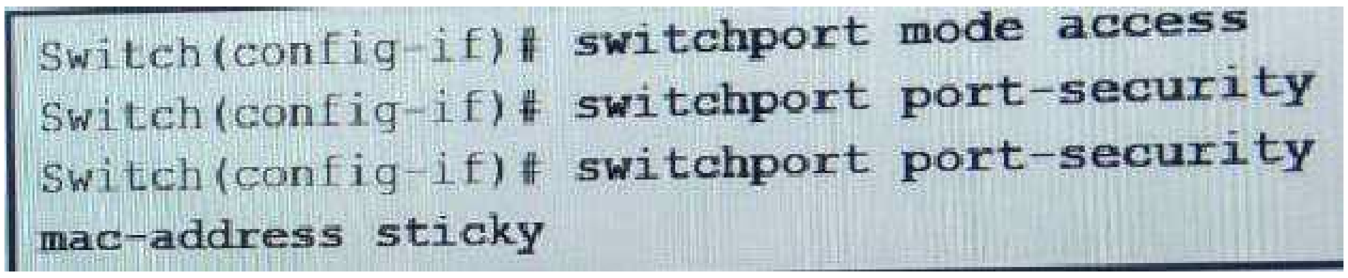
Exam Questions 300-206

Implementing Cisco Edge Network Security Solutions

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

NEW QUESTION 1
Refer to the exhibit.



```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security
mac-address sticky
```

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.

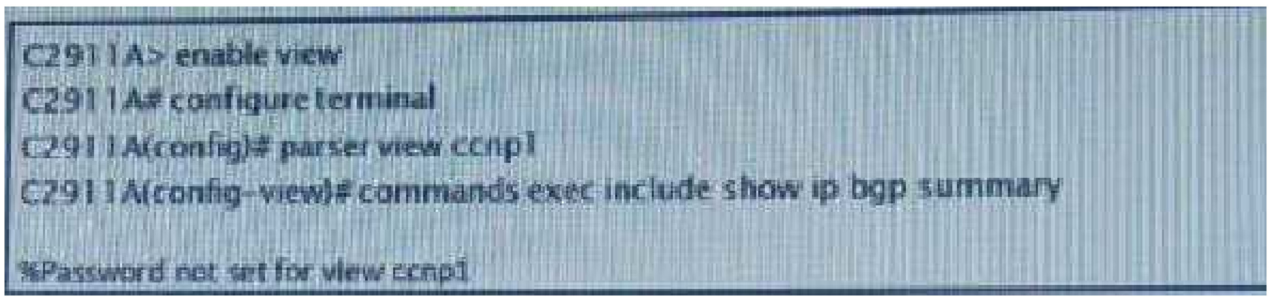
Answer: BE

NEW QUESTION 2
A network engineer wants to add new view to an IOS device configured with RBAC. Which privilege is required for that task?

A. Level 16
B. Level 15
C. root view
D. admin view

Answer: B

NEW QUESTION 3
Refer to the exhibit.



```
C2911A> enable view
C2911A# configure terminal
C2911A(config)# parser view ccnp1
C2911A(config-view)# commands exec include show ip bgp summary

%Password not set for view ccnp1
```

An engineer is configuring IOS rote based CLI access and is getting an error upon entering the command* exec include show ip bgp summary parser view command. Based on the console message received, which command would fix this error?

A. enable secret <password>
B. username <user> secret <password>
C. password <password>
D. secret 5 <encrypted password>

Answer: D

NEW QUESTION 4
After a session has been secured with MACsec, which two types of traffic can be sent and received unencrypted?

A. EAPOL-Start
B. DHCP offer
C. Cisco Discovery Protocol
D. DHCP discover
E. EAPOL-Logoff

Answer: AC

NEW QUESTION 5
Which two main functions for application inspection on ASA are true?

A. When services use dynamically assigned ports, the application inspection identifies dynamic port and permits data on these ports.
B. When services embed IP addresses in the packet, the application inspection translates embedded addresses and updates the checksum.
C. When services are operating on nonstandard ports, the application inspection identifies the nonstandard port and allows the service to run normally.
D. When services need IP options to function, the application inspection keeps IP options during the packet transition through the appliance.
E. When services use load balancing, the application inspection ensures that connections are load blanaced across the servers equally.

Answer: AB

NEW QUESTION 6
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 7
A security engineer is troubleshooting traffic across a Cisco ASA firewall using a packet tracer. When configuring the packet tracer, which option must be used first?

A. interface
B. protocol
C. source
D. destination

Answer: A

NEW QUESTION 8
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 9
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 10
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 10
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 14
A company is concerned with valid time sources and has asked for NTP authentication to be configured.
Multiple NTP sources are on the network. Which configuration is required on the client device to authenticate and synchronize with an NTP source?

A. trusted key
B. stratum hash
C. SSL
D. certificate preshared key

Answer:

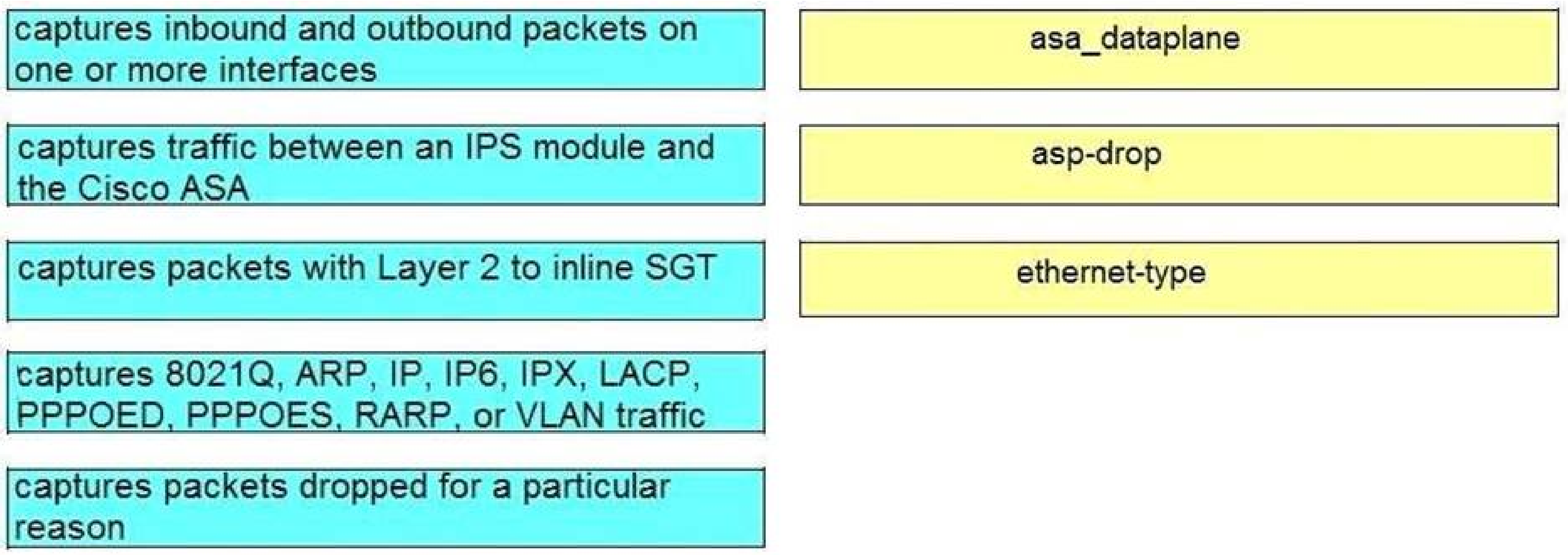
A

NEW QUESTION 16
An engineer is asked to configure SNMP Version 3 with authentication and encryption of each SNMP packet.
Which SNMP V3 mode must be configured to meet that requirement?

A. priv
B. auth
C. pub
D. encr

Answer: A

NEW QUESTION 21
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

captures traffic between an IPS module and the Cisco ASA

captures packets with Layer 2 to inline SGT

captures 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, or VLAN traffic

captures packets dropped for a particular reason

asa_dataplane

asp-drop

ethernet-type

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 26
An engineer is adding devices to Cisco Prime Infrastructure using Discovery and wants to use Web Services Management Agent for configuring devices. Which credential setting must be used?

