CCNA Security

Number: Cisco 210-260
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Implementing Cisco Network Security
Version: 5.0

Exam A

QUESTION 1
Which two services define cloud networks? (Choose two.)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
CD

QUESTION 2
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 administrator access from multiple locations
D. when you require ROMMON access
E. when the control plane fails to respond

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
AD

QUESTION 3
In which three ways does the TACACS protocol differ from RADIUS? (Choose three.)

A. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
B. TACACS can encrypt the entire packet that is sent to the NAS.
C. TACACS uses UDP to communicate with the NAS.

D. TACACS supports per-command authorization.
E. TACACS uses TCP to communicate with the NAS.
F. TACACS encrypts only the password field in an authentication packet.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
BDE

QUESTION 4
According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

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

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:
CEF

QUESTION 5
Which two next-generation encryption 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:
AF

QUESTION 6
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:
DEF

QUESTION 7
What are two default Cisco IOS privilege levels? (Choose two.)

A. 0
B. 1
C. 5
D. 7
E. 10
F. 15

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

BF

QUESTION 8
Which two authentication types does OSPF support? (Choose two.)

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
AE

QUESTION 9
Which two features do CoPP and CPPr use to protect the control plane? (Choose two.)

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

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
CF

QUESTION 10
Which two statements about stateless firewalls are true? (Choose two.)

A. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

B. They cannot track connections.
C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
D. They compare the 5-tuple of each incoming packet against configurable rules.
E. Cisco IOS cannot implement them because the platform is stateful by nature.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
BD

QUESTION 11
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. 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:
ABC

QUESTION 12
What three actions are limitations when running IPS in promiscuous mode? (Choose three.)

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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
CDE

QUESTION 13
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Deny the connection inline.
B. Perform a Layer 6 reset.
C. Deploy an antimalware system.
D. Enable bypass mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 14
What is an advantage of implementing a Trusted Platform Module for disk encryption?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 15
What is the purpose of the Integrity component of the CIA triad?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 16
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:
A

QUESTION 17
Which type of secure connectivity does an extranet provide?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

B

QUESTION 18
Which tool can an attacker use to attempt a DDoS attack?

A. Trojan horse
B. adware
C. botnet
D. virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 19
What type of security support is provided by the Open Web Application Security Project?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 20
What type of attack was the Stuxnet virus?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

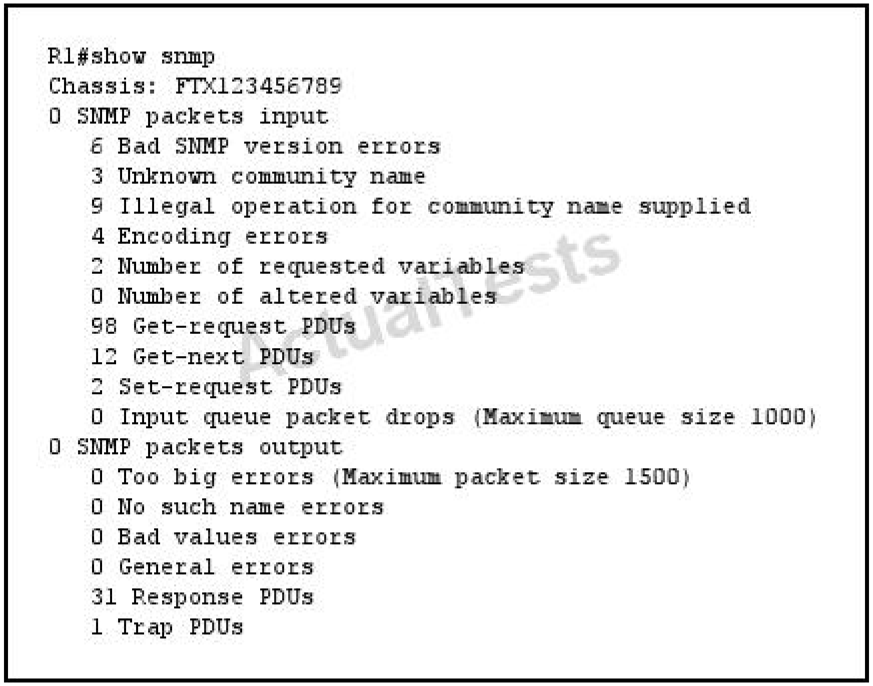
QUESTION 21
What type of algorithm uses the same key to encrypt and decrypt data?

A. an IP security algorithm
B. a Public Key Infrastructure algorithm
C. an asymmetric algorithm
D. a symmetric algorithm

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 22
Refer to the exhibit.



```
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
```

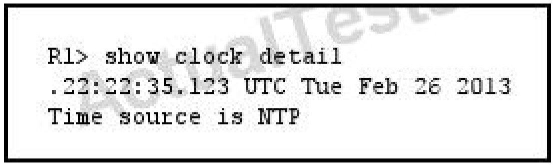
How many times was a read-only string used to attempt a write operation?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
E

QUESTION 23
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 clock is out of sync.
C. The time is authoritative, but the NTP process has lost contact with its servers.
D. NTP is configured incorrectly.
E. The time is not authoritative.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 24
How does the Cisco ASA use Active Directory to authorize VPN users?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

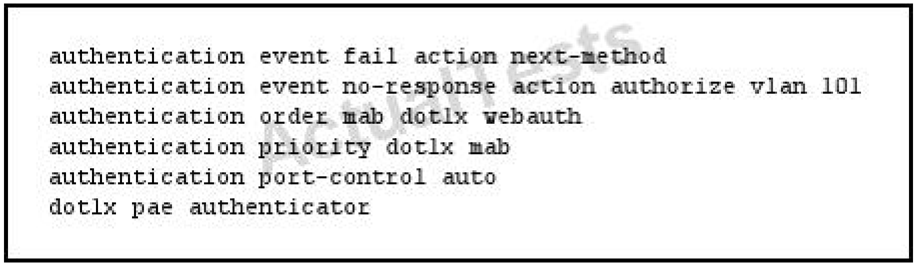
QUESTION 25
Which statement about Cisco ACS authentication and authorization is true?

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 allow or deny requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 26
Refer to the exhibit.



```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dotlx webauth
authentication priority dotlx mab
authentication port-control auto
dotlx 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 authentication attempt will time out and the switch will place the port into the unauthorized state.
C. The supplicant will fail to advance beyond the webauth method.
D. The authentication attempt will time out and the switch will place the port into VLAN 101.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 27
Which EAP method uses Protected Access Credentials?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 28
What is one requirement for locking a wired or wireless device from ISE?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 29
What VPN feature allows traffic to exit the security appliance through the same interface it entered?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

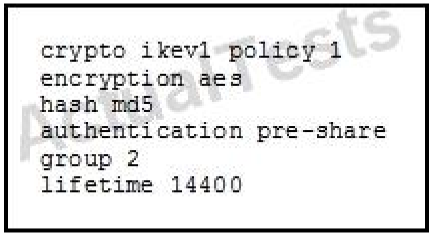
QUESTION 30
What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 31
Refer to the exhibit.



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

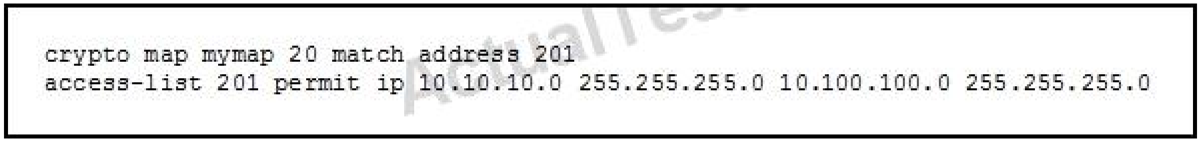
What is the effect of the given command sequence?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 32
Refer to the exhibit.



```
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
```

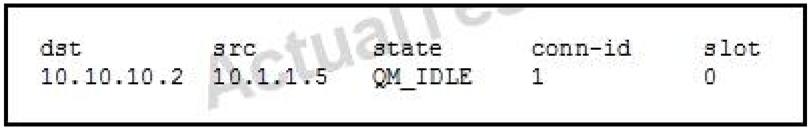
What is the effect of the given command sequence?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 33
Refer to the exhibit.



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

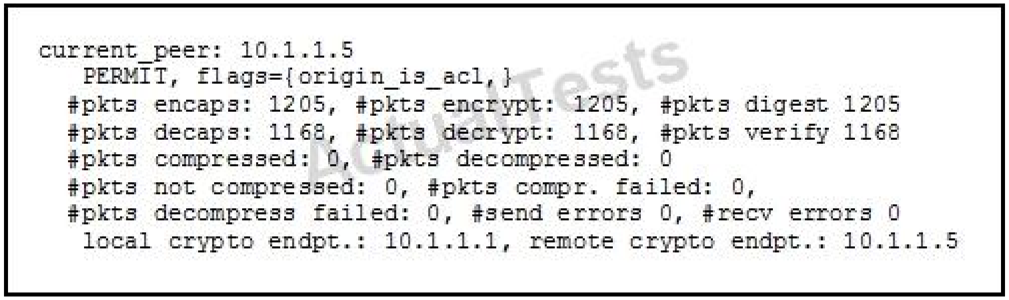
While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 34
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
```

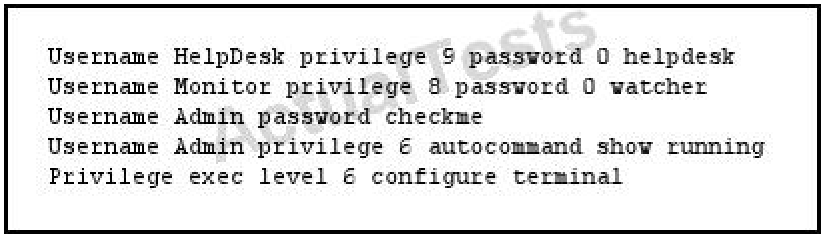
While troubleshooting site-to-site VPN, you issued the show crypto ipsec sa command. What does the given output show?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 35
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. Change the Privilege exec level value to 15.
B. Remove the autocommand keyword and arguments from the Username Admin privilege line.
C. Remove the Privilege exec line.
D. Remove the two Username Admin lines.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 36
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:
A

QUESTION 37
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:
B

QUESTION 38
What type of packet creates and performs network operations on a network device?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 39
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:
B

QUESTION 40
In what type of attack does an attacker virtually change a device's 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:
D

QUESTION 41
What command can you use to verify the binding table status?

A. show ip dhcp source binding
B. show ip dhcp pool

C. show ip dhcp snooping
D. show ip dhcp snooping binding
E. show ip dhcp snooping statistics
F. show ip dhcp snooping database

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
F

QUESTION 42
If a switch receives a superior BPDU and goes directly into a blocked state, what mechanism must be in use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 43
Which statement about a PVLAN isolated port configured on a switch is true?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 44
If you change the native VLAN on the trunk port to an unused VLAN, what happens if an attacker attempts a double-tagging attack?

A. The trunk port would go into an error-disabled 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:
C

QUESTION 45
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:
A

QUESTION 46
Which statement about personal firewalls is true?

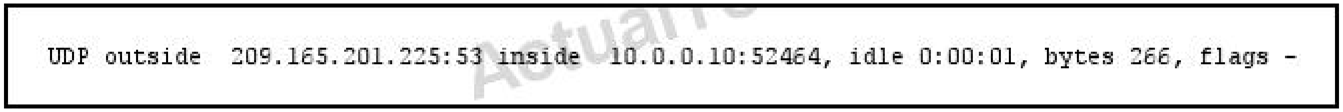
A. They are resilient against kernel attacks.
B. They can protect a system by denying probing requests.

C. They can protect email messages and private documents in a similar way to a VPN.
D. They can protect the network against attacks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 47
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 personal firewall
B. a proxy firewall
C. an application firewall
D. a stateless firewall
E. a stateful firewall

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
E

QUESTION 48
What is the only permitted operation for processing multicast traffic on zone-based firewalls?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 49
How does a zone-based firewall implementation handle traffic between interfaces in the same zone?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 50
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:
Answer: A,E

QUESTION 51
Which statement about communication over failover interfaces is true?

A. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default.
B. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default.
C. All information that is sent over the failover and stateful failover interfaces is encrypted by default.
D. User names, passwords, 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: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 52
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 all matching class maps it finds for the feature type.
B. The ASA will apply the actions from only the last matching class map it finds for the feature type.
C. The ASA will apply the actions from only the most specific 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:
D

QUESTION 53
For what reason would you configure multiple security contexts on the ASA firewall?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 54
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:
B

QUESTION 55
What is the FirePOWER impact flag used for?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 56
Which FirePOWER preprocessor engine is used to prevent SYN attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 57
Which Sourcefire logging action should you choose to record the most detail about a connection?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 58
What can the SMTP preprocessor in FirePOWER normalize?

A. It can look up the email sender.
B. It compares known threats to the email sender.
C. It can forward the SMTP traffic to an email filter server.
D. It uses the Traffic Anomaly Detector.

E. It can extract and decode email attachments in client to server traffic.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
E

QUESTION 59
You want to allow all of your company’s 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 address 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 60
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 whitelist and add the appropriate IP address to allow the traffic.
B. Create a custom blacklist to allow the traffic.
C. Create a user based access control rule to allow 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: A
Section: (none)

Explanation

Explanation/Reference:
A

QUESTION 61
A specific URL has been identified as containing malware. What action can you take to block users from accidentally 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 router's local URL list.
B. Enable URL filtering on the perimeter router and add the URLs you want to block to the router's local URL list.
C. Enable URL filtering on the perimeter router and add the URLs you want to allow to the firewall's local URL list.
D. Create a blacklist that contains the URL you want to block and activate the blacklist on the perimeter router.
E. Create a whitelist that contains the URLs you want to allow and activate the whitelist on the perimeter router.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 62
When is the best time to perform an anti-virus signature update?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 63
Which statement about application blocking is true?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 64
Which two statements regarding the ASA VPN configurations are correct? (Choose two)

A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_TrustPoint1.
B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server method.
C. The Inside-SRV bookmark references thehttps://192.168.1.2URL
D. Only Clientless SSL VPN access is allowed with the Sales group policy
E. AnyConnect, IPSec IKEv1, and IPSec IKEv2 VPN access is enabled on the outside interface
F. The Inside-SRV bookmark has not been applied to the Sales group policy

