CCNA Security

Number: 210-260
Passing Score: 860
Time Limit: 45 min
File Version: 1.0

CCNA Security 210-260 11/2/2015

Exam A

QUESTION 1
What is the purpose of the Integrity component of the CIA triad?

A. to ensure that only authorized parties can modify data
B. to determine whether data is relevant
C. to create a process for accessing data
D. to ensure that only authorized parties can view data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which two statements about Telnet access to the ASA are true? (Choose two).

A. You may VPN to the lowest security interface to telnet to an inside interface.
B. You must configure an AAA server to enable Telnet.
C. You can access all interfaces on an ASA using Telnet.
D. You must use the command virtual telnet to enable Telnet.
E. Best practice is to disable Telnet and use SSH.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What is an advantage of placing an IPS on the inside of a network?

A. It can provide higher throughput.
B. It receives traffic that has already been filtered.
C. It receives every inbound packet.
D. It can provide greater security.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which three statements about host-based IPS are true? (Choose three.)

A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
What type of security support is provided by the Open Web Application Security Project?

A. Education about common Web site vulnerabilities.
B. A Web site security framework.
C. A security discussion forum for Web site developers.
D. Scoring of common vulnerabilities and exposures.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What is the FirePOWER impact flag used for?

A. A value that indicates the potential severity of an attack.
B. A value that the administrator assigns to each signature.
C. A value that sets the priority of a signature.
D. A value that measures the application awareness.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which two services define cloud networks? (Choose two.)

A. Infrastructure as a Service
B. Platform as a Service
C. Compute as a Service
D. Security as a Service
E. Tenancy as a Service

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?

A. It configures the device to begin transmitting the authentication key to other devices at 00:00:00 local time on January 1, 2014 and continue using the key indefinitely.
B. It configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely.
C. It configures the device to begin accepting the authentication key from other devices immediately and stop accepting the key at 23:59:00 local time on December 31, 2013.

D. It configures the device to generate a new authentication key and transmit it to other devices at 23:59 00 local time on December 31, 2013.

E. It configures the device to begin accepting the authentication key from other devices at 23:59:00 local time on December 31, 2013 and continue accepting the key indefinitely.

F. It configures the device to begin accepting the authentication key from other devices at 00:00:00 local time on January 1, 2014 and continue accepting the key indefinitely.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason could the image file fail to appear in the dir output?

A. The secure boot-image command is configured

B. The secure boot-comfit command is configured

C. The confreg 0x24 command is configured.

D. The reload command was issued from ROMMON.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
What is a reason for an organization to deploy a personal firewall?

A. To protect endpoints such as desktops from malicious activity

B. To protect one virtual network segment from another

C. To determine whether a host meets minimum security posture requirements

D. To create a separate, non-persistent virtual environment that can be destroyed after a session

E. To protect the network from DoS and syn-flood attacks

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 11
Which FirePOWER preprocessor engine is used to prevent SYN attacks?

A. Rate-Based Prevention
B. Portscan Detection
C. IP Defragmentation
D. Inline Normalization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What VPN feature allows traffic to exit the security appliance through the same interface it entered?

A. Hairpinning
B. NAT
C. NAT traversal
D. split tunneling

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
What are two default Cisco IOS privilege levels? (Choose two)

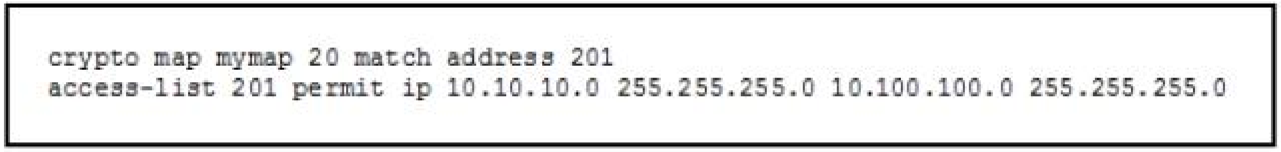
A. 0
B. 5

C. 1
D. 7
E. 10
F. 15

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14



```
crypto map mymap 20 match address 201
access-list 201 permit ip 10.10.10.0 255.255.255.0 10.100.100.0 255.255.255.0
```

What is the effect of the given command sequence?

A. It defines IPSec policy for traffic sourced from 10.10.10.0/24 with a desstination of 10.100.100.0/24
B. It defines IPSec policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24
C. it defines IKE policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24
D. It defines IKE policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which tool can an attacker use to attempt a DDos attack?

A. botnet

B. Trojan horse
C. virus
D. adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
how does the Cisco ASA use Active Directory to authorize VPN users?

A. It queries the Active Directory server for a Specfic attribute for the specific user
B. It sends the username and password to retire an ACCEPT or Reject message from the Active Directory server
C. It downloads and stores the Active Directory databas to query for future authorization
D. It redirects requests to the Active Directory server defined for the VPN group

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
In a security context, which action can you take to address compliance?

A. Implement rules to prevent a vulnerability
B. Correct or counteract a vulnerability
C. Reduce the severity of a vulnerability
D. Follow directions from the security appliance manufacturer to remediate a vulnerability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

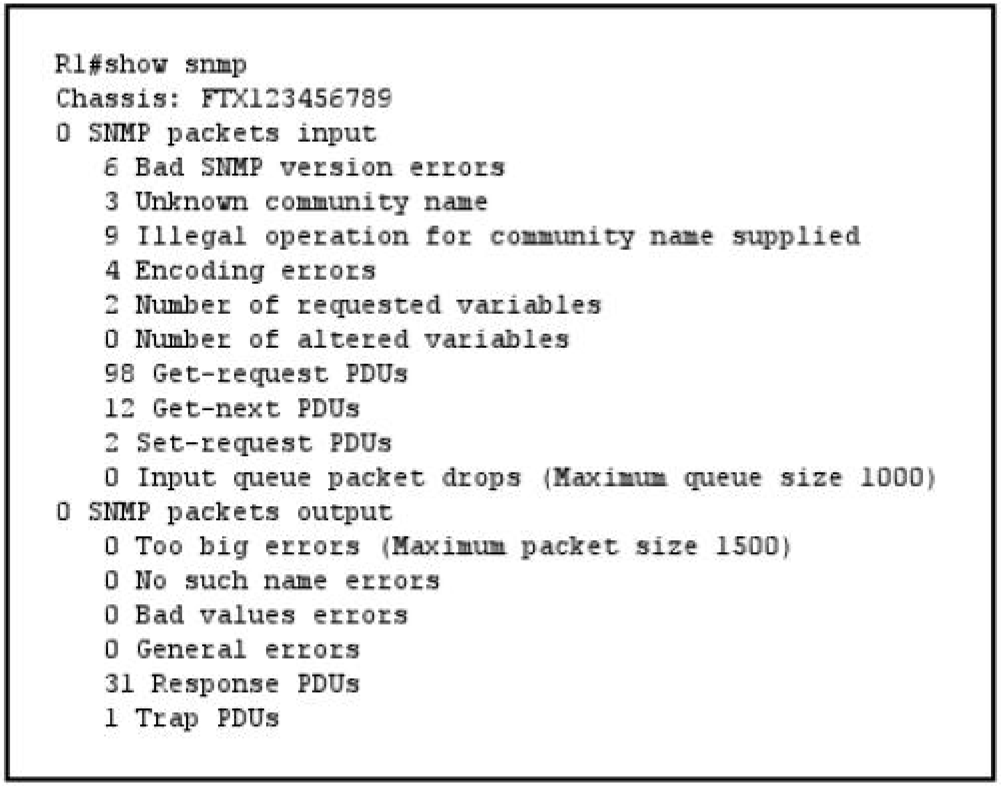
QUESTION 18
What can the SMTP preprocessor in a FirePOWER normalize?

A. It can extract and decode email attachments in client to server traffic
B. It can look up the email sender
C. it compares known threats to the email sender
D. It can forward the SMTP traffic to an email filter server
E. It uses the Traffic Anomaly Detector

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19



```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
   6 Bad SNMP version errors
   3 Unknown community name
   9 Illegal operation for community name supplied
   4 Encoding errors
   2 Number of requested variables
   0 Number of altered variables
   98 Get-request PDUs
   12 Get-next PDUs
   2 Set-request PDUs
   0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   0 No such name errors
   0 Bad values errors
   0 General errors
   31 Response PDUs
   1 Trap PDUs
```

How many times was a read-only string used to attempt a write operation?

A. 6
B. 9
C. 4
D. 3
E. 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
You want to allow all of your companies users to access the Internet without allowing other Web servers to collect the IP addresses of individual users.
What two solutions can you use? (Choose two).

A. Configure a proxy server to hide users local IP addresses
B. Assign unique IP addresses to all users.
C. Assign the same IP addresses to all users
D. Install a Web content filter to hide users local IP addresses
E. Configure a firewall to use Port Address Translation.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

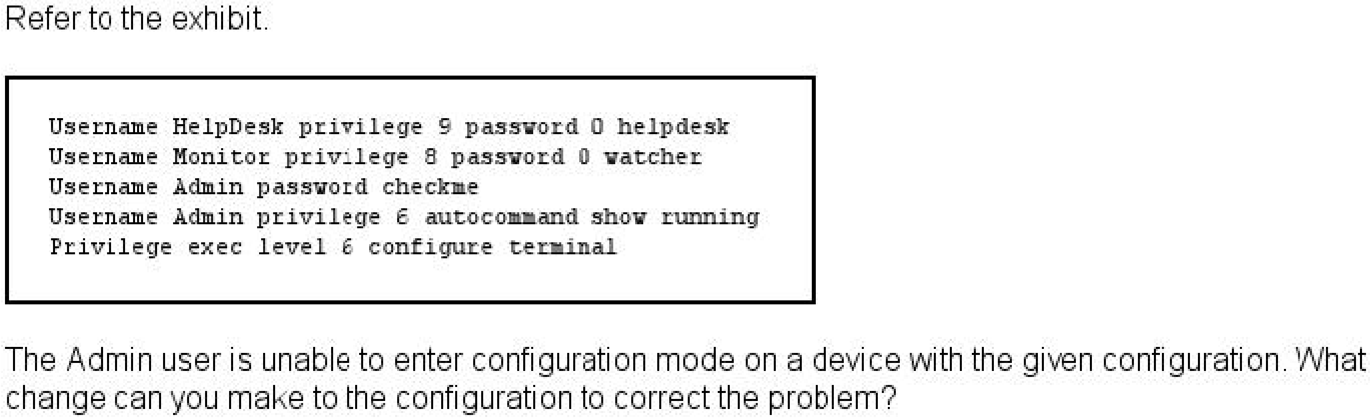
QUESTION 21
Which two authentication types does OSPF support? (Choose two)

A. plaintext
B. MD5
C. HMAC
D. AES 256
E. SHA-1
F. DES

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22



Refer to the exhibit.

```
Username HelpDesk privilege 9 password 0 helpdesk
Username Monitor privilege 8 password 0 watcher
Username Admin password checkme
Username Admin privilege 6 autocommand show running
Privilege exec level 6 configure terminal
```

The Admin user is unable to enter configuration mode on a device with the given configuration. What change can you make to the configuration to correct the problem?

A. Remove the Autocommand keyword and arguments from the Username Admin privilege line
B. Change the Privilege exec level value to 15
C. Remove the two Username Admin lines
D. Remove the Privilege exec line.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What command can you use to verify the binding table status?

A. Show ip dhcp snooping binding
B. Show ip dhcp snooping database
C. show ip dhcp snooping statistics
D. show ip dhcp pool
E. show ip dhcp source binding
F. show ip dhcp snooping

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 24
Which statement about application blocking is true?

A. It blocks access to files with specific extensions
B. It blocks access to specific network addresses
C. It blocks access to specific programs
D. It blocks access to specific network services.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
For what reason would you configure multiple security contexts on the ASA firewall?

A. To enable the use of VFRs on routers that are adjacently connected
B. To provide redundancy and high availability within the organization
C. To enable the use of multicast routing and QoS through the firewall
D. To seperate different departments and business units

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which statement about communication over failover interfaces is true?

A. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default.
B. All information that is sent over the failover and stateful failover interfaces is encrypted by default

C. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default
D. Usernames, password and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is sent as clear text

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which three ESP fields can be encrypted during transmission? (Choose three)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length
F. Next Header

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
According to Cisco best practices, which three protocols should the default ACL allow an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three)

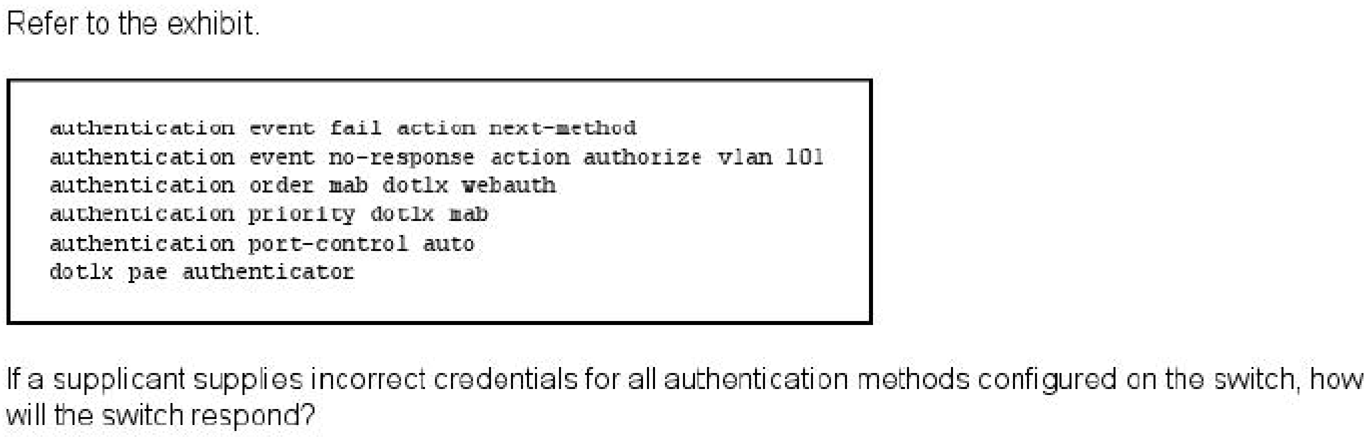
A. BOOTP
B. TFTP
C. DNS
D. MAB
E. HTTP
F. 802.1x

Correct Answer: ABC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 29



Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dot1x webauth
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
```

If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

A. The switch will cycle through the configured authentication methods indefinitely
B. The supplicant will fail to advance beyond the webauth method.
C. The authentication attempt will time out and the switch will place the port into the unathorized state
D. The authentication attempt will time out and the switch will place the port into VLAN 101

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which SOURCEFIRE logging action should you choose to record the most detail about a connection.

A. Enable logging at the beginning of the session
B. Enable logging at the end of the session
C. Enable alerts via SNMP to log events off-box

D. Enable eStreamer to log events off-box

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
What type of algorithm uses the same key to encryp and decrypt data?

A. a symmetric algorithm
B. an asymetric algorithm
C. a Public Key infrastructure algorithm
D. an IP Security algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

A. The ASA will apply the actions from only the most specific matching class map it finds for the feature type
B. The ASA will apply the actions from all matching class maps it finds for the feature type
C. The ASA will apply the actions from only the last matching class map it finds for the feature type.
D. The ASA will apply the actions from only the first matching class map it finds for the feature type.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP address Reputation. A user calls

and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

A. Create a custom blacklist to allow traffic
B. Create a whitelist and add the appropriate IP address to allow traffic.
C. Create a user based access control rule to allo the traffic.
D. Create a network based access control rule to allow the traffic.
E. Create a rule to bypass inspection to allow the traffic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which EAP method uses protected Access Credentials?

A. EAP-TLS
B. EAP-PEAP
C. EAP-FAST
D. EAP-GTC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
In which two situations should you use out-of-band management? (Choose two)

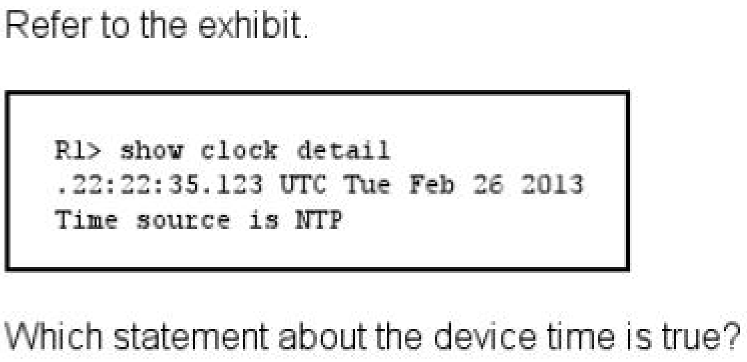
A. when a network device fails to forward packets
B. when management applications need concurrent access to the device
C. when you require ROMMON access
D. when you require adminstrator access from multiple locations
E. when the control plane fails to respond

Correct Answer: AC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 36



Refer to the exhibit.