A. SNMPv2 Credential
B. SNMPv3 Credential
C. Telnet Credential
D. SSH Credential

Answer: D

NEW QUESTION 28
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

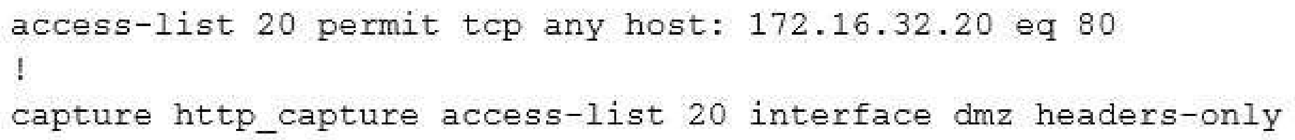
NEW QUESTION 31
An engineer is using Cisco Security Manager and is using default ports configuration. What port must be open to connect the Cisco Security Manager Client to an ASA?

A. 22
B. 23
C. 80

D. 443

Answer: D

NEW QUESTION 32
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 36
What is the maximum number of servers configurable in a Cisco Prime Infrastructure high availability implementation?

A. 2 servers
B. 4 servers
C. 8 servers
D. 16 servers

Answer: A

NEW QUESTION 40
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 44
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

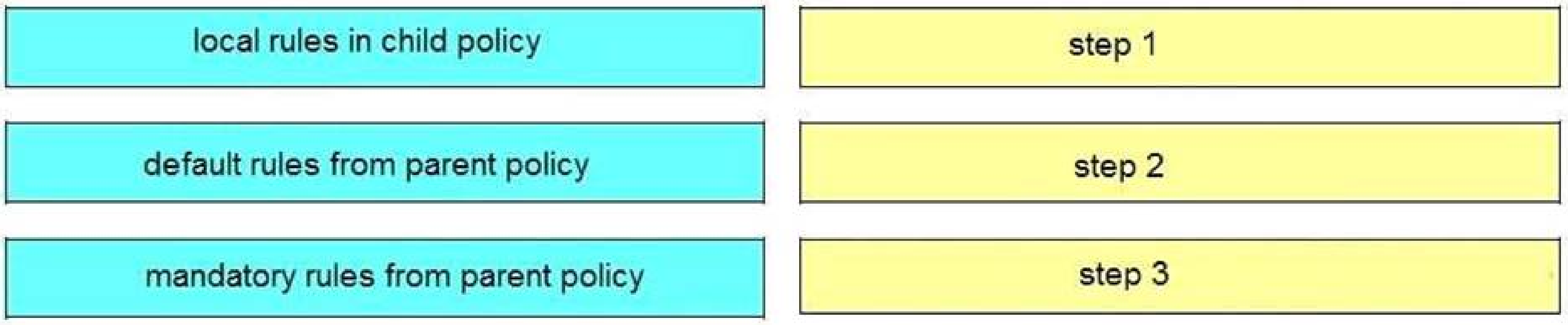
NEW QUESTION 46
Which type of traffic would make use of the ASA’s default route while running in transparent mode?

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 51
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.



local rules in child policy

default rules from parent policy

mandatory rules from parent policy

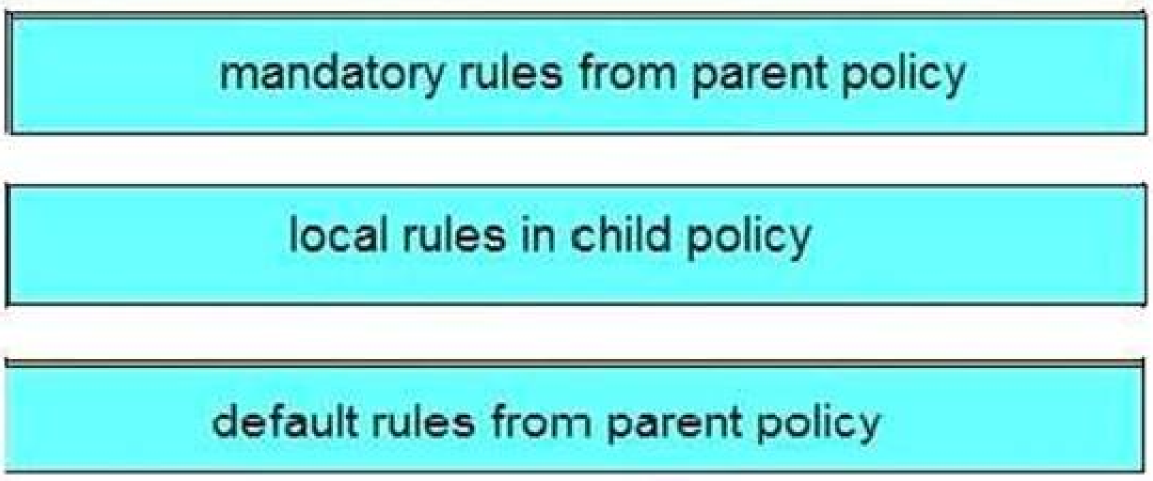
step 1

step 2

step 3

Answer:

Explanation:



mandatory rules from parent policy

local rules in child policy

default rules from parent policy

NEW QUESTION 54
Which Cisco ASA command authenticates the Cisco ASDM client that accesses the security appliance using HTTPS with local user database?

A. aaa authentication ssh console LOCAL
B. aaa authentication serial console LOCAL
C. aaa authentication telnet console LOCAL
D. aaa authentication http console LOCAL

Answer: A

NEW QUESTION 57
An engineer is configuring control-plane protocol queue thresholding. For which protocol can the engineer set queue limits?

A. CDP
B. ARP
C. IPX
D. BGP

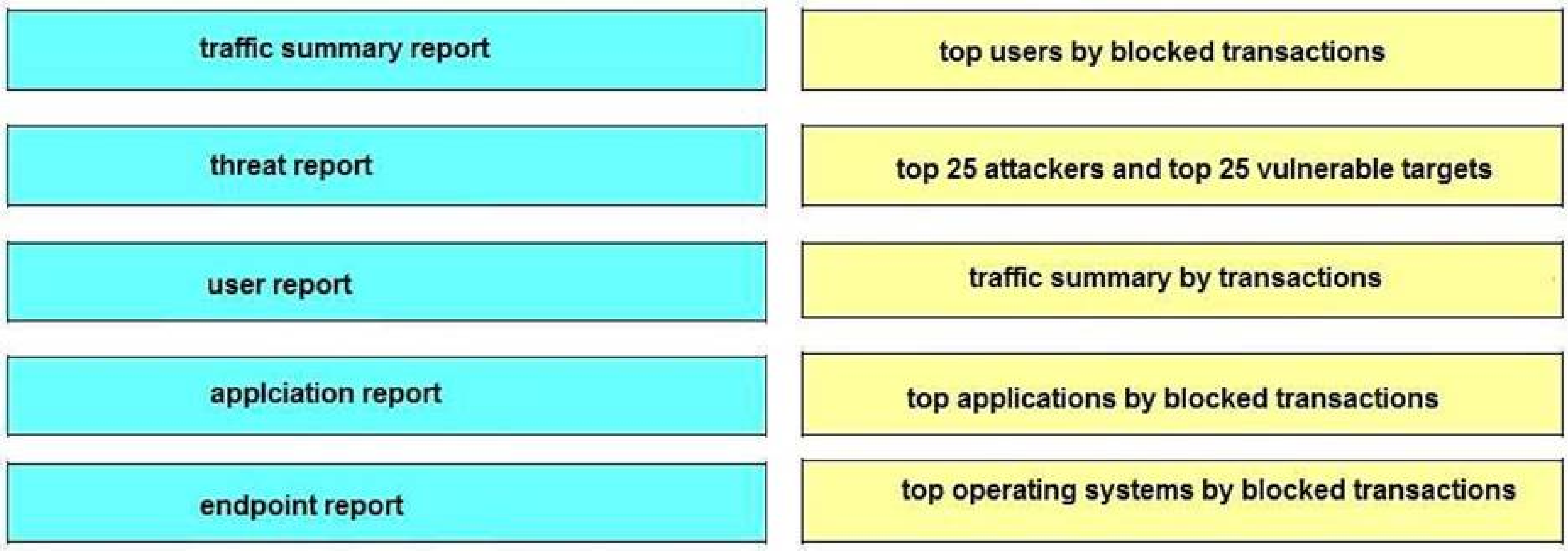
Answer: D

NEW QUESTION 59
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 64
DRAG DROP
Drag and drop the Cisco Prime Security Manager available reports on the left onto the correct report examples on the right.