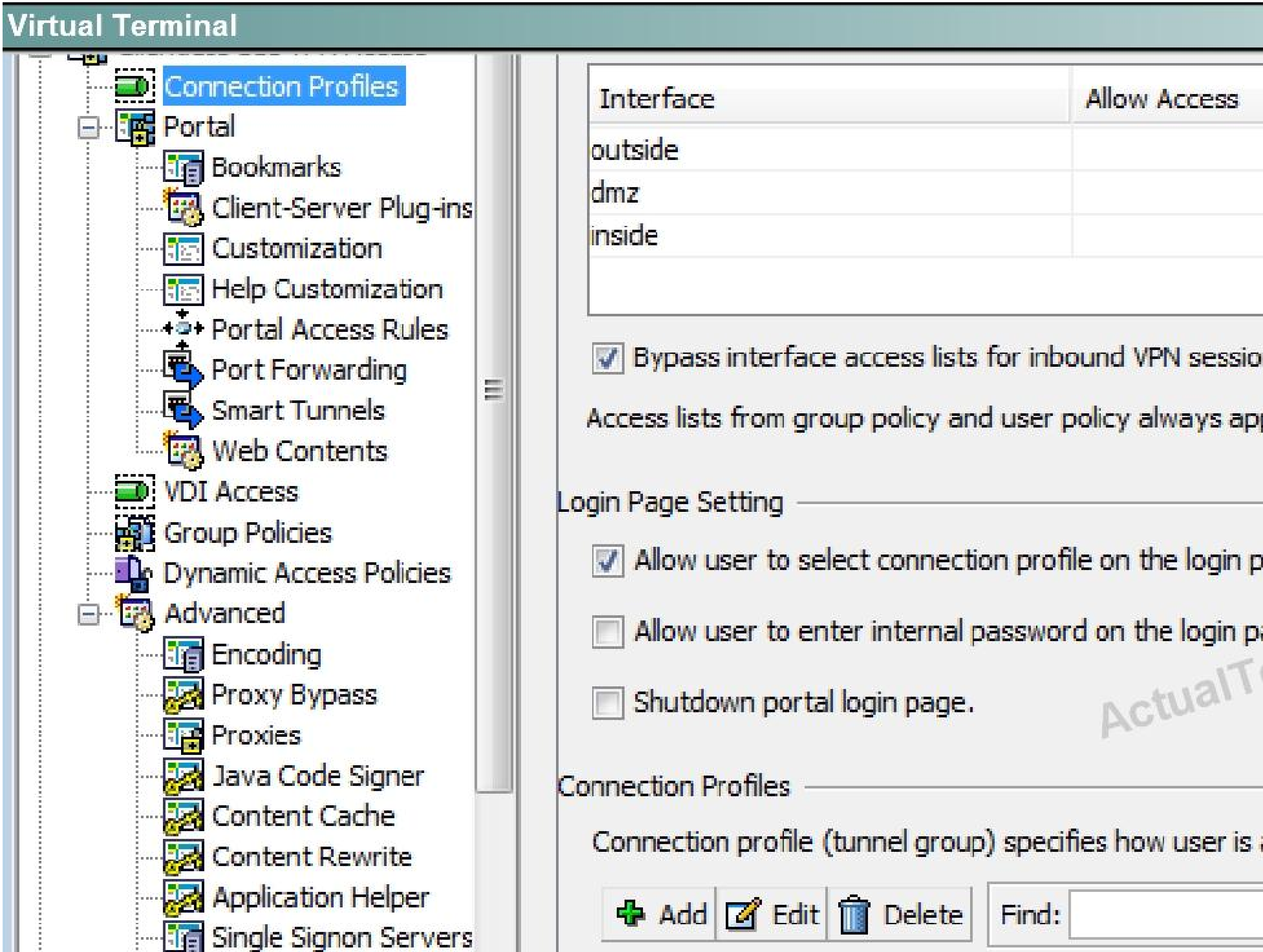
Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

Answer: B,C

Explanation:

For B:



Interface	Allow Access
outside	
dmz	
inside	

☑ Bypass interface access lists for inbound VPN sessio

Access lists from group policy and user policy always ap

Login Page Setting

☑ Allow user to select connection profile on the login p

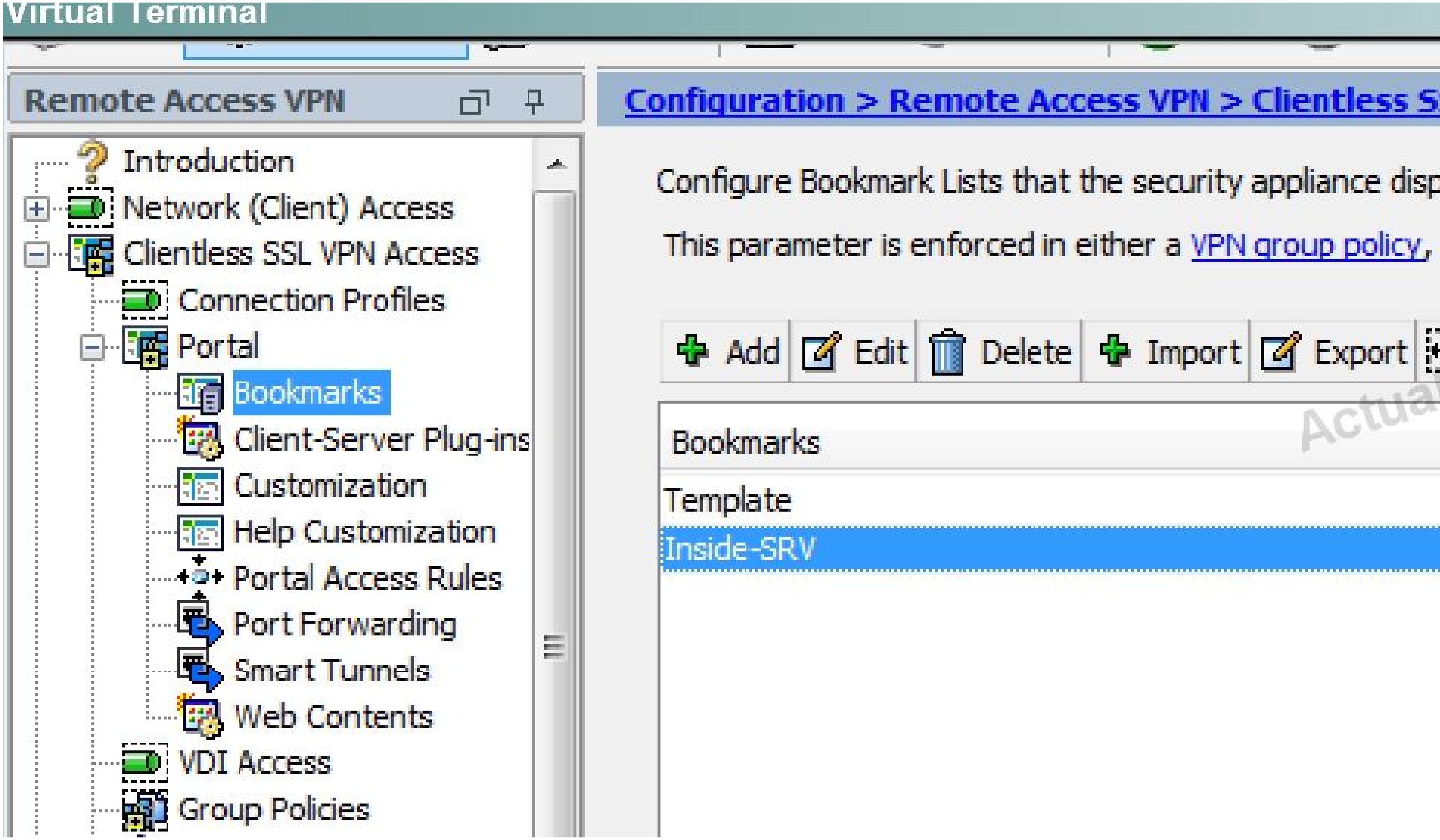
☐ Allow user to enter internal password on the login p

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is

For C, Navigate to the Bookmarks tab:



Virtual Terminal

Remote Access VPN

Configuration > Remote Access VPN > Clientless S

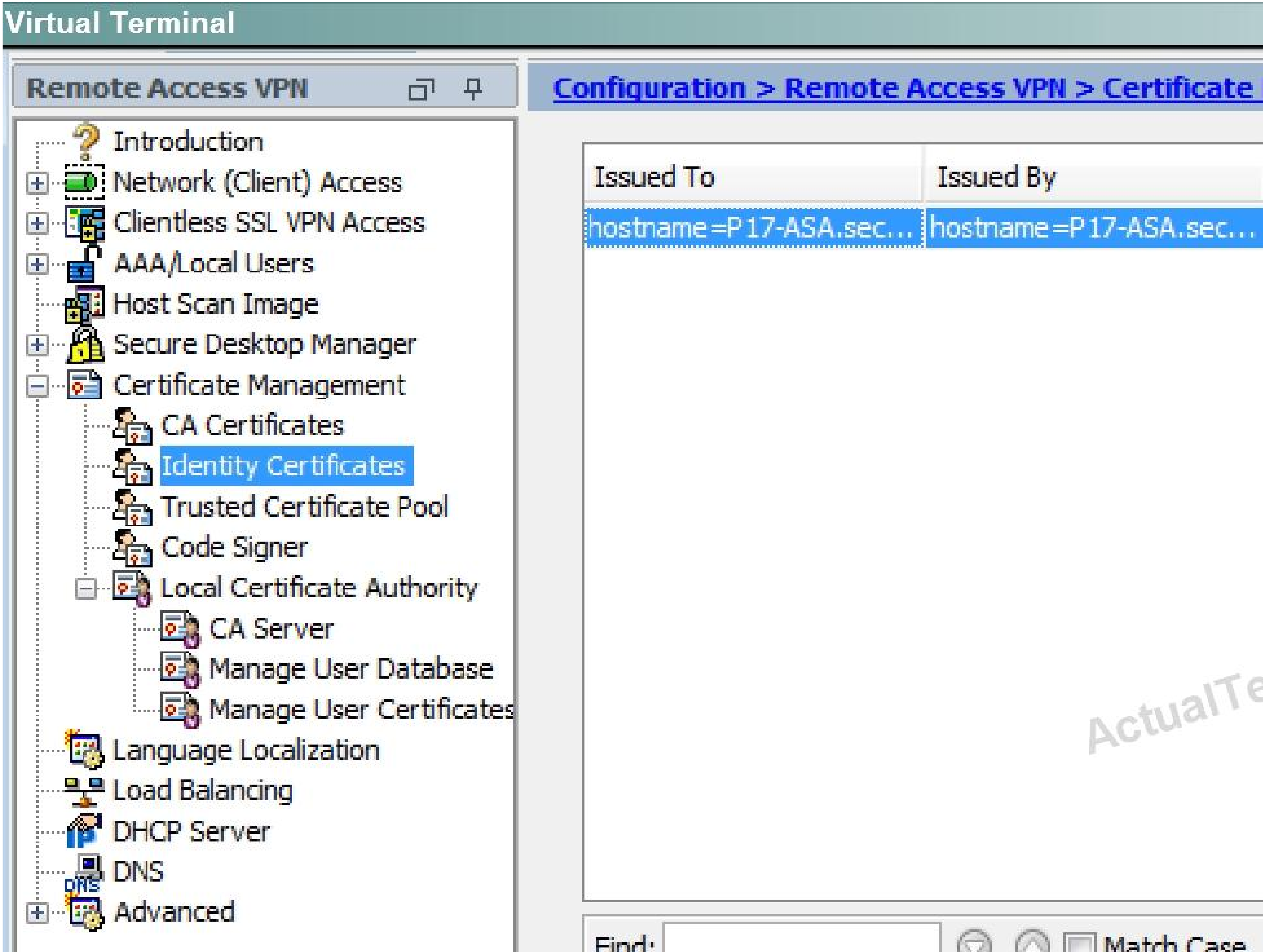
Configure Bookmark Lists that the security appliance disp

This parameter is enforced in either a VPN group policy,

Bookmarks
Template
Inside-SRV

Then hit “edit” and you will see this:

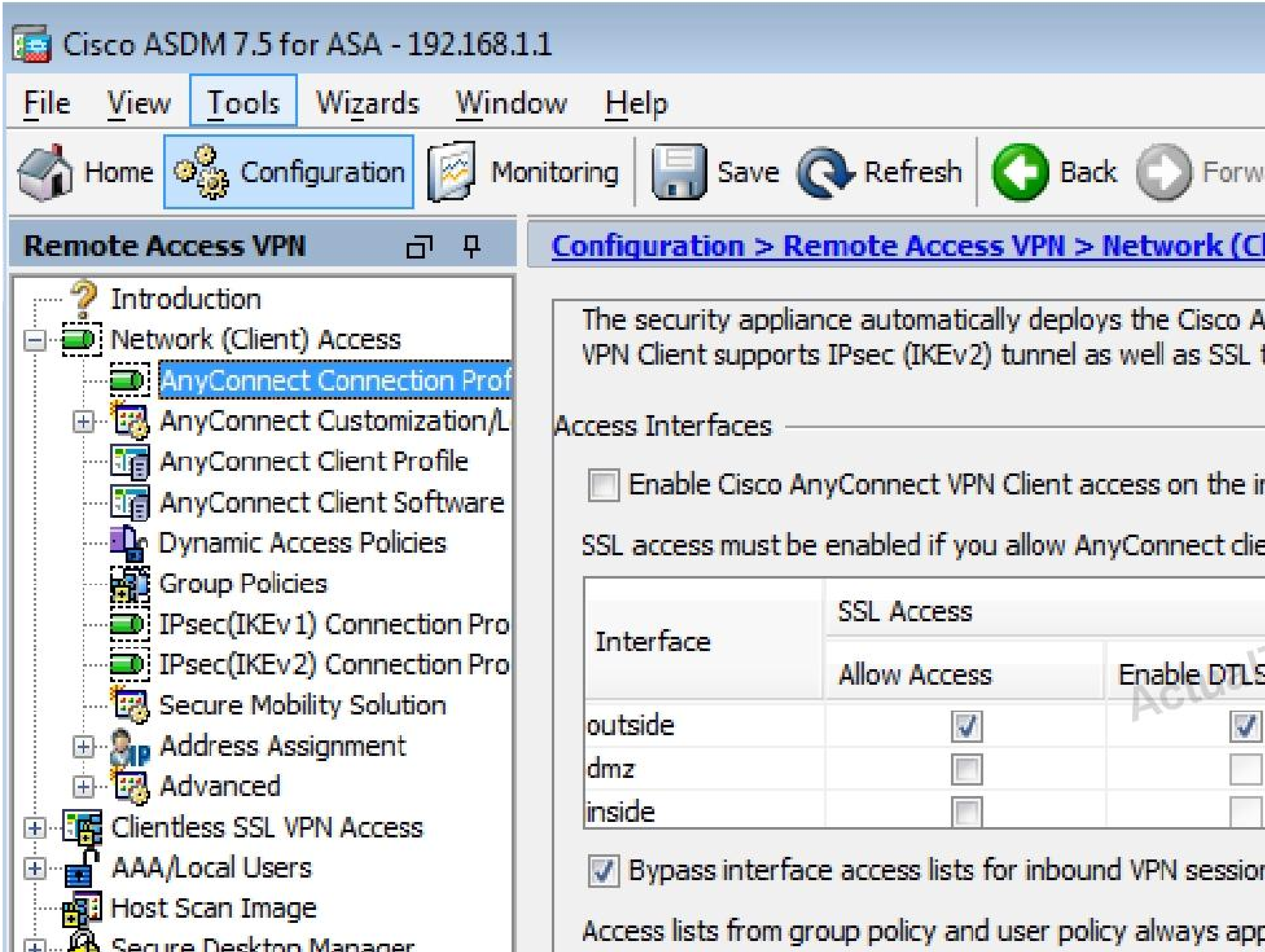
Not A, as this is listed under the Identity Certificates, not the CA certificates:



Configuration > Remote Access VPN > Certificate

Issued To	Issued By
hostname=P17-ASA.sec...	hostname=P17-ASA.sec...

Note E:



The security appliance automatically deploys the Cisco A
VPN Client supports IPsec (IKEv2) tunnel as well as SSL t

Access Interfaces

☐ Enable Cisco AnyConnect VPN Client access on the i

SSL access must be enabled if you allow AnyConnect clie

Interface	SSL Access	
	Allow Access	Enable DTLS
outside	☑	☑
dmz	☐	☐
inside	☐	☐

☑ Bypass interface access lists for inbound VPN sessio

Access lists from group policy and user policy always app

"

QUESTION 65
When users login to the Clientless SSLVPN using https://209.165.201.2/test, which group policy will be applied?

