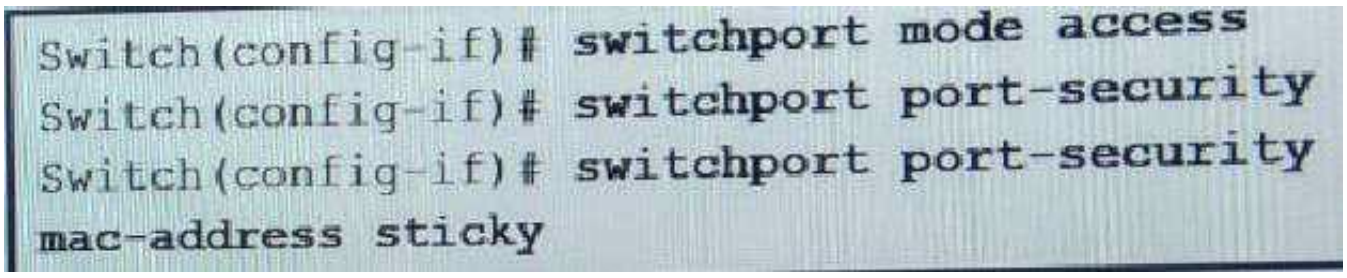
# Exam Questions 300-206

Implementing Cisco Edge Network Security Solutions

**https://www.2passeasy.com/dumps/300-206/**

**NEW QUESTION 1**
Refer to the exhibit.




Which two are true statements about the expected port security behavior? (Choose two)

A. If a violation occurs, the swith port waits one minute to recover by default.
B. Only one MAC address can be learnded by default on the switch port.
C. Up to five MAC addresses can be learned by default on the switch port.
D. If a violation occurs, the switch port remains active, but the traffic is dropped.
E. If a violation occurs, the swithc port shuts down.

**Answer:** BE

**NEW QUESTION 2**
An engineer is applying best practices to stop STP unauthorized changes from the uses port. Which two actions help accomplish this task? (Choose two)

A. Enable STP Guard
B. Configure RSTP
C. Disable STP
D. Enable BPDU Guard
E. Enable Root Guard

**Answer:** DE

**NEW QUESTION 3**
HTTPS server is configured on a router for management. Which command will change the router's listening port from 433 to 444?

A. ip https secure-port 444
B. ip http secure-server 444
C. ip http server secure-port 444
D. ip http secure-port 444

**Answer:** D

**NEW QUESTION 4**
Which two statements about the utilization of IPv4 and IPv6 addresses in the Cisco ASA 9.x firewall access list configuration are true? (Choose two.)

A. Mixed IPv4 and IPv6 addresses cannot be used in the same access list entry
B. Mixed IPv4 and IPv6 addresses can be used in the same access list entry
C. Mixed IPv4 and IPv6 addresses can be used in the same access list for network object group
D. Mixed IPv4 and IPv6 addresses cannot be used in the same access list
E. Mixed IPv4 and IPv6 addresses cannot be used in the same access list for network object group

**Answer:** BC

**Explanation:** Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ acl_extended.pdf

**NEW QUESTION 5**
A user is having trouble connecting to websites on the Internet. The network engineer proposes configuring a packet capture that captures only the HTTP response traffic on the Cisco Adaptive Security Appliance between the user's workstation and Internet. If the user's workstation IP address is 10.0.0.101, which ACE is needed to achieve this capture?

A. access-list capture permit tcp host 10.0.0.101 eq 80 any
B. access-list capture permit tcp host 10.0.0.101 any eq 80
C. access-list capture permit tcp any eq 80 host 10.0.0.101
D. access-list capture permit tcp any host 10.0.0.101 eq 80

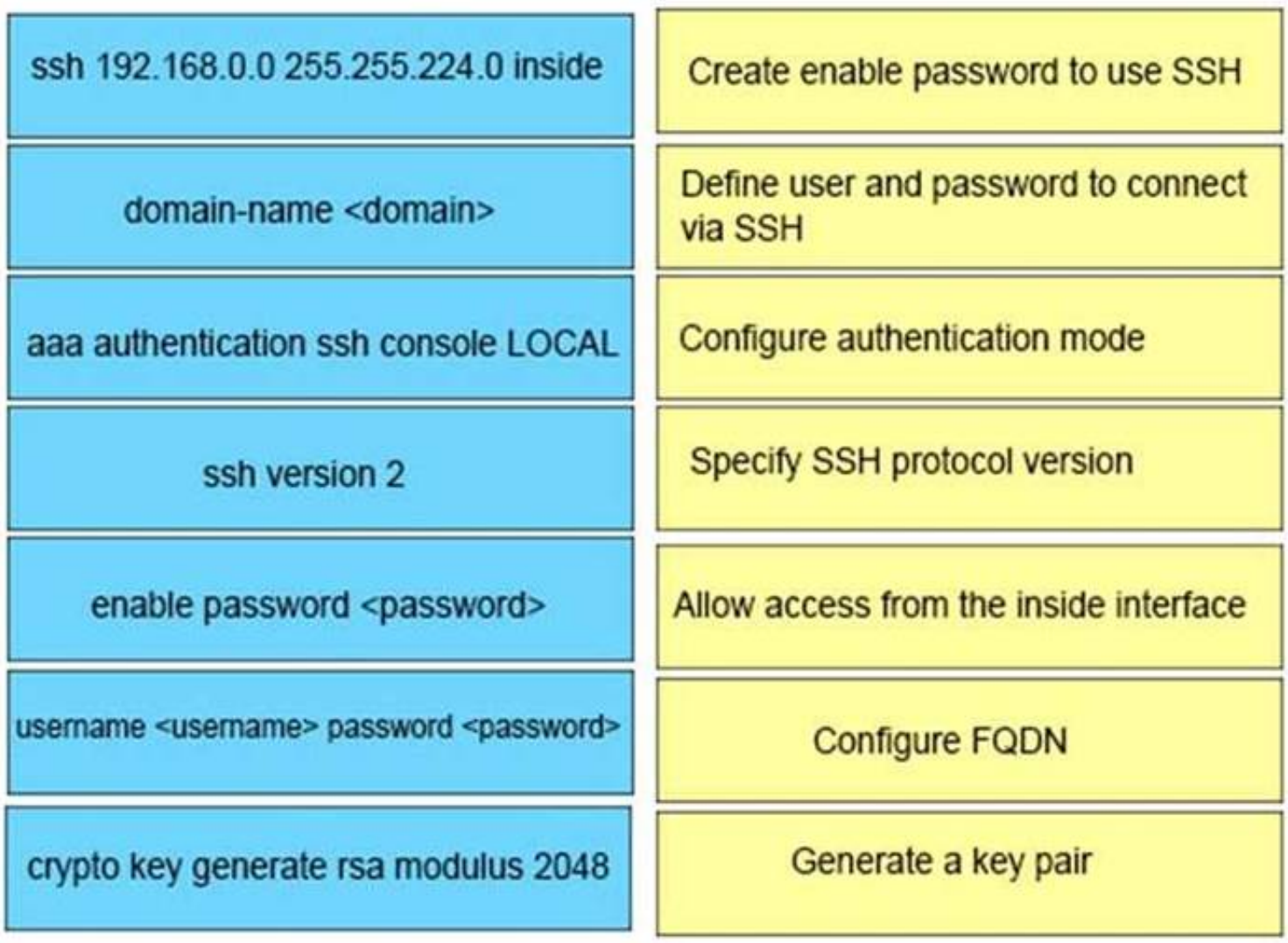
**Answer:** D

**NEW QUESTION 6**
Which two mandatory policies are needed to support a regular IPsec VPN in a Cisco Security Manager environment? (Choose two.)

A. GRE modes
B. IKE proposal
C. group encryption
D. server load balance

**Answer:** BC

**NEW QUESTION 7**
DRAG DROP
An engineer must create an SSHv2 configuration for a remote user with a key size of 2048 on the inside network of 192.168.0.0/19 with a fully qualified domain name. Drag and drop the Cisco ASA commands on the left onto the matching function on the right.




**Answer:**

**Explanation:**

**NEW QUESTION 8**
An engineer has downloaded the database files for botnet traffic filtering on an AS

A. Where are these database files stored?
B. flash memory
C. SSD drive
D. ROMMON
E. running memory

**Answer:** A

**NEW QUESTION 9**
Which benefit of using centralized management to manage a Cisco IronPort ESA is true?

A. It reduces licensing cost
B. It requires no initial setup
C. It requires a light client on managed devices
D. It reduces administration time

**Answer:** D

**NEW QUESTION 10**
Which action can be taken as a preventive measure against VLAN hopping attacks?

A. Configure an uplink to another switch as access port
B. Set an unused VLAN as native VLAN on a trunk port
C. Limit number of MAC addresses on a trunk port
D. Configure port security on all switch ports

**Answer:** B

**NEW QUESTION 10**
DRAG DROP
Drag and drop the function on the left onto the matching packet capture configuration types on th right. Not all options are used.

| | |
|---|---|
| captures inbound and outbound packets on one or more interfaces | asa_dataplane |
| captures traffic between an IPS module and the Cisco ASA | asp-drop |
| captures packets with Layer 2 to inline SGT | ethernet-type |
| captures 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, or VLAN traffic | |
| captures packets dropped for a particular reason | |

**Answer:**

**Explanation:** Reference:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118097-configure-asa-00.html

**NEW QUESTION 15**
A hacker is sniffing network traffic from a Cisco Catalyst switch on a company network. Which three pieces of information can be obtained from intercepted Cisco Discovery Protocol traffic? (Choose three.)

A. routing protocol
B. encapsulation type
C. bridge ID
D. hardware platform
E. VTP domain
F. interface MAC address

**Answer:** DEF

**NEW QUESTION 16**

An engineer is using Cisco Security Manager and is using default ports configuration. What port must be open to connect the Cisco Security Manager Client to an ASA?

A. 22
B. 23
C. 80
D. 443

**Answer:** D

**NEW QUESTION 19**
Which command must be used to implement the unicast RPF feature on a Cisco ASA device?

A. ip verify source port-security
B. ip source-route
C. ip verify unicast reverse-path
D. ip verify reverse-path interface <interface name>

**Answer:** D

**NEW QUESTION 23**
Refer to the exhibit.

```
access-list 20 permit tcp any host: 172.16.32.20 eq 80
!
capture http_capture access-list 20 interface dmz headers-only
```

A network engineer applies the configuration shown to set up a capture on a Cisco Adaptive Security Appliance. When attempting to start a capture, this error message is observed:
ERROR: Capture doesn't support access-list <20> containing mixed policies For which two reasons does this error message occur? (Choose two.)

A. The ACL number is incorrect.
B. Access list type is incorrect.
C. IPv6 is enabled on the Cisco ASA.
D. A named ACL is required.
E. IPv6 is not specified on the access list with "any4" keyword.

**Answer:** DE

**NEW QUESTION 28**
An enterprise is hosting an application that opens a secondary UDP point. The initial session on a well-known port is used to negotiate the secondary dynamically assigned port. Which feature on Cisco ASA monitors sessions to identify the dynamic port assignments and permits sata exchange on these ports?

A. Allow Any
B. NAT
C. Protocol Inspection
D. High & Low Security level

**Answer:** C

**NEW QUESTION 32**
An engineer must secure a current monitoring environment by using the strongest encryption allowed within SNMPv3 configuration. Which two encryption methods meet this requirement? (Choose two.)

A. 3DES
B. AES
C. RSA-SIG
D. DES
E. MD5

**Answer:** AB

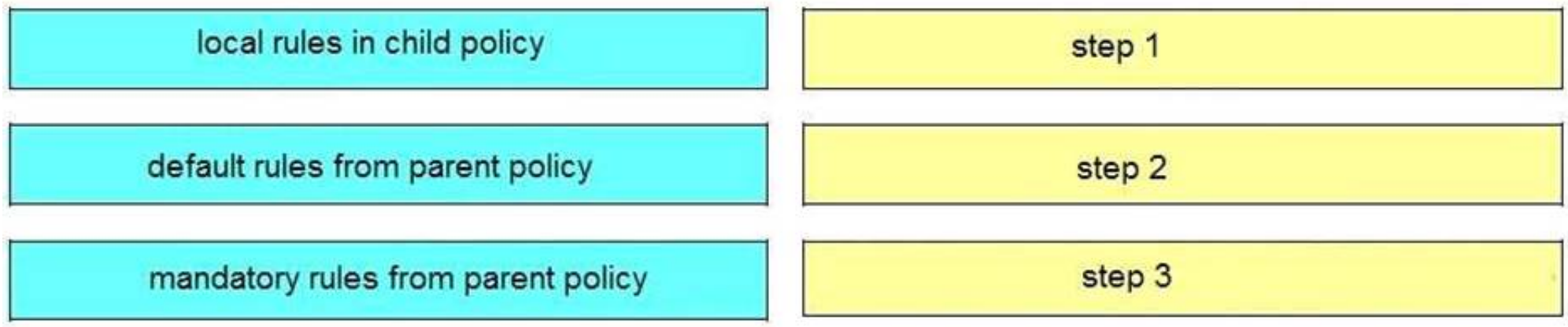
**NEW QUESTION 37**
Which type of traffic would make use of the ASA's default route while running in transparent mode?

A. untrusted traffic
B. NAT traffic
C. encrypted traffic
D. management traffic
E. Internet traffic

**Answer:** D

**Explanation:** Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/intro-fw.pdf

**NEW QUESTION 38**
DRAG DROP
Drag and drop the steps on the left into the correct order of Cisco Security Manager rules when using inheritance on the right.




**Answer:**

**Explanation:**


**NEW QUESTION 40**
An engineer is applying best practices to step STP unauthorized changes from the user port. Which two actions help to accomplish this task? (Choose two.)

A. configure RSTP.
B. enable STP Guard.
C. disable STP
D. enable BPDU Guard.
E. enable Root Guard.

**Answer:** DE

**NEW QUESTION 41**
An enterprise has enforced DHCP snooping on the enterprise switches. In which two cases does the switch drop a DHCP packet? (Choose two.)

A. A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address match.
B. A DHCP relay agent forwards a DHCP packet that includes a 0.0.0.0 relay-agent IP address.
C. The switch receives a DHCPRELEASE broadcast message that has a MAC address in the DHCP snooping binding database, and the interface information in the binding database matches the interface on which the message was received.
D. A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
E. A packet from a DHCP server, such as a DHCPOFFER or DHCPLEASEQUERY packet, is received from outside the network or firewall.

**Answer:** DE

**NEW QUESTION 43**
Which statement describes a unique feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

A. Multiple NetFlow collectors and NetFlow exporters are supported.
B. Secure NetFlow connections are optimized for Cisco Prime Infrastructure.
C. Flow-create events are delayed, which reduce overall traffic.
D. Advanced NetFlow v9 templates and legacy v5 formatting are supported.

**Answer:** C

**NEW QUESTION 47**
An engineer is configuring Cisco ASA 1000V Cloud Firewall. Which element allows for application of a security policy based on a class of VMs instead of based on IP addresses?

A. port profiles
B. port groups
C. security groups
D. security profiles

**Answer:** A

**NEW QUESTION 51**
Which characteristic of community ports in a PVLAN is true?

A. can communicate with isolated ports
B. cannot communicate with other community ports in the same community.
C. can communicate with promiscuous ports
D. are separated at Layer 3 from all other ports

**Answer:** C

**NEW QUESTION 55**
Which option is a Cisco best practice when configuring traffic storm control?

A. Configure 100 percent level to suppress all traffic.
B. Configure on the port channel interface of an EtherChannel.
C. Configure traffic storm control on ports that are members of an EtherChannel.
D. Configure additional capacity as port speed increase.

**Answer:** B

**NEW QUESTION 57**
What are three features of the Cisco ASA 1000V? (Choose three.)

A. cloning the Cisco ASA 1000V
B. dynamic routing
C. the Cisco VNMC policy agent
D. IPv6
E. active/standby failover
F. QoS

**Answer:** ACE

**NEW QUESTION 61**
If the Cisco ASA 1000V has too few licenses, what is its behavior?

A. It drops all traffic.
B. It drops all outside-to-inside packets.
C. It drops all inside-to-outside packets.
D. It passes the first outside-to-inside packet and drops all remaining packets.