```
R1> show clock detail
.22:22:35.123 UTC Tue Feb 26 2013
Time source is NTP
```

Which statement about the device time is true?

A. The time is authoritative because the clock is in sync
B. The time is authoritative, but the NTP process has lost contact with its servers
C. The clock is out of sync
D. NTP is configured incorrectly
E. The time is not authoritative

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
In what type of attack does an attacker virtually change a devices burned in address in an attempt to circumvent access lists and mask the device's true identity?

A. gratuitous ARP
B. ARP poisoning

C. IP Spoofing
D. MAC Spoofing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which Statement about personal firewalls is true?

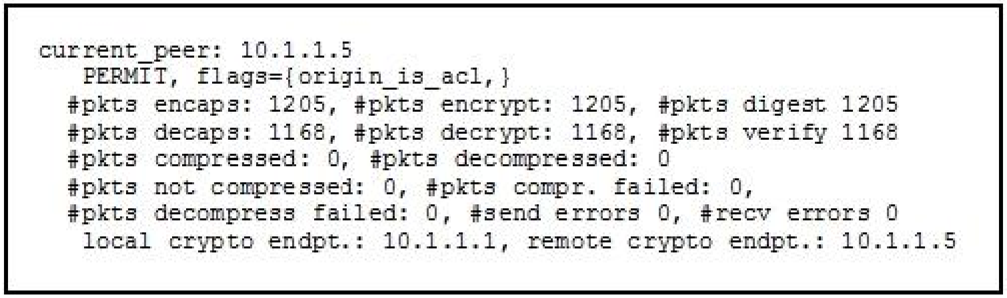
A. They are resilient against kernal attacks
B. They can protect email messages and private documents in a similar way to a VPN
C. They can protect the network against attacks
D. They can protect a system by denying probing requests

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39

Refer to the exhibit.



```
current_peer: 10.1.1.5
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 1205, #pkts encrypt: 1205, #pkts digest 1205
  #pkts decaps: 1168, #pkts decrypt: 1168, #pkts verify 1168
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 0, #recv errors 0
   local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.5
```

While troubleshooting site-to-site VPN, you issued the show crypto ipsec sa command. What does the given output show?

A. ISAKMP security associations are established between 10.1.1.5 and 10.1.1.1
B. IPSec Phase 2 is established between 10.1.1.1 and 10.1.1.5
C. IKE version 2 security associations are established between 10.1.1.1 and 10.1.1.5
D. IPSec Phase 2 is down due to a mismatch between encrypted and decrypted packets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which statement about a PVLAN isolated port configured on a switch is true?

A. The isolated port can communicate only with the promiscous port
B. The isolated port can communicate with other isolated ports and the promiscuous port
C. The isolated port can communicate only with community ports
D. The isolated port can communicate only with other isolated ports

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 41
Which three statements about host-based IPS are true? (Choose three)

A. It can view encrypted files
B. It can be deployed at the perimeter
C. It uses signature-based policies
D. It can have more restrictive policies than network-based IPS
E. It works with deployed firewalls
F. It can generate alerts based on behavior at the desktop level.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
What type of security support is provided by the Open Web Application Security Project?

A. Education about common Web site vulnerabilities
B. A wb site security framework
C. A security discussion forum for Web site developers
D. Scoring of common vulnerabilities and exposures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
How does a zone-based firewall implementation handle traffic between Interfaces in the same Zone?

A. traffic between interfaces in the same zone is blocked unless yoc configure the same-security permit command
B. Traffic between interfaces in the same zone is always blocked
C. Traffic between two interfaces in the same zone is allowed by default
D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain
D. The switch could become a transparent bridge.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which two next generation encrytption algorithms does Cisco recommend? (Choose two)

A. AES
B. 3DES
C. DES
D. MD5
E. DH-1024
F. SHA-384

Correct Answer: AF
Section: (none)

Explanation

Explanation/Reference:

QUESTION 46
What three actions are limitations when running IPS in promiscous mode? (Choose three)

A. deny attacker
B. request block connection
C. deny packet
D. modify packet
E. request block host
F. reset TCP connection

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which two feature do CoPP and CPPr use to protect the control plane? (Choose two)

A. QoS
B. traffic classification
C. access lists
D. policy maps
E. class maps
F. Cisco Express Forwarding

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

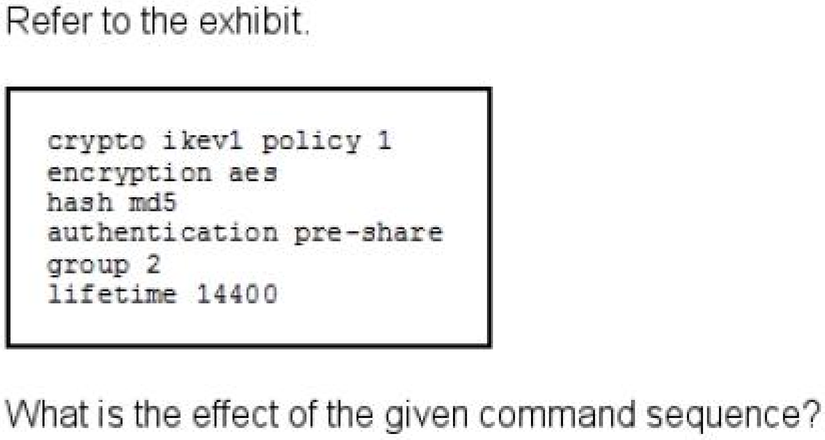
What is an advantage of implementing a Trusted Platform Module for disk encryption?

A. It provides hardware authentication
B. It allows the hard disk to be transferred to another device without requiring re-encryption.dis
C. it supports a more complex encryption algorithm than other disk-encryption technologies.
D. it can protect against single poins of failure.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49



Refer to the exhibit.

```
crypto ikev1 policy 1
encryption aes
hash md5
authentication pre-share
group 2
lifetime 14400
```

What is the effect of the given command sequence?

A. It configures IKE Phase 1
B. It configures a site-to-site VPN Tunnel
C. It configures a crypto policy with a key size of 14400
D. It configures IPSec Phase 2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A specific URL has been identified as containing malware. What action can you take to block users from accidentaly visiting the URL and becoming infected with malware?

A. Enable URL filtering on the perimeter firewall and add the URLs you want to allow to the routers local URL list
B. Enable URL filtering on the perimeter router and add the URLs you want to allow to the firewalls local URL list
C. Create a blacklist that contains the URL you want to block and activate the blacklist on the perimeter router.
D. Enable URL filtering on the perimeter router and add the URLs you want to block to the routers local URL list
E. Create a whitelist that contains the URls you want to allow and activate the whitelist on the perimeter router.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
If you change the native VLAN on the port to an unused VLAN, what happens if an attacker attempts a double tagging attack?

A. The trunk port would go into an error-disable state.
B. A VLAN hopping attack would be successful
C. A VLAN hopping attack would be prevented
D. the attacked VLAN will be pruned

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Perform a Layer 6 reset

B. Deploy an antimalware system
C. Enable bypass mode
D. Deny the connection inline

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which statement about Cisco ACS authentication and authorization is true?

A. ACS servers can be clustered to provide scalability
B. ACS can query multiple Active Directory domains
C. ACS uses TACACS to proxy other authentication servers
D. ACS can use only one authorization profile to allo or deny requests

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
What is the only permitted operation for processing multicast traffic on zone-based firewalls?

A. Stateful inspection of multicast traffic is supported only for the self zone
B. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone
C. Only control plane policing can protect the control plane against multicast traffic.
D. Stateful inspection of multicast traffic is supported only for the internal zone.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
If a switch receives a superior BPDU and goes directly into a blocked state, what mecanism must be in use?

A. Etherchannel guard
B. root guard
C. loop guard
D. BPDU guard

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

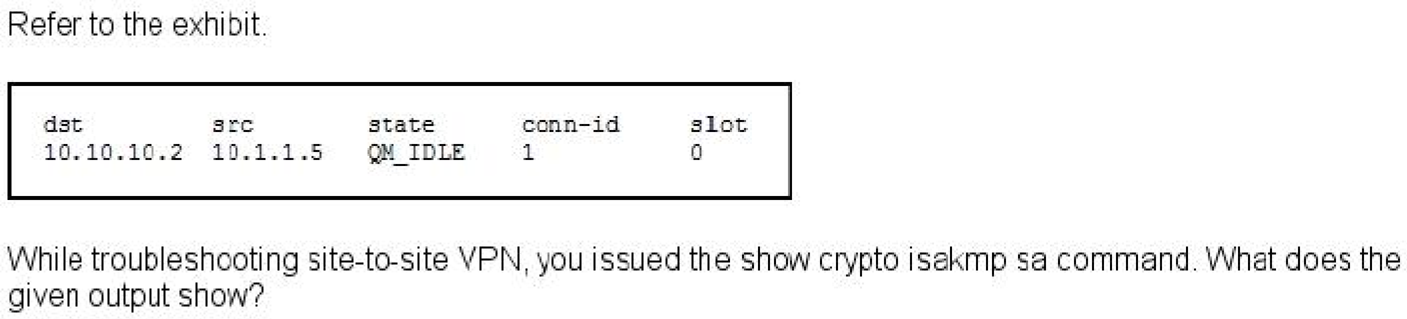
QUESTION 56
What type of packet creates and performs network operations on a network device?

A. data plane packets
B. management plane packets
C. services plane packets
D. control plane packets

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57



Refer to the exhibit.

```
dst         src        state      conn-id     slot
10.10.10.2  10.1.1.5   QM_IDLE    1           0
```

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

A. IPSec Phase 1 is established between 10.10.10.2 and 10.1.1.5
B. IPSec Phase 2 is established between 10.10.10.2 and 10.1.1.5
C. IPSec Phase 1 is down due to a QM_IDLE state
D. IPSEc Phase 2 is down due to a QM_IDLE state

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
What type of attack was the Stuxnet virus?

A. cyber warfare
B. hactivism
C. botnet
D. social engineering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which type of secure connectivity does an extranet provide?

A. remote branch offices to your company network
B. your company network to the Internet
C. new networks to your company network
D. other company networks to your company network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection.

A. split tunneling
B. hairpinning
C. tunnel mode
D. transparent mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
When is the best time to perform an anti-virus signature update?

A. When the local scanner has detected a new virus
B. When a new virus is discovered in the wild
C. Every time a new update is available
D. When the system detects a browser hook

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62

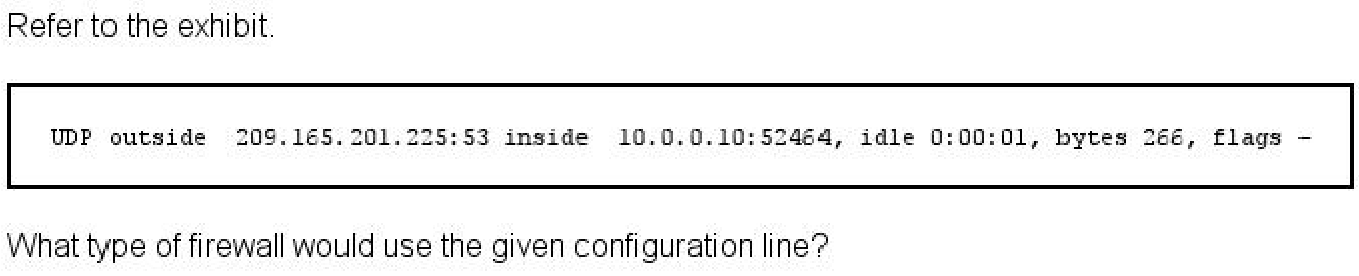
What is one requirement for locking a wired or wireless device from ISE?

A. The ISE agent must be installed on the device
B. The device must be connnected to the network when the lock command is executed
C. The user must approve the locking action
D. The organization must implement an acceptable use policy allowing device locking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63



Refer to the exhibit.

```
UDP outside  209.165.201.225:53 inside  10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

What type of firewall would use the given configuration line?