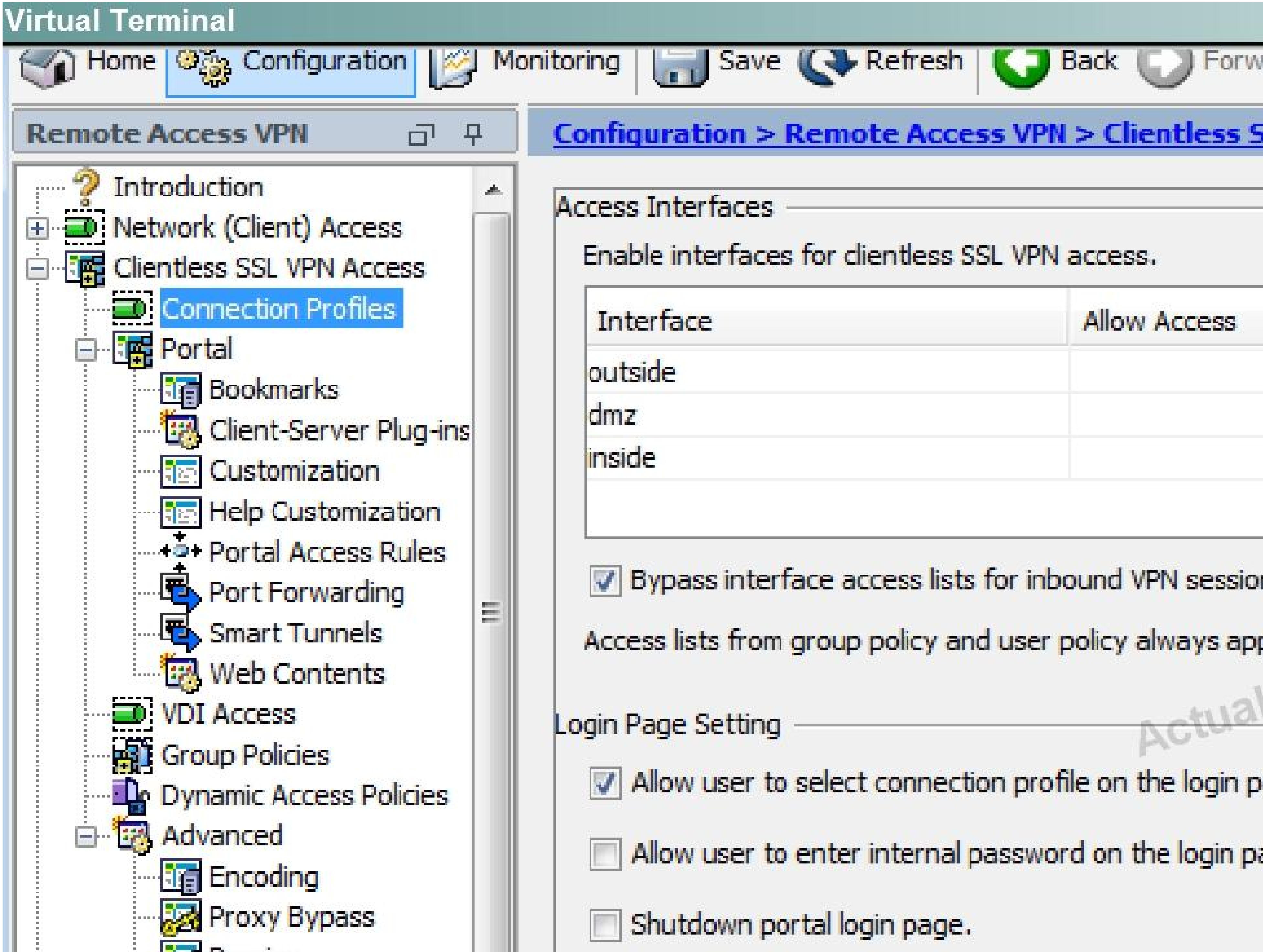
A. test
B. clientless
C. Sales
D. DfltGrpPolicy
E. DefaultRAGroup
F. DefaultWEBVPNGroup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

Explanation:

First navigate to the Connection Profiles tab as shown below, highlight the one with the test alias:



Configuration > Remote Access VPN > Clientless S

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	
dmz	
inside	

☑ Bypass interface access lists for inbound VPN sessio

Access lists from group policy and user policy always app

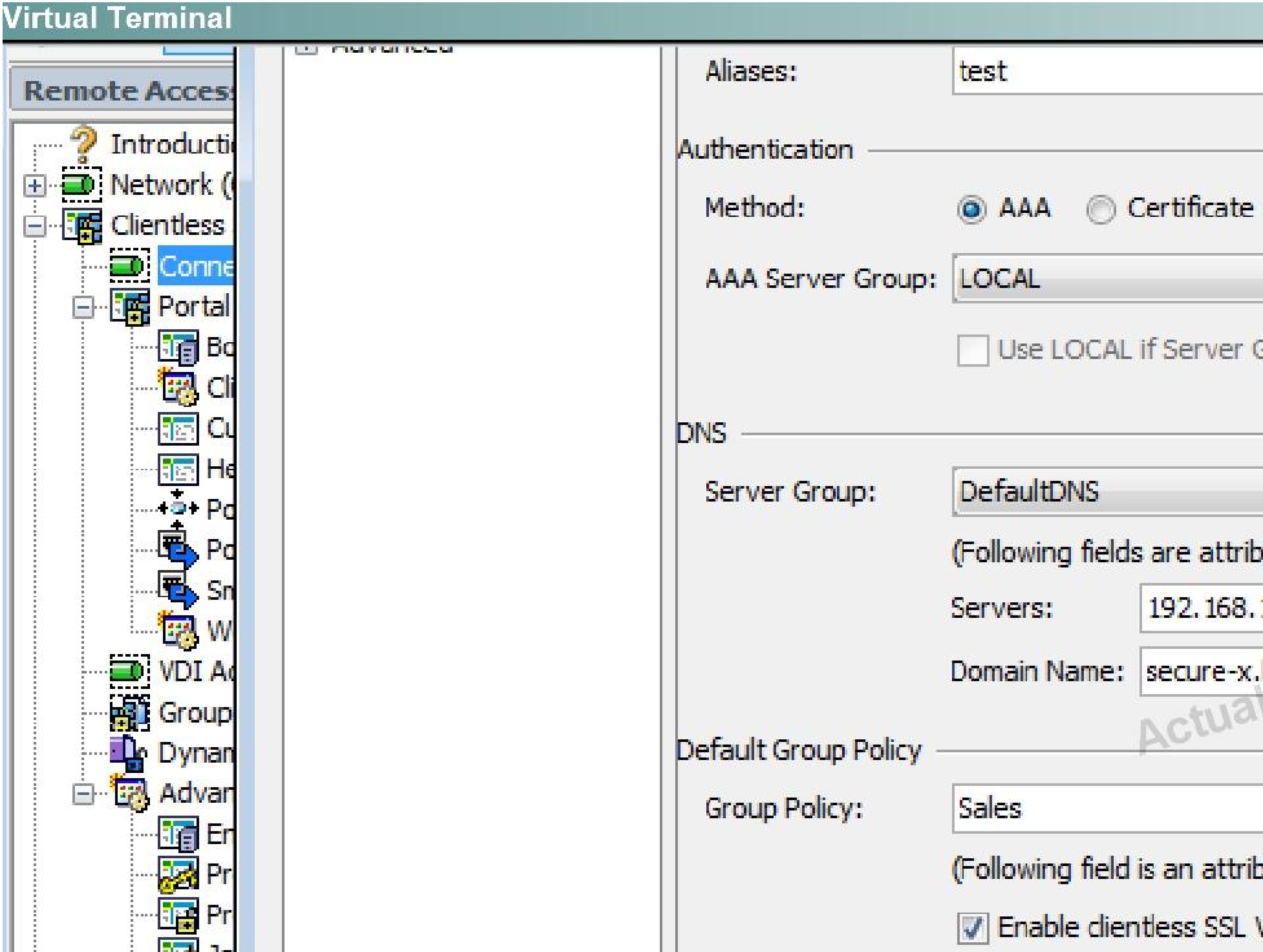
Login Page Setting

☑ Allow user to select connection profile on the login p

☐ Allow user to enter internal password on the login pa

☐ Shutdown portal login page.

Then hit the “edit” button and you can clearly see the Sales Group Policy being applied.



Aliases: test

Authentication

Method: ● AAA ○ Certificate

AAA Server Group: LOCAL

□ Use LOCAL if Server G

DNS

Server Group: DefaultDNS

(Following fields are attrib

Servers: 192.168.

Domain Name: secure-x.

Default Group Policy

Group Policy: Sales

(Following field is an attrib

☑ Enable clientless SSL V

QUESTION 66
How many crypto map sets can you apply to a router interface?

A. 3
B. 2
C. 4
D. 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 67
What is the transition order of STP states on a Layer 2 switch interface?

A. listening, learning, blocking, forwarding, disabled
B. listening, blocking, learning, forwarding, disabled
C. blocking, listening, learning, forwarding, disabled
D. forwarding, listening, learning, blocking, disabled

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which sensor mode can deny attackers inline?

A. IPS
B. fail-close
C. IDS
D. fail-open

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which options are filtering options used to display SDEE message types? (Choose two.)

A. stop
B. none
C. error
D. all

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
C,D

QUESTION 70
When a company puts a security policy in place, what is the effect on the company's business?

A. Minimizing risk
B. Minimizing total cost of ownership
C. Minimizing liability
D. Maximizing compliance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which wildcard mask is associated with a subnet mask of /27?

A. 0.0.0.255

B. 0.0.027
C. 0.0.0.31
D. 0.0.0.224

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 72
Which actions can a promiscuous IPS take to mitigate an attack? (Choose three.)

A. Modifying packets
B. Requesting connection blocking
C. Denying packets
D. Resetting the TCP connection
E. Requesting host blocking
F. Denying frames

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Answer: B,D,E

QUESTION 73
Which command will configure a Cisco ASA firewall to authenticate users when they enter the enable syntax using the local database with no fallback method?

A. aaa authentication enable console LOCAL SERVER_GROUP
B. aaa authentication enable console SERVER_GROUP LOCAL
C. aaa authentication enable console local
D. aaa authentication enable console LOCAL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: D

QUESTION 74
Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?

A. FlexConfig
B. Device Manager
C. Report Manager
D. Health and Performance Monitor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 75
Which command is needed to enable SSH support on a Cisco Router?

A. crypto key lock rsa
B. crypto key generate rsa
C. crypto key zeroize rsa
D. crypto key unlock rsa

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: B
Explanation:

QUESTION 76
Which protocol provides security to Secure Copy?

A. IPsec

B. SSH
C. HTTPS
D. ESP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which security zone is automatically defined by the system?

A. The source zone
B. The self zone
C. The destination zone
D. The inside zone

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.)

A. The Internet Key Exchange protocol establishes security associations
B. The Internet Key Exchange protocol provides data confidentiality
C. The Internet Key Exchange protocol provides replay detection
D. The Internet Key Exchange protocol is responsible for mutual authentication

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which address block is reserved for locally assigned unique local addresses?

A. 2002::/16
B. FD00::/8
C. 2001::/32
D. FB00::/8

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: B
Explanation:

QUESTION 80
What is a possible reason for the error message?Router(config)#aaa server?% Unrecognized command

A. The command syntax requires a space after the word “server”
B. The command is invalid on the target device
C. The router is already running the latest operating system
D. The router is a new device on which the aaa new-model command must be applied before continuing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: D
Explanation:

QUESTION 81
If the native VLAN on a trunk is different on each end of the link, what is a potential consequence?

A. The interface on both switches may shut down
B. STP loops may occur

C. The switch with the higher native VLAN may shut down
D. The interface with the lower native VLAN may shut down

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: B
Explanation:

QUESTION 82
Which option describes information that must be considered when you apply an access list to a physical interface?

A. Protocol used for filtering
B. Direction of the access class
C. Direction of the access group
D. Direction of the access list

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: C
Explanation:

QUESTION 83
Which of the following are features of IPsec transport mode? (Choose three.)

A. IPsec transport mode is used between end stations
B. IPsec transport mode is used between gateways
C. IPsec transport mode supports multicast
D. IPsec transport mode supports unicast
E. IPsec transport mode encrypts only the payload
F. IPsec transport mode encrypts the entire packet

Correct Answer: ADE

Section: (none)
Explanation

Explanation/Reference:
Answer: A,D,E

QUESTION 84
Which command causes a Layer 2 switch interface to operate as a Layer 3 interface?

A. no switchport nonnegotiate
B. switchport
C. no switchport mode dynamic auto
D. no switchport

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: D

QUESTION 85
Which TACACS+ server-authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

A. EAP
B. ASCII
C. PAP
D. PEAP
E. MS-CHAPv1
F. MS-CHAPv2

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Answer: B,C,E
Explanation:

QUESTION 86
Which type of IPS can identify worms that are propagating in a network?

A. Policy-based IPS
B. Anomaly-based IPS
C. Reputation-based IPS
D. Signature-based IPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: B

QUESTION 87
Which command verifies phase 1 of an IPsec VPN on a Cisco router?

A. show crypto map
B. show crypto ipsec sa
C. show crypto isakmp sa
D. show crypto engine connection active

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: C

QUESTION 88
What is the purpose of a honeypot IPS?

A. To create customized policies
B. To detect unknown attacks
C. To normalize streams
D. To collect information about attacks

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Answer: D

QUESTION 89
Which type of firewall can act on the behalf of the end device?

A. Stateful packet
B. Application
C. Packet
D. Proxy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: D

QUESTION 90
Which syslog severity level is level number 7?

A. Warning
B. Informational
C. Notification
D. Debugging

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
By which kind of threat is the victim tricked into entering username and password information at a disguised website?

A. Spoofing
B. Malware
C. Spam
D. Phishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: D

QUESTION 92
Which tasks is the session management path responsible for? (Choose three.)

A. Verifying IP checksums
B. Performing route lookup
C. Performing session lookup
D. Allocating NAT translations
E. Checking TCP sequence numbers
F. Checking packets against the access list

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Answer: B,D,F

QUESTION 93
Which network device does NTP authenticate?

A. Only the time source
B. Only the client device
C. The firewall and the client device
D. The client device and the time source

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

Answer: A

Explanation:

QUESTION 94

Which Cisco product can help mitigate web-based attacks within a network?

A. Adaptive Security Appliance
B. Web Security Appliance
C. Email Security Appliance
D. Identity Services Engine

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Answer: B

QUESTION 95

What hash type does Cisco use to validate the integrity of downloaded images?

A. Sha1
B. Sha2
C. Md5
D. Md1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Answer: C

QUESTION 96

Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path?

A. Unidirectional Link Detection

B. Unicast Reverse Path Forwarding
C. TrustSec
D. IP Source Guard

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: B

QUESTION 97
What is the most common Cisco Discovery Protocol version 1 attack?

A. Denial of Service
B. MAC-address spoofing
C. CAM-table overflow
D. VLAN hopping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 98
What is the Cisco preferred countermeasure to mitigate CAM overflows?

A. Port security
B. Dynamic port security
C. IP source guard
D. Root guard

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Answer: B

QUESTION 99
Which option is the most effective placement of an IPS device within the infrastructure?

A. Promiscuously, after the Internet router and before the firewall
B. Promiscuously, before the Internet router and the firewall
C. Inline, behind the internet router and firewall
D. Inline, before the internet router and firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
c

QUESTION 100
If a router configuration includes the line aaa authentication login default group tacacs+ enable, which events will occur when the TACACS+ server returns an error? (Choose two.)