traffic summary report

threat report

user report

applciation report

endpoint report

top users by blocked transactions

top 25 attackers and top 25 vulnerable targets

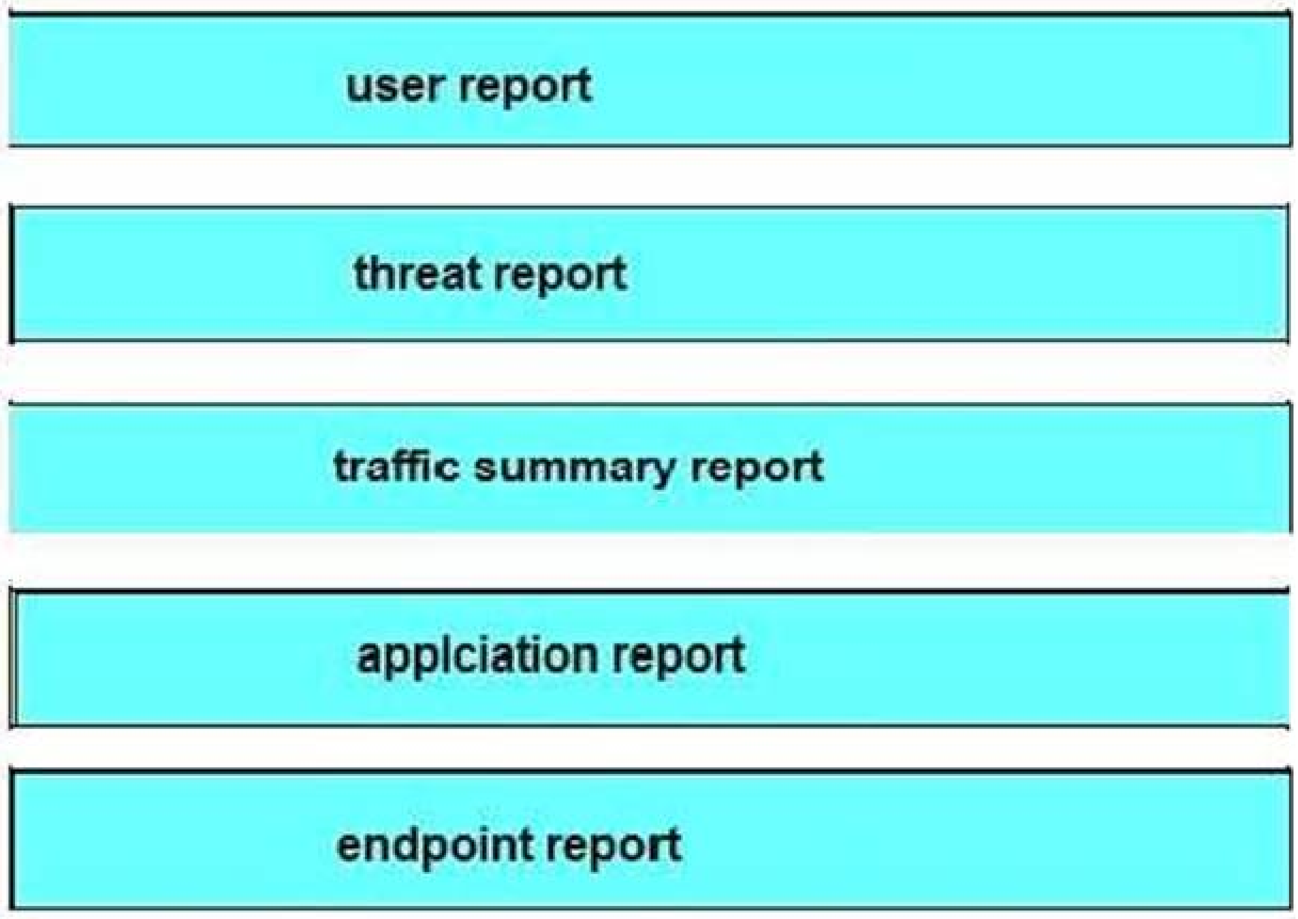
traffic summary by transactions

top applications by blocked transactions

top operating systems by blocked transactions

Answer:

Explanation:



user report

threat report

traffic summary report

applciation report

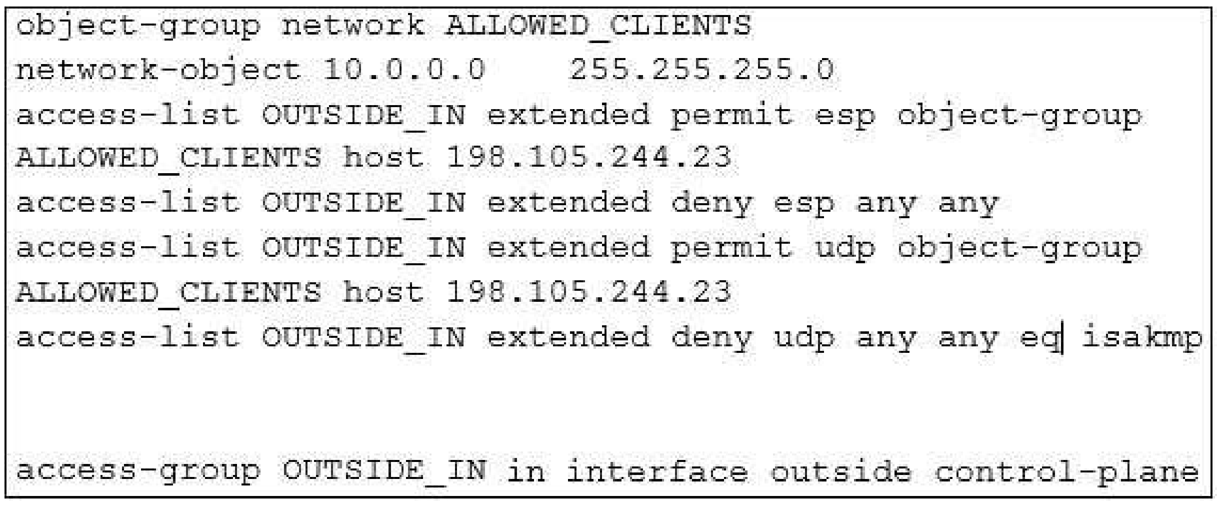
endpoint report

NEW QUESTION 65
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 69
Refer to the exhibit.



```
object-group network ALLOWED_CLIENTS
network-object 10.0.0.0    255.255.255.0
access-list OUTSIDE_IN extended permit esp object-group
ALLOWED_CLIENTS host 198.105.244.23
access-list OUTSIDE_IN extended deny esp any any
access-list OUTSIDE_IN extended permit udp object-group
ALLOWED_CLIENTS host 198.105.244.23
access-list OUTSIDE_IN extended deny udp any any eq isakmp


access-group OUTSIDE_IN in interface outside control-plane
```

What is the effect of this firewall configuration?

A. It controls IP traffic is sourced from the OUTSIDE interface.
B. It controls IPsec packets that terminate at the firewall.
C. It controls IP traffic to the OUTSIDE interface.
D. It controls IPsec packets that are sourced from the firewall.

Answer: B

NEW QUESTION 72
An engineer has been asked to confirm packet process on an AS

A. In which mode is packet-tracer command unsupported?
B. multiple security context
C. single security context
D. transparent
E. routed
F. HA

Answer: C

NEW QUESTION 77
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 78
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 79
Which command sets the source IP address of the NetFlow exports of a device?