A. a stateful firewall
B. a personal firewall
C. a proxy firewall
D. an application firewall
E. a stateless firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
In which three ways does the TACACS protocol differ from RADIUS? (Choose three)

A. TACACS uses TCP to communicate with the NAS
B. TACACS can encrypt the entire packet that is sent to the NAS
C. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted
D. TACACS uses UDP to communicate with the NAS
E. TACACS encrypts only the password field in an authentication packet
F. TACACS support per-command authorization

Correct Answer: ABF
Section: (none)
Explanation

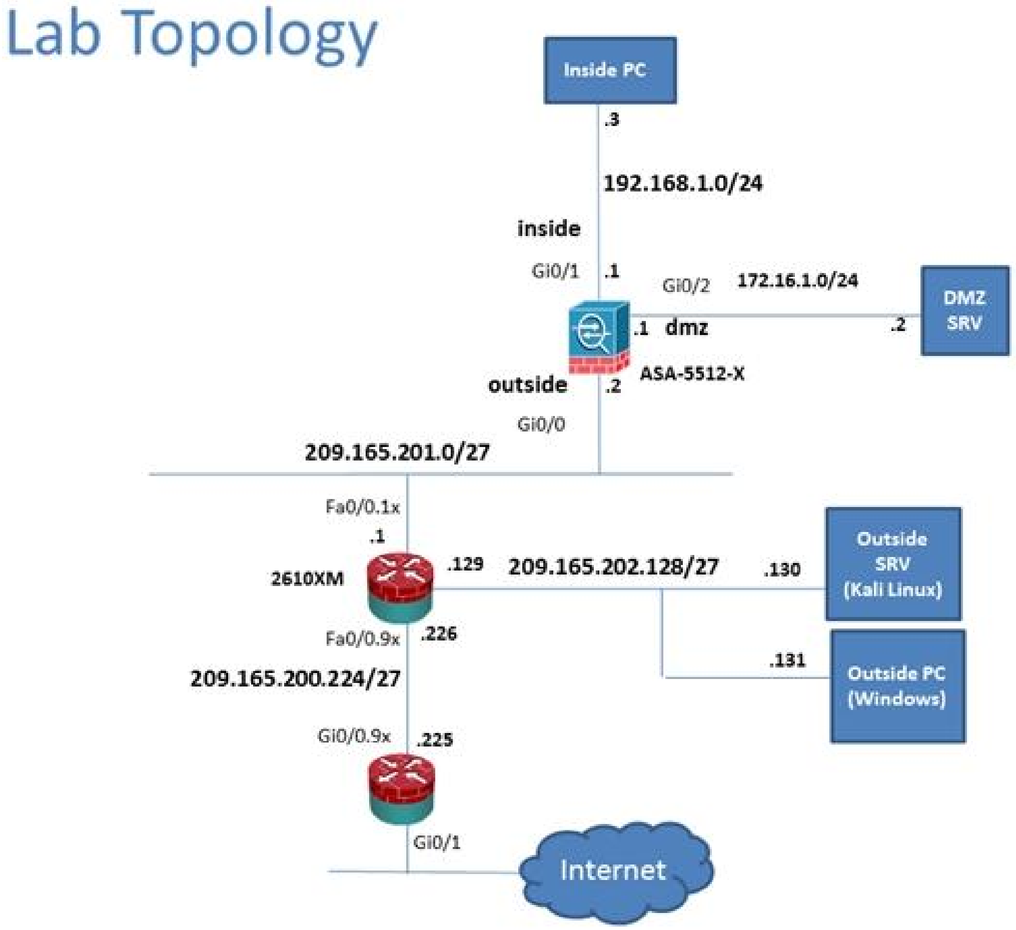
Explanation/Reference:

QUESTION 65

Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questio

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

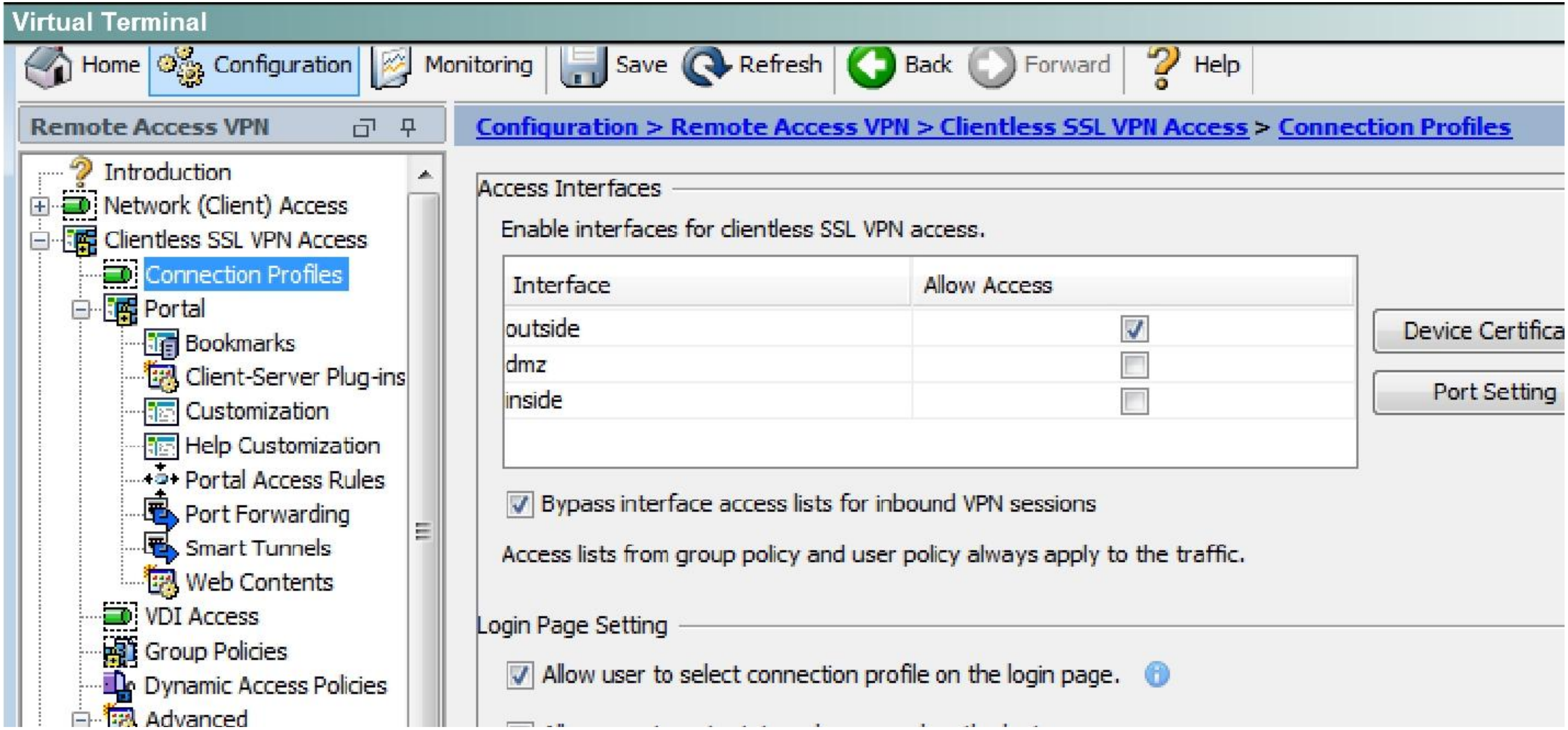


Which user authentication method is used when users login to the Clientless SSL VPN portal using https://209165.201.2/test?

A. Both Certificate and AAA with LOCAL database
B. AAA with RADIUS server
C. Both Certificate and AAA with RADIUS server
D. AAA with LOCAL database
E. Certificate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:



Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Access Interfaces

Enable interfaces for clientless SSL VPN access.

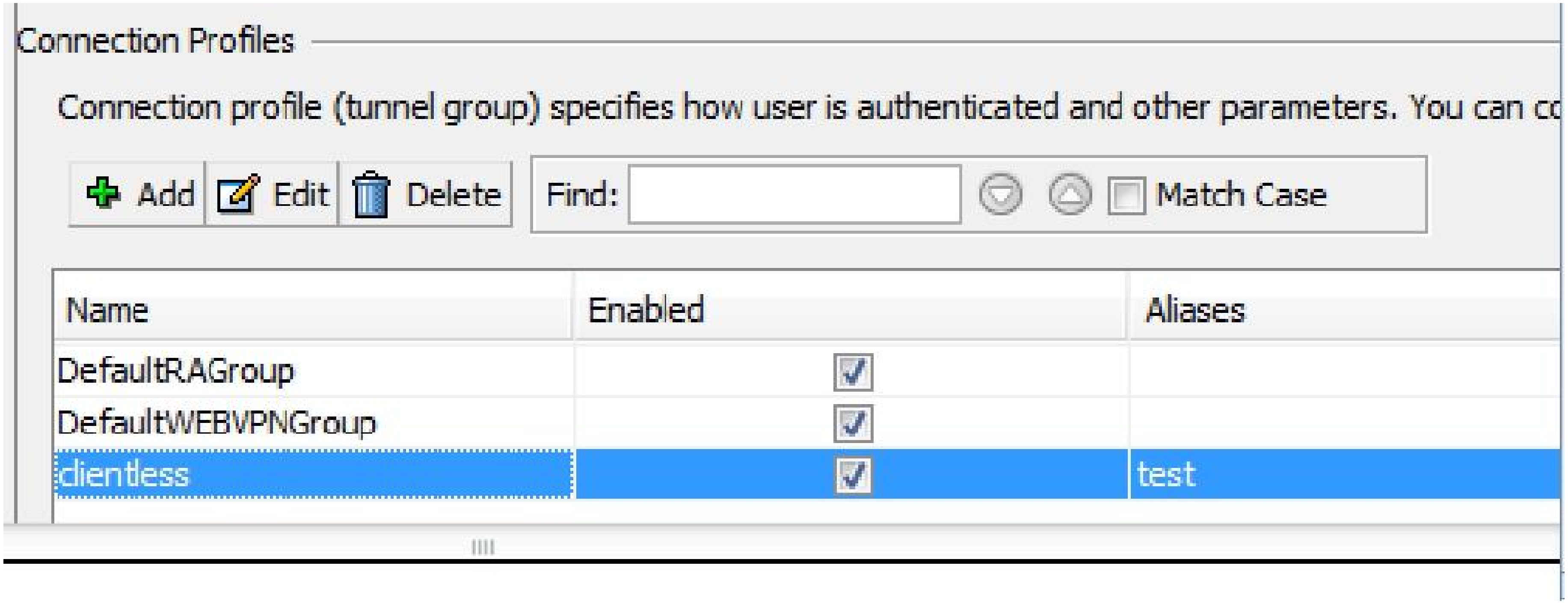
Interface	Allow Access
outside	☑
dmz	□
inside	□

☑ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

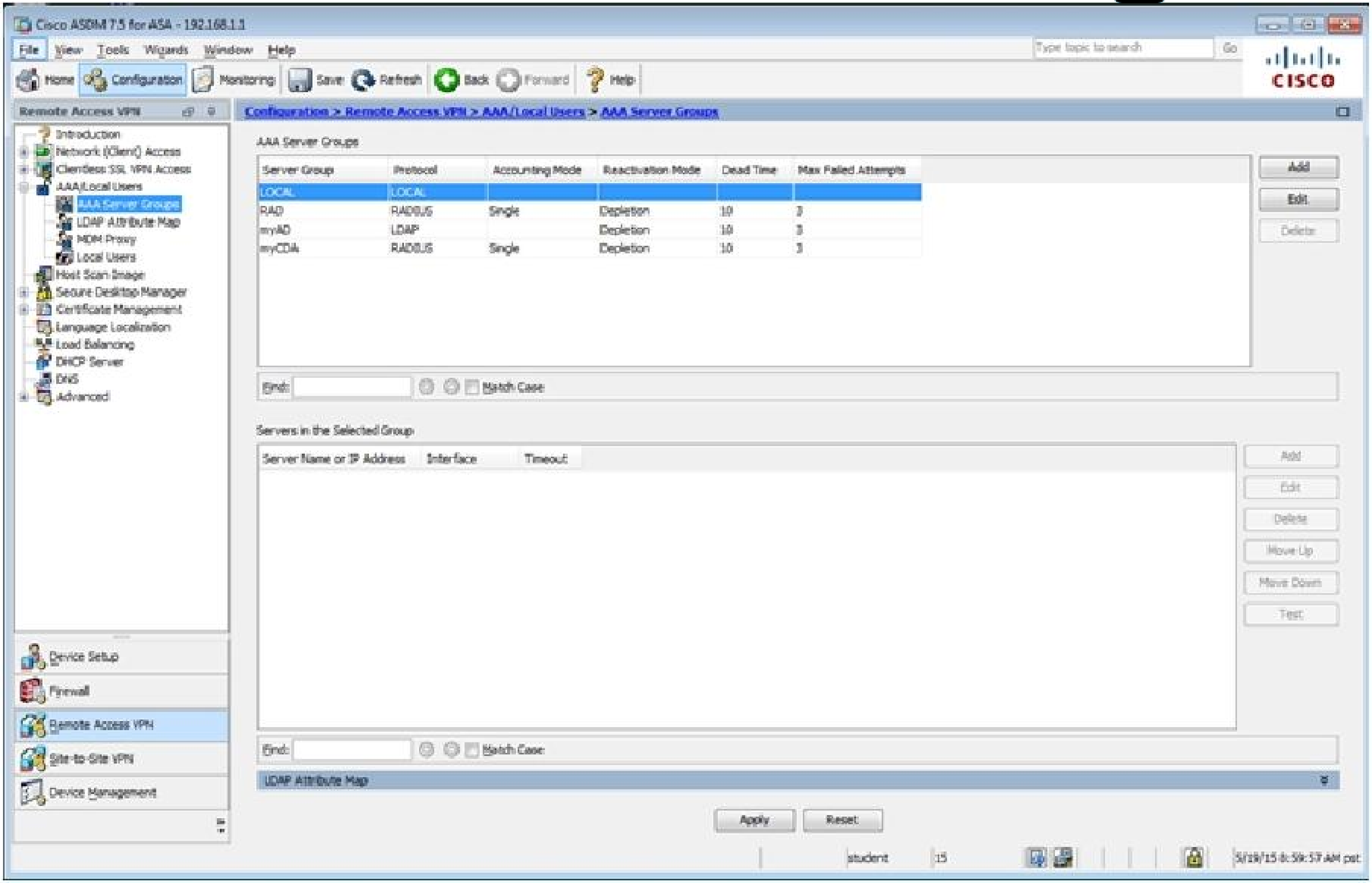
☑ Allow user to select connection profile on the login page.



Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can co

Name	Enabled	Aliases
DefaultRAGroup	☑	
DefaultWEBVPNGroup	☑	
clientless	☑	test



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

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
RAD	RADIUS	Single	Depletion	10	3
myAD	LDAP		Depletion	10	3
myCDA	RADIUS	Single	Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout

student 15 5/19/15 8:59:57 AM pst

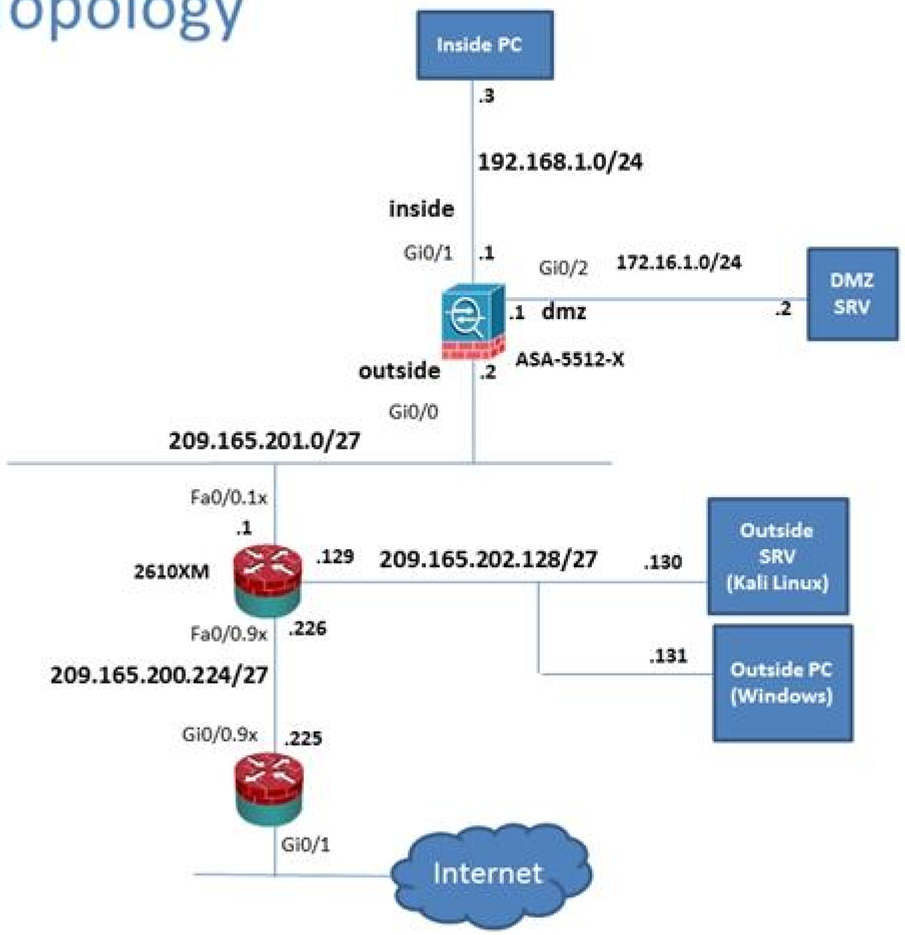
QUESTION 66

Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice q

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

Lab Topology

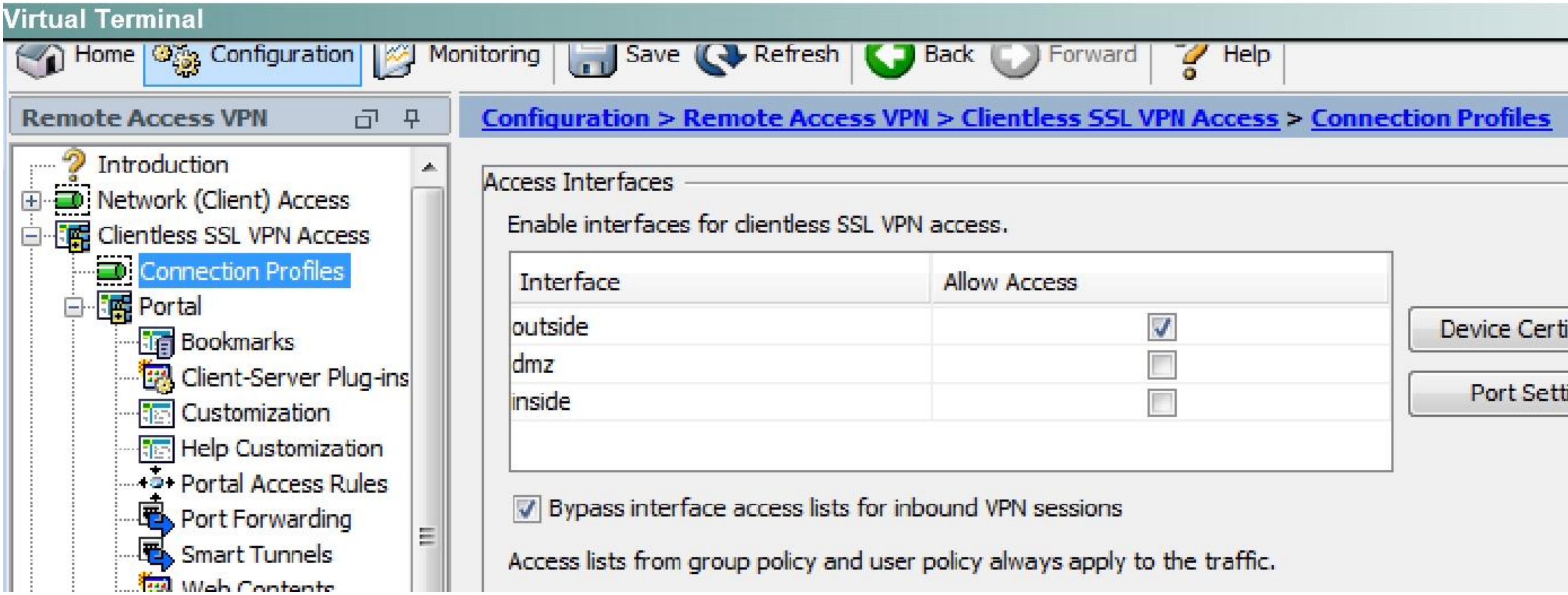


When users login to the Clientless SSL VPN using https://209.165.201.2/test, which group policy will be applied?

A. test
B. Sales
C. DefaultRAGroup
D. DefaultWEBVPNGroup
E. clientless
F. DFTGrpPolicy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:



Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Access Interfaces

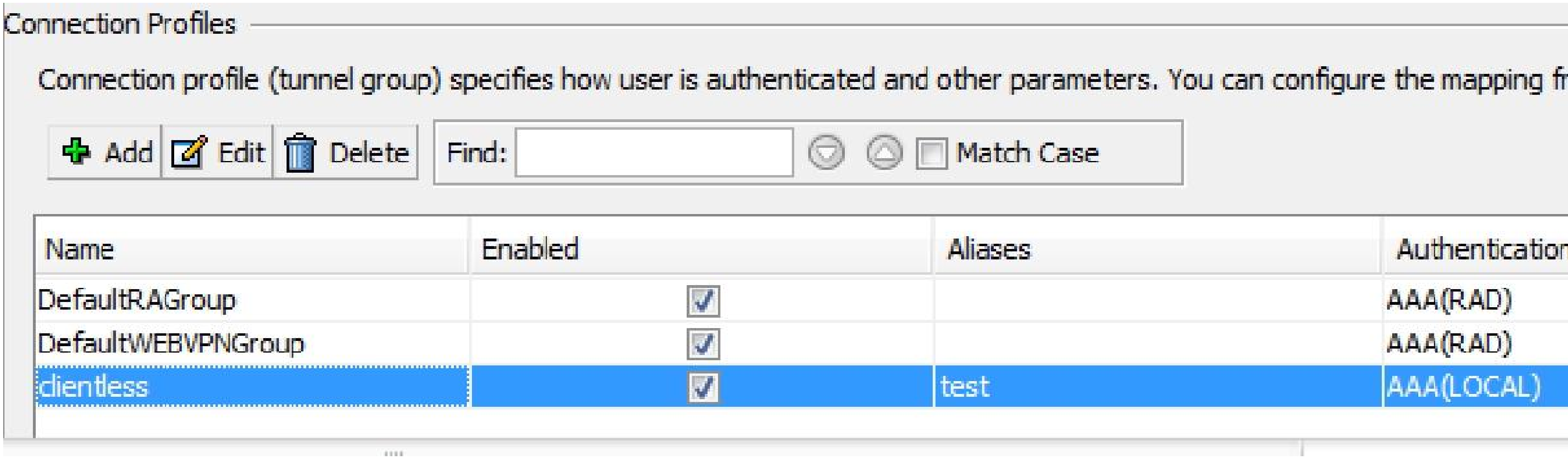
Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

☑ Bypass interface access lists for inbound VPN sessions

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

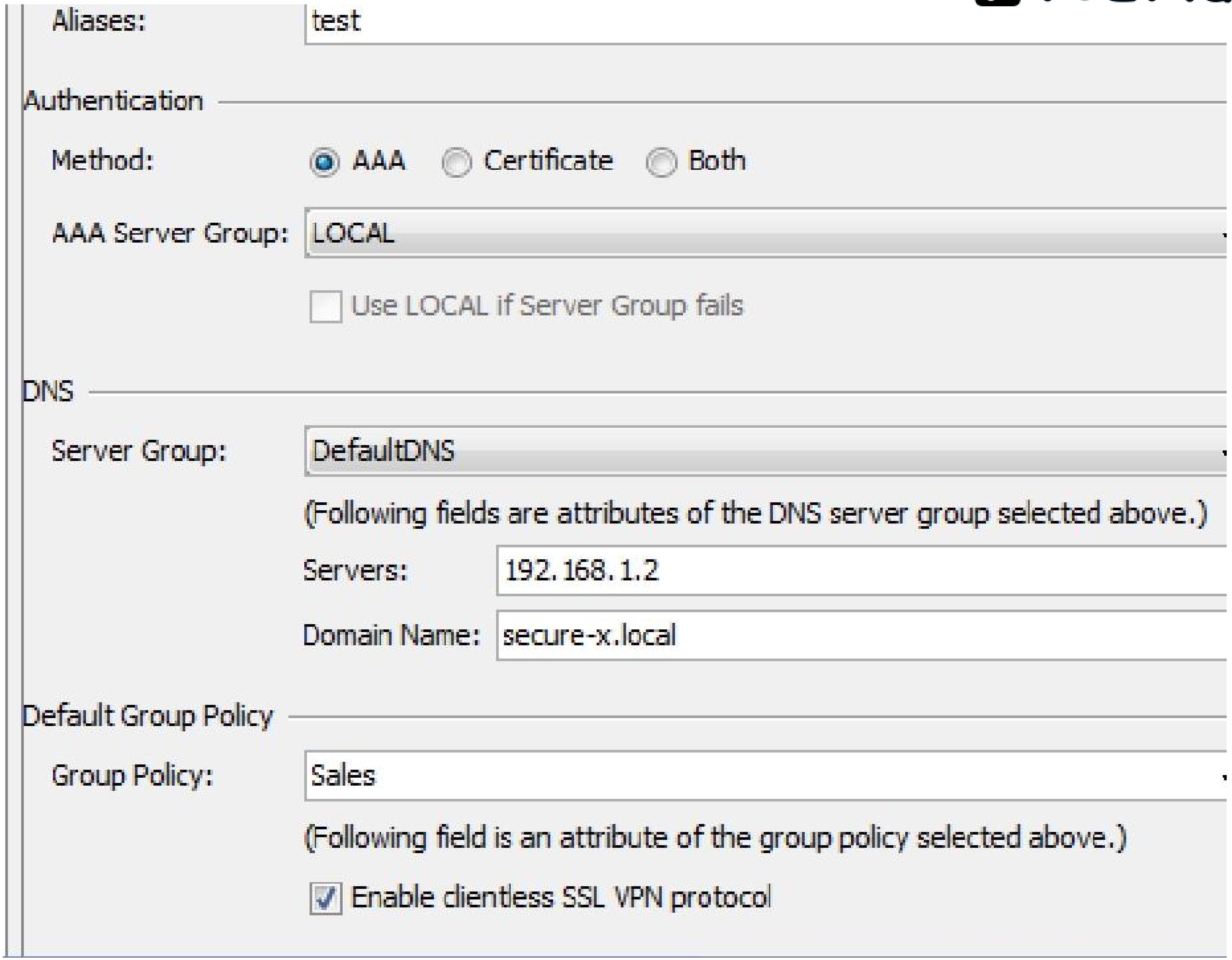
Press Edit button



Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping fr

Name	Enabled	Aliases	Authenticatior
DefaultRAGroup	☑		AAA(RAD)
DefaultWEBVPNGroup	☑		AAA(RAD)
clientless	☑	test	AAA(LOCAL)



Aliases: test

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected above.)