A. The user will be prompted to authenticate using the enable password
B. Authentication attempts to the router will be denied
C. Authentication will use the router‘s local database
D. Authentication attempts will be sent to the TACACS+ server

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which alert protocol is used with Cisco IPS Manager Express to support up to 10 sensors?

A. SDEE
B. Syslog
C. SNMP
D. CSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 102
Which type of address translation should be used when a Cisco ASA is in transparent mode?

A. Dynamic PAT
B. Dynamic NAT
C. Overload
D. Static NAT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 103
Which components does HMAC use to determine the authenticity and integrity of a message?
(Choose two.)

A. The password
B. The hash
C. The key
D. The transform set

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
What is the default timeout interval during which a router waits for responses from a TACACS

server before declaring a timeout failure?

A. 15 seconds
B. 10 seconds
C. 5 seconds
D. 20 seconds

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 105
Which command initializes a lawful intercept view?

A. username cisco1 view lawful-intercept password cisco
B. parser view cisco li-view
C. li-view cisco user cisco1 password cisco
D. parser view li-view inclusive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: C
Explanation:

QUESTION 106
Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)

A. Port security
B. DHCP snooping
C. IP source guard
D. Dynamic ARP inspection

Correct Answer: BD
Section: (none)

Explanation

Explanation/Reference:

Answer: B,D

QUESTION 107

Which of the following statements about access lists are true? (Choose three.)

A. Extended access lists should be placed as near as possible to the destination
B. Extended access lists should be placed as near as possible to the source
C. Standard access lists should be placed as near as possible to the destination
D. Standard access lists should be placed as near as possible to the source
E. Standard access lists filter on the source address
F. Standard access lists filter on the destination address

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

Answer: B,C,E

QUESTION 108

Which statement about extended access lists is true?

A. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the destination
B. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the source
C. Extended access lists perform filtering that is based on destination and are most effective when applied to the source
D. Extended access lists perform filtering that is based on source and are most effective when applied to the destination

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Answer: B

QUESTION 109
In which stage of an attack does the attacker discover devices on a target network?

A. Reconnaissance
B. Covering tracks
C. Gaining access
D. Maintaining access

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 110
Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)

A. FTP
B. SSH
C. Telnet
D. AAA
E. HTTPS
F. HTTP

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Answer: B,E

QUESTION 111
What are the primary attack methods of VLAN hopping? (Choose two.)

A. VoIP hopping
B. Switch spoofing

C. CAM-table overflow
D. Double tagging

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
How can the administrator enable permanent client installation in a Cisco AnyConnect VPN firewall configuration?

A. Issue the command anyconnect keep-installer under the group policy or username webvpn mode
B. Issue the command anyconnect keep-installer installed in the global configuration
C. Issue the command anyconnect keep-installer installed under the group policy or username webvpn mode
D. Issue the command anyconnect keep-installer installer under the group policy or username webvpn mode

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: C

QUESTION 113
Which type of security control is defense in depth?

A. Overt and covert channels
B. Threat mitigation
C. Botnet mitigation
D. Risk analysis

Correct Answer: B
Section: (none)
Explanation

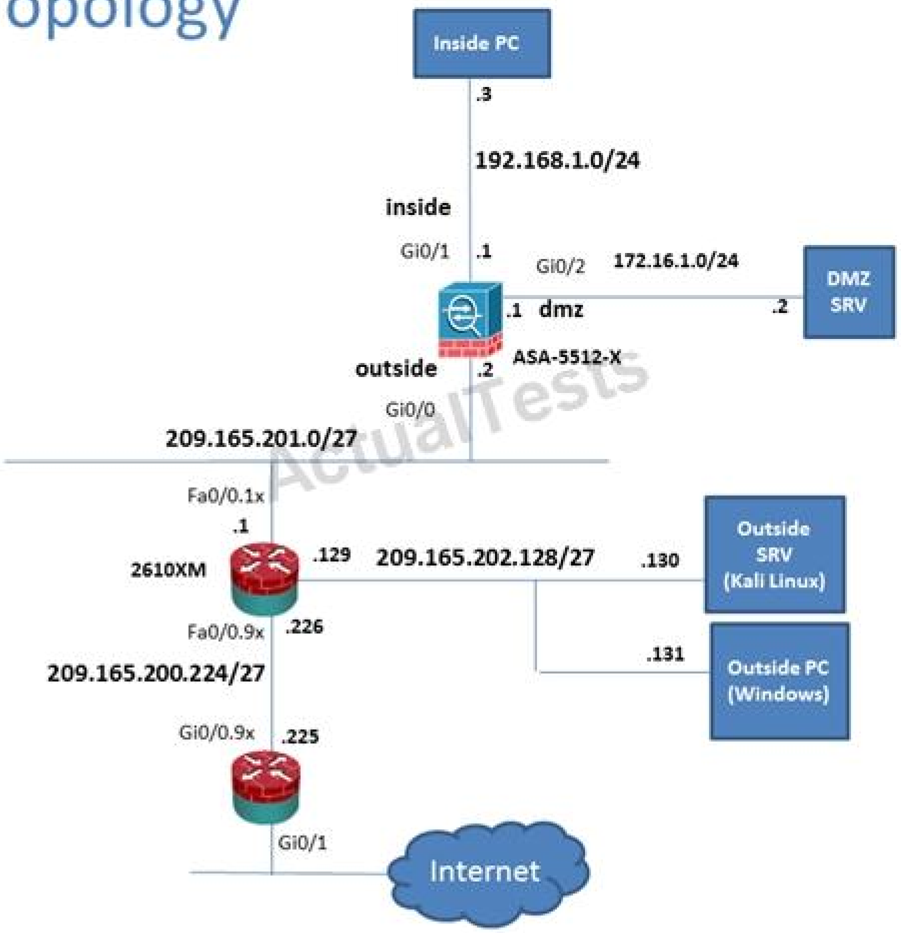
Explanation/Reference:
B

Exam B

QUESTION 1

SIMULATION
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
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.
Cisco 210-260 Exam
"

Lab Topology



Case Study Title (Case Study):
Which four tunneling protocols are enabled in the DfltGrpPolicy group policy? (Choose four)

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

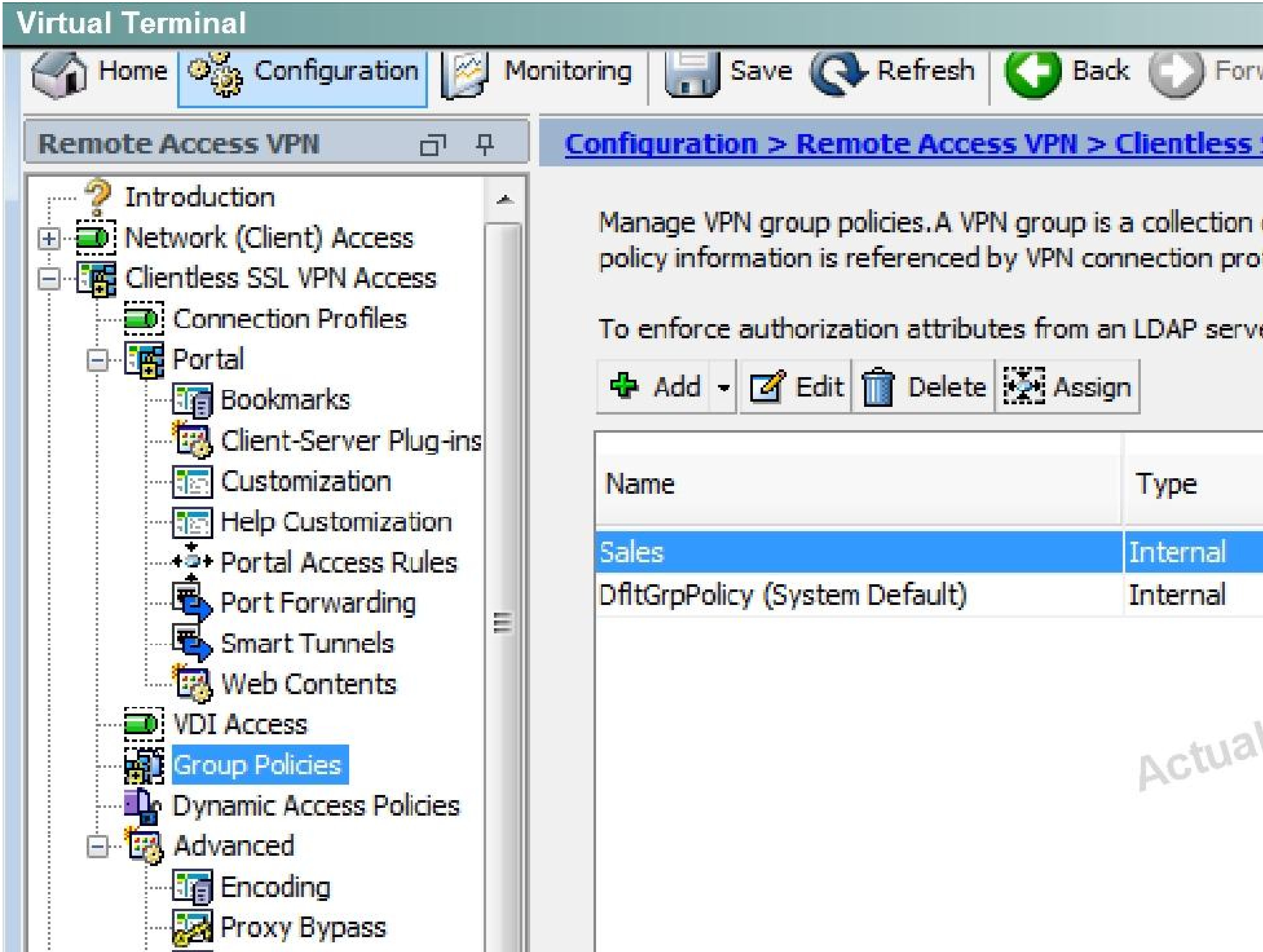
F. IPsec IKEv2

Correct Answer: ADEF
Section: (none)
Explanation

Explanation/Reference:
Answer:
A, D, E, F

Explanation:

By clicking one the Configuration-> Remote Access -> Clientless CCL VPN Access-> Group Policies tab you can view the DfltGrpPolicy protocols as shown below:



Configuration > Remote Access VPN > Clientless

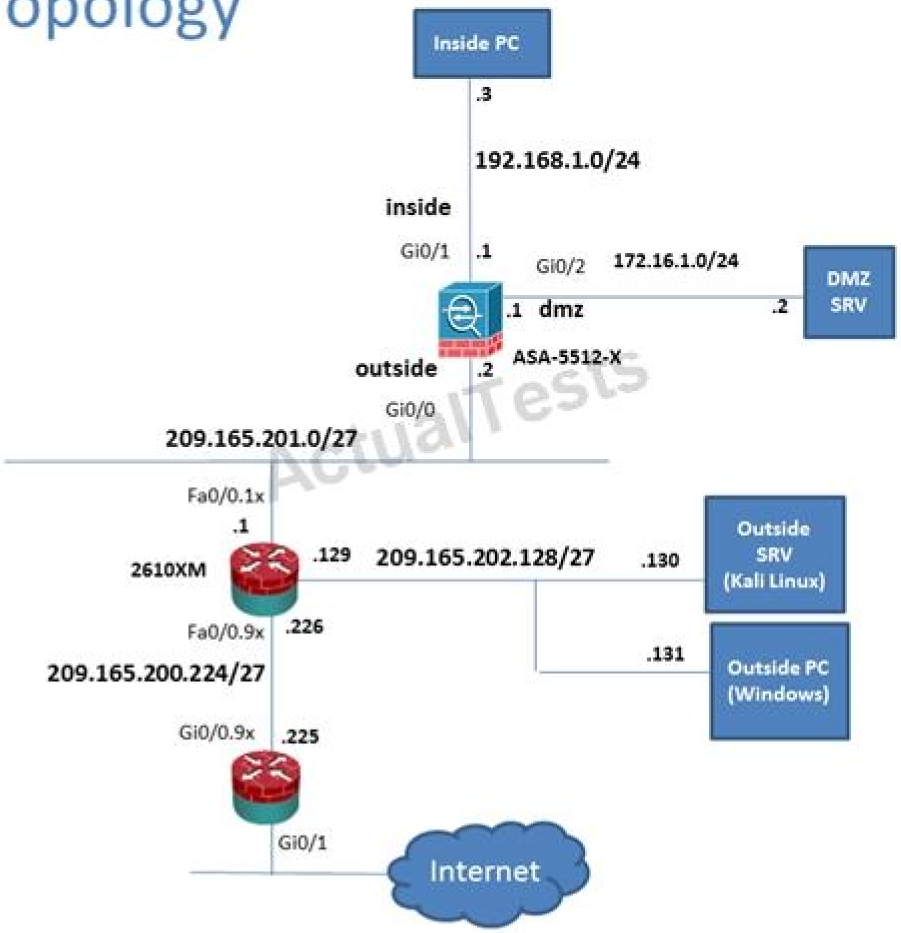
Manage VPN group policies.A VPN group is a collection
policy information is referenced by VPN connection pro

To enforce authorization attributes from an LDAP serve

Name	Type
Sales	Internal
DfltGrpPolicy (System Default)	Internal

QUESTION 2
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
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.
Cisco 210-260 Exam
"

Lab Topology



Which user authentication method is used when users login to the Clientless SSLVPN portal using https://209.165.201.2/test?

