

# 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

What are two benefits of DMVPN Phase 3? (Choose two.)

- A. Administrators can use summarization of routing protocol updates from hub to spokes.
- B. It introduces hierarchical DMVPN deployments.
- C. It introduces non-hierarchical DMVPN deployments.
- D. It supports L2TP over IPsec as one of the VPN protocols.

**Answer:** AB

#### NEW QUESTION 3

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

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

**Answer:** D

#### NEW QUESTION 4

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

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

**Answer:** C

#### NEW QUESTION 5

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

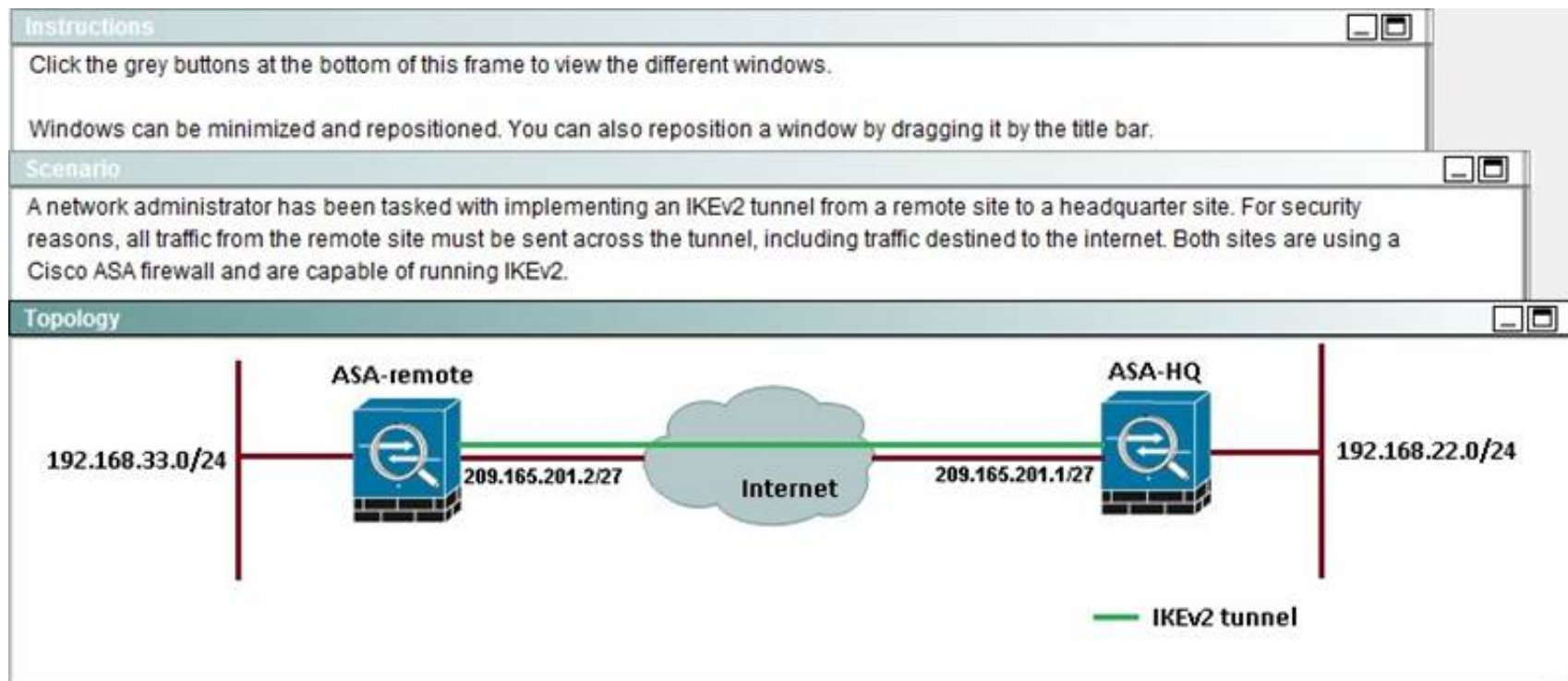
#### NEW QUESTION 6

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 7



**ASDM-HQ**

File View Tools Wizards Window Help Look For:

Home Configuration Monitoring Save Refresh Back Forward Help

**Site-to-Site VPN**

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces  
Enable interfaces for IPsec access.

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

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

+ Add Edit Delete

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

**ASDM-Remote**

File View Tools Wizards Window Help Look For:

Home Configuration Monitoring Save Refresh Back Forward Help

**Site-to-Site VPN**

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces  
Enable interfaces for IPsec access.

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

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

+ Add Edit Delete

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

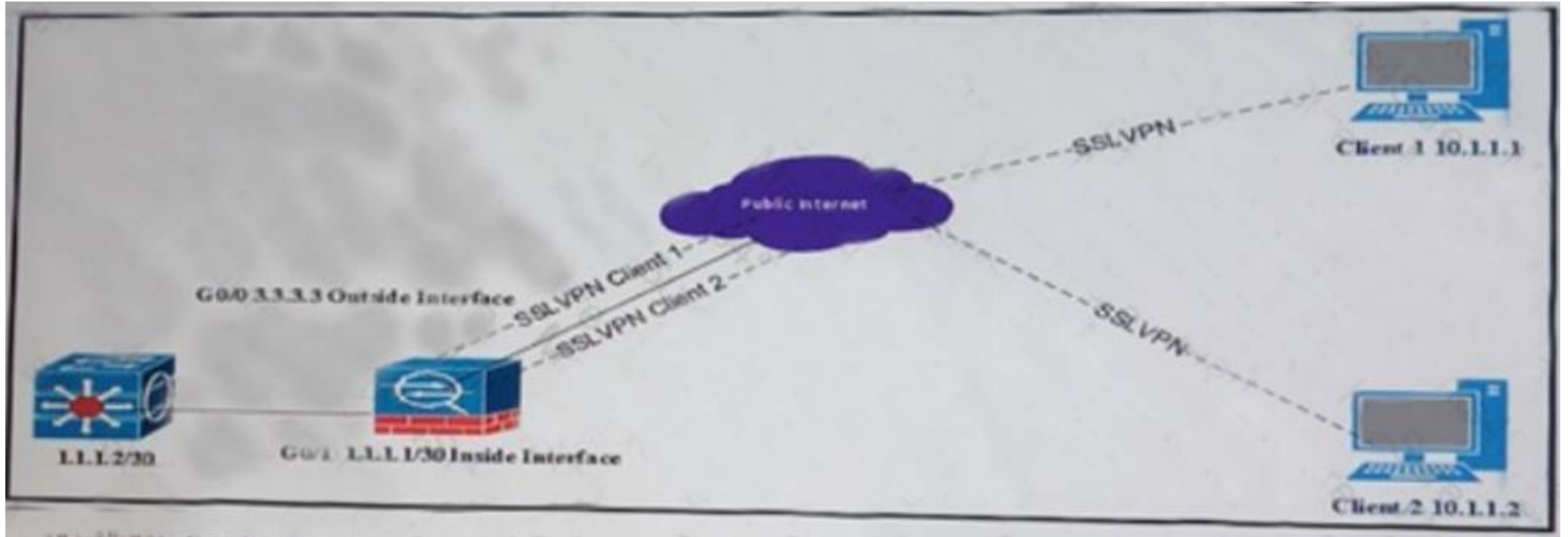
E. AES256

**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 8

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 9

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 10

Which two statements describe effects of the DoNothing option within the untrusted network policy on a Cisco AnyConnect profile? (Choose two.)

- A. The client initiates a VPN connection upon detection of an untrusted network.
- B. The client initiates a VPN connection upon detection of a trusted network.
- C. The always-on feature is enabled.
- D. The always-on feature is disabled.
- E. The client does not automatically initiate any VPN connection.

**Answer:** AD

#### NEW QUESTION 10

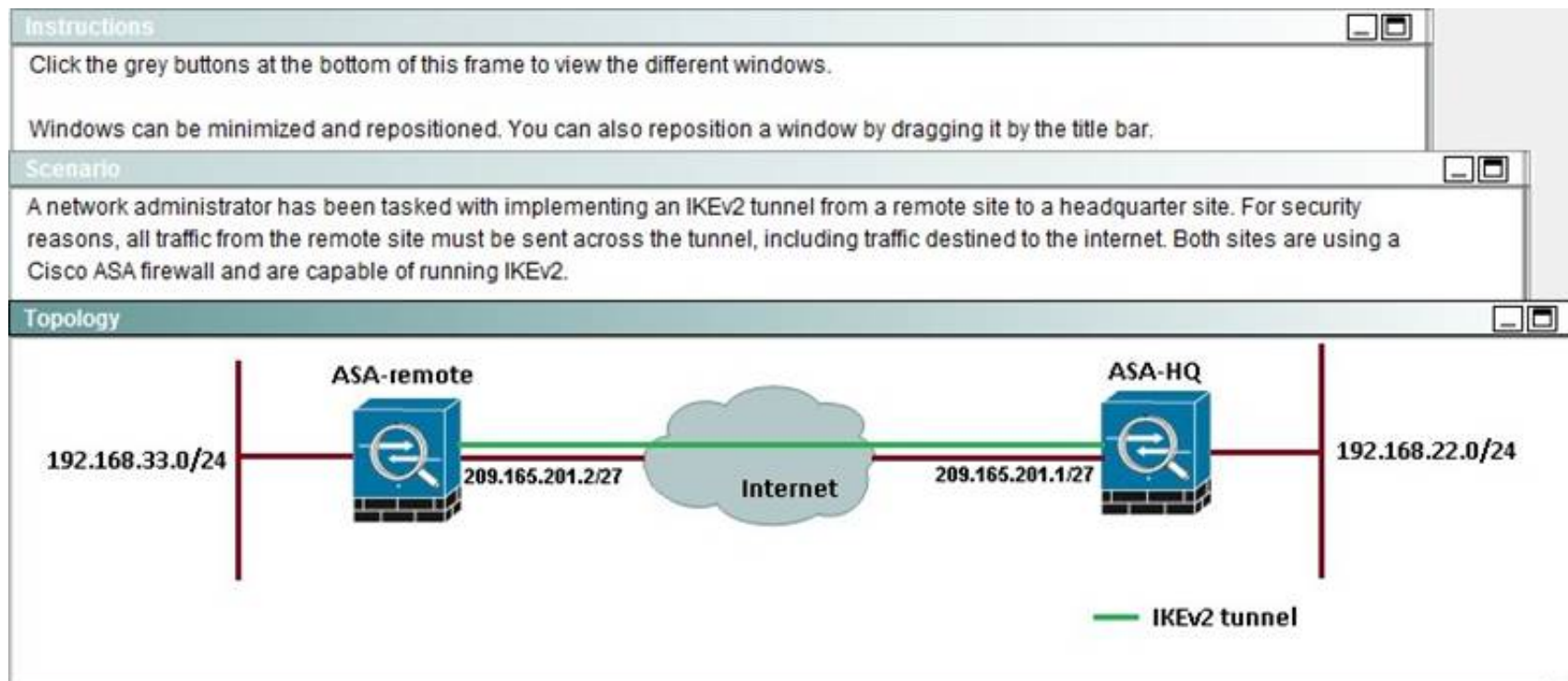
What is the Cisco recommended TCP maximum segment on a DMVPN tunnel interface when the MTU is set to 1400 bytes?

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

**Answer:** C

#### NEW QUESTION 11





**ASDM-HQ**

File View Tools Wizards Window Help Look For:

Home Configuration Monitoring Save Refresh Back Forward Help

**Site-to-Site VPN**

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces  
Enable interfaces for IPsec access.

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

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

+ Add Edit Delete

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

**ASDM-Remote**

File View Tools Wizards Window Help Look For:

Home Configuration Monitoring Save Refresh Back Forward Help

**Site-to-Site VPN**

Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces  
Enable interfaces for IPsec access.

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

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

+ Add Edit Delete

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

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

- A. Change the Diffie-Hellman group on the headquarter ASA to group5forthe dynamic crypto map
- B. Change the remote traffic selector on the remote ASA to 192.168.22.0/24
- C. Change to an IKEv1 configuration since IKEv2 does not support a full tunnel with static peers

- D. Change the local traffic selector on the headquarter ASA to 0.0.0.0/0
- E. Change the remote traffic selector on the headquarter ASA to 0.0.0.0/0

**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 to 192.168.22.0/24.

#### NEW QUESTION 14

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 15

A customer has two ASAs configured in high availability and is experiencing connection drops that require re-establishment each time failover occurs. Which type of failover has been implemented?

- A. Stateless
- B. routed
- C. trans parent
- D. stateful

**Answer:** D

#### NEW QUESTION 20

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 24

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 27

An engineer is using DMVPN to provide secure connectivity between a data center and remote sites. Which two routing protocols are recommended for use between the routers? (Choose two.)

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

**Answer:** AE

#### NEW QUESTION 32

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 34

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 35

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 36

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

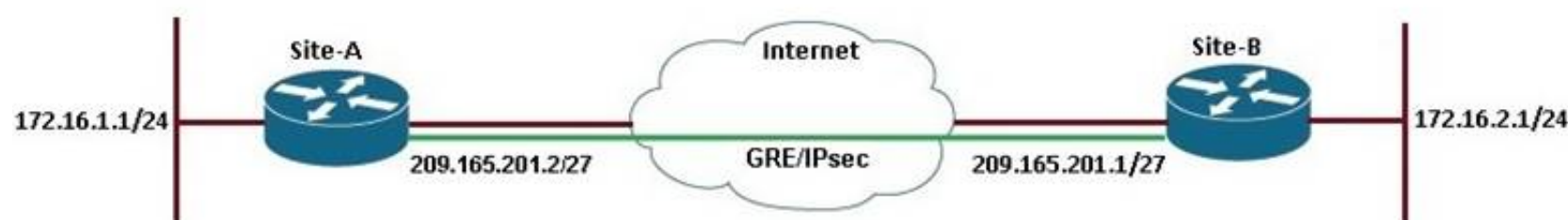
#### NEW QUESTION 40

##### 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 41

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

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

**Answer:** BE

#### NEW QUESTION 42

After completing a site-to-site VPN setup between two routers, application performance over the tunnel is slow. You issue the show crypto ipsec sa command and see the following output. What does this output suggest?

```
interfacE. Tunnel100
Crypto map tag: Tunnel100-head-0, local addr 10.10.10.10 protected vrF. (none)
local ident (addr/mask/prot/port): (10.10.10.10/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (10.20.20.20/255.255.255.255/47/0) current_peer
209.165.200.230 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34836, #pkts encrypt: 34836, #pkts digest: 34836
#pkts decaps: 26922, #pkts decrypt: 19211, #pkts verify: 19211
#pkts compressD. 0, #pkts decompressD. 0
#pkts not compressD. 0, #pkts compr. failedD. 0
#pkts not decompressD. 0, #pkts decompress failedD. 0
#send errors 0, #recv errors 0
```

- A. The VPN has established and is functioning normally.
- B. There is an asymmetric routing issue.
- C. The remote peer is not receiving encrypted traffic.



- D. The remote peer is not able to decrypt traffic.
- E. Packet corruption is occurring on the path between the two peers.

**Answer:** E

#### NEW QUESTION 46

A company has acquired a competitor whose network infrastructure uses only IPv6. An engineer must configure VPN access sourced from the new company. Which remote access VPN solution must be used?

- A. GET VPN
- B. Any Connect
- C. EzVPN
- D. DMVPN

**Answer:** C

#### NEW QUESTION 48

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 52

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

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0 1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE. Processing of Main Mode failed with peer at 10.10.10.10
```

- A. Phase 1 policy does not match on both sides.
- B. The transform set does not match on both sides.
- C. ISAKMP is not enabled on the remote peer.
- D. There is a mismatch in the ACL that identifies interesting traffic.

**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 60

An engineer wants to ensure that Diffie-Helman keys are re-generated upon a phase-2 rekey. What option can be configured to allow this?

- A. Aggressive mode
- B. Dead-peer detection
- C. Main mode
- D. Perfect-forward secrecy

**Answer:** D

#### NEW QUESTION 65

ACisco router may have a fan issue that could increase its temperature and trigger a failure. What troubleshooting steps would verify the issue without causing additional risks?

- A. Configure logging using commands "logging on", "logging buffered 4", and check for fan failure logs using "show logging"
- B. Configure logging using commands "logging on", "logging buffered 6", and check for fan failure logs using "show logging"
- C. Configure logging using commands "logging on", "logging discriminator msglog1 console 7", and check for fan failure logs using "show logging"
- D. Configure logging using commands "logging host 10.11.10.11", "logging trap 2", and check for fan failure logs at the syslog server 10.11.10.11

**Answer:** A

#### NEW QUESTION 66

Which statement is true when implementing a router with a dynamic public IP address in a crypto map based site-to-site VPN?

- A. The router must be configured with a dynamic crypto map.

- B. Certificates are always used for phase 1 authentication.
- C. The tunnel establishment will fail if the router is configured as a responder only.
- D. The router and the peer router must have NAT traversal enabled.

**Answer:** C

#### NEW QUESTION 69

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 70

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 72

Refer to the exhibit.

Tunnel-id	Local	Remote	fvr/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				

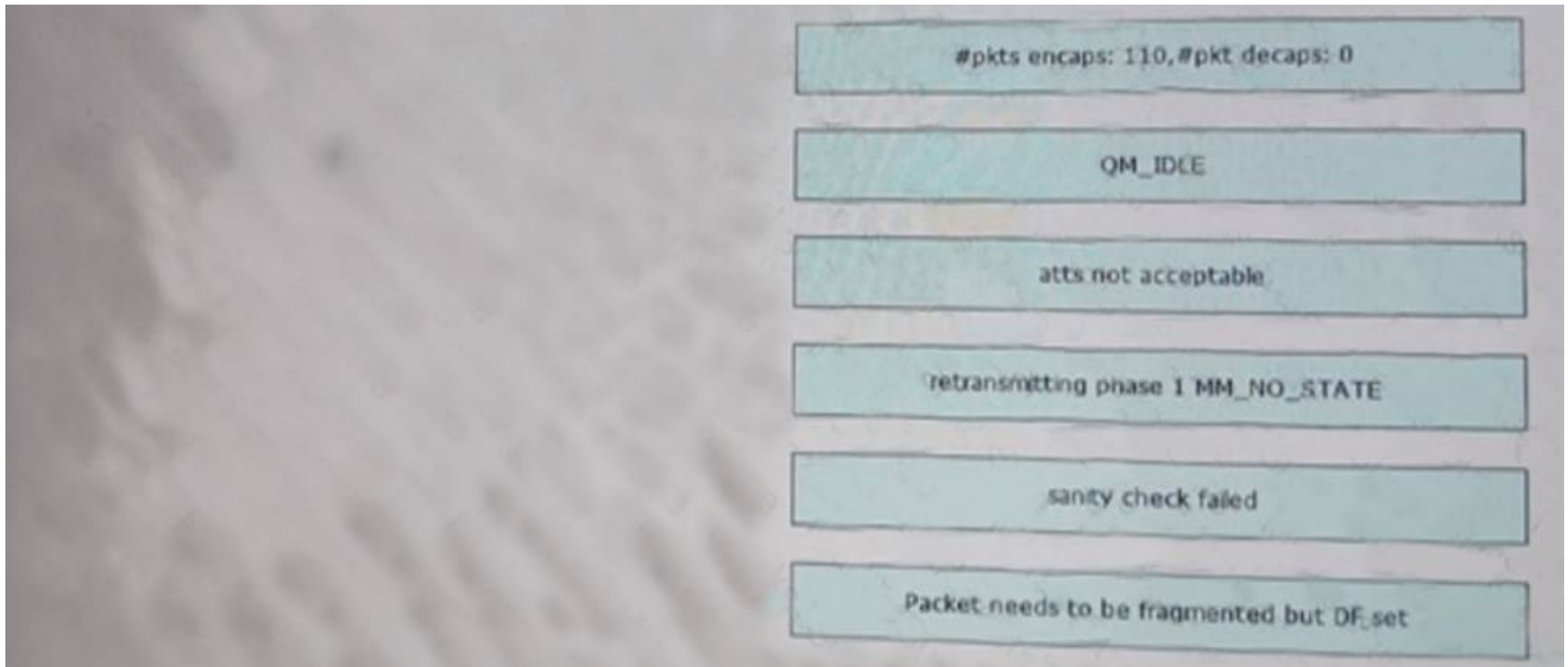
Which authentication method was used by the remote peer to prove its identity?

- A. Extensible Authentication Protocol
- B. certificate authentication
- C. pre-shared key
- D. XAUTH

**Answer:** C

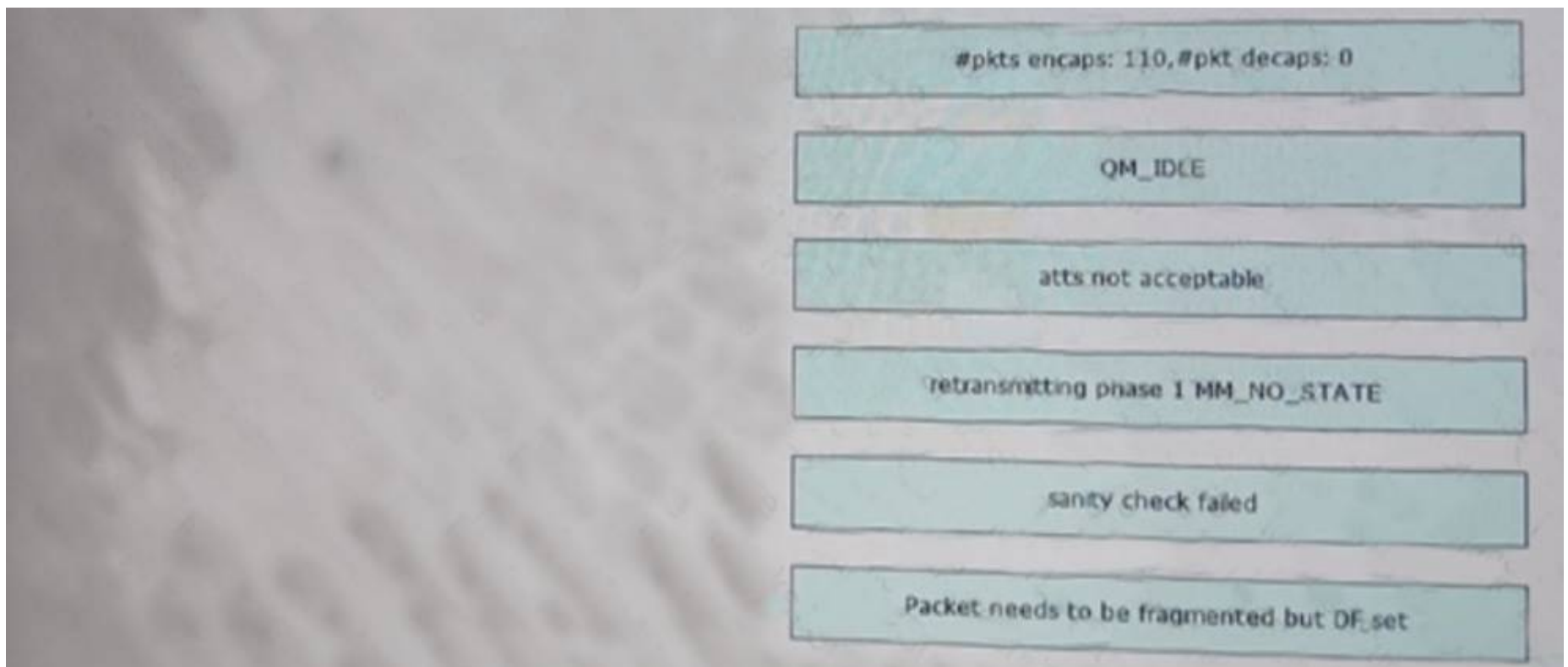
#### NEW QUESTION 73

Drag and drop the debug messages on the left onto the associated function during trouble shooting on the right.



**Answer:**

**Explanation:**



#### NEW QUESTION 75

Instructions

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

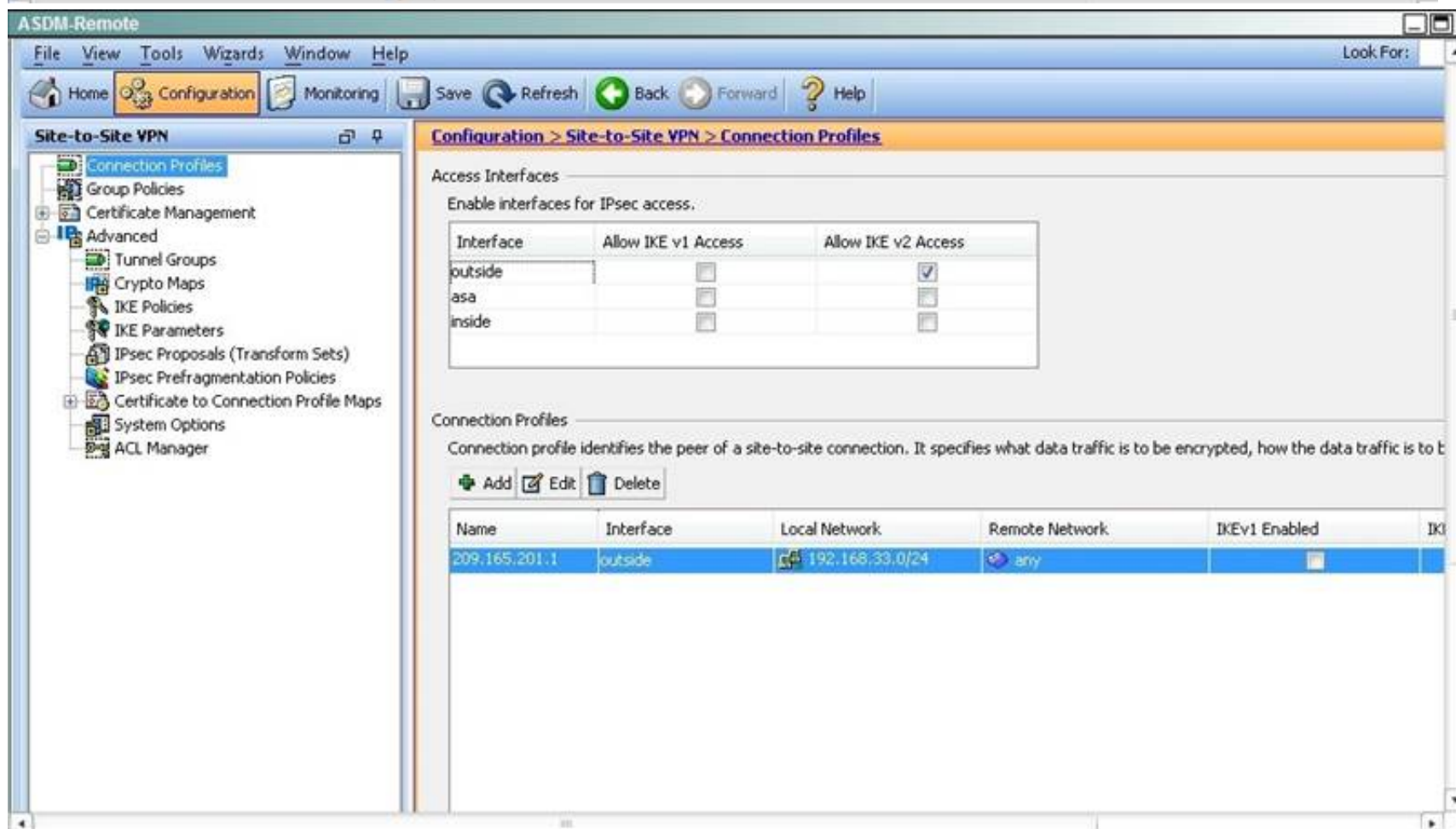
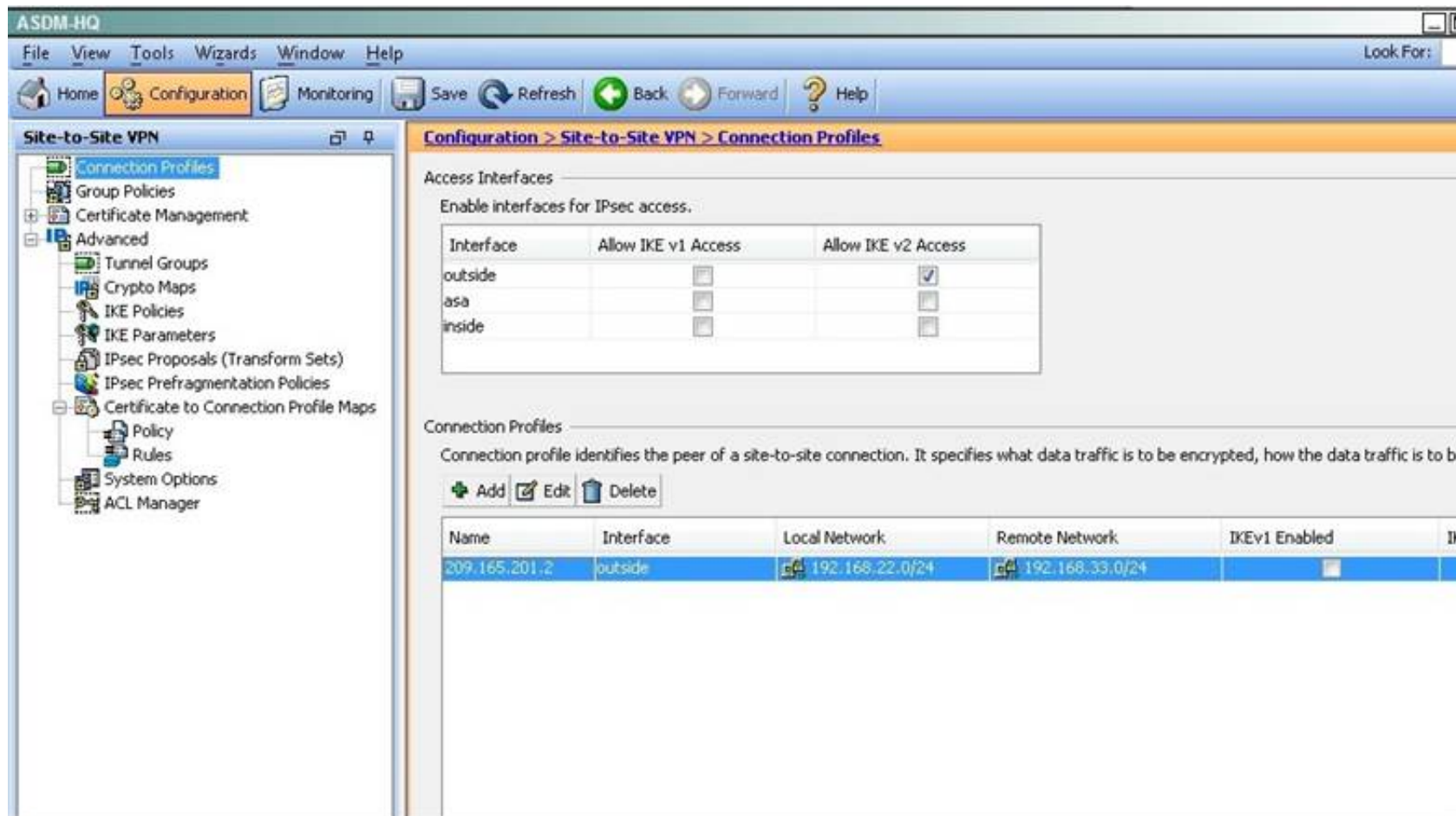
Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

Scenario

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

Topology





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

- A. An access-list must be configured on the outside interface to permit inbound VPN traffic
- B. A route to 192.168.22.0/24 will not be automatically installed in the routing table
- C. The ASA will use a window of 128 packets (64x2) to perform the anti-replay check
- D. The tunnel can also be established on TCP port 10000

**Answer: C**

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

#### NEW QUESTION 79

A network administrator has deployed Cisco, AnyConnect Secure Mobility Client to each member of the sales force. Which option is the verification method for this deployment?

- A. RADIUS server
- B. AM authentication
- C. NI domain
- D. RSA SDI

**Answer: A**

#### NEW QUESTION 84

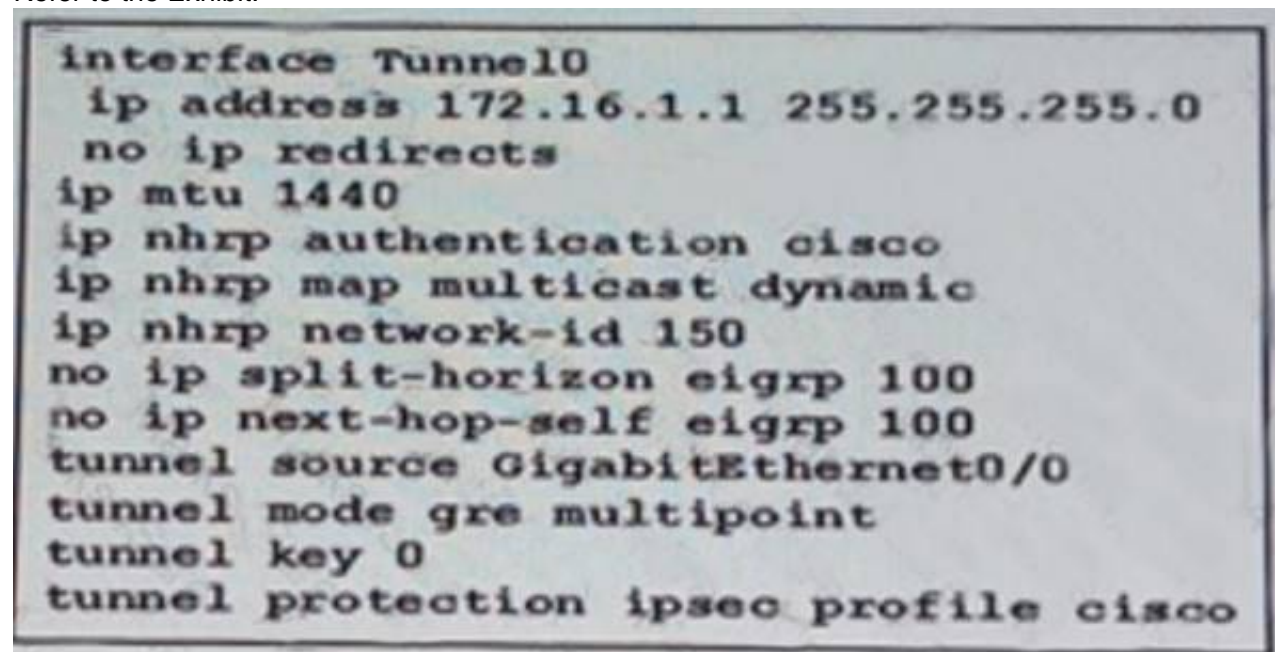
When an IPsec SVTI is configured, which technology processes traffic forwarding for encryption?

- A. ACL
- B. IP routing
- C. RRI
- D. front door VPN routing and forwarding

**Answer:** B

#### NEW QUESTION 89

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 90

A private wan connection is suspected of intermittently corrupting data. Which technology can a network administrator use to detect and drop the altered data traffic?

- A. AES-128
- B. RSACertificates
- C. SHA2-HMAC
- D. 3DES
- E. Diffie-Helman Key Generation

**Answer:** C

#### NEW QUESTION 91

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

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

**Answer:** A

#### NEW QUESTION 94

Which of the following could be used to configure remote access VPN Host-scan and pre-login policies?

- A. ASDM
- B. Connection-profile CLI command
- C. Host-scan CLI command under the VPN group policy
- D. Pre-login-check CLI command

**Answer:** A

#### NEW QUESTION 97

You are configuring a Cisco IOS SSL VPN gateway to operate with DVTI support. Which command must you configure on the virtual template?

- A. tunnel protection ipsec

- B. ip virtual-reassembly
- C. tunnel mode ipsec
- D. ip unnumbered

**Answer:** D

#### NEW QUESTION 100

Which command configures IKEv2 symmetric identity authentication?

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

**Answer:** C

#### NEW QUESTION 104

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 109

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 114

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 119



An engineer is assisting in the continued implementation of a VPN solution and discovers an NHRP server configuration. Which type of VPN solution has been implemented?

- A. DM VPN
- B. IPsec VPN
- C. SSL VPN
- D. GET VPN

**Answer:** A

#### NEW QUESTION 123

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 125

Which two GDOI encryption keys are used within a GET VPN network? (Choose two.)

- A. key encryption key
- B. group encryption key
- C. user encryption key
- D. traffic encryption key

**Answer:** AD

#### NEW QUESTION 126

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 130

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 132

Refer to the exhibit.

```
crypto pki certificate map CERTMAP
subject-name co cn=cisco.com
crypto ikev2 profile IKEPROFILE
authentication local pre-share
authentication remote rsa-sig
keyring local KEYRING1
match identity remote address 209.165.200.225 255.255.255.255
match identity remote address 209.165.202.155 255.255.255.255
match certificate CERTMAP
pki trustpoint TRUSTPOINT1
```

After the configuration is performed, which combination of devices can connect?

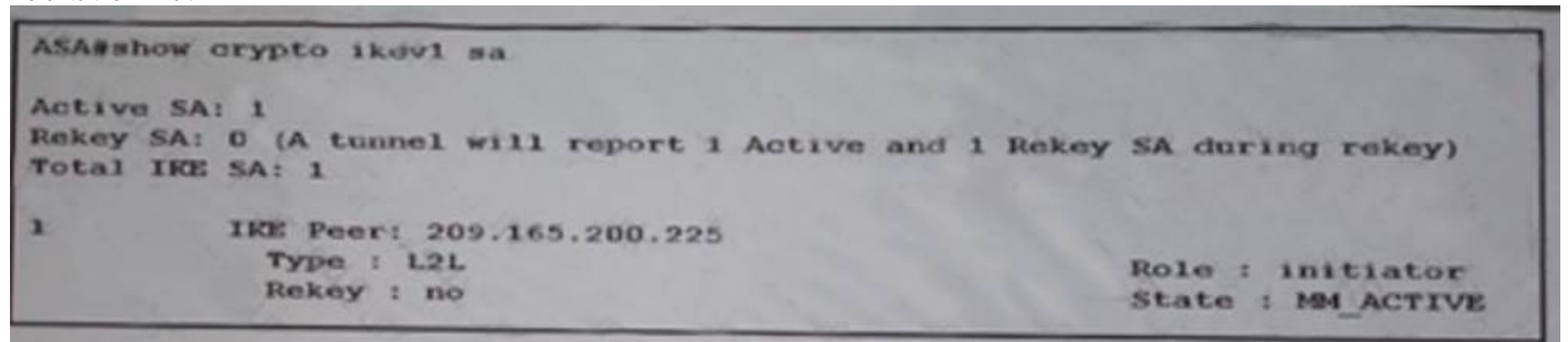
- A. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name of "cisco.com"

- B. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 or a certificate with subject name containing "cisco.com"
- C. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 and a certificate with subject name containing "cisco.com"
- D. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name containing "cisco.com"

**Answer:** D

#### NEW QUESTION 133

Refer to the Exhibit:



Users at each end of this VPN tunnel cannot communicate with each other. Which cause of this behavior is true?

- A. The Diffie-Hellman groups configured are different
- B. The pre shared key does not match.
- C. Phase 1 is not completed and troubleshooting is required.
- D. The issue occurs in phase 2 of the tunnel.

**Answer:** C

#### NEW QUESTION 136

Which two IKEv1 policy options must match on each peer when you configure an IPsec site-to-site VPN? (Choose two.)

- A. priority number
- B. hash algorithm
- C. encryption algorithm
- D. session lifetime
- E. PRF algorithm

**Answer:** BC

#### NEW QUESTION 139

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 140

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 141

Which hash algorithm is required to protect classified information?

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

**Answer:** D

#### NEW QUESTION 146

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 147

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

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

**Answer:** AB

#### NEW QUESTION 148

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 152

Refer to the Exhibit:



```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
Dst          src          state      conn-id    slot    status
10.10.10.1    172.16.1.1    MM_NO_STATE  0          0      ACTIVE
10.10.10.1    172.16.1.1    MM_NO_STATE  0          0      ACTIVE (deleted)
172.17.0.5    172.16.1.1    MM_NO_STATE  0          0      ACTIVE
172.17.0.5    172.16.1.1    MM_NO_STATE  0          0      ACTIVE (deleted)

Router#debug crypto isakmp

01:12:45.250: ISAKMP:(0):Old State = IKE_READY
                  New State = IKE_I_MM1
01:12:45.250: ISAKMP:(0): beginning Main Mode exchange
01:12:45.250: ISAKMP:(0): sending packet to 10.10.10.1
                  my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:45.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:12:55.250: ISAKMP (0:0): incrementing error counter on sa,
                  attempt 1 of 5: retransmit phase 1
01:12:55.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
01:12:55.250: ISAKMP:(0): sending packet to 10.10.10.1
                  my_port 500 peer_port 500 (I) MM_NO_STATE
01:12:55.250: ISAKMP:(0):Sending an IKE IPv4 Packet.
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
01:13:04.250: ISAKMP (0:0): incrementing error counter on sa,
                  attempt 2 of 5: retransmit phase 1
01:13:04.250: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

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 155

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

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

Answer: AC

#### NEW QUESTION 158

Which command does a network engineer type on both spoke routers to check for unidirectional traffic within the VPN tunnel?

- A. Show eigrp neighbors
- B. Show crypto ipsec summary
- C. Show crypto isakmp sa detail
- D. Show crypto ipsec sa peer <ip-address>

Answer: C

#### NEW QUESTION 162

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 166

A company has decided to migrate an existing IKEv1 VPN tunnel to IKEv2. Which two are valid configuration constructs on a Cisco IOS router? (Choose two.)

- A. crypto ikev2 keyring keyring-name peer peer1address 209.165.201.1 255.255.255.255pre-shared-key local key1 pre-shared-key remote key2
- B. crypto ikev2 transform-set transform-set-name esp-3des esp-md5-hmac esp-aes esp-sha-hmac
- C. crypto ikev2 map crypto-map-nameset crypto ikev2 tunnel-group tunnel-group-name set crypto ikev2 transform-set transform-set-name
- D. crypto ikev2 tunnel-group tunnel-group-name match identity remote address 209.165.201.1 authentication local pre-shareauthentication remote pre-share

E. crypto ikev2 profile profile-namematch identity remote address 209.165.201.1 authentication local pre-shareauthentication remote pre-share

**Answer:** AE

#### NEW QUESTION 170

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 174

**Instructions**

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

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

**Scenario**

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

**Topology**

**ASDM-HQ**

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

**Site-to-Site VPN**

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

**Configuration > Site-to-Site VPN > Connection Profiles**

Access Interfaces

Enable interfaces for IPsec access.

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

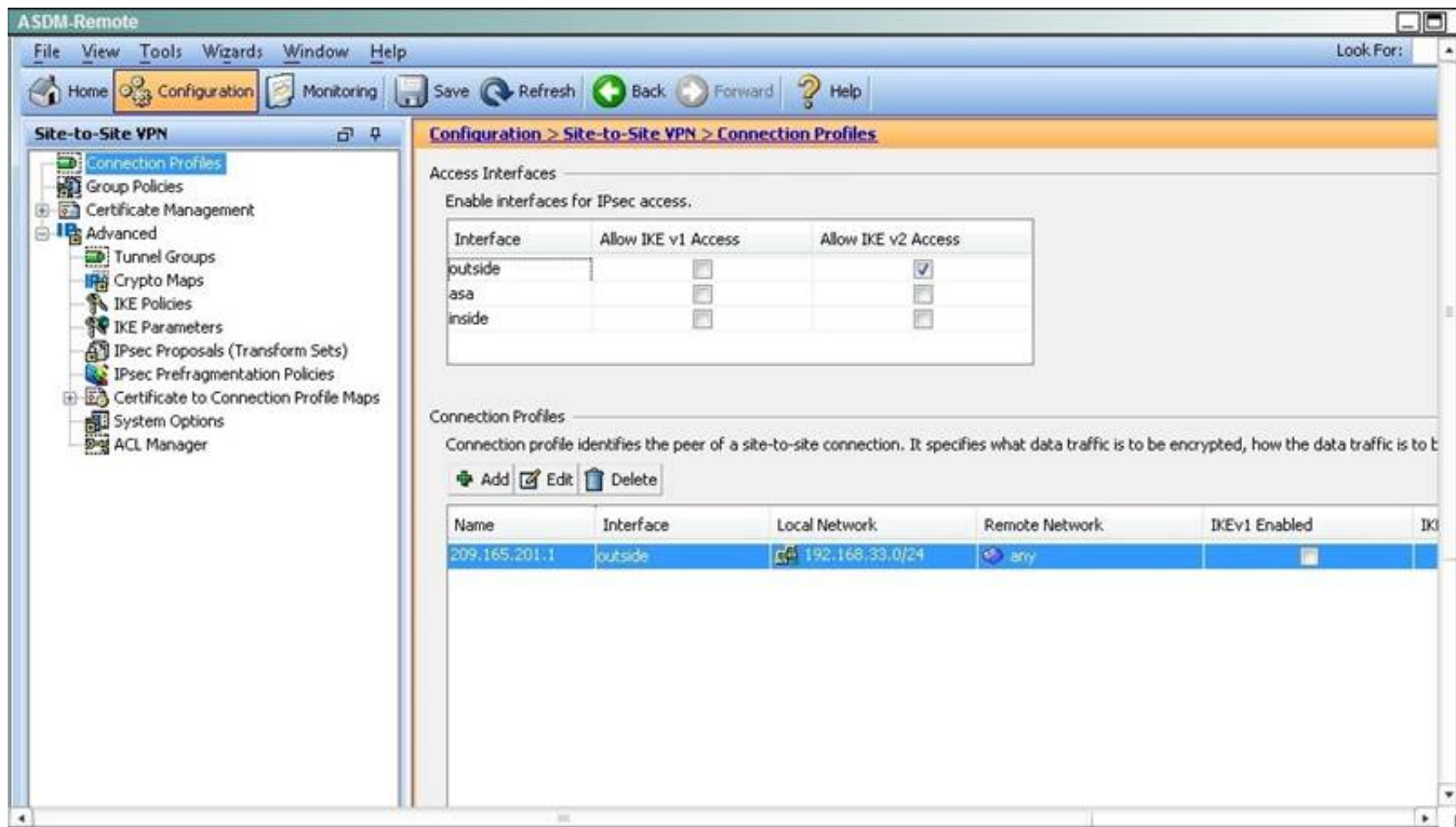
Connection Profiles

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

[Add](#) [Edit](#) [Delete](#)

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



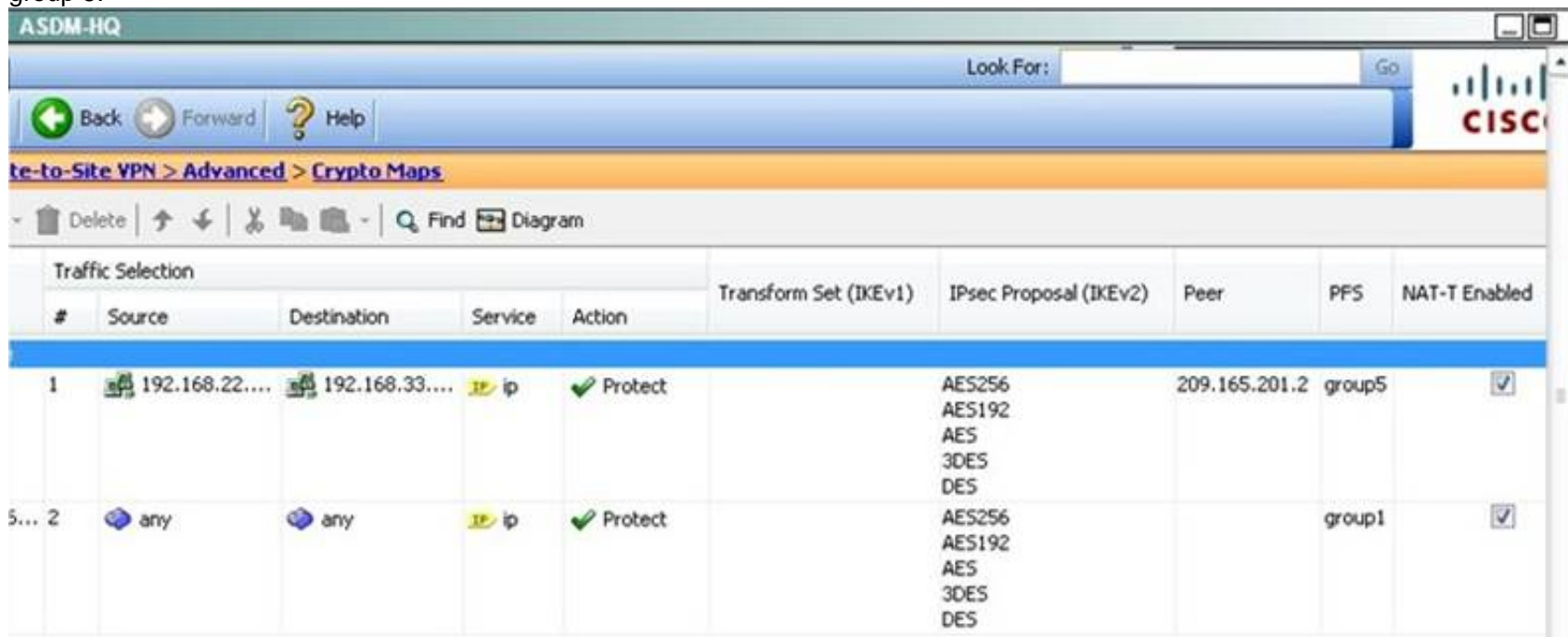


When a tunnel is initiated by the headquarter ASA, which one of the following Diffie-Hellman groups is selected by the headquarter ASA during CREATE\_CHILD\_SA exchange?

- A. 1
- B. 2
- C. 5
- D. 14
- E. 19

**Answer: C**

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



#### NEW QUESTION 175

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 178

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 182

When Cisco ASA applies VPN permissions, what is the first set of attributes that it applies?