A. ip source flow-export
B. ip source netflow-export
C. ip flow-export source
D. ip netflow-export source

Answer: C

NEW QUESTION 81
Which three options are default settings for NTP parameters on a Cisco device? (Choose three.)

A. NTP authentication is enabled.
B. NTP authentication is disabled.
C. NTP logging is enabled.
D. NTP logging is disabled.
E. NTP access is enabled.
F. NTP access is disabled.

Answer: BDE

NEW QUESTION 86
Which two features are supported when configuring clustering of multiple Cisco ASA appliances?
(Choose two.)

A. NAT
B. dynamic routing
C. SSL remote access VPN
D. IPSec remote access VPN

Answer: AB

NEW QUESTION 88
Which two device types can Cisco Prime Security Manager manage in Multiple Device mode?

(Choose two.)

A. Cisco ESA
B. Cisco ASA
C. Cisco WSA
D. Cisco ASA CX

Answer: BD

NEW QUESTION 92
Which technology provides forwarding-plane abstraction to support Layer 2 to Layer 7 network services in Cisco Nexus 1000V?

A. Virtual Service Node
B. Virtual Service Gateway
C. Virtual Service Data Path
D. Virtual Service Agent

Answer: C

NEW QUESTION 95
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 99
A network administrator is creating an ASA-CX administrative user account with the following parameters:
- The user will be responsible for configuring security policies on networkdevices.
- The user needs read-write access to policies.
- The account has no more rights than necessary for the job. What role will be assigned to the user?

A. Administrator
B. Security administrator
C. System administrator
D. Root Administrator
E. Exec administrator

Answer: B

NEW QUESTION 104
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 106
Where in the Cisco ASA appliance CLI are Active/Active Failover configuration parameters configured?

A. admin context
B. customer context
C. system execution space
D. within the system execution space and admin context
E. within each customer context and admin context

Answer: C

NEW QUESTION 110
Which Cisco ASA show command groups the xlates and connections information together in its output?

A. show conn
B. show conn detail
C. show xlate
D. show asp
E. show local-host

Answer: E

NEW QUESTION 113
When a Cisco ASA is configured in multiple context mode, within which configuration are the interfaces allocated to the security contexts?

A. each security context
B. system configuration
C. admin context (context with the "admin" role)
D. context startup configuration file (.cfg file)

Answer: B

NEW QUESTION 115
On the Cisco ASA, where are the Layer 5-7 policy maps applied?

A. inside the Layer 3-4 policy map
B. inside the Layer 3-4 class map
C. inside the Layer 5-7 class map
D. inside the Layer 3-4 service policy
E. inside the Layer 5-7 service policy

Answer: A

NEW QUESTION 117
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 119
Which four are IPv6 First Hop Security technologies? (Choose four.)

A. Send
B. Dynamic ARP Inspection
C. Router Advertisement Guard
D. Neighbor Discovery Inspection
E. Traffic Storm Control
F. Port Security
G. DHCPv6 Guard

Answer: ACDG

NEW QUESTION 123
IPv6 addresses in an organization's network are assigned using Stateless Address Autoconfiguration. What is a security concern of using SLAAC for IPv6 address assignment?

A. Man-In-The-Middle attacks or traffic interception using spoofed IPv6 Router Advertisements
B. Smurf or amplification attacks using spoofed IPv6 ICMP Neighbor Solicitations
C. Denial of service attacks using TCP SYN floods
D. Denial of Service attacks using spoofed IPv6 Router Solicitations

Answer: A

NEW QUESTION 126
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 130
A network engineer is troubleshooting and configures the ASA logging level to debugging. The
logging-buffer is dominated by %ASA-6-305009 log messages. Which command suppresses those syslog messages while maintaining ability to troubleshoot?

A. no logging buffered 305009
B. message 305009 disable
C. no message 305009 logging
D. no logging message 305009

Answer: D

NEW QUESTION 134
Which three Cisco ASA configuration commands are used to enable the Cisco ASA to log only the debug output to syslog? (Choose three.)

A. logging list test message 711001
B. logging debug-trace
C. logging trap debugging
D. logging message 711001 level 7
E. logging trap test

Answer: ABE

NEW QUESTION 138
Which two configurations are the minimum needed to enable EIGRP on the Cisco ASA appliance? (Choose two.)

A. Enable the EIGRP routing process and specify the AS number.
B. Define the EIGRP default-metric.
C. Configure the EIGRP router ID.
D. Use the neighbor command(s) to specify the EIGRP neighbors.
E. Use the network command(s) to enable EIGRP on the Cisco ASA interface(s).

Answer: AE

NEW QUESTION 142
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 146
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 151
What is the lowest combination of ASA model and license providing 1 Gigabit Ethernet interfaces?

A. ASA 5505 with failover license option
B. ASA 5510 Security+ license option
C. ASA 5520 with any license option
D. ASA 5540 with AnyConnect Essentials License option

Answer: B

NEW QUESTION 152
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 156
Which two statements about Cisco IOS Firewall are true? (Choose two.)

A. It provides stateful packet inspection.
B. It provides faster processing of packets than Cisco ASA devices provide.
C. It provides protocol-conformance checks against traffic.

D. It eliminates the need to secure routers and switches throughout the network.
E. It eliminates the need to secure host machines throughout the network.

Answer: AC

NEW QUESTION 158
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 159
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 163
What is the default behavior of NAT control on Cisco ASA Software Version 8.3?

A. NAT control has been deprecated on Cisco ASA Software Version 8.3.
B. It will prevent traffic from traversing from one enclave to the next without proper access configuration.
C. It will allow traffic to traverse from one enclave to the next without proper access configuration.
D. It will deny all traffic.

Answer: A

NEW QUESTION 167
What is the CLI command to enable SNMPv3 on the Cisco Web Security Appliance?

A. snmpconfig
B. snmpenable
C. configsnmp
D. enablesnmp

Answer: A

NEW QUESTION 170
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 171
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 175
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 176
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 179
When a Cisco ASA is configured in transparent mode, how can ARP traffic be controlled?

A. By enabling ARP inspection; however, it cannot be controlled by an ACL
B. By enabling ARP inspection or by configuring ACLs
C. By configuring ACLs; however, ARP inspection is not supported
D. By configuring NAT and ARP inspection

Answer: A

NEW QUESTION 181
What is the primary purpose of stateful pattern recognition in Cisco IPS networks?

A. mitigating man-in-the-middle attacks
B. using multi packet inspection across all protocols to identify vulnerability-based attacks and to thwart attacks that hide within a data stream
C. detecting and preventing MAC address spoofing in switched environments
D. identifying Layer 2 ARP attacks

Answer: B

NEW QUESTION 182
What are two reasons to implement Cisco IOS MPLS Bandwidth-Assured Layer 2 Services? (Choose two.)

A. guaranteed bandwidth and peak rates as well as low cycle periods, regardless of which systems access the device
B. increased resiliency through MPLS FRR for AToM circuits and better bandwidth utilization through MPLS TE
C. enabled services over an IP/MPLS infrastructure, for enhanced MPLS Layer 2 functionality
D. provided complete proactive protection against frame and device spoofing

Answer: BC

NEW QUESTION 183
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 187
Which statement about the Cisco ASA configuration is true?

A. All input traffic on the inside interface is denied by the global ACL.
B. All input and output traffic on the outside interface is denied by the global ACL.
C. ICMP echo-request traffic is permitted from the inside to the outside, and ICMP echo-reply will be permitted from the outside back to inside.
D. HTTP inspection is enabled in the global policy.
E. Traffic between two hosts connected to the same interface is permitted.

Answer: B

NEW QUESTION 191
In the default global policy, which traffic is matched for inspections by default?

