which option is one of the difference between FlexVPN and DMVPN?

- A. flexvpn uses ikev2 and dmvpn can use ikev1 or ikev2
- B. dmvpn can use ikev1 and ikev2 where flexvpn only uses ikev1
- C. flexvpn can use ikev1 and ikev2 where dmvpn uses only ikev2
- D. dmvp uses ikev1 and flexvpn use ikev3

Answer: A

NEW QUESTION 494

Which command will allow a referenced ASA interface to become accessible across a site-to-site VPN?

- A. access-list 101 extended permit ICMP any any
- B. crypto map vpn 10 match address 101
- C. crypto map vpn interface inside
- D. management-access <interface name>

Answer: B

NEW QUESTION 496

A customer requires site-to-site VPNs to connect third-party business partners and has purchased two ASAs.

The customer requests an active/active configuration.

Which model is needed to support an active/active solution?

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

Answer: C

NEW QUESTION 500

An engineer is configuring SSL VPN to provide access to a corporate network for remote users.

Traffic destined to the enterprise IP range should go over the tunnel and all other traffic should go directly to the internet.

Which feature should be configured?

- A. dual-horning
- B. hairpinning
- C. split-tunnel
- D. U-turning

Answer: C

NEW QUESTION 505

A company's remote locations connect to data centers via MPLS.

A new request requires that unicast traffic that exist the remote location be encrypted. Which no tunneled technology can be used to satisfy this requirement?

- A. SSL
- B. GET VPN
- C. DMVPN
- D. EzVPN

Answer: B

NEW QUESTION 507

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 First Try
- * 300-209 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 300-209 Practice Test Here](#)