- A. dynamic access policy attributes
- B. group policy attributes
- C. connection profile attributes
- D. user attributes

**Answer:** A

#### NEW QUESTION 183

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

- A. access-list splitlist standard permit 209.165.201.0 255.255.255.224 access-list splitlist standard permit 209.165.202.128 255.255.255.224!group-policy GroupPolicy1 internal group-policy GroupPolicy1 attributes split-tunnel-policy tunnelspecifiedsplit-tunnel-network-list value splitlist
- B. access-list splitlist standard permit 209.165.201.0 255.255.255.224 access-list splitlist standard permit 209.165.202.128 255.255.255.224!group-policy GroupPolicy1 internal group-policy GroupPolicy1 attributes split-tunnel-policy tunnelallsplit-tunnel-network-list value splitlist
- C. group-policy GroupPolicy1 internal group-policy GroupPolicy1 attributes split-tunnel-policy tunnelspecifiedsplit-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224split-tunnel-network-list ipv4 2 209.165.202.128 255.255.255.224
- D. access-list splitlist standard permit 209.165.201.0 255.255.255.224 access-list splitlist standard permit 209.165.202.128 255.255.255.224!crypto anyconnect vpn-tunnel-policy tunnelspecified crypto anyconnect vpn-tunnel-network-list splitlist
- E. crypto anyconnect vpn-tunnel-policy tunnelspecifiedcrypto anyconnect split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224crypto anyconnect split-tunnel-network-list ipv4 2 209.165.202.128 255.255.255.224

**Answer:** A

#### NEW QUESTION 188

Refer to the exhibit:

```
ASA#show crypto ikev1 sa

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: 209.165.200.225
      Type : L2L
      Rekey : no
      Role : initiator
      State : MM_WAIT_MSG_6
```

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 191

Refer to the exhibit.

#### Config for Router1

```
crypto ikev2 keyring KR1
 peer Router2
  address 209.165.201.15
  pre-shared-key local apples
  pre-shared-key remote Oranges
```

#### Config for Router2

```
crypto ikev2 keyring KR1
 peer Router1
  address 209.165.202.0 255.255.255.0
  pre-shared-key local apples
  pre-shared-key remote Oranges
```



The IKEv2 tunnel between Router1 and Router2 is failing during session establishment. Which action will allow the session to establish correctly?

- A. The address command on Router2 must be narrowed down to a /32 mask.
- B. The local and remote keys on Router2 must be switched.
- C. The pre-shared key must be altered to use only lowercase letters.
- D. The local and remote keys on Router2 must be the same.

**Answer: B**

#### NEW QUESTION 193

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 198

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 203

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 204

Which access lists are used in a typical IPsec VPN configuration?

- A. ACL to NAT traffic across the VPN tunnel
- B. ACL to define policy based routing

- C. ACL to define what traffic to exempt from NAT
- D. ACL for routing neighbors across the tunnel

**Answer:** C

**NEW QUESTION 207**

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 210**

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

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

**Answer:** C

**NEW QUESTION 212**

ACisco IOS SSL VPN gateway is configured to operate in clientless mode so that users can access file shares on a Microsoft Windows 2003 server. Which protocol is used between the Cisco IOS router and the Windows server?

- A. HTTPS
- B. NetBIOS
- C. CIFS
- D. HTTP

**Answer:** C

**NEW QUESTION 213**

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 217**

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

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

**Answer:** A

**NEW QUESTION 218**

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 222**

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 225

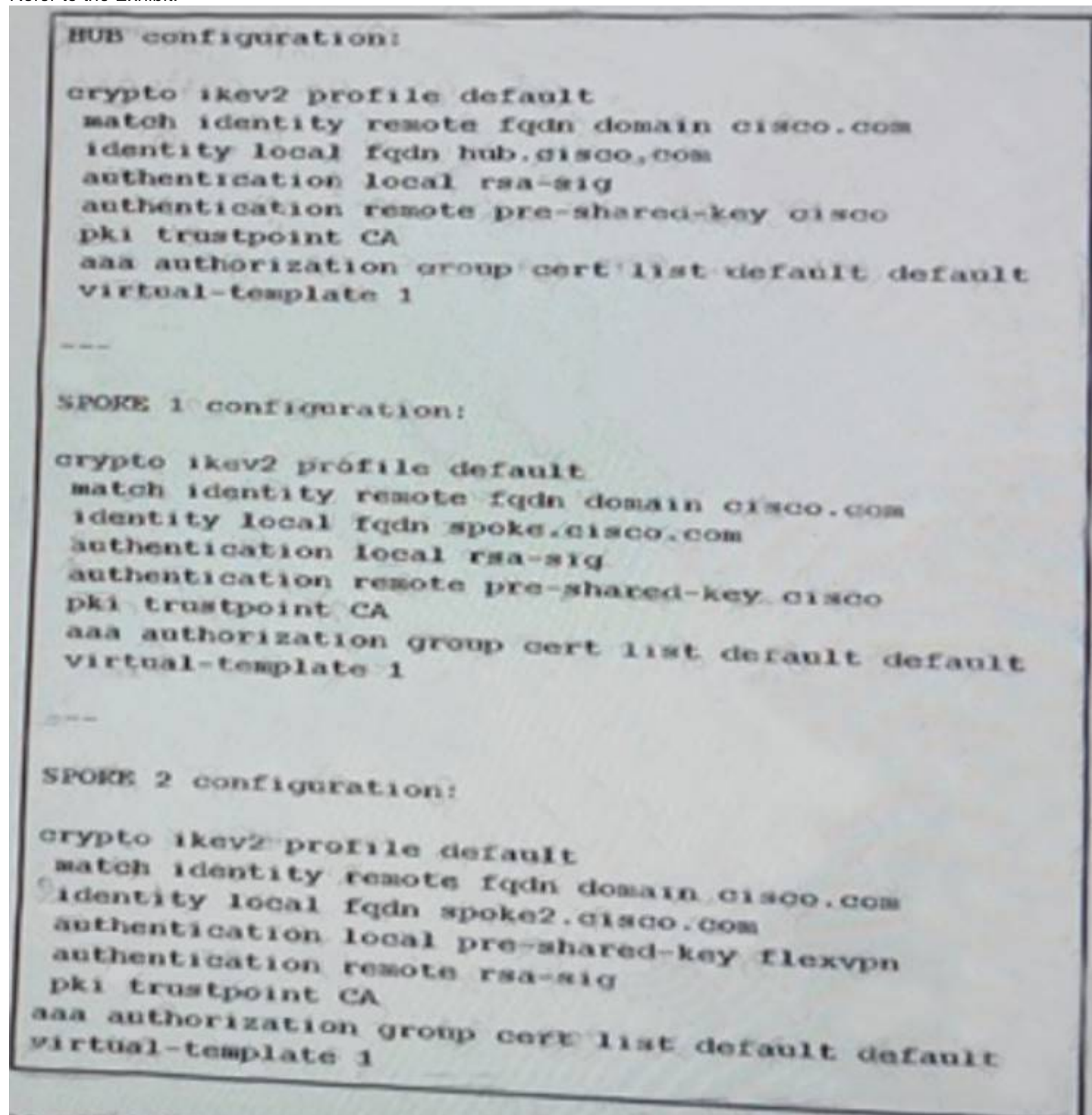
Which two option, are benefits of AES compared to 3DES? (Choose two.)

- A. switches encryption keys every 32 GB of data transfer
- B. faster encryption
- C. shorter encryption keys
- D. longer encryption block length
- E. repeating encryption keys

**Answer:** BD

#### NEW QUESTION 230

Refer to the Exhibit:



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 234

Which Cisco ASDM option configures forwarding syslog messages to email?

- A. Configuration > Device Management > Logging > E-Mail Setup
- B. Configuration > Device Management > E-Mail Setup > Logging Enable
- C. Select the syslogs to email, click Edit, and select the Forward Messages option.
- D. Select the syslogs to email, click Settings, and specify the Destination Email Address option.

**Answer:** A

#### NEW QUESTION 235

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 240

In FlexVPN, what command can an administrator use to create a virtual template interface that can be configured and applied dynamically to create virtual access interfaces?

- A. interface virtual-template number type template
- B. interface virtual-template number type tunnel
- C. interface template number type virtual
- D. interface tunnel-template number

**Answer:** B

**Explanation:** Here is a reference an explanation that can be included with this test.

[http://www.cisco.com/en/US/docs/ios-xml/ios/sec\\_conn\\_ike2vpn/configuration/15-2mt/sec-flex-spoke.html#GU](http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex-spoke.html#GU)

Configuring the Virtual Tunnel Interface on FlexVPN Spoke SUMMARY STEPS

1. enable
2. configure terminal
3. interface virtual-template number type tunnel
4. ip unnumbered tunnel number
5. ip nhrp network-id number
6. ip nhrp shortcut virtual-template-number
7. ip nhrp redirect [timeout seconds]
8. exit

#### NEW QUESTION 241

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

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

**Answer:** ABC

#### NEW QUESTION 246

Which is used by GETVPN, FlexVPN and DMVPN?

- A. NHRP
- B. MPLS
- C. GRE
- D. ESP

**Answer:** D

#### NEW QUESTION 251

Scenario

You are the network security administrator for your organization. Your company is growing and a remote branch office is being created. You are tasked with configuring your headquarters Cisco ASA to create a site-to-site IPsec VPN connection to the branch office Cisco ISR. The branch office ISR has already been deployed and configured and you need to complete the IPsec connectivity configurations on the HQ ASA to bring the new office online.

Use the following parameters to complete your configuration using ASDM. For this exercise, not all ASDM screens are active.

? Enable IKEv1 on outside I/F for Site-to-site VPN

? Add a Connection Profile with the following parameters:

? Peer IP: 203.0.113.1

? Connection name: 203.0.113.1

? Local protected network: 10.10.9.0/24

? Remote protected network: 10.11.11.0/24

? Group Policy Name: use the default policy name supplied

? Preshared key: cisco

? Disable IKEv2

? Encryption Algorithms: use the ASA defaults

? Disable pre-configured NAT for testing of the IPsec tunnel

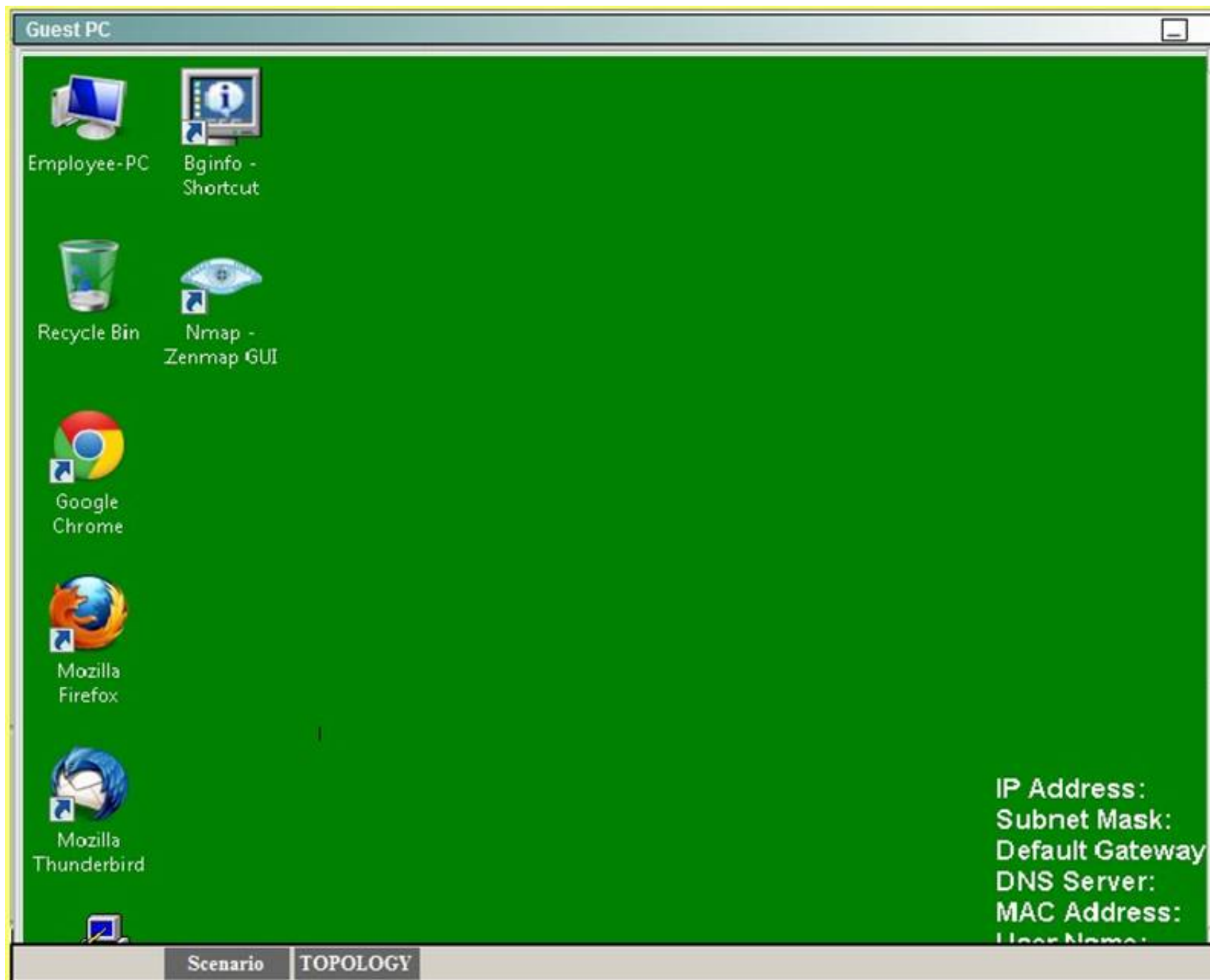
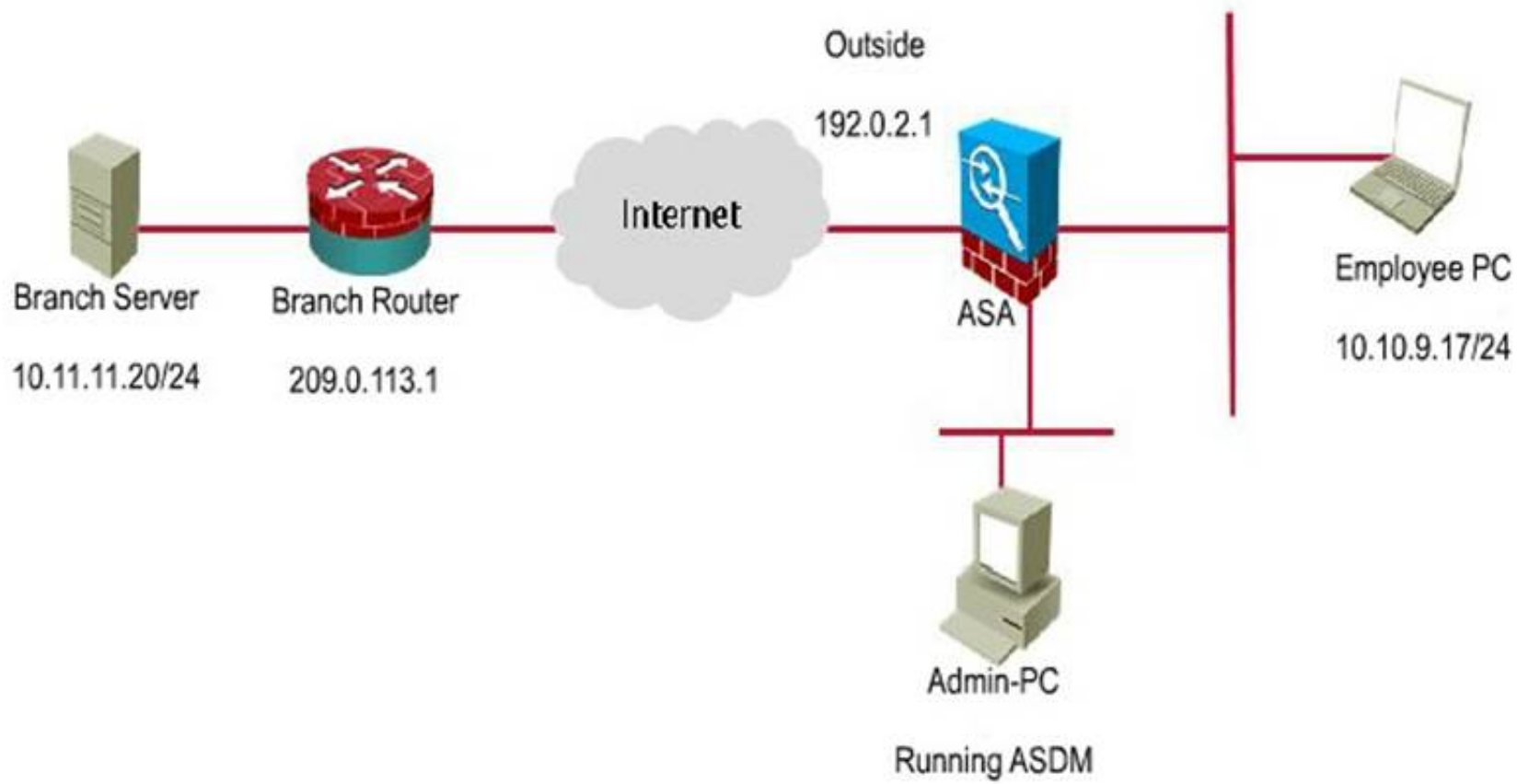
? Disable the outside NAT pool rule

? Establish the IPsec tunnel by sending ICMP pings from the Employee PC to the Branch Server at IP address 10.11.11.20

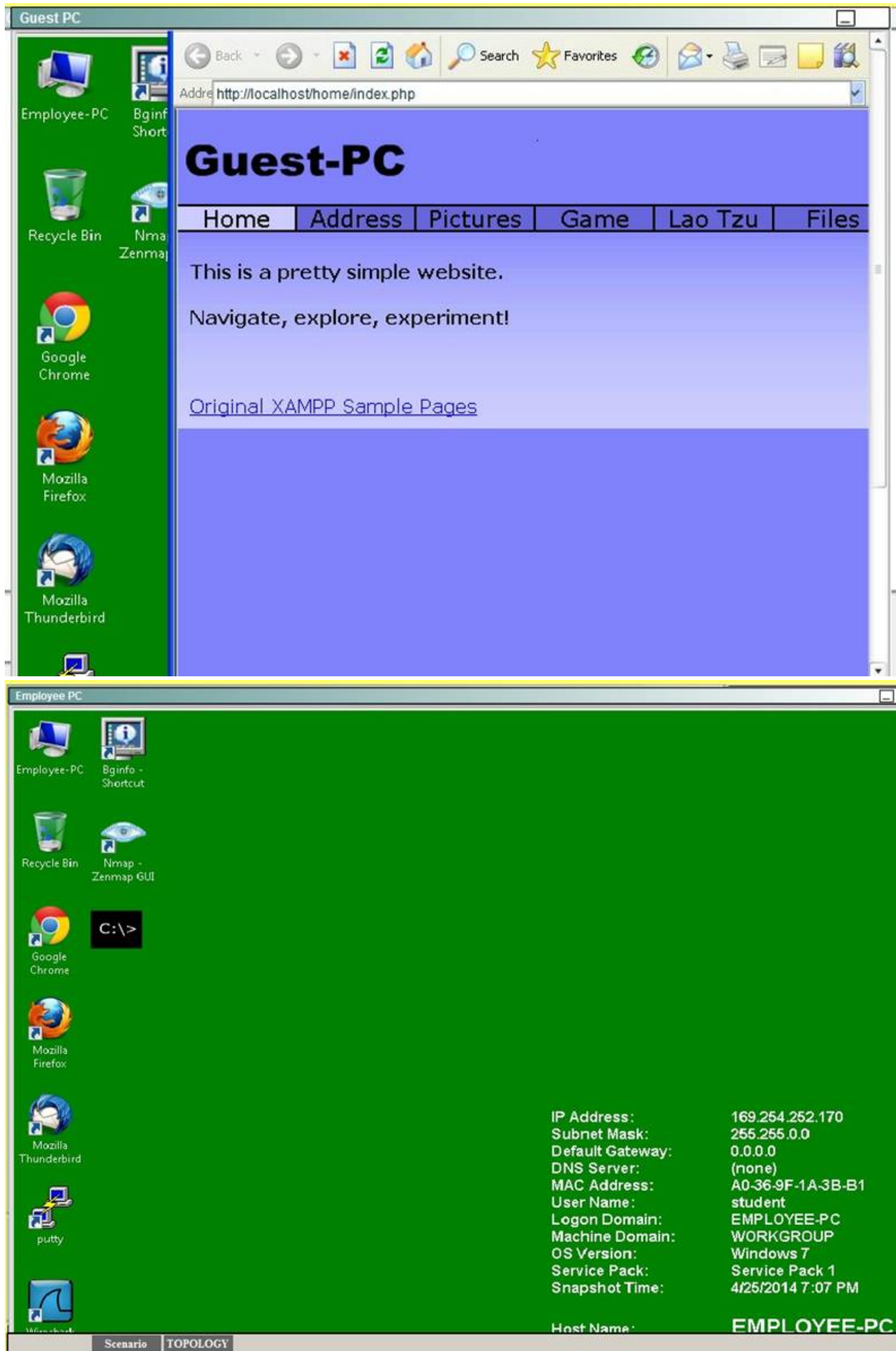
? Verify tunnel establishment in ASDM VPN Statistics> Sessions window pane

You have completed this exercise when you have successfully configured, established, and verified site-to-site IPsec connectivity between the ASA and the

Branch ISR.  
Topology







Employee-PC

Press RETURN to get started!

Cisco ASDM 7.1 for ASA - 10.10.2.1

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**

ASA Version: **9.1(1)4** Device Uptime: **0d 0h 28m 16s**

ASDM Version: **7.1(2)** Device Type: **ASA 5515, IPS**

Firewall Mode: **Routed** Context Mode: **Single**

Environment Status: OK 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	4
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](#)

Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

Memory Usage (MB)
4000
3500
3000
2500
2000
733MB

Traffic Status

Connections Per Second Usage

Legend: UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination	Description
6	May 09 2014	16:37:47	302016	64.103.34.15	123	10.10.3.20	123	Teardown UDP connection 527 for outside:64.103.34.15/123 to inside:10.10.3.20/123 duration
6	May 09 2014	16:37:24	302021	10.10.2.40	10246	10.10.1.1	0	Teardown ICMP connection for faddr 10.10.2.40/10246 gaddr 10.10.1.1/0 laddr 10.10.1.1/0
6	May 09 2014	16:37:24	302020	10.10.2.40	10246	10.10.1.1	0	Built inbound ICMP connection for faddr 10.10.2.40/10246 gaddr 10.10.1.1/0 laddr 10.10.1.1/0



Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help

CISCO

Home
Device Dashboard
Firewall Dashboard
Intrusion Prevention

### Traffic Overview

Last updated: 9:56:53 PM

Connection Statistics

Connections: 21 NAT Xlates: 12

Dropped Packets Rate

ACL Dropped: 0 Inspection Dropped: 0

Possible Scan and SYN Attack Rates

Scanning Attacks: 0 Syn Attacks: 0

The Top 200 Hosts feature is disabled in the Security Appliance. Please click the button to enable it.

Enable

### Top Botnet Traffic Filter Hits

Last updated: 9:56:13 PM

Top 10 Malware Sites Top 10 Malware Ports Top 10 Infected Hosts

Based on: Connections Logged Display: Pie Last cleared: Never

41.109.132.70 (3) 50%

144.76.98.92 (3) 50%

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help

CISCO

Botnet Traffic Filter
Statistics
Real-time Reports
Infected Hosts
Updater Client
DNS Snooping
Dynamic Database
ASP Table Hits

### Monitoring > Botnet Traffic Filter > Real-time Reports

Real-time Reports

Top Malware Sites

Save as PDF Clear Report Whois Last cleared: Never

IP Address	Malware Site	Connections Logged	Drop...	Threat Level
41.109.132.70	bot-sparta.no-ip.org	3	3	Very ...
144.76.98.92	superzarabotok-gid.ru	3	3	Very ...

Top Malware Ports

Save as PDF Clear Report Last cleared: Never

Malware Port	Connections Logged
tcp 80	

Refresh

Last Updated: 5/15/14 2:57:48 PM



Home

Configuration

Monitoring

Save

Refresh

Back

Forward

Help

Device List

Interfaces

ARP Table

DHCP

Dynamic ACLs

Interface Graphs

IPv6 Neighbor Discovery Cache

PPPoE Client

Interfaces

VPN

Botnet Traffic Filter

Routing

Properties

Logging

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	192.0.2.2	000c.3014.3720	No
inside	10.10.1.2	0006.f6c2.de47	No
DMZ	172.16.1.55	0050.5692.7b9f	No
DMZ	172.16.1.50	0050.5666.6666	No
Site-To-Site management	172.16.2.3	6c41.6af1.1438	No
	10.10.2.40	0050.5600.5555	No

Clear Dynamic ARP Entries

Refresh

Last Updated: 6/27/14 1:01:43 PM

Data Refreshed Successfully.

student

15

6/27/14 8:01:31 PM UTC

Home

Configuration

Monitoring

Save

Refresh

Back

Forward

Help

Device List

Logging

Real-Time Log Viewer

Log Buffer

Interfaces

VPN

Botnet Traffic Filter

Routing

Properties

Logging

Monitoring > Logging > Real-Time Log Viewer

Real-Time Log Viewer

Click the View button below to start displaying syslog messages in real time. Select the desired logging level to see messages at that severity or higher.

Logging Level:

Debugging

Buffer Limit:

1000

View...

Data Refreshed Successfully.

student

15

6/27/14 8:00:21 PM UTC

Real-Time Log Viewer - 10.10.2.1

File Tools Window Help

Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help

Filter By: Filter Build Filter Show All Find:

Severity	Date	Time	Syslog	SourceIP	SourcePort	DestinationIP	Destination	Description
6	Nov 3 2015	15:44:18	302017	208.90.57.75	443	10.10.1.50	62270	Teardown TCP conenction 81
6	Nov 3 2015	15:44:18	302017	10.10.2.40	0	10.10.1.1	0	Teardown TCP conenction for
6	Nov 3 2015	15:44:18	302017	10.10.2.40	0	10.10.1.1	0	Built inbound ICMP connection
6	Nov 3 2015	15:44:18	302017	10.10.9.50	62270	208.90.57.75	443	Built outbound TCP connectio
6	Nov 3 2015	15:44:18	302017	10.10.9.50	62270	208.90.57.75	443	Built outbound TCP connectio
6	Nov 3 2015	15:44:18	302017	10.10.9.50	62270	208.90.57.75	443	Built outbound TCP connectio
6	Nov 3 2015	15:44:18	302017	23.72.38.160	80	172.16.1.55	12730	Teardown TCP conenction 81
6	Nov 3 2015	15:44:18	302017	172.16.1.55	12730	23.72.38.160	80	Built outbound TCP connectio
6	Nov 3 2015	15:44:18	302017	10.10.2.40	0	10.10.1.1	0	Teardown ICMP connection fo
6	Nov 3 2015	15:44:18	302017	172.16.1.55	12730	23.72.38.160	80	Built outbound TCP connectio
6	Nov 3 2015	15:44:18	302017	10.10.2.40	0	10.10.1.1	0	Teardown ICMP connection fo
6	Nov 3 2015	15:44:18	302017	209.165.200.233	53	10.10.3.20	65394	Teardown UDP connection 81

Syslog Details

Severity: 4 (Warnings) Date: May 15 2014 Source IP: 10.10.9.17 Source Port: 1057  
 Syslog ID: 338006 Time: 21:49:30 Destination IP: 41.109.132.70 Destination Port: 80  
 Description: Dynamic Filter dropped blacklisted TCP traffic from inside:10.10.9.17/1057 (192.0.2.178/1057) to outside:41.109.132.70/80 (41.109.132.70/80), destination 41.109.132.70 resolved from dynamic list: bot-sparta.no-ip.org, threat-level: very-high,  
 Explanation Recommended Action Details

Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN Statistics Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN		0	8	2
Browser		0	8	2
Site-to-Site VPN		1	2	1
IKEv1 IPsec		1	2	1

Filter By: IPsec Site-to-Site -- All Sessions -- Filter

ConnectionProfileIPAddress	ProtocolEncryption	LoginTimeDuration	BytesTxBytesRx

Details Logout Ping

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions -- Logout Sessions Refresh



The screenshot displays the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The top navigation bar includes Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help. The left sidebar shows the Device List with categories like AAA Servers, Device Access, Connection Graphs, CRL, DNS Cache, Fallover, Status, Graphs, Identity, AD Agent, Groups, Memory, Interfaces, VPN, Botnet Traffic Filter, Routing, Properties, and Logging.

The main content area is titled "Monitoring > Properties > AAA Servers". It shows a table of AAA Servers with the following data:

Server Group	Protocol	IP Address	Status
LOCAL	Local database	None	Active

Below the table, there are statistics for the selected server:

- Server port: None
- Number of pending requests: 0
- Average round trip time: 0ms
- Number of authentication requests: 1
- Number of authorization requests: 0
- Number of accounting requests: 0
- Number of retransmissions: 0
- Number of accepts: 1
- Number of rejects: 0
- Number of challenges: 0

Buttons for "Clear Server Statistics", "Update Server Status...", and "Refresh" are present. The status bar at the bottom indicates "Data Refreshed", "Data Refreshed Successfully", "student", "15", and "6/27/14 8:07:31 PM UTC".

The second screenshot shows the "Configuration > Firewall > Botnet Traffic Filter" page. The left sidebar shows the Device List with categories like Access Rules, NAT Rules, Service Policy Rules, AAA Rules, Filter Rules, Public Servers, URL Filtering Servers, Threat Detection, Identity Options, Identity by TrustSec, Botnet Traffic Filter, Botnet Database, Black and White Lists, DNS Snooping, Traffic Settings, Objects, Unified Communications, and Advanced.

The main content area is titled "Configuration > Firewall > Botnet Traffic Filter". It contains a list of items:

- Botnet Database
- Black and White Lists
- DNS Snooping
- Traffic Settings

The status bar at the bottom indicates "admin", "2", and "7/10/14 6:07:41 PM UTC".



The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Device Setup' menu with options: Startup Wizard, Interfaces, Routing, Device Name/Password, System Time, and EtherChannel. The main content area is titled 'Configuration > Device Setup > Startup Wizard'. It contains the following text:

Click the "Launch Startup Wizard" button to start the wizard.

**Startup Wizard**

The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

At the bottom of the main content area is a button labeled 'Launch Startup Wizard'.

The bottom status bar shows the user 'admin', the session number '2', and the timestamp '7/10/14 6:03:51 PM UTC'.

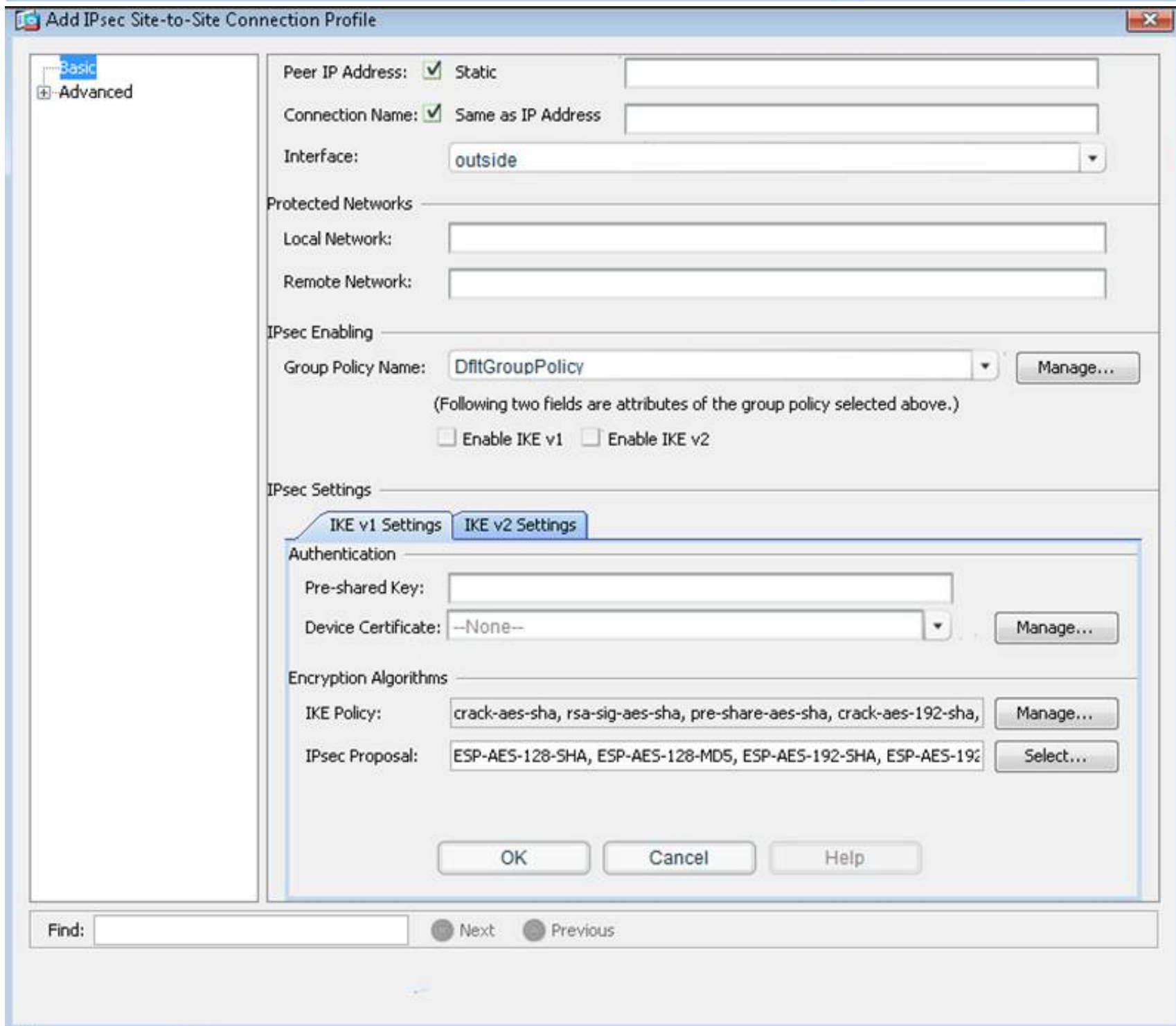
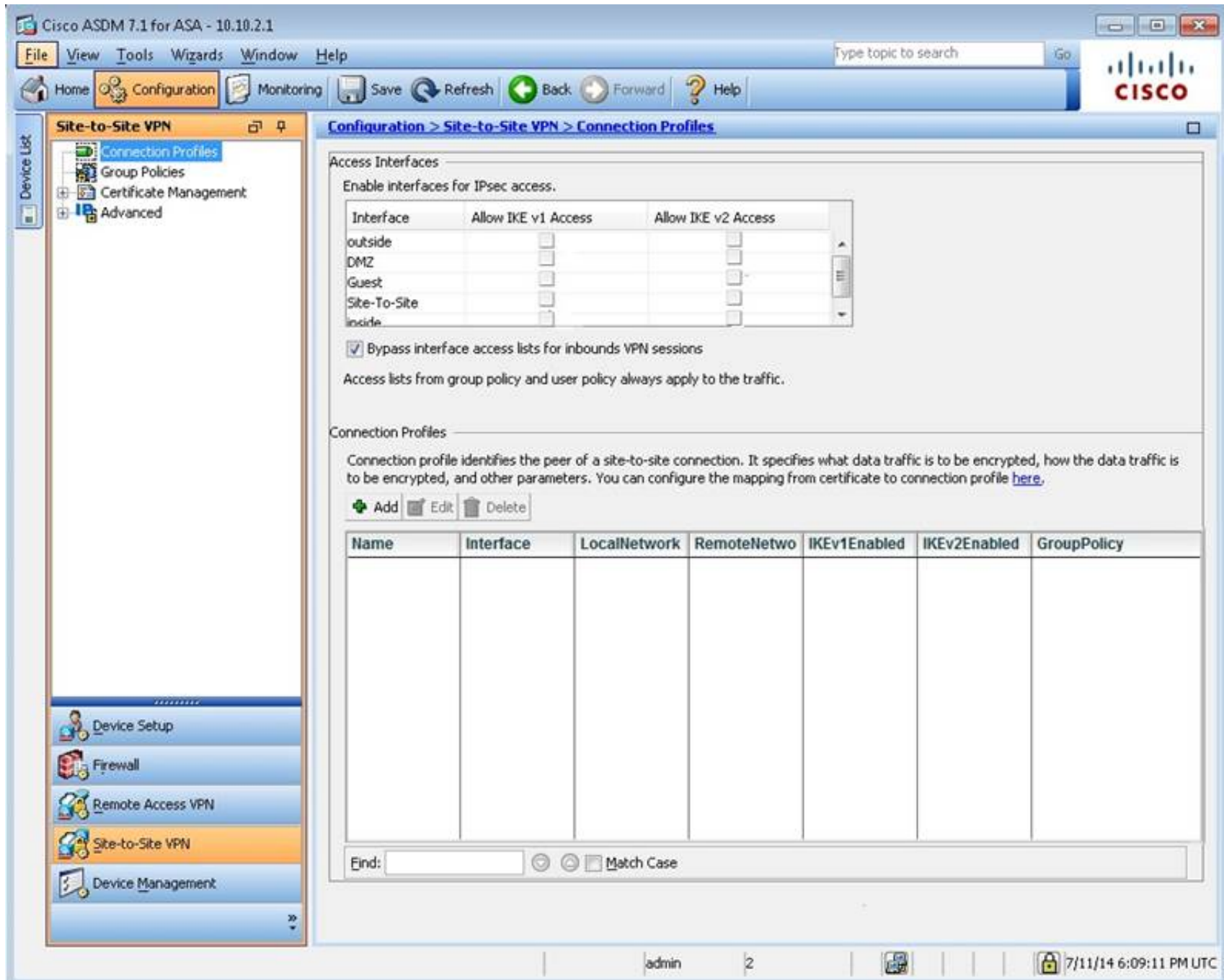
The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Device Setup' menu with options: Startup Wizard, Interfaces, Routing, Device Name/Password, System Time, and EtherChannel. The main content area is titled 'Configuration > Device Setup > Interfaces'. It contains a table with the following data:

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	

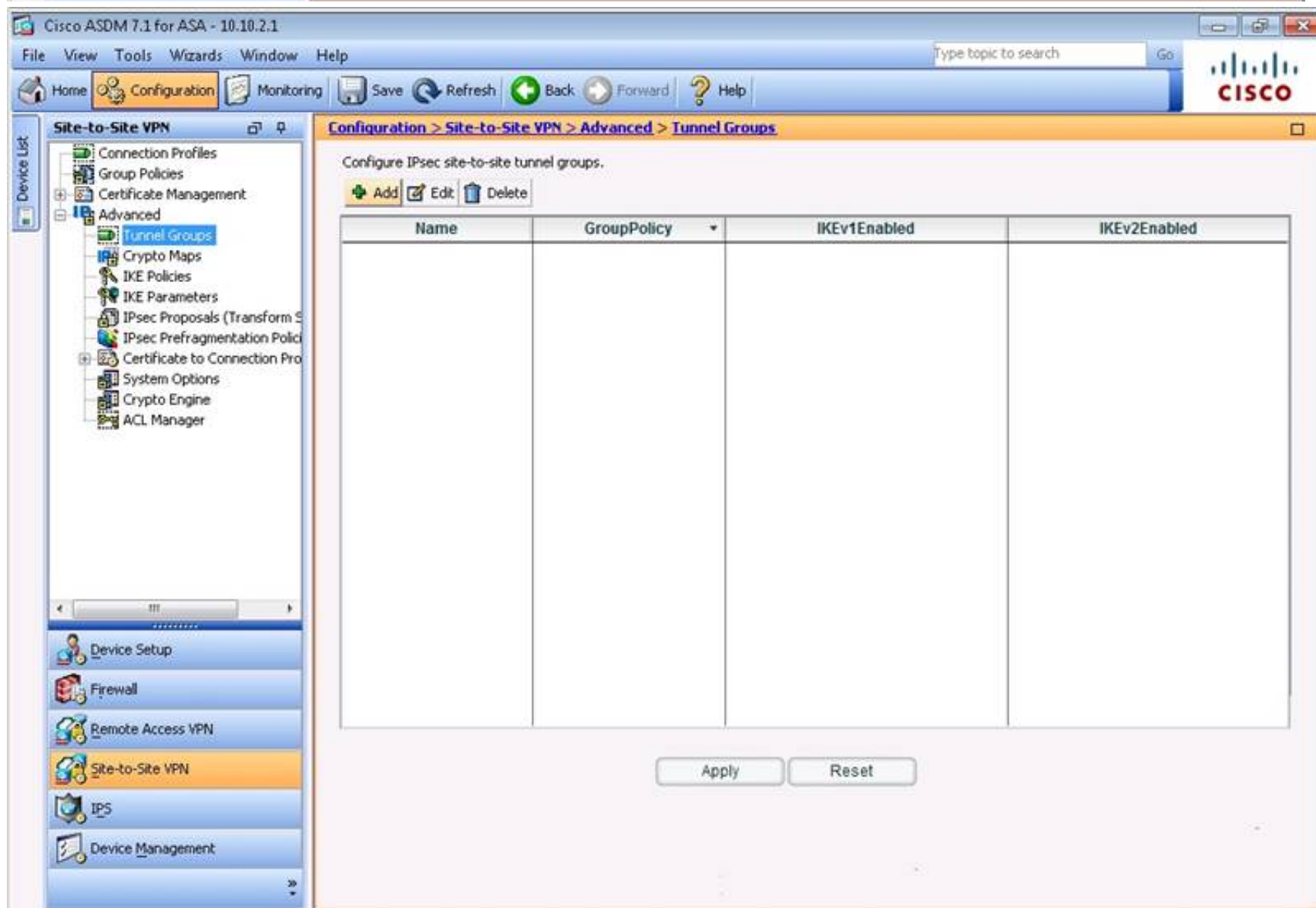
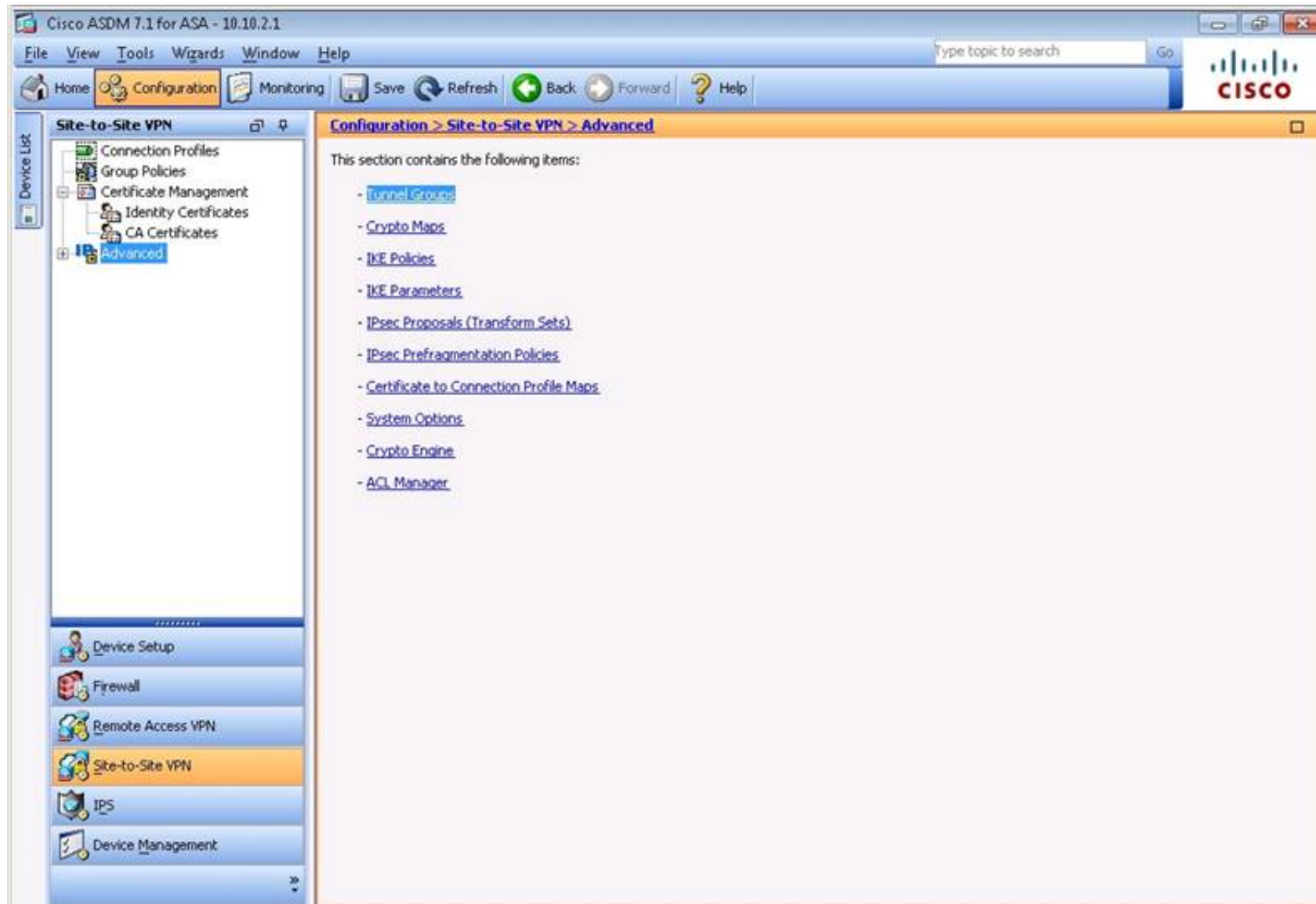
Below the table, there are three checkboxes:

- ☐ 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

At the bottom of the main content area are two buttons: 'Apply' and 'Reset'.









Edit IPsec Site-to-site Tunnel Group: 203.0.113.1

Name:

IPsec Enabling

Group Policy Name: Manage...

(Following two fields are attributes of the group policy selected above.)

Enable IKE v1 ☐ Enable IKE v2 ☐

IPsec Settings

IKE v1 Settings

Authentication

Pre-shared Key:

Device Certificate: -- None -- Manage...

IKE Peer ID Validation: Required

IKE Keepalive

☐ Disable keepalives

☒ Monitor keepalives

Confidence Interval:  seconds

Retry Interval:  seconds

☐ Headend will never initiate keepalive monitoring

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Site-to-Site VPN

Configuration > Site-to-Site VPN > Advanced > ACL Manager

#	Enabled	Source	User	Security Group	Destination	Security
<b>DMZ_access_in</b>						
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	
<b>outside_access_in</b>						
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	
<b>outside_cryptomap</b>						
1	<input checked="" type="checkbox"/>	10.10.9.0/24			10.11.11.0/24	
<b>permit-all</b>						
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 'Remote Access VPN' configuration tree, with 'Network (Client) Access' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access' page. The content includes an introduction, important concepts, and three main sections: 1. SSL tunnel and IPsec tunnel, 2. User and connection profile, and 3. Access policy.

**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.

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Device Management' configuration tree, with 'Management Access' selected. The main pane shows the 'Configuration > Device Management > Management Access' page. The content includes a list of items: ASDM/HTTPS/Telnet/SSH, Command Line (CLI), File Access, ICMP, Management Interface, SNMP, and Management Access Rules.

This section contains the following items:

- [ASDM/HTTPS/Telnet/SSH](#)
- [Command Line \(CLI\)](#)
- [File Access](#)
- [ICMP](#)
- [Management Interface](#)
- [SNMP](#)
- [Management Access Rules](#)



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**

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup Firewall Remote Access VPN Site-to-Site VPN IPS Device Management

**Configuration > Firewall > Access Rules**

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

Source Criteria:		Destination Criteria:	
#	Enabled	Source	Destination
<b>DMZ (9 incoming rules)</b>			
1	<input checked="" type="checkbox"/>	DMZ-server	any4
2	<input checked="" type="checkbox"/>	DMZ-server	any
3	<input checked="" type="checkbox"/>	ESA	any
4	<input checked="" type="checkbox"/>	ESA	HQ-srv
5	<input checked="" type="checkbox"/>	ESA	HQ-srv
6	<input checked="" type="checkbox"/>	ESA	any
7	<input checked="" type="checkbox"/>	ESA	any
8	<input checked="" type="checkbox"/>	ESA	HQ-srv
9	<input checked="" type="checkbox"/>	ESA	HQ-srv
<b>Guest (1 implicit incoming rule)</b>			
1	<input checked="" type="checkbox"/>	any	Any less secure ne...
<b>Site-To-Site (5 incoming rules)</b>			
1	<input checked="" type="checkbox"/>	any	HQ-srv
2	<input checked="" type="checkbox"/>	any	HQ-srv
3	<input checked="" type="checkbox"/>	any	any
4	<input checked="" type="checkbox"/>	any	HQ-srv
5	<input checked="" type="checkbox"/>	any	any
<b>inside (1 implicit incoming rule)</b>			
1	<input checked="" type="checkbox"/>	any	Any less secure ne...
<b>management (1 implicit incoming rule)</b>			
1	<input checked="" type="checkbox"/>	any	Any less secure ne...
<b>outside (9 incoming rules)</b>			
1	<input checked="" type="checkbox"/>	any4	DMZ-server
2	<input checked="" type="checkbox"/>	any4	DMZ-server

Apply Reset Advanced...

admin 15 S/9/14 7:13:38 PM GMT

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**

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup Firewall Remote Access VPN Site-to-Site VPN IPS Device Management

**Configuration > Firewall > Service Policy Rules**

Add Edit Delete Find Diagram Packet Trace

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service
<b>Global Policy: global_policy</b>								
inspection_de...		<input checked="" type="checkbox"/>	Match	any		any		default-insp

Apply Reset



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**

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects**
  - Network Objects/Groups
  - Service Objects/Groups
  - Local Users
  - Local User Groups
  - Security Group Object Groups
  - Class Maps
  - Inspect Maps
  - Regular Expressions
  - TCP Maps
  - Time Ranges

Device Setup Firewall Remote Access VPN Site-to-Site VPN IPS Device Management

**Configuration > Firewall > Objects**

This section contains the following items:

- [Network Objects/Groups](#)
- [Service Objects/Groups](#)
- [Local Users](#)
- [Local User Groups](#)
- [Security Group Object Groups](#)
- [Class Maps](#)
- [Inspect Maps](#)
- [Regular Expressions](#)
- [TCP Maps](#)
- [Time Ranges](#)

admin 15 5/9/14 7:24:48 PM GMT

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**

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects**
  - Network Objects/Groups
  - Service Objects/Groups**
  - Local Users
  - Local User Groups
  - Security Group Object Groups
  - Class Maps
  - Inspect Maps
  - Regular Expressions
  - TCP Maps
  - Time Ranges

Device Setup Firewall Remote Access VPN Site-to-Site VPN IPS Device Management

**Configuration > Firewall > Objects > Service Objects/Groups**

+ Add Edit Delete Where Used

Filter: Filter/Clear

Name	Protocol	Source Ports	Destination Ports	ICMP	Description
Protocol Groups					
TCPUDP					
Service Objects					
any					

Apply Reset

admin 15 5/14/14 6:06:28 PM GMT

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

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
  - Network Objects/Groups
  - Service Objects/Groups
  - Local Users
  - Local User Groups
  - Security Group Object Groups**
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

IPS

Device Management

Configuration > Firewall > Objects > Security Group Object Groups

Add Edit Delete Where Used

Filter: Filter Clear

Name	Count	Security Type	Description
------	-------	---------------	-------------

Apply Reset

admin 15 5/14/14 6:09:18 PM GMT

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

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
  - Network Objects/Groups**
  - Service Objects/Groups
  - Local Users
  - Local User Groups
  - Security Group Object Groups
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Firewall > Objects > Network Objects/Groups

Add Edit Delete Where Used Not Used

Network Object... Network Object Group...