**Answer:** D

**NEW QUESTION 64**
Which two web browsers are supported for the Cisco ISE GUI? (Choose two.)

A. HTTPS-enabled Mozilla Firefox version 3.x
B. Netscape Navigator version 9
C. Microsoft Internet Explorer version 8 in Internet Explorer 8-only mode
D. Microsoft Internet Explorer version 8 in all Internet Explorer modes
E. Google Chrome (all versions)

**Answer:** AC

**NEW QUESTION 69**
With Cisco ASA active/standby failover, by default, how many monitored interface failures will cause failover to occur?

A. 1
B. 2
C. 3
D. 4
E. 5

**Answer:** A

**NEW QUESTION 71**
Which statement about SNMP support on the Cisco ASA appliance is true?

A. The Cisco ASA appliance supports only SNMPv1 or SNMPv2c.
B. The Cisco ASA appliance supports read-only and read-write access.
C. The Cisco ASA appliance supports three built-in SNMPv3 groups in Cisco ASDM: Authentication and Encryption, Authentication Only, and No Authentication, No Encryption.
D. The Cisco ASA appliance can send SNMP traps to the network management station only using SNMPv2.

**Answer:** C

**NEW QUESTION 73**
Which statement about Cisco ASA multicast routing support is true?

A. The Cisco ASA appliance supports PIM dense mode, sparse mode, and BIDIR-PIM.
B. The Cisco ASA appliance supports only stub multicast routing by forwarding IGMP messages from multicastreceivers to the upstream multicast router.
C. The Cisco ASA appliance supports DVMRP and PIM.
D. The Cisco ASA appliance supports either stub multicast routing or PIM, but both cannot be enabled at thesame time.
E. The Cisco ASA appliance supports only IGMP v1.

**Answer:** D

**NEW QUESTION 75**
What is the default log level on the Cisco Web Security Appliance?

A. Trace
B. Debug
C. Informational
D. Critical

**Answer:** C

**NEW QUESTION 80**
Which two SNMPv3 features ensure that SNMP packets have been sent securely?" Choose two.

A. host authorization
B. authentication
C. encryption
D. compression

**Answer:** BC

**NEW QUESTION 84**
You are configuring a Cisco IOS Firewall on a WAN router that is operating as a Trusted Relay Point
(TRP) in a voice network. Which feature must you configure to open data- channel pinholes for voice packets that are sourced from a TRP within the WAN?

A. CAC
B. ACL
C. CBAC
D. STUN

**Answer:** D

**NEW QUESTION 88**
If you encounter problems logging in to the Cisco Security Manager 4.4 web server or client or
backing up its databases, which account has most likely been improperly modified?

A. admin (the default administrator account)
B. casuser (the default service account)
C. guest (the default guest account)
D. user (the default user account)

**Answer:** B

**NEW QUESTION 92**
Which of the following would need to be created to configure an application-layer inspection of
SMTP traffic operating on port 2525?

A. A class-map that matches port 2525 and applying an inspect ESMTP policy-map for that class in the globalinspection policy
B. A policy-map that matches port 2525 and applying an inspect ESMTP class-map for that policy
C. An access-list that matches on TCP port 2525 traffic and applying it on an interface with the inspect option
D. A class-map that matches port 2525 and applying it on an access-list using the inspect option

**Answer:** A

**NEW QUESTION 94**
Which statement about the Cisco ASA botnet traffic filter is true?

A. The four threat levels are low, moderate, high, and very high.
B. By default, the dynamic-filter drop blacklist interface outside command drops traffic with a threat level of high or very high.
C. Static blacklist entries always have a very high threat level.
D. A static or dynamic blacklist entry always takes precedence over the static whitelist entry.

**Answer:** C

**NEW QUESTION 97**
Which Cisco ASA object group type offers the most flexibility for grouping different services together based on arbitrary protocols?

A. network
B. ICMP
C. protocol
D. TCP-UDP
E. service

**Answer:** E

**NEW QUESTION 100**
A Cisco ASA requires an additional feature license to enable which feature?

A. transparent firewall
B. cut-thru proxy
C. threat detection
D. botnet traffic filtering
E. TCP normalizer

**Answer:** D

**NEW QUESTION 103**
Which two parameters must be configured before you enable SCP on a router? (Choose two.)

A. SSH
B. authorization
C. ACLs
D. NTP
E. TACACS+

**Answer:** AB

**NEW QUESTION 105**
Which set of commands enables logging and displays the log buffer on a Cisco ASA?

A. enable loggingshow logging
B. logging enableshow logging
C. enable logging int e0/1view logging
D. logging enablelogging view config

**Answer:** B

**NEW QUESTION 110**
The Cisco ASA must support dynamic routing and terminating VPN traffic. Which three Cisco ASA options will not support these requirements? (Choose three.)

A. transparent mode
B. multiple context mode
C. active/standby failover mode
D. active/active failover mode
E. routed mode
F. no NAT-control

**Answer:** ABD

**NEW QUESTION 112**
Which command displays syslog messages on the Cisco ASA console as they occur?

A. Console logging <level>
B. Logging console <level>
C. Logging trap <level>
D. Terminal monitor
E. Logging monitor <level>

**Answer:** B

**NEW QUESTION 116**
Which three configurations are needed to enable SNMPv3 support on the Cisco ASA? (Choose three.)

A. SNMPv3 Local EngineID
B. SNMPv3 Remote EngineID
C. SNMP Users
D. SNMP Groups
E. SNMP Community Strings
F. SNMP Hosts

**Answer:** CDF

**NEW QUESTION 117**
All 30 users on a single floor of a building are complaining about network slowness. After investigating the access switch, the network administrator notices that the MAC address table is full (10,000 entries) and all traffic is being flooded out of every port. Which action can the administrator take to prevent this from occurring?

A. Configure port-security to limit the number of mac-addresses allowed on each port
B. Upgrade the switch to one that can handle 20,000 entries
C. Configure private-vlans to prevent hosts from communicating with one another
D. Enable storm-control to limit the traffic rate
E. Configure a VACL to block all IP traffic except traffic to and from that subnet

**Answer:** A

**NEW QUESTION 118**
A network printer has a DHCP server service that cannot be disabled. How can a layer 2 switch be configured to prevent the printer from causing network issues?

A. Remove the ip helper-address
B. Configure a Port-ACL to block outbound TCP port 68
C. Configure DHCP snooping
D. Configure port-security

**Answer:** C

**NEW QUESTION 119**
A switch is being configured at a new location that uses statically assigned IP addresses. Which will ensure that ARP inspection works as expected?

A. Configure the 'no-dhcp' keyword at the end of the ip arp inspection command
B. Enable static arp inspection using the command 'ip arp inspection static vlan vlan- number
C. Configure an arp access-list and apply it to the ip arp inspection command
D. Enable port security

**Answer:** C

**NEW QUESTION 121**
Which two voice protocols can the Cisco ASA inspect? (Choose two.)

A. MGCP
B. IAX
C. Skype
D. CTIQBE

**Answer:** AD

**NEW QUESTION 122**
Enabling what security mechanism can prevent an attacker from gaining network topology information from CDP?

A. MACsec
B. Flex VPN
C. Control Plane Protection
D. Dynamic Arp Inspection

**Answer:** A

**NEW QUESTION 123**
Which URL matches the regex statement "http"*/"www.cisco.com/"*[^E]"xe"?

A. https://www.cisco.com/ftp/ios/tftpserver.exe
B. https://cisco.com/ftp/ios/tftpserver.exe
C. http:/www.cisco.com/ftp/ios/tftpserver.Exe
D. https:/www.cisco.com/ftp/ios/tftpserver.EXE

**Answer:** A

**NEW QUESTION 128**
What are three attributes that can be applied to a user account with RBAC? (Choose three.)

A. domain
B. password
C. ACE tag
D. user roles
E. VDC group tag
F. expiry date

**Answer:** BDF

**NEW QUESTION 132**
What is the default behavior of an access list on the Cisco ASA security appliance?

A. It will permit or deny traffic based on the access-list criteria.
B. It will permit or deny all traffic on a specified interface.
C. An access group must be configured before the access list will take effect for traffic control.
D. It will allow all traffic.

**Answer:** C

**NEW QUESTION 135**
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

A. sslconfig
B. sslciphers
C. tlsconifg
D. certconfig

**Answer:** A

**NEW QUESTION 139**
The Cisco Email Security Appliance can be managed with both local and external users of different privilege levels. What three external modes of authentication are supported? (Choose three.)

A. LDAP authentication
B. RADIUS Authentication
C. TACAS
D. SSH host keys
E. Common Access Card Authentication
F. RSA Single use tokens

**Answer:** ABD

**NEW QUESTION 141**
Which statement about the Cisco Security Manager 4.4 NAT Rediscovery feature is true?

A. It provides NAT policies to existing clients that connect from a new switch port.
B. It can update shared policies even when the NAT server is offline.
C. It enables NAT policy discovery as it updates shared polices.
D. It enables NAT policy rediscovery while leaving existing shared polices unchanged.

**Answer:** D

**NEW QUESTION 145**
When you install a Cisco ASA AIP-SSM, which statement about the main Cisco ASDM home page is true?

A. It is replaced by the Cisco AIP-SSM home page.
B. It must reconnect to the NAT policies database.
C. The administrator can manually update the page.
D. It displays a new Intrusion Prevention panel.

**Answer:** D

**NEW QUESTION 148**
Which statement about Cisco IPS Manager Express is true?

A. It provides basic device management for large-scale deployments.
B. It provides a GUI for configuring IPS sensors and security modules.
C. It enables communication with Cisco ASA devices that have no administrative access.
D. It provides greater security than simple ACLs.

**Answer:** B

**NEW QUESTION 151**
Which three options describe how SNMPv3 traps can be securely configured to be sent by IOS? (Choose three.)

A. An SNMPv3 group is defined to configure the read and write views of the group.
B. An SNMPv3 user is assigned to SNMPv3 group and defines the encryption and authentication credentials.
C. An SNMPv3 host is configured to define where the SNMPv3 traps will be sent.
D. An SNMPv3 host is used to configure the encryption and authentication credentials for SNMPv3 traps.

E. An SNMPv3 view is defined to configure the address of where the traps will be sent.
F. An SNMPv3 group is used to configure the OIDs that will be reported.

**Answer:** ABC

**NEW QUESTION 152**
Cisco Security Manager can manage which three products? (Choose three.)

A. Cisco IOS
B. Cisco ASA
C. Cisco IPS
D. Cisco WLC
E. Cisco Web Security Appliance
F. Cisco Email Security Appliance
G. Cisco ASA CX
H. Cisco CRS

**Answer:** ABC

**NEW QUESTION 156**
What are two primary purposes of Layer 2 detection in Cisco IPS networks? (Choose two.)

A. identifying Layer 2 ARP attacks
B. detecting spoofed MAC addresses and tracking 802.1X actions and data communication after a successful client association
C. detecting and preventing MAC address spoofing in switched environments
D. mitigating man-in-the-middle attacks

**Answer:** AD

**NEW QUESTION 161**
Which two statements about Cisco IDS are true? (Choose two.)

A. It is preferred for detection-only deployment.
B. It is used for installations that require strong network-based protection and that include sensor tuning.
C. It is used to boost sensor sensitivity at the expense of false positives.
D. It is used to monitor critical systems and to avoid false positives that block traffic.
E. It is used primarily to inspect egress traffic, to filter outgoing threats.

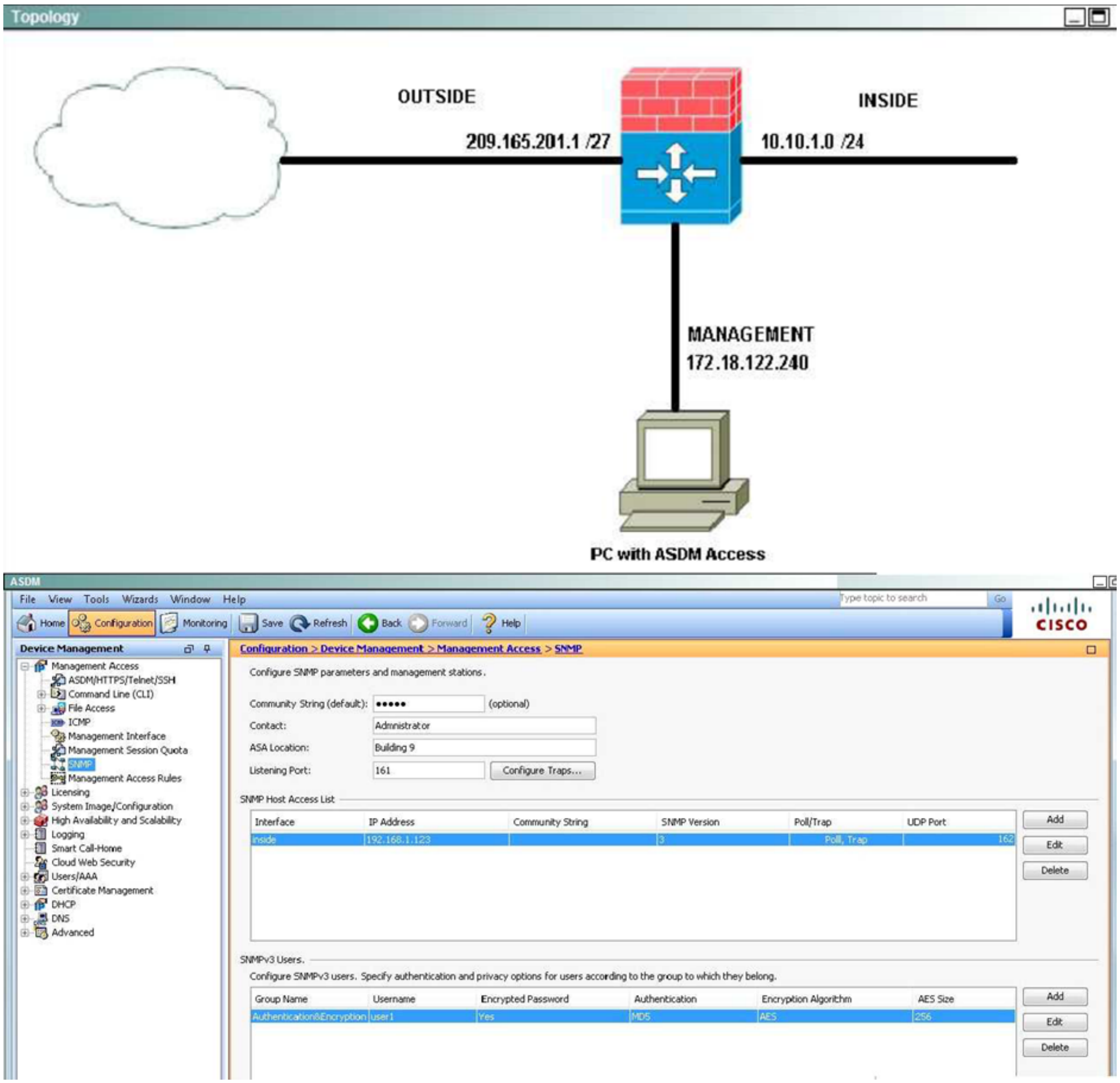
**Answer:** AD

**NEW QUESTION 166**
Which set of commands creates a message list that includes all severity 2 (critical) messages on a Cisco security device?