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

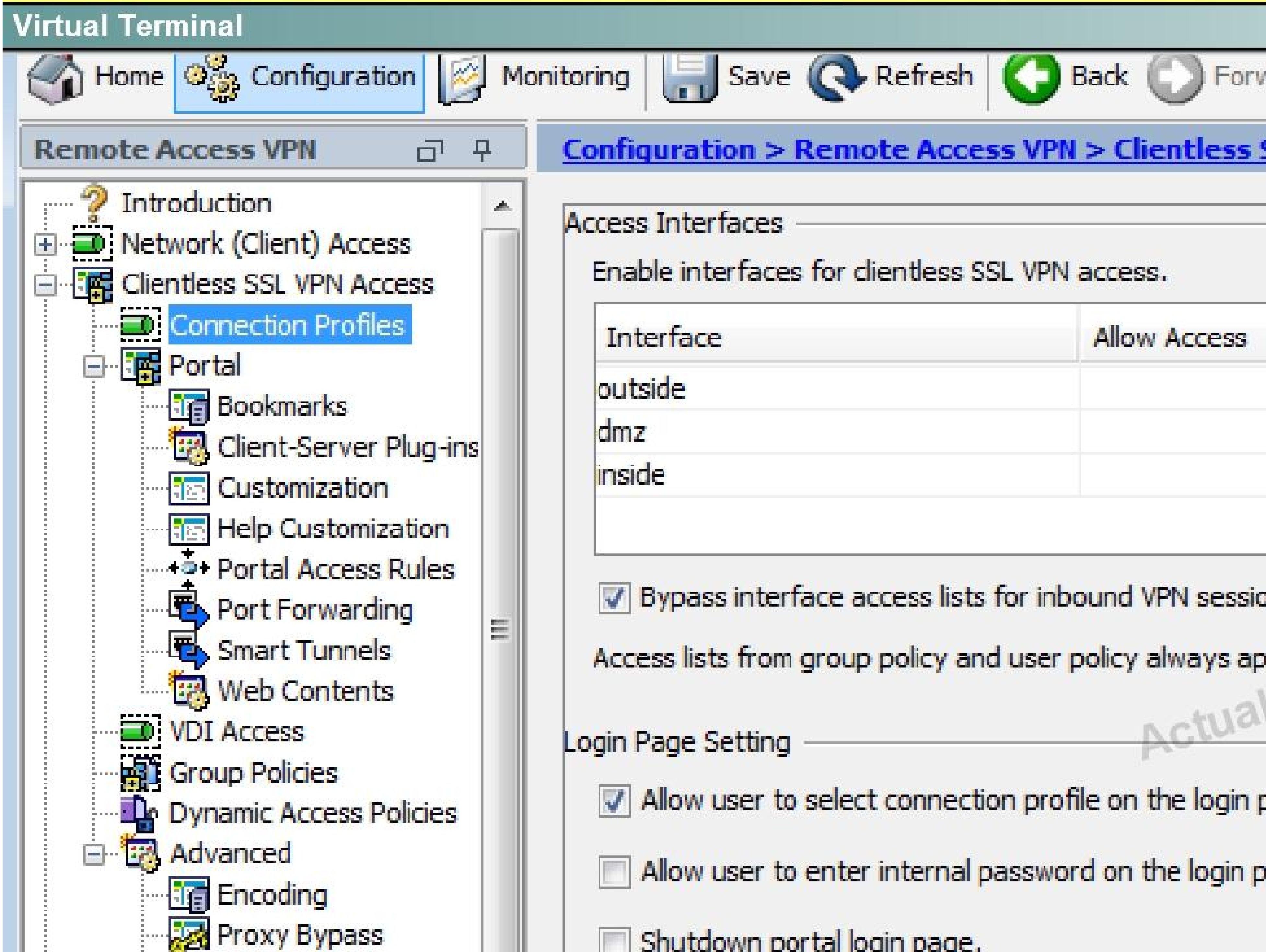
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Answer: A

Explanation:

This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration, where the alias of test is being used,
Cisco 210-260 Exam
"



Configuration > Remote Access VPN > Clientless S

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	
dmz	
inside	

☑ Bypass interface access lists for inbound VPN sessio

Access lists from group policy and user policy always ap

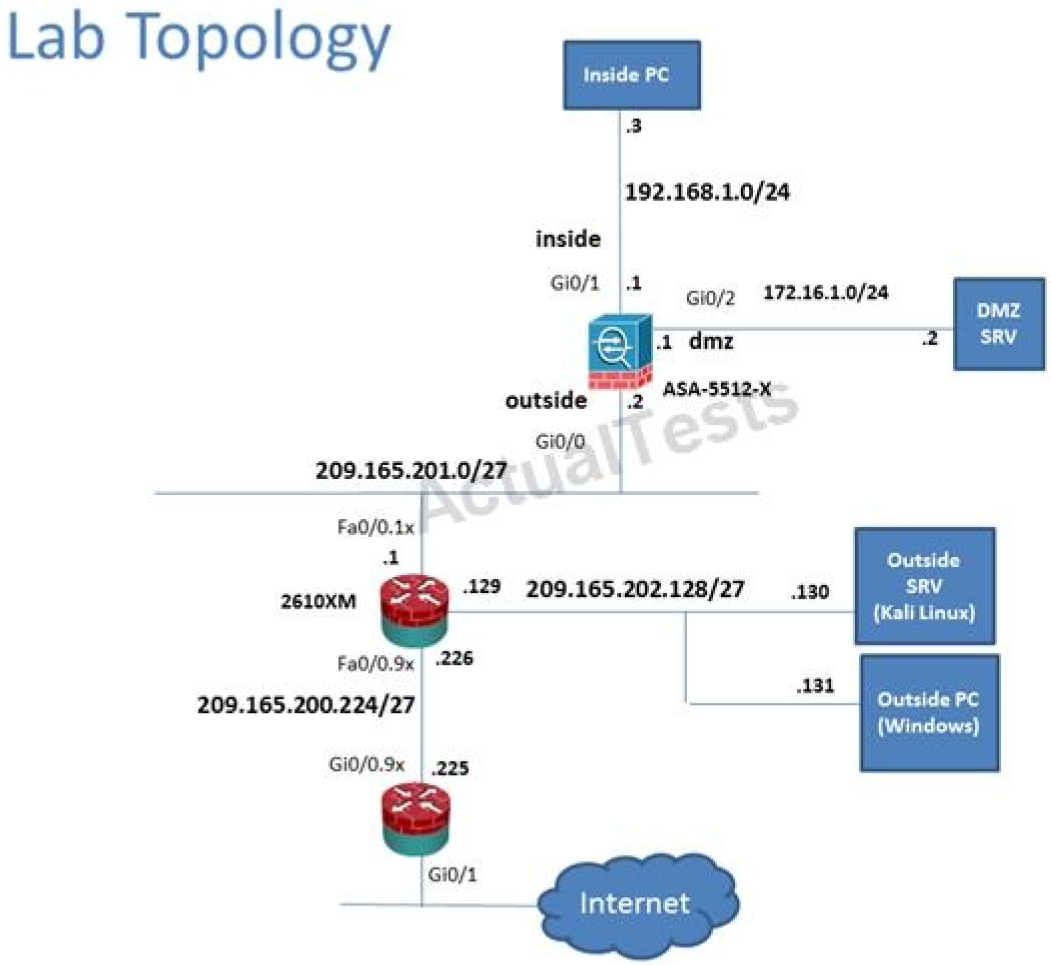
Login Page Setting

☑ Allow user to select connection profile on the login p

☐ Allow user to enter internal password on the login p

☐ Shutdown portal login page.

QUESTION 3
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
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.



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

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

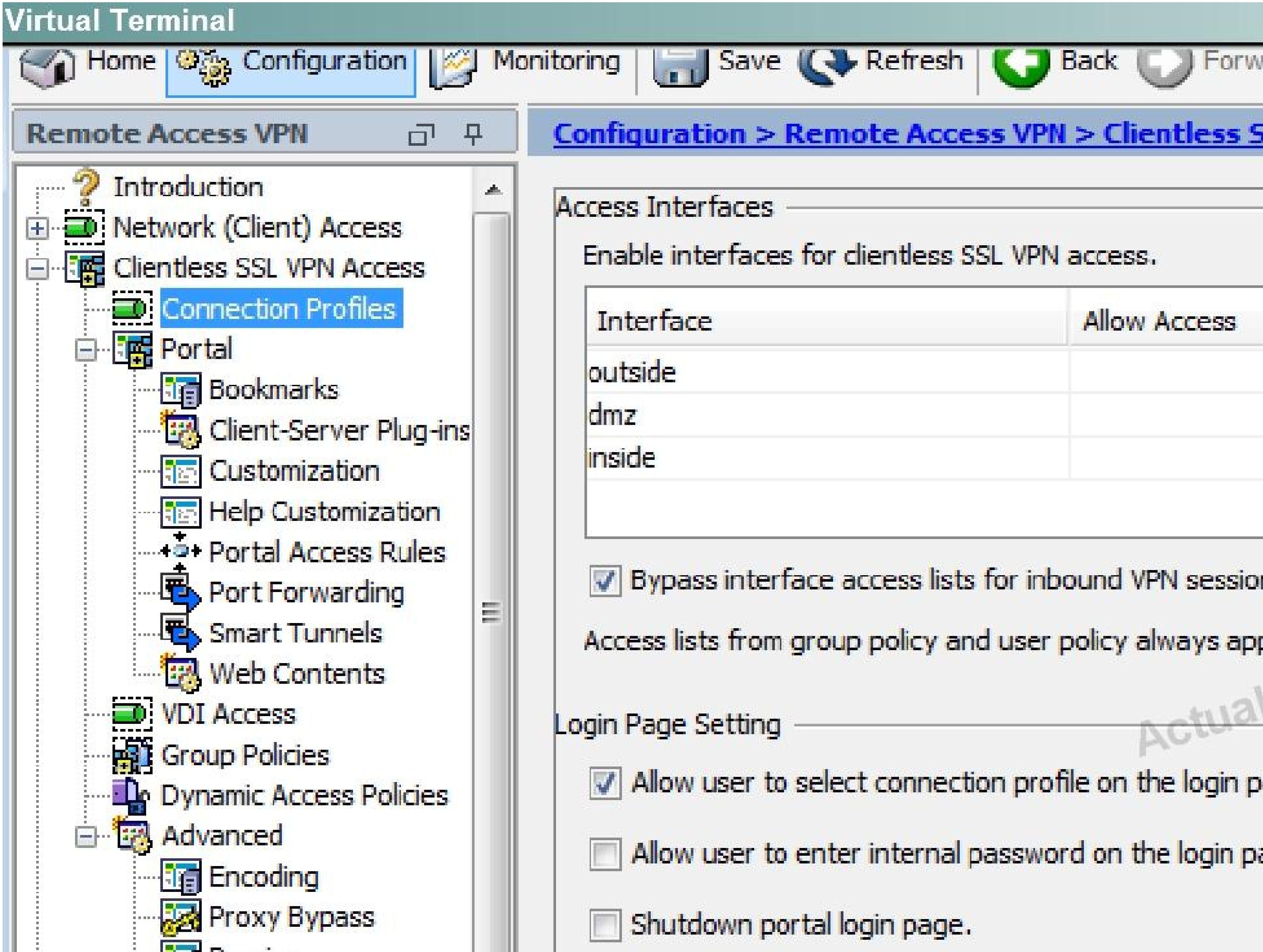
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Answer: C

Explanation:

First navigate to the Connection Profiles tab as shown below, highlight the one with the test alias:



Configuration > Remote Access VPN > Clientless S

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	
dmz	
inside	

☑ Bypass interface access lists for inbound VPN sessio

Access lists from group policy and user policy always app

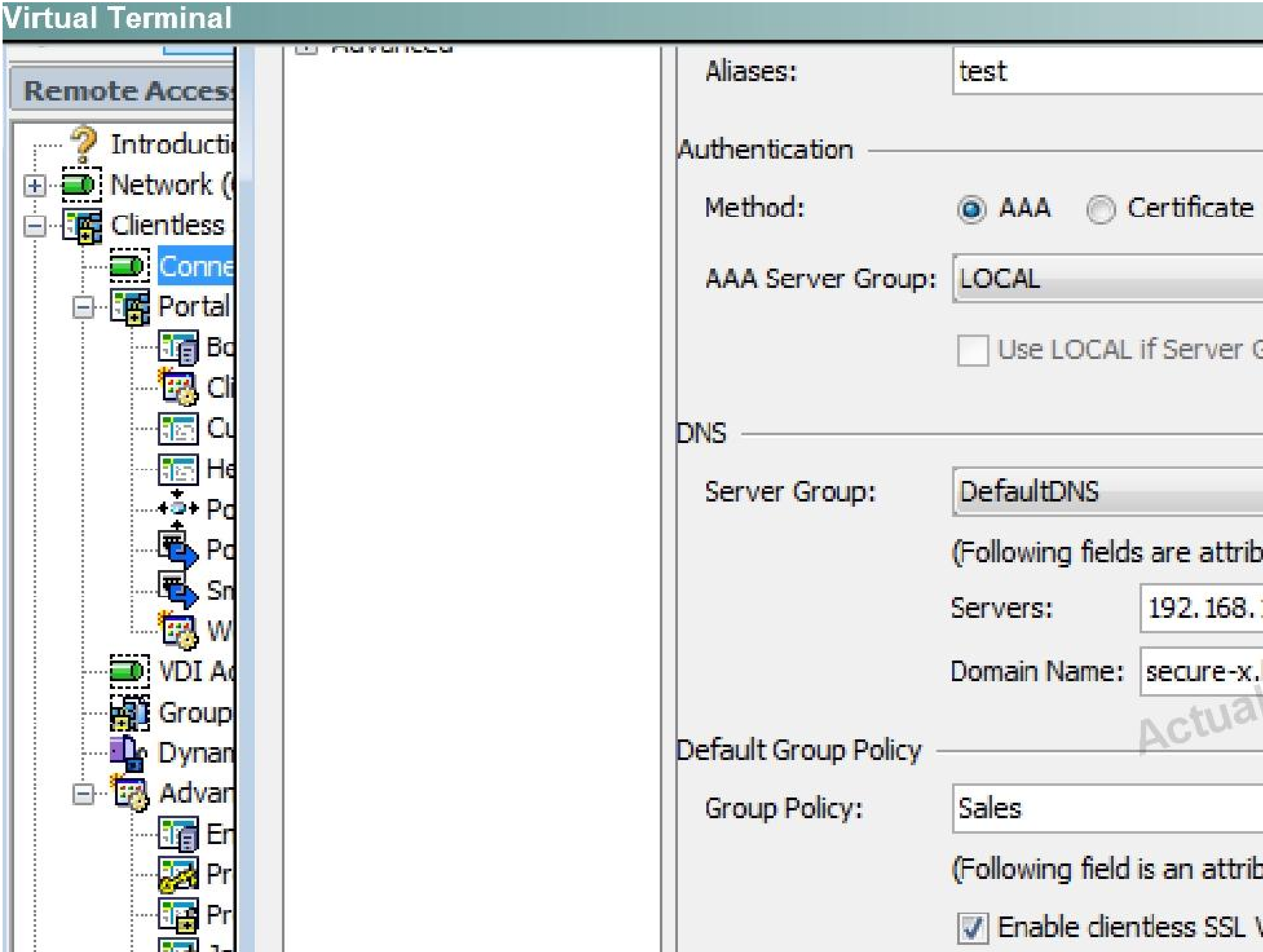
Login Page Setting

☑ Allow user to select connection profile on the login p

□ Allow user to enter internal password on the login pa

□ Shutdown portal login page.

Then hit the “edit” button and you can clearly see the Sales Group Policy being applied.



Aliases: test

Authentication

Method: ● AAA ○ Certificate

AAA Server Group: LOCAL

□ Use LOCAL if Server G

DNS

Server Group: DefaultDNS

(Following fields are attrib

Servers: 192.168.

Domain Name: secure-x.

Default Group Policy

Group Policy: Sales

(Following field is an attrib

☑ Enable clientless SSL V

QUESTION 4

SIMULATION

Scenario

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

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 ASDM to configure the ASA to also allow any host only. on the 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 the DMZ server.

Currently, hosts on the ASA higher security level interfaces are not able to ping any hosts on the lower security level interfaces. Your task in this simulation is to use ASDM to enable the ASA to dynamically allow the echo-reply responses back through the ASA.

Once the correct ASA configurations have been configured:

You can test the connectivity to http://209.165.201.30 from 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 testing pings to www.cisco.com will work.

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.