Filter: Filter Clear

Name	IPAddress	Netmask	Description	Object NAT Address
------	-----------	---------	-------------	--------------------

Apply Reset

student 15 7/3/14 3:50:41 PM UTC

Add Network Object

Name:
Type: Network
IP Version: ☒ IPv4 ☐ IPv6
IP Address:
Netmask: 0.0.0.0

NAT

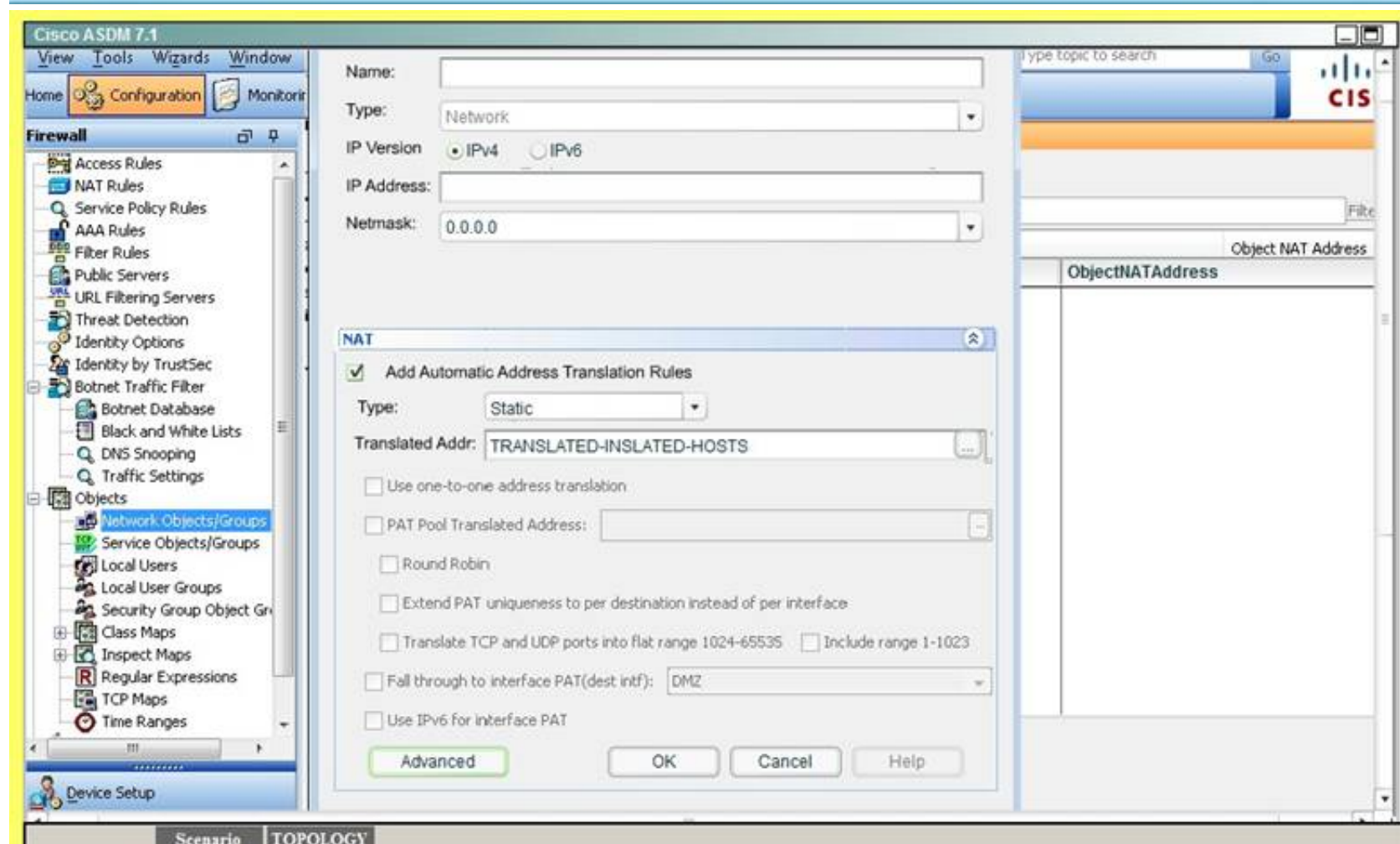
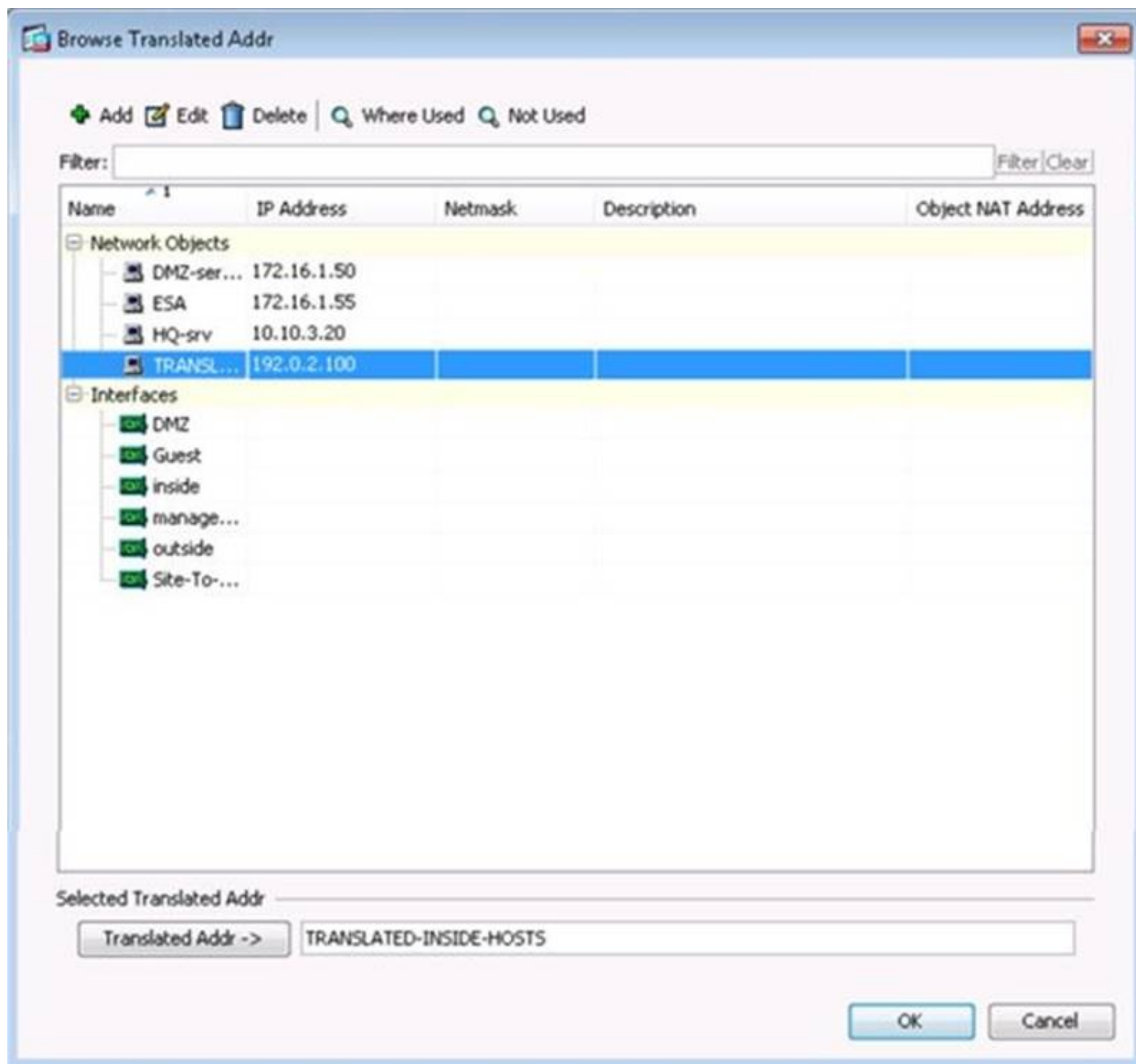
☐ Add Automatic Address Translation Rules

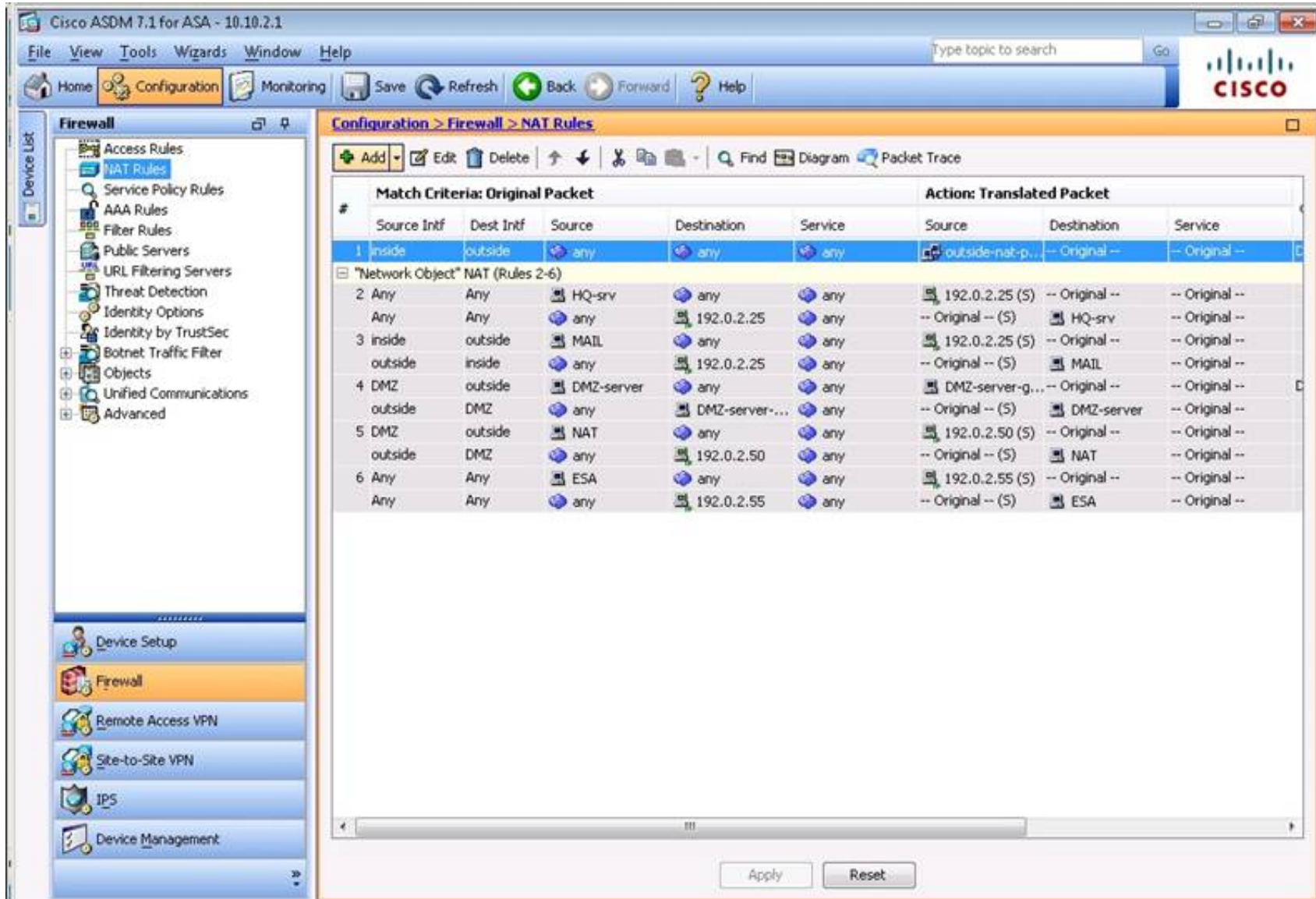
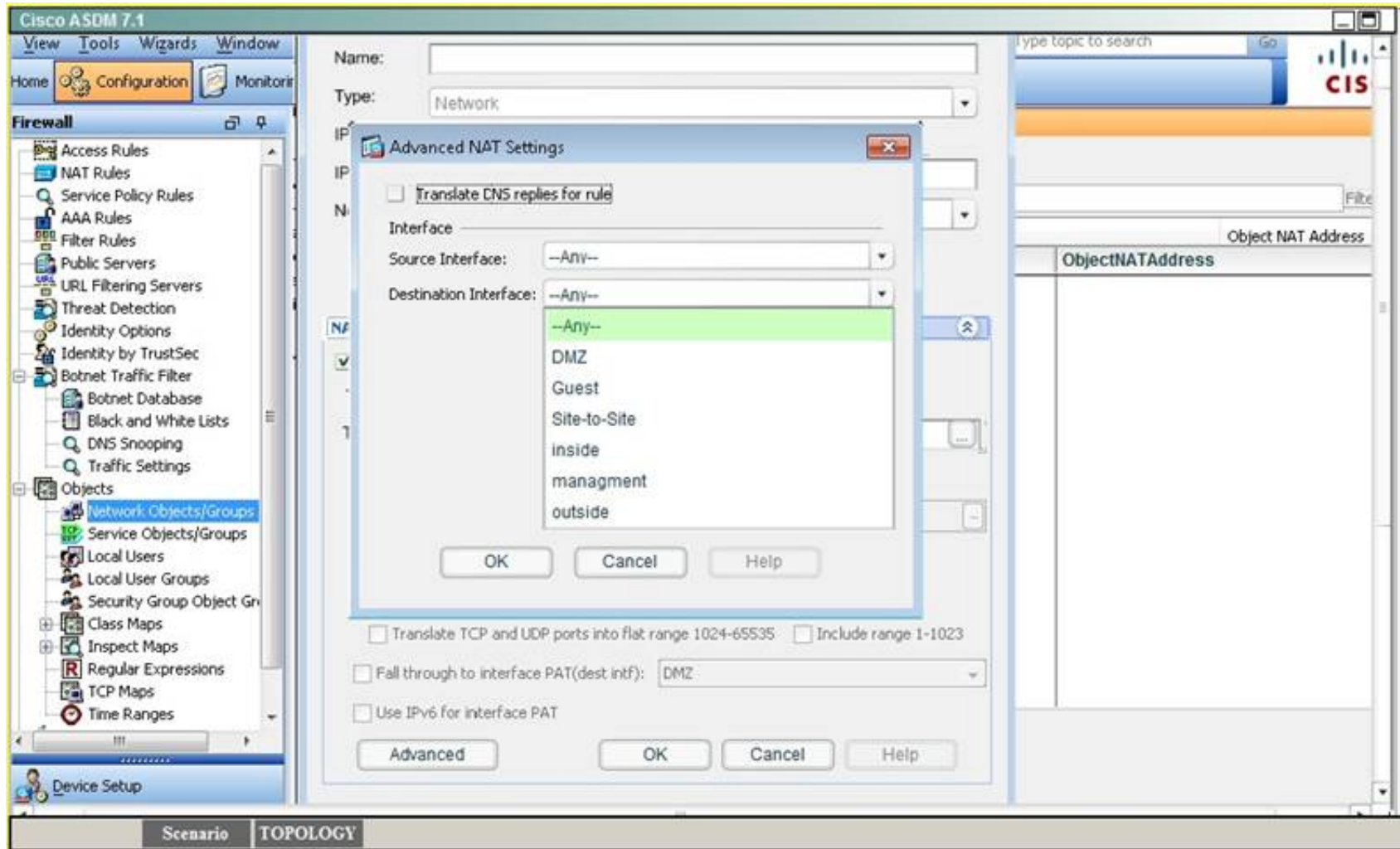
Type: Static
Translated Addr:

☐ Use one-to-one address translation
☐ PAT Pool Translated Address:
☐ 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(dest intf): DMZ
☐ Use IPv6 for interface PAT

Advanced 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

Access Rules  
 NAT Rules  
 Service Policy Rules  
 AAA Rules  
 Filter Rules  
 Public Servers  
 URL Filtering Servers  
 Threat Detection  
 Identity Options  
 Identity by TrustSec  
 Botnet Traffic Filter  
 Objects  
 Unified Communications  
 Advanced

Device Setup  
 Firewall  
 Remote Access VPN  
 Site-to-Site VPN  
 IPS  
 Device Management

Configuration > Firewall > NAT Rules

Add Edit Delete Find Diagram Packet Trace

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 --
"Network Object" NAT (Rules 2-6)								
2	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 --
3	inside	outside	MAIL	any	any	192.0.2.25 (S)	-- Original --	-- Original --
	outside	inside	any	192.0.2.25	any	-- Original -- (S)	MAIL	-- Original --
4	DMZ	outside	DMZ-server	any	any	DMZ-server-g...	-- Original --	-- Original --
	outside	DMZ	any	DMZ-server...	any	-- Original -- (S)	DMZ-server	-- Original --
5	DMZ	outside	NAT	any	any	192.0.2.50 (S)	-- Original --	-- Original --
	outside	DMZ	any	192.0.2.50	any	-- Original -- (S)	NAT	-- Original --
6	Any	Any	ESA	any	any	192.0.2.55 (S)	-- Original --	-- Original --
	Any	Any	any	192.0.2.55	any	-- Original -- (S)	ESA	-- Original --

Apply Reset

**Edit NAT Rule**

Match Criteria: Original Packet

Source Interface:  Destination Interface:

Source Address:  Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address:  Destination Address:

☐ Use one-to-one address translation

☐ PAT Pool Translated Address:  Service:

☐ 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:

Description:

OK Cancel Help



The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Device List' with a tree view under 'Device Management'. The main pane shows the 'Configuration > Device Management > Management Access' page. The page content lists the following items:

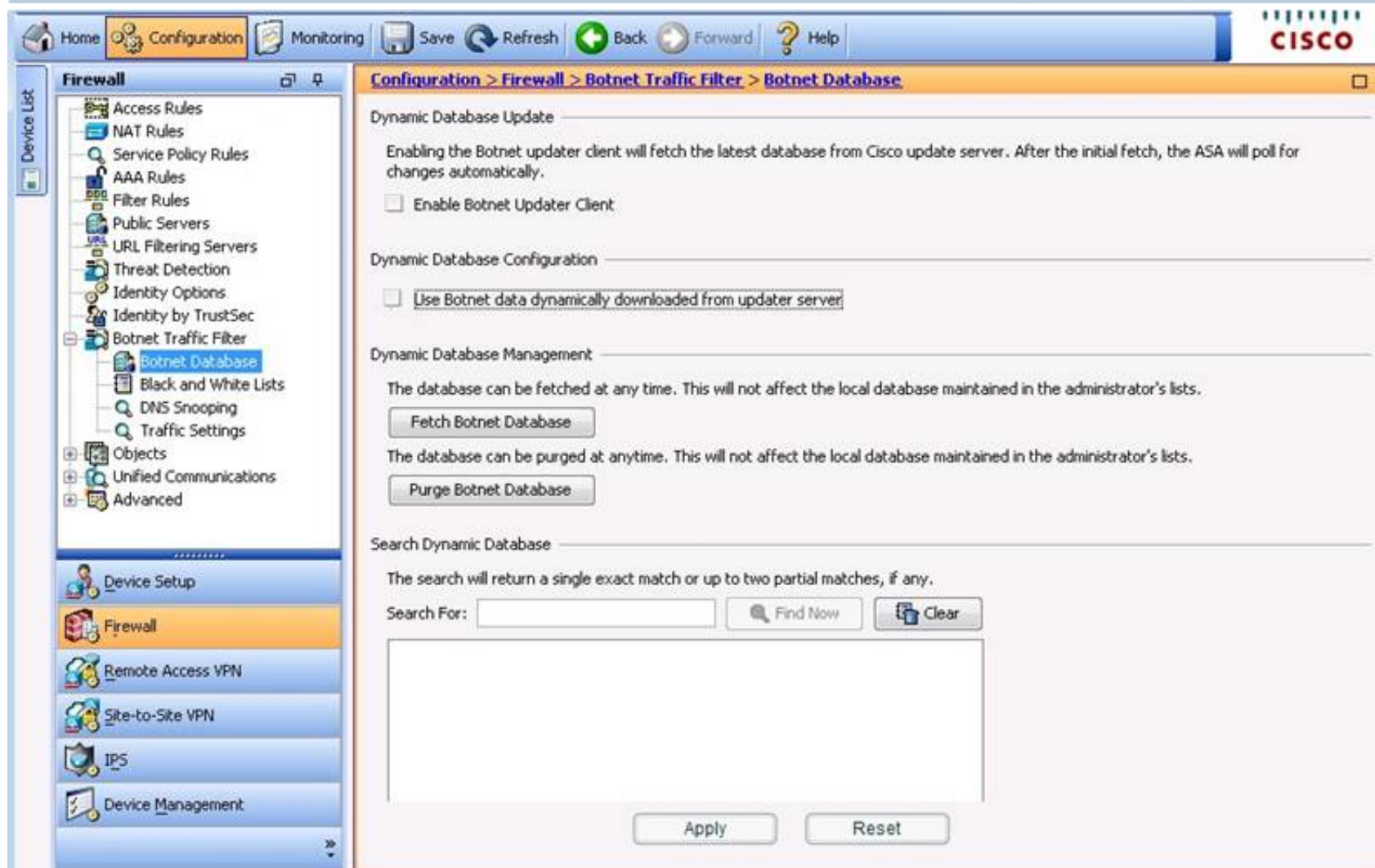
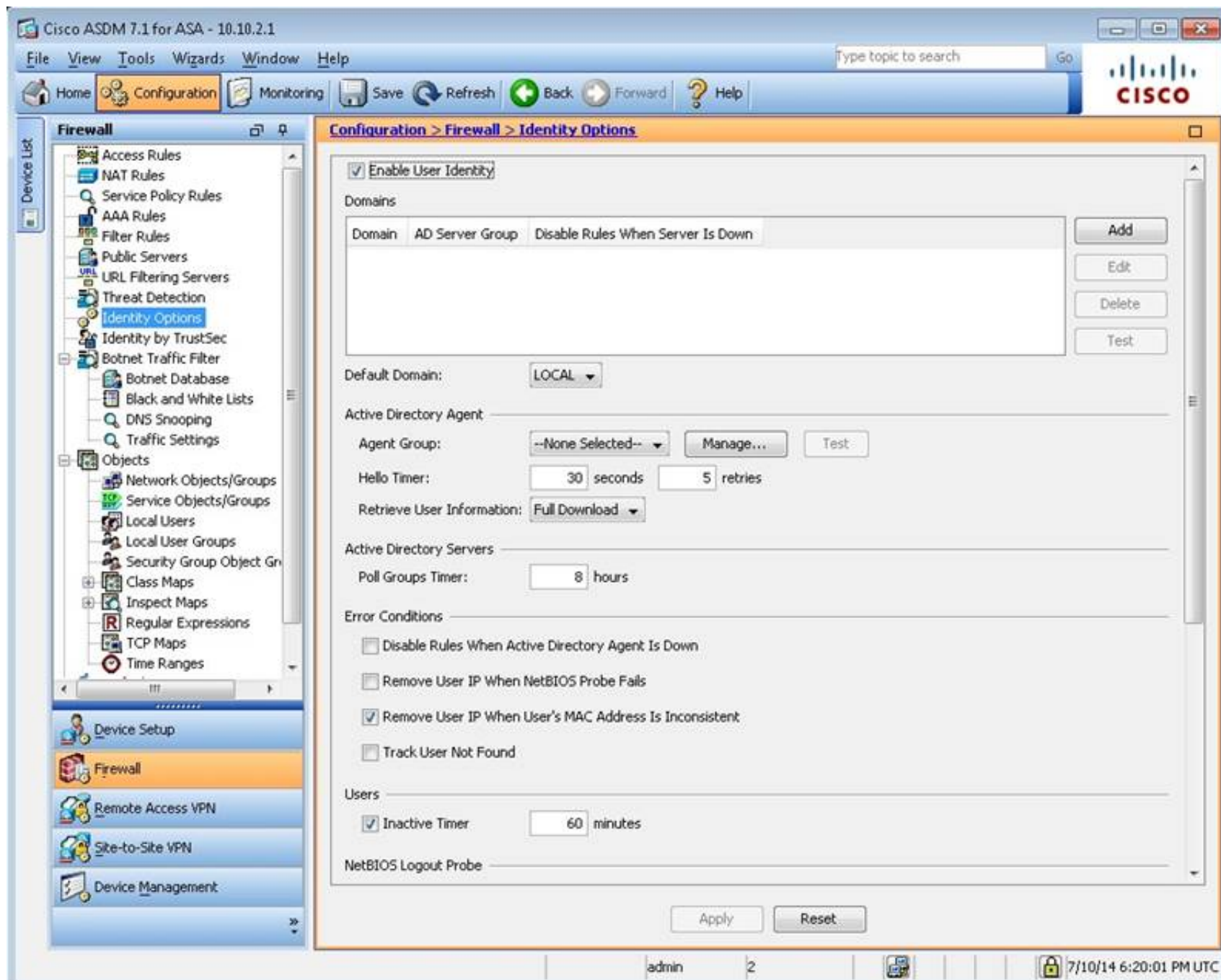
- [ASDM/HTTPS/Telnet/SSH](#)
- [Command Line \(CLI\)](#)
- [File Access](#)
- [ICMP](#)
- [Management Interface](#)
- [SNMP](#)
- [Management Access Rules](#)

The bottom status bar shows the user 'admin' and the time '7/10/14 6:12:21 PM UTC'.

The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar displays the 'Device List' with a tree view under 'Firewall'. The main pane shows the 'Configuration > Firewall > Advanced' page. The page content lists the following items:

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

The bottom status bar shows the user 'admin' and the time '5/14/14 6:05:08 PM GMT'.





Home Configuration Monitoring Save Refresh Back Forward Help

**Firewall**

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
  - Botnet Database
  - Black and White Lists
  - DNS Snooping**
  - Traffic Settings
- Objects
- Unified Communications
- Advanced

Device Setup  
**Firewall**  
 Remote Access VPN  
 Site-to-Site VPN  
 IPS  
 Device Management

**Configuration > Firewall > Botnet Traffic Filter > DNS Snooping**

Enable DNS snooping for existing DNS inspection service policy rules. To add or edit a service policy rule for DNS inspection, go to [Configuration > Firewall > Service Policy Rules](#).

Interface	Source	Destination	Service	DNS Snooping Enabled	DNS Map Name	Description
global	any4	any4	default-in...	<input type="checkbox"/>	preset_dns_map	

Apply Reset

Home Configuration Monitoring Save Refresh Back Forward Help

**Firewall**

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
  - Botnet Database
  - Black and White Lists
  - DNS Snooping
  - Traffic Settings**
- Objects
- Unified Communications
- Advanced

Device Setup  
**Firewall**  
 Remote Access VPN  
 Site-to-Site VPN  
 IPS  
 Device Management

**Configuration > Firewall > Botnet Traffic Filter > Traffic Settings**

Traffic Classification  
 Define Botnet traffic classification for individual interfaces and/or globally.

Interface	Traffic Classified	ACL Used
Site-to-Site	<input type="checkbox"/>	DISABLED
Guest	<input type="checkbox"/>	DISABLED
inside	<input type="checkbox"/>	DISABLED
management	<input type="checkbox"/>	DISABLED
DMZ	<input type="checkbox"/>	DISABLED
outside	<input type="checkbox"/>	ALL TRAFFIC

Manage ACL...

Ambiguous Traffic Handling  
☐ Treat ambiguous (greylisted) traffic as malicious (blacklisted) traffic.

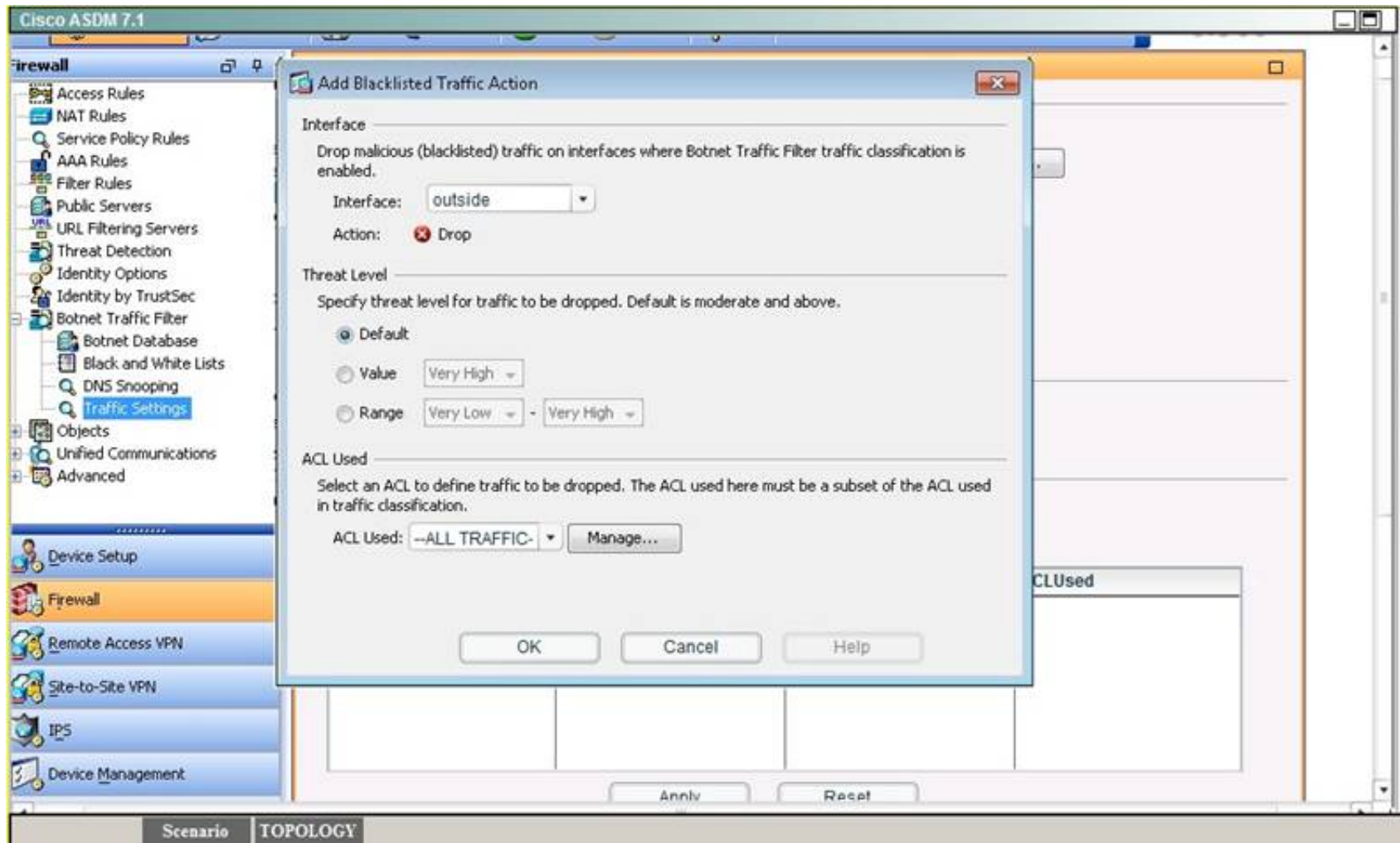
Blacklisted Traffic Actions  
 Define blacklisted traffic actions.

+ Add Edit Delete

Interface	Action	ThreatLevel	ACLUsed

Apply Reset



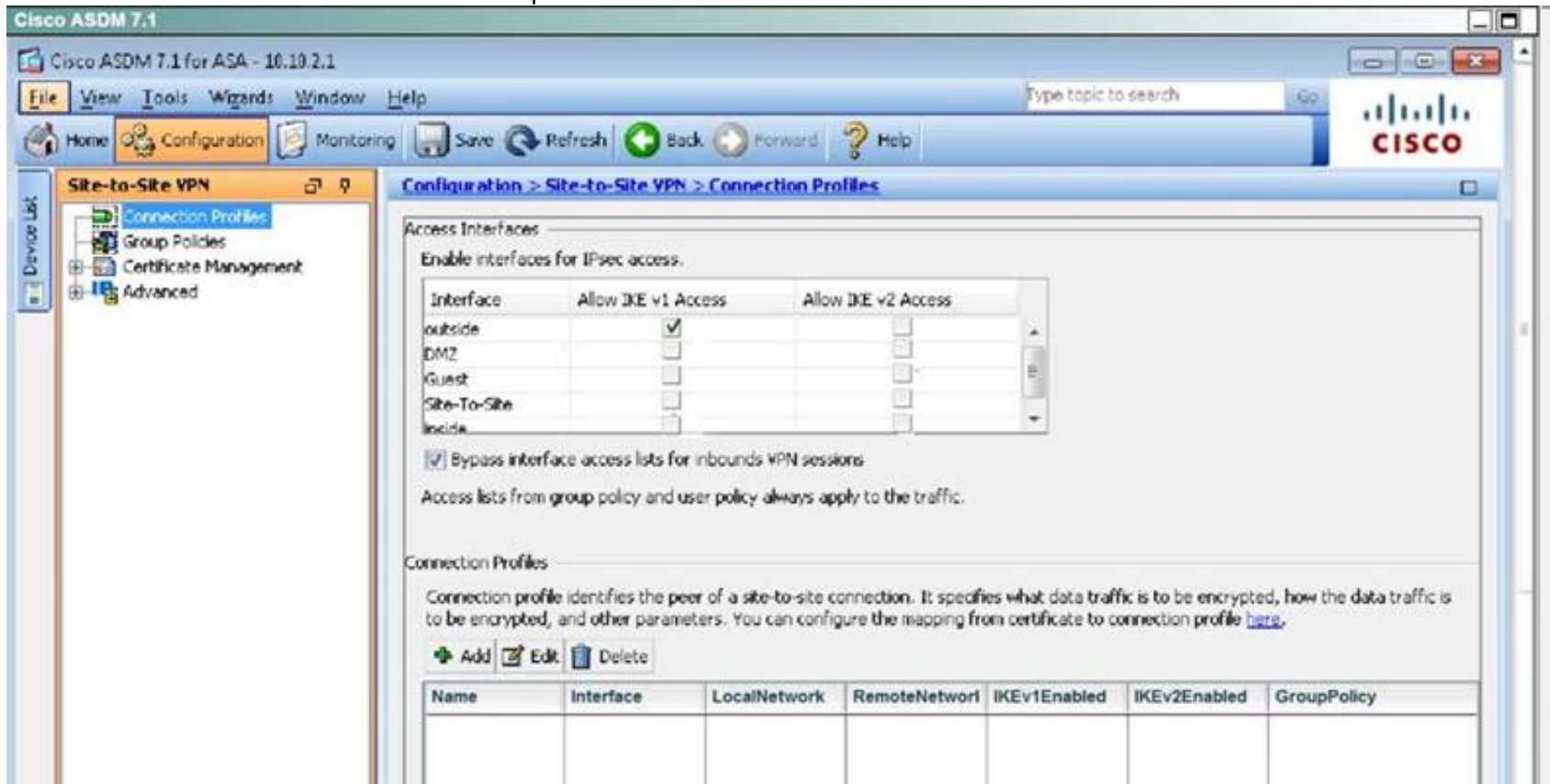


**Answer:**

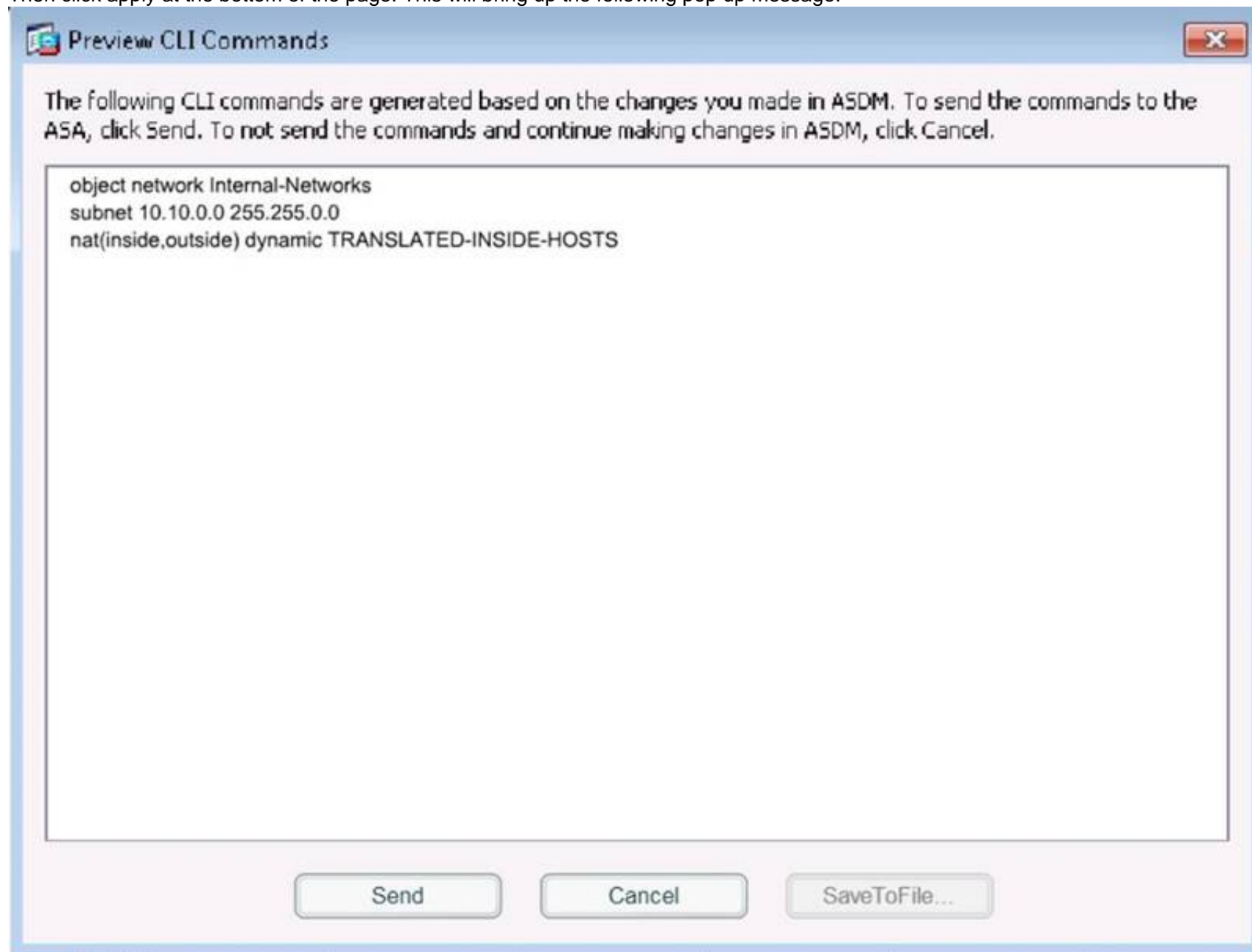
**Explanation:** First, click on Configuration ->Site-to-Site VPN to bring up this screen:



Click on "allow IKE v1 Access" for the outside per the instructions as shown below:

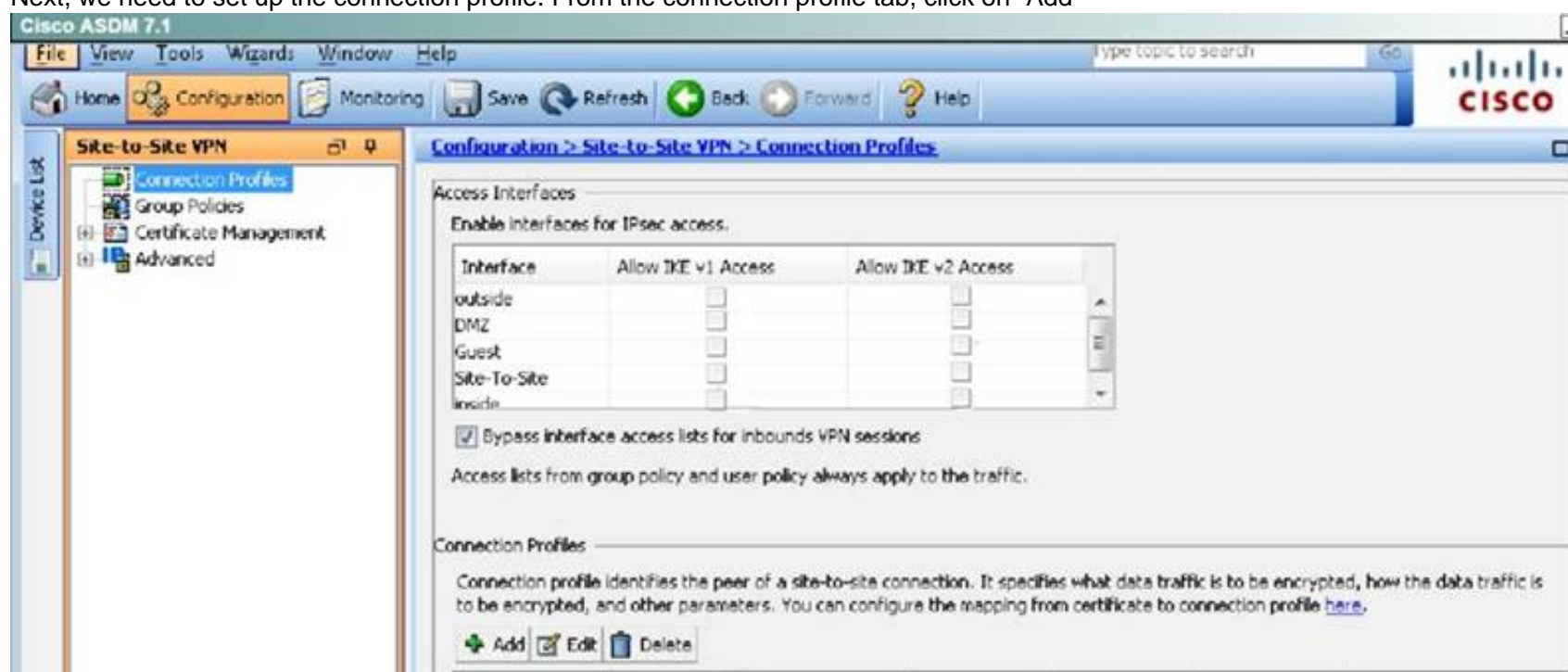


Then click apply at the bottom of the page. This will bring up the following pop up message:



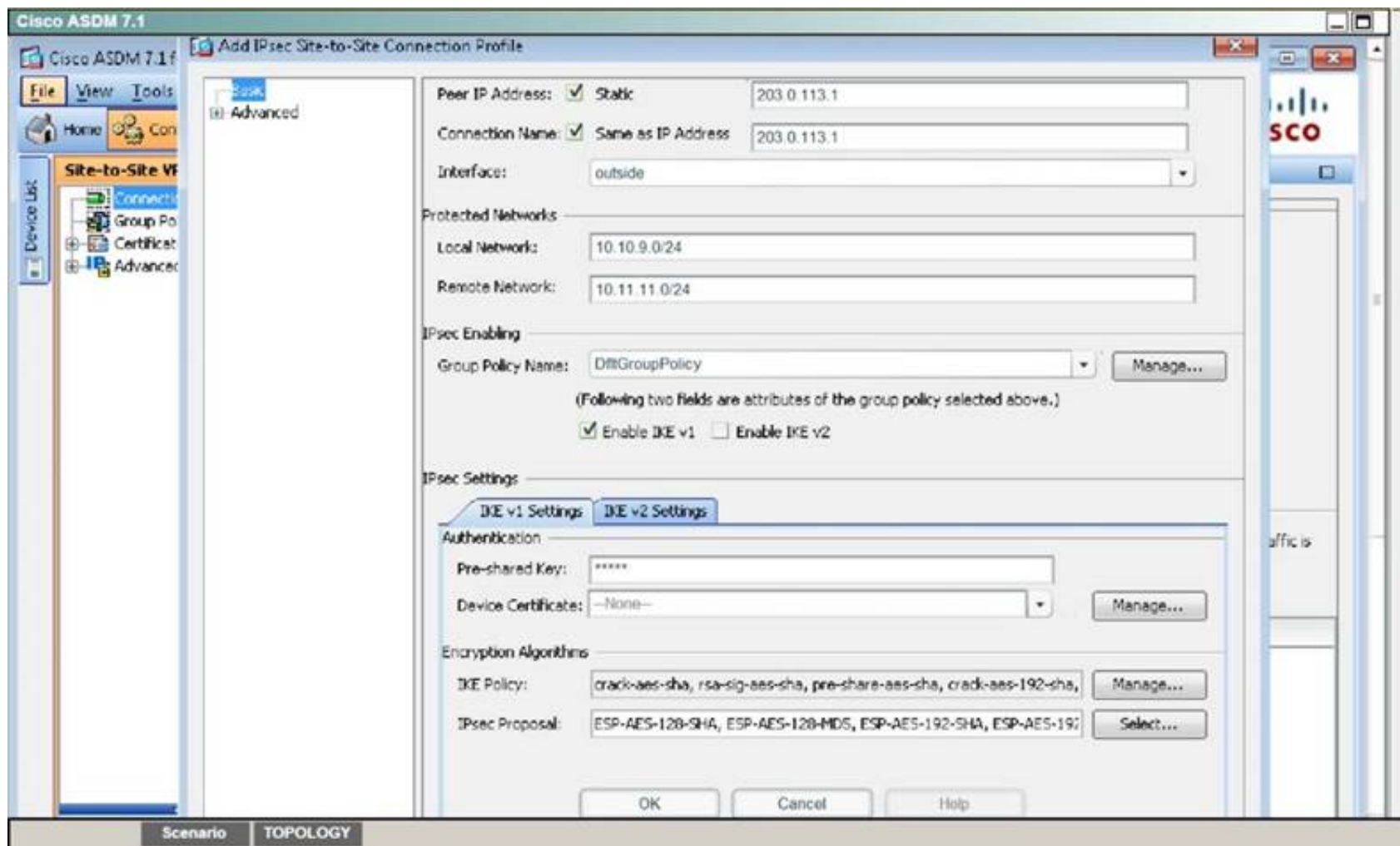
Click on Send.