A. logging list critical_messages level 2console logging critical_messages
B. logging list critical_messages level 2logging console critical_messages
C. logging list critical_messages level 2logging console enable critical_messages
D. logging list enable critical_messages level 2 console logging critical_messages

**Answer:** B

**NEW QUESTION 167**

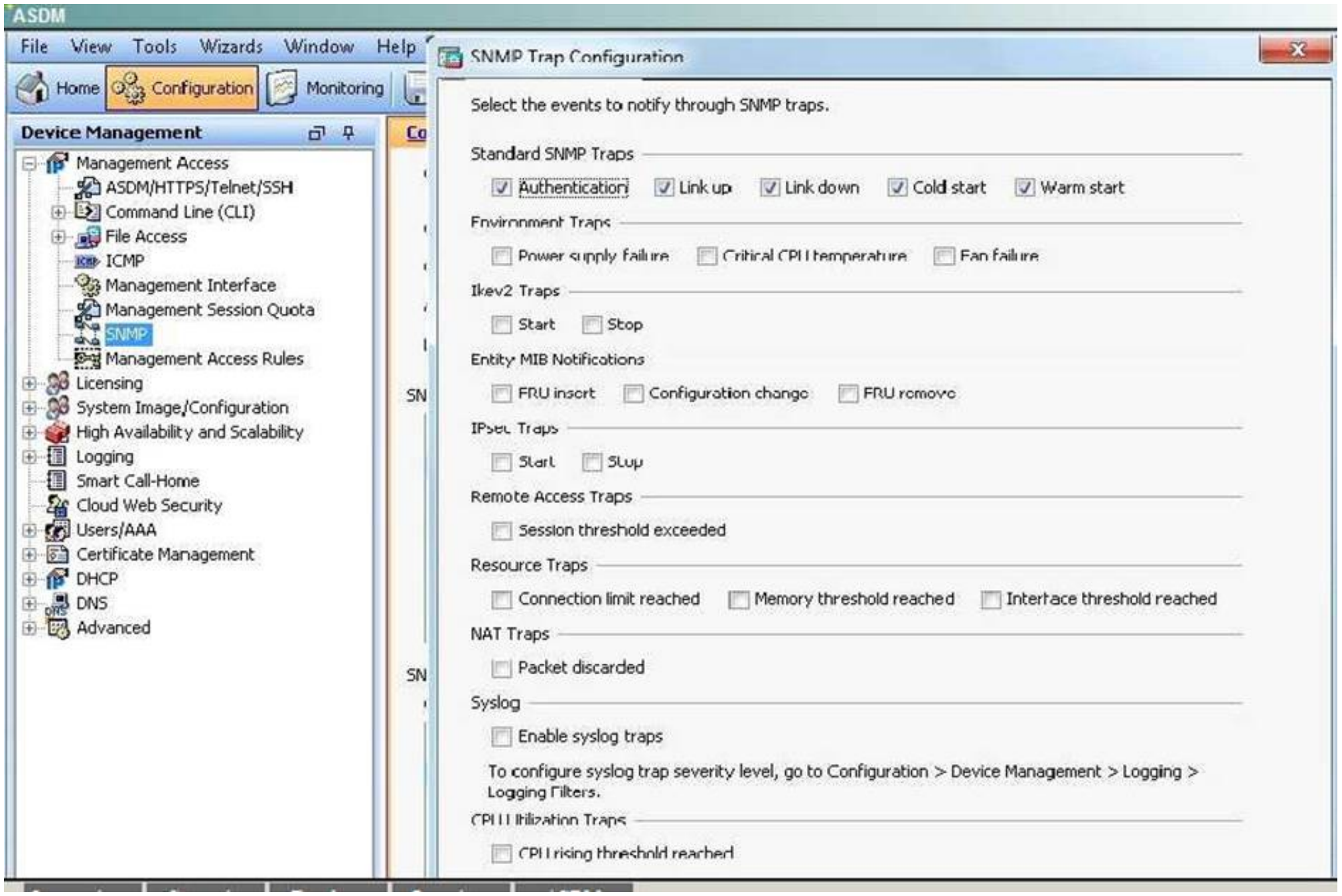



Which statement about how the Cisco ASA supports SNMP is true?

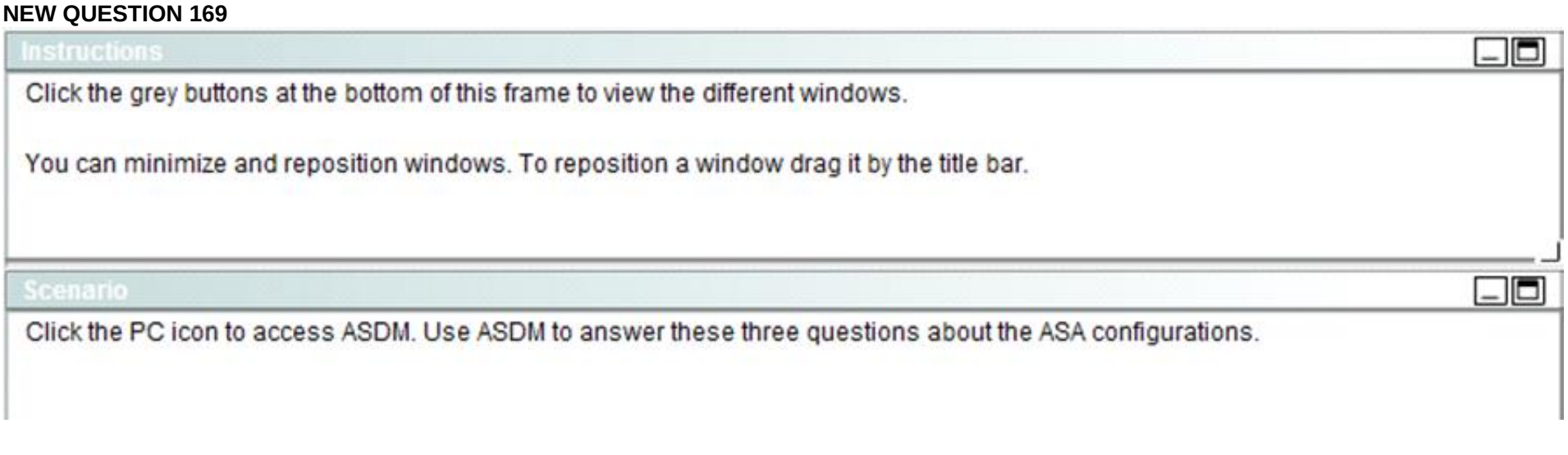
A. All SNMFV3 traffic on the inside interface will be denied by the global ACL
B. The Cisco ASA and ASASM provide support for network monitoring using SNMP Versions 1,2c, and 3, butdo not support the use of all three versions simultaneously.
C. The Cisco ASA and ASASM have an SNMP agent that notifies designated management ,.stations if events occur that are predefined to require a notification, for example, when a link in the network goes up or down.
D. SNMPv3 is enabled by default and SNMP v1 and 2c are disabled by default.
E. SNMPv3 is more secure because it uses SSH as the transport mechanism.

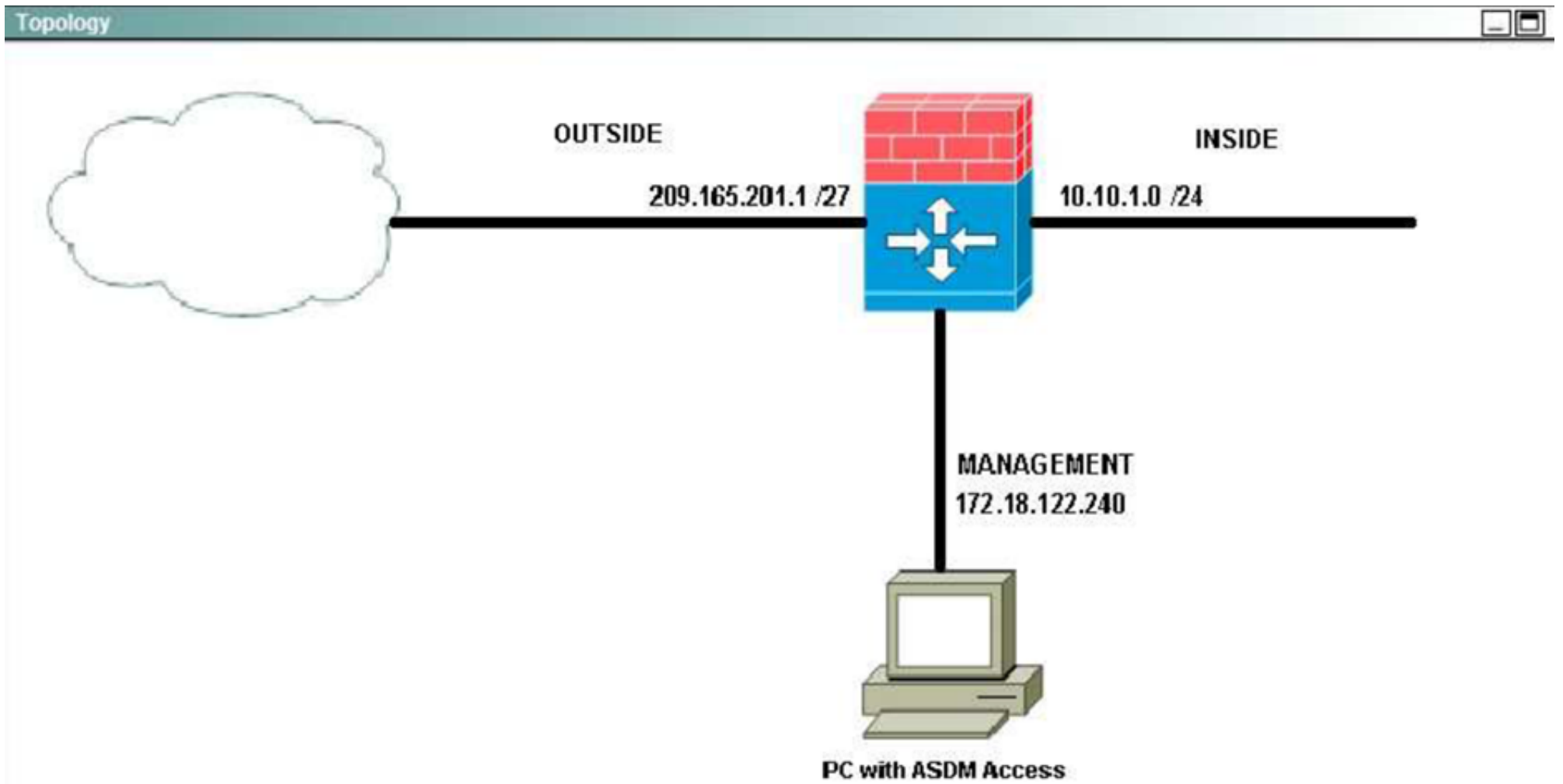
**Answer:** C

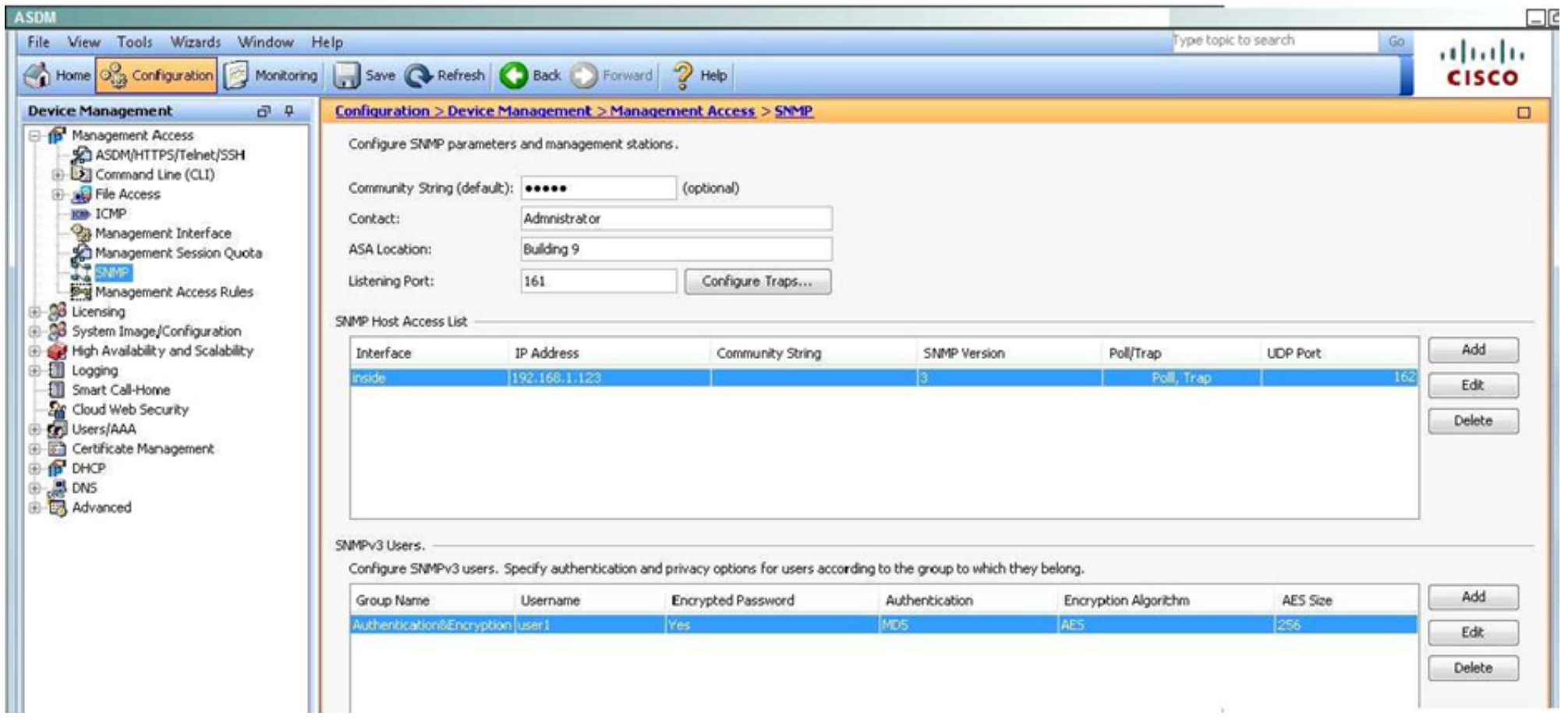
**Explanation:** This can be verified by this ASDM screen shot:




**NEW QUESTION 169**





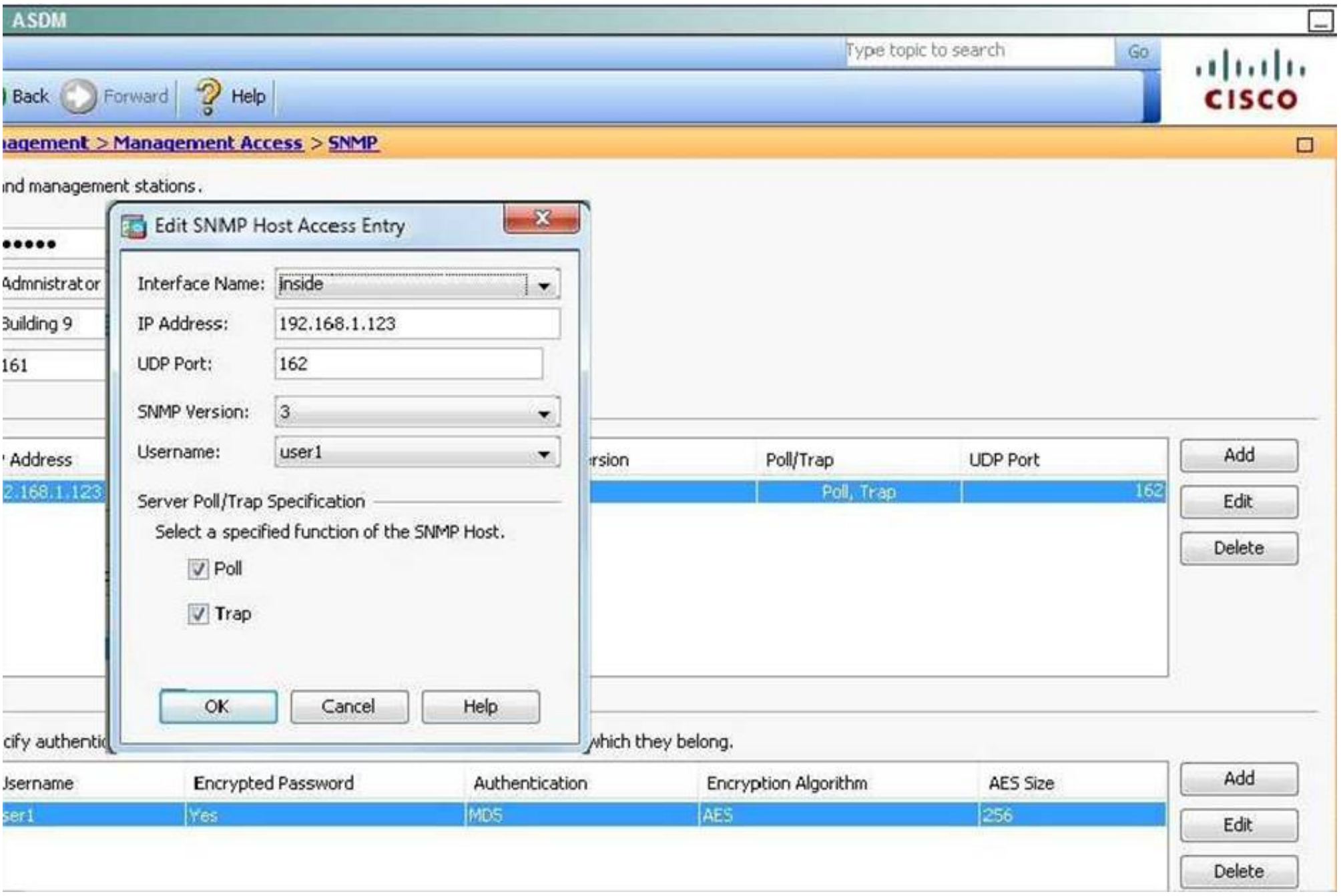




An SNMP host is an IP address to which SNMP notifications and traps are sent. To configure SNMFV3 hosts, which option must you configure in addition to the target IP address?