Servers: 192.168.1.2

Domain Name: secure-x.local

Default Group Policy

Group Policy: Sales

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

☑ Enable clientless SSL VPN protocol

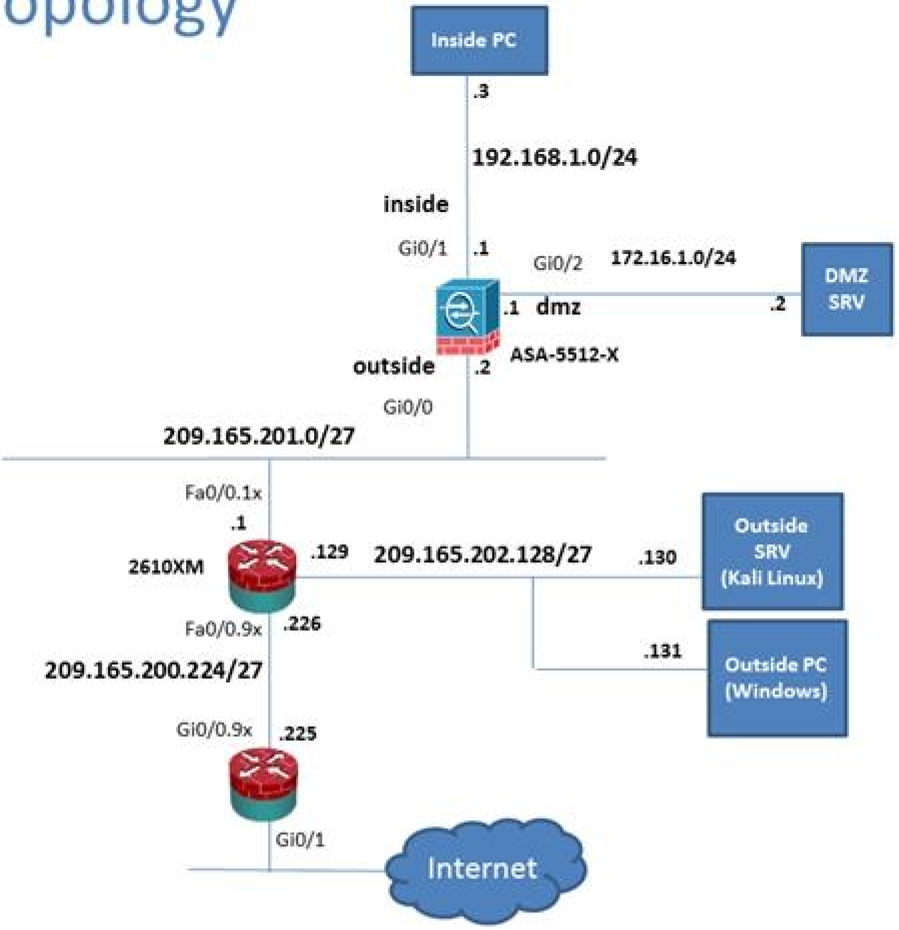
QUESTION 67

Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice q

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

Lab Topology

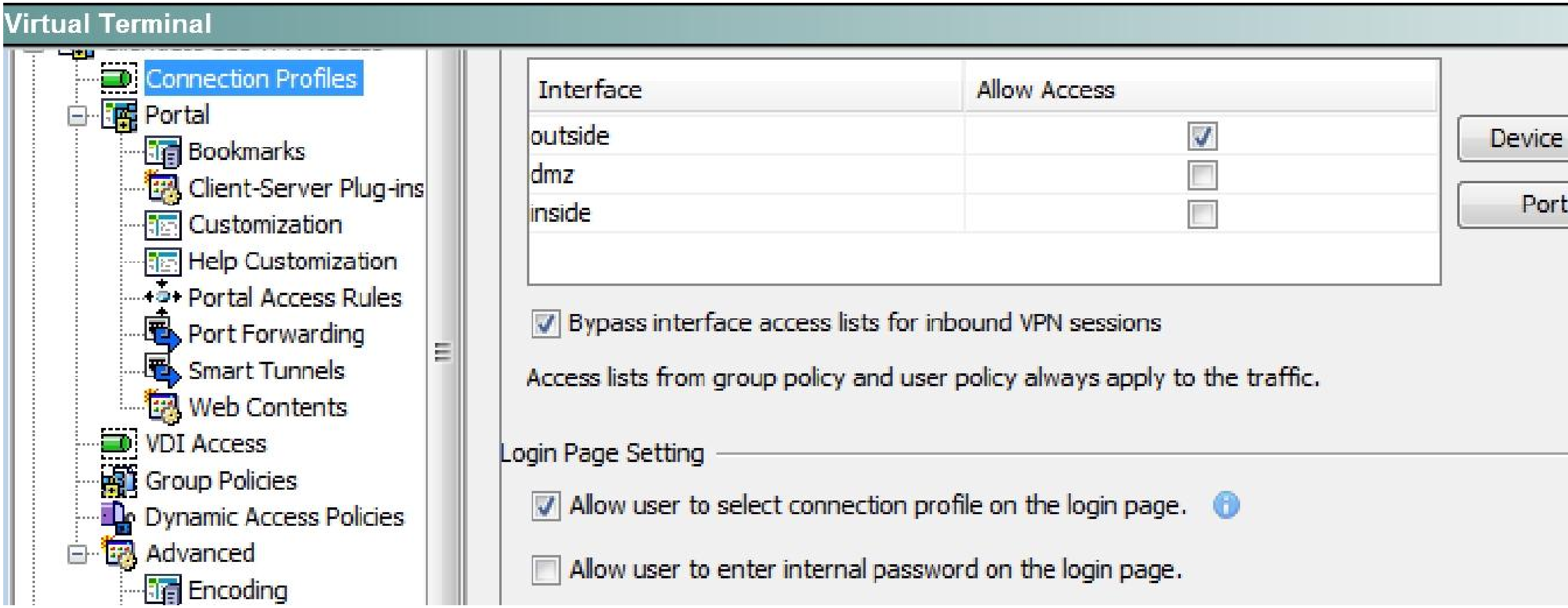


Which two statements regarding the ASA VPN configurations are correct? (Choose two)

A. The Inside-SRV bookmark has not been applied to the Sales group policy
B. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_Trustpoint1
C. The Inside-SRV bookmark references the https://192.168.1.2 URL
D. Any Connect, IPSec IKEv1 and IPSec IKEv2 VPN access is enabled on the outside interface
E. Only Clientless SSL VPN VPN access is allowed with the Sales group Policy
F. The DefaultWEBVPNGroup Connection Profile is using the AAA with Radius server method

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:



Interface	Allow Access
outside	☑
dmz	☐
inside	☐

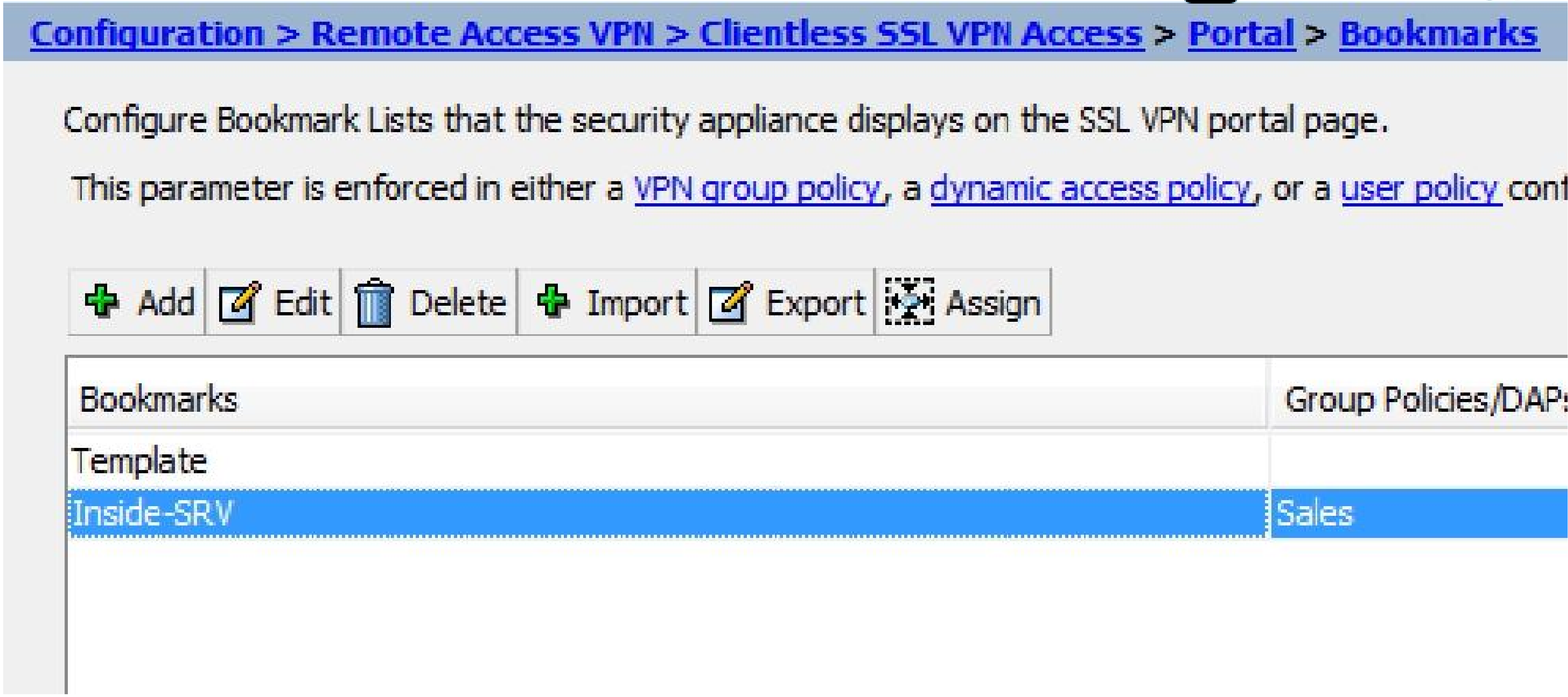
☑ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

☑ Allow user to select connection profile on the login page.

☐ Allow user to enter internal password on the login page.

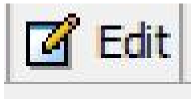


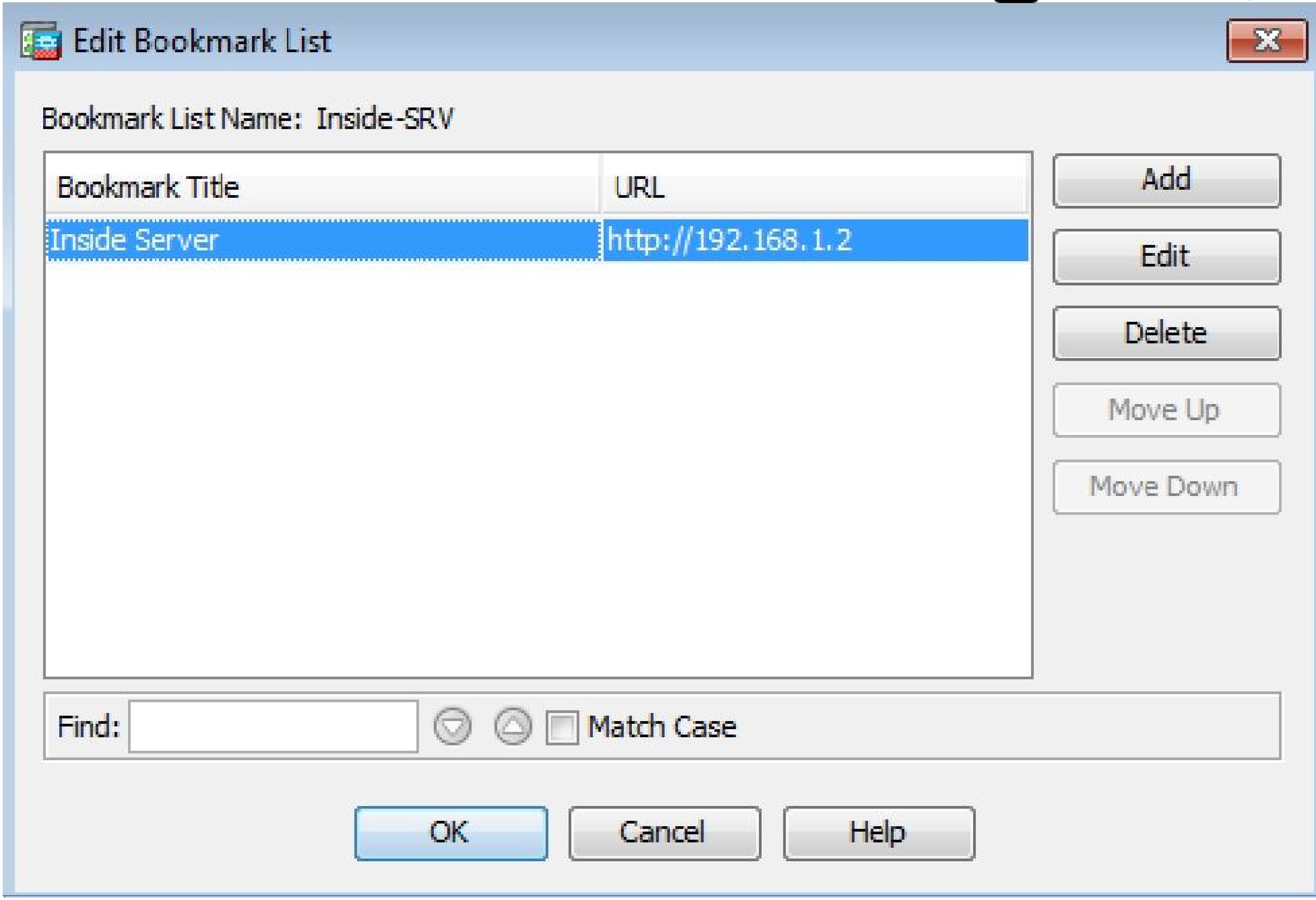
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy conf