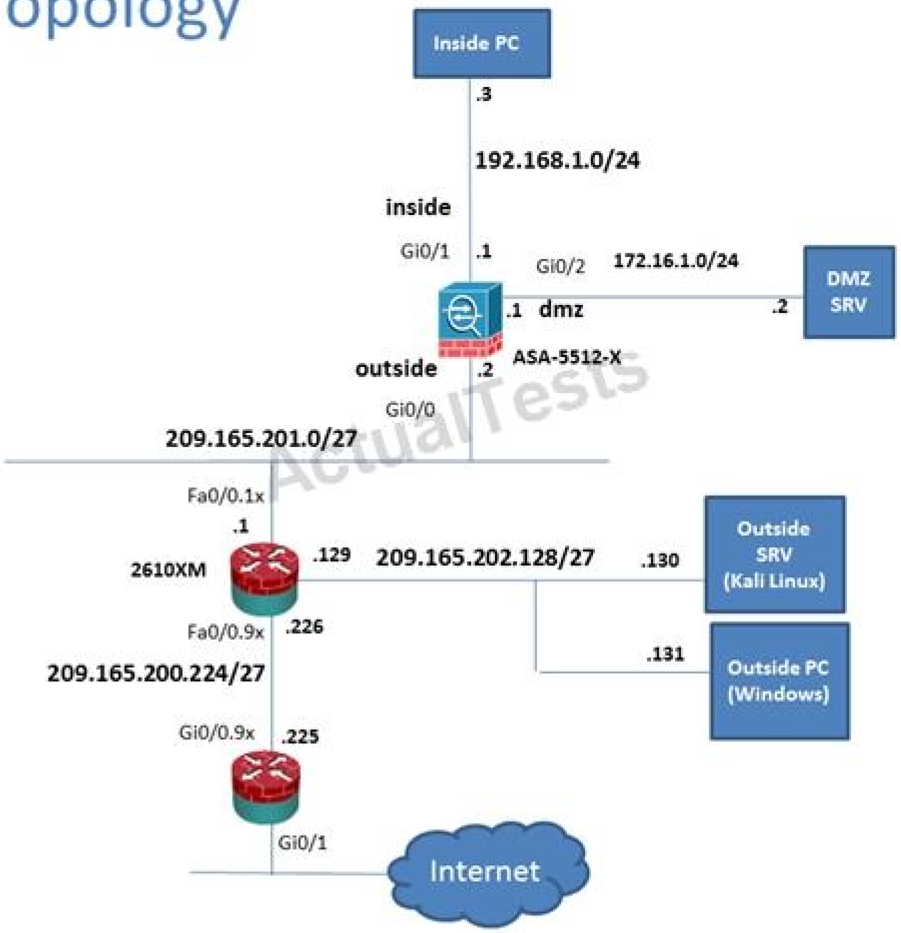
Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.

In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM.

Cisco 210-260 Exam

"

Lab Topology



Point and Shoot:

Correct Answer:

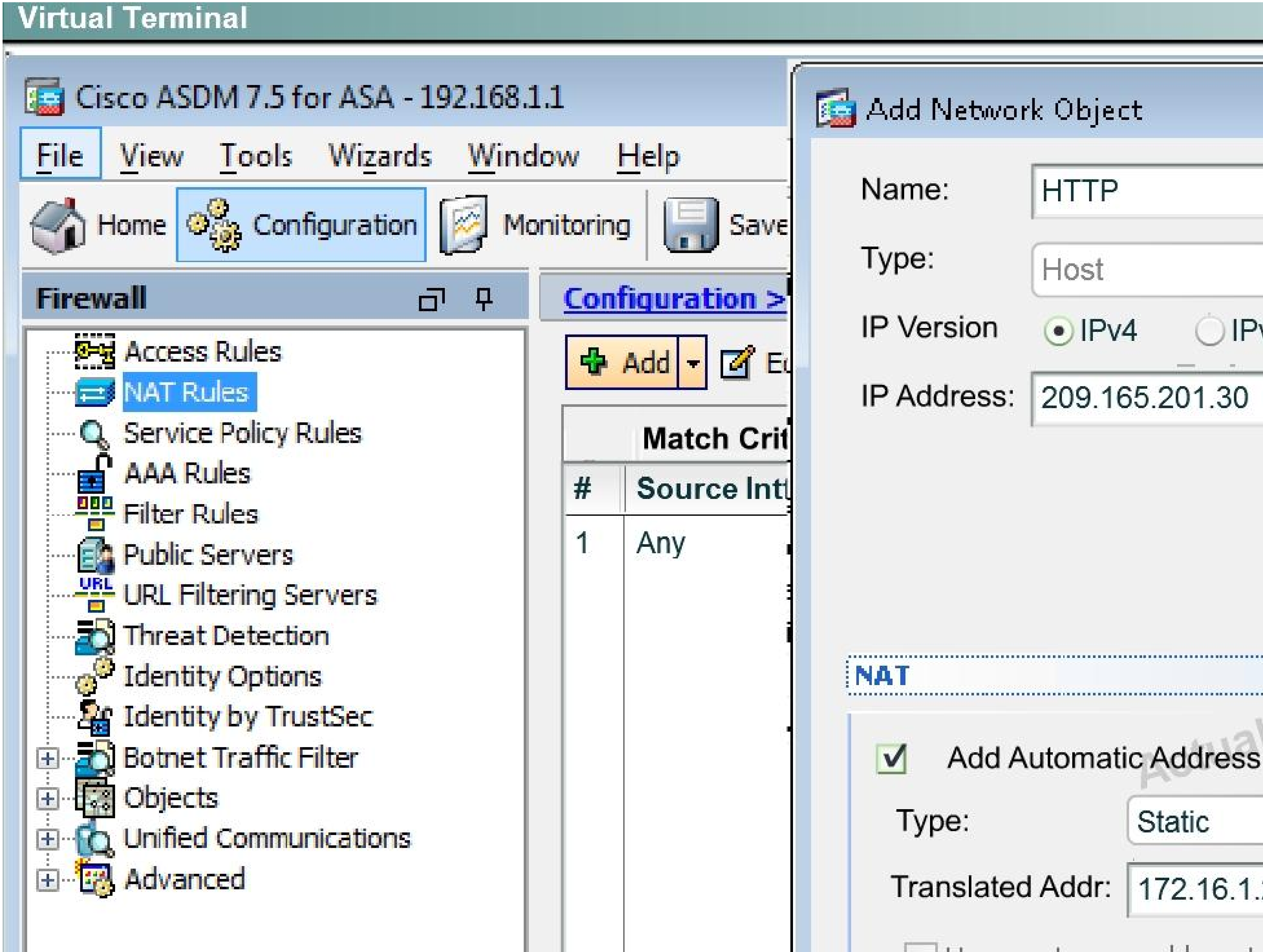
Section: (none)

Explanation

Explanation/Reference:
Answer:
Follow the explanation part to get answer on this sim question.

Explanation:

First, for the HTTP access we need to creat a NAT object. Here I called it HTTP but it can be given any name.
Then, create



#	Source Intf
1	Any

Name: HTTP

Type: Host

IP Version ● IPv4 ○ IPv

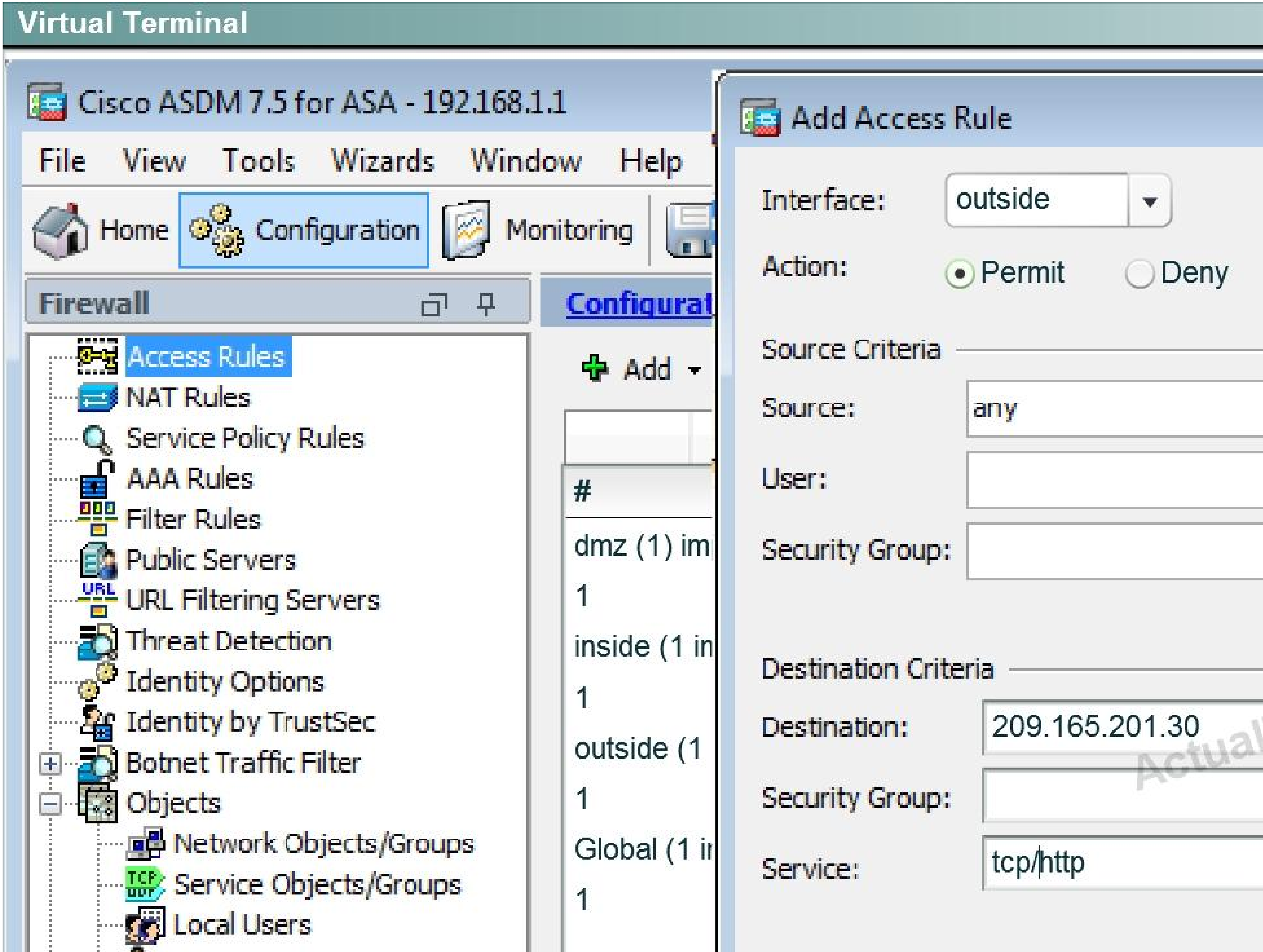
IP Address: 209.165.201.30

☑ Add Automatic Address

Type: Static

Translated Addr: 172.16.1.

Then, create the firewall rules to allow the HTTP access:



Add Access Rule

Interface: outside

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

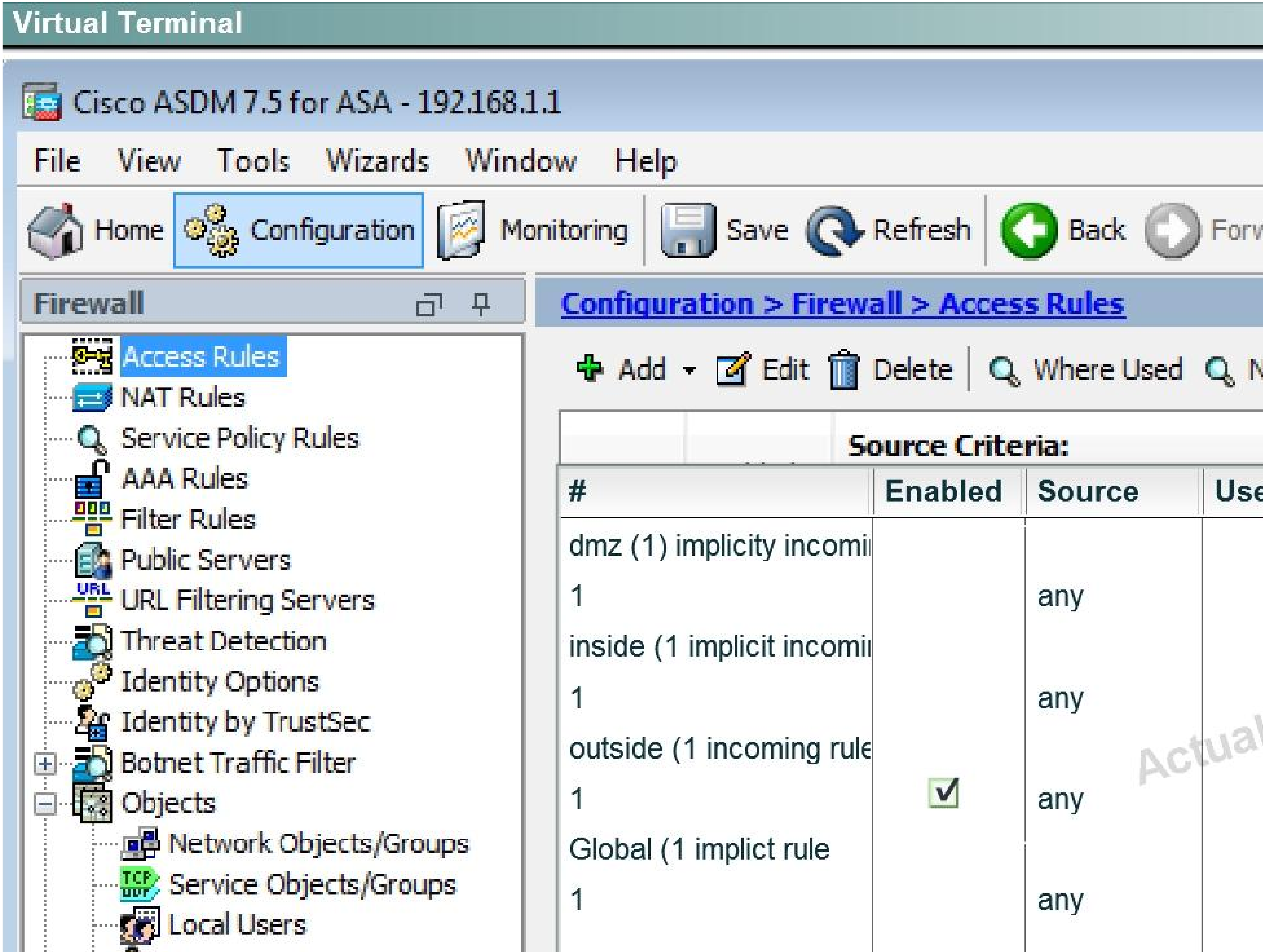
Security Group:

Destination Criteria

Destination: 209.165.201.30

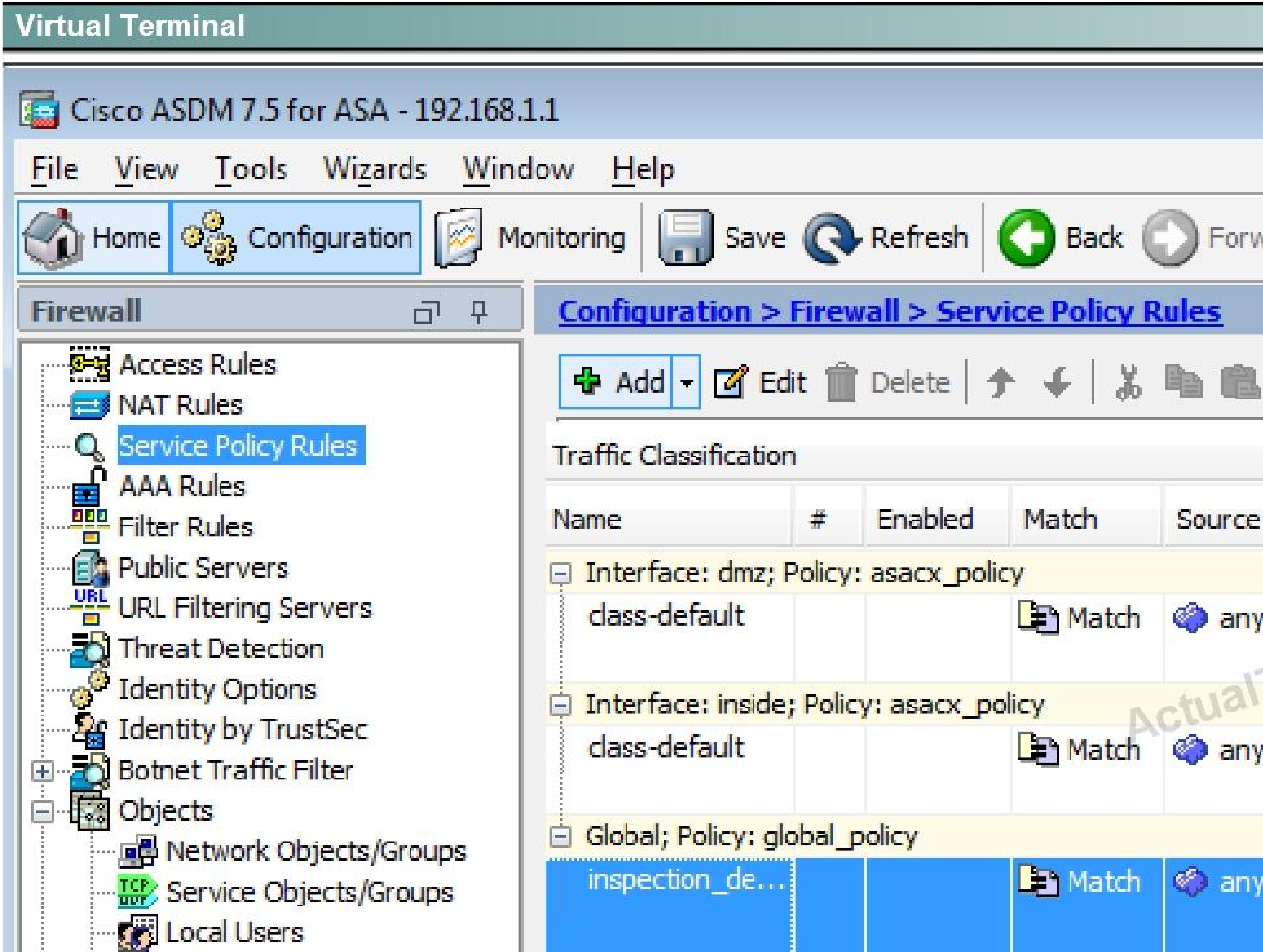
Security Group:

Service: tcp/http



		Source Criteria:	
#	Enabled	Source	Use
dmz (1) implicity incomi			
1		any	
inside (1 implicit incomi			
1		any	
outside (1 incoming rule			
1	☑	any	
Global (1 implict rule			
1		any	

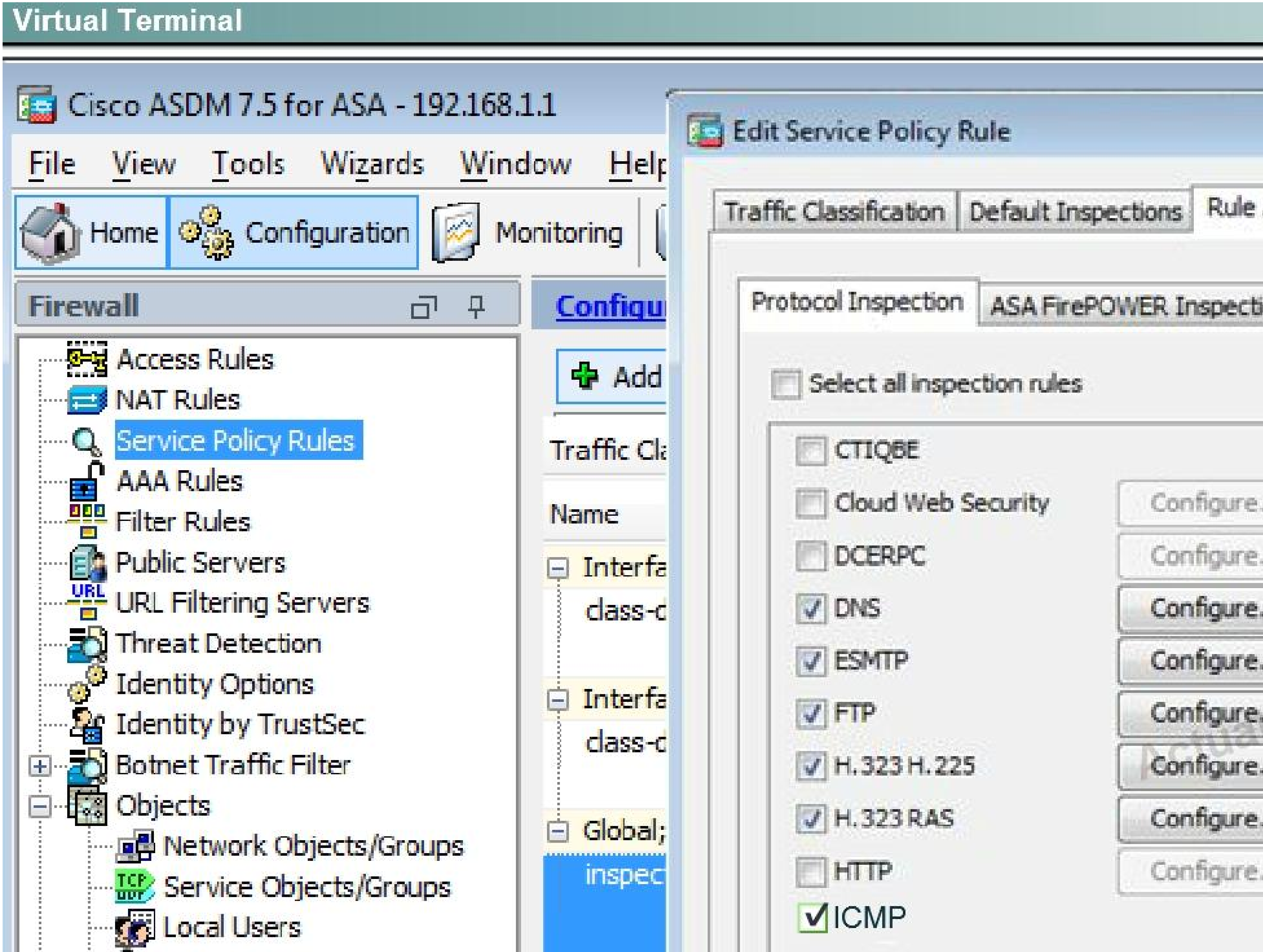
You can verify using the outside PC to HTTP into 209.165.201.30.
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:



Traffic Classification

Name	#	Enabled	Match	Source
Interface: dmz; Policy: asacx_policy				
class-default			Match	any
Interface: inside; Policy: asacx_policy				
class-default			Match	any
Global; Policy: global_policy				
inspection_de...			Match	any

And then check the ICMP box only as shown below, then hit Apply.



□ Select all inspection rules

□ CTIQBE

□ Cloud Web Security

□ DCERPC

☑ DNS

☑ ESMTP

☑ FTP

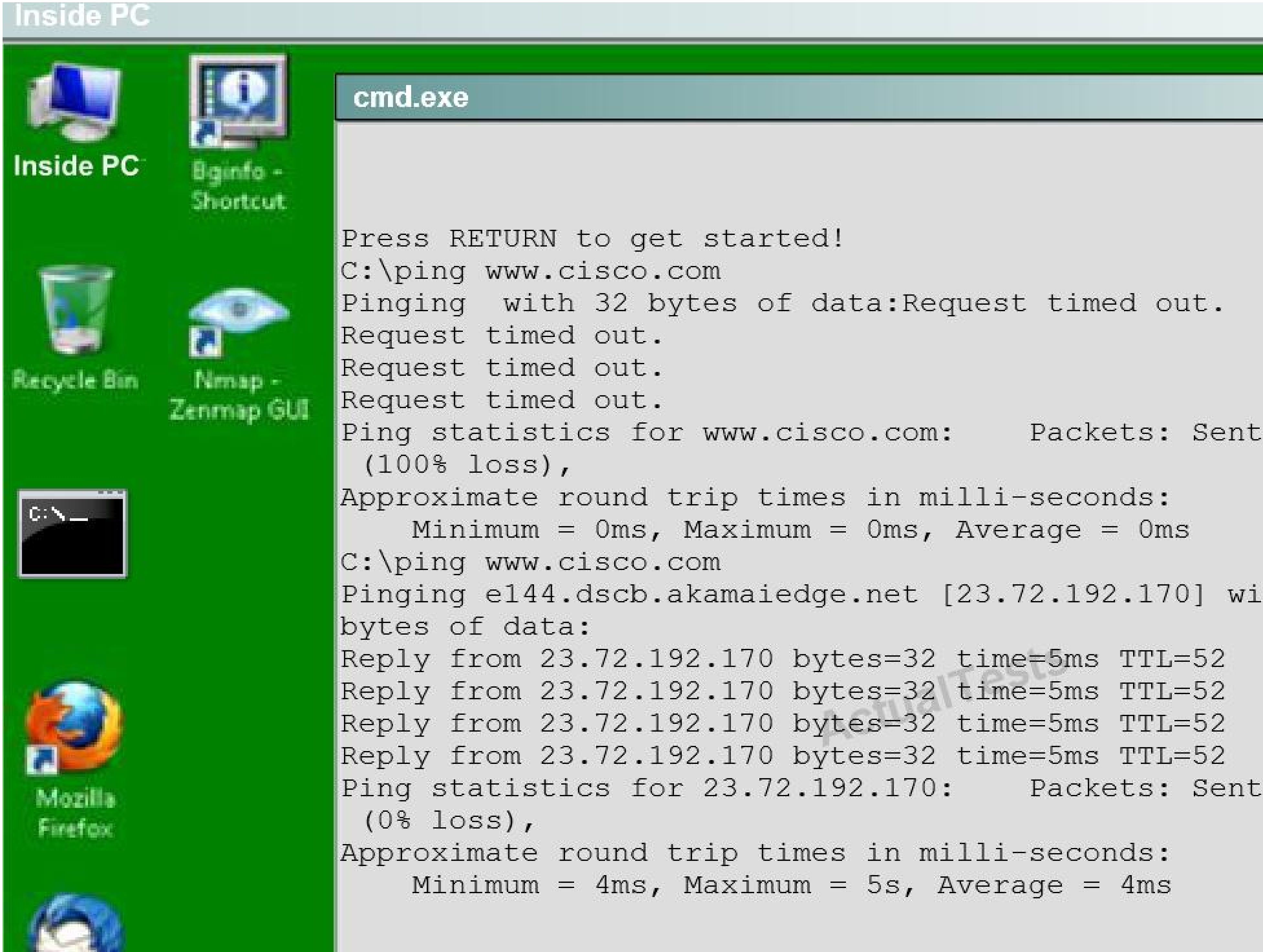
☑ H.323 H.225

☑ H.323 RAS

□ HTTP

☑ ICMP

After that is done, we can ping www.cisco.com again to verify:
Cisco 210-260 Exam
"



```
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
 (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] wi
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
 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5s, Average = 4ms
```

Exam C

QUESTION 1
What are two uses of SIEM software? (Choose two.)

A. performing automatic network audits
B. collecting and archiving syslog data
C. alerting administrators to security events in real time
D. configuring firewall and IDS devices
E. scanning email for suspicious attachments

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
BC

QUESTION 2
What are the three layers of a hierarchical network design? (Choose three.)

A. distribution
B. user
C. core
D. server
E. access
F. Internet

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
ACE

QUESTION 3
What are two ways to prevent eavesdropping when you perform device-management tasks?
(Choose two.)

A. Use SNMPv3

B. Use out-of-band management.
C. Use SNMPv2
D. Use an SSH connection.
E. Use in-band management.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
AD

QUESTION 4
In which three ways does the RADIUS protocol differ from TACACS? (Choose three.)

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

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:
AEF

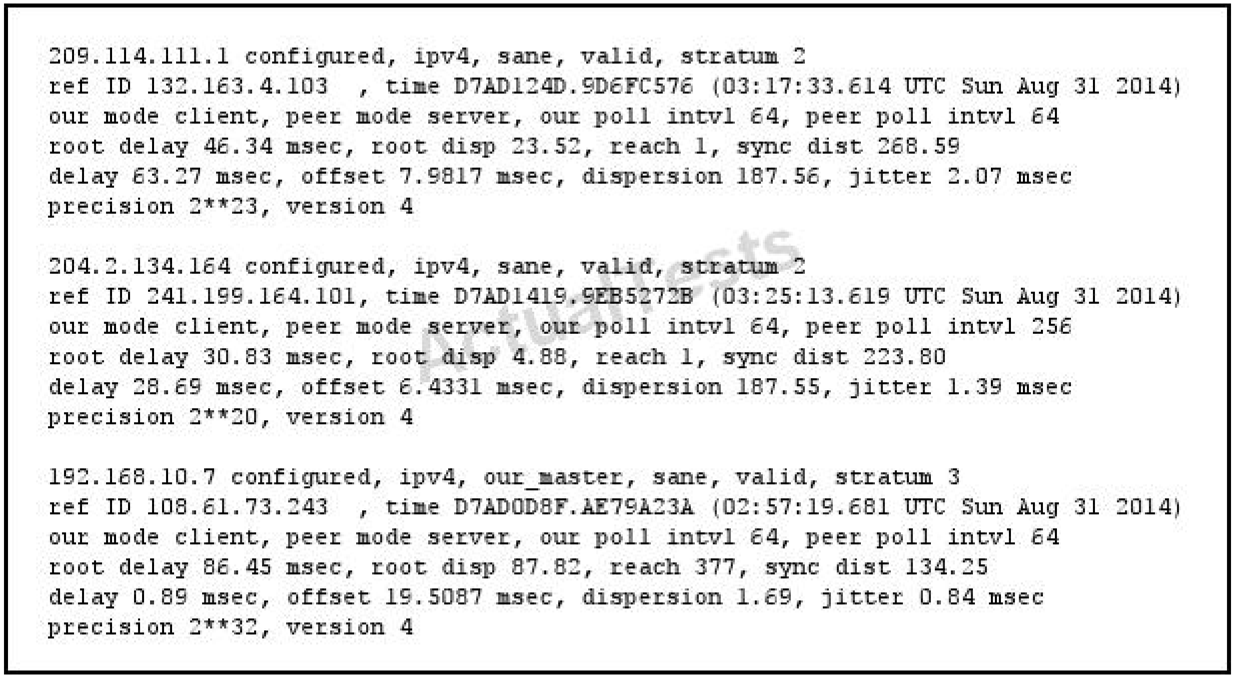
QUESTION 5
Which three statements describe DHCP spoofing attacks? (Choose three.)