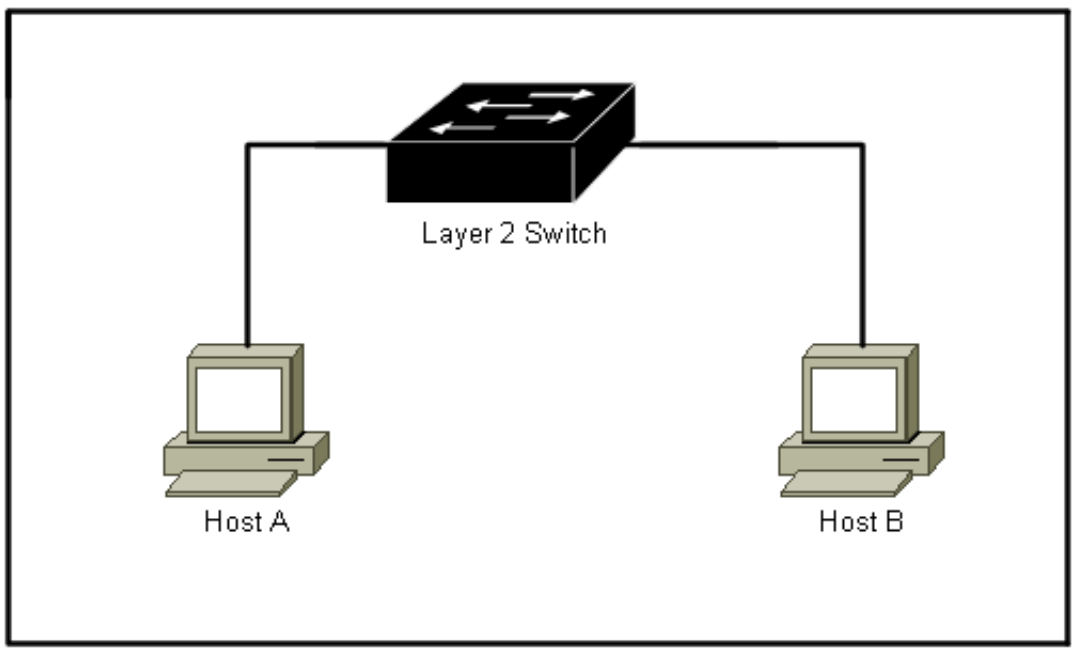
A. the Cisco ASA as a DHCP server, so the SNMFV3 host can obtain an IP address
B. a username, because traps are only sent to a configured user
C. SSH, so the user can connect to the Cisco ASA
D. the Cisco ASA with a dedicated interface only for SNMP, to process the SNMP host traffic.

**Answer:** B

**Explanation:** The username can be seen here on the ASDM simulator screen shot:




**NEW QUESTION 170**
Refer to the exhibit.




To protect Host A and Host B from communicating with each other, which type of PVLAN port should be used for each host?

A. Host A on a promiscuous port and Host B on a community port
B. Host A on a community port and Host B on a promiscuous port
C. Host A on an isolated port and Host B on a promiscuous port
D. Host A on a promiscuous port and Host B on a promiscuous port
E. Host A on an isolated port and host B on an isolated port
F. Host A on a community port and Host B on a community port

**Answer:** E

**NEW QUESTION 173**
Which two features block traffic that is sourced from non-topological IPv6 addresses? (Choose two.)

A. DHCPv6 Guard
B. IPv6 Prefix Guard
C. IPv6 RA Guard
D. IPv6 Source Guard

**Answer:** BD

**NEW QUESTION 176**
An attacker has gained physical access to a password protected router. Which command will prevent access to the startup-config in NVRAM?

A. no service password-recovery
B. no service startup-config
C. service password-encryption
D. no confreg 0x2142

**Answer:** A

**NEW QUESTION 178**
When you set a Cisco IOS Router as an SSH server, which command specifies the RSA public key of the remote peer when you set the SSH server to perform RSA-based authentication?

A. router(config-ssh-pubkey-user)#key
B. router(conf-ssh-pubkey-user)#key-string
C. router(config-ssh-pubkey)#key-string
D. router(conf-ssh-pubkey-user)#key-string enable ssh

**Answer:** B

**NEW QUESTION 182**
Enabling what security mechanism can prevent an attacker from gaining network topology information from CDP via a man-in-the-middle attack?

A. MACsec
B. Flex VPN
C. Control Plane Protection
D. Dynamic Arp Inspection

**Answer:** A

**NEW QUESTION 186**
What is the default behavior of an access list on a Cisco ASA?

A. It will permit or deny traffic based on the access list criteria.
B. It will permit or deny all traffic on a specified interface.
C. It will have no affect until applied to an interface, tunnel-group or other traffic flow.
D. It will allow all traffic.

**Answer:** C

**NEW QUESTION 187**
When configuring a new context on a Cisco ASA device, which command creates a domain for the context?

A. domain config name
B. domain-name
C. changeto/domain name change
D. domain context 2

**Answer:** B

**NEW QUESTION 191**
Which statement describes the correct steps to enable Botnet Traffic Filtering on a Cisco ASA version 9.0 transparent-mode firewall with an active Botnet Traffic Filtering license?

A. Enable DNS snooping, traffic classification, and actions.
B. Botnet Traffic Filtering is not supported in transparent mode.
C. Enable the use of the dynamic database, enable DNS snooping, traffic classification, and actions.
D. Enable the use of dynamic database, enable traffic classification and actions.

**Answer:** C

**NEW QUESTION 194**
Which Cisco switch technology prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast flood on a port?

A. port security
B. storm control
C. dynamic ARP inspection
D. BPDU guard
E. root guard
F. dot1x

**Answer:** B

**NEW QUESTION 199**
You are a security engineer at a large multinational retailer. Your Chief Information Officer recently attended a security conference and has asked you to secure the network infrastructure from VLAN hopping. Which statement describes how VLAN hopping can be avoided?

A. There is no such thing as VLAN hopping because VLANs are completely isolated.
B. VLAN hopping can be avoided by using IEEE 802.1X to dynamically assign the access VLAN to all endpoints and setting the default access VLAN to an unused VLAN ID.
C. VLAN hopping is avoided by configuring the native (untagged) VLAN on both sides of an ISL trunk to an unused VLAN ID.
D. VLAN hopping is avoided by configuring the native (untagged) VLAN on both sides of an IEEE 802.1Q trunk to an unused VLAN ID.

**Answer:** D

**NEW QUESTION 203**
A router is being enabled for SSH command line access.
The following steps have been taken:
- The vty ports have been configured with transport input SSH and login local.
- Local user accounts have been created.
- The enable password has been configured.
What additional step must be taken if users receive a 'connection refused' error when attempting to access the router via SSH?

A. A RSA keypair must be generated on the router
B. An access list permitting SSH inbound must be configured and applied to the vty ports
C. An access list permitting SSH outbound must be configured and applied to the vty ports
D. SSH v2.0 must be enabled on the router

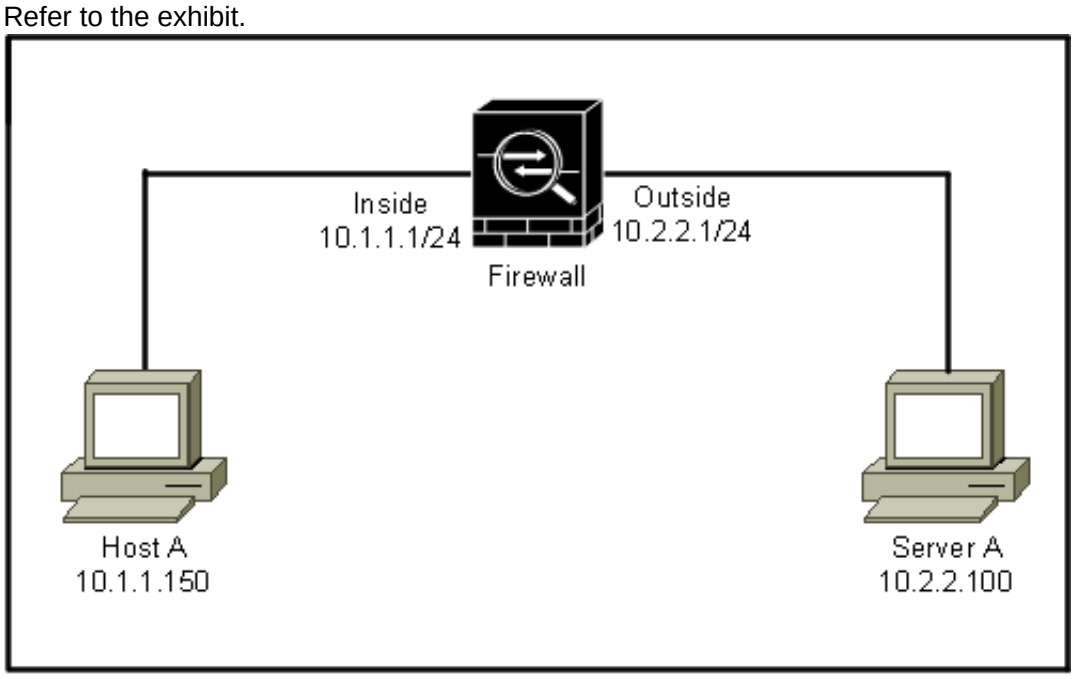
**Answer:** A

**NEW QUESTION 206**
Which three options are default settings for NTP parameters on a Cisco ASA? (Choose three.)

A. NTP authentication is enabled.
B. NTP authentication is disabled.
C. NTP logging is enabled.
D. NTP logging is disabled.
E. NTP traffic is not restricted.
F. NTP traffic is restricted.

**Answer:** BDE

**NEW QUESTION 209**
Refer to the exhibit.




Server A is a busy server that offers these services:
- World Wide Web - DNS
Which command captures http traffic from Host A to Server A?

A. capture traffic match udp host 10.1.1.150 host 10.2.2.100
B. capture traffic match 80 host 10.1.1.150 host 10.2.2.100
C. capture traffic match ip 10.2.2.0 255.255.255.192 host 10.1.1.150
D. capture traffic match tcp host 10.1.1.150 host 10.2.2.100
E. capture traffic match tcp host 10.2.2.100 host 10.1.1.150 eq 80

**Answer:** D

**NEW QUESTION 210**
Your company is replacing a high-availability pair of Cisco ASA 5550 firewalls with the newer Cisco ASA 5555X models. Due to budget constraints, one Cisco ASA 5550 will be replaced at a time.
Which statement about the minimum requirements to set up stateful failover between these two firewalls is true?

A. You must install the USB failover cable between the two Cisco ASAs and provide a 1 Gigabit Ethernetinterface for state exchange.

B. It is not possible to use failover between different Cisco ASA models.
C. You must have at least 1 Gigabit Ethernet interface between the two Cisco ASAs for state exchange.
D. You must use two dedicated interface
E. One link is dedicated to state exchange and the other link is forheartbeats.

**Answer:** B

**NEW QUESTION 211**
When it is configured in accordance to Cisco best practices, the switchport port-security maximum command can mitigate which two types of Layer 2 attacks? (Choose two.)

A. rogue DHCP servers
B. ARP attacks
C. DHCP starvation
D. MAC spoofing
E. CAM attacks
F. IP spoofing

**Answer:** CE

**NEW QUESTION 213**
When configured in accordance to Cisco best practices, the ip verify source command can mitigate which two types of Layer 2 attacks? (Choose two.)

A. rogue DHCP servers
B. ARP attacks
C. DHCP starvation
D. MAC spoofing
E. CAM attacks
F. IP spoofing

**Answer:** DF

**NEW QUESTION 216**
You have installed a web server on a private network. Which type of NAT must you implement to enable access to the web server for public Internet users?

A. static NAT
B. dynamic NAT
C. network object NAT
D. twice NAT

**Answer:** A

**NEW QUESTION 217**
When you configure a Botnet Traffic Filter on a Cisco firewall, what are two optional tasks? (Choose two.)

A. Enable the use of dynamic databases.
B. Add static entries to the database.
C. Enable DNS snooping.
D. Enable traffic classification and actions.
E. Block traffic manually based on its syslog information.

**Answer:** BE

**NEW QUESTION 222**
When you configure a Cisco firewall in multiple context mode, where do you allocate interfaces?

A. in the system execution space
B. in the admin context
C. in a user-defined context
D. in the global configuration

**Answer:** A

**NEW QUESTION 226**
What are two security features at the access port level that can help mitigate Layer 2 attacks? (Choose two.)

A. DHCP snooping
B. IP Source Guard
C. Telnet
D. Secure Shell
E. SNMP

**Answer:** AB

**NEW QUESTION 229**
At which layer does MACsec provide encryption?

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

**Answer:** B

**NEW QUESTION 233**
What are two enhancements of SSHv2 over SSHv1? (Choose two.)

A. VRF-aware SSH support
B. DH group exchange support
C. RSA support
D. keyboard-interactive authentication
E. SHA support

**Answer:** AB

**NEW QUESTION 234**
What is the result of the default ip ssh server authenticate user command?

A. It enables the public key, keyboard, and password authentication methods.
B. It enables the public key authentication method only.
C. It enables the keyboard authentication method only.
D. It enables the password authentication method only.

**Answer:** A

**NEW QUESTION 238**
What are two high-level task areas in a Cisco Prime Infrastructure life-cycle workflow? (Choose two.)

A. Design
B. Operate
C. Maintain
D. Log
E. Evaluate

**Answer:** AB

**NEW QUESTION 240**
What are three ways to add devices in Cisco Prime Infrastructure? (Choose three.)

A. Use an automated process.
B. Import devices from a CSV file.
C. Add devices manually.
D. Use RADIUS.
E. Use the Access Control Server.
F. Use Cisco Security Manager.

**Answer:** ABC

**NEW QUESTION 244**
Which function in the Cisco ADSM ACL Manager pane allows an administrator to search for a specfic element?