Bookmarks	Group Policies/DAPs
Template	
Inside-SRV	Sales





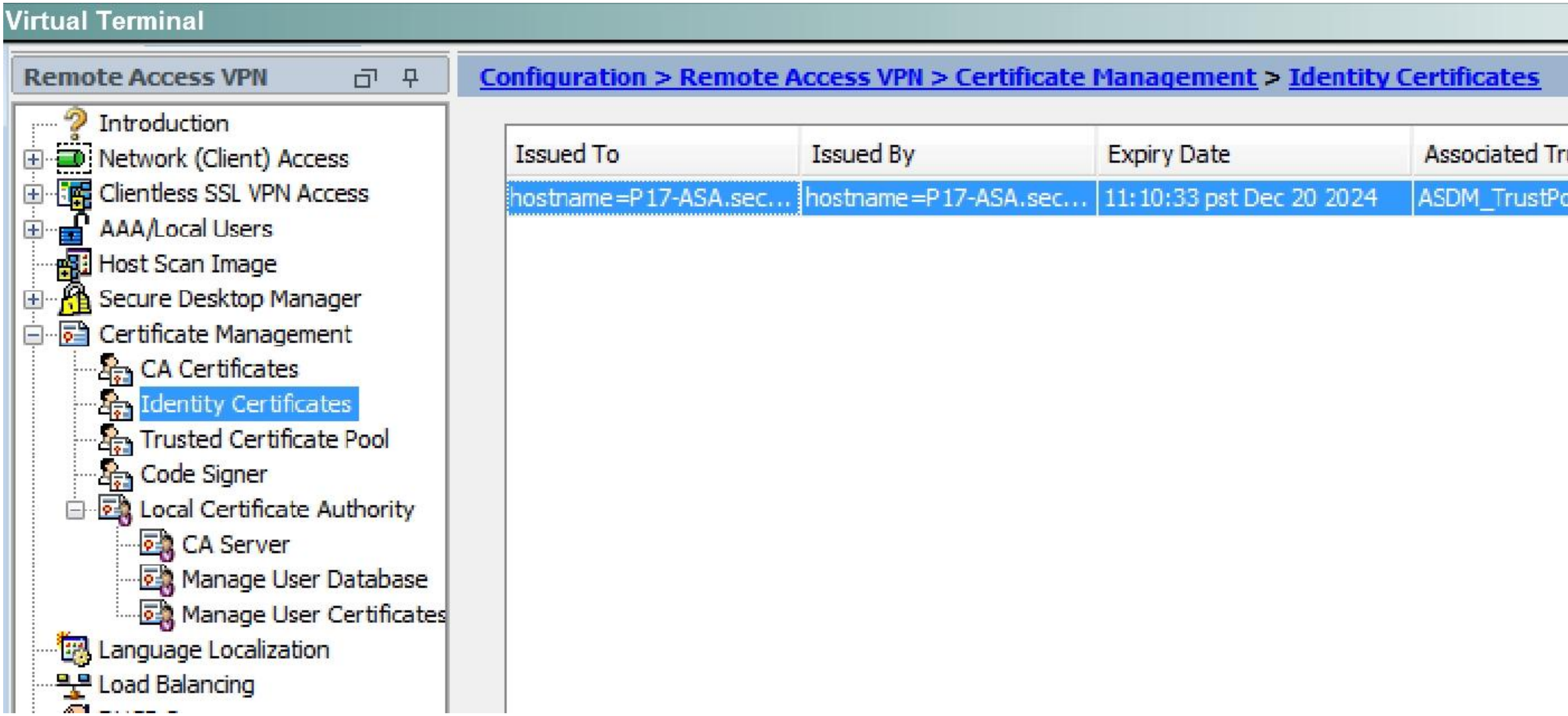
Edit Bookmark List

Bookmark List Name: Inside-SRV

Bookmark Title	URL
Inside Server	http://192.168.1.2

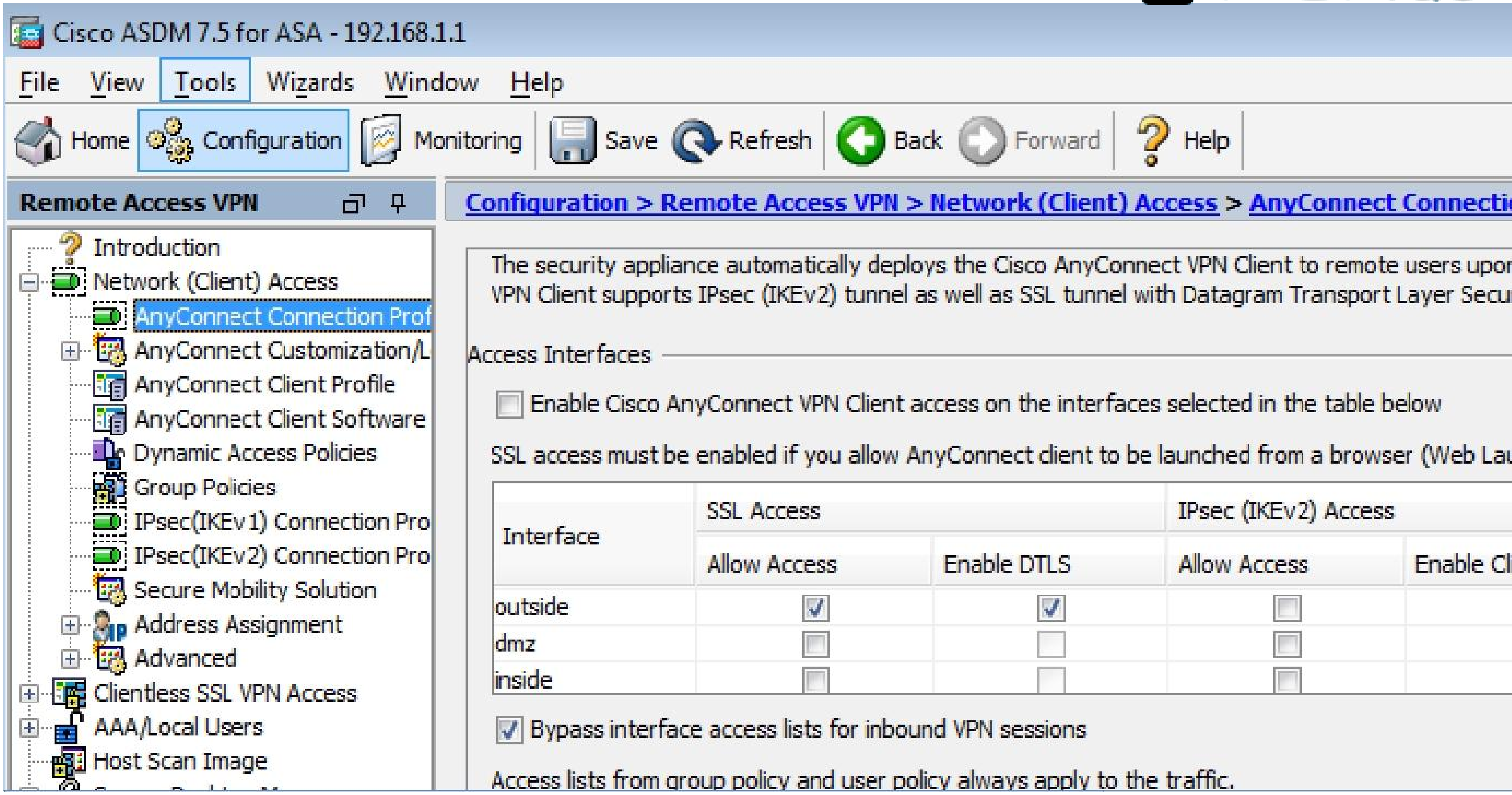
Find:

□ Match Case



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Tr
hostname=P17-ASA.sec...	hostname=P17-ASA.sec...	11:10:33 pst Dec 20 2024	ASDM_TrustPo



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connecti

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upor
VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Secu

Access Interfaces

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

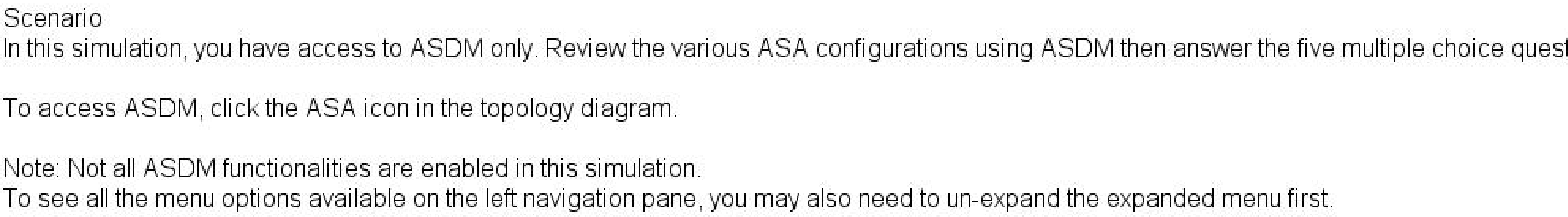
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Lau

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Cl
outside	☑	☑	□	
dmz	□	□	□	
inside	□	□	□	

☑ Bypass interface access lists for inbound VPN sessions

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

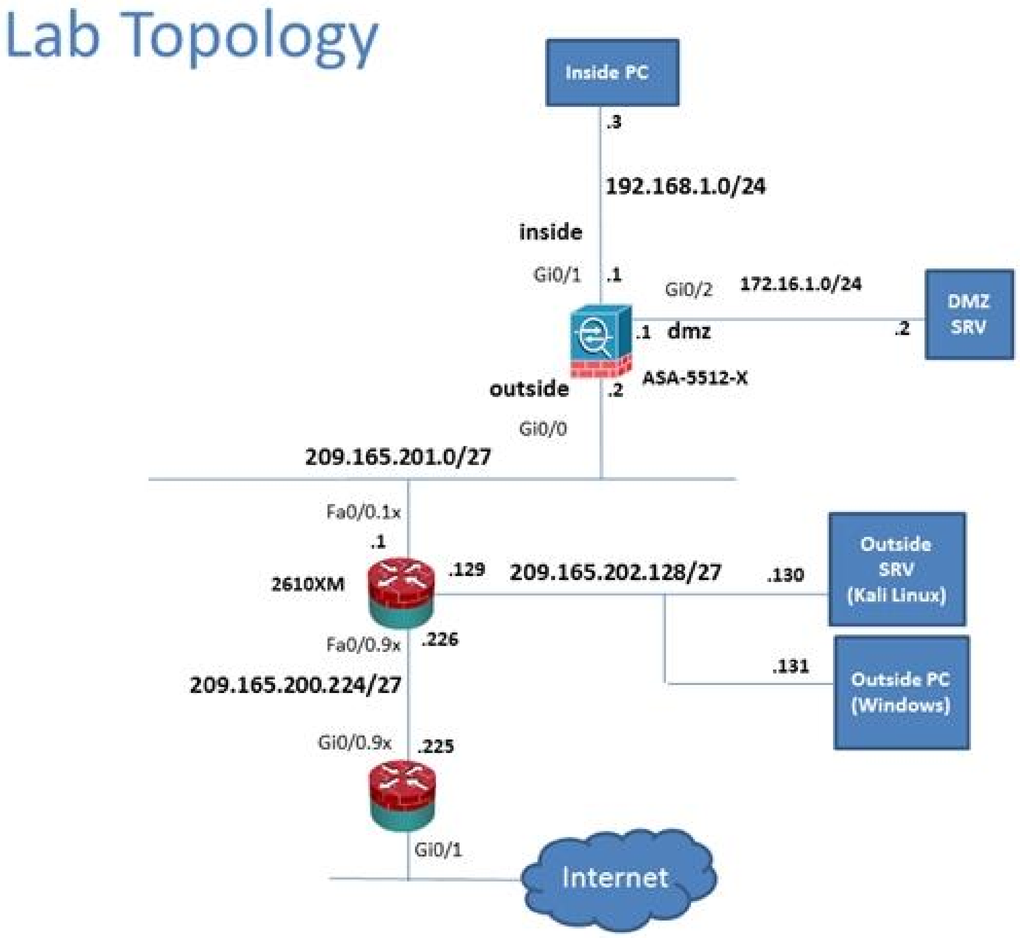
QUESTION 68



Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice quest

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

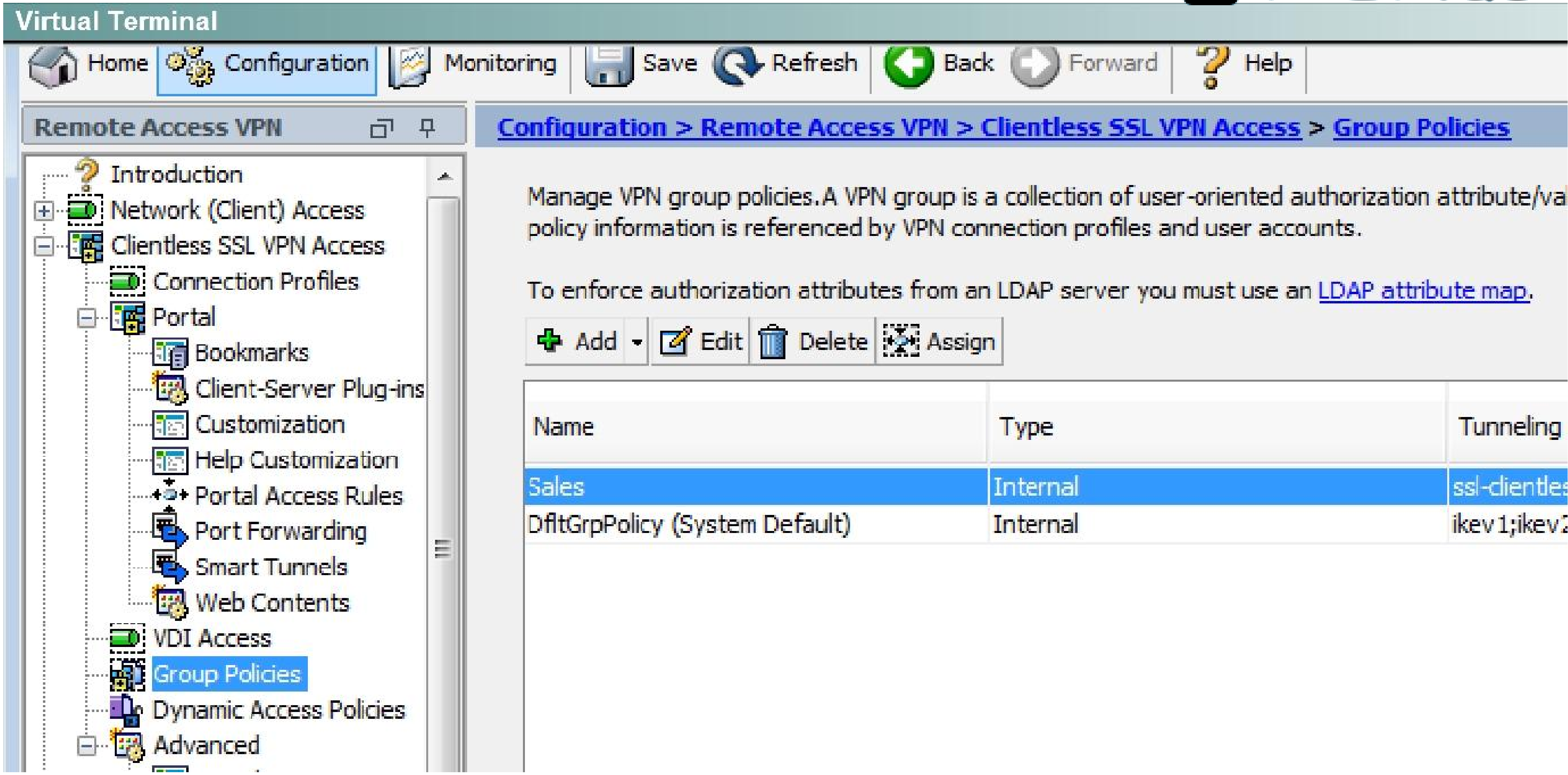


Which four tunneling protocols are enabled in the DfltGrpPolicy group policy? (choose four)

A. IPsec IKEv1
B. IPsec IKEv2
C. L2TP/IPsec
D. Clientless SSL VPN
E. SSL VPN Client
F. PPTP

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

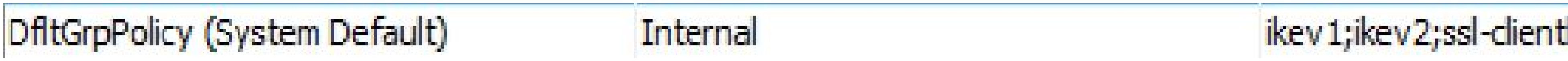


Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/va
policy information is referenced by VPN connection profiles and user accounts.

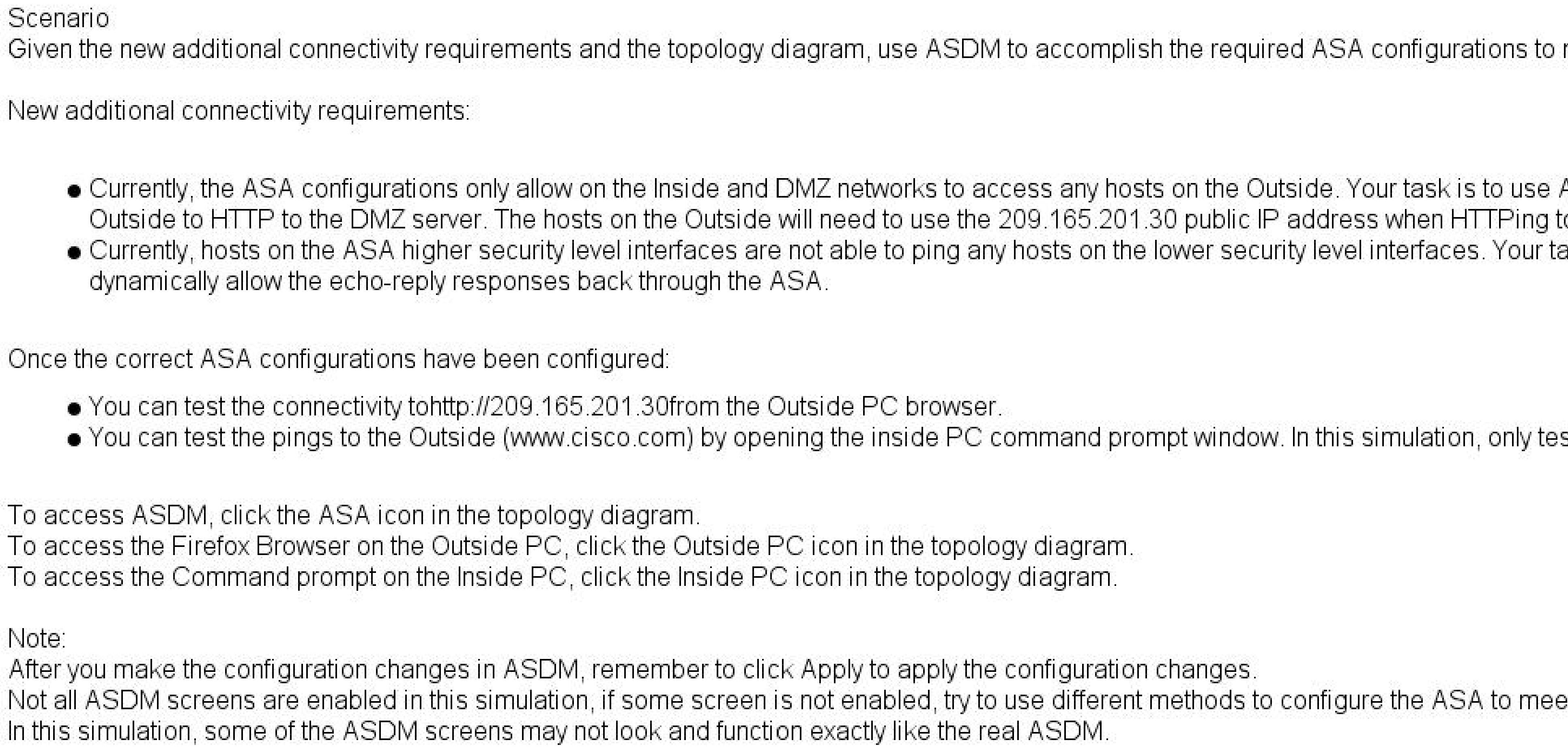
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling
Sales	Internal	ssl-clientles
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2



DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-client

QUESTION 69



Scenario
Given the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to r

New additional connectivity requirements:

- Currently, the ASA configurations only allow on the Inside and DMZ networks to access any hosts on the Outside. Your task is to use A Outside to HTTP to the DMZ server. The hosts on the Outside will need to use the 209.165.201.30 public IP address when HTTPing to
- Currently, hosts on the ASA higher security level interfaces are not able to ping any hosts on the lower security level interfaces. Your ta dynamically allow the echo-reply responses back through the ASA.