Next, we need to set up the connection profile. From the connection profile tab, click on "Add"

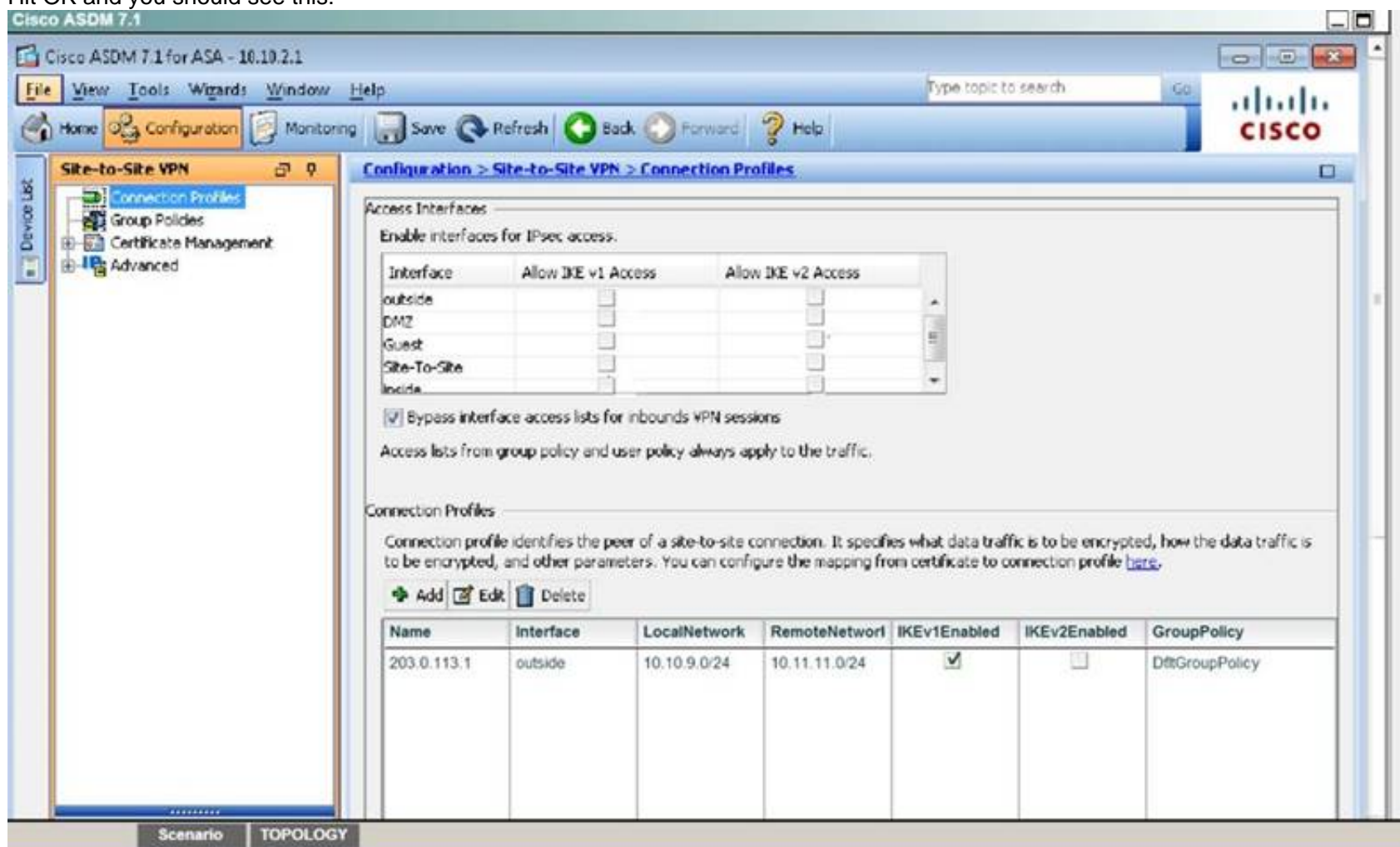


Then, fill in the information per the instructions as shown below:



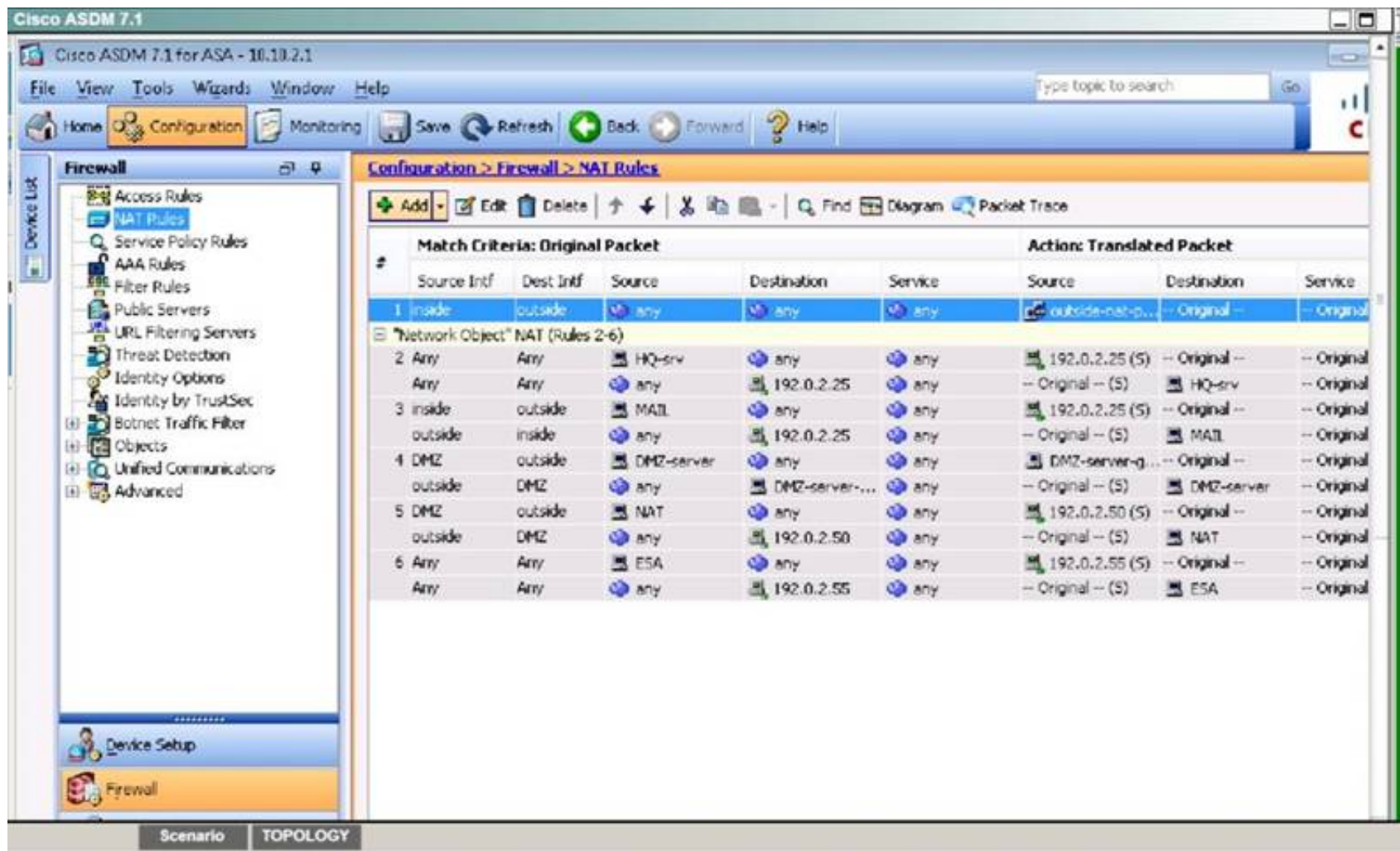


Hit OK and you should see this:

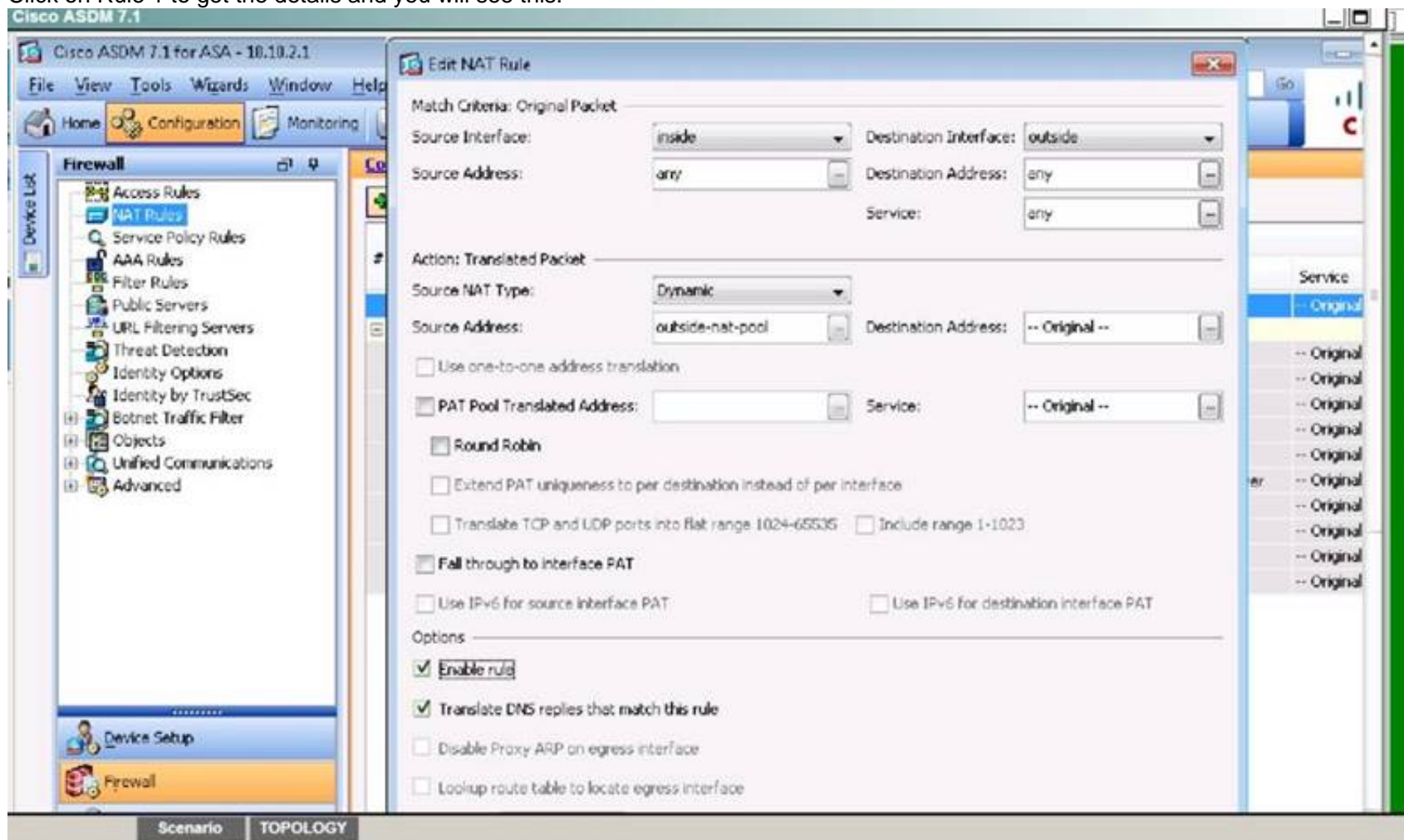


To test this, we need to disable NAT. Go to Configuration -> Firewall -> NAT rules and you should see this:



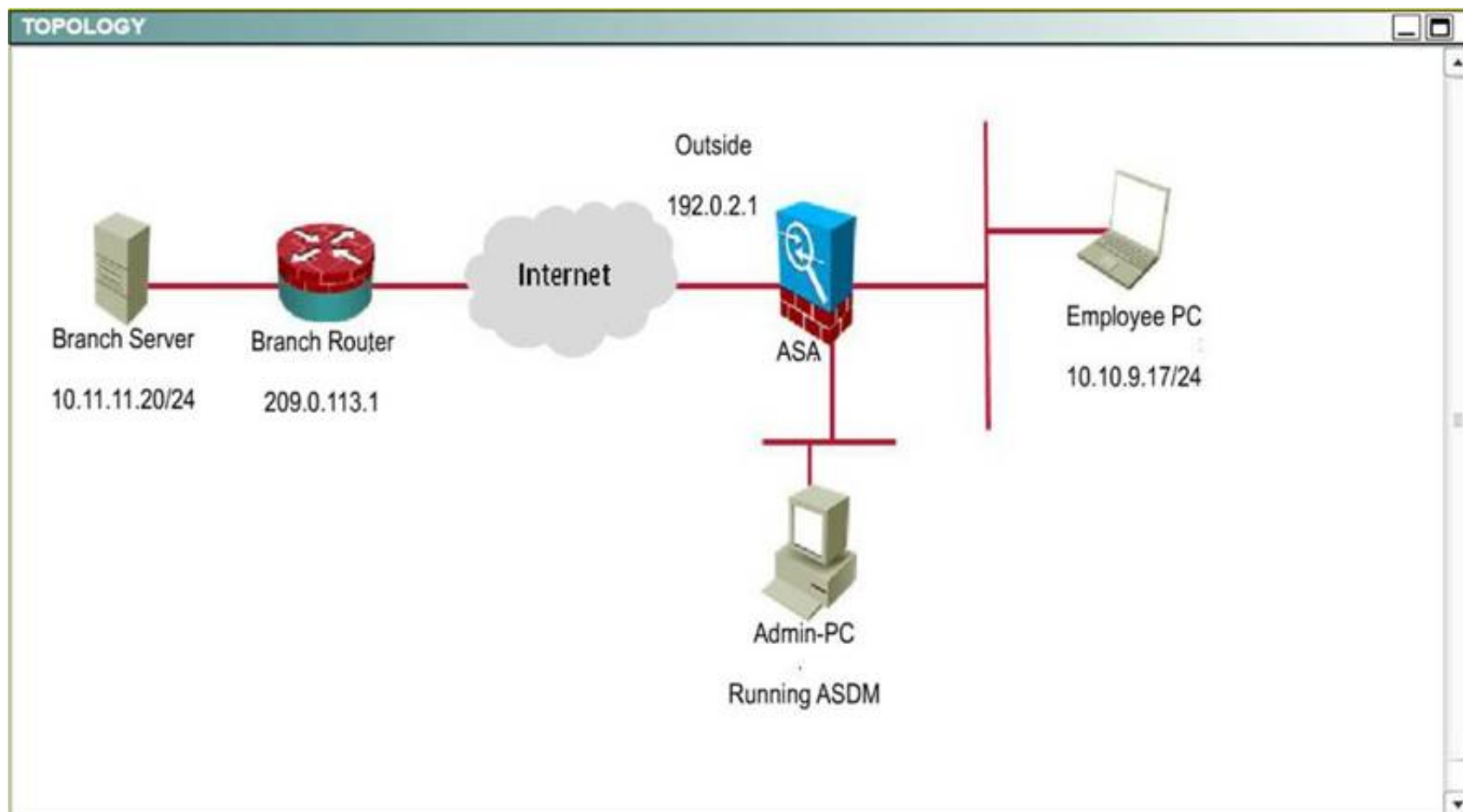


Click on Rule 1 to get the details and you will see this:

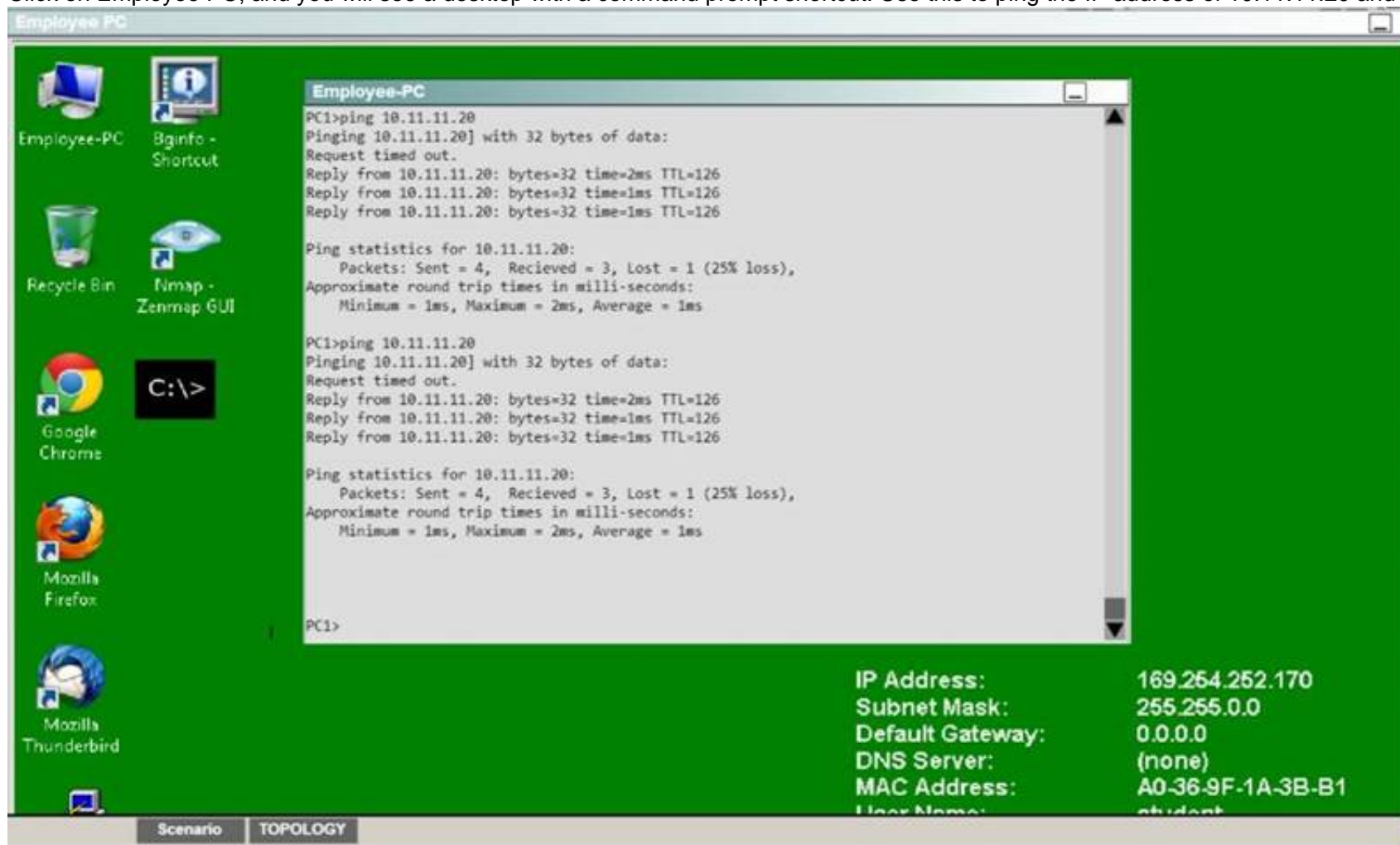


We need to uncheck the "Enable rule" button on the bottom. It might also be a good idea to uncheck the "Translate DNS replies that match the rule" but it should not be needed.

Then, go back to the topology:

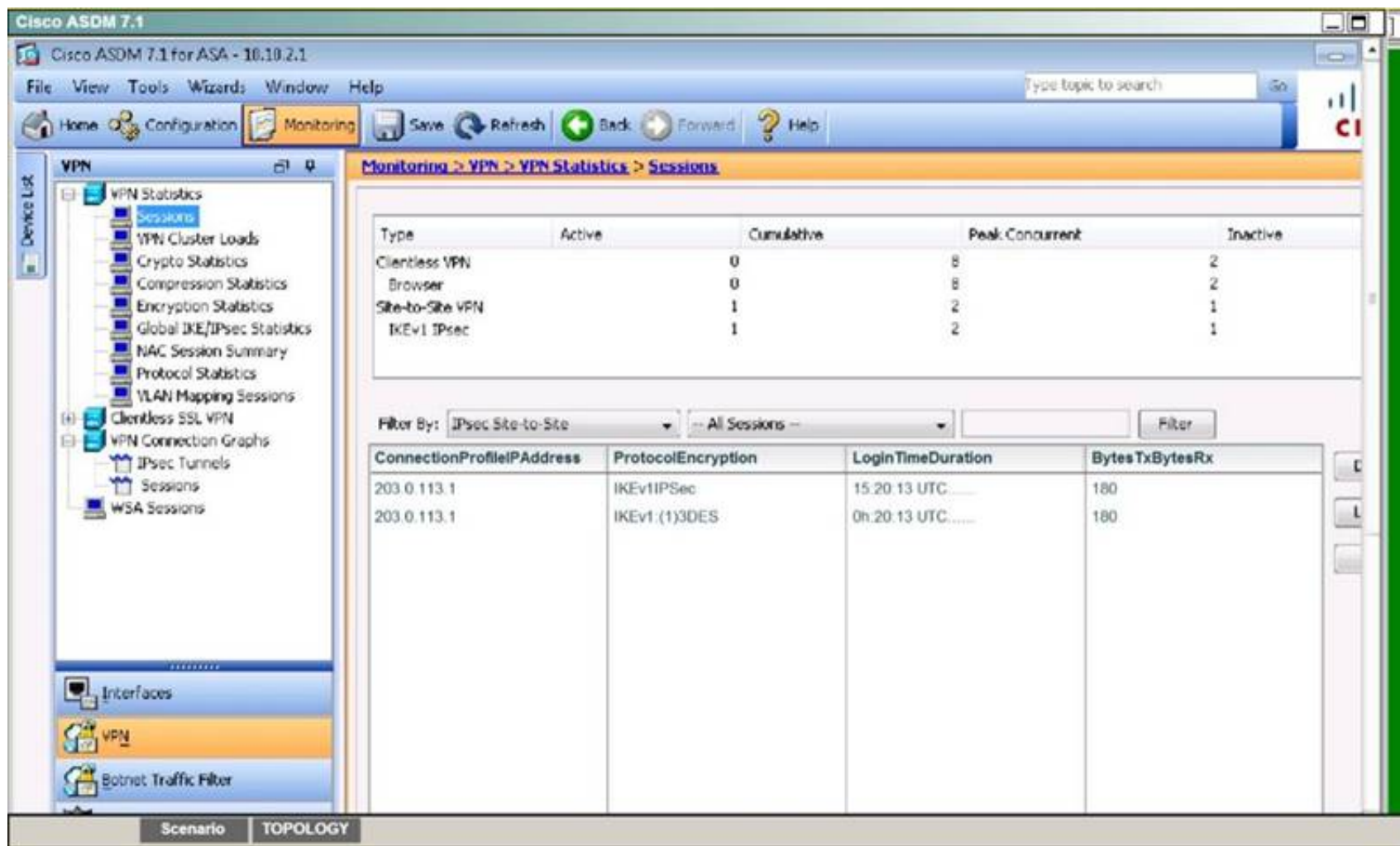


Click on Employee PC, and you will see a desktop with a command prompt shortcut. Use this to ping the IP address of 10.11.11.20 and you should see replies:



We can also verify by viewing the VPN Statistics -> Sessions and see the bytes in/out incrementing as shown below:





#### NEW QUESTION 252

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 256

Which two statements about the Cisco ASA Clientless SSL VPN solution are true? (Choose two.)

- A. When a client connects to the Cisco ASA WebVPN portal and tries to access HTTP resources through the URL bar, the client uses the local DNS to perform FQDN resolution.
- B. The `rewriter enable` command under the global `webvpn` configuration enables the rewriter functionality because that feature is disabled by default.
- C. A Cisco ASA with an AnyConnect Premium Peers license can simultaneously allow Clientless SSL VPN sessions and AnyConnect client sessions.
- D. Content rewriter functionality in the Clientless SSL VPN portal is not supported on Apple mobile devices.
- E. Clientless SSLVPN provides Layer 3 connectivity into the secured network.

**Answer: CD**

#### NEW QUESTION 259

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 264

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 265

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

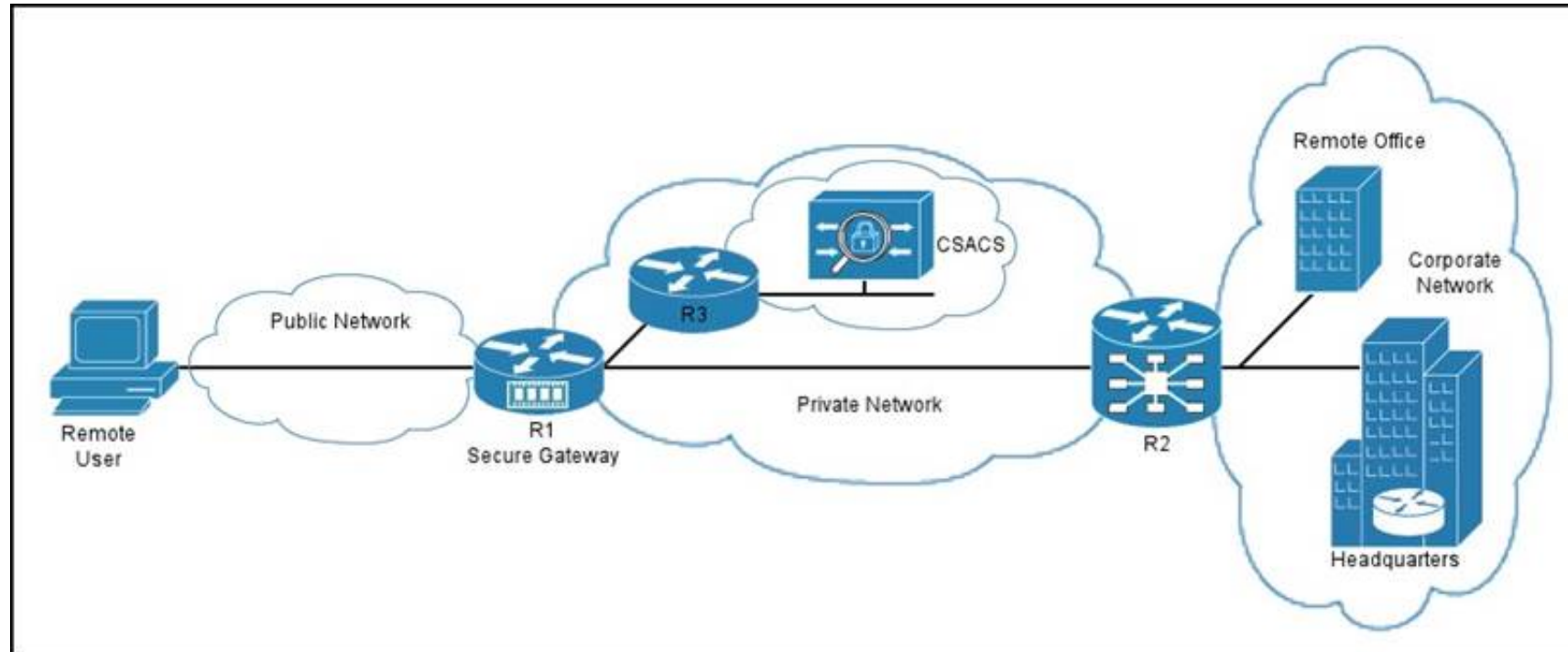


- A. Enable EIGRP next-hop-self on the hub.
- B. Disable EIGRP next-hop-self on the hub.
- C. Enable EIGRP split-horizon on the hub.
- D. Add NHRP redirects on the hub.
- E. Add NHRP shortcuts on the spoke.
- F. Add NHRP shortcuts on the hub.

**Answer:** BDE

#### NEW QUESTION 266

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 268

Which algorithm provides both encryption and authentication for data plane communication?

- A. SHA-96
- B. SHA-384
- C. 3DES
- D. AES-256
- E. AES-GCM
- F. RC4

**Answer:** E

#### NEW QUESTION 271

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 272

Scenario

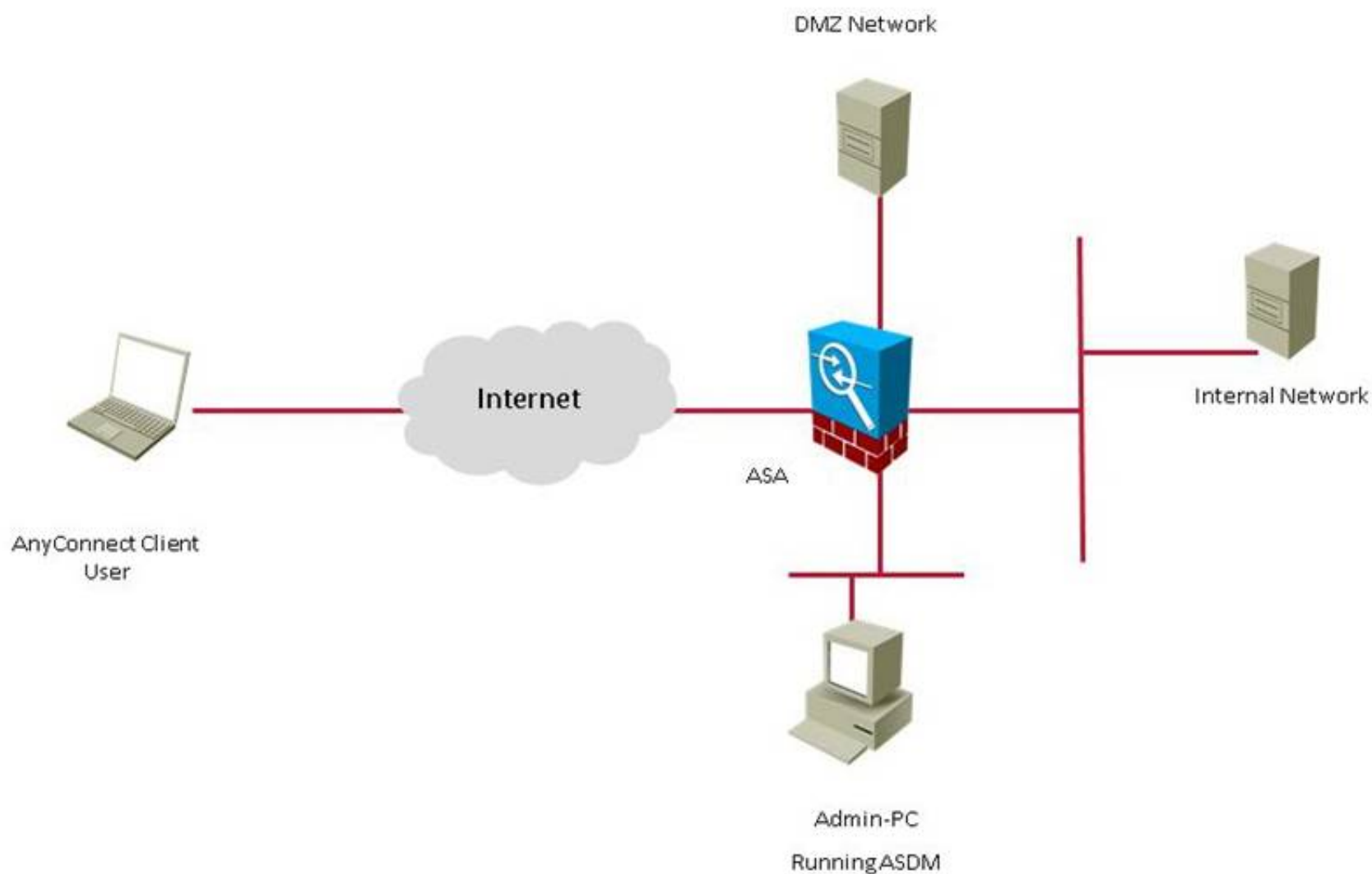
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

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

Home

Device Dashboard Firewall Dashboard Intrusion Prevention

### Device Information

General License

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

ASA Version: **9.1(1)4** Device Uptime: **16d 12h 29m 22s**

ASDM Version: **7.1(2)** Device Type: **ASA 5515, IPS**

Firewall Mode: **Routed** Context Mode: **Single**

Environment Status: **OK** 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	4
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)

772MB

14:33:25

### Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

### Traffic Status

Connections Per Second Usage

14:29 14:30 14:31 14:32 14:33

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

14:29 14:30 14:31 14:32 14:33

Input Kbps: 0 Output Kbps: 0

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Device Setup > Interfaces

### Device Setup

Startup Wizard

Interfaces

Routing

Device Name/Password

System Time

EtherChannel

### 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	

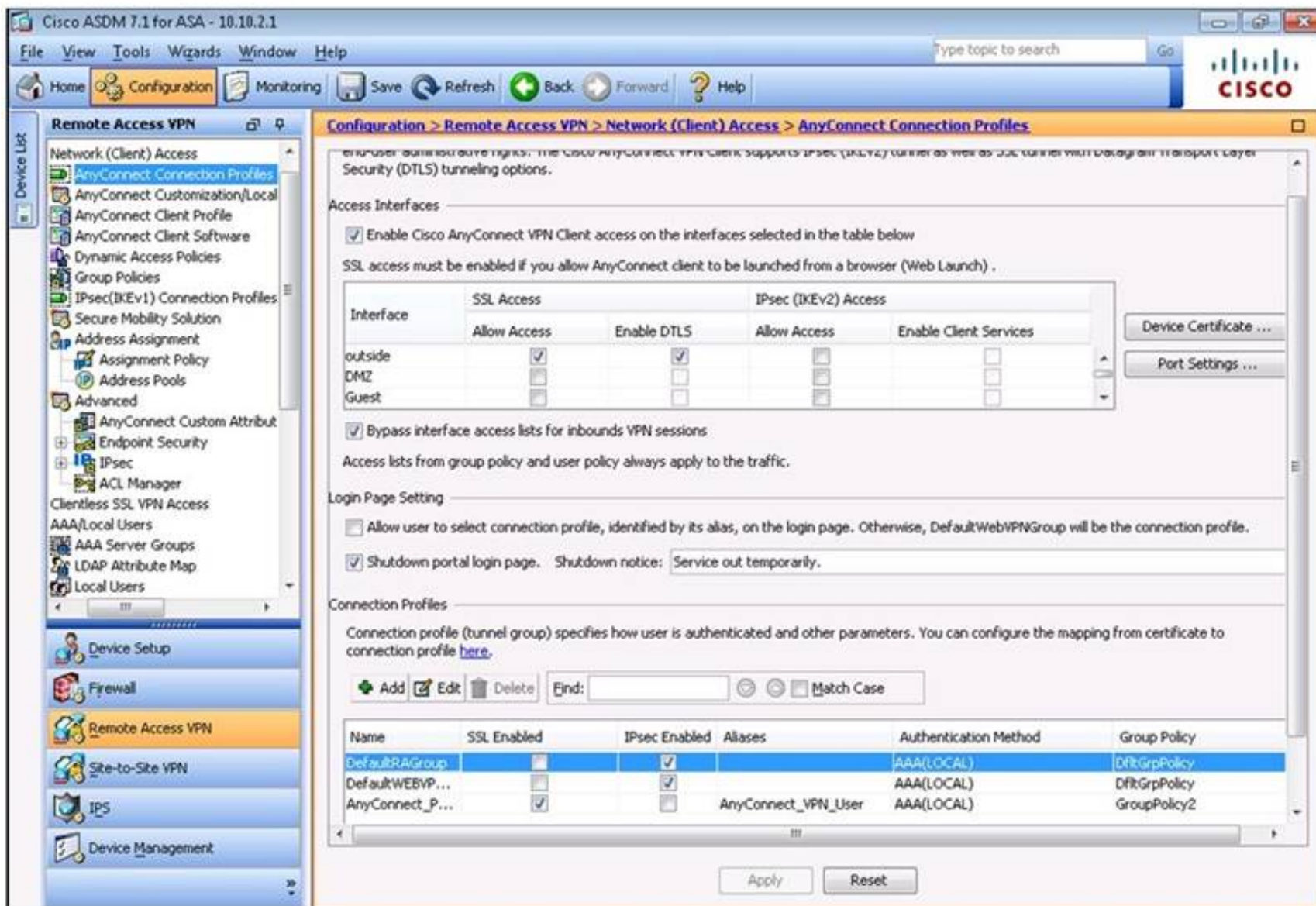
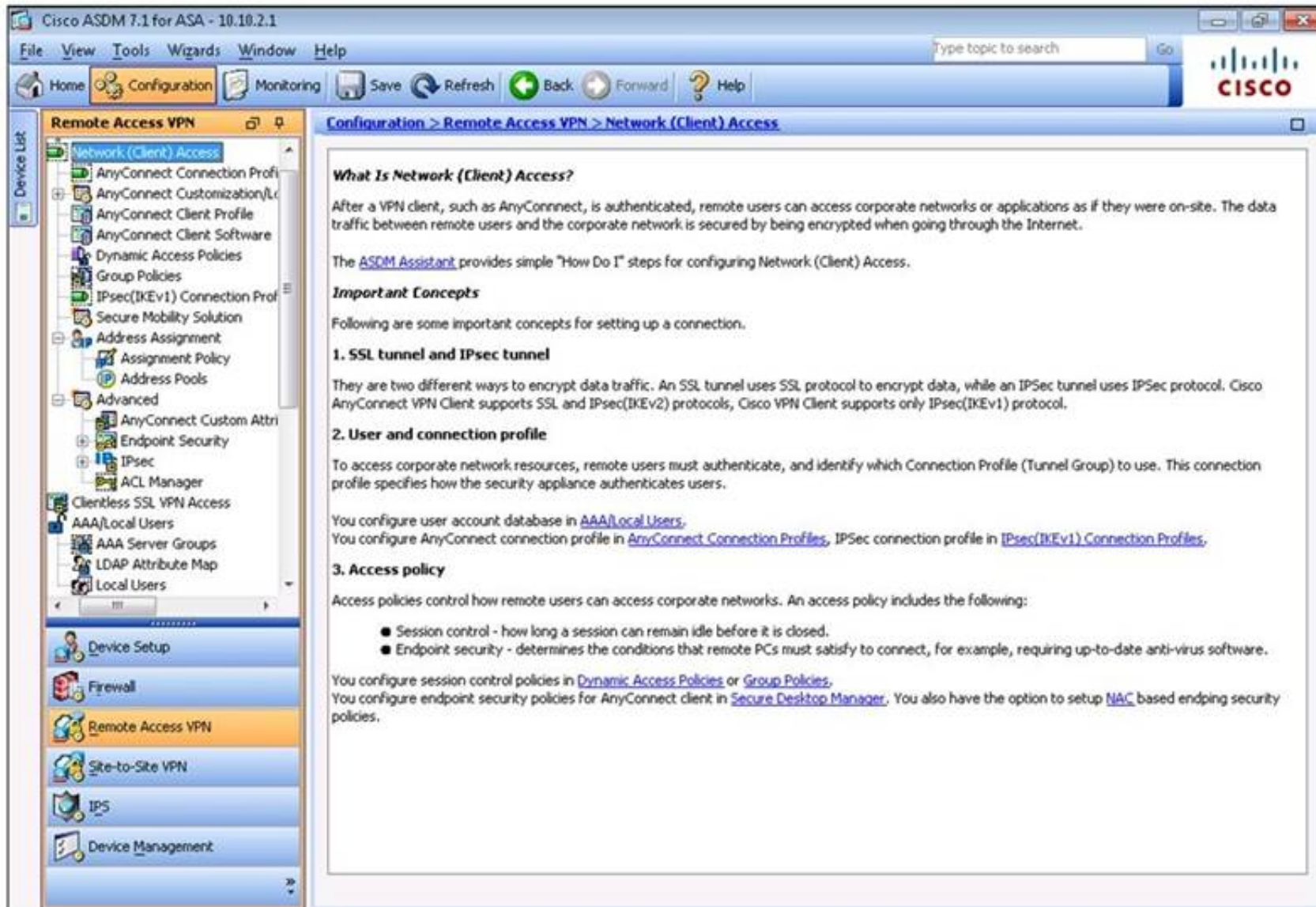
Enable traffic between two or more interfaces which are configured with same security levels

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




Enable jumbo frame reservation

Apply Reset





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 

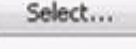
☐ Use LOCAL if Server Group fails

Client Address Assignment

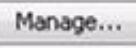
DHCP Servers:

☒ 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

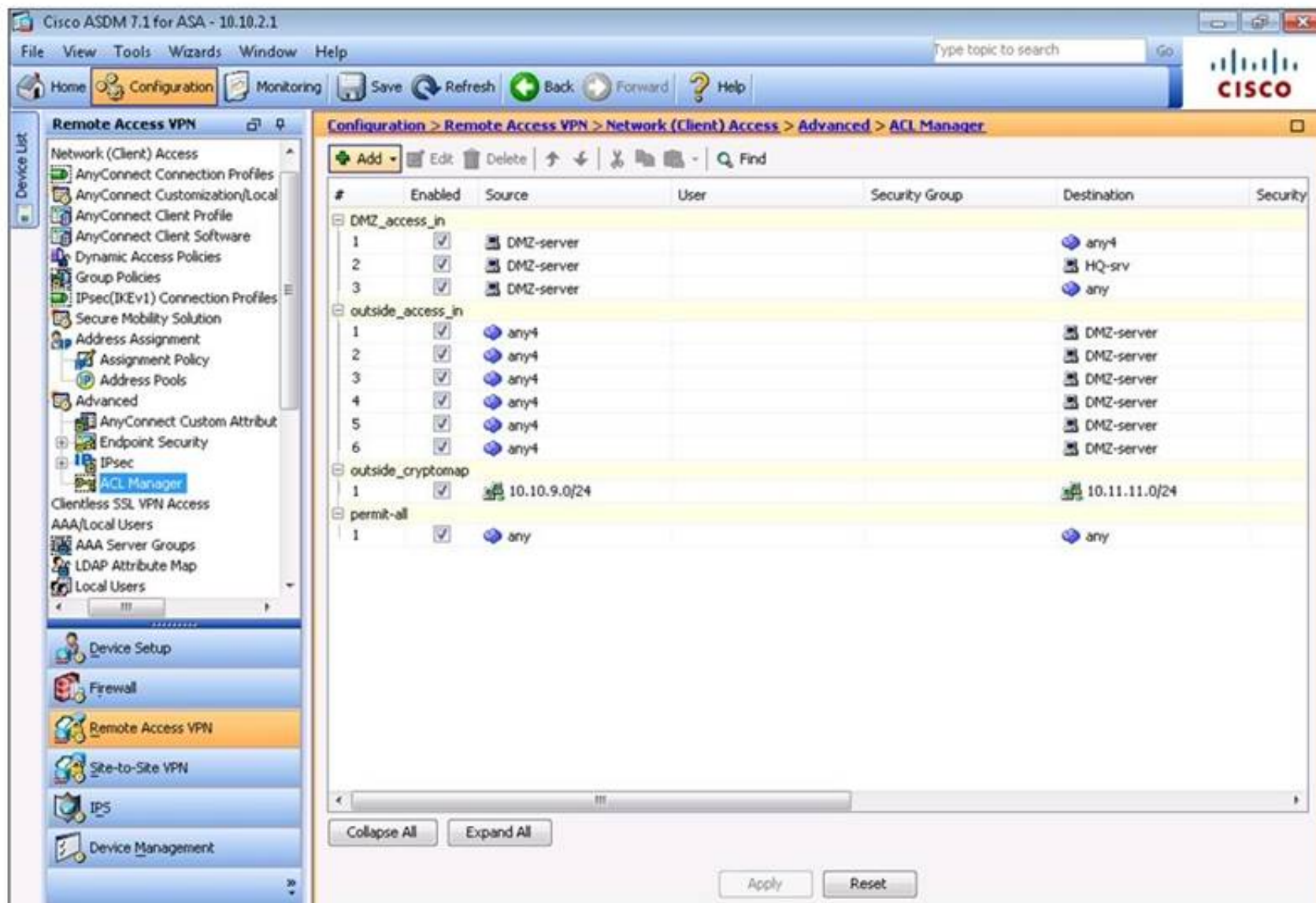
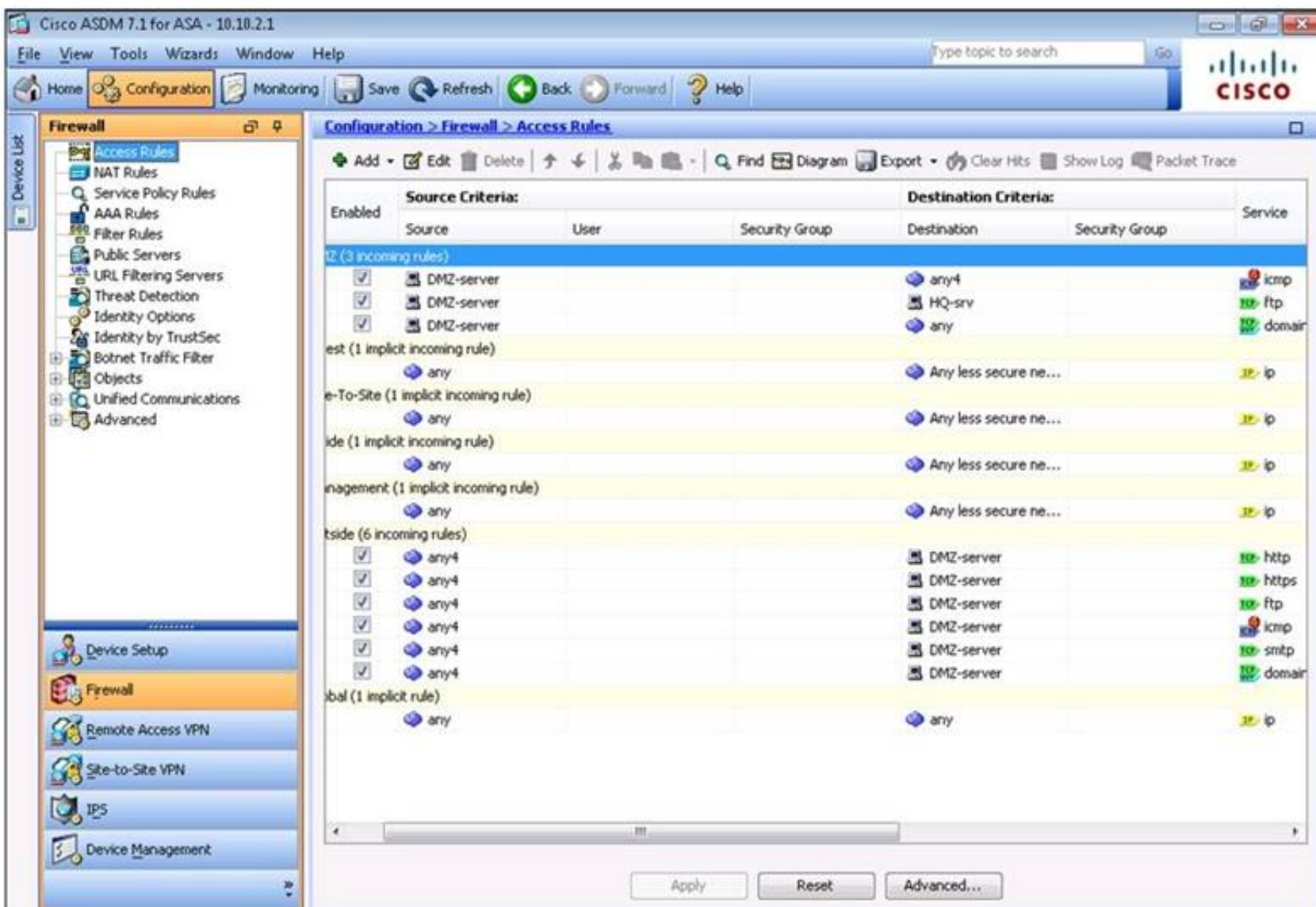
WINS Servers:

Domain Name: secure-x.local

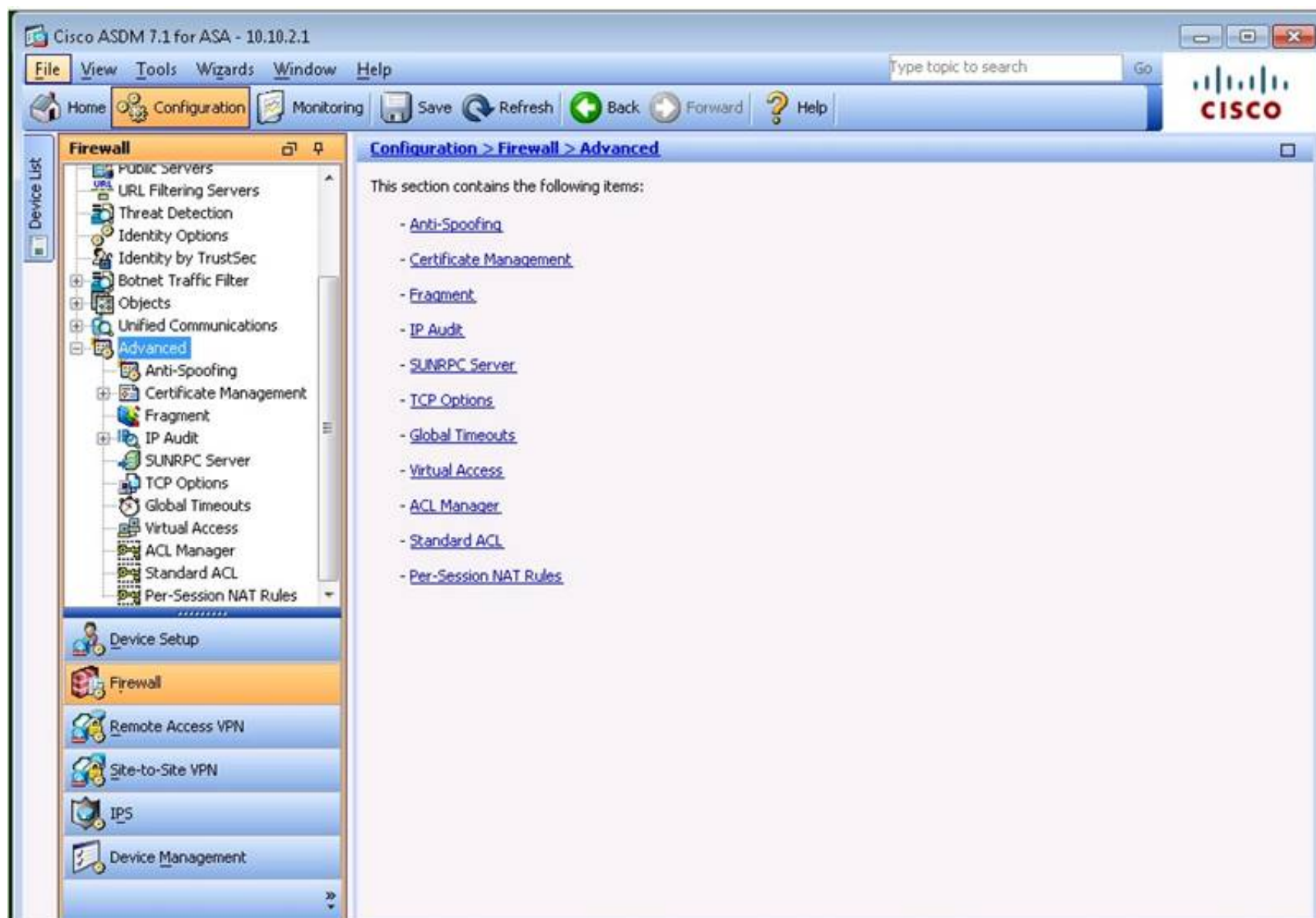
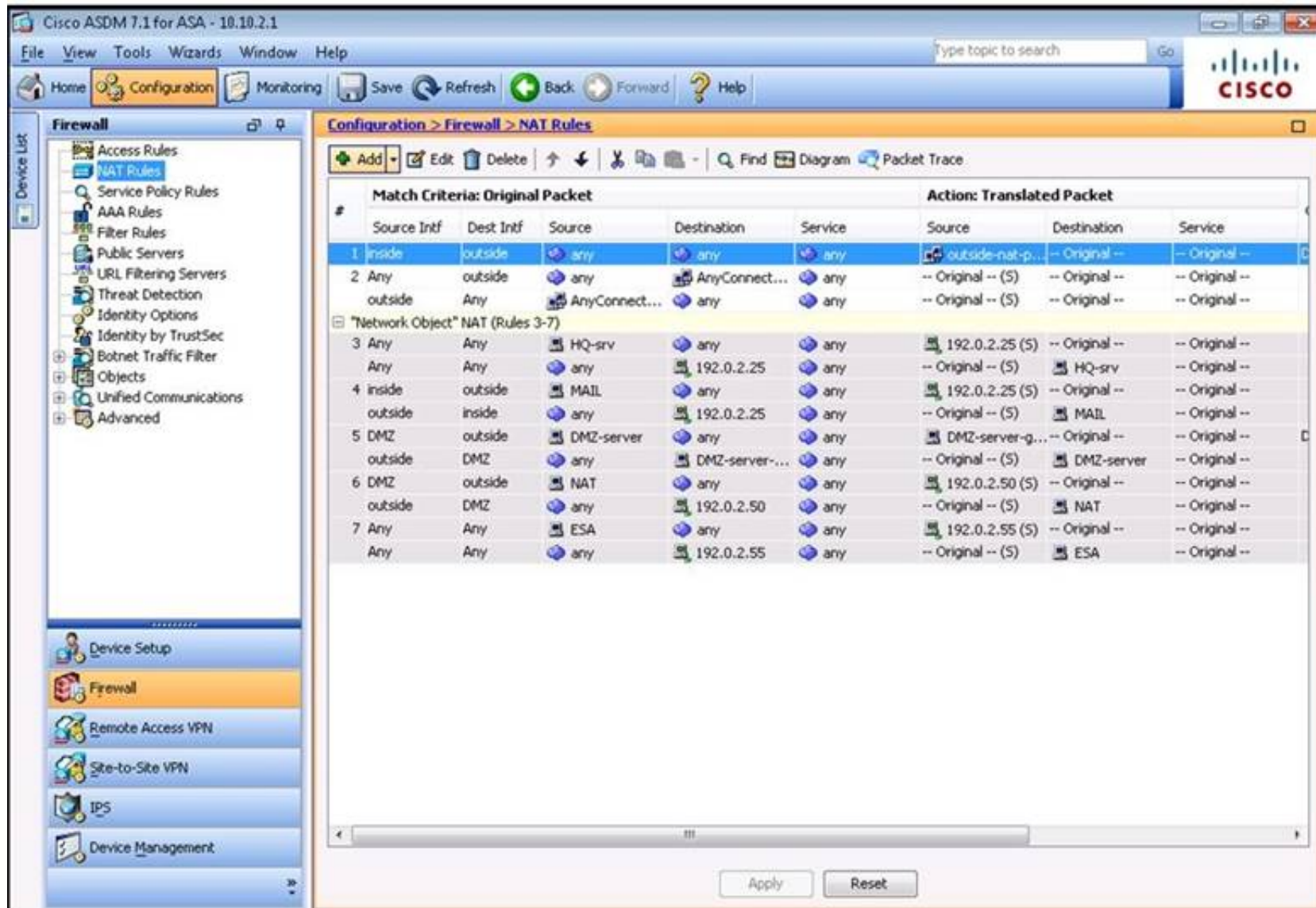
Find:   

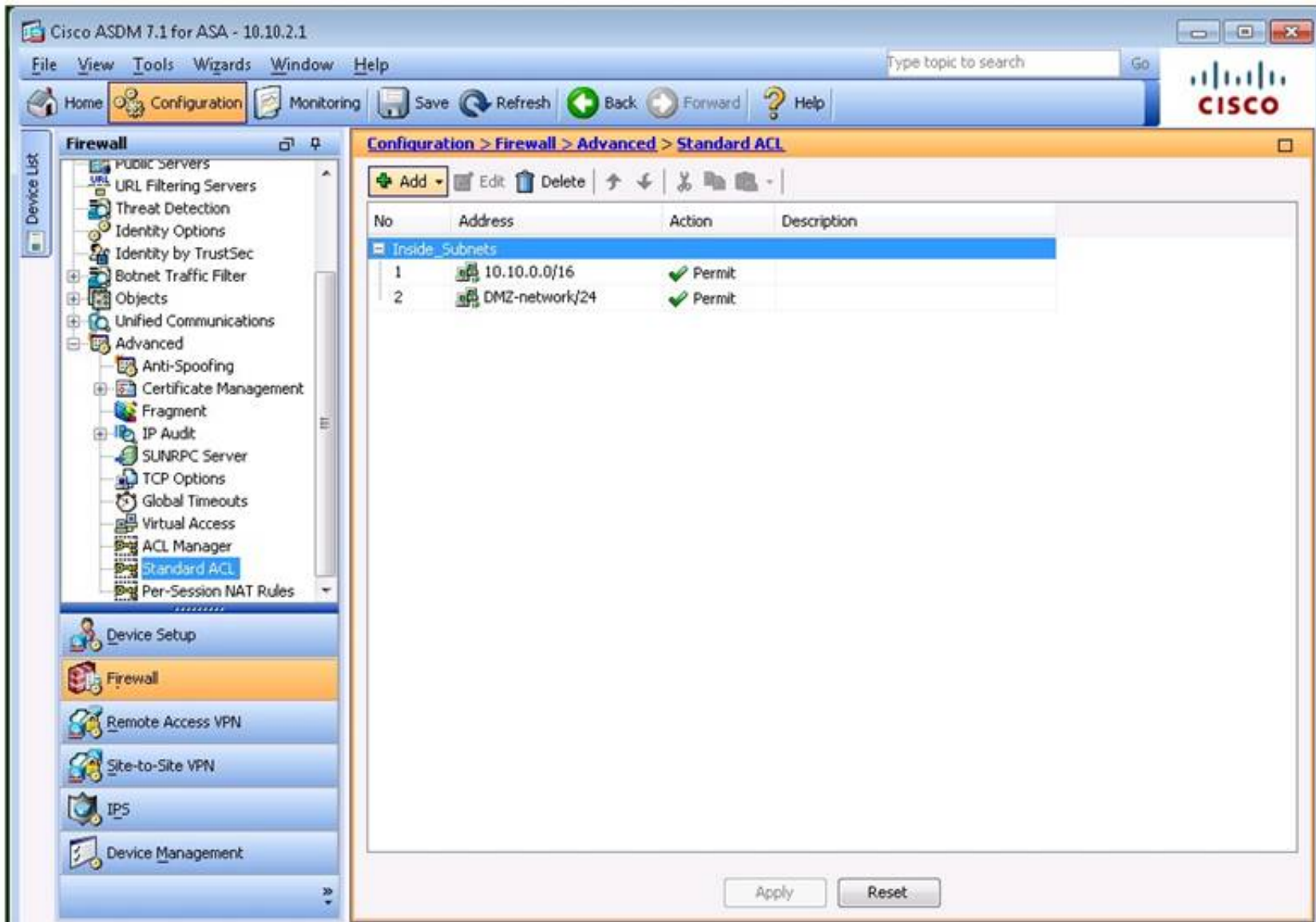
OK Cancel Help












The screenshot shows the Cisco ASDM 7.1 for ASA - 10.10.2.1 interface. The left sidebar contains a 'Device List' and a 'Configuration' tree. The 'Configuration' tree is expanded to 'Firewall > Advanced > Standard ACL'. The main pane displays a table of ACL rules under the heading 'Inside Subnets'.