A. Find
B. Device Management
C. Search
D. Device Setup

**Answer:** A

**NEW QUESTION 248**
Which two router commands enable NetFlow on an interface? (Choose two.)

A. ip flow ingress
B. ip flow egress
C. ip route-cache flow infer-fields
D. ip flow ingress infer-fields
E. ip flow-export version 9

**Answer:** AB

**NEW QUESTION 252**
Refer to the exhibit.

```
router# show snmp engineID
Local SNMP engineID: 000000090200000000C025808
Remote Engine ID              IP-addr          Port
123456789ABCDEF000000000      192.168.1.1      162
```

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

A. The router's IP address is 192.168.1.1.
B. The SNMP server's IP address is 192.168.1.1.
C. Only the local SNMP engine is configured.
D. Both the local and remote SNMP engines are configured.
E. The router is connected to the SNMP server via port 162.

**Answer:** BD

**NEW QUESTION 255**
What is a required attribute to configure NTP authentication on a Cisco ASA?

A. Key ID
B. IPsec
C. AAA
D. IKEv2

**Answer:** A

**NEW QUESTION 258**
Refer to the exhibit.

```
Phase: 3
   Type: ACCESS-LIST
   Subtype: log
   Result: ALLOW
   Config: access-group inside in interface inside access-list inside extended permit ip any 192.168.1.0 255.255.255.0
```

Which two statements about this firewall output are true? (Choose two.)

A. The output is from a packet tracer debug.
B. All packets are allowed to 192.168.1.0 255.255.0.0.
C. All packets are allowed to 192.168.1.0 255.255.255.0.
D. All packets are denied.
E. The output is from a debug all command.

**Answer:** AC

**NEW QUESTION 263**
What can an administrator do to simultaneously capture and trace packets in a Cisco ASA?

A. Install a Cisco ASA virtual appliance.
B. Use the trace option of the capture command.
C. Use the trace option of the packet-tracer command.
D. Install a switch with a code that supports capturing, and configure a trunk to the Cisco ASA.

**Answer:** B

**NEW QUESTION 264**
Refer to the exhibit. Which command can produce this packet tracer output on a firewall?

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0         0.0.0.0         DMZ

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group INSIDE_IN in interface INSIDE
access-list INSIDE_IN extended permit tcp host 192.168.1.100 any
Additional Information:

Phase: 3
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map classdefault
   match any
policy-map global_policy
   class classdefault
      set connection decrement-ttl
service-policy global_policy global
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (INSIDE,DMZ) source dynamic 192.168.1.100 1.1.1.1
Additional Information:

Phase: 6
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group DMZ_LEAVING out interface DMZ
access-list DMZ_LEAVING extended permit tcp host 192.168.1.100 any
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: DMZ
output-status: up
output-line-status: up
Action: allow
```

A. packet-tracer input INSIDE tcp 192.168.1.100 88 192.168.2.200 3028
B. packet-tracer output INSIDE tcp 192.168.1.100 88 192.168.2.200 3028
C. packet-tracer input INSIDE tcp 192.168.2.200 3028 192.168.1.100 88
D. packet-tracer output INSIDE tcp 192.168.2.200 3028 192.168.1.100 88

**Answer:** A

**NEW QUESTION 269**
At which firewall severity level will debugs appear on a Cisco ASA?

A. 7
B. 6
C. 5
D. 4

**Answer:** A

**NEW QUESTION 271**
What can you do to enable inter-interface firewall communication for traffic that flows between two interfaces of the same security level?

A. Run the command same-security-traffic permit inter-interface globally.
B. Run the command same-security-traffic permit intra-interface globally.
C. Configure both interfaces to have the same security level.
D. Run the command same-security-traffic permit inter-interface on the interface with the highest security level.

**Answer:** A

**NEW QUESTION 272**
How many bridge groups are supported on a firewall that operate in transparent mode?

A. 8
B. 16
C. 10
D. 6

**Answer:** A

**NEW QUESTION 276**
Which kind of Layer 2 attack targets the STP root bridge election process and allows an attacker to control the flow of traffic?

A. man-in-the-middle
B. denial of service
C. distributed denial of service
D. CAM overflow

**Answer:** A

**NEW QUESTION 277**
Which Layer 2 security feature validates ARP packets?

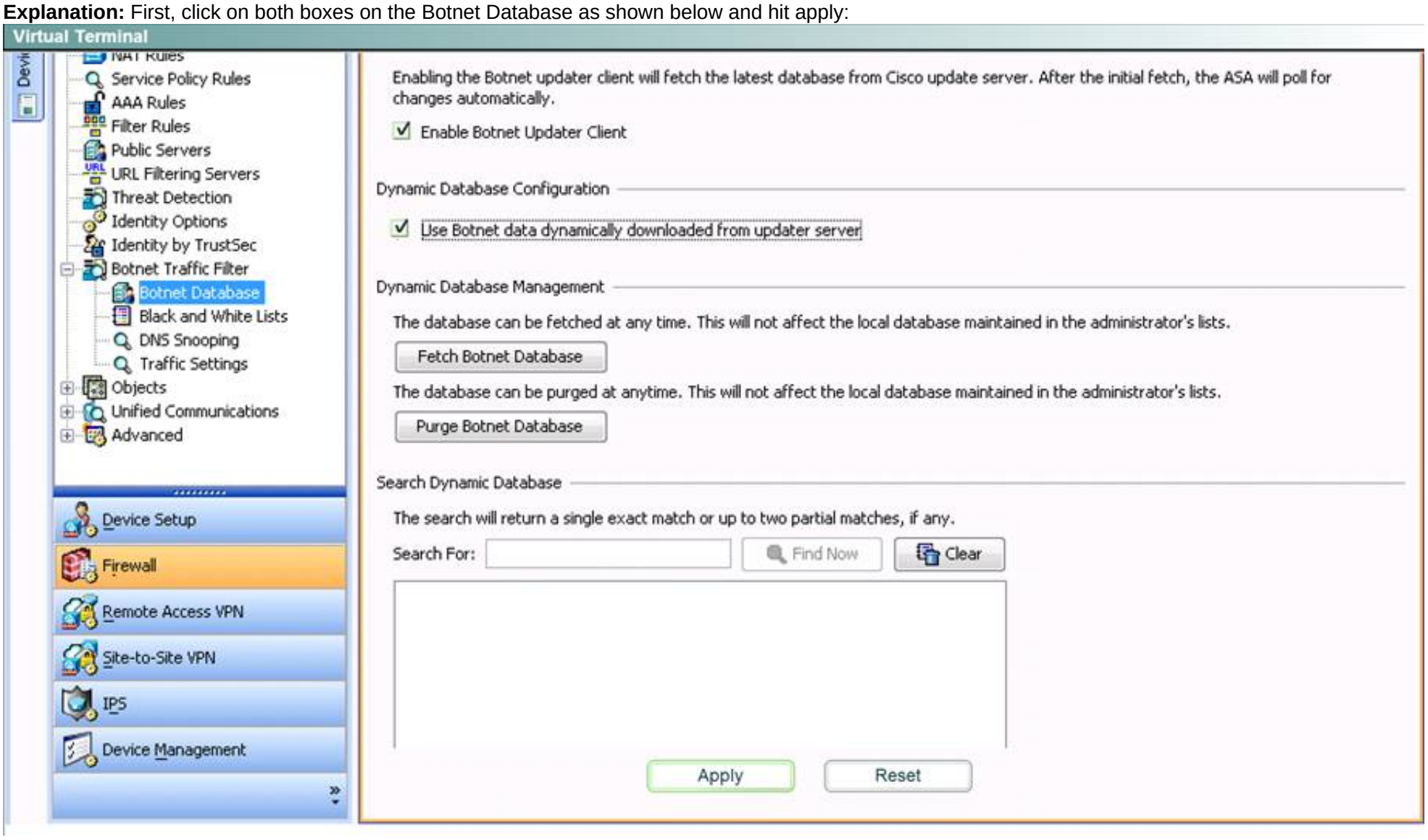
A. DAI
B. DHCP server
C. BPDU guard
D. BPDU filtering

**Answer:** A

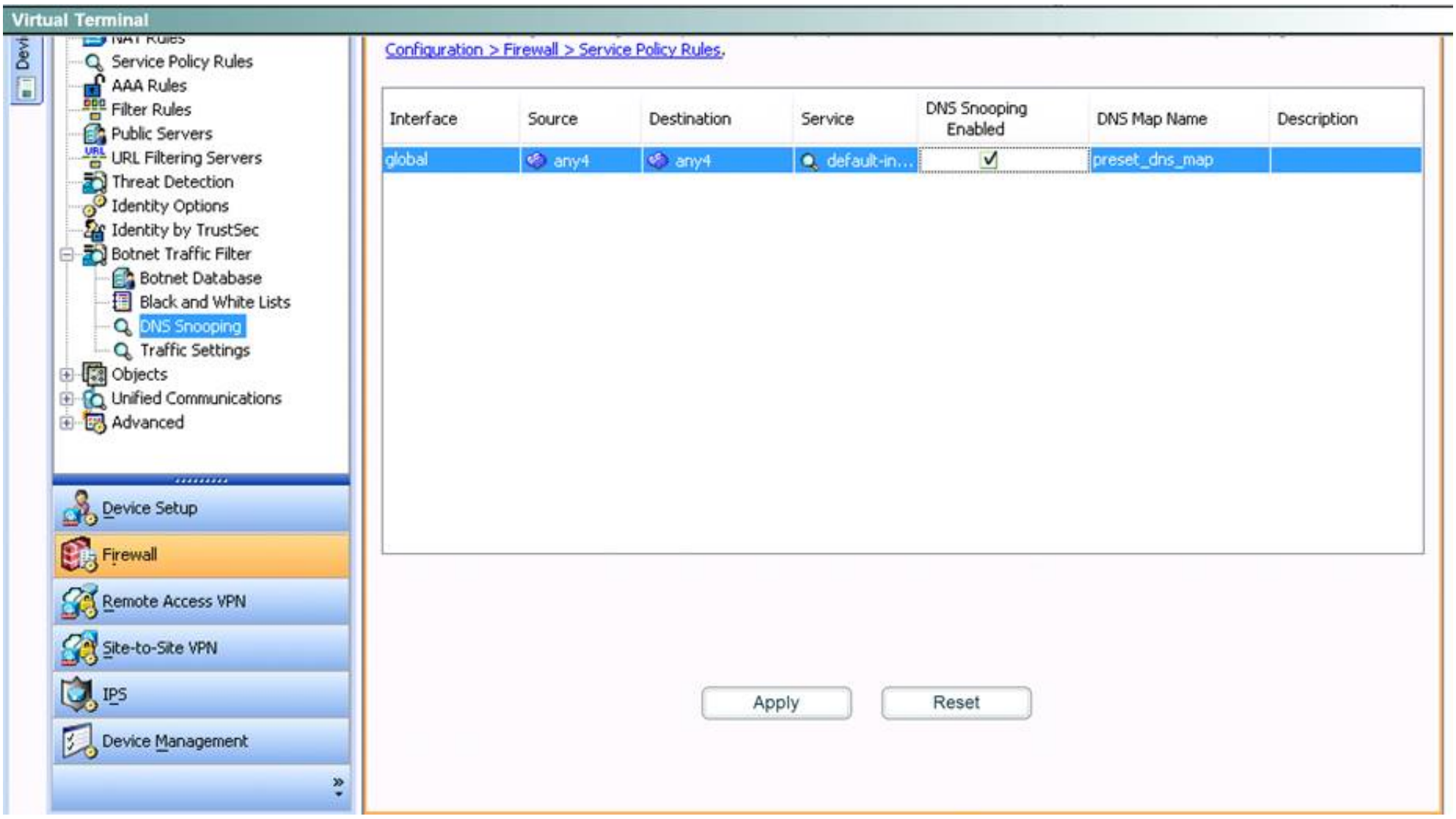
**NEW QUESTION 281**
You are the network security engineer for the Secure-X network. The company has recently detected
Increase of traffic to malware Infected destinations. The Chief Security Officer deduced that some PCs in the internal networks are infected with malware and communicate with malware infected destinations.
The CSO has tasked you with enable Botnet traffic filter on the Cisco ASA to detect and deny further
connection attempts from infected PCs to malware destinations. You are also required to test your configurations by initiating connections through the Cisco ASA and then display and observe the Real-Time Log Viewer in ASDM.
To successfully complete this activity, you must perform the following tasks:
* Download the dynamic database and enable use of it.
• Enable the ASA to download of the dynamic database
• Enable the ASA to download of the dynamic database.
• Enable DNS snooping for existing DNS inspection service policy rules..
• Enable Botnet Traffic Filter classification on the outside interface for All Traffic.
• Configure the Botnet Traffic Filter to drop blacklisted traffic on the outside interface. Use the default Threat Level settings
NOTE: The database files are stored in running memory; they are not stored in flash memory. NOTE: DNS is enabled on the inside interface and set to the HQ-SRV (10.10.3.20).
NOTE: Not all ASDM screens are active for this exercise.
• Verify that the ASA indeed drops traffic to blacklisted destinations by doing the following:
• From the Employee PC, navigate to http://www.google.com to make sure that access to the Internet is working.
• From the Employee PC, navigate to http://bot-spart

**Answer:**

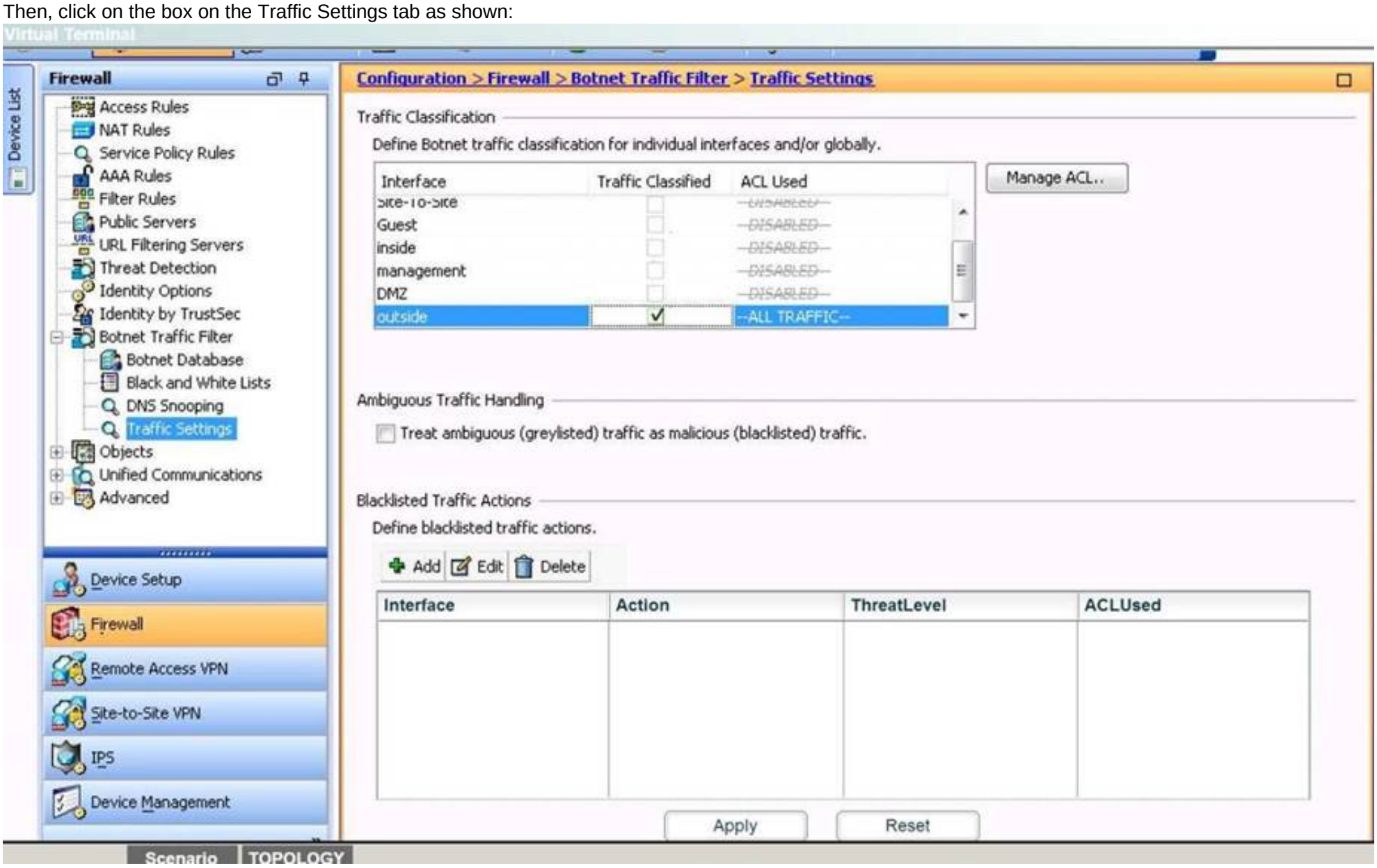
**Explanation:** First, click on both boxes on the Botnet Database as shown below and hit apply:



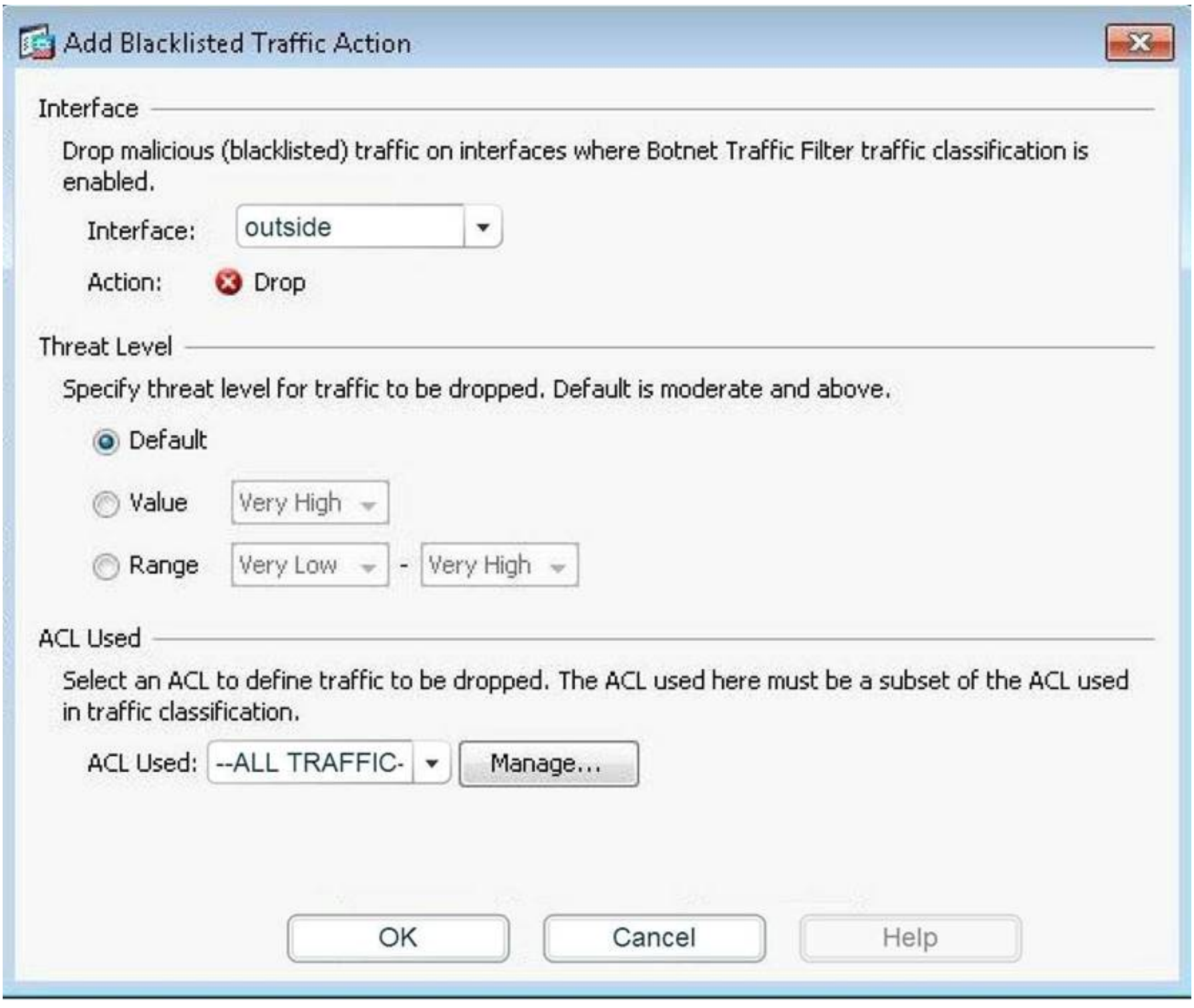

Click Yes to send the commands when prompted.
Then, click on the box on the DNS Snooping page as shown below and hit apply:




Click Yes to send the commands when prompted.
Then, click on the box on the Traffic Settings tab as shown:




At which point this pop-up box will appear when you click on the Add button:

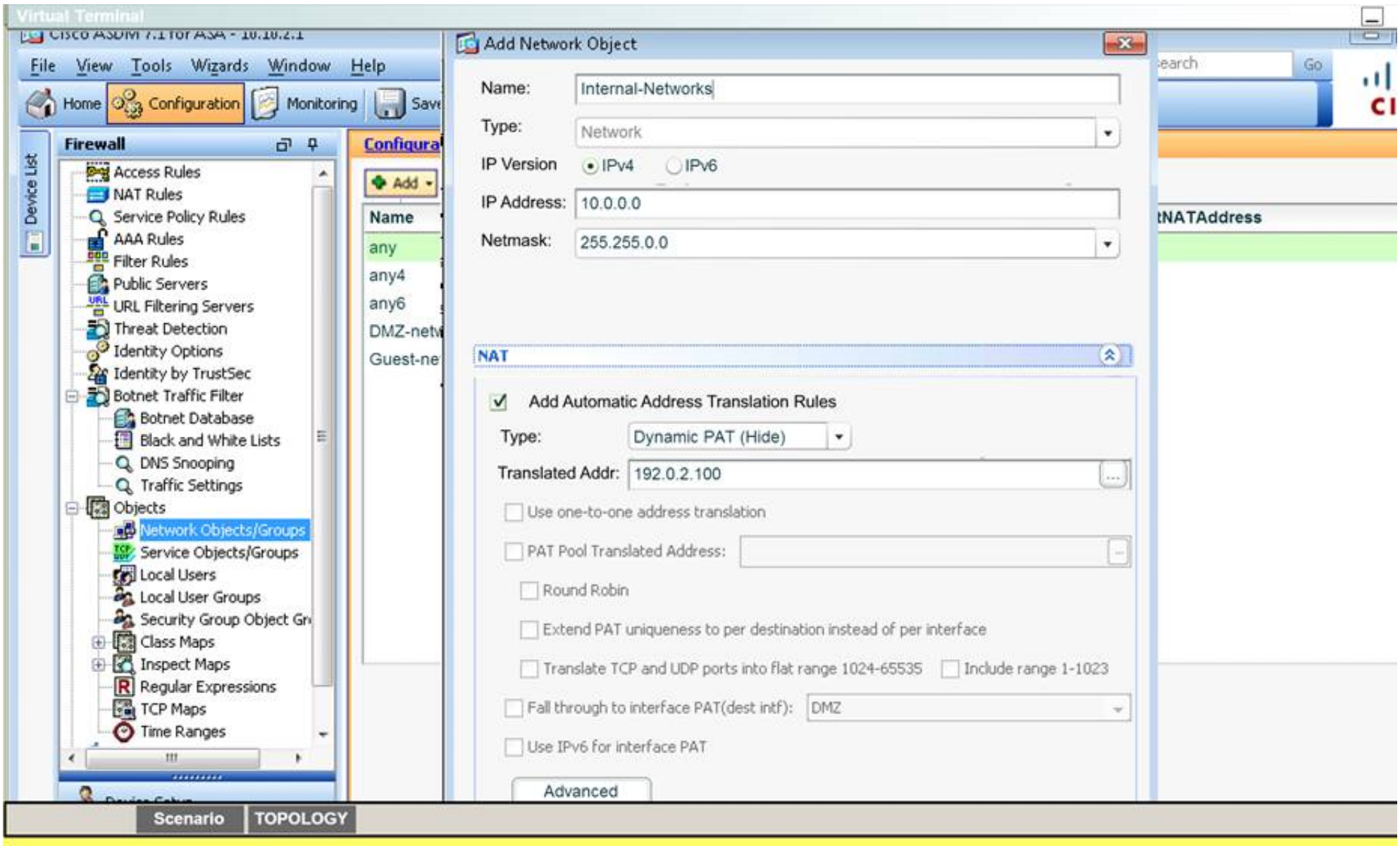



Click OK. Then Apply. Then Send when prompted.
Then verify that all is working according to the instructions given in the question.

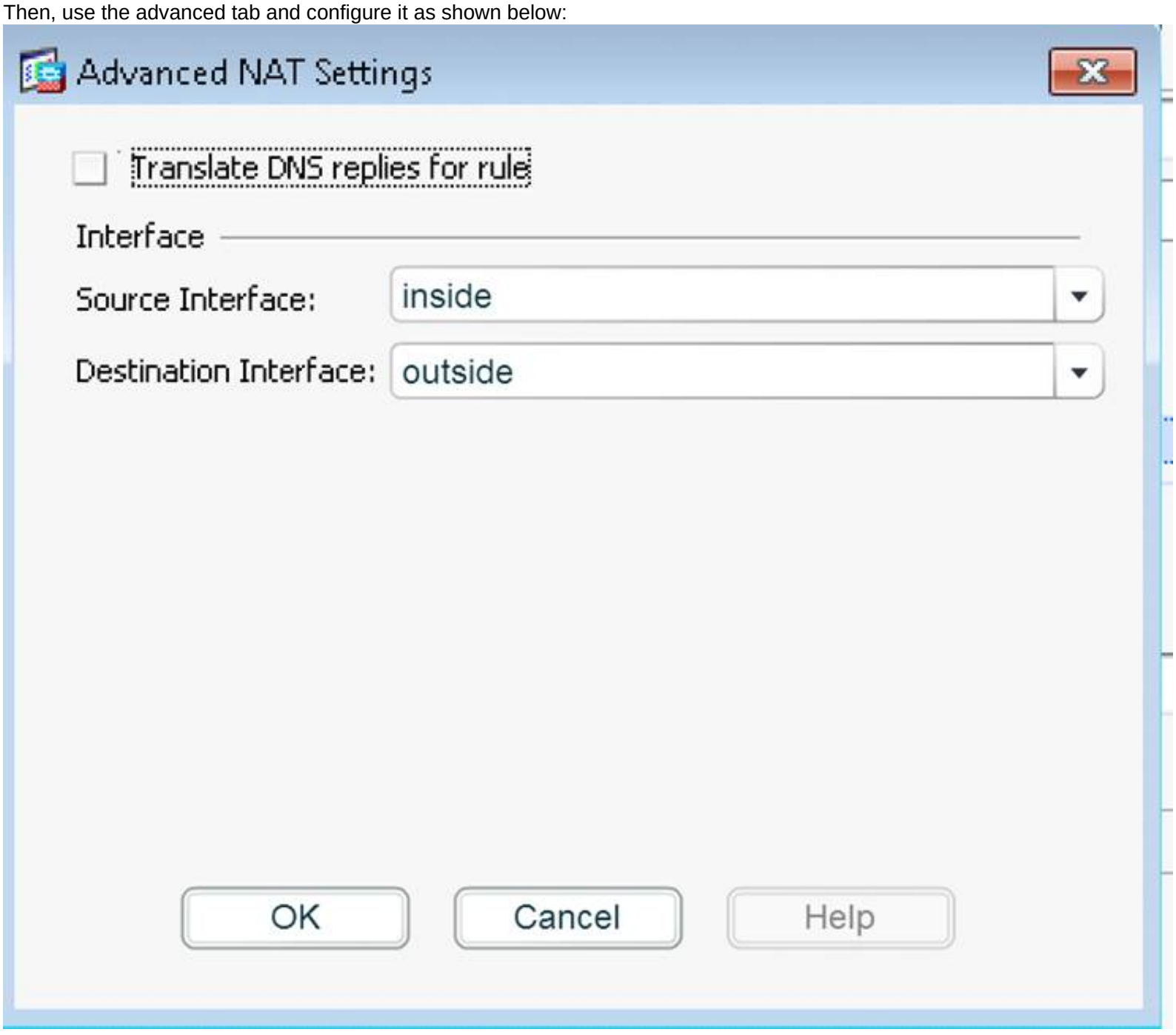
**NEW QUESTION 284**
You are a network security engineer for the Secure-X network. You have been tasked with implementing dynamic network object NAT with PAT on a Cisco AS

**Answer:**

**Explanation:** First, click on Add – Network Objects on the Network Objects/Groups tab and fill in the information as shown below:




Then, use the advanced tab and configure it as shown below:




Then hit OK, OK again, Apply, and then Send when prompted. You can verify using the instructions provided in the question

**NEW QUESTION 286**

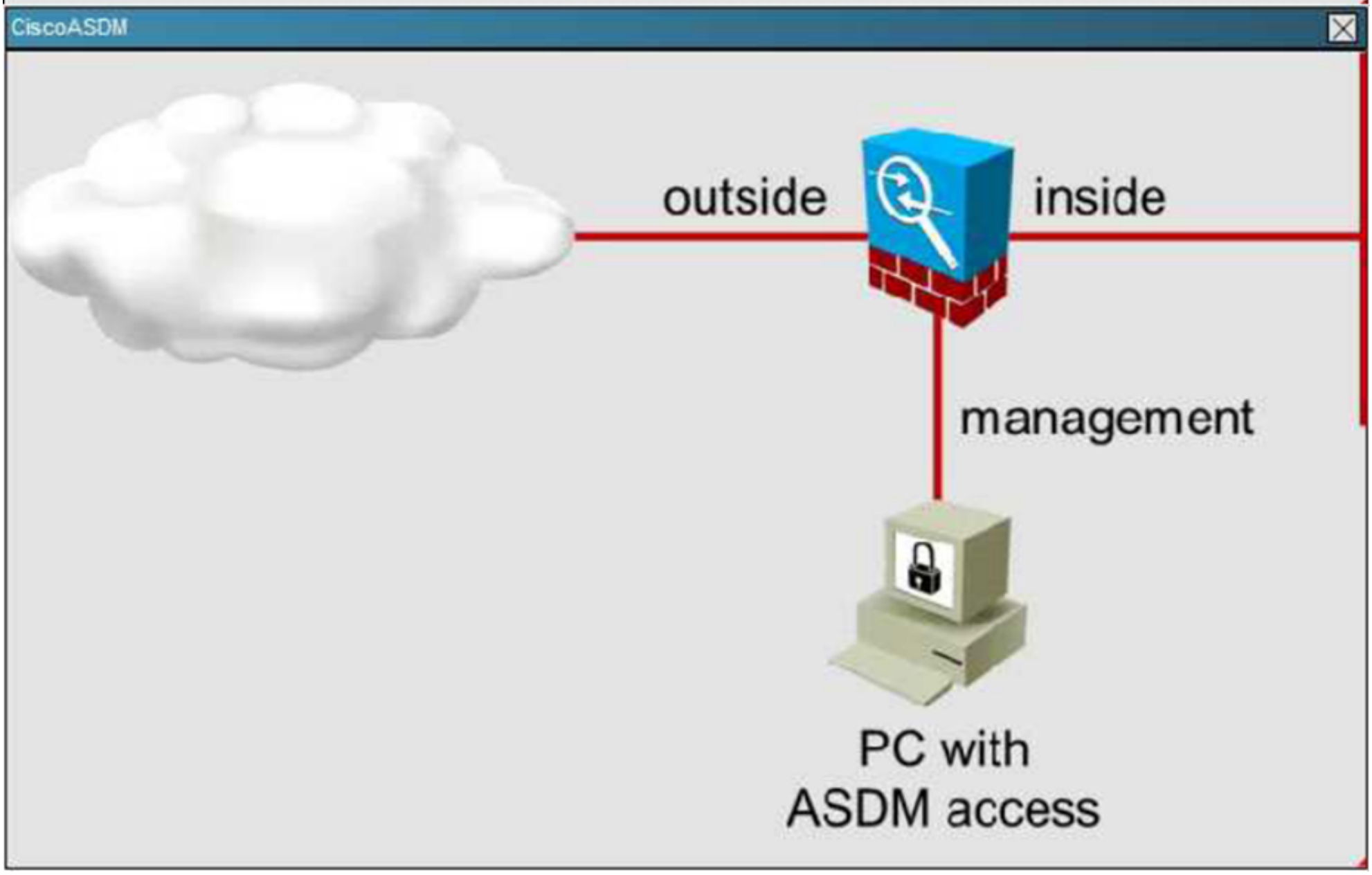
**Scenario**

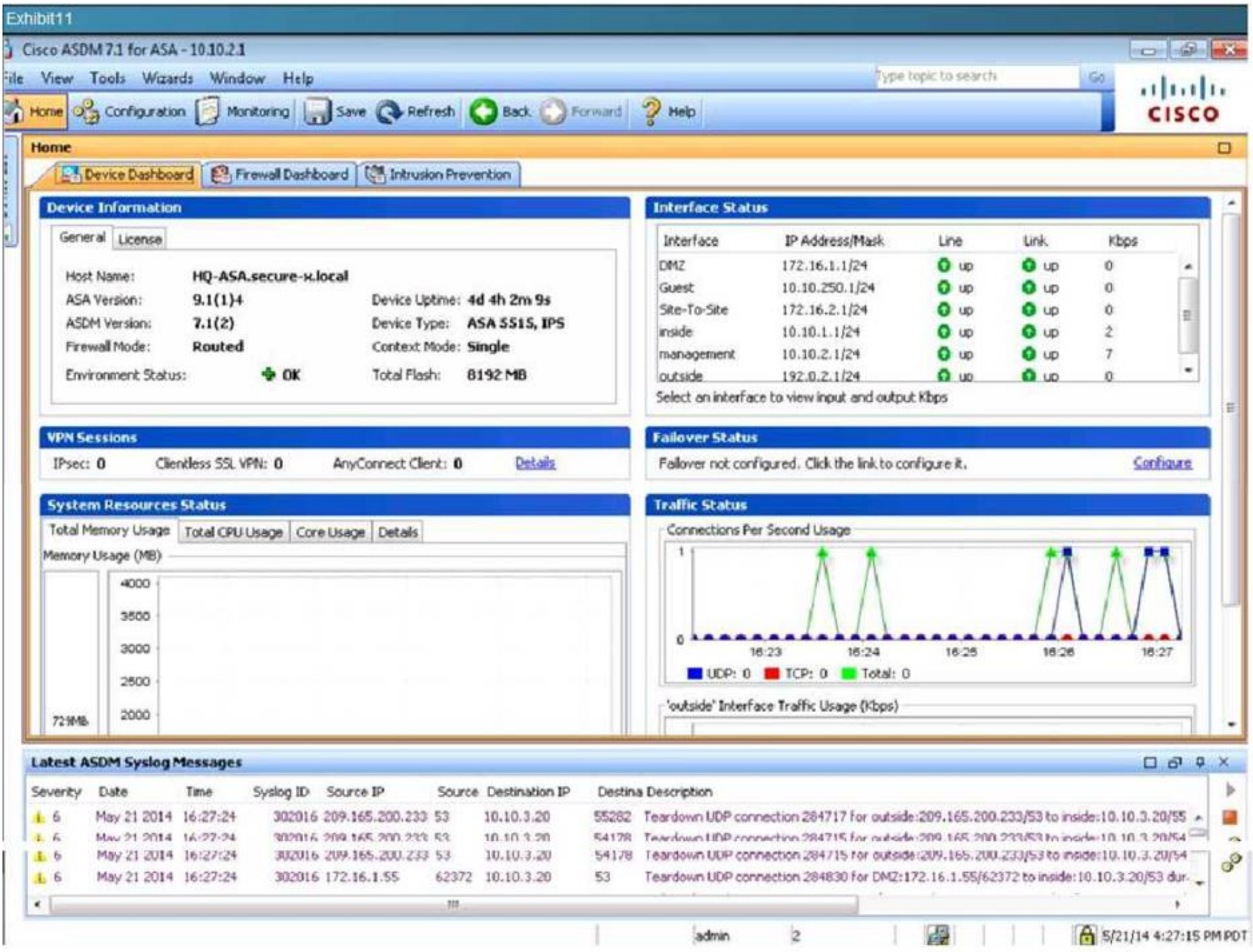
Click on the PC icon to access the Cisco ASDM. Using ASDM, answer the following three questions regarding the ASA configurations. (1 pt each per question)

**Instructions**

- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on the Console PC to gain access to the console of the router. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.

CiscoASDM



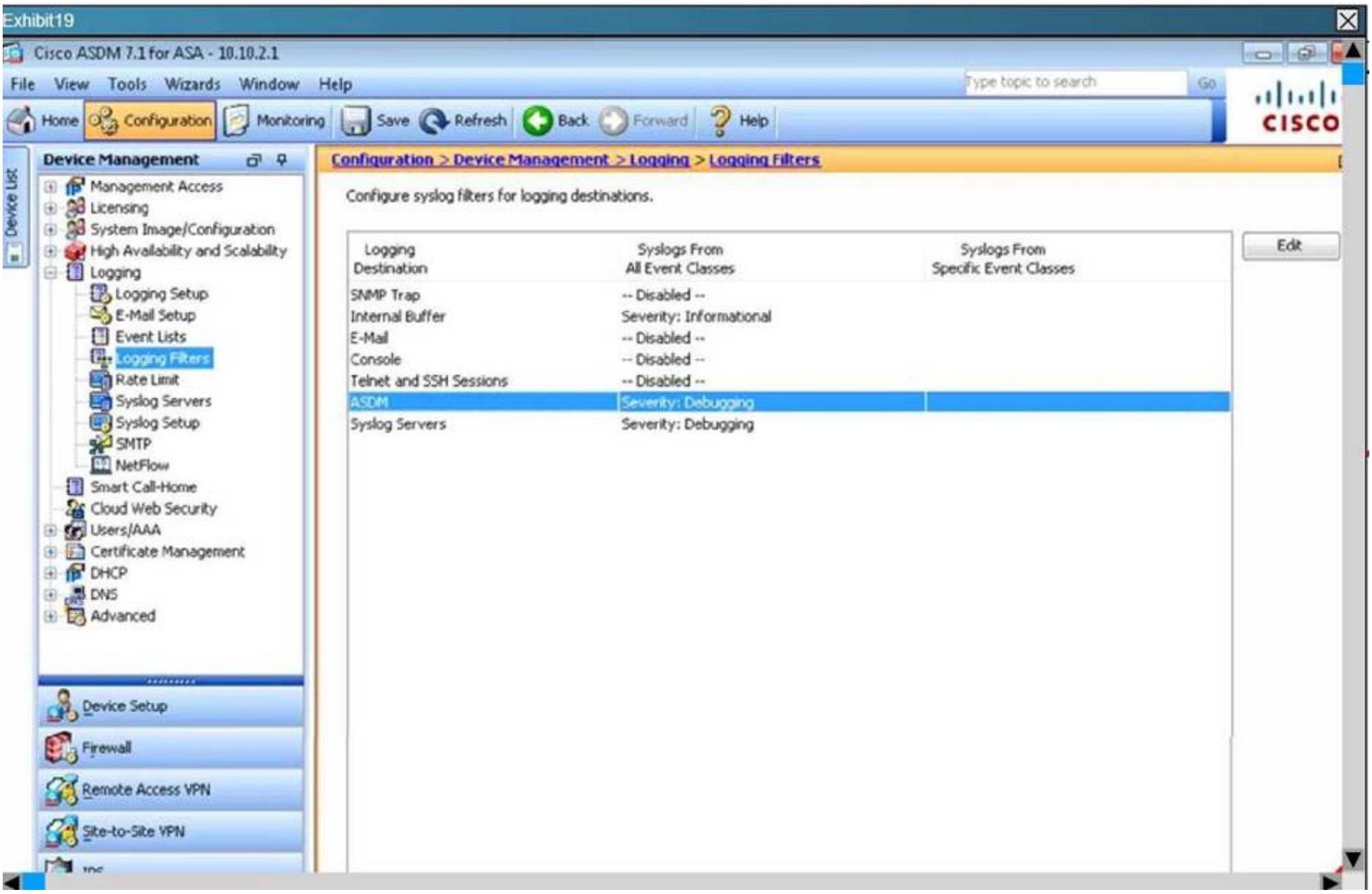



According to the logging configuration on the Cisco ASA, what will happen if syslog server 10.10.2.40 fails?

A. New connections through the ASA will be blocked and debug system logs will be sent to the internal buffer.
B. New connections through the ASA will be blocked and informational system logs will be sent to the internalbuffer.
C. New connections through the ASA will be blocked and system logs will be sent to server 10.10.2.41.
D. New connections through the ASA will be allowed and system logs will be sent to server 10.10.2.41.
E. New connections through the ASA will be allowed and informational system logs will be sent to the internalbuffer.
F. New connections through the ASA will be allowed and debug system logs will be sent to the internal buffer.

**Answer:** B

**Explanation:** This is shown by the following screen shot:




**NEW QUESTION 289**
Which statement about Cisco ASA NetFlow v9 (NSEL) is true?

A. NSEL events match all traffic classes in parallel
B. NSEL is has a time interval locked at 20 seconds and is not user configurable
C. NSEL tracks flow-create, flow-teardown, and flow-denied events and generates appropriate NSEL datarecords
D. You cannot disable syslog messages that have become redundant because of NSEL
E. NSEL tracks the flow continuously and provides updates every 10 second
F. NSEL provides stateless IP flow tracking that exports all record od a specific flow

**Answer:** C

**Explanation:**
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_nse l.html

**NEW QUESTION 293**
When a Cisco ASA CX module is management by Cisco Prime Security Manager in a Multiple Devices Mode, which mode does the firewall use ?

A. Managed Mode
B. Unmanaged mode
C. Single mode
D. Multi mode

**Answer:** A

**Explanation:**
http://www.cisco.com/c/en/us/td/docs/security/asacx/9-1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1b_User_Guide_for_ASA_CX_and_PRSM_9_1_chapter_0 110.ht ml#task_7E648F43AD724DA2983699B12E92A528

**NEW QUESTION 296**
Which option is the default logging buffer size In memory of the Cisco ASA adaptive security appliance?

A. 8KB
B. 32KB
C. 2KB
D. 16KB
E. 4KB

**Answer:** E

**Explanation:**
http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_c onfig/ monitor_syslog.html

**NEW QUESTION 301**
Which options lists cloud deployment modes?