A. match any
B. match default-inspection-traffic
C. match access-list
D. match port

E. match class-default

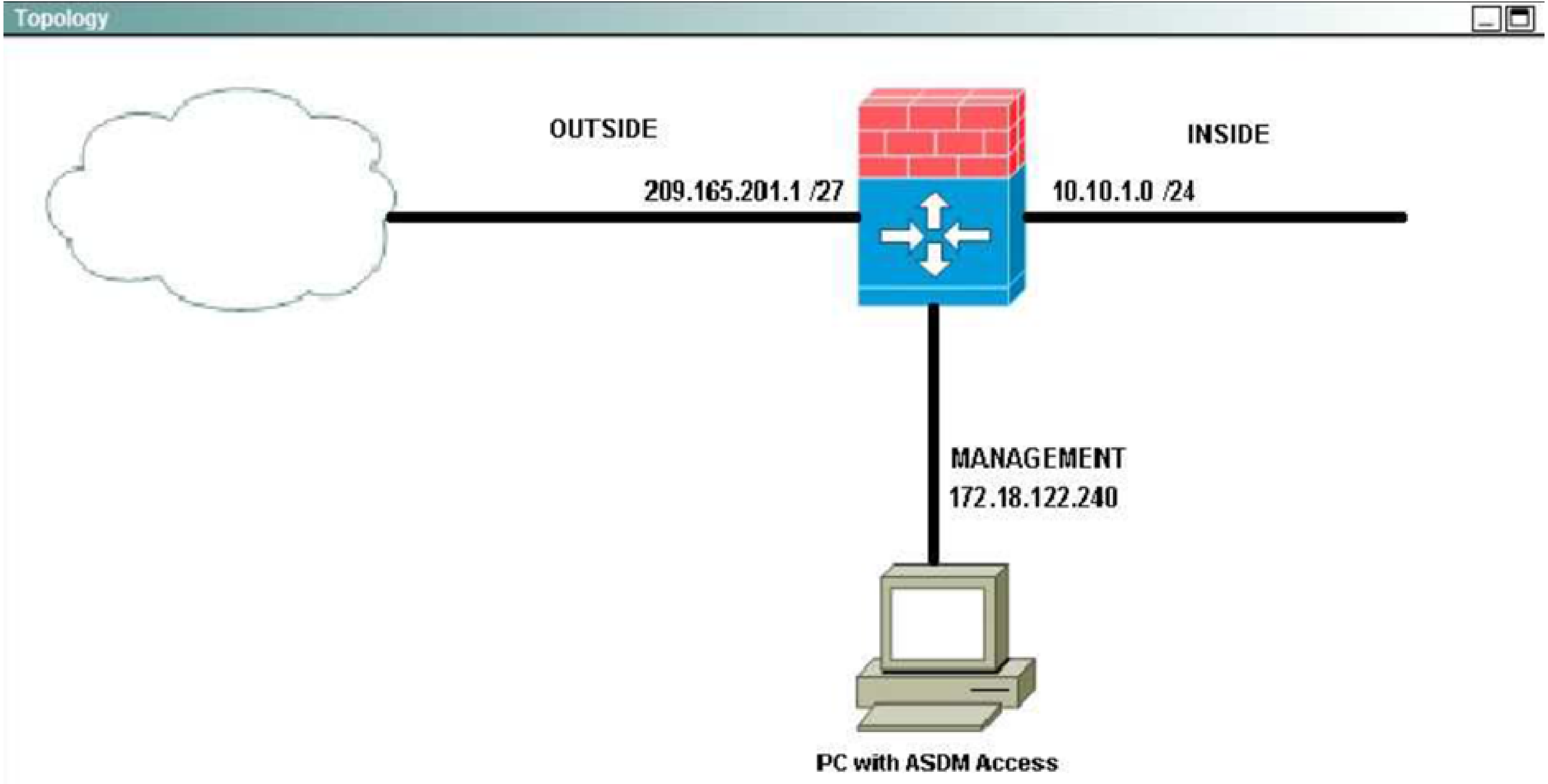
Answer: B

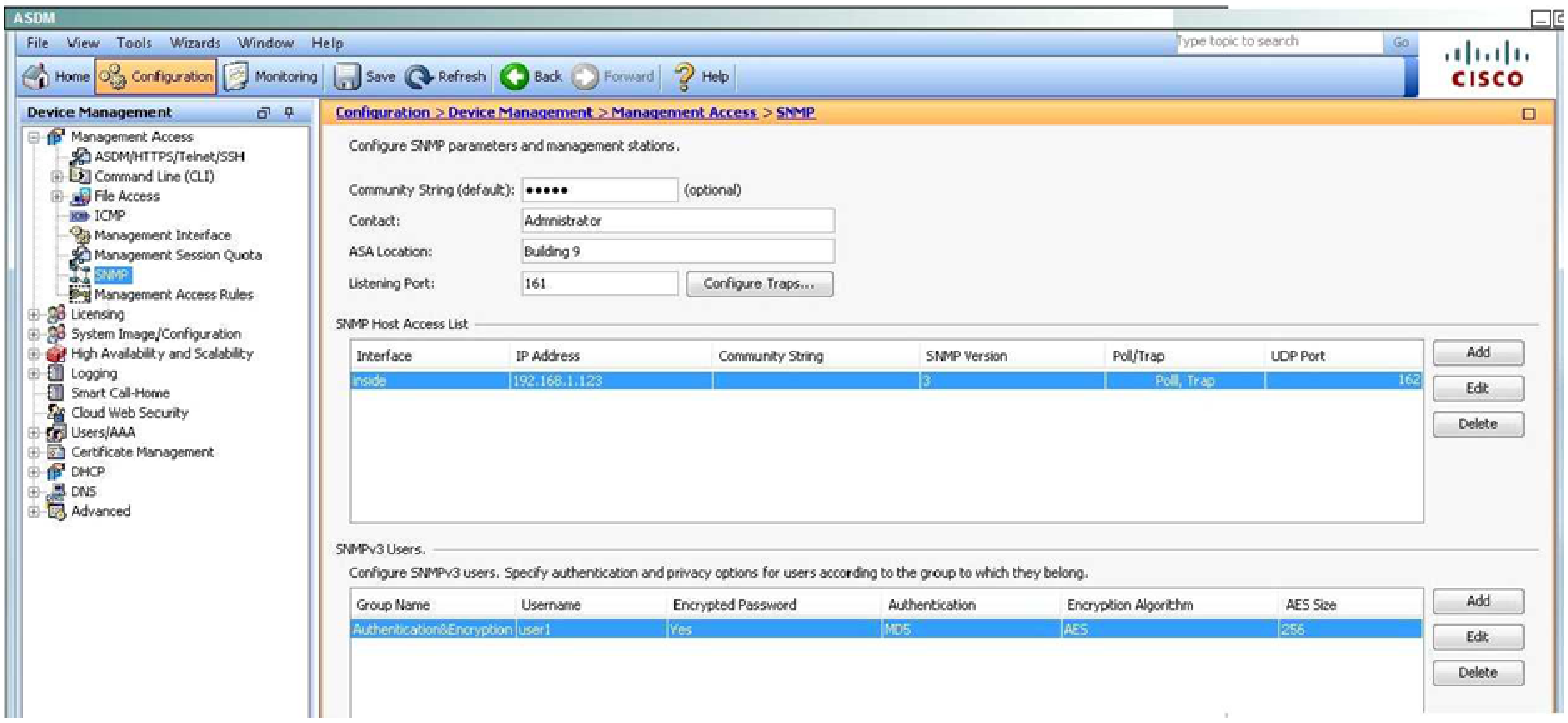
NEW QUESTION 192
Which command configures the SNMP server group1 to enable authentication for members of the access list east?

A. snmp-server group group1 v3 auth access east
B. snmp-server group1 v3 auth access east
C. snmp-server group group1 v3 east
D. snmp-server group1 v3 east access

Answer: A

NEW QUESTION 194





Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

Community String (default): ●●●●● (optional)
Contact: Administrator
ASA Location: Building 9
Listening Port: 161 Configure Traps...

SNMP Host Access List

Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.123		3	Poll, Trap	162

Add Edit Delete

SNMPv3 Users.

Configure SNMPv3 users. Specify authentication and privacy options for users according to the group to which they belong.