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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>


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

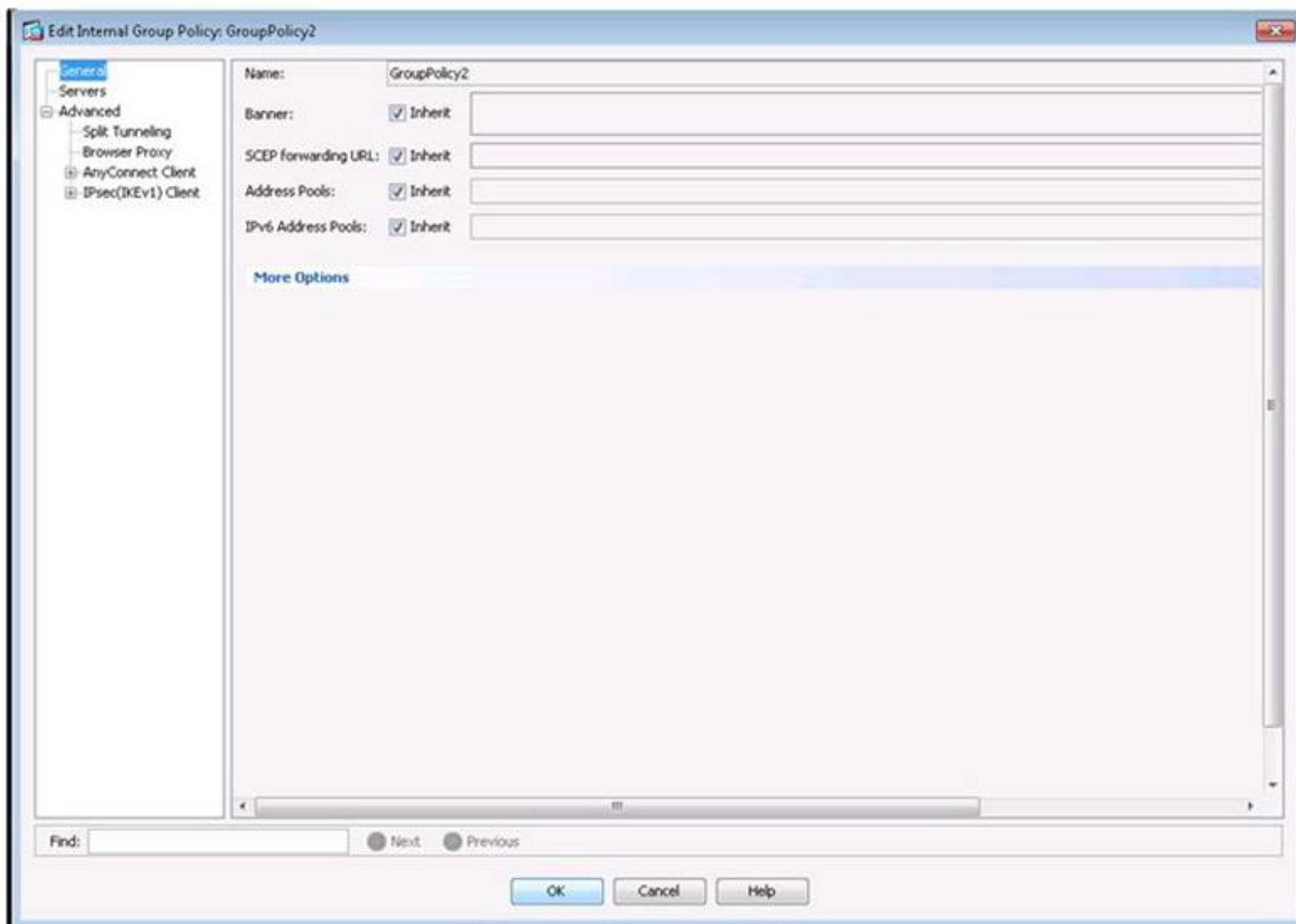
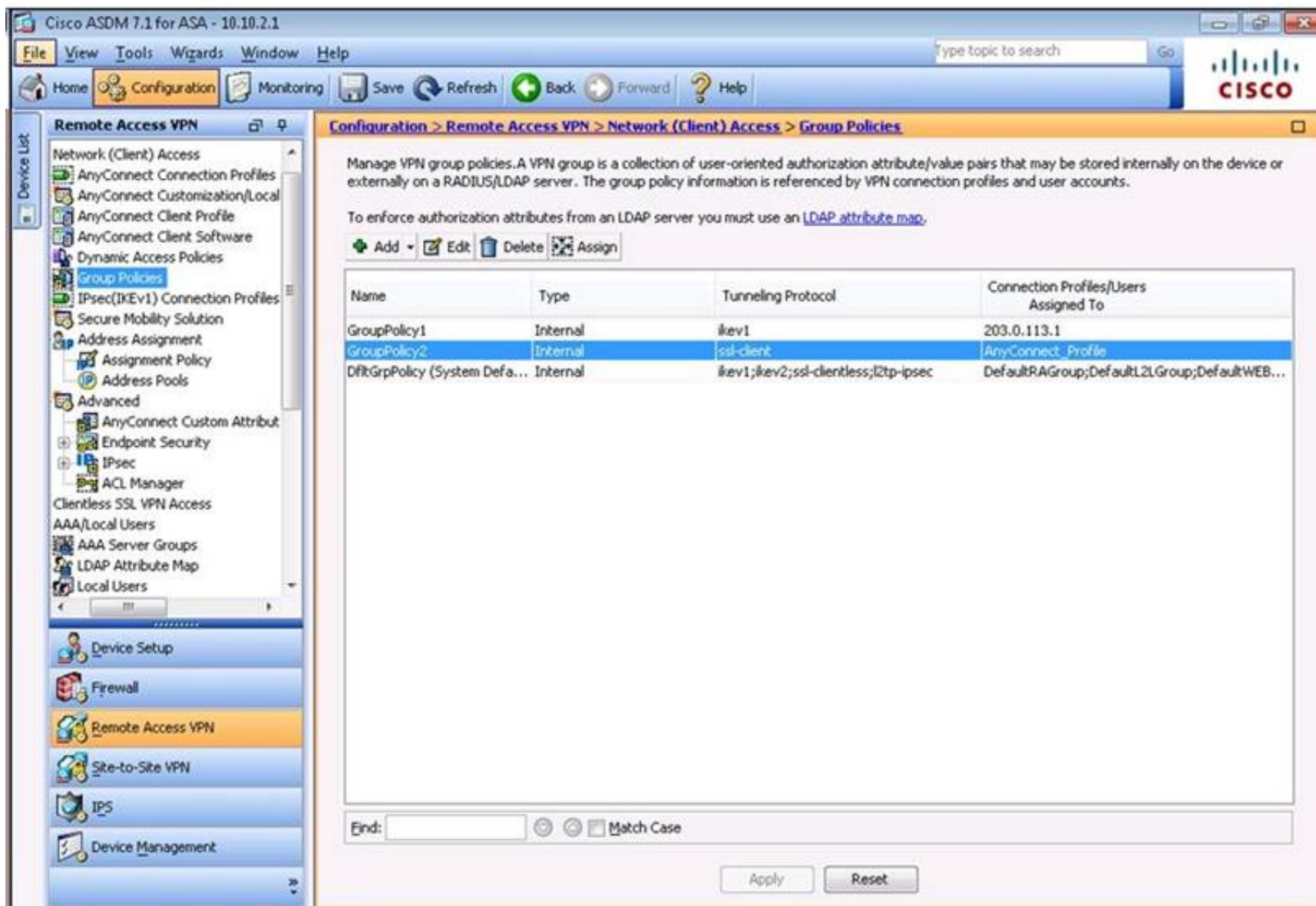
Cancel

Help

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>





**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

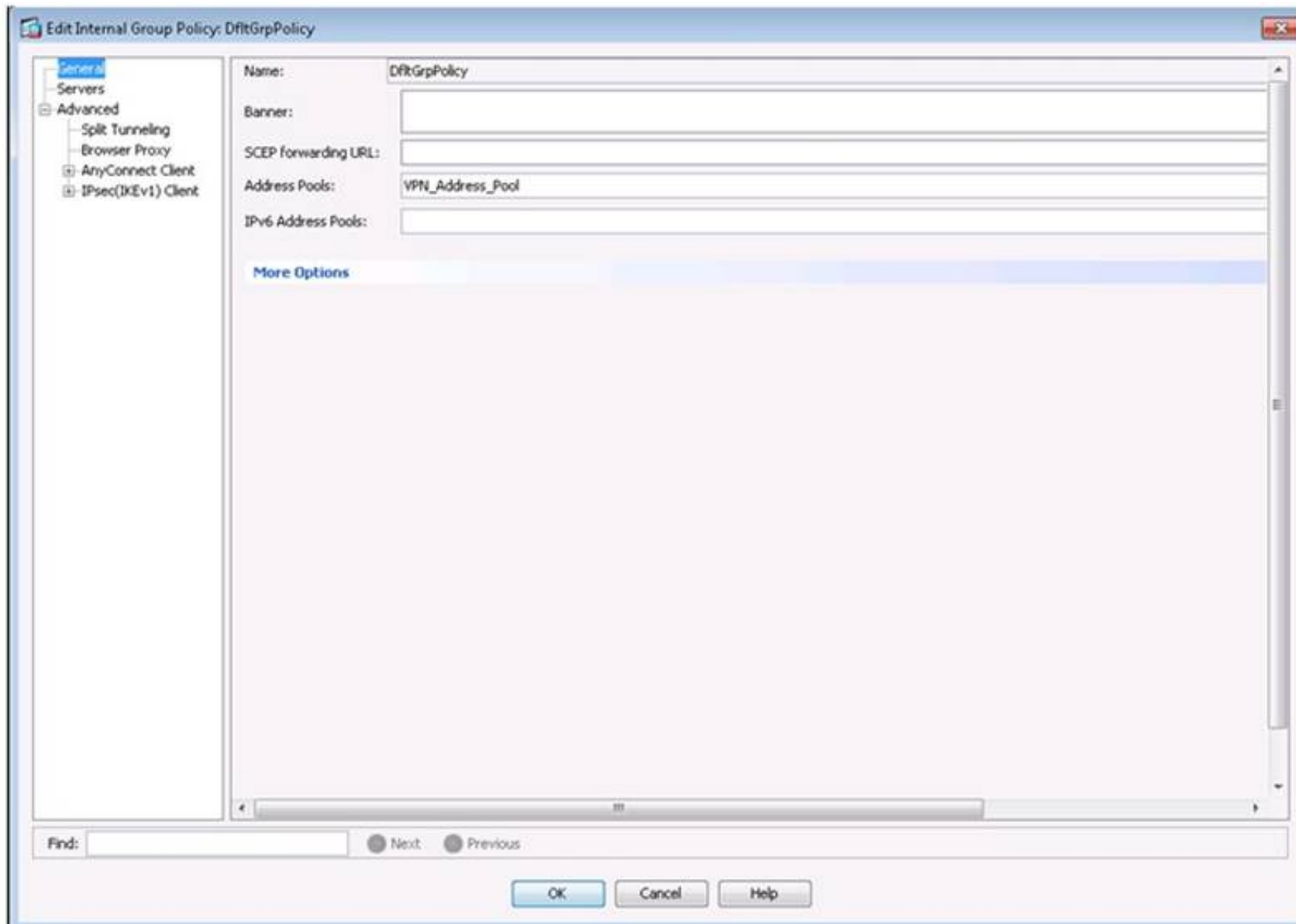
Pressing this button to set up split exclusion for Web Security proxies.  
 Set up split exclusion for Web Se...

Intercept DHCP Configuration Message from Microsoft Clients

Find:  ☐ Next ☐ Previous

OK Cancel Help



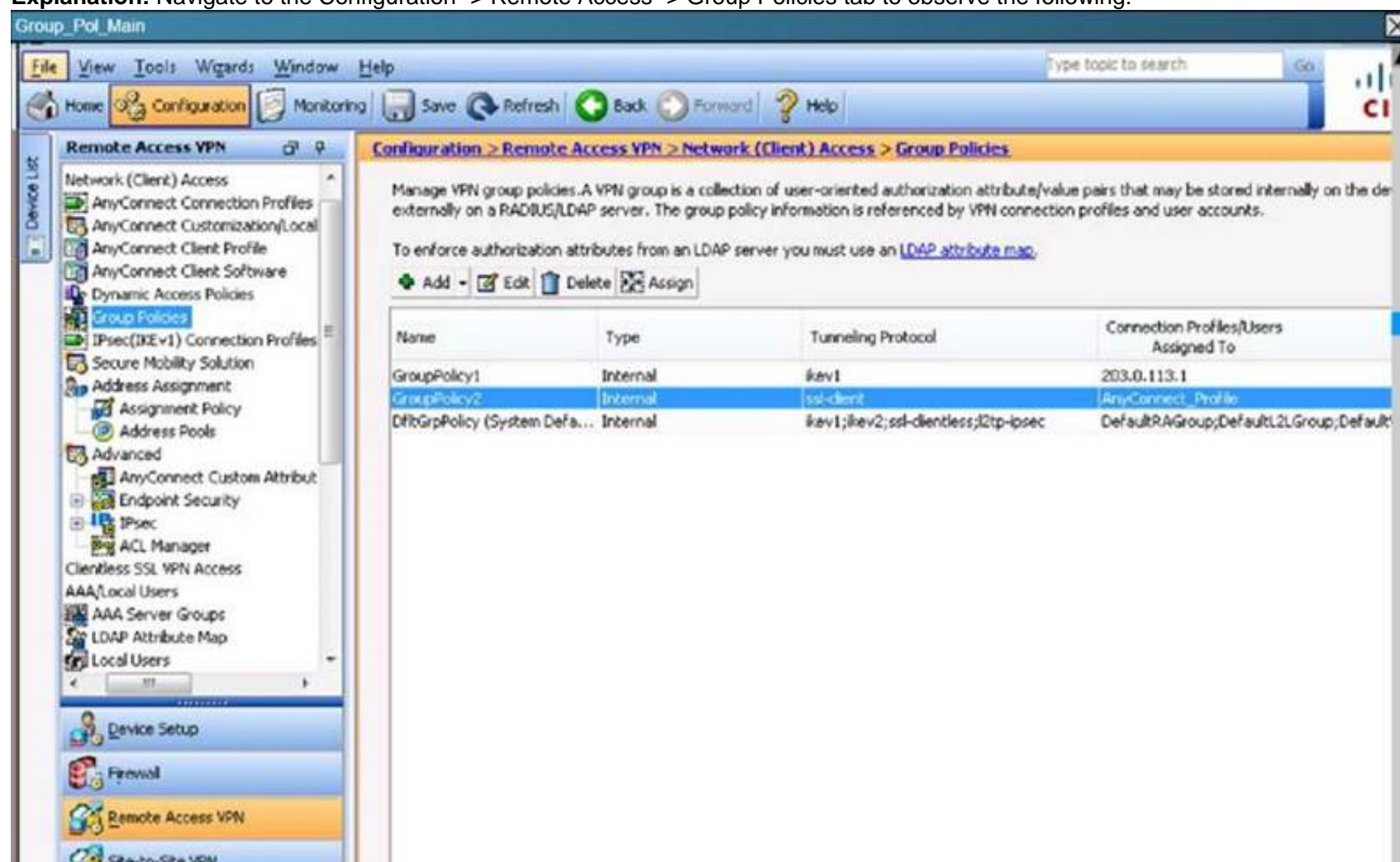


Which two networks will be included in the secured VPN tunnel? (Choose two.)

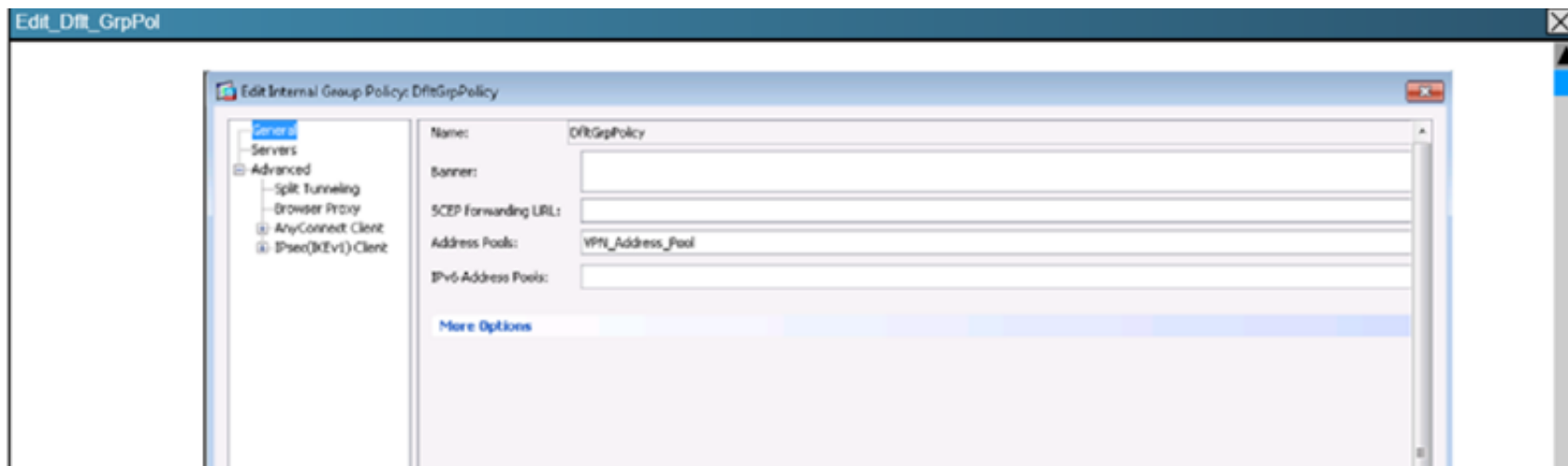
- A. 10.10.0.0/16
- B. All networks will be securely tunneled
- C. Networks with a source of any4
- D. 10.10.9.0/24
- E. DMZ network

**Answer:** AE

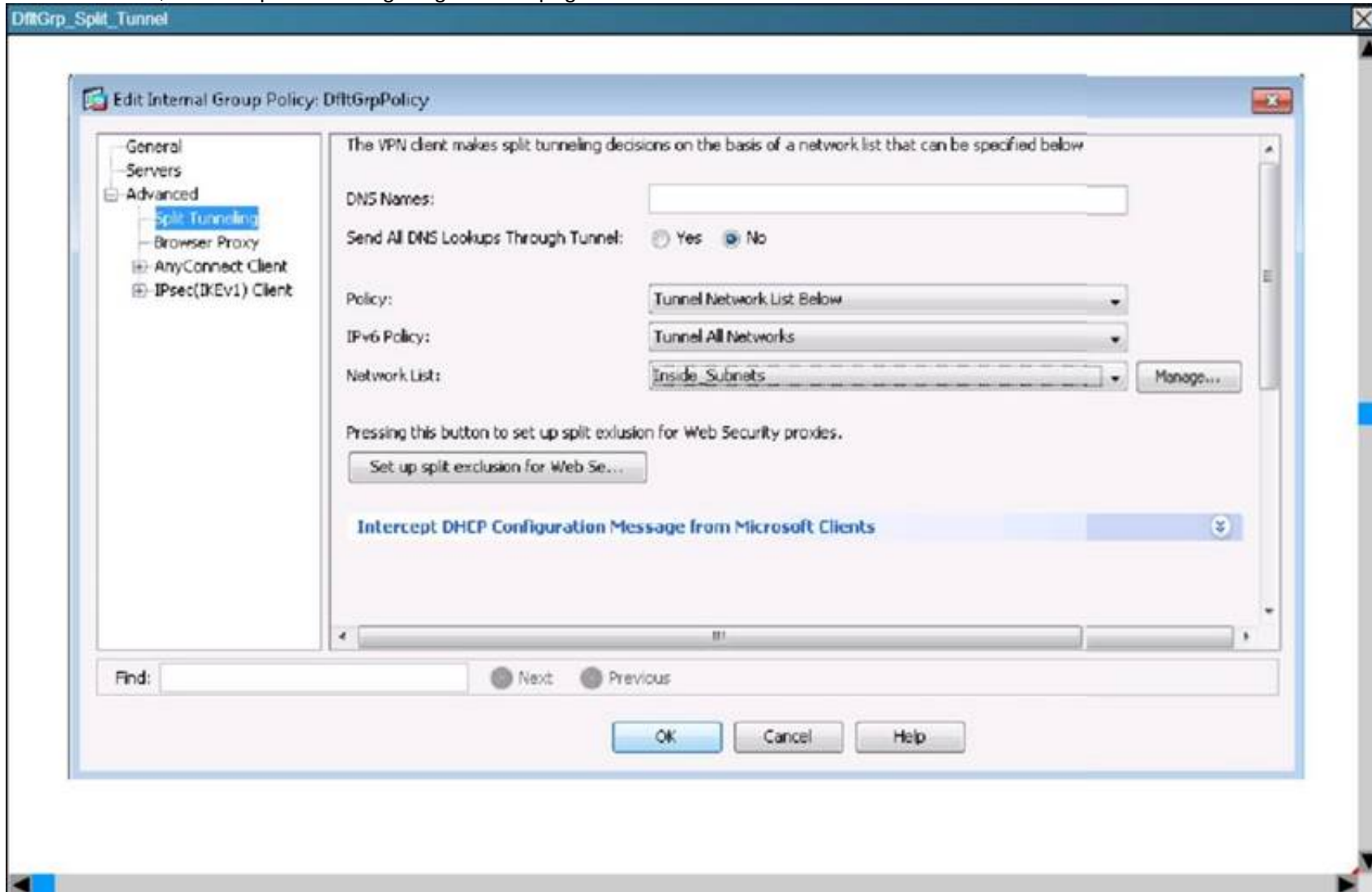
**Explanation:** Navigate to the Configuration -> Remote Access -> Group Policies tab to observe the following:



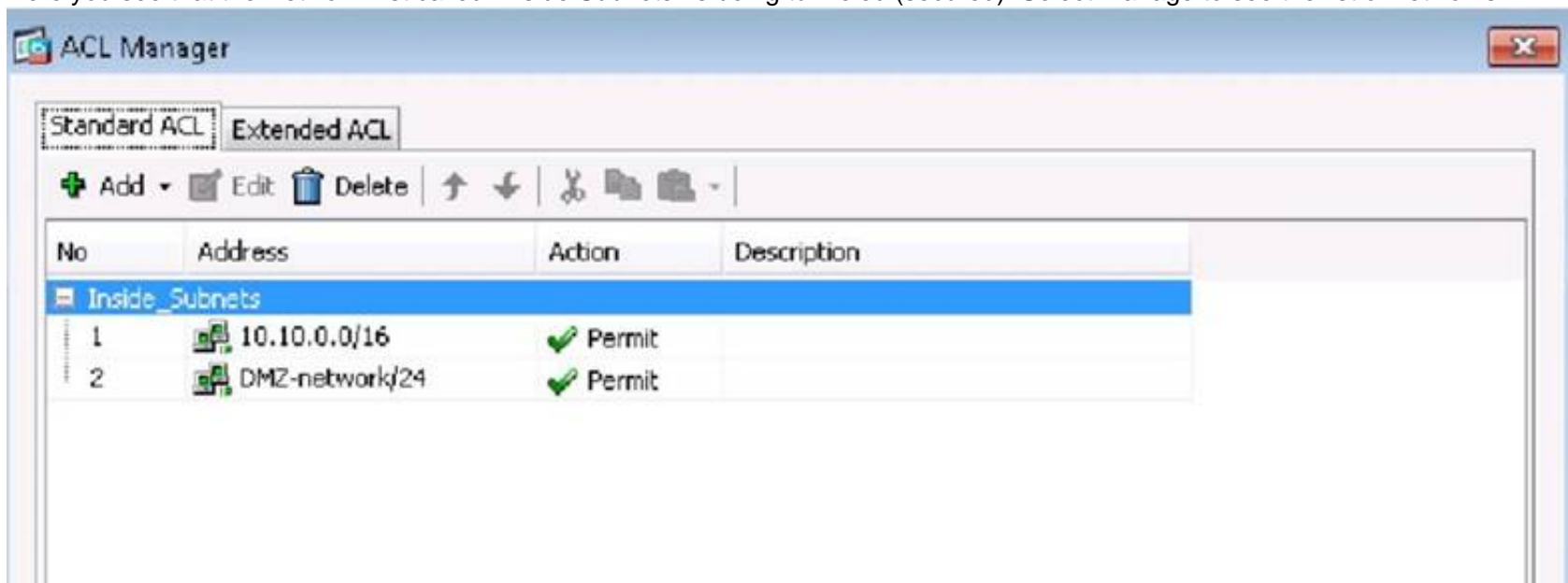
Then, click on the DfltGrpPolicy to see the following:



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 275

Which option describes what address preservation with IPsec Tunnel Mode allows when GETVPN is used?

- A. stronger encryption methods
- B. Network Address Translation of encrypted traffic
- C. traffic management based on original source and destination addresses
- D. Tunnel Endpoint Discovery

**Answer: C**

#### NEW QUESTION 277

Which two are features of GETVPN but not DMVPN and FlexVPN? (Choose two.)



- A. one IPsec SA for all encrypted traffic
- B. no requirement for an overlay routing protocol
- C. design for use over public or private WAN
- D. sequence numbers that enable scalable replay checking
- E. enabled use of ESP or AH
- F. preservation of IP protocol in outer header

**Answer:** AB

#### NEW QUESTION 280

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 284

Refer to the exhibit.

```
crypto ikev2 name-mangler GET_NAME
email username
```

Which technology is represented by this configuration?

- A. AAA for FlexVPN
- B. AAA for EzVPN
- C. TACACS+ command authorization
- D. local command authorization

**Answer:** A

#### NEW QUESTION 286

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 290

Refer to the exhibit.

XML profile

```
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
```

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 295

Which feature is enabled by the use of NHRP in a DMVPN network?

- A. host routing with Reverse Route Injection
- B. BGP multiaccess
- C. host to NBMA resolution
- D. EIGRP redistribution

**Answer:** C

#### NEW QUESTION 296

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 301

Which option is one component of a Public Key Infrastructure?

- A. the Registration Authority
- B. Active Directory
- C. RADIUS
- D. TACACS+

**Answer:** A

#### NEW QUESTION 303

What URL do you use to download a packet capture file in a format which can be used by a packet analyzer?

- A. ftp://<hostname>/capture/<capture\_name>/
- B. https://<asdm\_enabled\_interface:port>/<capture\_name>/
- C. https://<asdm\_enabled\_interface:port>/admin/capture/<capture\_name>/pcap
- D. https://<hostname>/<capture\_name>/pcap

**Answer:** C

#### NEW QUESTION 308

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 309

Which option is a required element of Secure Device Provisioning communications?

- A. the introducer
- B. the certificate authority
- C. the requestor
- D. the registration authority

**Answer:** A

#### NEW QUESTION 312

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.

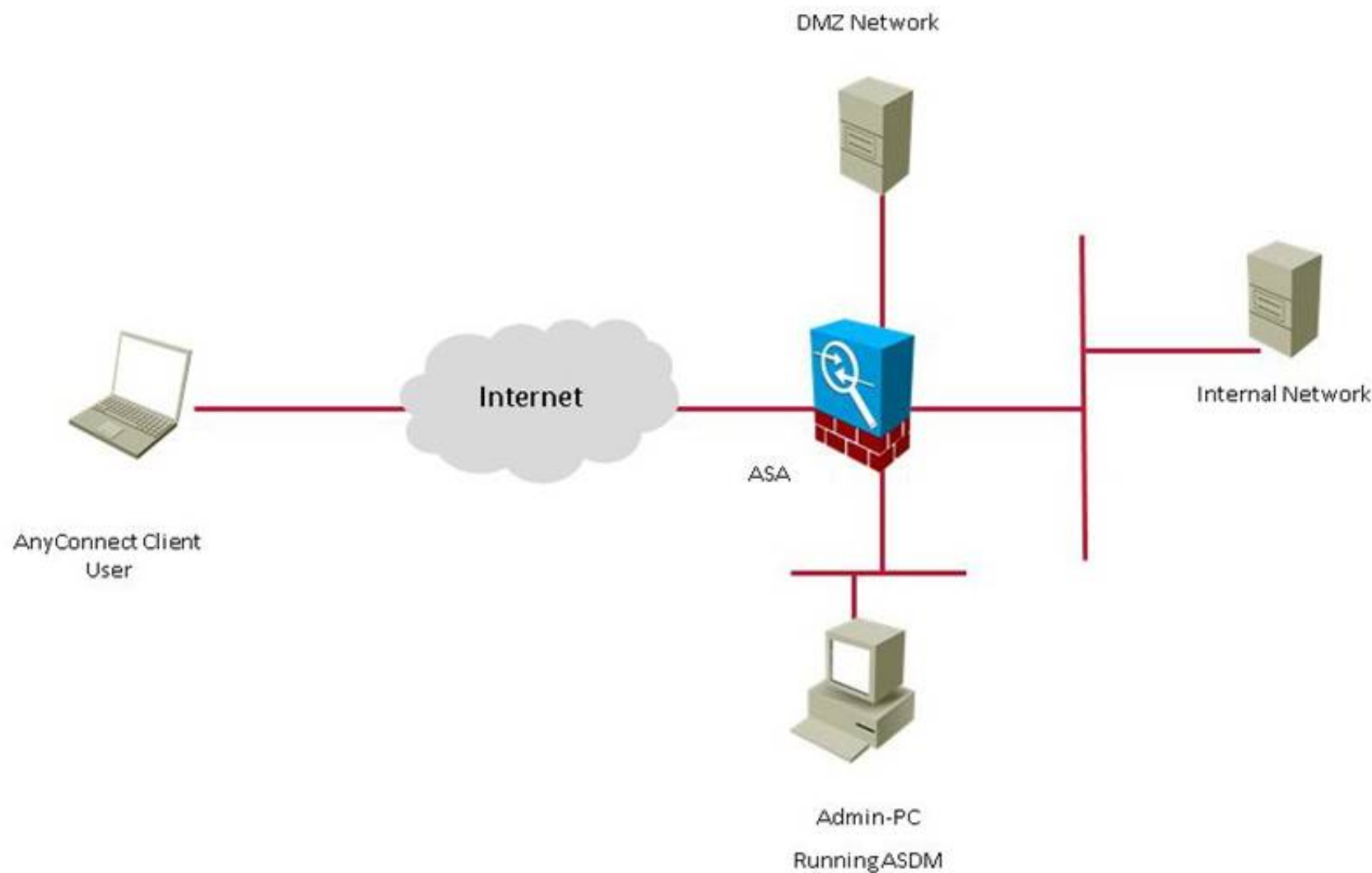
##### Instructions



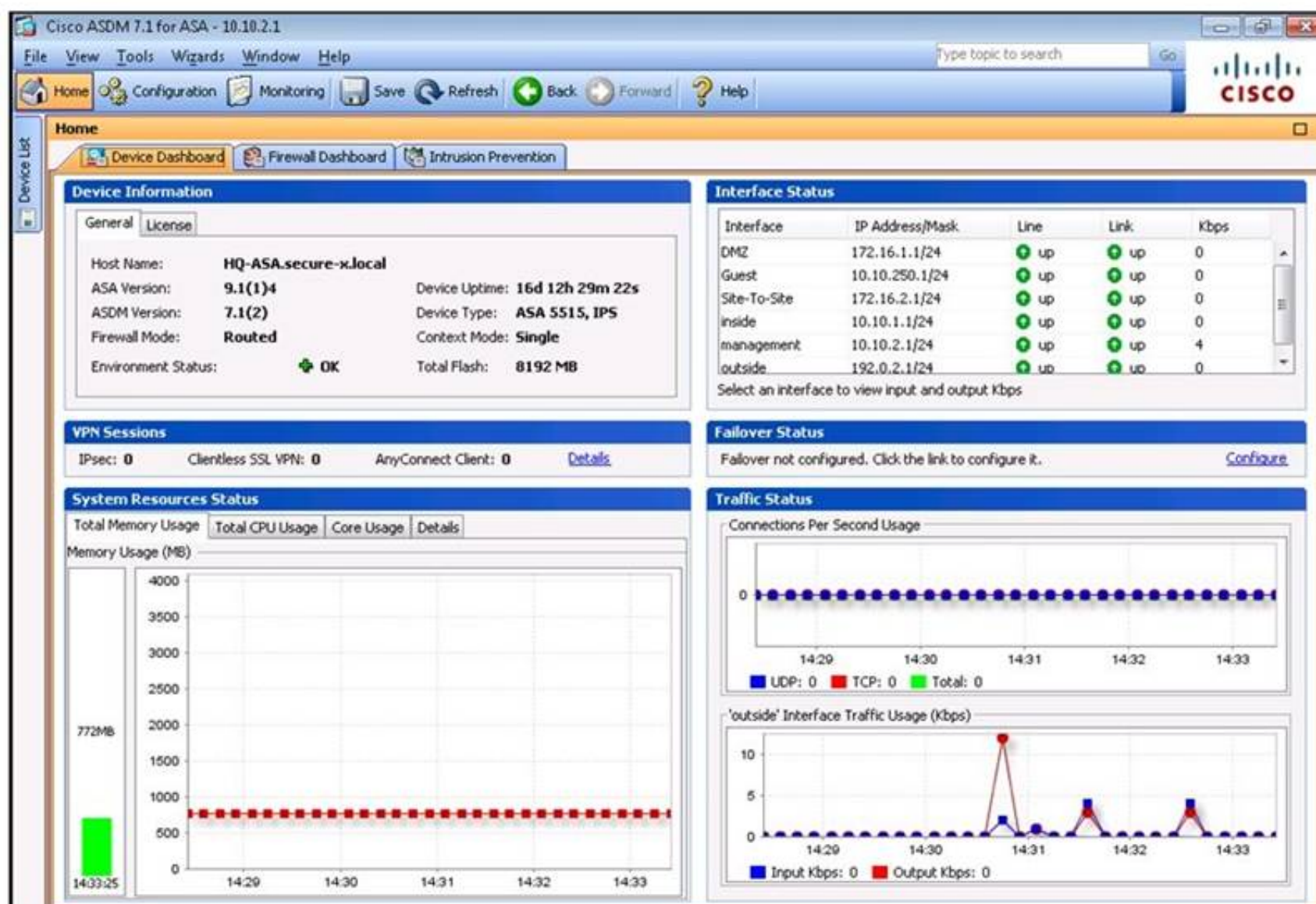
- Navigate the ASDM GUI on the device to verify network operation and answer for multiple-choice questions.
- You may have to use the scroll bars to view the entire ASDM Configuration screens.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- **NOT ALL SCREENS AND SELECTIONS ARE AVAILABLE FOR 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.

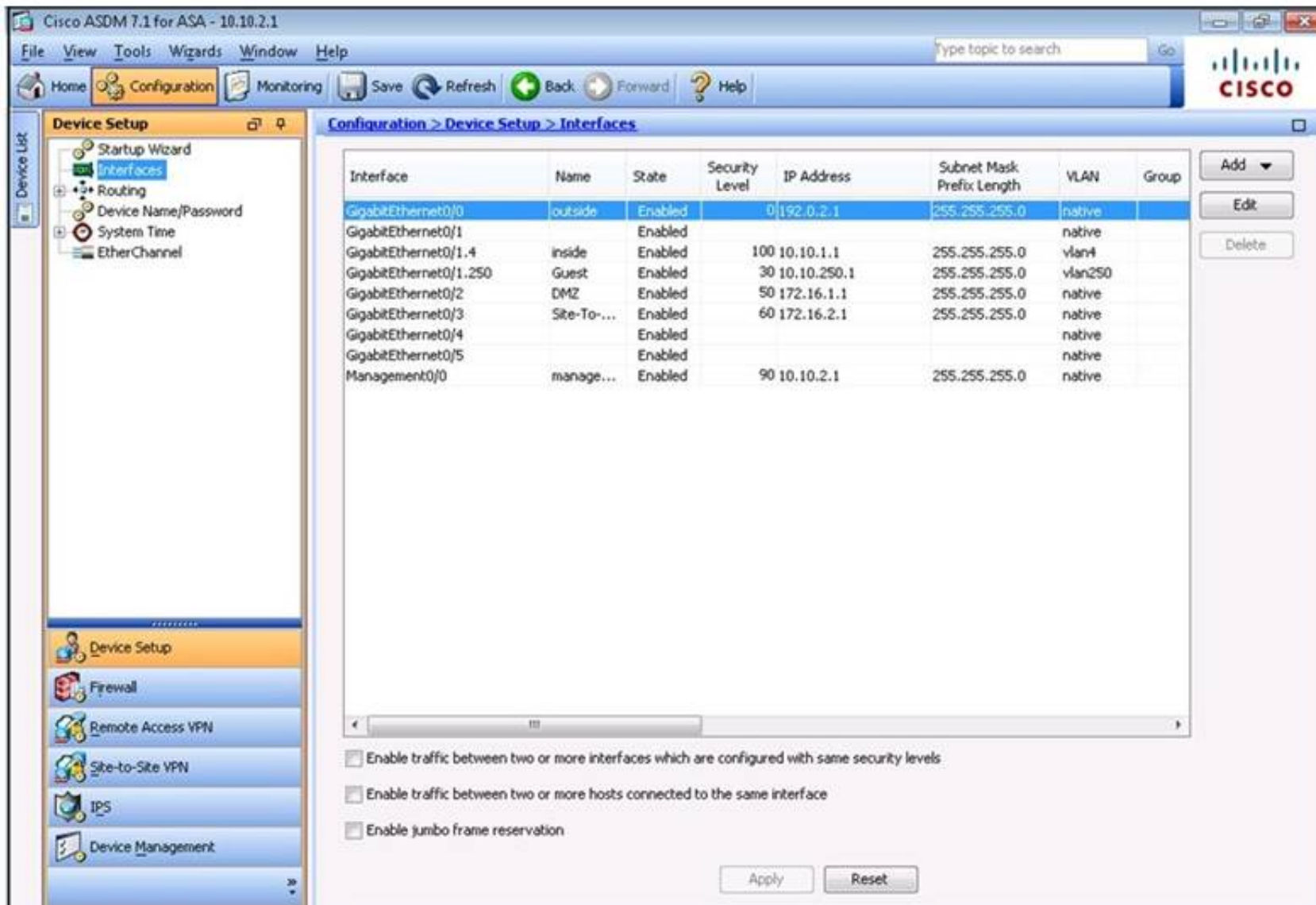
Topology





Default\_Home



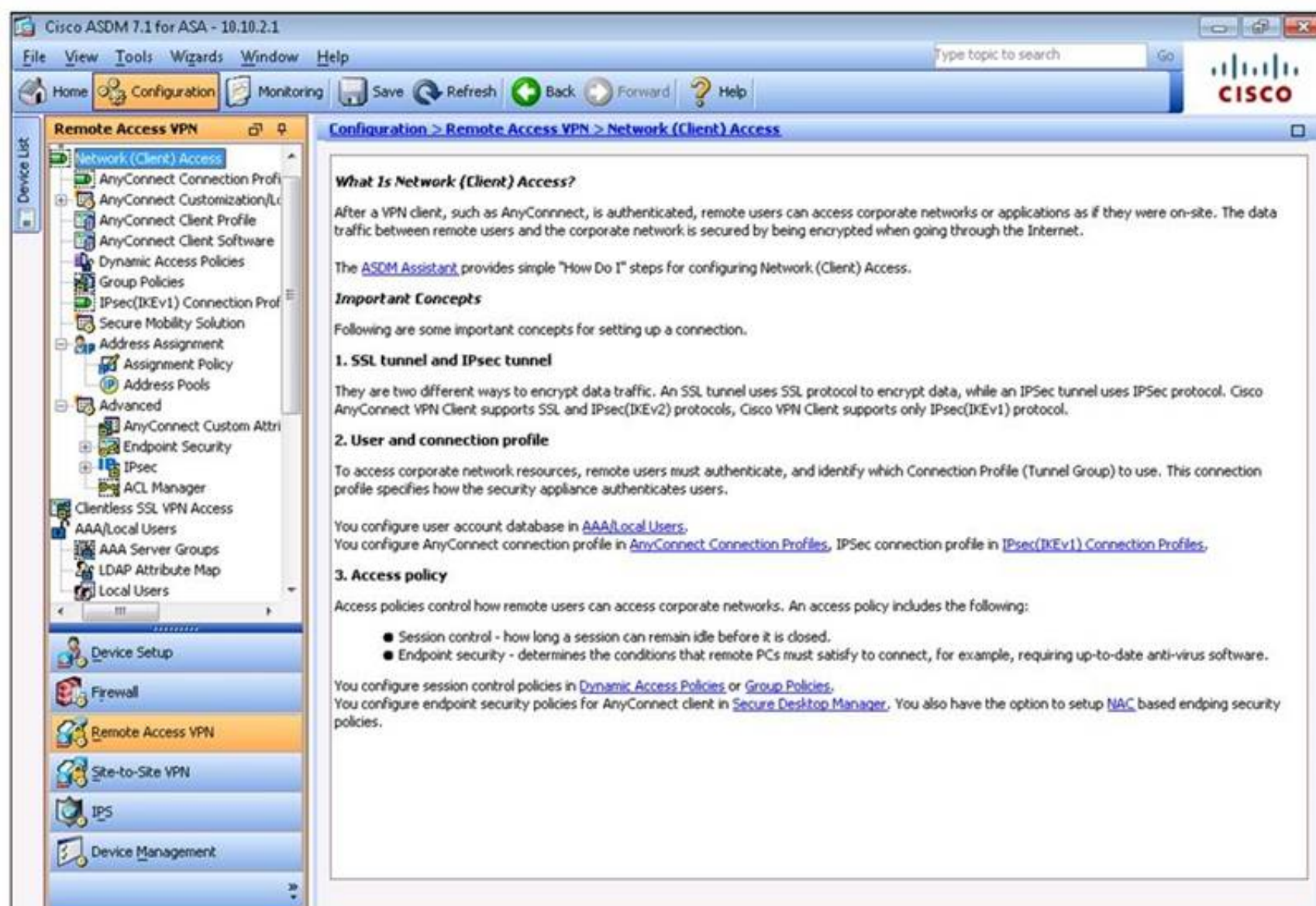


**Configuration > Device Setup > Interfaces**

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](#).