A. Private, public, hydrid, community
B. Private, public, hydrid, shared
C. IaaS, PaaS, SaaS
D. Private, public, hydrid

**Answer:** A

**Explanation:**
https://www.ibm.com/developerworks/community/blogs/722f6200-f4ca-4eb3-9d64- 8d2b58b2d4e8/
entry/4_Types_of_Cloud_Computing_Deployment_Model_You_Need_to_Know1?lang=en

**NEW QUESTION 305**
Prior to a software upgrade, which Cisco Prime Infrastructure feature determines if the devices being upgraded have sufficient RAM to support to new software ?

A. Software Upgrade Report
B. Image Management Report
C. Upgrade Analysis Report
D. Image Analysis Report

**Answer:** C

**Explanation:**
http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2- 0/user/guide/prime_infra_ug/ maint_images.html

**NEW QUESTION 309**
Which two options are private-VLAN secondary VLAN types? (Choose two)

A. Isolated
B. Secured
C. Community
D. Common
E. Segregated

**Answer:** AC

**Explanation:**
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html

**NEW QUESTION 310**
Which cloud characteristic is used to describes the sharing of physical resource between various entities ?

A. Elasticity
B. Ubiquitous access
C. Multitenancy
D. Resiliency

**Answer:** C

**NEW QUESTION 313**
Which feature is a limitation of a Cisco ASA 5555-X running 8.4.5 version with multiple contexts?

A. Deep packet inspection
B. Packet tracer
C. IPsec
D. Manual/auto NAT
E. Multipolicy packet capture

**Answer:** C

**NEW QUESTION 317**
Which statement about Dynamic ARP Inspection is true ?

A. In a typical network, you make all ports as trusted expect for the ports connection to switches , which areuntrusted
B. DAI associates a trust state with each switch

C. DAI determines the validity of an ARP packet based on valid IP to MAC address binding from the DHCPsnooping database
D. DAI intercepts all ARP requests and responses on trusted ports only
E. DAI cannot drop invalid ARP packets

**Answer:** C

**NEW QUESTION 321**
Which action is needed to set up SSH on the Cisco ASA firewall?

A. Create an ACL to aloew the SSH traffic to the Cisco ASA.
B. Configure DHCP for the client that will connect via SSH.
C. Generate a crypto key
D. Specify the SSH version level as either 1 or 2.
E. Enable the HTTP server to allow authentication.

**Answer:** C

**NEW QUESTION 326**
Which action is considered a best practice for the Cisco ASA firewall?

A. Use threat detection to determine attacks
B. Disable the enable password
C. Disable console logging
D. Enable ICMP permit to monitor the Cisco ASA interfaces
E. Enable logging debug-trace to send debugs to the syslog server

**Answer:** C

**NEW QUESTION 331**
Which policy map action makes a Cisco router behave as a stateful firewall for matching traffic?

A. Log
B. Inspect
C. Permit
D. Deny

**Answer:** B

**NEW QUESTION 333**
Which configuration on a switch would be unsuccessful in preventing a DHCP starvation attack?

A. DHCP snooping
B. Port security
C. Source Guard
D. Rate Limiting

**Answer:** C

**NEW QUESTION 335**
Which three statements about transparent firewall are true? ( Choose three)

A. Transparent firewall works at Layer 2
B. Both interfaces must be configured with private IP Addresses
C. It can have only a management IP address
D. It does not support dynamic routing protocols
E. It only support PAT

**Answer:** ACD

**NEW QUESTION 339**
For which management session types does ASDM allow a maximum simultaneous connection limit to be set?

A. ASDM, Telnet, SSH
B. ASDM, Telnet, SSH, console
C. ASDM, Telnet, SSH, VTY
D. ASDM, Telnet, SSH, other

**Answer:** A

**NEW QUESTION 343**
A firewall administrator must write a short script for network operations that will login to all cisco ASA firewalls and check that the current running version is compliant with company policy. The administrator must first configure a restricted local username on each of the Cisco ASA firewalls so that the current running version can be validated. Which configuration command provides the least access in order to perform this function?

A. username version user password cisco
B. username version user password cisco privilege 0
C. username version user password cisco privilege 2
D. username version user password cisco privilege 15

**Answer:** B

**Explanation:**
When typing the following command, we get the following result.
ciscoasa# show run all privilege | in version
privilege show level 0 mode exec command version
Based on that we can use the show version command with privilege 0
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/p.html#wp1921158

**NEW QUESTION 347**
An engineer has configured a unified IPV6/IPV4 ACL to be used for access control on the Cisco ASA in routed mode. Which additional IPV4/IPv6 components is needed for the ACL to function properly?

A. mixed object group
B. network address translation
C. explicit deny statement
D. service object

**Answer:** B

**NEW QUESTION 348**
When an engineer is configuring DHCP snooping, which configuration parameter is enabled by default?

A. DHCP snooping host tracking feature
B. DHCP snooping MAC address verification
C. DHCP snooping relay agent
D. DHCP snooping information option-82

**Answer:** D

**Explanation:**
Default Configuration Values for DHCP Snooping DHCP snooping Disabled
DHCP snooping host tracking feature Disabled DHCP snooping information option Enabled
DHCP option-82 on untrusted port feature Disabled DHCP snooping limit rate None
DHCP snooping trust Untrusted DHCP snooping vlan Disabled
DHCP snooping spurious server detection Disabled DHCP snooping detect spurious interval 30 minutes
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12- 2SX/configuration/guide/book/snoodhcp.html#wp1108657

**NEW QUESTION 350**
Which statement describes a unifeature of cisco netflow secure event logging?

A. multiple net flow collectors
B. secure netflow connections are optmiedfor ciscoprime
C. advanced netflow V9 templates and legacy V5 formattingare supported
D. flow-create events are delayed which overall traffic

**Answer:** D

**NEW QUESTION 354**
Which of the following that Cisco engineer must secure a current monitoring environment? (Choose Two)

A. RSA-SIG
B. MD5
C. AES
D. 3DES
E. DES

**Answer:** CD

**NEW QUESTION 358**
What is a benefit of the IOS Control plane protection feature?

A. it allows QOS policing of aggregate control-panel
B. it provides for early dropping of packets directed toward closed
C. it prevents the input guide from being overwhelmed by any single
D. it minimizes the number of unprocessed packets a protocol can have

**Answer:** B

**NEW QUESTION 361**
An engineer is applying best practices to stop vlan hopping attacks? (Choose Two)

A. disable DTP on user facing ports
B. configure DHCP snooping on all switches
C. use the vlan dot 1Q tag native command
D. disable cisco discovary protocol on all switches
E. configure IP on source Guard on all switches

**Answer:** AC

**NEW QUESTION 362**
A network engineer must mange and configurations to a cisco networking environment solutions accomplishes this task?

A. cisco IPS manage express and pushing configuration to the ips units
B. cisco security 4.5 or later and pushing configuration bundles to each of the,,,,,
C. cisco adaptive security device manager to push configuration to each of the IPS
D. fire SIGHT manager to bundle and push configuration to the IPS units installed

**Answer:** D

**NEW QUESTION 366**
A network engineer has installed Cisco Security Manager 4.7 on a windows 2008 R2 SP1 server with 8 GB of RAM. When using the reporting feature, Cisco Security Manager frequently fails. Which option is the reason for this fault?