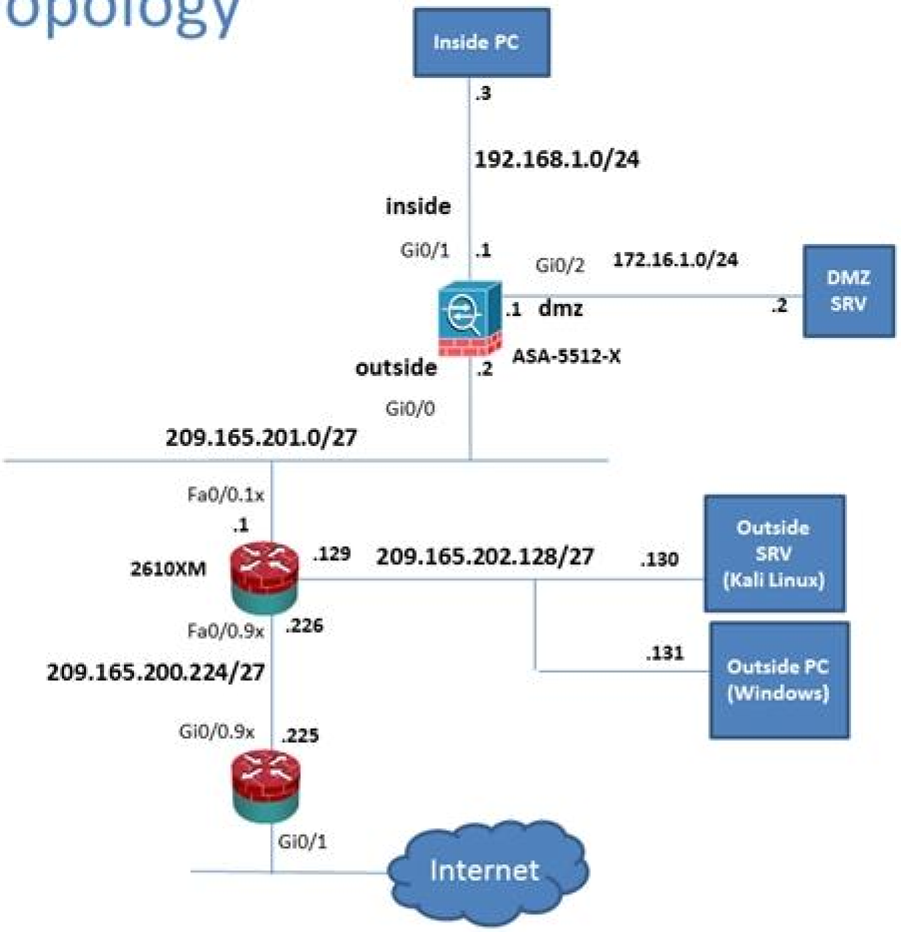
Once the correct ASA configurations have been configured:

- You can test the connectivity tohttp://209.165.201.30from the Outside PC browser.
- You can test the pings to the Outside (www.cisco.com) by opening the inside PC command prompt window. In this simulation, only tes

To access ASDM, click the ASA icon in the topology diagram.
To access the Firefox Browser on the Outside PC, click the Outside PC icon in the topology diagram.
To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram.

Note:
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.
Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to mee
In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM.

Lab Topology

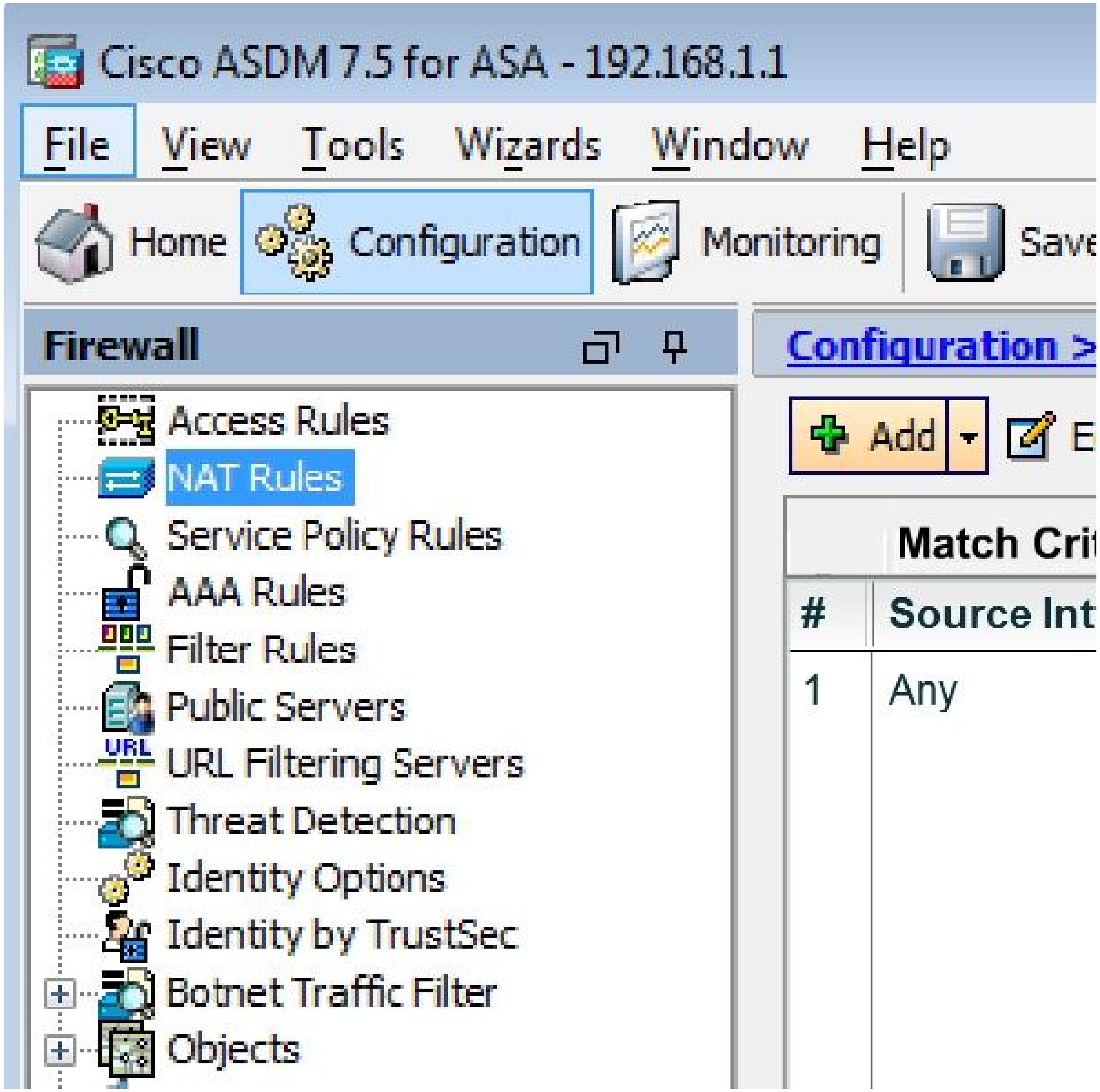


A. Firewall, Configuration, NAT Rules, Name=http, IP version=IPv4, IP address=209.165.201.30, Static NAT=172.16.1.2

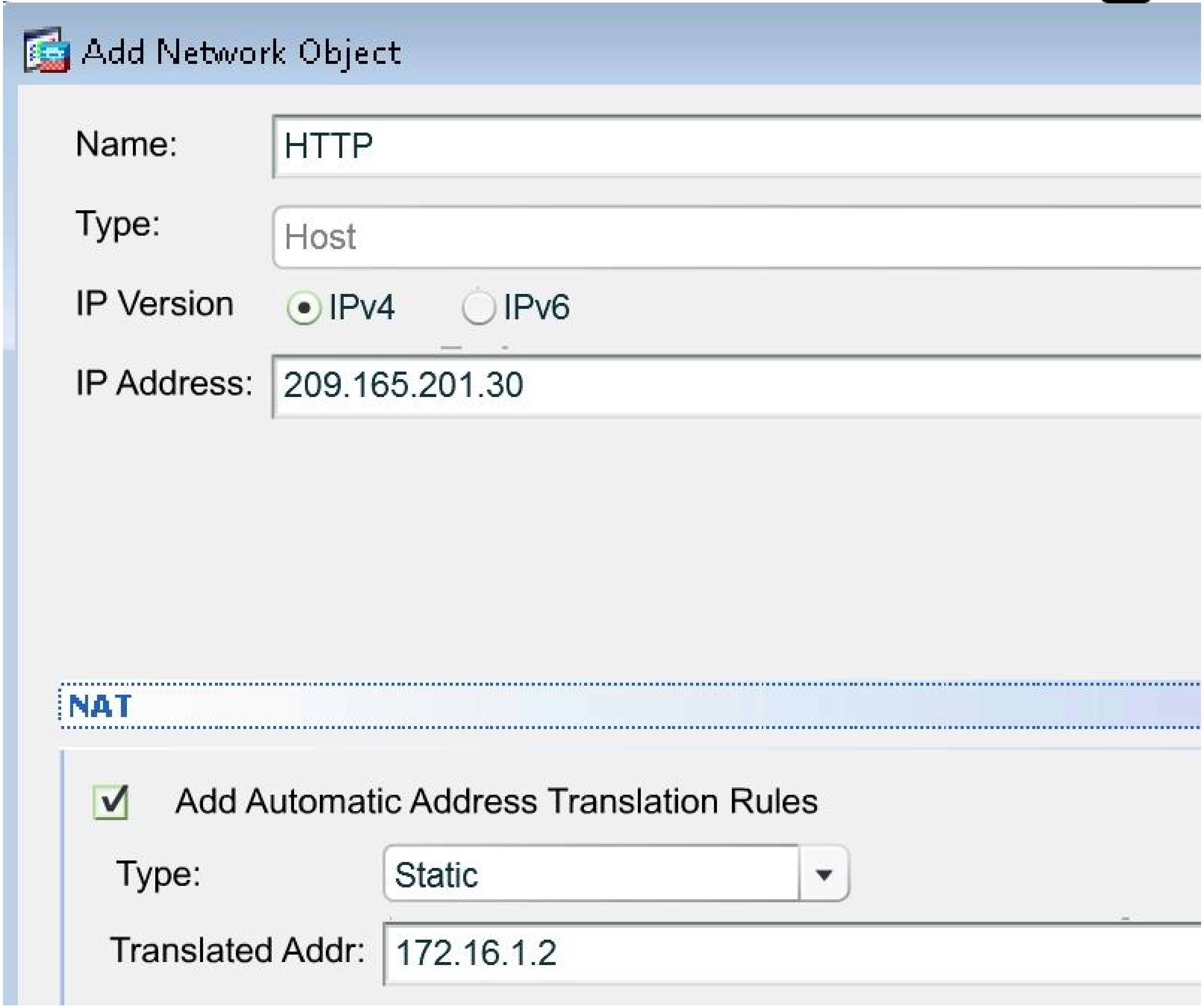
B. Firewall, Config, NAT Rules, Interface=Outside, Action=Permit, Source=any, Destination=209.165.201.30, Service= tcp/http
C. Firewall, Config, Service policy Rules, Click Global Policy and edit, Rule Action tab, Click ICMP and apply
D. Ping www.cisco.com from Inside PC

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:



	Match Crit
#	Source Int
1	Any



Add Network Object

Name: HTTP

Type: Host

IP Version ● IPv4 ○ IPv6

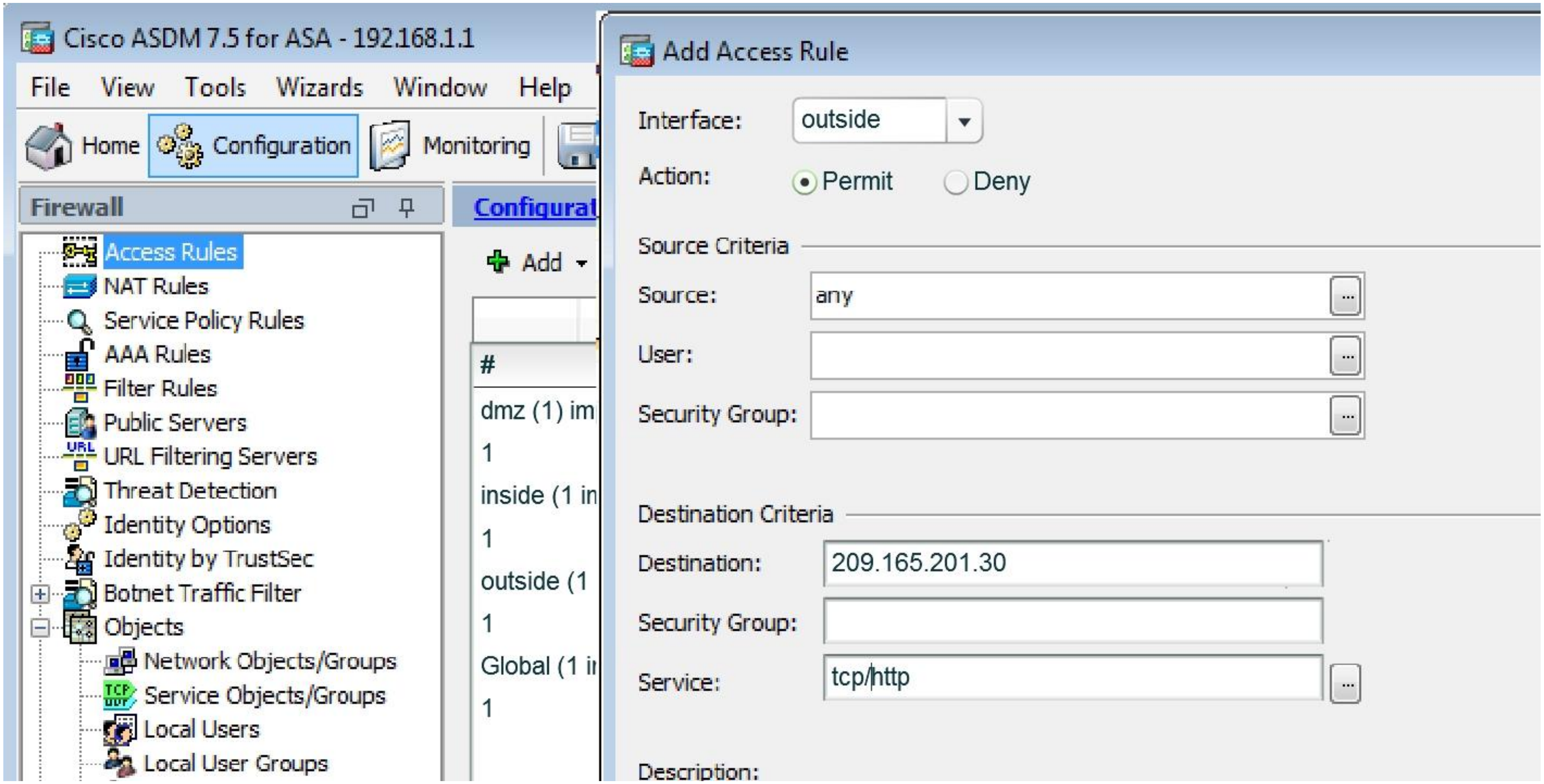
IP Address: 209.165.201.30

NAT

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr: 172.16.1.2



Add Access Rule

Interface: outside

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

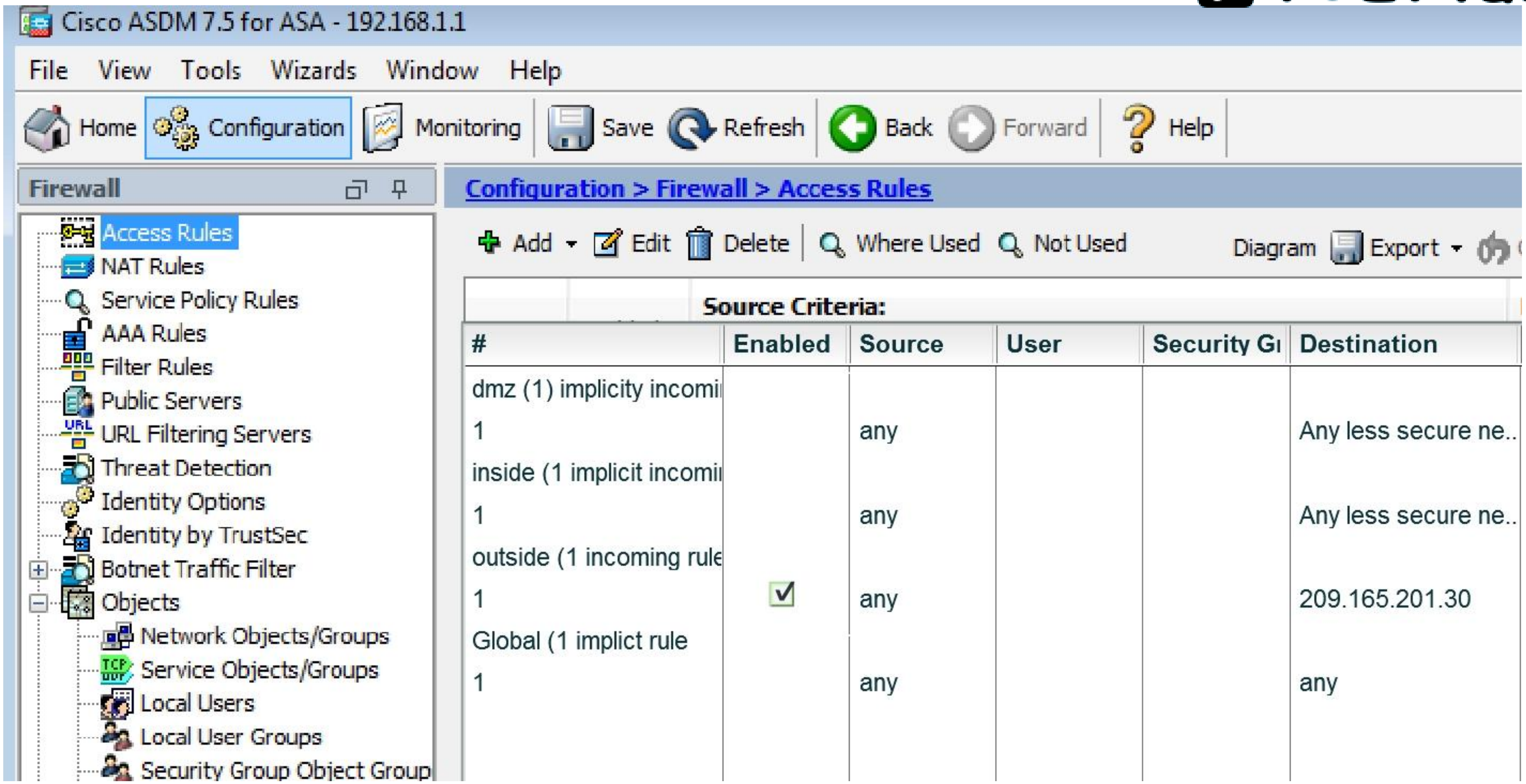
Destination: 209.165.201.30

Security Group:

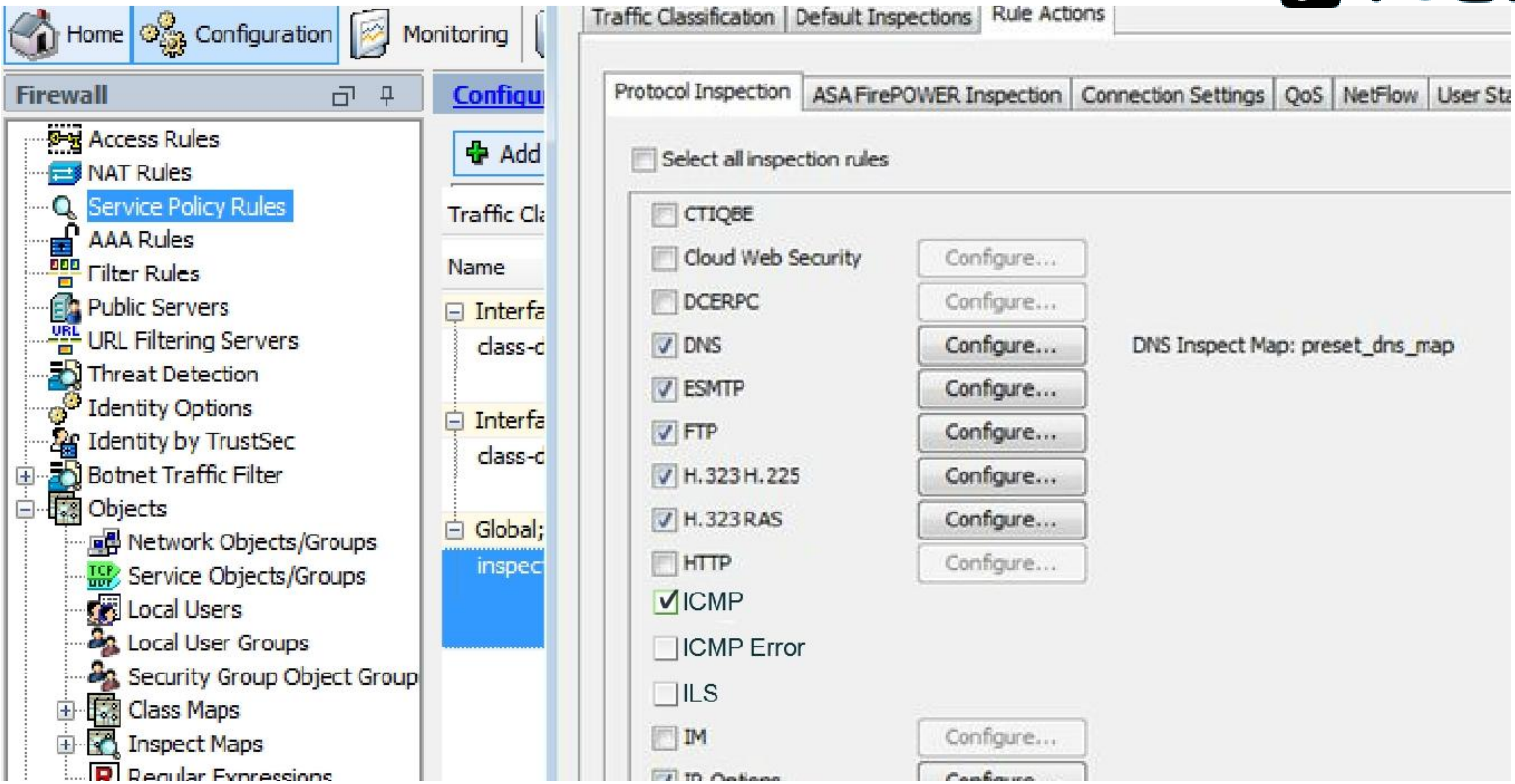
Service: tcp/http

Description:

2nd Part Permit ICMP



		Source Criteria:			
#	Enabled	Source	User	Security Gı	Destination
dmz (1) implicity incomi					
1		any			Any less secure ne..
inside (1 implicit incomi					
1		any			Any less secure ne..
outside (1 incoming rule					
1	☑	any			209.165.201.30
Global (1 implict rule					
1		any			any



☐ Select all inspection rules

☐ CTIQBE

☐ Cloud Web Security Configure...

☐ DCERPC Configure...

☑ DNS Configure... DNS Inspect Map: preset_dns_map

☑ ESMTP Configure...

☑ FTP Configure...

☑ H.323 H.225 Configure...

☑ H.323 RAS Configure...

☐ HTTP Configure...

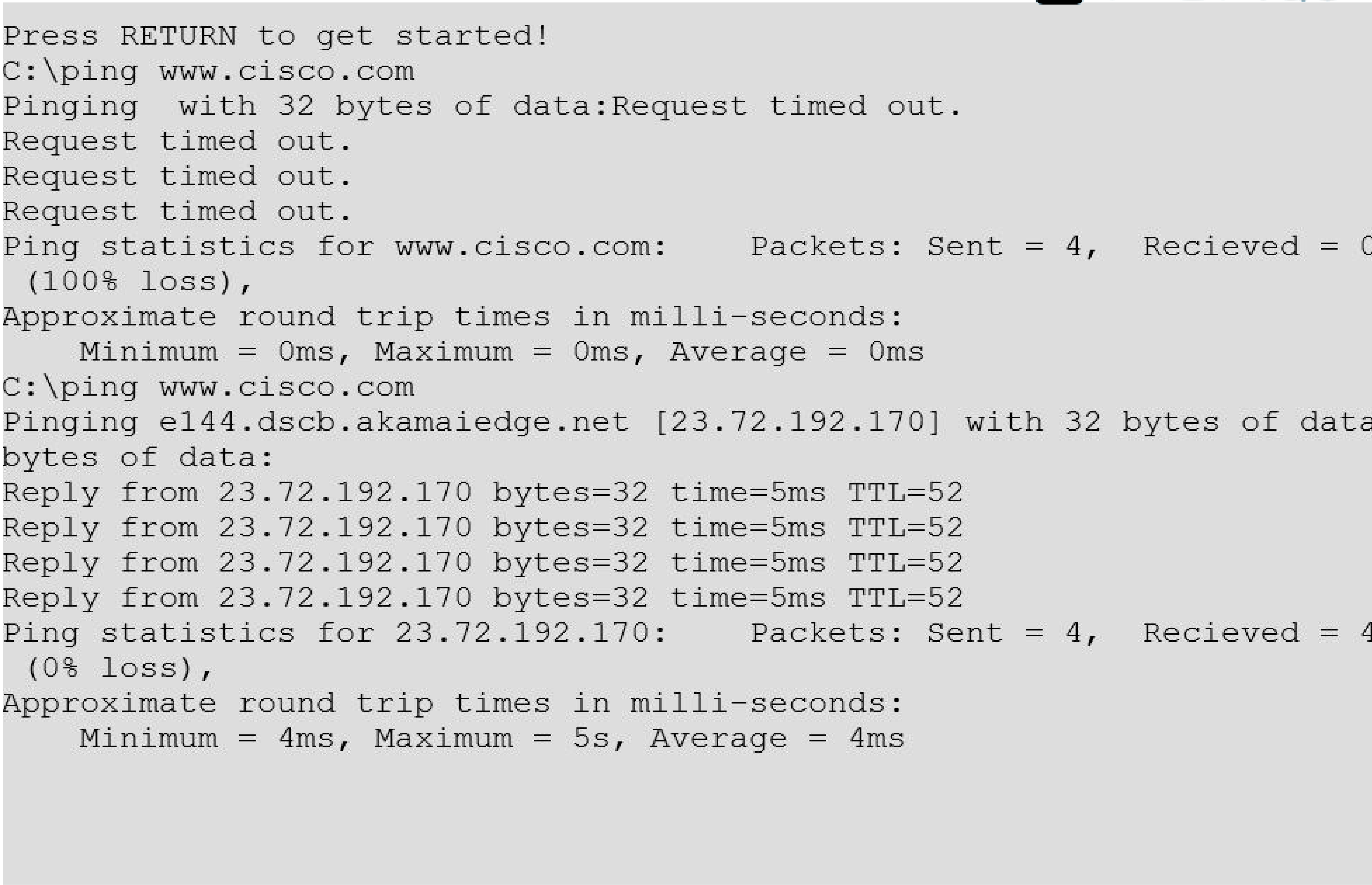
☑ ICMP

☐ ICMP Error

☐ ILS

☐ IM Configure...

☑ IP Options Configure...



```
Press RETURN to get started!
C:\ping www.cisco.com
Pinging  with 32 bytes of data:Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for www.cisco.com:    Packets: Sent = 4,  Recieved =
 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\ping www.cisco.com
Pinging e144.dscb.akamaiedge.net [23.72.192.170] with 32 bytes of data
bytes of data:
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Ping statistics for 23.72.192.170:    Packets: Sent = 4,  Recieved =
 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5s, Average = 4ms
```