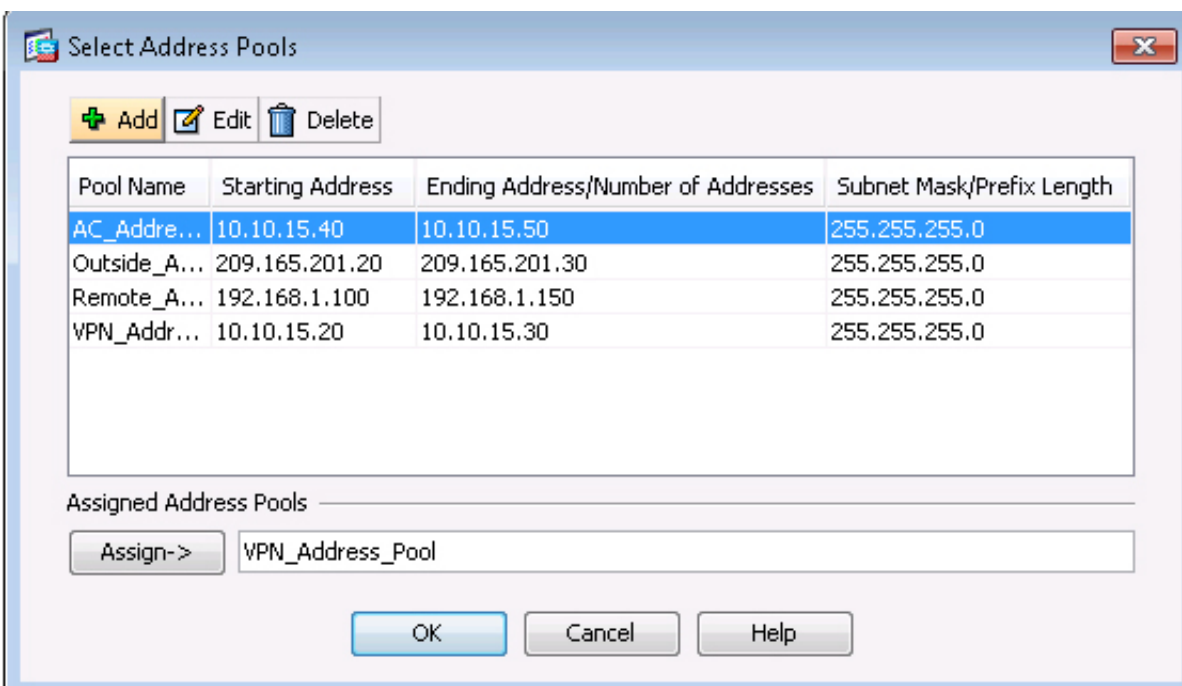
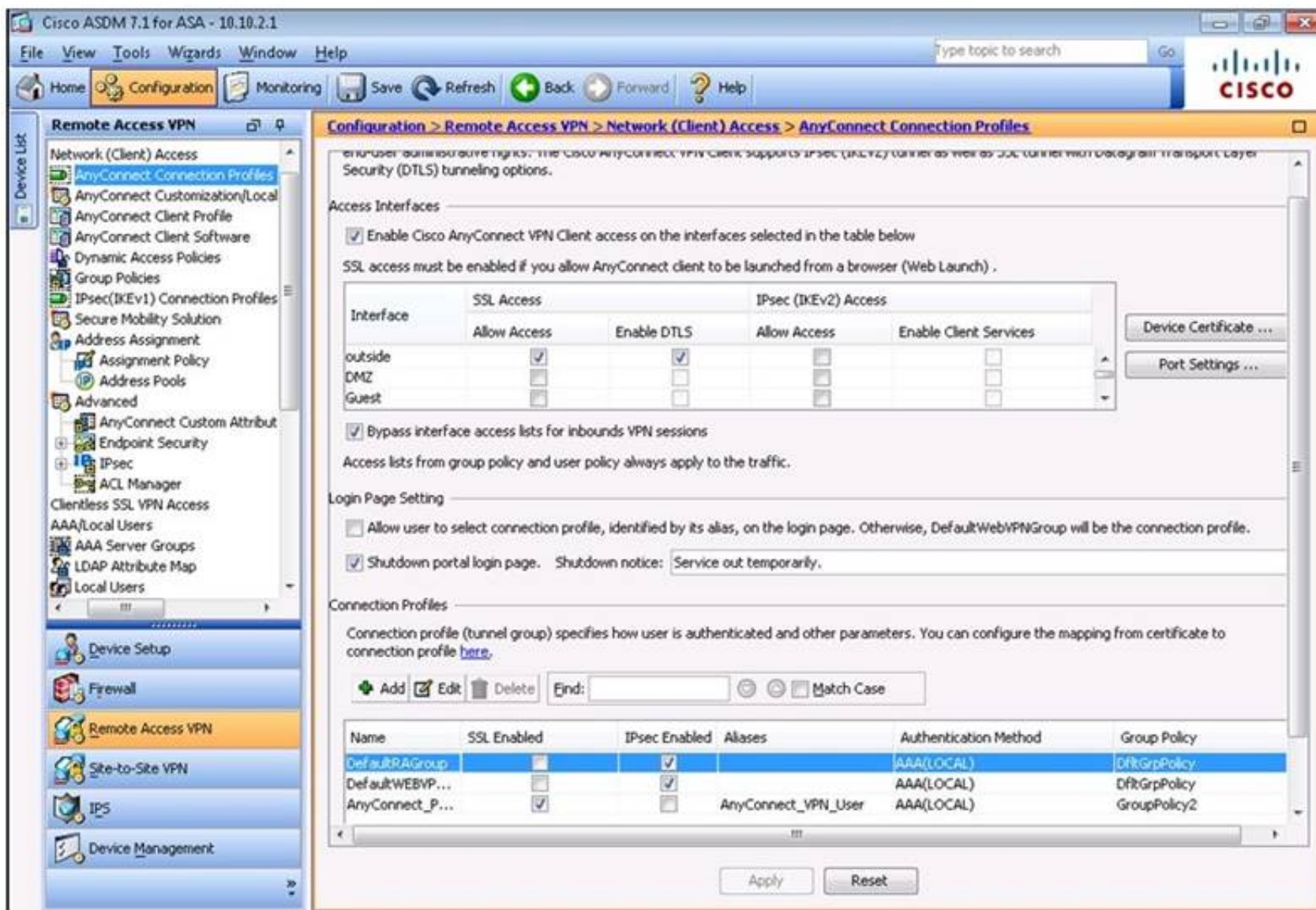
**3. Access policy**

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.







**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

**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**  
 Access Rules  
 NAT Rules  
 Service Policy Rules  
 AAA Rules  
 Filter Rules  
 Public Servers  
 URL Filtering Servers  
 Threat Detection  
 Identity Options  
 Identity by TrustSec  
 Botnet Traffic Filter  
 Objects  
 Unified Communications  
 Advanced

**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	
<b>in (3 incoming rules)</b>						
<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
<b>est (1 implicit incoming rule)</b>						
	any			Any less secure ne...		ip
<b>e-To-Site (1 implicit incoming rule)</b>						
	any			Any less secure ne...		ip
<b>ide (1 implicit incoming rule)</b>						
	any			Any less secure ne...		ip
<b>inagement (1 implicit incoming rule)</b>						
	any			Any less secure ne...		ip
<b>tside (6 incoming rules)</b>						
<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
<b>lobal (1 implicit rule)</b>						
	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

#	Enabled	Source	User	Security Group	Destination	Security
<b>DMZ_access_in</b>						
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	
<b>outside_access_in</b>						
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	
<b>outside_cryptomap</b>						
1	<input checked="" type="checkbox"/>	10.10.9.0/24			10.11.11.0/24	
<b>permit-all</b>						
1	<input checked="" type="checkbox"/>	any			any	

Collapse All Expand All

Apply Reset

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

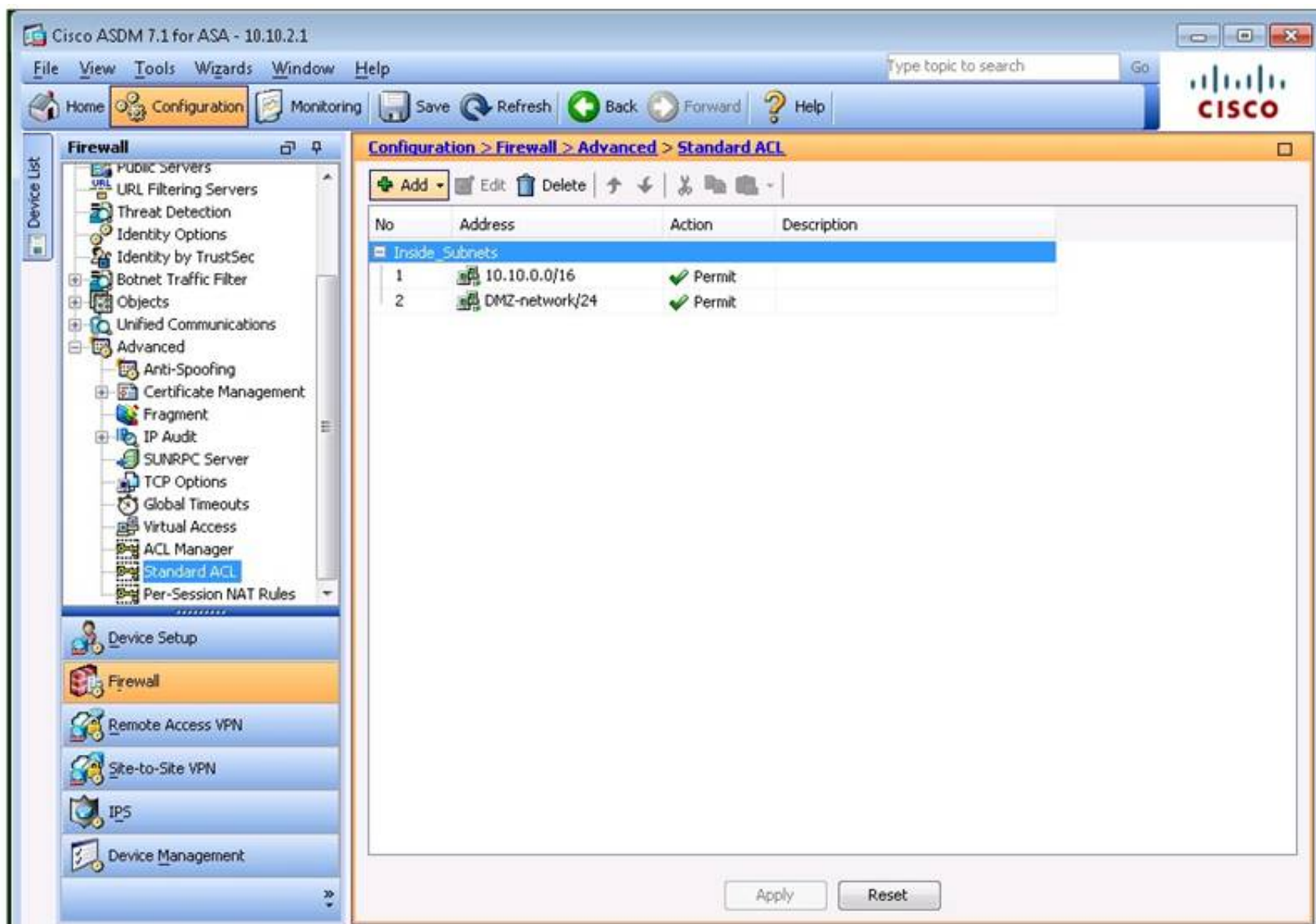
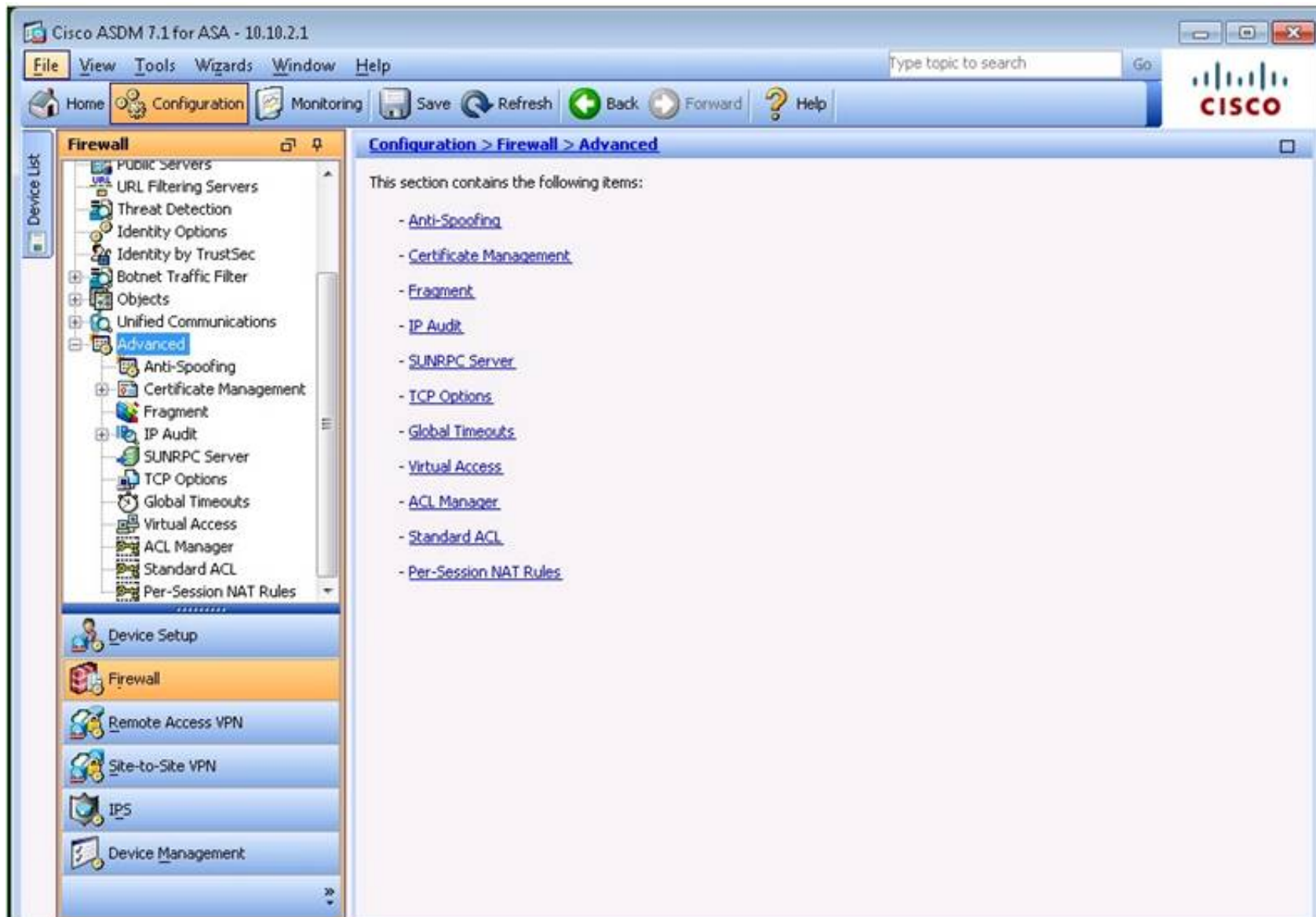
Firewall

Configuration > Firewall > NAT Rules


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 --
<b>"Network Object" NAT (Rules 3-7)</b>								
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 --

Apply Reset







 Edit NAT Rule

Match Criteria: Original Packet

Source Interface: 
 Destination Interface:

Source Address: 
 Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: 
 Destination Address:

☐ Use one-to-one address translation

☒ PAT Pool Translated Address: 
 Service:

☐ 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:

Description:

 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

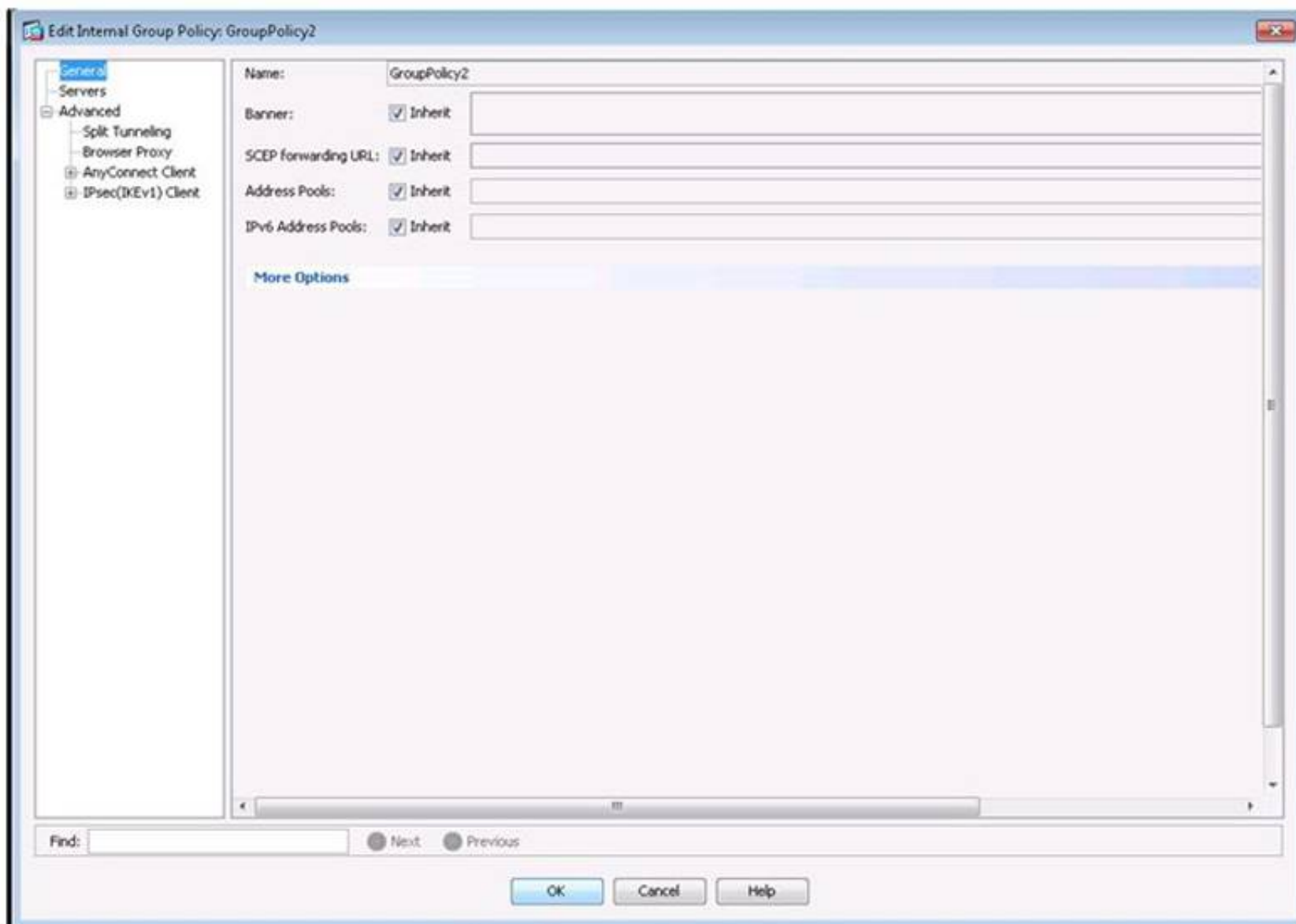
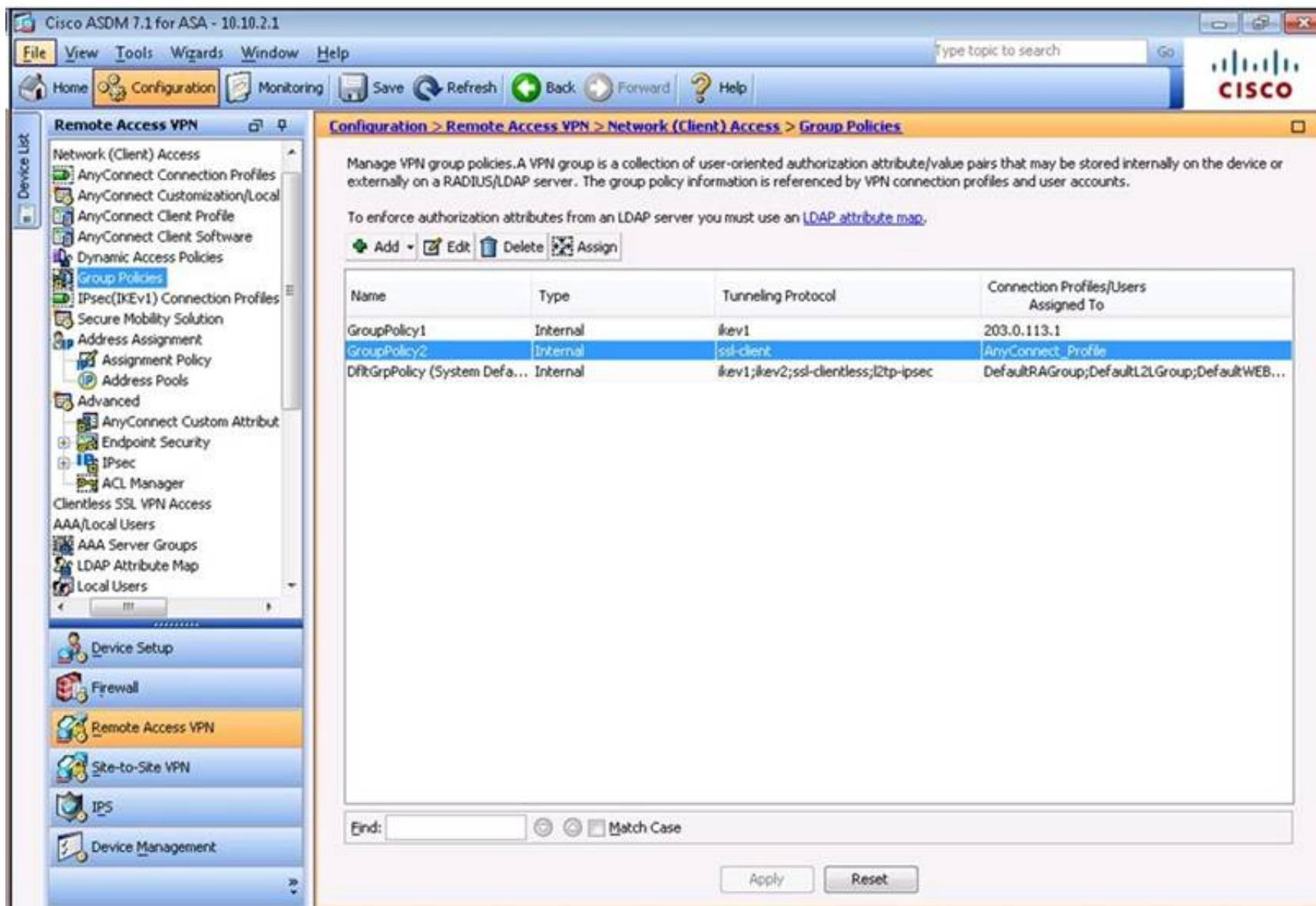
Description:

OK

Cancel

Help





**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

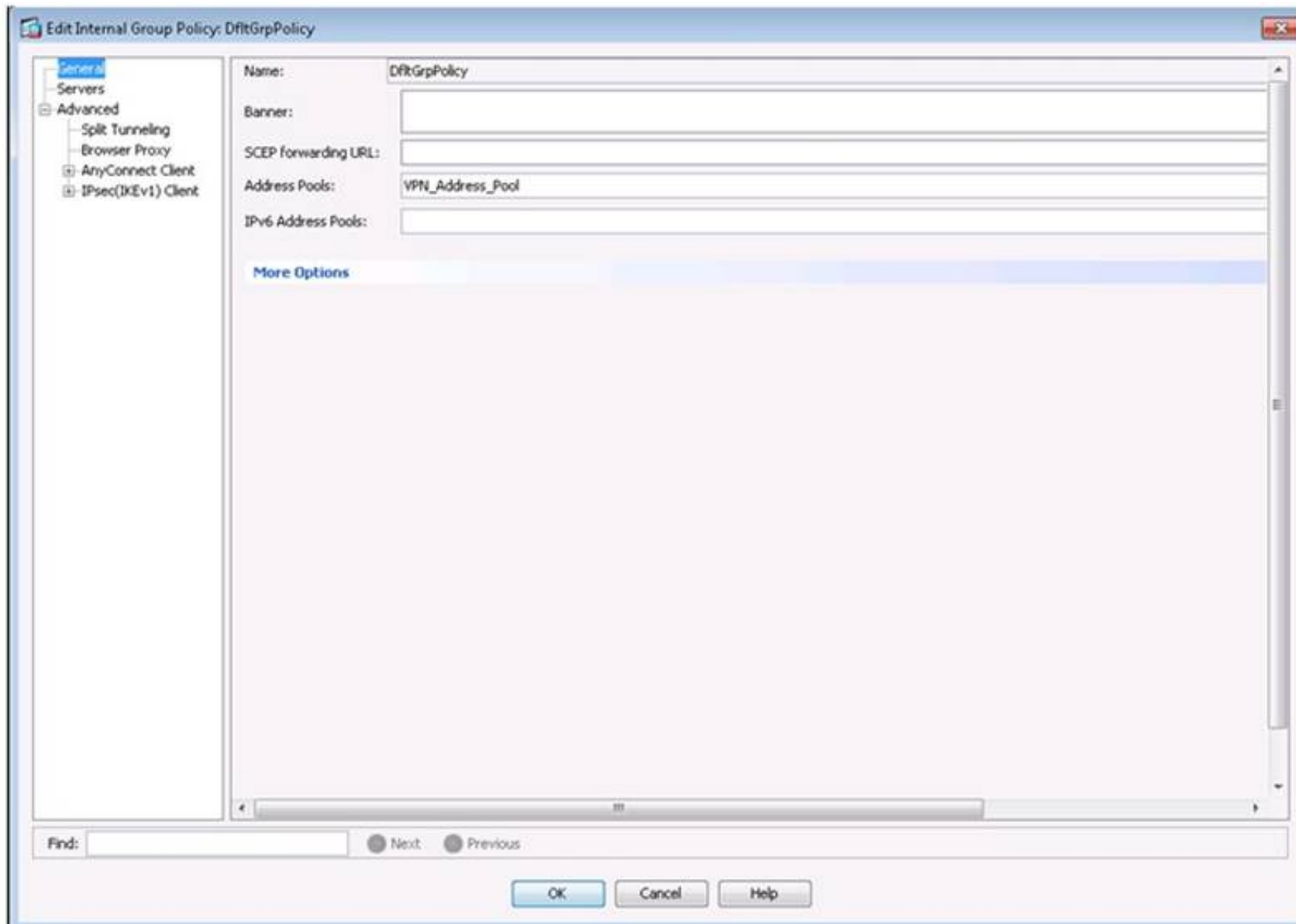
Pressing this button to set up split exclusion for Web Security proxies.  
 Set up split exclusion for Web Se...

Intercept DHCP Configuration Message from Microsoft Clients

Find:  ☐ Next ☐ Previous

OK Cancel Help



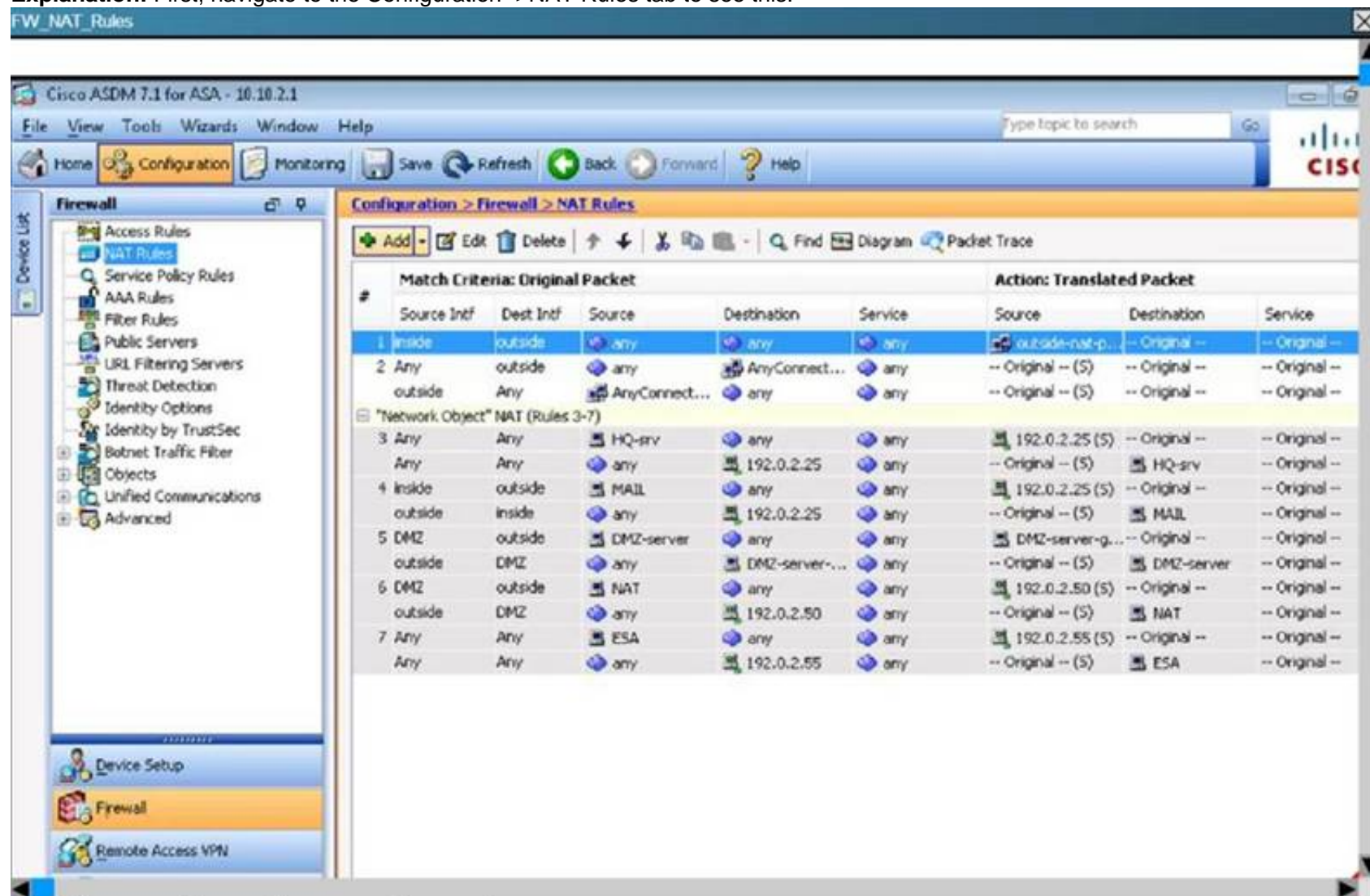


What two actions will be taken on translated packets when the AnyConnect users connect to the ASA? (Choose two.)

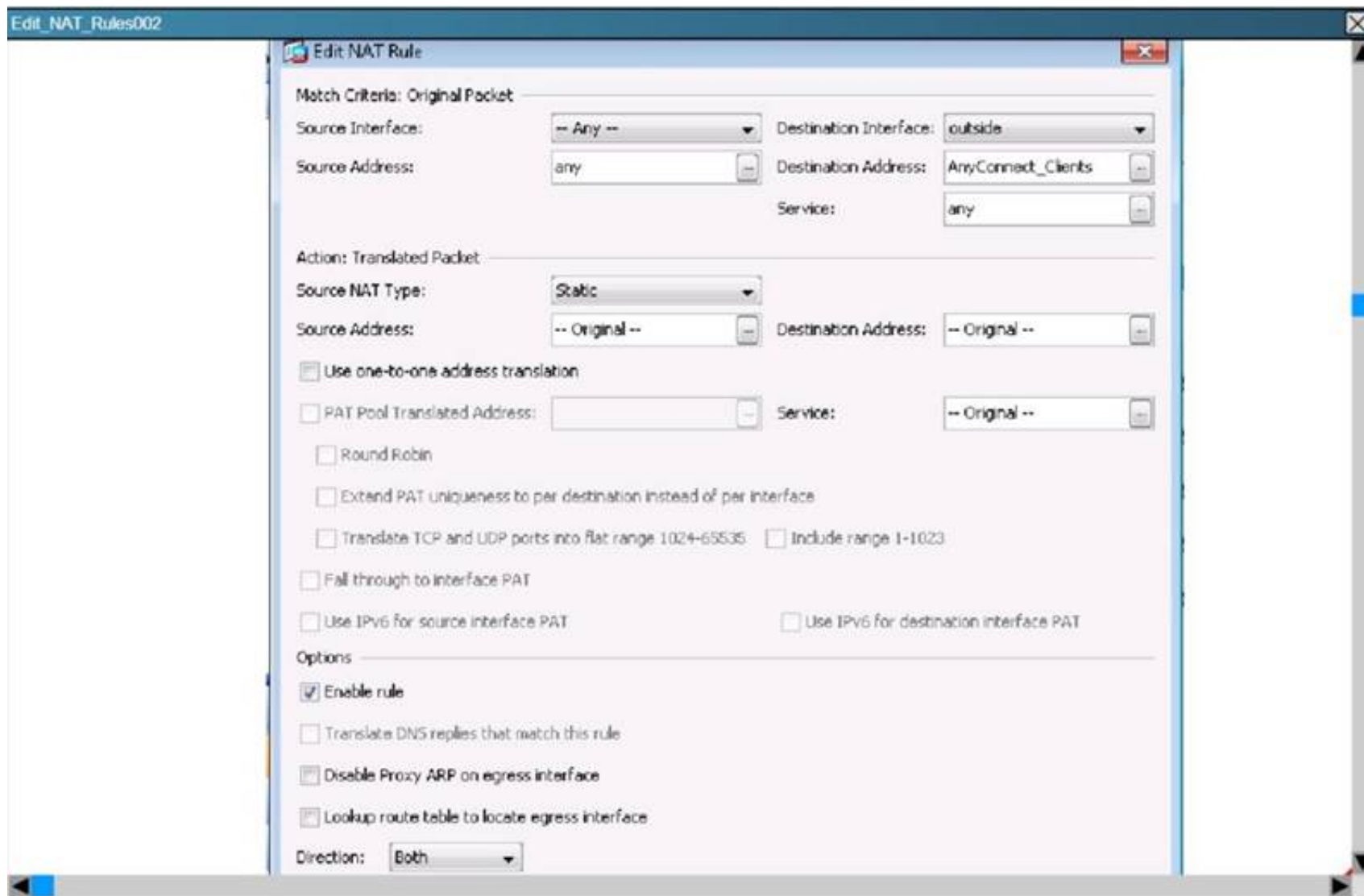
- A. No action will be taken, they will keep their original assigned addresses
- B. The source address will use the outside-nat-pool
- C. The source NAT type will be a static translation
- D. The source NAT type will be a dynamic translation
- E. DNS will be translated on rule matches

**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 315

You have deployed new Cisco AnyConnect start before logon modules and set the configuration to download modules before logon, but all client connections continue to use the previous version of the module. Which action must you take to correct the problem?

- A. Configure start before logon in the client profile.
- B. Configure a group policy to prompt the user to download the updated module.
- C. Define the modules for download in the client profile.
- D. Define the modules for download in the group policy.

**Answer: A**

#### NEW QUESTION 316

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

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

**Answer: B**

#### NEW QUESTION 317

If Web VPN bookmarks are grayed out on the home screen, which action should you take to begin troubleshooting?

- A. Determine whether the Cisco ASA can resolve the DNS names.
- B. Determine whether the Cisco ASA has DNS forwarders set up.
- C. Determine whether an ACL is present to permit DNS forwarding.
- D. Replace the DNS name with an IP address.

**Answer: A**

#### NEW QUESTION 319

Which technology is FlexVPN based on?

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

**Answer: C**

#### NEW QUESTION 321



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 323

Which command clears all Cisco AnyConnect VPN sessions?

- A. vpn-sessiondb logoff anyconnect
- B. vpn-sessiondb logoff webvpn
- C. vpn-sessiondb logoff l2l
- D. clear crypto isakmp sa

**Answer: A**

#### NEW QUESTION 324

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 328

Where do you configure AnyConnect certificate-based authentication in ASDM?

- A. group policies
- B. AnyConnect Connection Profile
- C. AnyConnect Client Profile
- D. Advanced Network (Client) Access