A. They can access most network devices.
B. They can modify traffic in transit.
C. They are used to perform man-in-the-middle attacks.
D. They use ARP poisoning.
E. They protect the identity of the attacker by masking the DHCP address.
F. They can physically modify the network gateway.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
BCD

QUESTION 6
Refer to the exhibit.



```
209.114.111.1 configured, ipv4, sane, valid, stratum 2
ref ID 132.163.4.103  , time D7AD124D.9D6FC576 (03:17:33.614 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 46.34 msec, root disp 23.52, reach 1, sync dist 268.59
delay 63.27 msec, offset 7.9817 msec, dispersion 187.56, jitter 2.07 msec
precision 2**23, version 4

204.2.134.164 configured, ipv4, sane, valid, stratum 2
ref ID 241.199.164.101, time D7AD1419.9EB5272B (03:25:13.619 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 256
root delay 30.83 msec, root disp 4.88, reach 1, sync dist 223.80
delay 28.69 msec, offset 6.4331 msec, dispersion 187.55, jitter 1.39 msec
precision 2**20, version 4

192.168.10.7 configured, ipv4, our_master, sane, valid, stratum 3
ref ID 108.61.73.243  , time D7AD0D8F.AE79A23A (02:57:19.681 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 86.45 msec, root disp 87.82, reach 377, sync dist 134.25
delay 0.89 msec, offset 19.5087 msec, dispersion 1.69, jitter 0.84 msec
precision 2**32, version 4
```

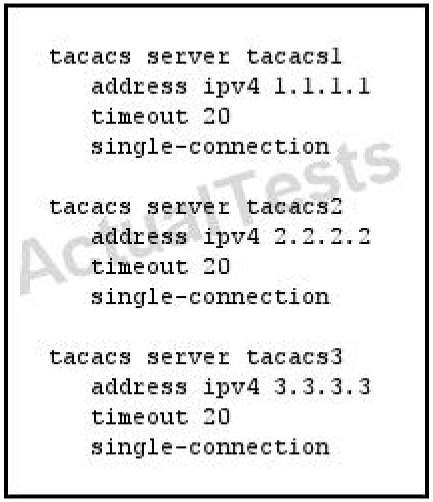
With which NTP server has the router synchronized?

A. 108.61.73.243
B. 192.168.10.7
C. 209.114.111.1
D. 132.163.4.103
E. 204.2.134.164
F. 241.199.164.101

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 7
Refer to the exhibit.



```
tacacs server tacacs1
   address ipv4 1.1.1.1
   timeout 20
   single-connection

tacacs server tacacs2
   address ipv4 2.2.2.2
   timeout 20
   single-connection

tacacs server tacacs3
   address ipv4 3.3.3.3
   timeout 20
   single-connection
```

Which statement about the given configuration is true?

A. The single-connection command causes the device to process one TACACS request and then move to the next server.
B. The timeout command causes the device to move to the next server after 20 seconds of TACACS inactivity.
C. The single-connection command causes the device to establish one connection for all TACACS transactions.
D. The router communicates with the NAS on the default port, TCP 1645.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 8
What is the best way to confirm that AAA authentication is working properly?

A. Use the test aaa command.
B. Ping the NAS to confirm connectivity.
C. Use the Cisco-recommended configuration for AAA authentication.
D. Log into and out of the router, and then check the NAS authentication log.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 9
How does PEAP protect the EAP exchange?

A. It encrypts the exchange using the server certificate.
B. It encrypts the exchange using the client certificate.
C. It validates the server-supplied certificate, and then encrypts the exchange using the client certificate.
D. It validates the client-supplied certificate, and then encrypts the exchange using the server certificate.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 10
What improvement does EAP-FASTv2 provide over EAP-FAST?

A. It supports more secure encryption protocols.
B. It allows multiple credentials to be passed in a single EAP exchange.
C. It allows faster authentication by using fewer packets.
D. It addresses security vulnerabilities found in the original protocol.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 11
How does a device on a network using ISE receive its digital certificate during the new-device registration process?

A. ISE issues a certificate from its internal CA server.
B. ISE acts as a SCEP proxy to enable the device to receive a certificate from a central CA server.
C. ISE issues a pre-defined certificate from a local database
D. The device requests a new certificate directly from a central CA.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 12
When an administrator initiates a device wipe command from the ISE, what is the immediate effect?

A. It immediately erases all data on the device.
B. It requests the administrator to choose between erasing all device data or only managed corporate data.
C. It notifies the device user and proceeds with the erase operation.
D. It requests the administrator to enter the device PIN or password before proceeding with the operation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 13
What configuration allows AnyConnect to automatically establish a VPN session when a user logs in to the computer?

A. proxy
B. always-on
C. transparent mode
D. Trusted Network Detection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

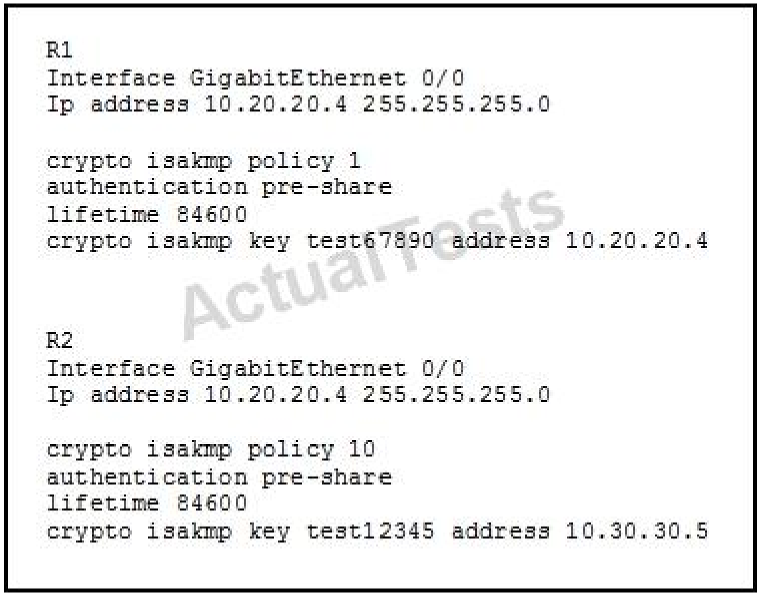
QUESTION 14
What security feature allows a private IP address to access the Internet by translating it to a public address?

A. NAT
B. hairpinning
C. Trusted Network Detection
D. Certification Authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 15
Refer to the exhibit.



```
R1
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 1
authentication pre-share
lifetime 84600
crypto isakmp key test67890 address 10.20.20.4


R2
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 10
authentication pre-share
lifetime 84600
crypto isakmp key test12345 address 10.30.30.5
```

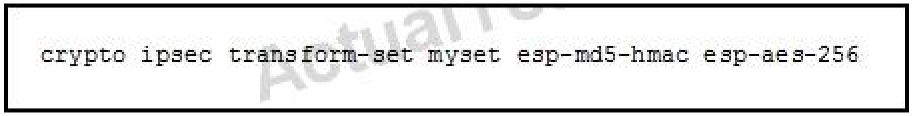
You have configured R1 and R2 as shown, but the routers are unable to establish a site-to-site VPN tunnel. What action can you take to correct the problem?

A. Edit the crypto keys on R1 and R2 to match.
B. Edit the ISAKMP policy sequence numbers on R1 and R2 to match.
C. Set a valid value for the crypto key lifetime on each router.
D. Edit the crypto isakmp key command on each router with the address value of its own interface.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 16
Refer to the exhibit.



```
crypto ipsec transform-set myset esp-md5-hmac esp-aes-256
```

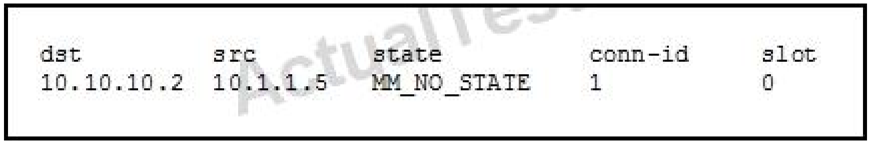
What is the effect of the given command?

A. It configures the network to use a different transform set between peers.
B. It merges authentication and encryption methods to protect traffic that matches an ACL.
C. It configures encryption for MD5 HMAC.
D. it configures authentication as AES 256.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 17
Refer to the exhibit.



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

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

A. IKE Phase 1 main mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.
B. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
C. IKE Phase 1 aggressive mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.
D. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D

QUESTION 18
Which statement about IOS privilege levels is true?

A. Each privilege level supports the commands at its own level and all levels above it.
B. Each privilege level supports the commands at its own level and all levels below it.

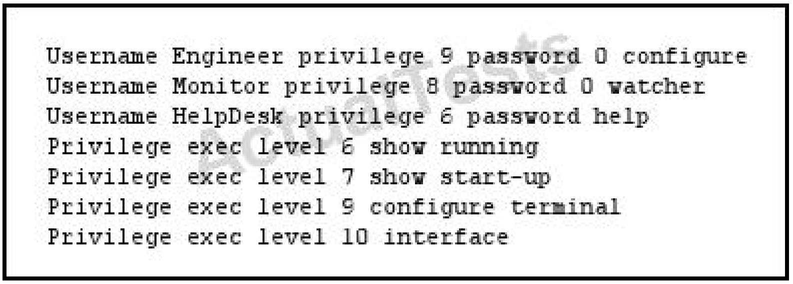
C. Privilege-level commands are set explicitly for each user.

D. Each privilege level is independent of all other privilege levels.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 19
Refer to the exhibit.
Cisco 210-260 Exam



```
Username Engineer privilege 9 password 0 configure
Username Monitor privilege 8 password 0 watcher
Username HelpDesk privilege 6 password help
Privilege exec level 6 show running
Privilege exec level 7 show start-up
Privilege exec level 9 configure terminal
Privilege exec level 10 interface
```

"
Which line in this configuration prevents the HelpDesk user from modifying the interface configuration?

A. Privilege exec level 9 configure terminal

B. Privilege exec level 10 interface

C. Username HelpDesk privilege 6 password help

D. Privilege exec level 7 show start-up

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 20
In the router ospf 200 command, what does the value 200 stand for?

A. area ID

B. administrative distance value
C. process ID
D. ABR ID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 21
Which feature filters CoPP packets?

A. class maps
B. policy maps
C. access control lists
D. route maps

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 22
In which type of attack does the attacker attempt to overload the CAM table on a switch so that the switch acts as a hub?

A. MAC spoofing
B. gratuitous ARP
C. MAC flooding
D. DoS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Answer: C

QUESTION 23
Which type of PVLAN port allows hosts in the same VLAN to communicate directly with each other?

A. community for hosts in the PVLAN
B. promiscuous for hosts in the PVLAN
C. isolated for hosts in the PVLAN
D. span for hosts in the PVLAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 24
What is a potential drawback to leaving VLAN 1 as the native VLAN?

A. Gratuitous ARPs might be able to conduct a man-in-the-middle attack.
B. The CAM might be overloaded, effectively turning the switch into a hub.
C. It may be susceptible to a VLAN hoping attack.
D. VLAN 1 might be vulnerable to IP address spoofing.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 25
In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three).

A. when matching NAT entries are configured
B. when matching ACL entries are configured
C. when the firewall receives a SYN-ACK packet

D. when the firewall receives a SYN packet
E. when the firewall requires HTTP inspection
F. when the firewall requires strict HTTP inspection

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Answer: A,B,D

QUESTION 26
Which firewall configuration must you perform to allow traffic to flow in both directions between two zones?

A. You must configure two zone pairs, one for each direction.
B. You can configure a single zone pair that allows bidirectional traffic flows for any zone.
C. You can configure a single zone pair that allows bidirectional traffic flows for any zone except the self zone.
D. You can configure a single zone pair that allows bidirectional traffic flows only if the source zone is the less secure zone.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 27
What is a valid implicit permit rule for traffic that is traversing the ASA firewall?

A. Unicast IPv4 traffic from a higher security interface to a lower security interface is permitted in routed mode only.
B. Unicast IPv6 traffic from a higher security interface to a lower security interface is permitted in transparent mode only.
C. Only BPDUs from a higher security interface to a lower security interface are permitted in transparent mode.
D. ARPs in both directions are permitted in transparent mode only.
E. Only BPDUs from a higher security interface to a lower security interface are permitted in routed

mode.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which statement about the communication between interfaces on the same security level is true?

A. Configuring interfaces on the same security level can cause asymmetric routing.
B. Interfaces on the same security level require additional configuration to permit inter-interface communication.
C. All traffic is allowed by default between interfaces on the same security level.
D. You can configure only one interface on an individual security level.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B

QUESTION 29
Which IPS mode provides the maximum number of actions?

A. bypass
B. failover
C. span
D. promiscuous
E. inline

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
E

QUESTION 30
How can you detect a false negative on an IPS?

A. View the alert on the IPS.
B. Review the IPS log.
C. Review the IPS console.
D. Use a third-party system to perform penetration testing.
E. Use a third-party to audit the next-generation firewall rules.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: D

QUESTION 31
What is the primary purpose of a defined rule in an IPS?

A. to configure an event action that takes place when a signature is triggered
B. to define a set of actions that occur when a specific user logs in to the system
C. to configure an event action that is pre-defined by the system administrator
D. to detect internal attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: A

QUESTION 32
Which Sourcefire event action should you choose if you want to block only malicious traffic from a particular end user?

A. Allow without inspection
B. Block
C. Allow with inspection

D. Trust
E. Monitor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
C

QUESTION 33
How can FirePOWER block malicious email attachments?

A. It forwards email requests to an external signature engine
B. It scans inbound email messages for known bad URLs.
C. It sends the traffic through a file policy.
D. It sends an alert to the administrator to verify suspicious email messages.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: C

QUESTION 34
You have been tasked with blocking user access to websites that violate company policy, but the sites use dynamic IP addresses. What is the best practice for URL filtering to solve the problem?

A. Enable URL filtering and use URL categorization to block the websites that violate company policy.
B. Enable URL filtering and create a blacklist to block the websites that violate company policy.
C. Enable URL filtering and create a whitelist to block the websites that violate company policy.
D. Enable URL filtering and use URL categorization to allow only the websites that company policy allows users to access.
E. Enable URL filtering and create a whitelist to allow only the websites that company policy allows users to access.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

Answer: A

QUESTION 35
What is a benefit of a web application firewall?

A. It blocks known vulnerabilities without patching applications.
B. It simplifies troubleshooting.
C. It accelerates web traffic.
D. It supports all networking protocols.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Answer: A

QUESTION 36
Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attacks?

A. signature-based IPS
B. graymail management and filtering
C. contextual analysis
D. holistic understanding of threats

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which NAT type allows only objects or groups to reference an IP address?

A. dynamic NAT

B. dynamic PAT
C. static NAT
D. identity NAT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: B

QUESTION 38
Which feature allows a dynamic PAT pool to select the next address in the PAT pool instead of the next port of an existing address?

A. next IP
B. round robin
C. dynamic rotation
D. NAT address rotation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: B

QUESTION 39
Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What are two possible types of attacks your team discovered? (Choose two.)

A. social activism
B. E Polymorphic Virus
C. advanced persistent threat
D. drive-by spyware
E. targeted malware

Correct Answer: CE
Section: (none)

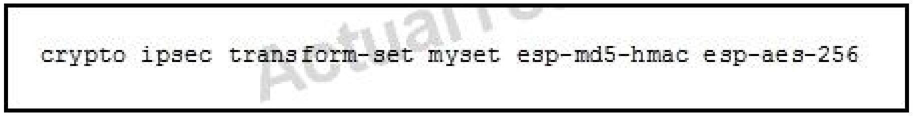
Explanation

Explanation/Reference:

Answer: C,E

QUESTION 40

Refer to the exhibit.



```
crypto ipsec transform-set myset esp-md5-hmac esp-aes-256
```

What are two effects of the given command? (Choose two.)

A. It configures authentication to use AES 256.
B. It configures authentication to use MD5 HMAC
C. It configures authorization use AES 256.
D. It configures encryption to use MD5 HMAC.
E. It configures encryption to use AES 256.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

Answer: B,E

QUESTION 41

In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three).

A. when a matching TCP connection is found
B. when the firewall requires strict HTTP inspection
C. when the firewall receives a FIN packet
D. when matching ACL entries are configured
E. when the firewall requires HTTP inspection
F. when matching NAT entries are configured

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

Answer: A,D,E

Explanation:

QUESTION 42

If a switch port goes directly into a blocked state only when a superior BPDU is received, what mechanism must be in use?

A. STP BPDU guard

B. loop guard

C. STP Root guard

D. EtherChannel guard

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Answer: A