Group Name	Username	Encrypted Password	Authentication	Encryption Algorithm	AES Size
Authentication&Encryption	user1	Yes	MD5	AES	256

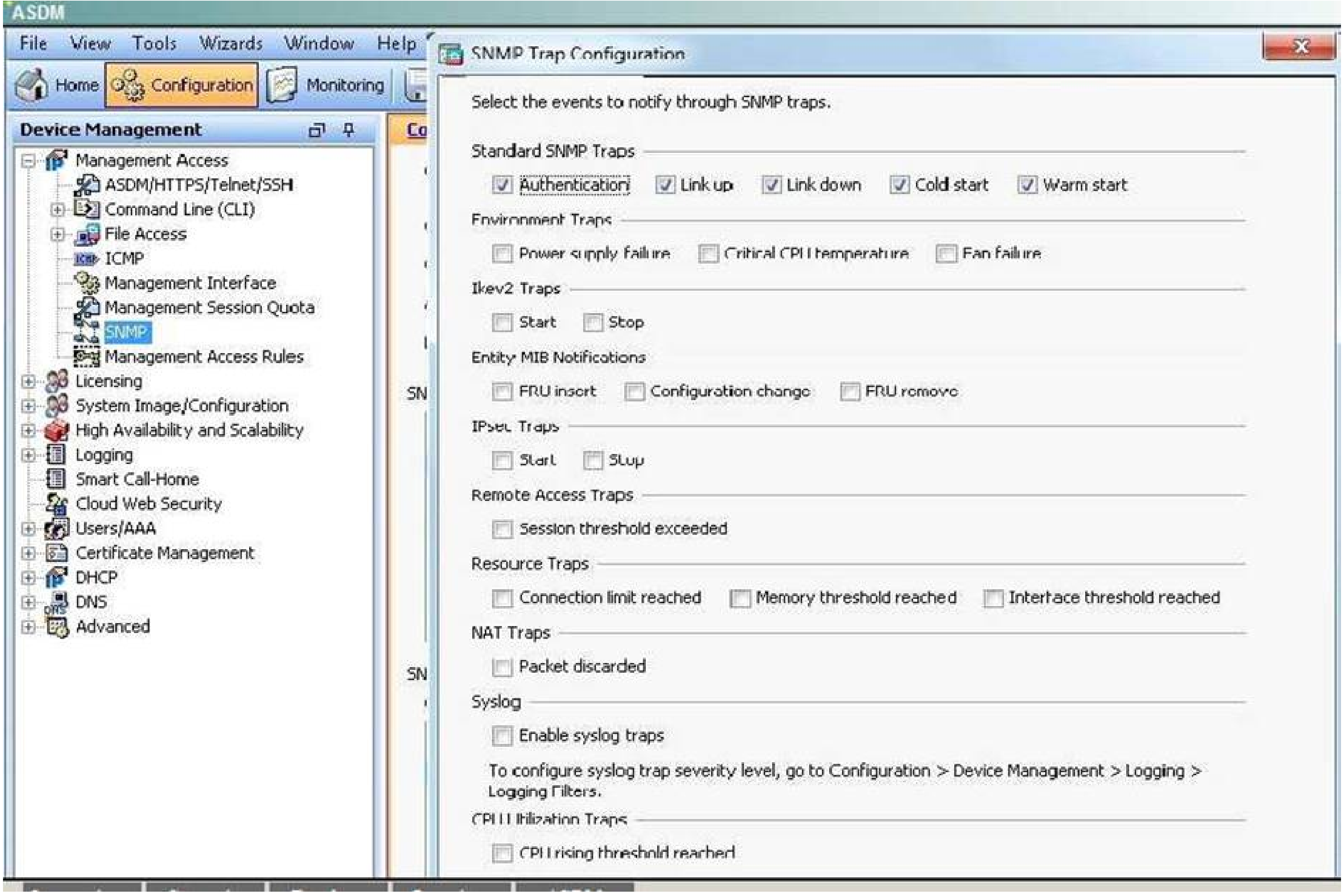
Add Edit Delete

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:



SNMP Trap Configuration

Select the events to notify through SNMP traps.

Standard SNMP Traps

☑ Authentication ☑ Link up ☑ Link down ☑ Cold start ☑ Warm start

Environment Traps

□ Power supply failure □ Critical CPU temperature □ Fan failure

Ikev2 Traps

□ Start □ Stop

Entity MIB Notifications

□ FRU insert □ Configuration change □ FRU remove

IPsec Traps

□ Start □ Stop

Remote Access Traps

□ Session threshold exceeded

Resource Traps

□ Connection limit reached □ Memory threshold reached □ Interface threshold reached

NAT Traps

□ Packet discarded

Syslog

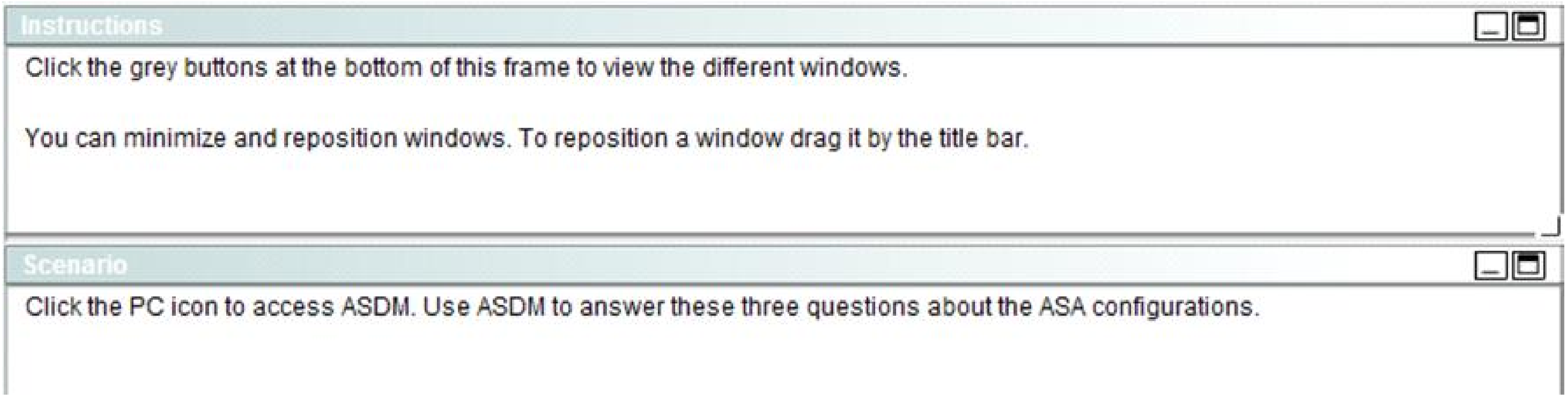
□ Enable syslog traps

To configure syslog trap severity level, go to Configuration > Device Management > Logging > Logging Filters.