**Answer: B**

#### NEW QUESTION 332

Refer to the exhibit.

```
tunnel-group IKEV2 type remote-access
tunnel-group IKEV2 general-attributes
  address-pool split
  default-group-policy GroupPolicy1
tunnel-group IKEV2 webvpn-attributes
  group-alias ikev2 enable

- <HostEntry>
<HostName>ikev2</HostName>
<HostAddress>10.106.45.221</HostAddress>
<UserGroup>ikev2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```

The customer can establish an AnyConnect connection on the first attempt only. Subsequent attempts fail. What might be the issue?

- A. IKEv2 is blocked over the path.
- B. UserGroup must be different than the name of the connection profile.
- C. The primary protocol should be SSL.
- D. UserGroup must be the same as the name of the connection profile.

**Answer:** D

#### NEW QUESTION 333

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 334

On which Cisco platform are dynamic virtual template interfaces available?

- A. Cisco Adaptive Security Appliance 5585-X
- B. Cisco Catalyst 3750X
- C. Cisco Integrated Services Router Generation 2
- D. Cisco Nexus 7000

**Answer:** C

#### NEW QUESTION 339

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 341

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.

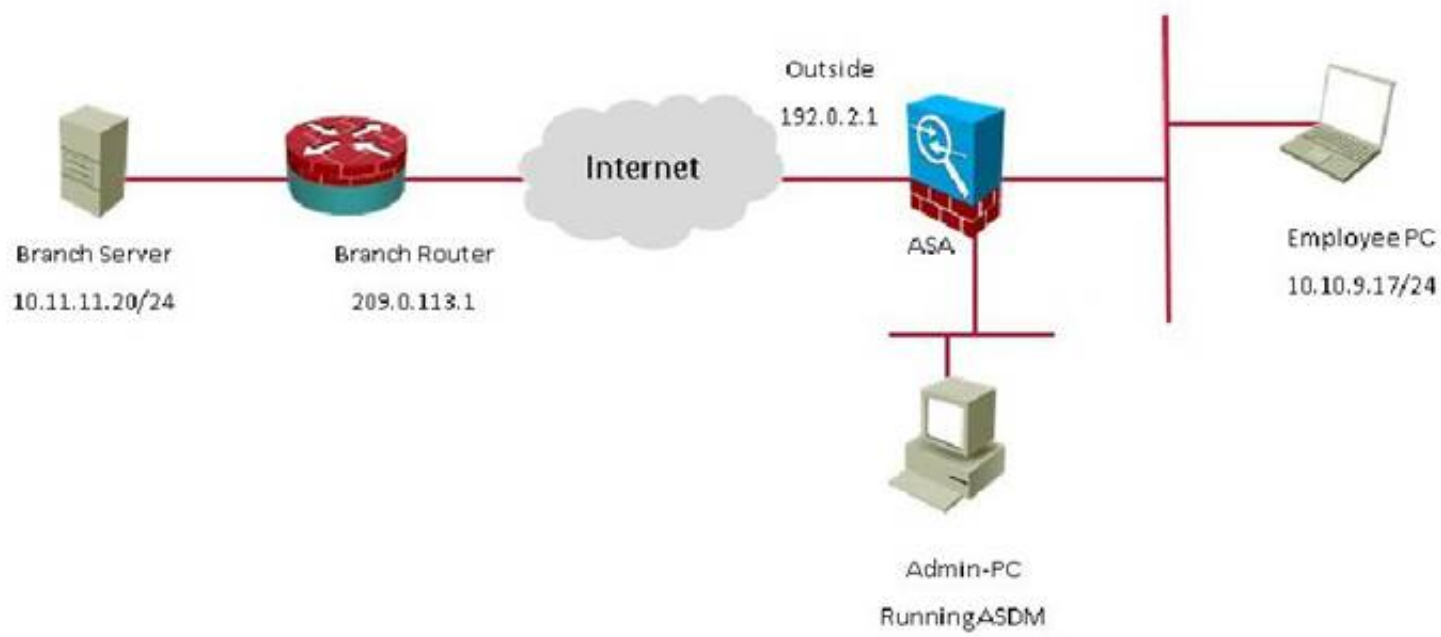
You are now tasked with verifying the IKEv1 IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.

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

Topology:

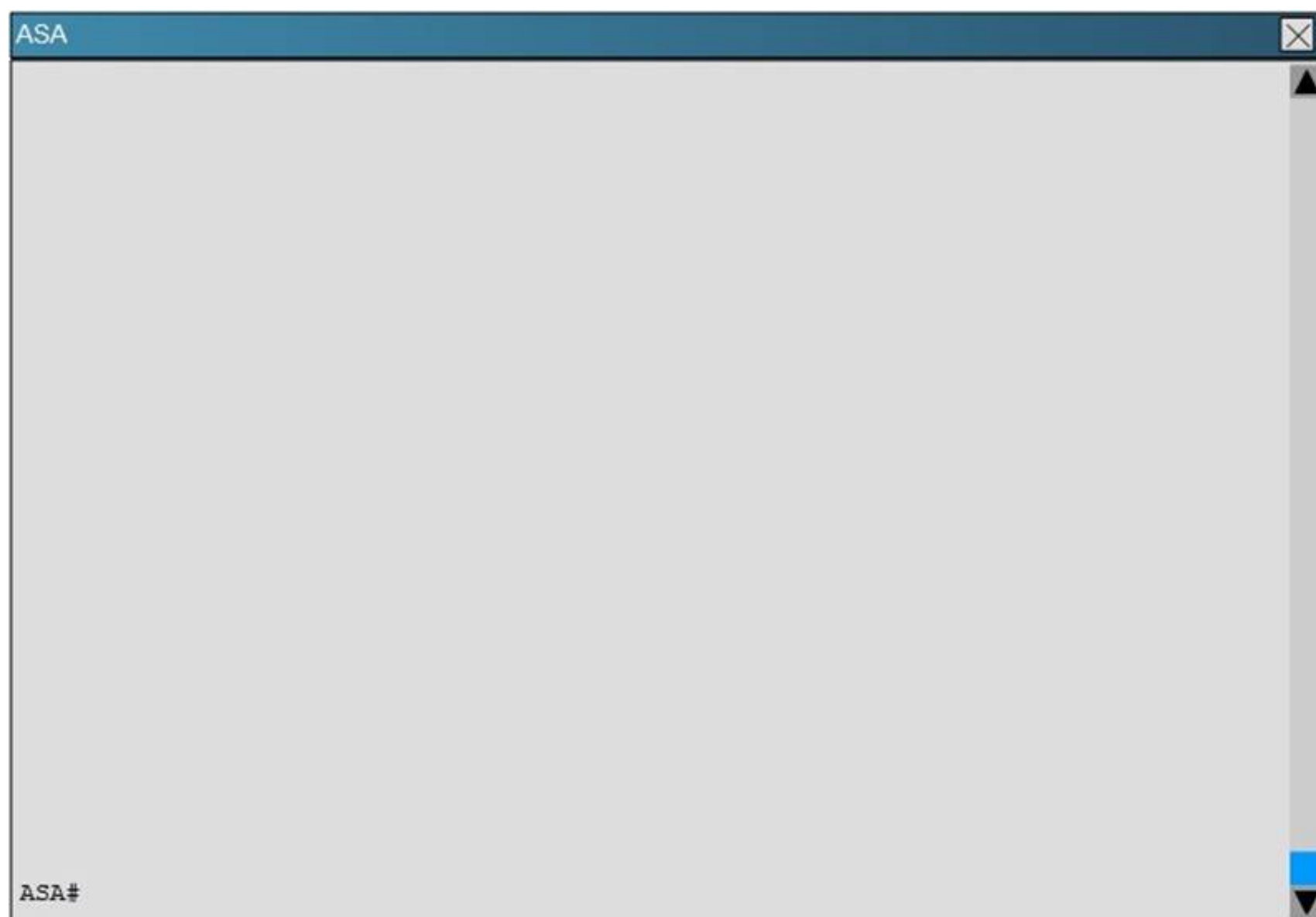


Topology



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 342

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 345

Scenario

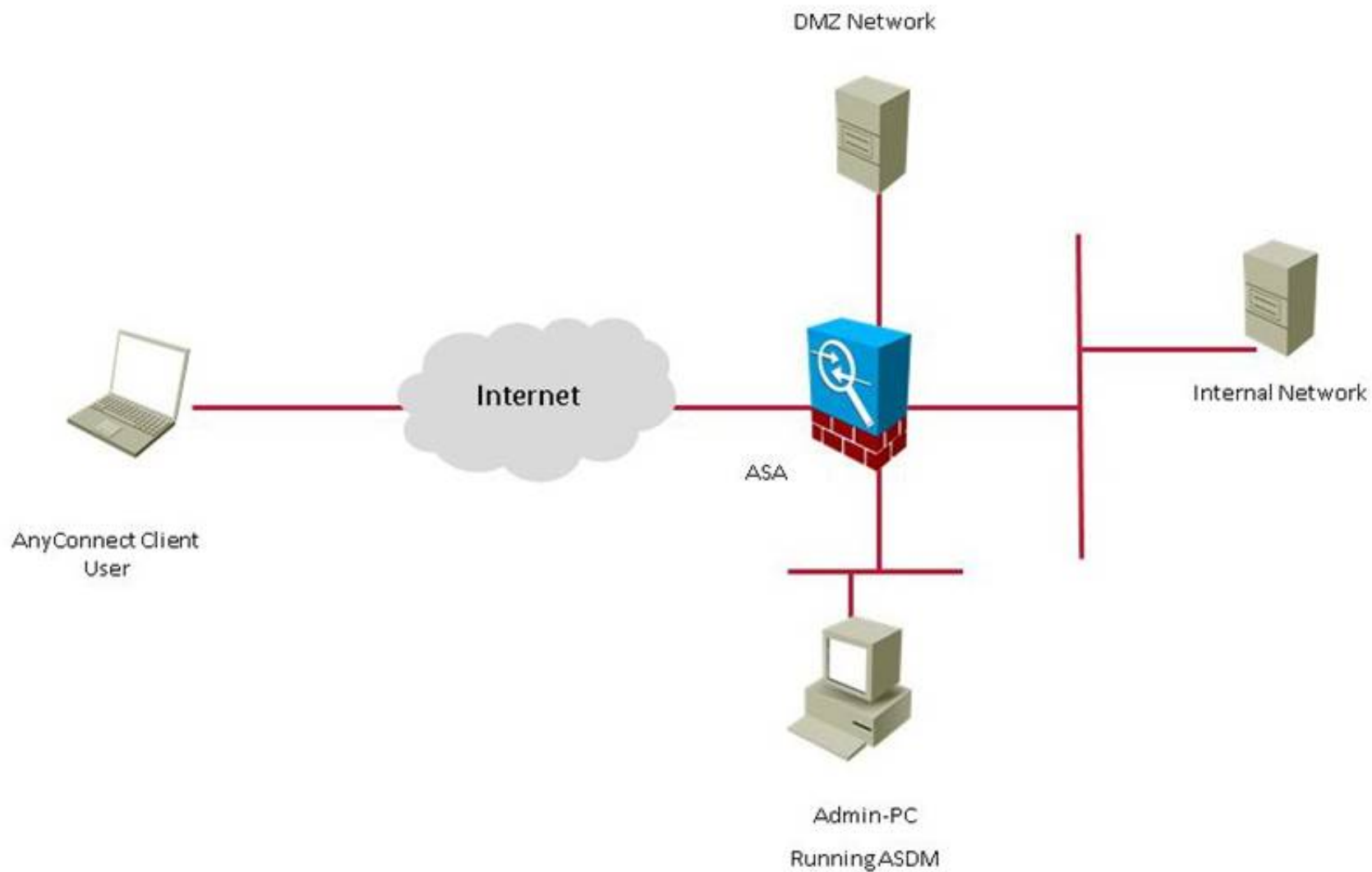
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

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](#).

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 

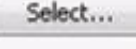
☐ Use LOCAL if Server Group fails

Client Address Assignment

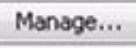
DHCP Servers:

☒ 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



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

Access Rules

NAT Rules

Service Policy Rules

AAA Rules

Filter Rules

Public Servers

URL Filtering Servers

Threat Detection

Identity Options

Identity by TrustSec

Botnet Traffic Filter

Objects

Unified Communications

Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

IPS

Device Management

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
<b>DMZ (3 incoming rules)</b>			
<input checked="" type="checkbox"/>	DMZ-server		any4
<input checked="" type="checkbox"/>	DMZ-server		HQ-srv
<input checked="" type="checkbox"/>	DMZ-server		any
<b>DMZ (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (6 incoming rules)</b>			
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<b>DMZ-to-Site (1 implicit rule)</b>			
<input checked="" type="checkbox"/>	any		any

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

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 > Advanced > ACL Manager

Add Edit Delete Find

#	Enabled	Source	User	Security Group	Destination	Security
<b>DMZ_access_in</b>						
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	
<b>outside_access_in</b>						
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	
<b>outside_cryptomap</b>						
1	<input checked="" type="checkbox"/>	10.10.9.0/24			10.11.11.0/24	
<b>permit-all</b>						
1	<input checked="" type="checkbox"/>	any			any	

Collapse All Expand All

Apply Reset



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 > NAT Rules

Match Criteria: Original Packet

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

Apply Reset

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

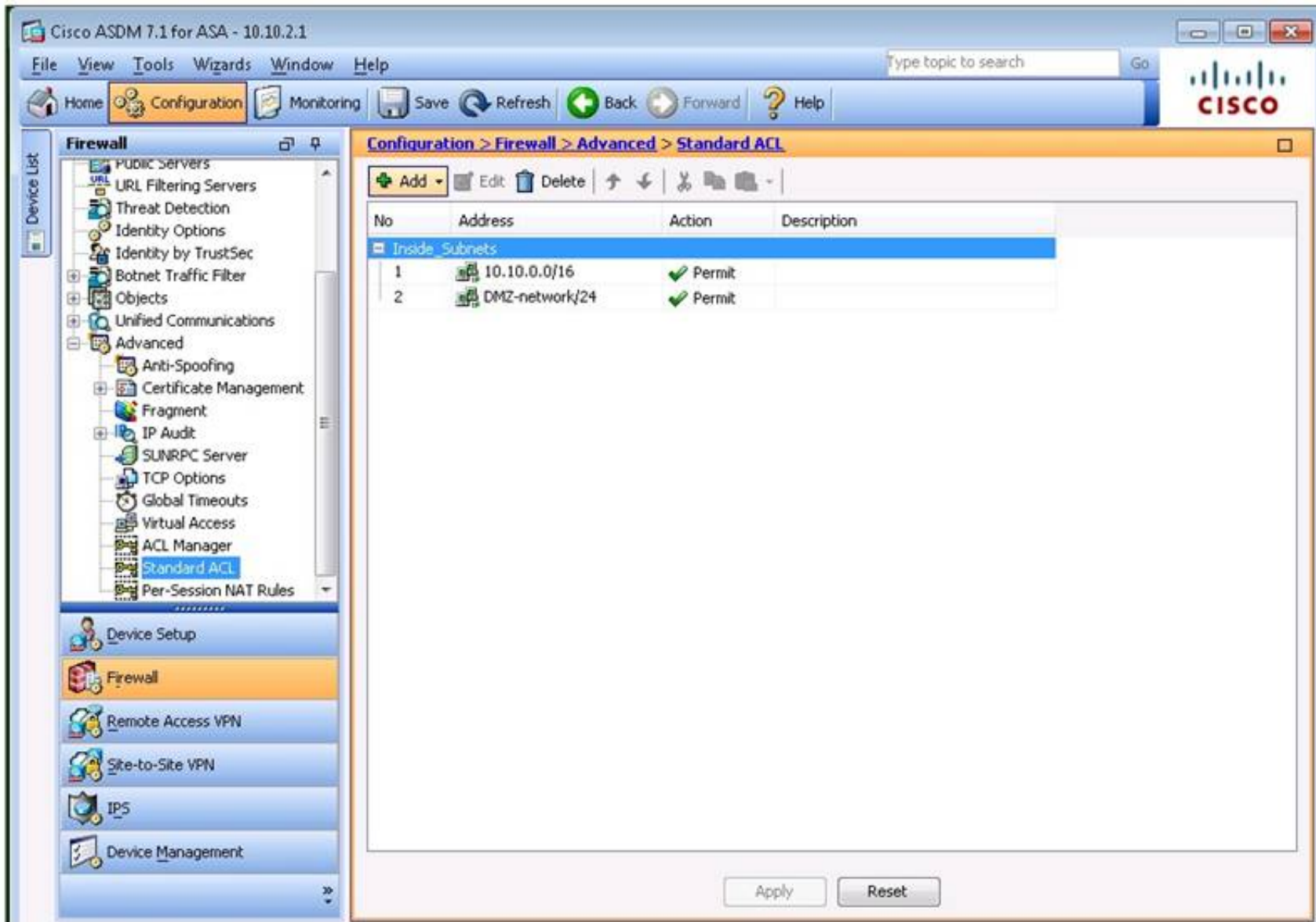
Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Advanced

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 displays the 'Firewall' configuration tree, with 'Standard ACL' selected under the 'Advanced' section. The main pane shows the 'Configuration > Firewall > Advanced > Standard ACL' configuration page. A table lists the ACL rules:

No	Address	Action	Description
<b>Inside Subnets</b>			
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

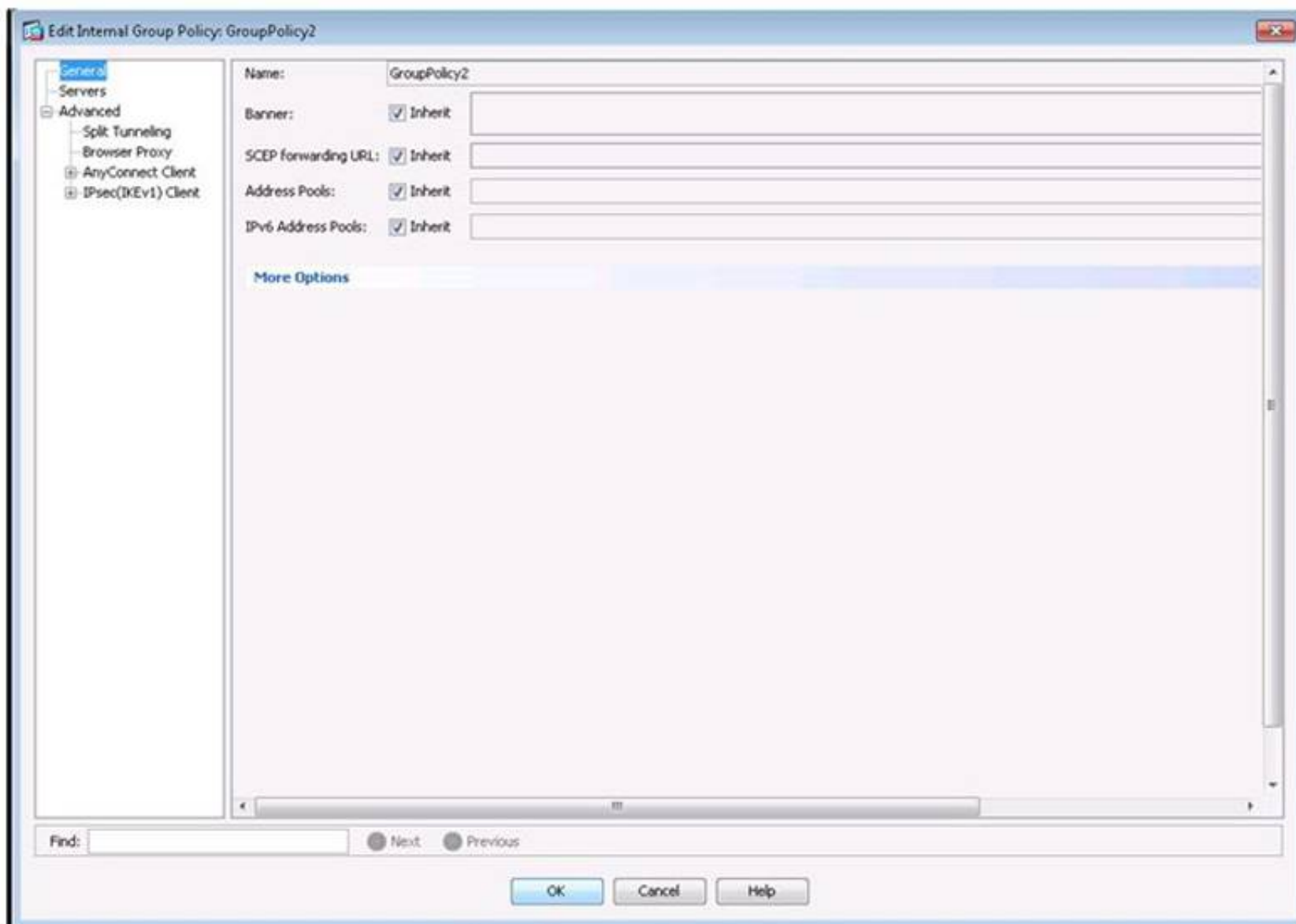
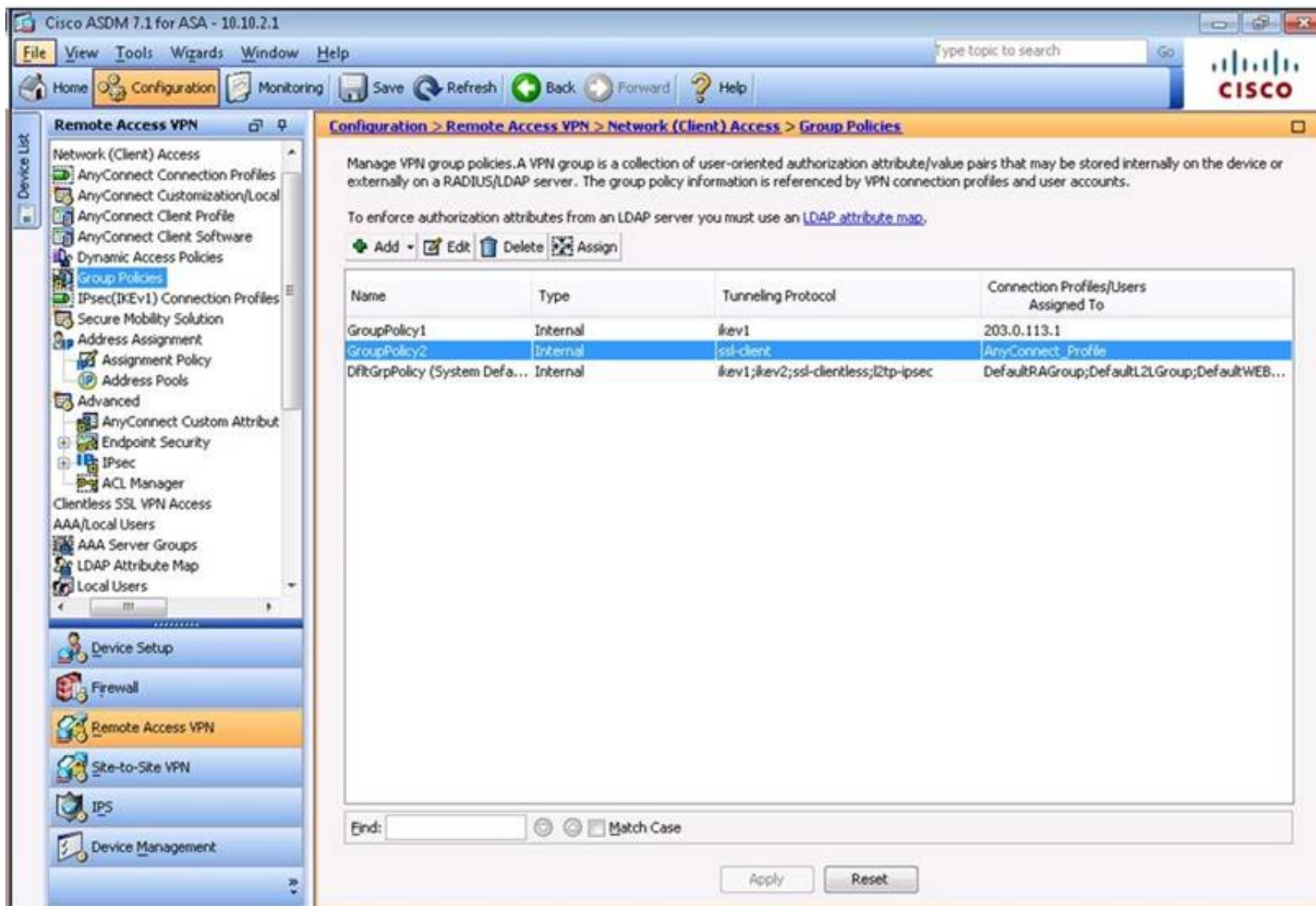
Direction: Both

Description:

OK

Cancel

Help





**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

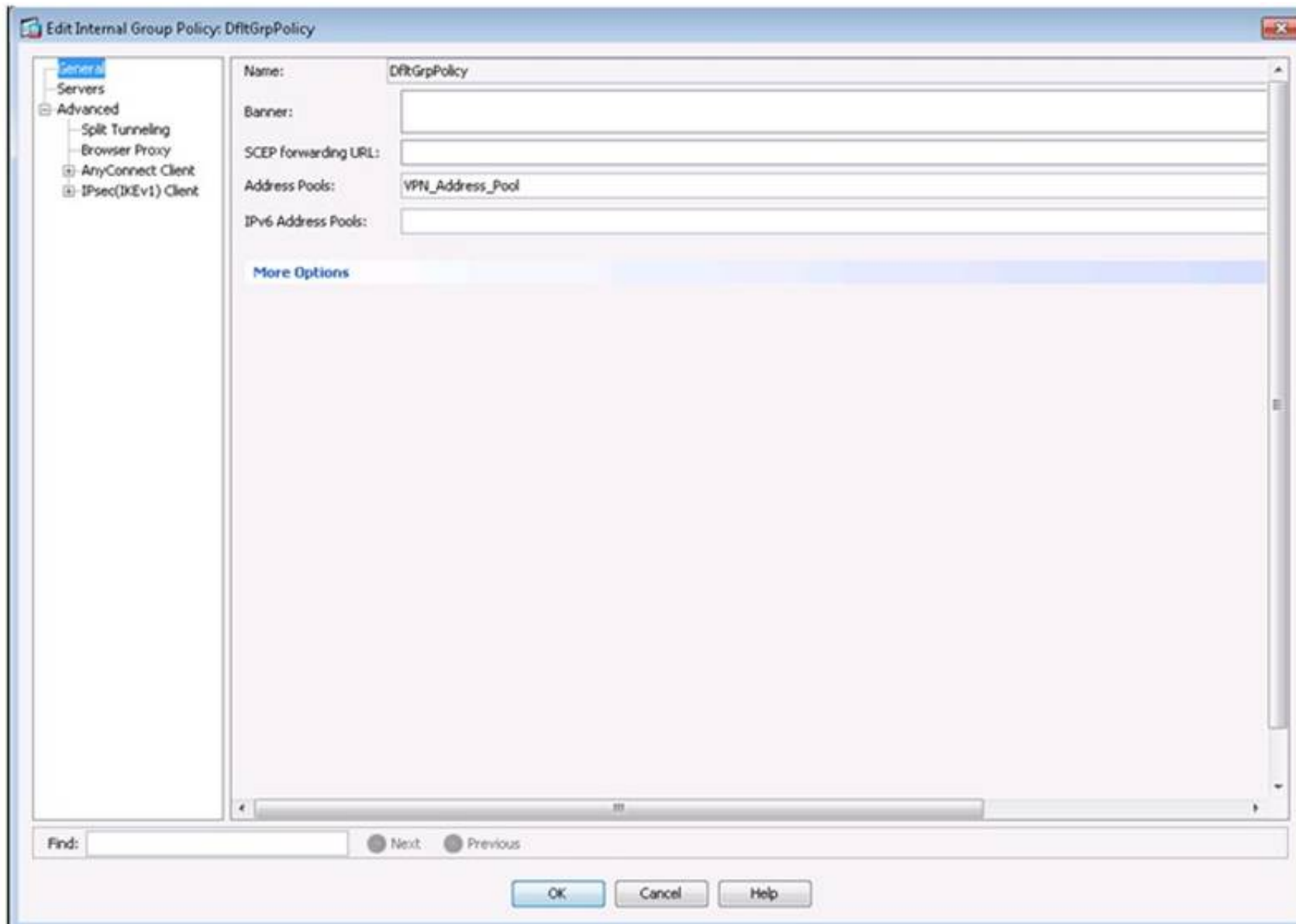
Network List: Inside\_Subnets

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

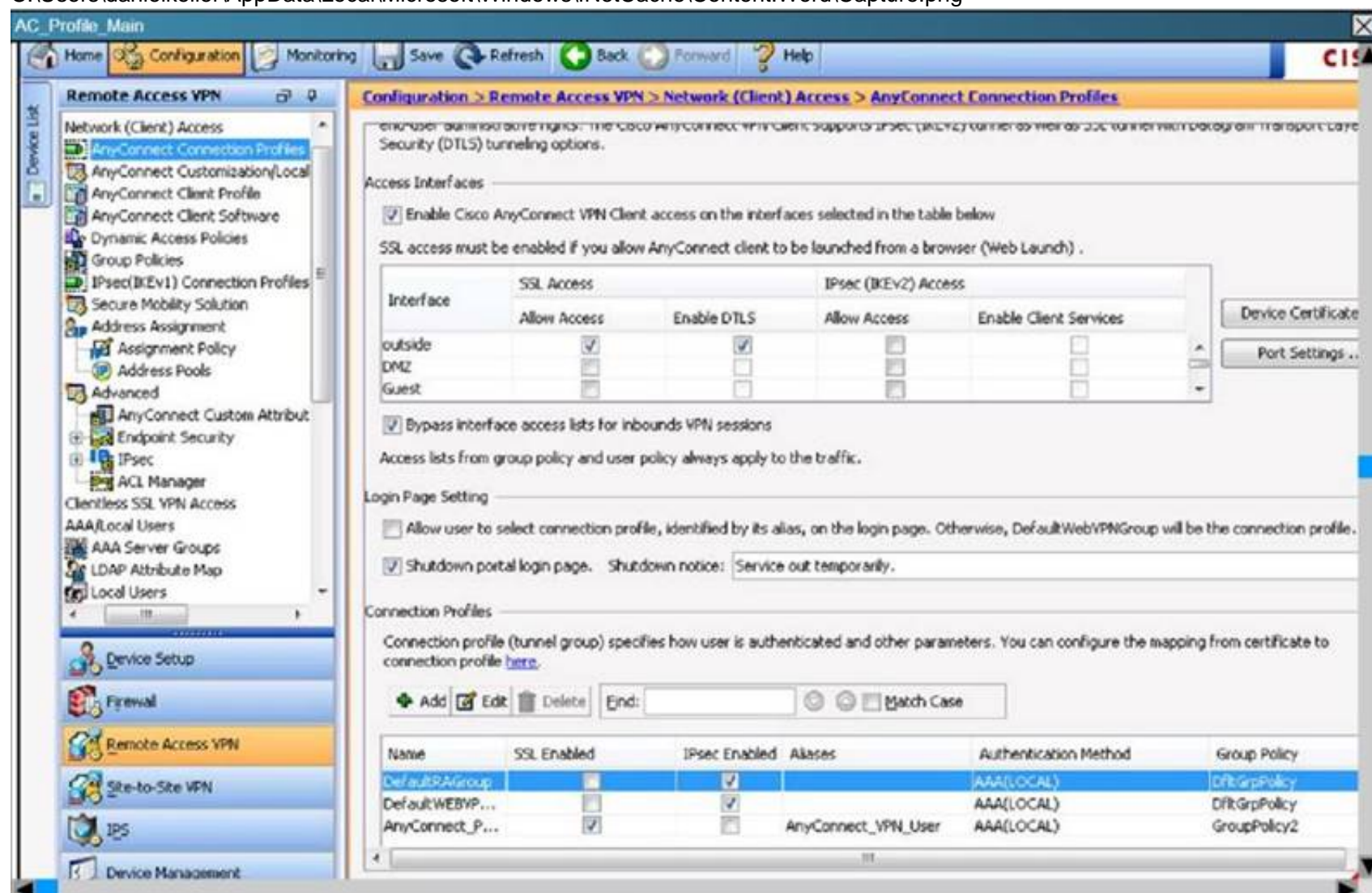


Which address range will be assigned to the AnyConnect users?

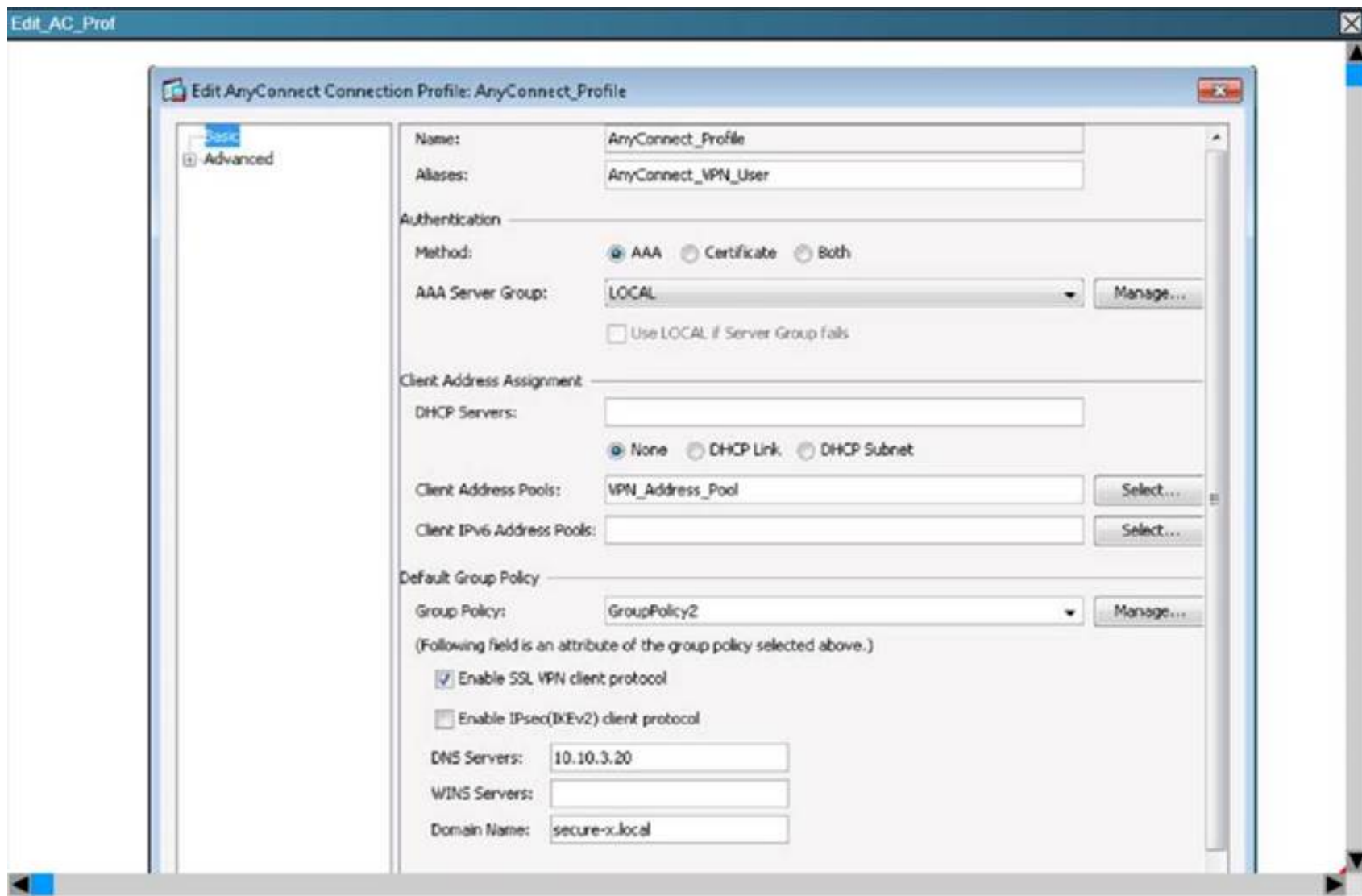
- A. 10.10.15.40-50/24
- B. 209.165.201.20-30/24
- C. 192.168.1.100-150/24
- D. 10.10.15.20-30/24

**Answer: D**

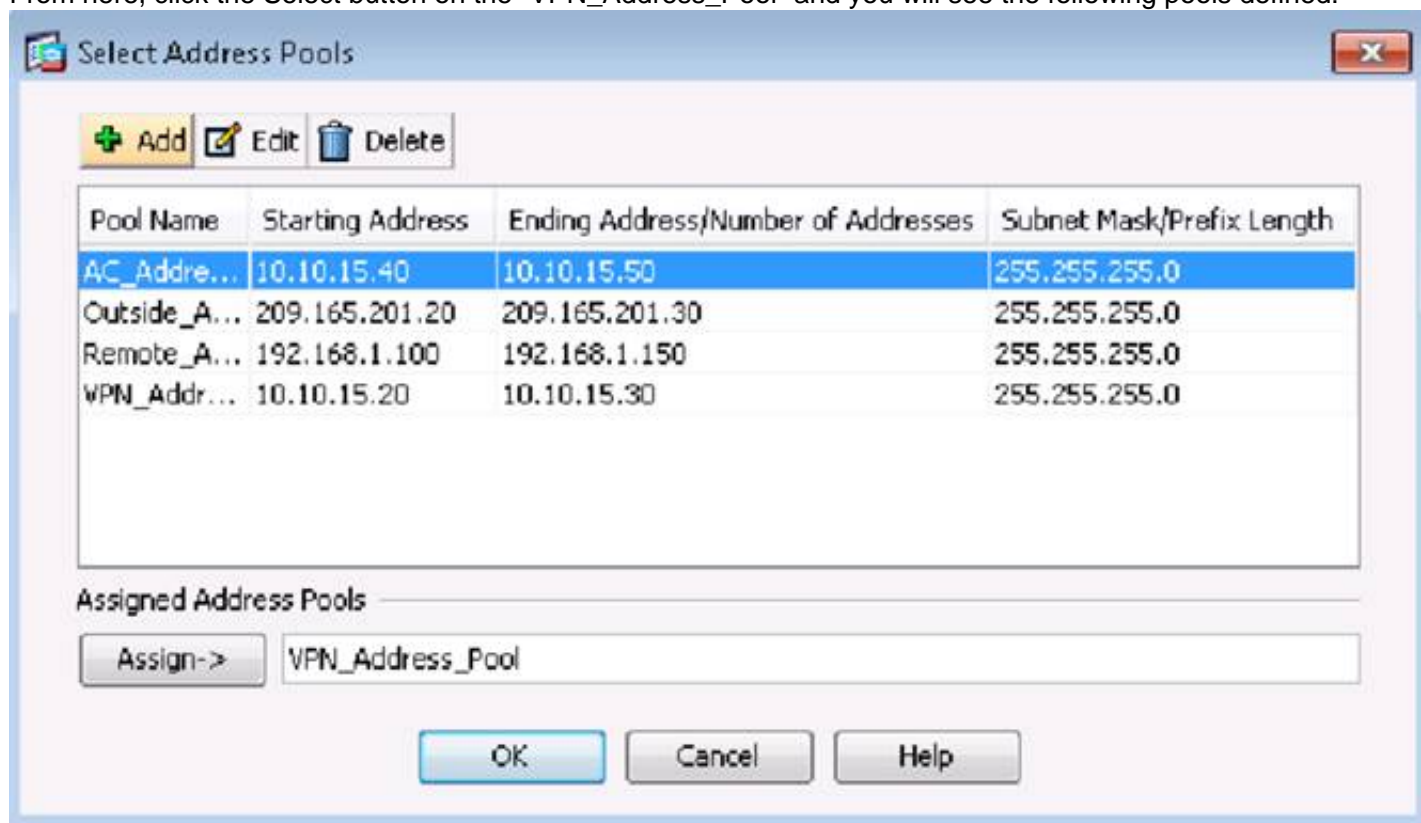
**Explanation:** First Navigate to the Configuration -> Remote Access VPN tab and then choose the "AnyConnect Connection Profile as shown below:  
C:\Users\danielkeller\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Capture.png



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 347

In which situation would you enable the Smart Tunnel option with clientless SSL VPN?

- A. when a user is using an outdated version of a web browser
- B. when an application is failing in the rewrite process
- C. when IPsec should be used over SSL VPN
- D. when a user has a nonsupported Java version installed
- E. when cookies are disabled

**Answer: B**

#### NEW QUESTION 350

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 355

Which two types of authentication are supported when you use Cisco ASDM to configure site-to-site IKEv2 with IPv6? (Choose two.)

- A. preshared key
- B. webAuth
- C. digital certificates
- D. XAUTH
- E. EAP

**Answer:** AC

#### NEW QUESTION 360

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](https://www.cisco.com/web/learning/le21/le39/docs/tdw166_prezo.pdf)

#### NEW QUESTION 362

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 365

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 367

When you troubleshoot Cisco AnyConnect, which step does Cisco recommend before you open a TAC case?

- A. Show applet Lifecycle exceptions.
- B. Disable cookies.
- C. Enable the WebVPN cache.
- D. Collect a DART bundle.

**Answer:** D

#### NEW QUESTION 372

Which command can you use to monitor the phase 1 establishment of a FlexVPN tunnel?

- A. show crypto ipsec sa
- B. show crypto isakmp sa
- C. show crypto ikev2 sa
- D. show ip nhrp

**Answer:** C

#### NEW QUESTION 373

Scenario

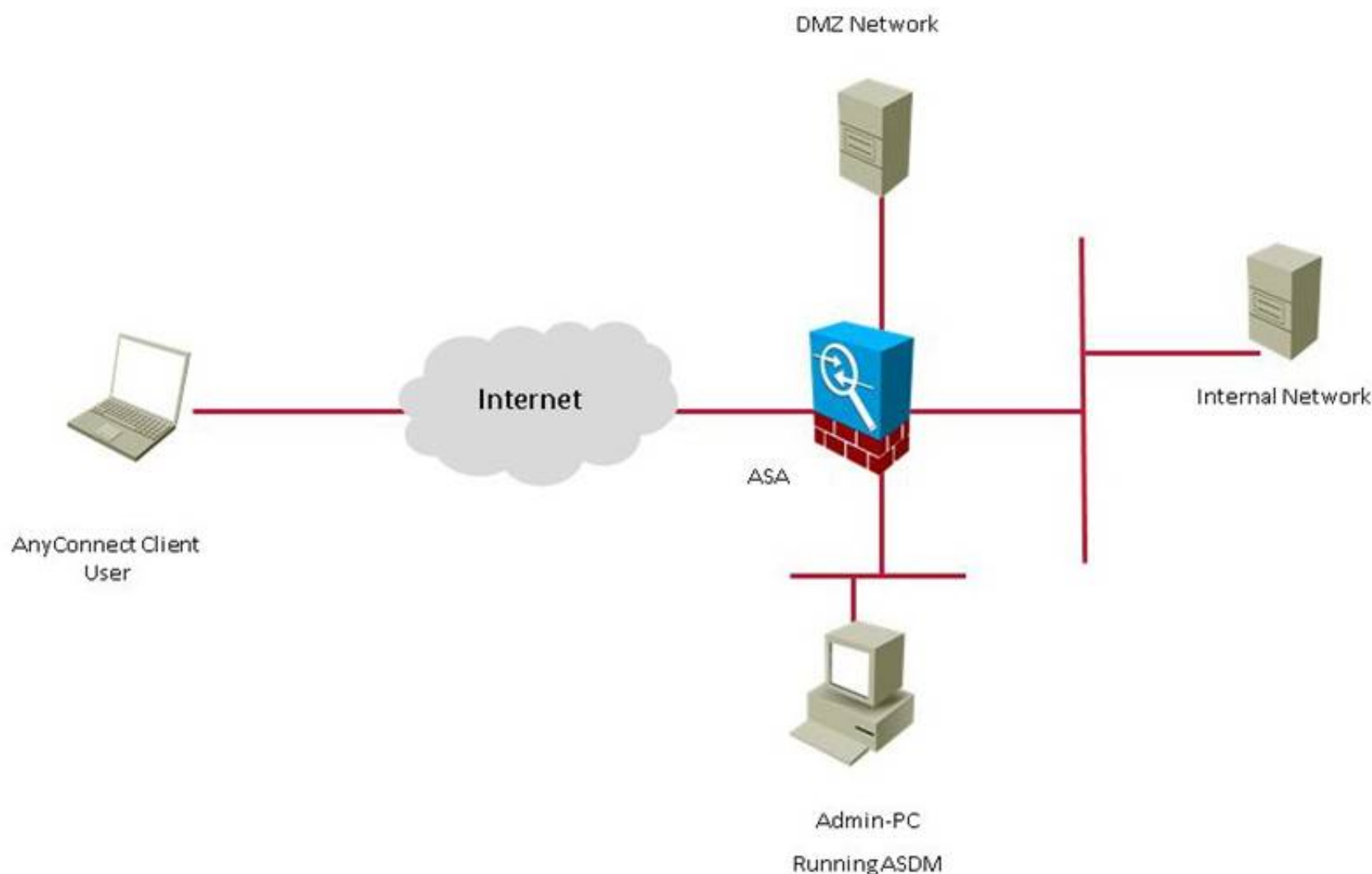
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

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

**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](#).

Buttons: Add, Edit, Delete, Find: [ ] Match Case

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

Buttons: Apply, Reset

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 

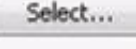
☐ Use LOCAL if Server Group fails

Client Address Assignment

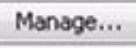
DHCP Servers:

☒ 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

Access Rules

NAT Rules

Service Policy Rules

AAA Rules

Filter Rules

Public Servers

URL Filtering Servers

Threat Detection

Identity Options

Identity by TrustSec

Botnet Traffic Filter

Objects

Unified Communications

Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

IPS

Device Management

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
<b>DMZ (3 incoming rules)</b>			
<input checked="" type="checkbox"/>	DMZ-server		any4
<input checked="" type="checkbox"/>	DMZ-server		HQ-srv
<input checked="" type="checkbox"/>	DMZ-server		any
<b>DMZ (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (1 implicit incoming rule)</b>			
<input checked="" type="checkbox"/>	any		Any less secure ne...
<b>DMZ-to-Site (6 incoming rules)</b>			
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<input checked="" type="checkbox"/>	any4		DMZ-server
<b>DMZ-to-Site (1 implicit rule)</b>			
<input checked="" type="checkbox"/>	any		any

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

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 > Advanced > ACL Manager

Add Edit Delete Find

#	Enabled	Source	User	Security Group	Destination	Security
<b>DMZ_access_in</b>						
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	
<b>outside_access_in</b>						
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	
<b>outside_cryptomap</b>						
1	<input checked="" type="checkbox"/>	10.10.9.0/24			10.11.11.0/24	
<b>permit-all</b>						
1	<input checked="" type="checkbox"/>	any			any	

Collapse All Expand All

Apply Reset



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

Access Rules  
 NAT Rules  
 Service Policy Rules  
 AAA Rules  
 Filter Rules  
 Public Servers  
 URL Filtering Servers  
 Threat Detection  
 Identity Options  
 Identity by TrustSec  
 Botnet Traffic Filter  
 Objects  
 Unified Communications  
 Advanced

Device Setup  
 Firewall  
 Remote Access VPN  
 Site-to-Site VPN  
 IPS  
 Device Management

Configuration > Firewall > NAT Rules

Add Edit Delete Find Diagram Packet Trace

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 --

Apply Reset

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

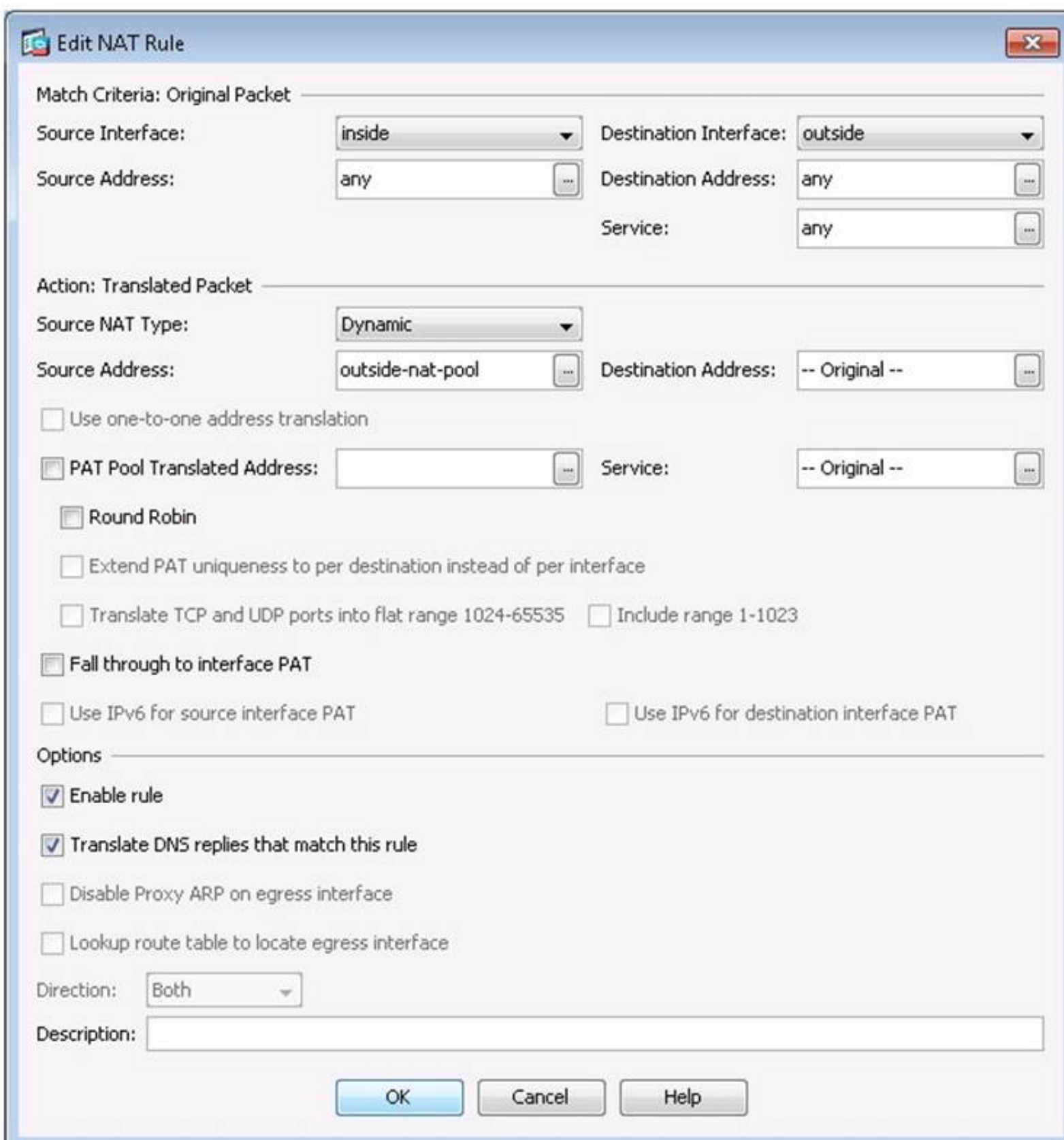
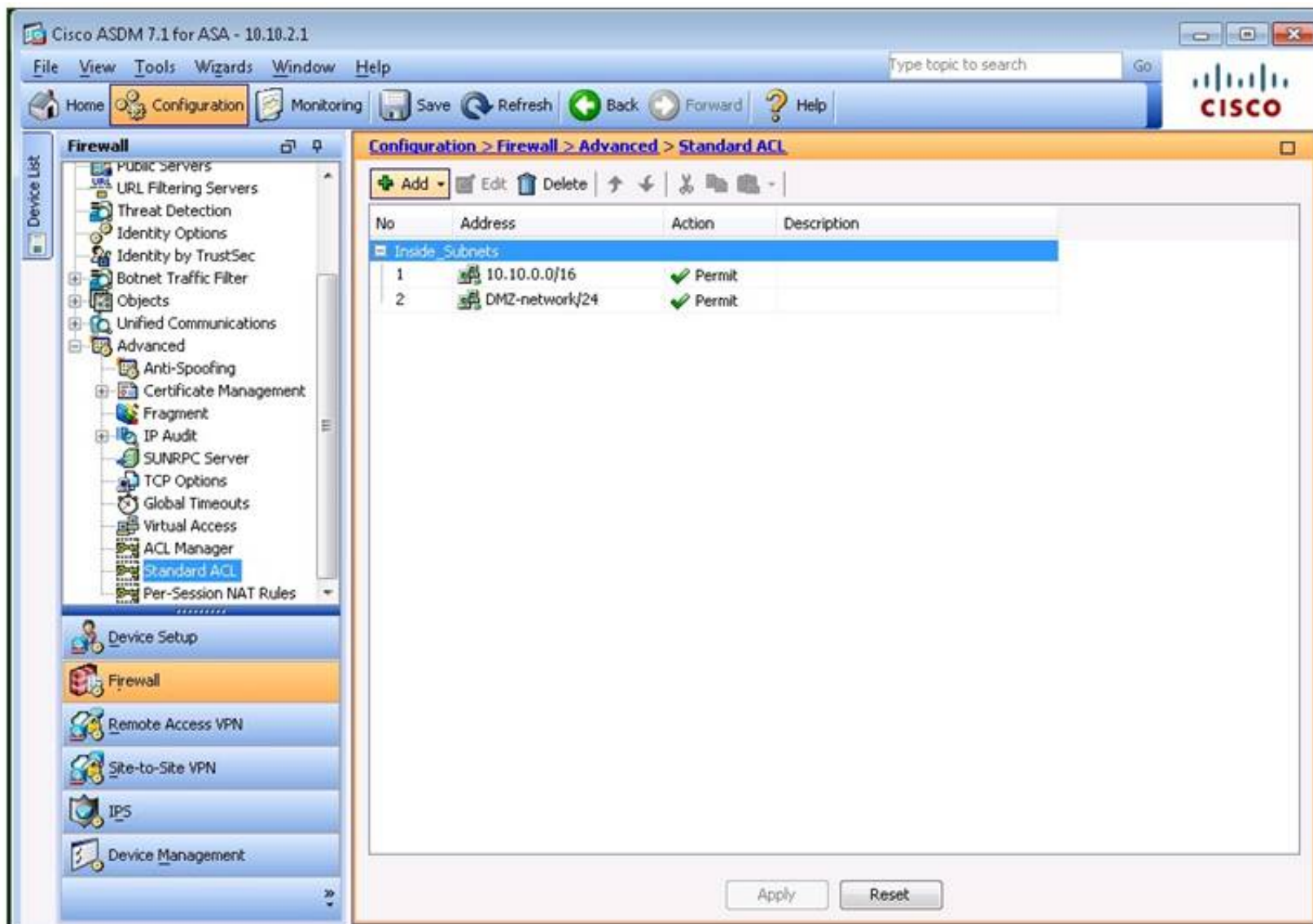
Public Servers  
 URL Filtering Servers  
 Threat Detection  
 Identity Options  
 Identity by TrustSec  
 Botnet Traffic Filter  
 Objects  
 Unified Communications  
 Advanced

Device Setup  
 Firewall  
 Remote Access VPN  
 Site-to-Site VPN  
 IPS  
 Device Management

Configuration > Firewall > Advanced

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](#)





### 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

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...

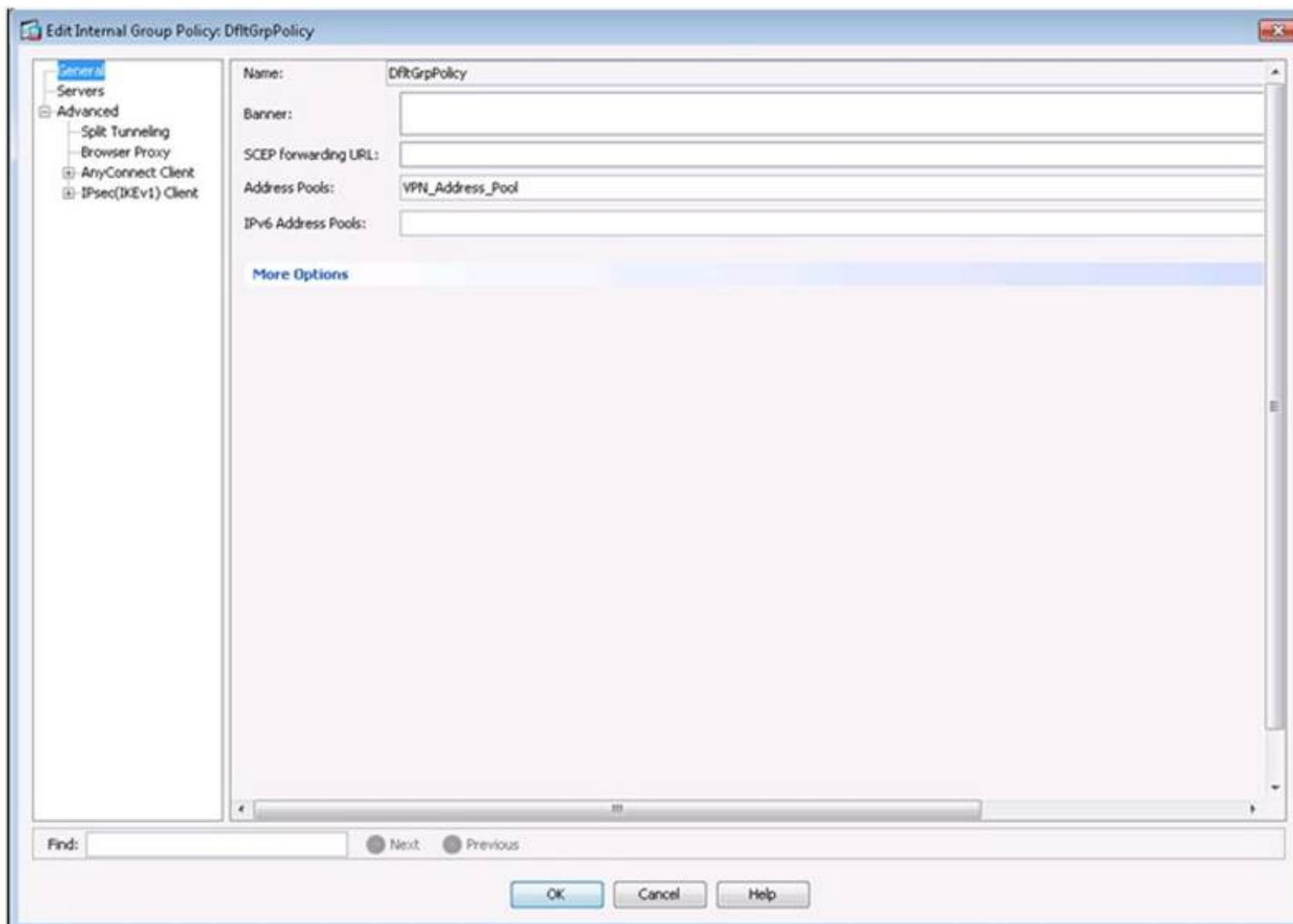
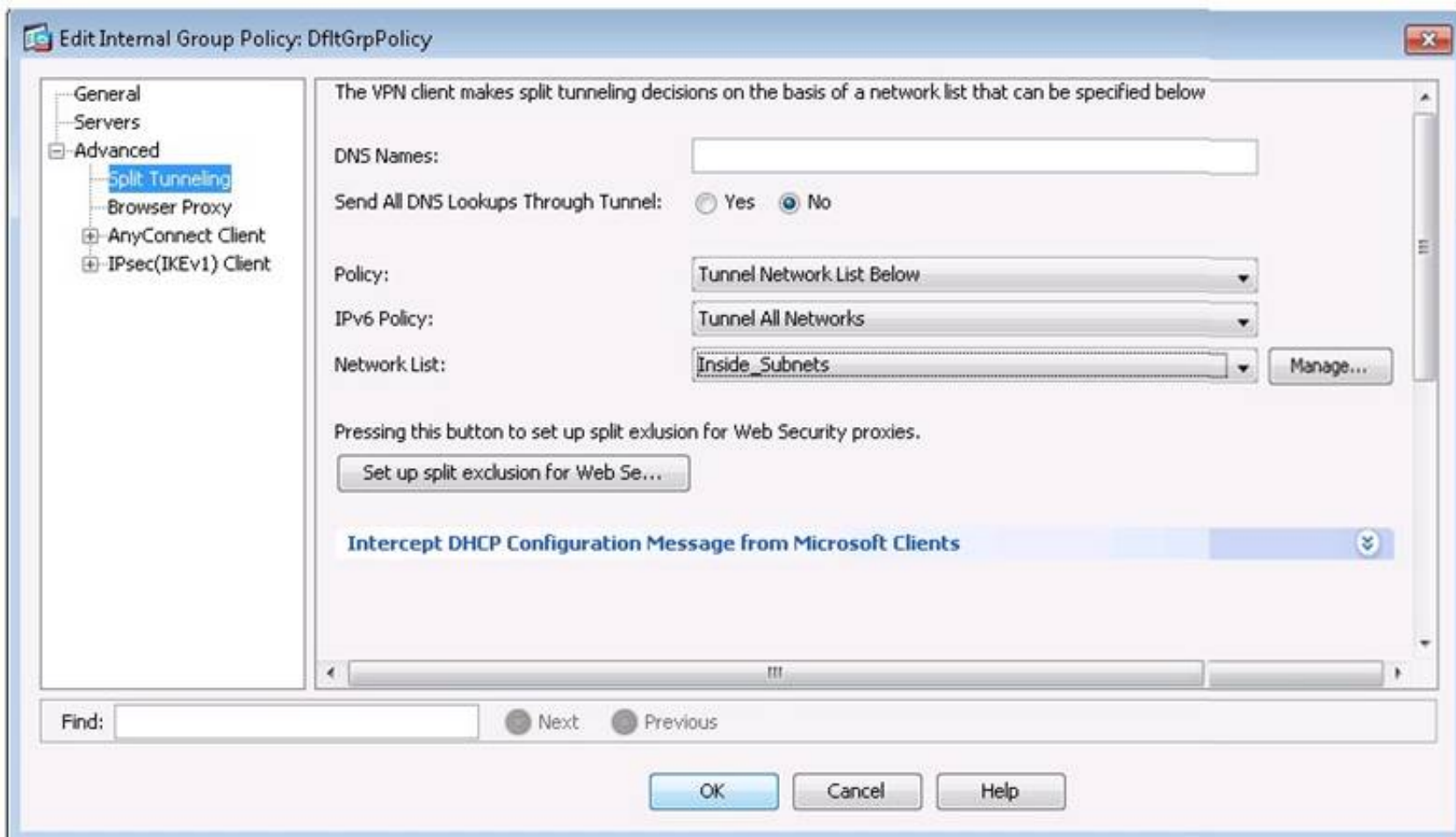
Intercept DHCP Configuration Message from Microsoft Clients

Find:

Next Previous

OK Cancel Help



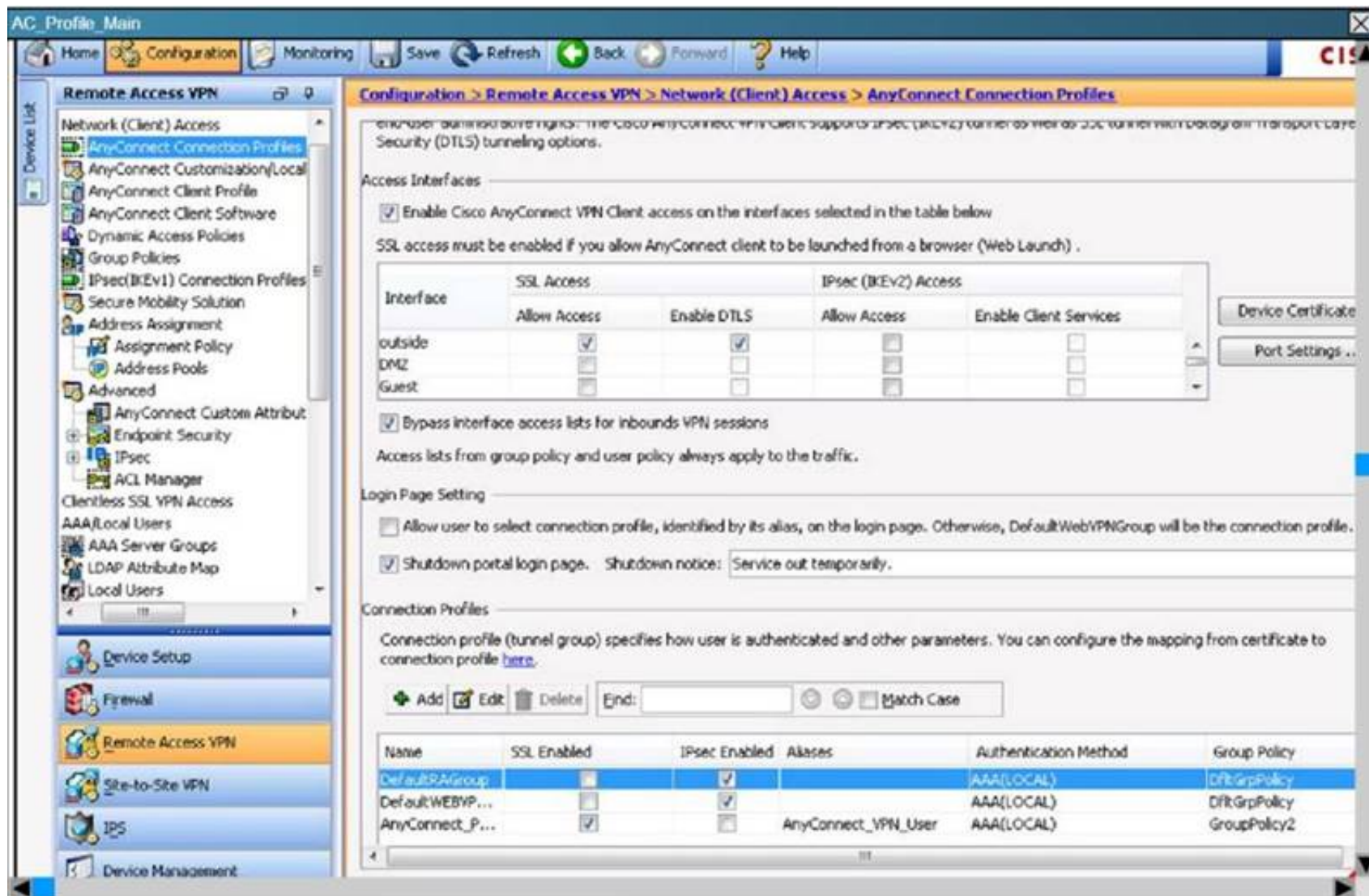


Which address pool is being assigned to the users connecting via the AnyConnect client?

- A. AC\_Address\_Pool
- B. Remote\_Address\_Pool
- C. Outside\_Address\_Pool
- D. VPN\_Address\_Pool

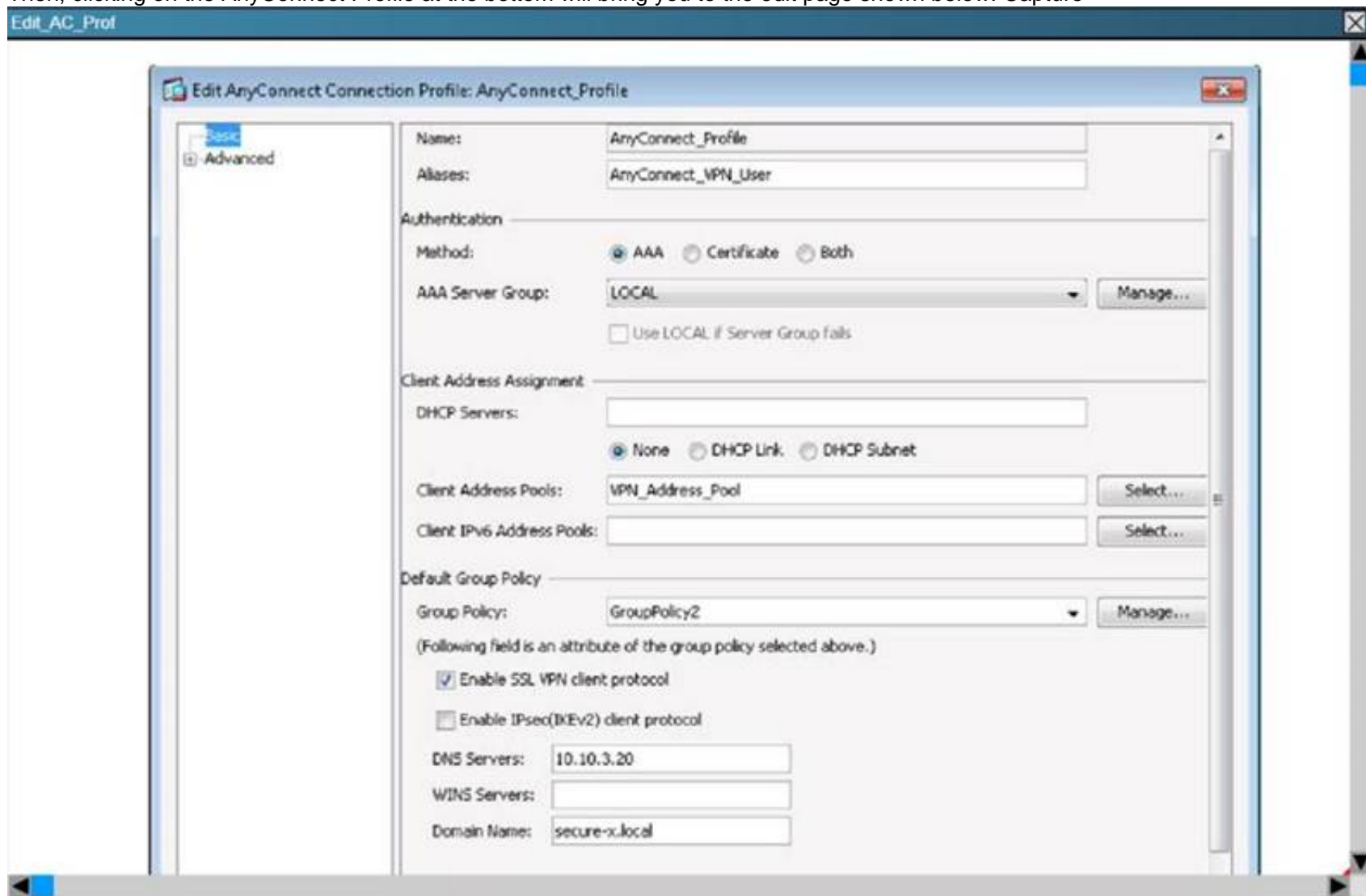
**Answer: D**

**Explanation:** First Navigate to the Configuration -> Remote Access VPN tab and then choose the "AnyConnect Connection Profile as shown below:



Capture

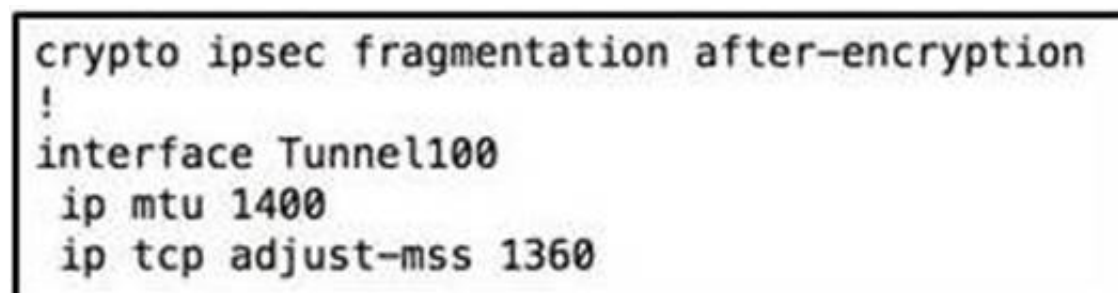
Then, clicking on the AnyConnect Profile at the bottom will bring you to the edit page shown below: Capture



From here we can see that the Client Address Pools in use is the "VPN\_Address\_Pool"

#### NEW QUESTION 374

Refer to the exhibit.



What is the purpose of the given configuration?



- A. Establishing a GRE tunnel.
- B. Enabling IPSec to decrypt fragmented packets.
- C. Resolving access issues caused by large packet sizes.
- D. Adding the spoke to the routing table.

**Answer:** C

#### NEW QUESTION 375

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 380

Which functionality is provided by L2TPv3 over FlexVPN?

- A. the extension of a Layer 2 domain across the FlexVPN
- B. the extension of a Layer 3 domain across the FlexVPN
- C. secure communication between servers on the FlexVPN
- D. a secure backdoor for remote access users through the FlexVPN

**Answer:** A

**Explanation:** Topic 3, Exam Pool B

#### NEW QUESTION 382

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 384

What command in cli you have to use to capture IKEv1 phase 1

- A. capture match ip q port 500 eq port 500
- B. capture match gre q port 500 eq port 500
- C. apture match ah q port 500 eq port 500
- D. capture match udp eq port 153 eq port 153
- E. capture match udp eq port 500 eq port 500

**Answer:** E

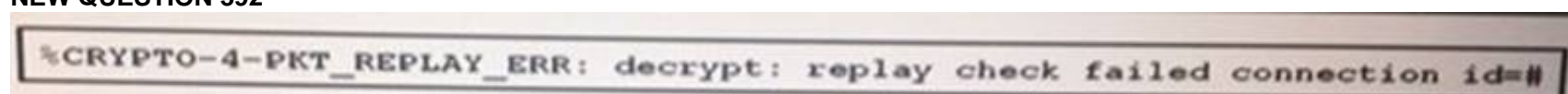
#### NEW QUESTION 389

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 392



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 397

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 398

Which algorithm provides both encryption and authentication for plane communication?

- A. RC4
- B. SHA-384
- C. AES-256
- D. SHA-96
- E. 3DES
- F. AES-GCM

**Answer:** F

#### NEW QUESTION 402

What is a valid reason for configuring a list of backup servers on the Cisco AnyConnect VPN Client profile?

- A. to access a backup authentication server
- B. to access a backup DHCP server
- C. to access a backup VPN server
- D. to access a backup CA server

**Answer:** C

#### NEW QUESTION 405

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 409

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 413

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](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 414

An engineer has integrated a new DMVPN to link remote offices across the internet using Cisco IOS routers. When connecting to remote sites, pings and voice data appear to flow properly and all tunnel stats seem to show that are up. However, when trying to connect to a remote server using RDP, the connection fails. Which action resolves this issue?

- A. Change DMVPN timeout values.
- B. Adjust the MTU size within the routers.
- C. Replace certificate on the RDP server.
- D. Add RDP port to the extended ACL.

**Answer:** C

#### NEW QUESTION 416

A company has a Flex VPN solution for remote access and one of their Cisco any Connect remote clients is having trouble connecting property. 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 417

Refer to the exhibit.

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

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

- A. dual DMVPN cloud setup with dual hub
- B. DMVPN Phase 3 implementation
- C. single DMVPN cloud setup with dual hub
- D. DMVPN Phase 1 implementation
- E. quad DMVPN cloud with quadra hub
- F. DMVPN Phase 2 implementation

**Answer:** BC

#### NEW QUESTION 420

Which command can be used to troubleshoot an IPv6 FlexVPN spoke-to-hub connectivity failure?

- A. show crypto lkev2 client flexvpn
- B. show crypto identity
- C. show crypto isakmp sa
- D. show crypto gkm

**Answer:** A

#### NEW QUESTION 422

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](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 424

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](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 426

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

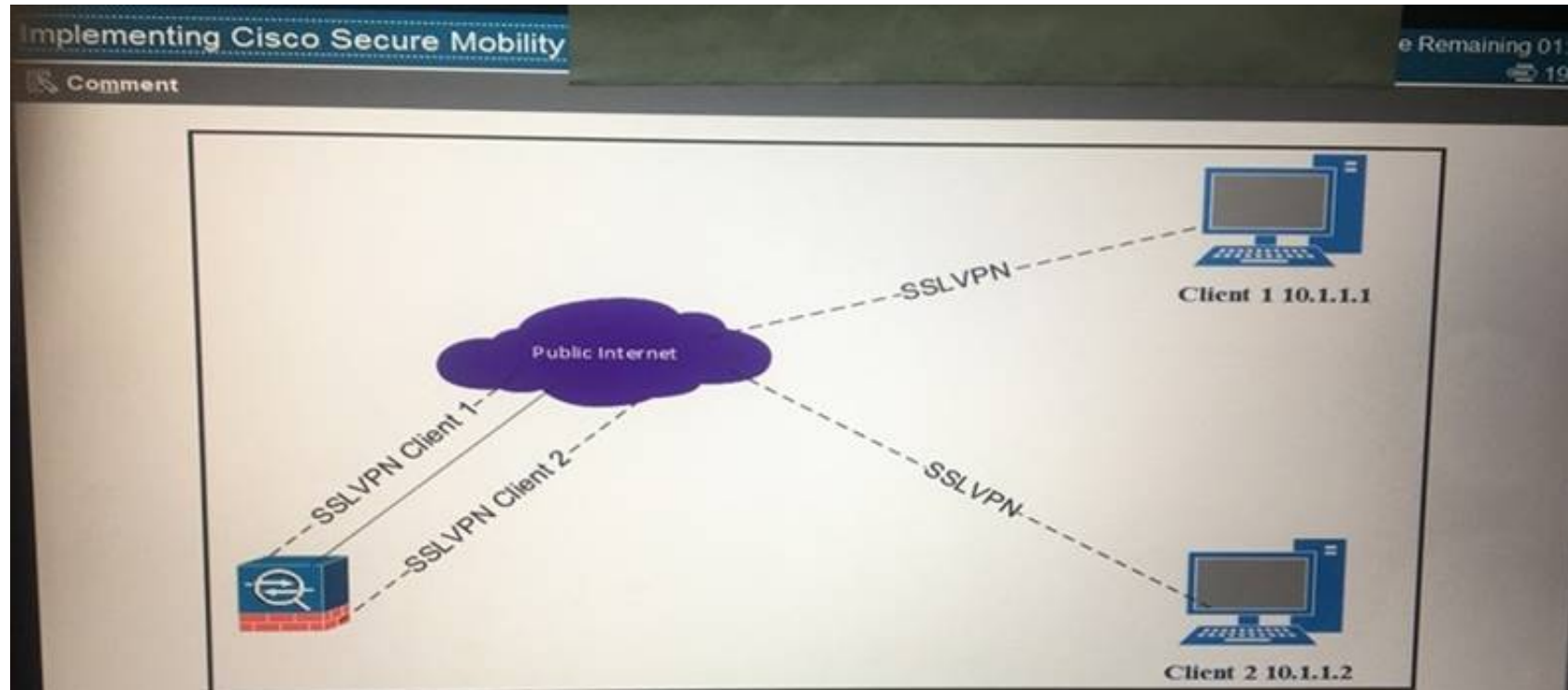
**NEW QUESTION 429**

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

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

**Answer:** BD

**NEW QUESTION 433**



Refer to the exhibit. Client 1 cannot communication with Client 2. Both clients are using Cisco AnyConnect and have established a successful SSL VPN connection to the hub ASA. Which command on the ASA is missing?

- A. same-security-traffic permit inter-interface
- B. same-security-traffic permit intra-interface
- C. dns-server value 10.1.1.3
- D. split-tunnel-network list

**Answer:** B

**NEW QUESTION 434**

Which two commands are include in the command show dmvpn detail? (Choose two.)

- A. Show ip nhrp
- B. Show ip nhrp nhs
- C. Show crypto ipsec sa detail
- D. Show crypto session detail
- E. Show crypto sockets

**Answer:** DE

**NEW QUESTION 436**

Which three configuration parameters are mandatory for an IKEv2 profile? (Choose three.)

- A. IKEv2 proposal
- B. local authentication method
- C. match identity or certificate
- D. IKEv2 policy
- E. PKI certificate authority
- F. remote authentication method
- G. IKEv2 profile description
- H. virtual template

**Answer:** BCF

**NEW QUESTION 437**

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

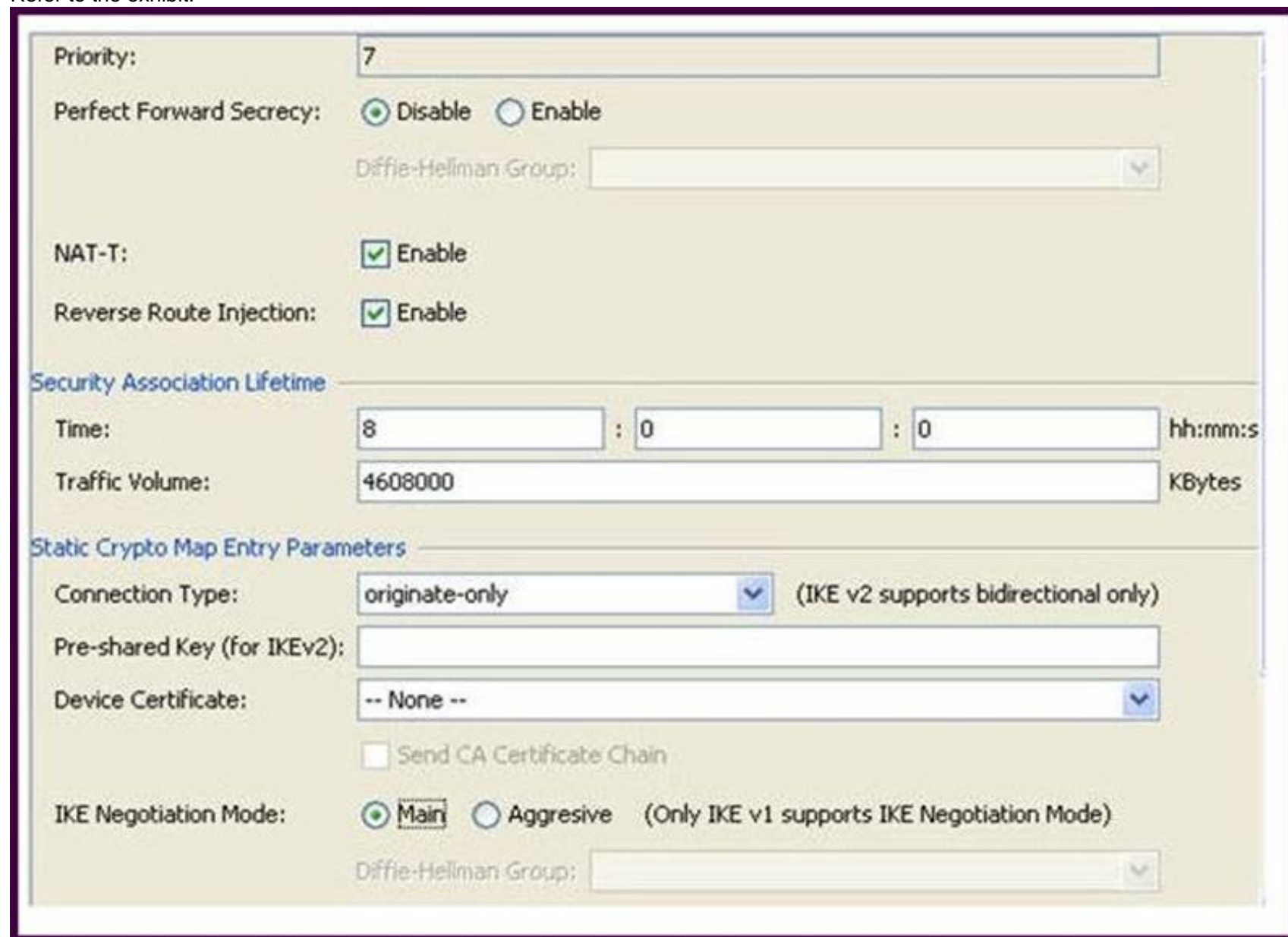
The aaa authentication command is entered to specify an authentication list or server group under a SSL VPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.

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 439

Refer to the exhibit.



While configuring a site-to-site VPN tunnel, a new NOC engineer encounters the Reverse Route Injection parameter.

Assuming that static routes are redistributed by the Cisco ASA to the IGP, what effect does enabling Reverse Route Injection on the local Cisco ASA have on a configuration?

- A. The local Cisco ASA advertises its default routes to the distant end of the site-to-site VPN tunnel.
- B. The local Cisco ASA advertises routes from the dynamic routing protocol that is running on the local Cisco ASA to the distant end of the site-to-site VPN tunnel.
- C. The local Cisco ASA advertises routes that are at the distant end of the site-to-site VPN tunnel.
- D. The local Cisco ASA advertises routes that are on its side of the site-to-site VPN tunnel to the distant end of the site-to-site VPN tunnel.

**Answer: C**

**Explanation:** [http://www.cisco.com/en/US/products/ps6120/products\\_configuration\\_example09186a00809d07de.shtml](http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809d07de.shtml)

#### NEW QUESTION 444

An engineer has successfully established a phase 1 tunnel, but notices that no packets are decrypted on the head end side of the tunnel. What is a potential cause for this issue?

- A. different phase 2 encryption
- B. misconfigured DH group
- C. disabled PFS
- D. firewall blocking Phase 2 ESP or AH

**Answer: A**

#### NEW QUESTION 448

An engineer is troubleshooting a DMVPN spoken router and sees a CRPTO-4-IKMP\_BAD\_MESSAGE debug message that a spoke router “failed its sanity check or is malformed” Which issue does the error message indicate?

- A. mismatched preshared key
- B. unsupported transform proposal
- C. invalid IP packet SPI
- D. incompatible transform set

**Answer:** A

#### **NEW QUESTION 452**

As network security architect, you must implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity. Which technology should you use?

- A. IPsec DVTI
- B. FlexVPN
- C. DMVPN
- D. IPsec SVTI
- E. GET VPN

**Answer:** E

#### **NEW QUESTION 455**

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 458**

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 461**

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 463**



## Implementing Cisco Secure Mobility

**Comment**

**Scenario**

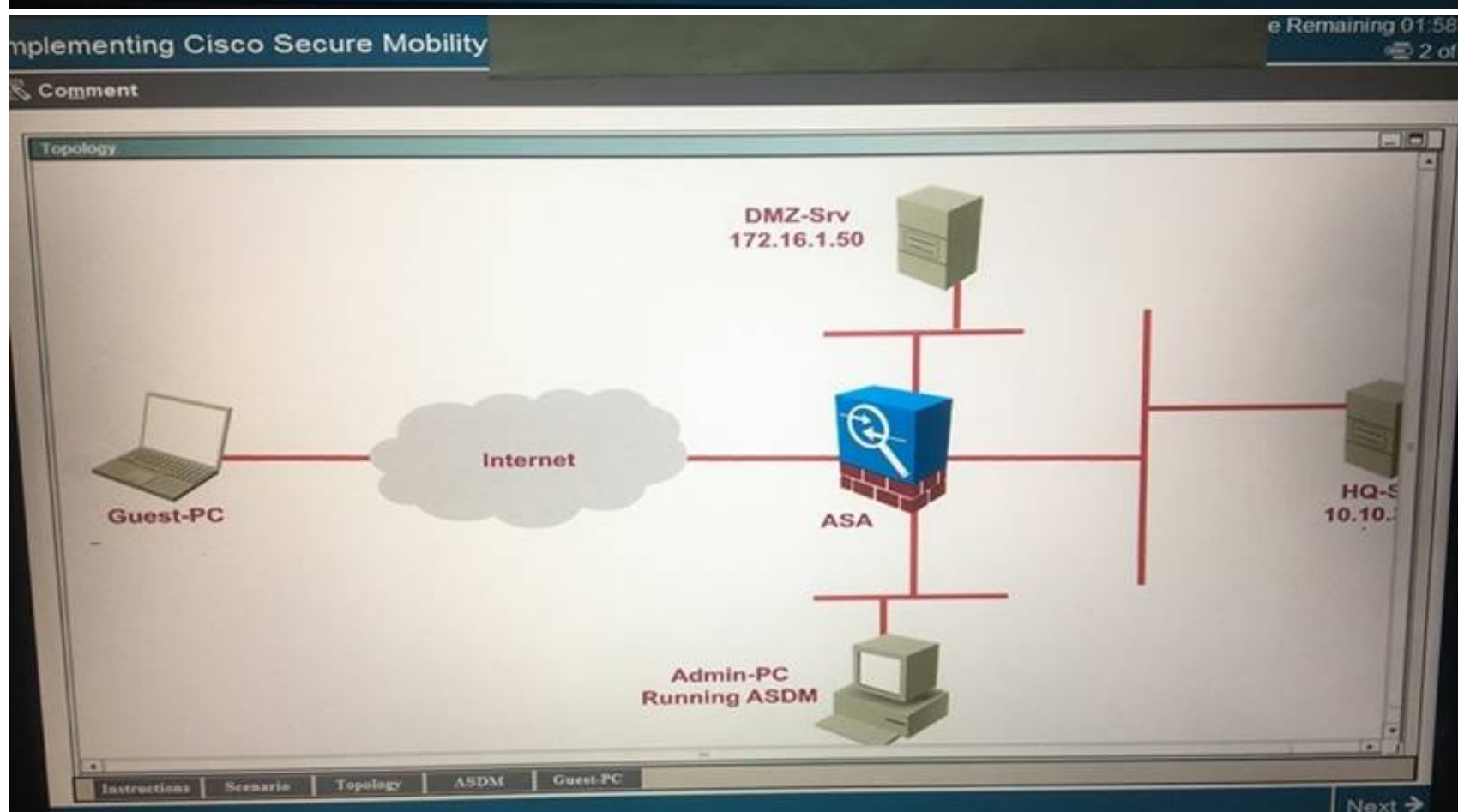
You are the network security manager for your organization. Your manager has received a request to allow an external user to access to your HQ

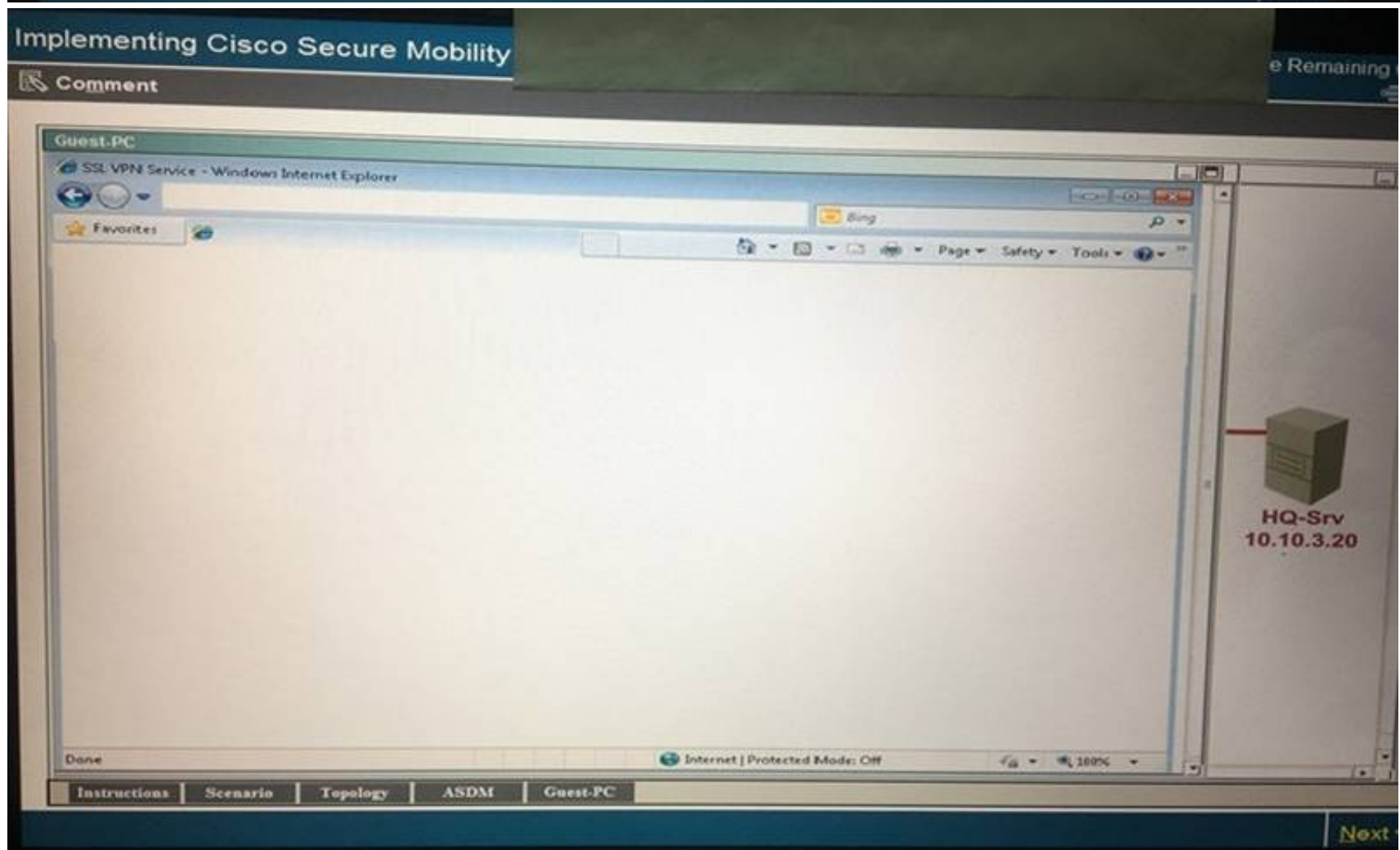
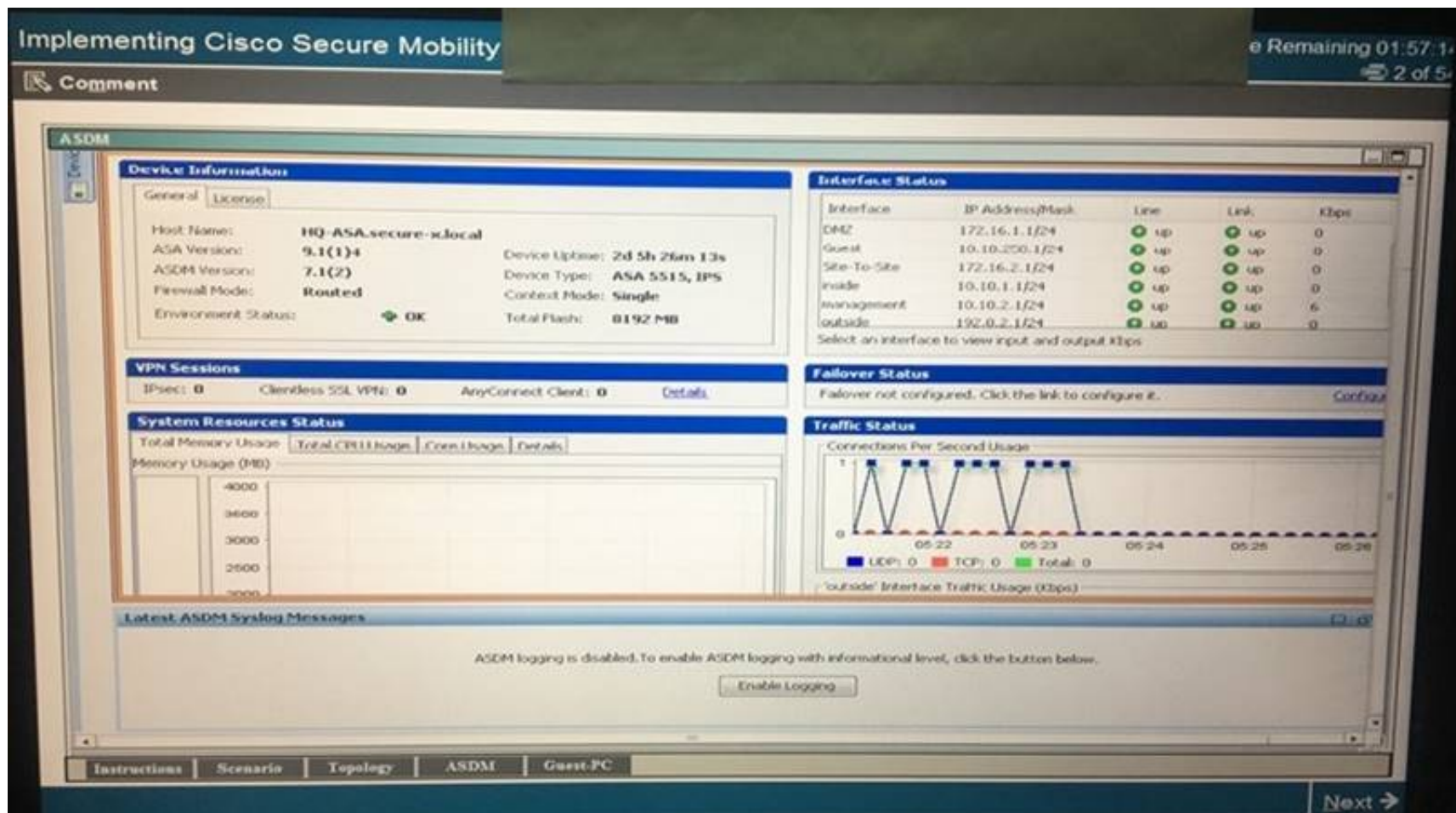
Using ASDM on the ASA, configure the parameters below and test your configuration by accessing the Guest PC. Not all ASDM screens are active

- 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://10.10.3.20>
  - a. You may notice a certificate error in the status bar, this can be ignored for this exercise
  - b. Username: **vpuser**
  - 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: vpuser**
- 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.

Instructions | Scenario | Topology | ASDM | Guest-PC





An engineer wants to ensure that employees cannot access corporate resources on untrusted networks, but does not want a new VPN session to be established each time they leave the trusted network. Which Cisco AnyConnect Trusted Network Policy option allows this ability?

- A. Pause
- B. Connect
- C. Do Nothing
- D. Disconnect

**Answer: A**

**NEW QUESTION 464**  
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 469