A. Cisco Security Manager must be running Windows 2008 R2 Service Pack 2.
B. Cisco Security Manager running all services must have minimum of 16 GB of RAM
C. Cisco Security Manager is running on a domain controller
D. Cisco Security Manager was not installed by a user with administrative rights.

**Answer:** B

**NEW QUESTION 371**
On a Cisco ASA, how can you allow traffic to enter and exit via same interface?

A. Configure both interfaces to have the same security level.
B. Issue the command same-security-traffic permit inter-interface.
C. Install a router on a stick.
D. Issue the command same-security-traffic permit intra-interface.

**Answer:** D

**Explanation:** To permit communication between interfaces with equal security levels, or to allow traffic to enter anciscoasad exit the same interface, use the same-security-traffic command in global configuration mode. To disable the same-security traffic, use the no form of this command.
same-security-traffic permit { inter-interface | intra-interface }
no same-security-traffic permit { inter-interface | intra-interface }
Syntax Description
inter-interface Permits communication between different interfaces that have the same security level.
intra-interface Permits communication in and out of the same interface. http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3/s1.html

**NEW QUESTION 373**
Refer to the Following.
NTP authentication-key 10 md5 cisco123 ntp trusted-key 10
A network engineer is testing NTP authentication, and realizes that any device can synchronize time with this router and that NTP authentication is not enforced.
Which option is likely the issue?

A. Only SHA-1 is allowed as a hashing algorithm for NTP authentication.
B. The key must be configured in hashed format, not plain text.
C. NTP authentication needs to be specifically enabled.
D. The router must be rebooted before NTP can update.

**Answer:** C

**NEW QUESTION 376**
Which two voice and video protocols does the Cisco ASA 5500 Series support with Cisco Unified Communications Application Inspection? (Chose two)

A. SCTP
B. SDP
C. H.323
D. H248
E. SCCP
F. SRTP

**Answer:** CE

**Explanation:** https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/product_data_sheet0900aecd8073cbbf.html

**NEW QUESTION 377**
Which device can be managed by the Cisco Prime Security Manager?

A. ASA CX
B. ISR G2
C. Nexus
D. UCM

**Answer:** A

**Explanation:** https://www.cisco.com/c/en/us/td/docs/security/asacx/9-2/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_2/prsm-ug-intro.html

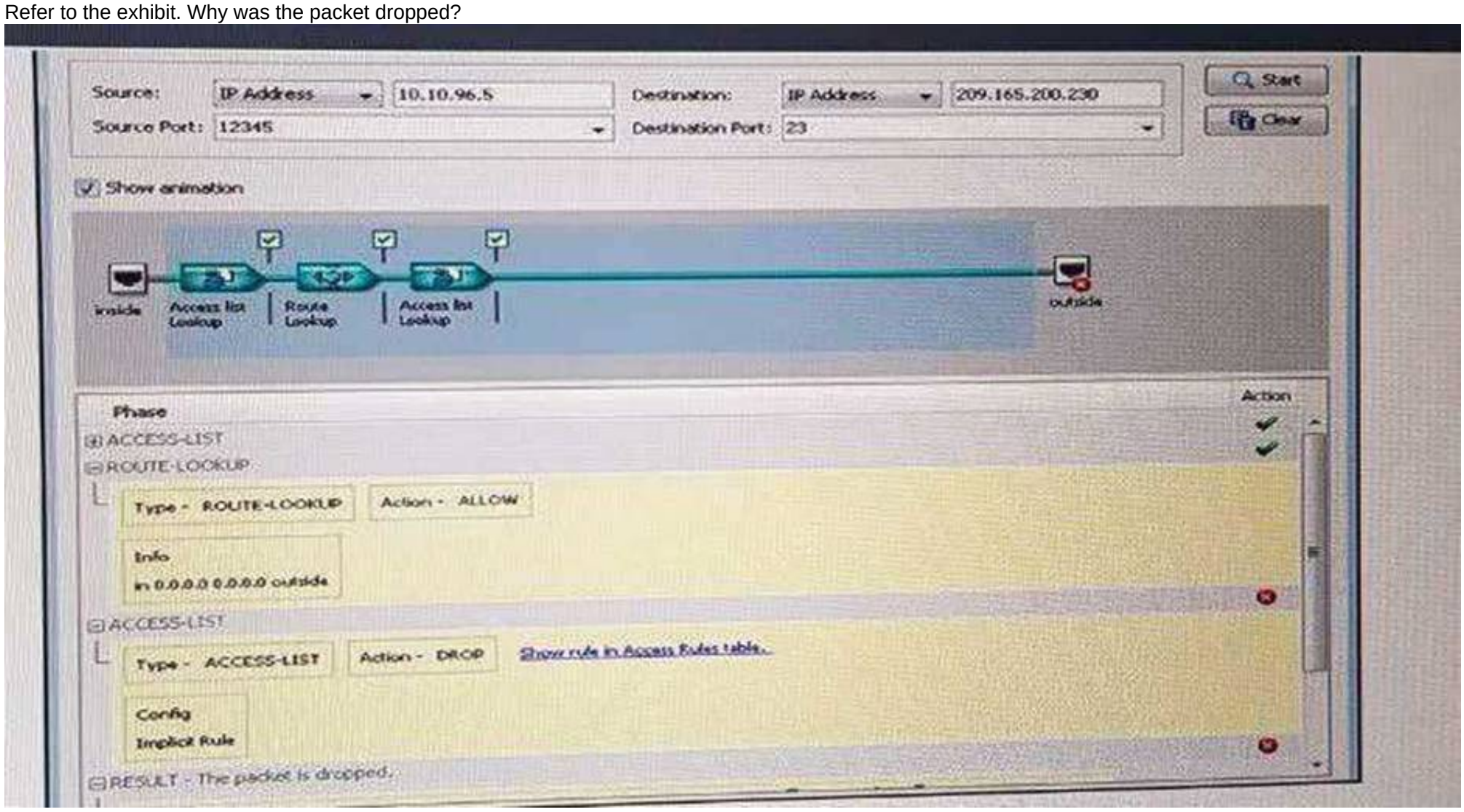
**NEW QUESTION 381**
Which hypervisor technology is supported by Cisco ASA 1000V Cloud Firewall?

A. KVM
B. XenServer
C. Hyper-V
D. VMware vSphere

**Answer:** D

**Explanation:** https://www.cisco.com/c/en/us/products/collateral/security/asa-1000v-cloud-firewall/data_sheet_c78-687960.html

**NEW QUESTION 386**
Refer to the exhibit. Why was the packet dropped?




(this exhibit is packet capture with traffic destination to port 23 and being drop by access-list)

A. Telnet access is not allowed between these two nodes.
B. NAT is not applied correctly for the 10.10.96.5 host
C. The source port is configured incorrectly In the capture
D. There is no route on the Cisco ASA to the destination host

**Answer:** A

**NEW QUESTION 388**
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. STP root guard
C. SPT bpdu filter

**Answer:** B

**NEW QUESTION 393**
Packet tracer doesn't work in which mode?

A. routed
B. transparent
C. single context
D. multicontext

**Answer:** B

**NEW QUESTION 394**
What are Options of capture command? (Choose Two)

A. host
B. real-time
C. type

**Answer:** BC

**Explanation:** real-time, type, interface,buffer, match, packet-lenght,trace,circular-buffer, ethernet-type,acces-list, headers-only

**NEW QUESTION 396**
An engineer suspect that client workstations are expecting poor response time due to man in the middle attack. How to fix it:

A. key exchange
B. private vlan
C. Rev DNS
D. link aggregation
E. dynamic inspection

**Answer:** E

**NEW QUESTION 401**
An engineer is configuring Cisco TrustSec NDAC MACsec . which two components?

A. switch-to-switch connection
B. user- facing downlink support
C. switch-to-host connection
D. switch port connected to other switches
E. host-facing links

**Answer:** AD

**NEW QUESTION 405**
What two are data and voice protocols do ASA 5500 supports? (Choose two)

A. CTIQBE Inspection
B. H.323 Inspection
C. MGCP Inspection
D. RTSP Inspection
E. SIP Inspection
F. Skinny (SCCP) Inspection

**Answer:** BD

**NEW QUESTION 410**
What is the best practice about storm control - where to implement?

A. PortChannel
B. interfaces of that Po

**Answer:** A

**Explanation:** Implement on a Port Channel Interface but never on ports which are configured as members of an Etherchannel because this put the ports into a suspended state.

**NEW QUESTION 414**
Company configure Private VLAN and it will add a new server. What port it will use that allow to communicate with all interfaces?

A. Promiscuous

B. Community
C. Isolated

**Answer:** B

**NEW QUESTION 415**
DRAG DROP
Drag and Drop Syslog security level to match its related.

| | |
|---|---|
| ( )%ASA-1-101001 | Critical |
| ( )%ASA-2-106001 | Warnings |
| ( )%ASA-3-105010 | Debugging |
| ( )%ASA-4-106027 | Alerts |
| ( )%ASA-5-103421 | Informational |
| ( )%ASA-6-104531 | Errors |
| ( )%ASA-7-102398 | Notifications |

**Answer:**

**Explanation:**

| | |
|---|---|
| ( )%ASA-1-101001 | Alerts |
| ( )%ASA-2-106001 | Critical |
| ( )%ASA-3-105010 | Errors |
| ( )%ASA-4-106027 | Warnings |
| ( )%ASA-5-103421 | Notifications |
| ( )%ASA-6-104531 | Informational |
| ( )%ASA-7-102398 | Debugging |

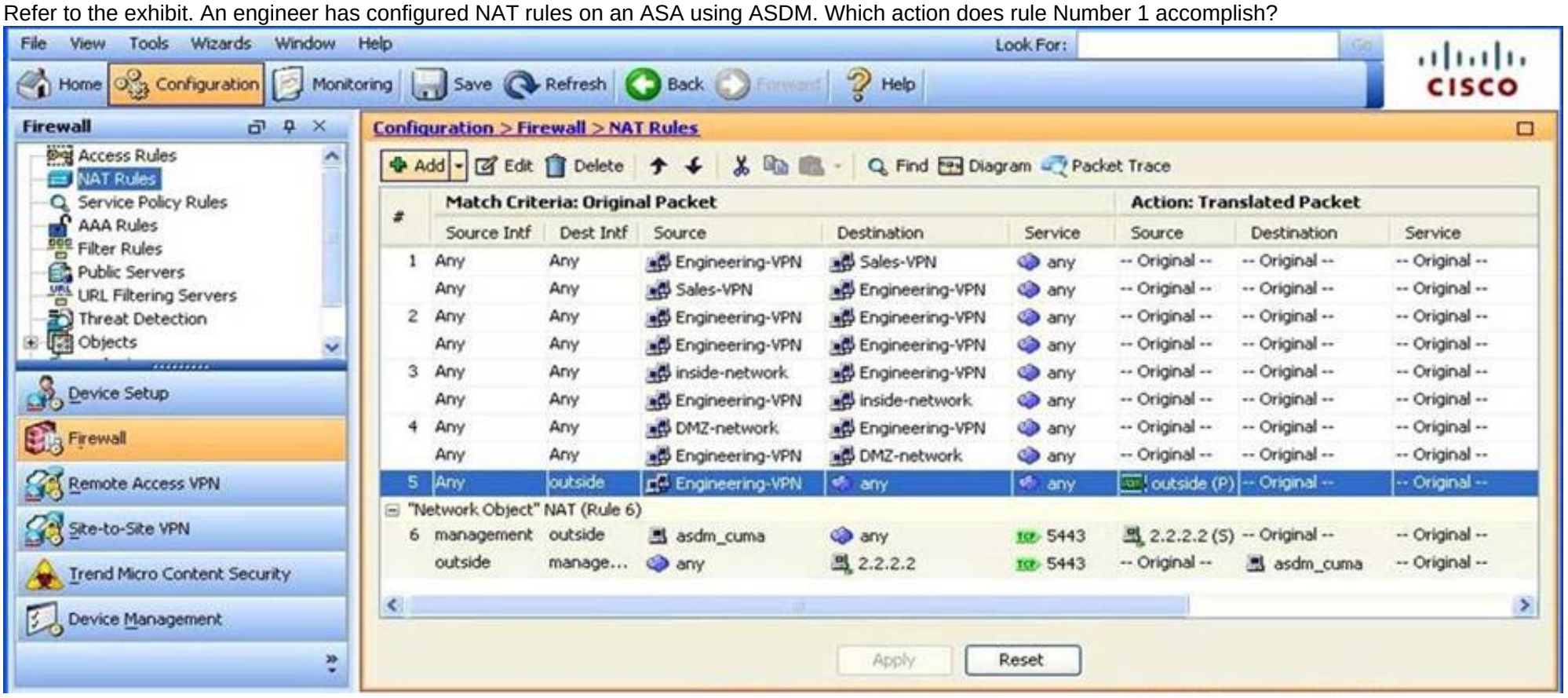
**NEW QUESTION 419**
Which ASA feature can inspect encrypted VoIP traffic between a Cisco IP phone and the Cisco UCM?

A. mobile proxy
B. TLS proxy
C. MGCP security services
D. content security services

**Answer:** B

**Explanation:** Reference:
https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next- generationfirewalls/
product_data_sheet0900aecd8073cbbf.html

**NEW QUESTION 421**
Refer to the exhibit. An engineer has configured NAT rules on an ASA using ASDM. Which action does rule Number 1 accomplish?




A. It allows the engineering VPN address pool to access the Internet through the tunnel
B. It allows hosts in the address pool to reach other hosts in the engineering VPN address pool
C. It allows hosts in the engineering VPN object to reach the hosts in the Sales VPN without being nat-ed
D. It allows the connection between the engineering VPN address pool and the DMZ network

**Answer:** C

**NEW QUESTION 424**
An engineer is adding devices to Cisco Prime Infrastructure using Discovery. Which protocol must be used when RTDM is processed?

A. LLDP
B. ARP
C. OSPF
D. BGP

**Answer:** B

**Explanation:**
Reference:
https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/user/guide/pi_ug/gettingstarted.html

**NEW QUESTION 428**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-206 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-206 Product From:

**https://www.2passeasy.com/dumps/300-206/**

## Money Back Guarantee

### 300-206 Practice Exam Features:

* 300-206 Questions and Answers Updated Frequently

* 300-206 Practice Questions Verified by Expert Senior Certified Staff

* 300-206 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-206 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year