CPU Utilization Traps

□ CPU rising threshold reached

NEW QUESTION 196



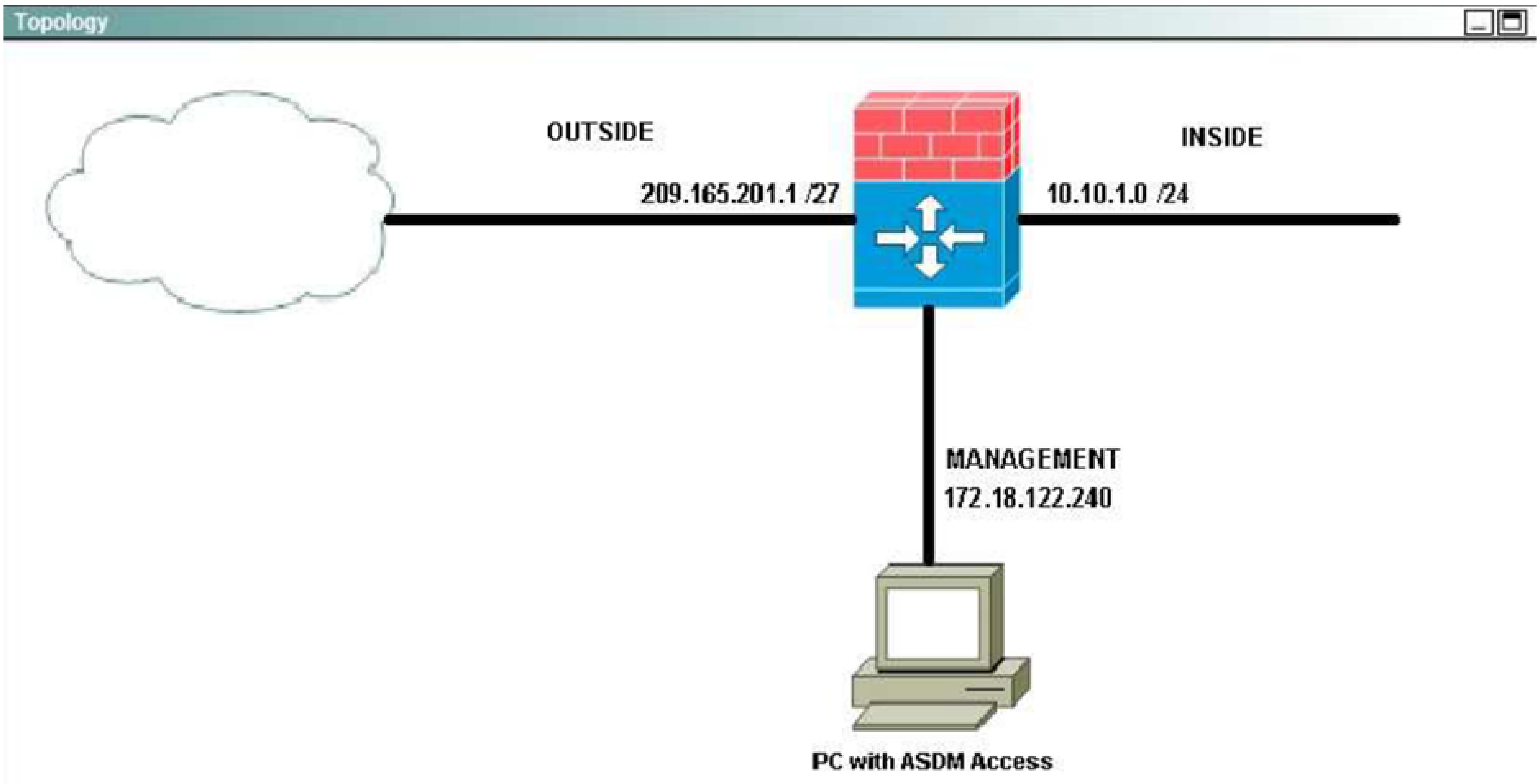
Instructions

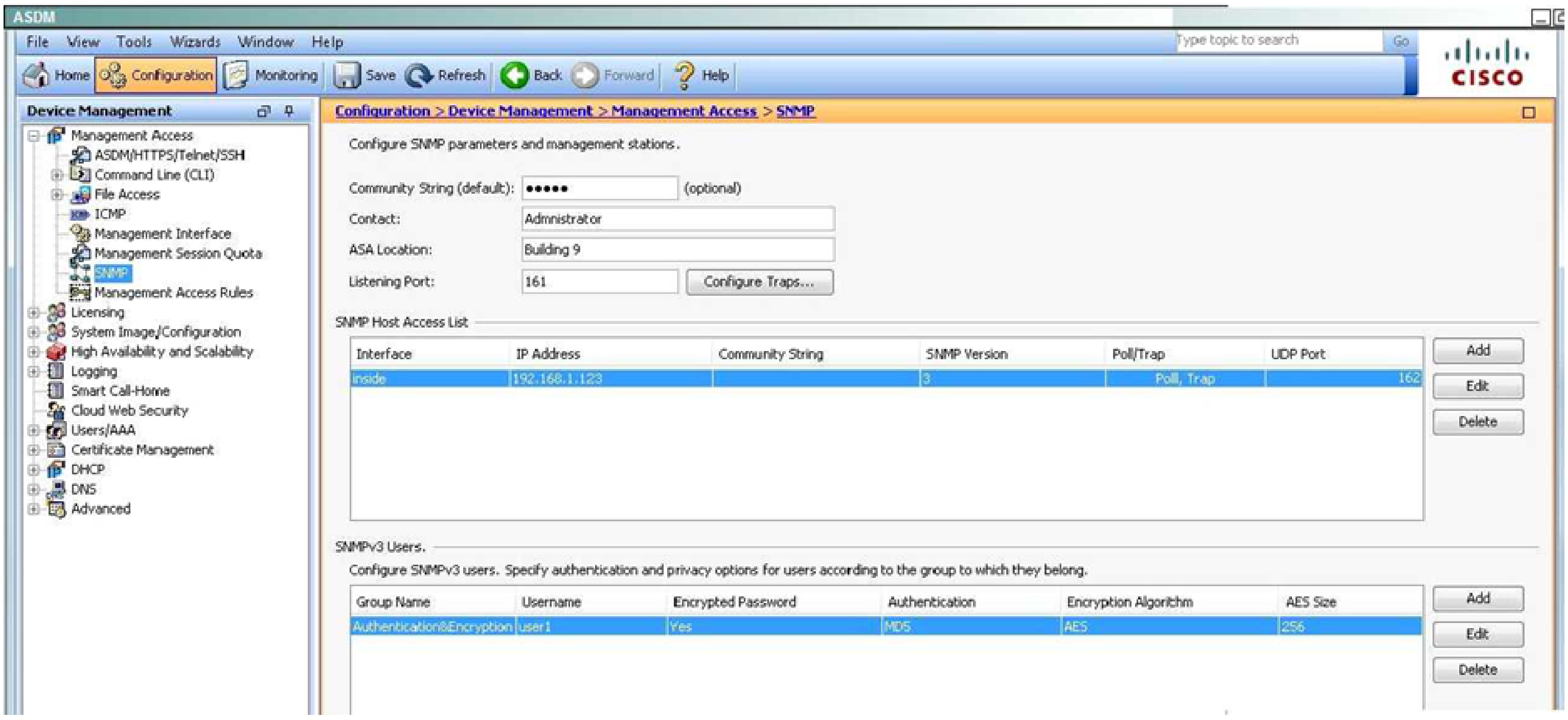
Click the grey buttons at the bottom of this frame to view the different windows.

You can minimize and reposition windows. To reposition a window drag it by the title bar.

Scenario

Click the PC icon to access ASDM. Use ASDM to answer these three questions about the ASA configurations.





Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

Community String (default): ●●●●● (optional)

Contact: Administrator

ASA Location: Building 9

Listening Port: 161 Configure Traps...

SNMP Host Access List

Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.123		3	Poll, Trap	162

SNMPv3 Users.

Configure SNMPv3 users. Specify authentication and privacy options for users according to the group to which they belong.