```
Spoke1#
local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
#pkts encaps: 200, #pkts encrypt: 200
#pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.2.1
inbound esp sas:
spi: 034B32CA36 (1261619766)
outbound esp sas:
spi: 0xD601918E (1760427022)

Spoke2#
local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
#pkts encaps: 210, #pkts encrypt: 210,
#pkts decaps: 200, #pkts decrypt: 200,
local crypto endpt.: 192.168.2.1,
remote crypto endpt.: 192.168.1.1
inbound esp sas:
spi: 03D601918E (1760427022)
outbound esp sas:
spi: 034BS2CA36 (1261619766)
```

Refer to the exhibit. An engineer is troubleshooting a new GRE over IPSEC tunnel. The tunnel is established, but the engineer cannot ping from spoke 1 to spoke 2. Which type of traffic is being blocked?

- A. ESP packets from spoke1 to spoke2
- B. ISAKMP packets from spoke2 to spoke1
- C. ESP packets from spoke2 to spoke1
- D. ISAKMP packets from spoke1 to spoke2

Answer: C

#### NEW QUESTION 473

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 476

Refer to the exhibit.



```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001:db8:100::1/64
!
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ikev2 ssl-client
 gateway-fqdn value asa.cisco.com
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
 anyconnect profiles value VPN type user
!
```

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
  <ClientInitialization>
    ...
    <IPProtocolSupport>IPv6,IPv4</IPProtocolSupport>
    ...
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>VPN</HostName>
      <HostAddress>asa.cisco.com</HostAddress> </HostEntry>
    </ServerList>
  </AnyConnectProfile>
```

Which technology does this configuration demonstrate?

- A. AnyConnect SSL over IPv4+IPv6
- B. AnyConnect FlexVPN over IPv4+IPv6
- C. AnyConnect FlexVPN IPv6 over IPv4
- D. AnyConnect SSL IPv6 over IPv4

**Answer:** A

#### NEW QUESTION 480

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.

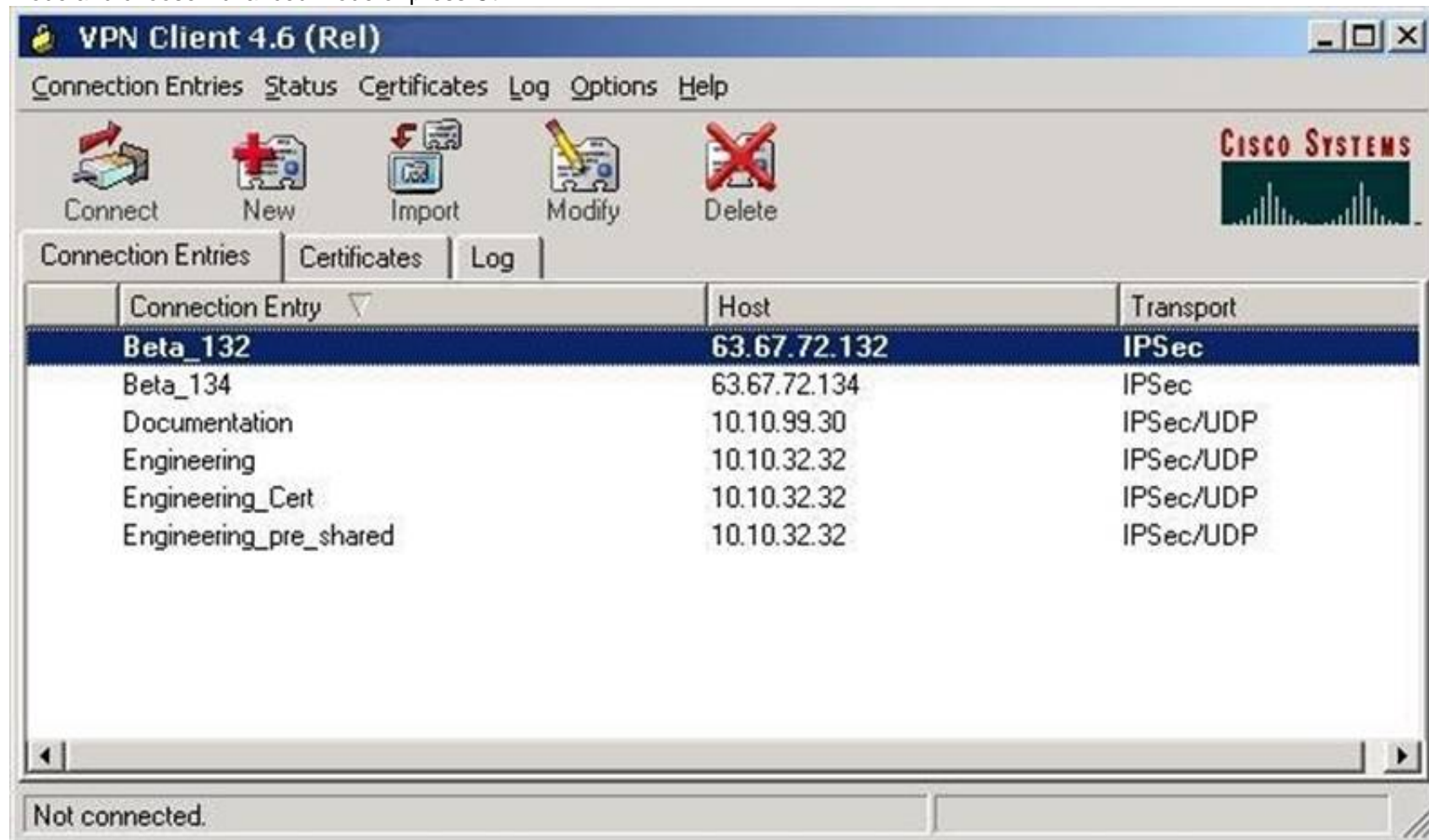
- C. In the Authentication tab, click the Group Authentication or Mutual Group Authentication radio button to enable symmetrical pre-shared key authentication.  
D. In the Name field, enter the name of the connection profile as it is specified on the Cisco ASA appliance.

**Answer: D**

**Explanation:** [http://www.cisco.com/en/US/docs/security/vpn\\_client/cisco\\_vpn\\_client/vpn\\_client46/win/user/guide/vc4.html#](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 482

A user is experiencing issues connecting to a Cisco AnyConnect VPN and receives this error message: The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again.

Which option is the likely cause of this issue?



- A. This Cisco ASA firewall has experienced a failure.
- B. The user is entering an incorrect password.
- C. The user's operating system is not supported with the ASA's current configuration.
- D. The user laptop clock is not synchronized with NTP.

**Answer:** A

#### NEW QUESTION 487

Refer to the exhibit.



The screenshot shows a web browser window titled "Login". Inside the window, there is a heading "Please enter your username and password." Below this, there are three input fields: "GROUP:" with a dropdown menu showing "contractor", "USERNAME:" with a text box, and "PASSWORD:" with a text box. At the bottom of the form is a "Login" button.

For the ABC Corporation, members of the NOC need the ability to select tunnel groups from a drop-down menu on the Cisco WebVPN login page. As the Cisco ASA administrator, how would you accomplish this task?

- A. Define a special identity certificate with multiple groups, which are defined in the certificate OU field, that will grant the certificate holder access to the named groups on the login page.
- B. Under Group Policies, define a default group that encompasses the required individual groups that will appear on the login page.
- C. Under Connection Profiles, define a NOC profile that encompasses the required individual profiles that will appear on the login page.
- D. Under Connection Profiles, enable "Allow user to select connection profile."

**Answer:** D

**Explanation:** Cisco ASDM User Guide Version 6.1

Add or Edit SSL VPN Connections > Advanced > SSL VPN

This dialog box lets you configure attributes that affect what the remote user sees upon login. Fields • Login Page Customization—Configures the look and feel of the user login page by specifying which preconfigured customization attributes to apply. The default is DfltCustomization. • Manage—Opens the Configure GUI Customization Objects window. • Connection Aliases—Lists in a table the existing connection aliases and their status and lets you add or delete items in that table. A connection alias appears on the user login page if the connection is configured to allow users to select a particular connection (tunnel group) at login. – Add—Opens the Add Connection Alias window, on which you can add and enable a connection alias. – Delete—Removes the selected row from the connection alias table. There is no confirmation or undo. • Group URLs—Lists in a table the existing group URLs and their status and lets you add or delete items in that table. A group URL appears on the user login page if the connection is configured to allow users to select a particular group at login. – Add—Opens the Add Group URL window, on which you can add and enable a group URL. – Delete—Removes the selected row from the connection alias table. There is no confirmation or undo.

#### NEW QUESTION 490

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 standby device; 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 492

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 495



Refer to the exhibit.

```

#Nov 26 00:52:20.002: IKEv2:(SESSION ID = 1,SA ID = 1):Received Packet [From 10.10.10.1:500/To 10.10.10.2:500/VRF i0:f0]
Initiator SPI : D6684E1462991856 - Responder SPI : 2162145C95256F6A Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
#Nov 26 00:52:20.002: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 236
Payload contents:
VID Next payload: IDr, reserved: 0x0, length: 20
IDr Next payload: AUTH, reserved: 0x0, length: 12
Id type: IPv4 address, Reserved: 0x0 0x0
AUTH Next payload: SA, reserved: 0x0, length: 28
Auth method PSK, reserved: 0x0, reserved 0x0
SA Next payload: TSi, reserved: 0x0, length: 40
last proposal: 0x0, reserved: 0x0, length: 36
Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: 3DES
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x0, reserved: 0x0: length: 8
type: 5, reserved: 0x0, id: Don't use ESN
TSi Next payload: TSr, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 30.30.30.0, end addr: 30.30.30.255
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
Num of TSs: 1, reserved 0x0, reserved 0x0
TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
start port: 0, end port: 65535
start addr: 20.20.20.0, end addr: 20.20.20.255
NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
Security protocol id: Unknown - 0, spi size: 0, type: SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: NON_FIRST_FRAGS

#Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Process auth response notify
#Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Searching policy based on peer's identity '10.10.10.1' of type 'IPv4 address'
#Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Failed to locate an item in the database
#Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Verification of peer's authentication data FAILED
#Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Auth exchange failed
#Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Router#
#Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Abort exchange
#Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA

```

The IKEv2 site-to-site VPN tunnel between two routers is down. Based on the debug output, which type of mismatch might be the problem?

- A. PSK
- B. crypto policy
- C. peer identity
- D. transform set

**Answer: C**

**NEW QUESTION 497**

Which algorith is an example of asymmetric encryption?

- A. RC4
- B. AES
- C. ECDSA
- D. 3DES

**Answer: C**

**NEW QUESTION 501**

Refer to the exhibit.

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

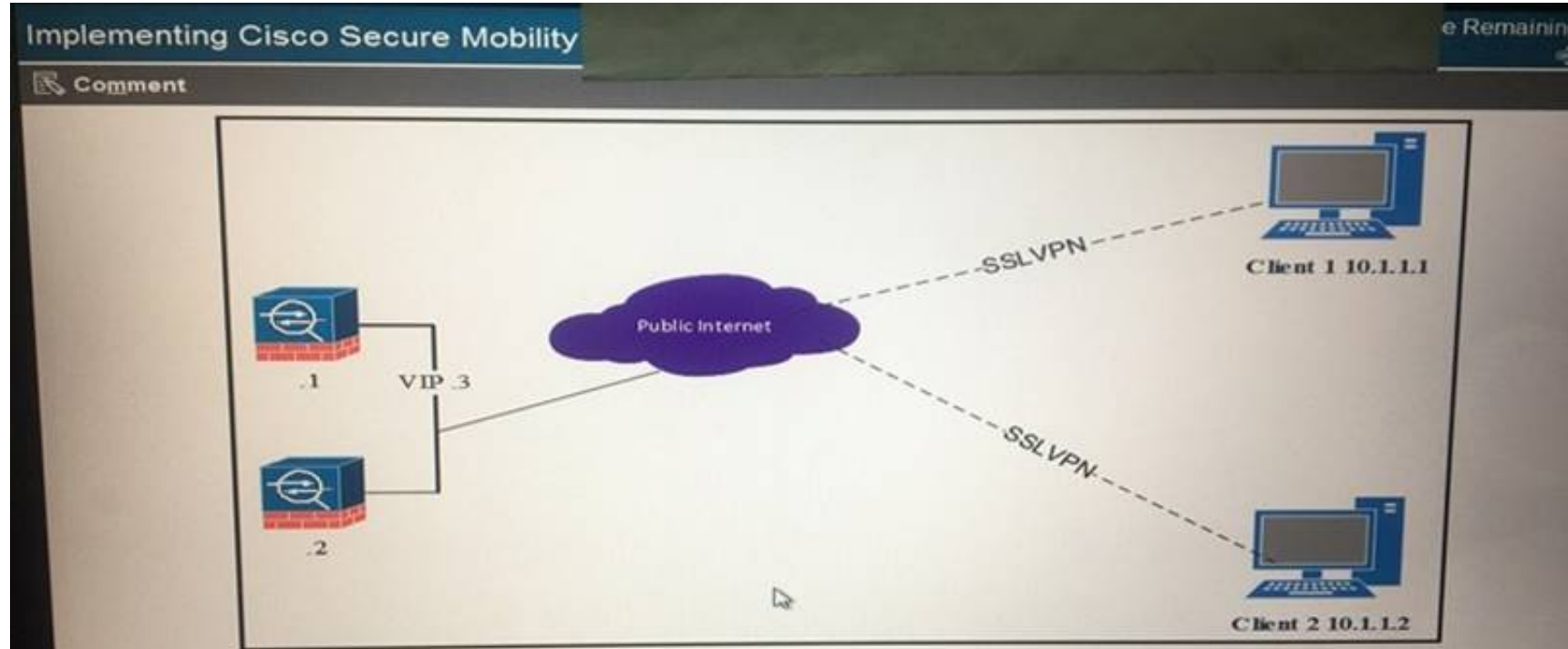
Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
employee1	15	Full	employee	-- Inherit Group Polic...	Add
manager1	2	No ASDM/CLI	management	-- Inherit Group Polic...	Edit
contractor	15	Full	-- Inherit Group Policy --	-- Inherit Group Polic...	Delete
contractor1	2	No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

The user "contractor" inherits which VPN group policy?

- A. employee
- B. management
- C. DefaultWEBVPNGroup
- D. DfltGrpPolicy
- E. new\_hire

**Answer: D**

**NEW QUESTION 502**



Refer to the exhibit. VPN load balancing provides a way to distribute remote access, IPsec, and SSL VPN connections across multiple security appliances. Which remote access client types does the load balancing feature support?

- A. IPsec site-to-site tunnels
- B. L2TP over IPsec
- C. OpenVPN
- D. Cisco AnyConnect Secure Mobility Client

**Answer: B**

**NEW QUESTION 504**

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 outdated.
- D. The installed version of Java is not compatible with Cisco AnyConnect.

**Answer: C**

**NEW QUESTION 508**

A temporary worker must use clientless SSL VPN with an SSH plug-in, in order to access the console of an internal corporate server, the projects.xyz.com server. For security reasons, the network security auditor insists that the temporary user is restricted to the one internal corporate server, 10.0.4.18. You are the network engineer who is responsible for the network access of the temporary user.

What should you do to restrict SSH access to the one projects.xyz.com server?

- A. Configure access-list temp\_user\_acl extended permit TCP any host 10.0.4.18 eq 22.
- B. Configure access-list temp\_user\_acl standard permit host 10.0.4.18 eq 22.
- C. Configure access-list temp\_acl webtype permit url ssh://10.0.4.18.
- D. Configure a plug-in SSH bookmark for host 10.0.4.18, and disable network browsing on the clientless SSL VPN portal of the temporary worker.

**Answer: C**

**Explanation:** Web ACLs

The Web ACLs table displays the filters configured on the security appliance applicable to Clientless SSL VPN traffic. The table shows the name of each access control list (ACL), and below and indented to the right of the ACL name, the access control entries (ACEs) assigned to the ACL. Each ACL permits or denies access permits or denies access to specific networks, subnets, hosts, and web servers. Each ACE specifies one rule that serves the function of the ACL. You can configure ACLs to apply to Clientless SSL VPN traffic. The following rules apply:

- If you do not configure any filters, all connections are permitted.
- The security appliance supports only an inbound ACL on an interface.
- At the end of each ACL, an implicit, unwritten rule denies all traffic that is not explicitly permitted. You can use the following wildcard characters to define more than one wildcard in the Webtype access list entry:
- Enter an asterisk "\*" to match no characters or any number of characters.
- Enter a question mark "?" to match any one character exactly.
- Enter square brackets "[]" to create a range operator that matches any one character in a range. The following examples show how to use wildcards in Webtype access lists.
- The following example matches URLs such as `http://www.cisco.com/` and `http://www.caco.com/`: `access-list test webtype permit url http://ww?.c*co*/`

**NEW QUESTION 509**

After adding a remote-access IPsec tunnel via the VPN wizard, an administrator needs to tune the IPsec policy parameters. Where is the correct place to tune the IPsec policy parameters in Cisco ASDM?

- A. IPsec user profile
- B. Crypto Map
- C. Group Policy
- D. IPsec Policy
- E. IKE Policy

**Answer: B**

#### NEW QUESTION 514

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 515

Which option is the main difference between GET VPN and DMVPN?

- A. AES encryption support
- B. dynamic spoke-to-spoke tunnel communications
- C. Next Hop Resolution Protocol
- D. Group Domain of Interpretation protocol

**Answer:** B

#### NEW QUESTION 520

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 524

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 528

While attempting to establish a site-to-site VPN, the engineer notices that phase 1 of the VPN tunnel fails. The engineer wants to run a capture to confirm that the outside interface is receiving phase 1 information from the thirdparty peer address. Which command must be run on the ASA to verify this information?

- A. capture capin interface outside match ipsec any any
- B. capture capin interface outside match gre any any
- C. capture capin interface outside match ah any any
- D. capture capin interface outside match udp any eq 500 any eq 500
- E. capture capin interface outside match Udp any eq 123 any eq 121

**Answer:** D

#### NEW QUESTION 529

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 534

Which two attributes can be matched from the identity of the remote peer when using IKEv2 Name Manager? (Choose two.)

- A. fqdn
- B. hostname
- C. IP address
- D. kerberos

**Answer:** AB



**NEW QUESTION 536**

An engineer is configuring IPsec VPN and wants to choose an authentication protocol that is reliable supports ACK and sequence. Which protocol accomplishes this goal?

- A. ESP
- B. AES-192
- C. IKEv1
- D. AES-256

**Answer:** A

**NEW QUESTION 538**

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 539**

.....

## 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](#)**