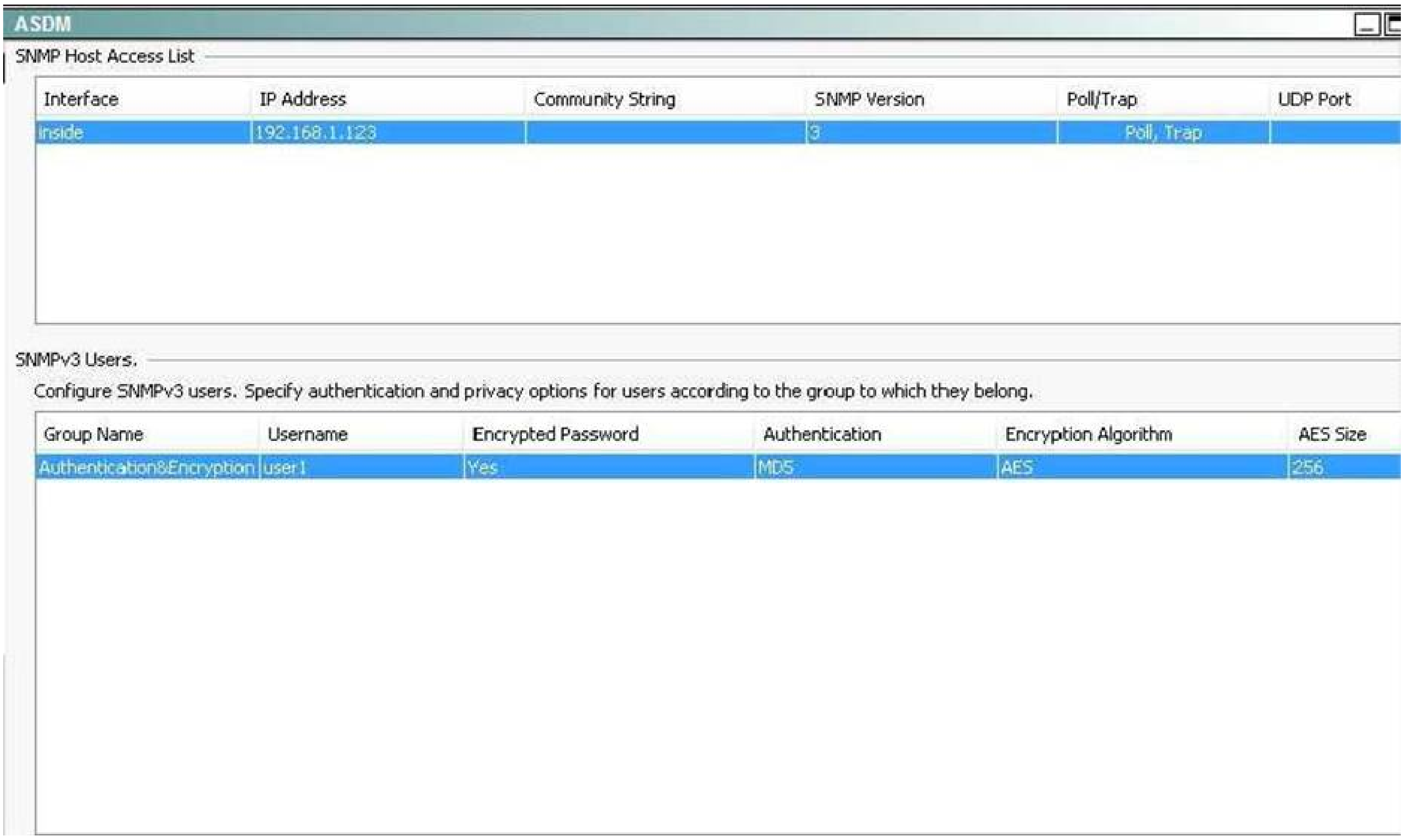
Group Name	Username	Encrypted Password	Authentication	Encryption Algorithm	AES Size
Authentication&Encryption	user1	Yes	MD5	AES	256

SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SH

A. The encryption algorithm options are DES, 3DES, andAES (which is available in 128,192, and 256 versions). When you create a user, with which option must you associate it?
B. an SNMP group
C. at least one interface
D. the SNMP inspection in the global_policy
E. at least two interfaces

Answer: A

Explanation: This can be verified via the ASDM screen shot shown here:



SNMP Host Access List

Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.123		3	Poll, Trap	

SNMPv3 Users.

Configure SNMPv3 users. Specify authentication and privacy options for users according to the group to which they belong.

Group Name	Username	Encrypted Password	Authentication	Encryption Algorithm	AES Size
Authentication&Encryption	user1	Yes	MD5	AES	256

NEW QUESTION 200
Which command tests authentication with SSH and shows a generated key?

A. show key mypubkey rsa
B. show crypto key mypubkey rsa
C. show crypto key
D. show key mypubkey

Answer: B

NEW QUESTION 204
In IOS routers, what configuration can ensure both prevention of ntp spoofing and accurate time ensured?

A. ACL permitting udp 123 from ntp server
B. ntp authentication
C. multiple ntp servers
D. local system clock

Answer: B

NEW QUESTION 208
Which product can manage licenses, updates, and a single signature policy for 15 separate IPS appliances?

A. Cisco Security Manager
B. Cisco IPS Manager Express
C. Cisco IPS Device Manager
D. Cisco Adaptive Security Device Manager

Answer: A

NEW QUESTION 213
On an ASA running version 9.0, which command is used to nest objects in a pre-existing group?

A. object-group
B. network group-object
C. object-group network
D. group-object

Answer: D

NEW QUESTION 215
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 219
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 224
You are the administrator of a Cisco ASA 9.0 firewall and have been tasked with ensuring that the
Firewall Admins Active Directory group has full access to the ASA configuration. The Firewall Operators Active Directory group should have a more limited level of access.
Which statement describes how to set these access levels?

A. Use Cisco Directory Agent to configure the Firewall Admins group to have privilege level 15 acces
B. Alsoconfigure the Firewall Operators group to have privilege level 6 access.
C. Use TACACS+ for Authentication and Authorization into the Cisco ASA CLI, with ACS as the AAA server.Configure ACS CLI command authorization sets for the Firewall Operators grou
D. Configure level 15 access to be assigned to members of the Firewall Admins group.
E. Use RADIUS for Authentication and Authorization into the Cisco ASA CLI, with ACS as the AAA server.Configure ACS CLI command authorization sets for the Firewall Operators grou
F. Configure level 15 access to be assigned to members of the Firewall Admins group.
G. Active Directory Group membership cannot be used as a determining factor for accessing the Cisco ASACLI.

Answer: B

NEW QUESTION 226
Which two configurations are necessary to enable password-less SSH login to an IOS router? (Choose two.)

A. Enter a copy of the administrator's public key within the SSH key-chain
B. Enter a copy of the administrator's private key within the SSH key-chain
C. Generate a 512-bit RSA key to enable SSH on the router
D. Generate an RSA key of at least 768 bits to enable SSH on the router
E. Generate a 512-bit ECDSA key to enable SSH on the router
F. Generate a ECDSA key of at least 768 bits to enable SSH on the router

Answer: AD

NEW QUESTION 231
Which two features does Cisco Security Manager provide? (Choose two.)

A. Configuration and policy deployment before device discovery
B. Health and performance monitoring
C. Event management and alerting
D. Command line menu for troubleshooting
E. Ticketing management and tracking

Answer: BC

NEW QUESTION 232
An administrator installed a Cisco ASA that runs version 9.1. You are asked to configure the firewall
through Cisco ASDM.
When you attempt to connect to a Cisco ASA with a default configuration, which username and password grants you full access?

A. admin / admin
B. asaAdmin / (no password)
C. It is not possible to use Cisco ASDM until a username and password are created via the usernameusernamepassword password CLI command.
D. enable_15 / (no password)
E. cisco / cisco

Answer: D

NEW QUESTION 236
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 240
Which two options are purposes of the packet-tracer command? (Choose two.)

A. to filter and monitor ingress traffic to a switch
B. to configure an interface-specific packet trace
C. to simulate network traffic through a data path
D. to debug packet drops in a production network
E. to automatically correct an ACL entry in an ASA

Answer: CD

NEW QUESTION 245
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 249
A rogue device has connected to the network and has become the STP root bridge, which has caused a network availability issue.
Which two commands can protect against this problem? (Choose two.)

A. switch(config)#spanning-tree portfast bpduguard default
B. switch(config)#spanning-tree portfast bpdufilter default
C. switch(config-if)#spanning-tree portfast
D. switch(config-if)#spanning-tree portfast disable
E. switch(config-if)#switchport port-security violation protect
F. switch(config-if)#spanning-tree port-priority 0

Answer: AC

NEW QUESTION 250
According to Cisco best practices, which two interface configuration commands help prevent VLAN hopping attacks? (Choose two.)

A. switchport mode access
B. switchport access vlan 2
C. switchport mode trunk
D. switchport access vlan 1
E. switchport trunk native vlan 1
F. switchport protected

Answer: AB

NEW QUESTION 251
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 252
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

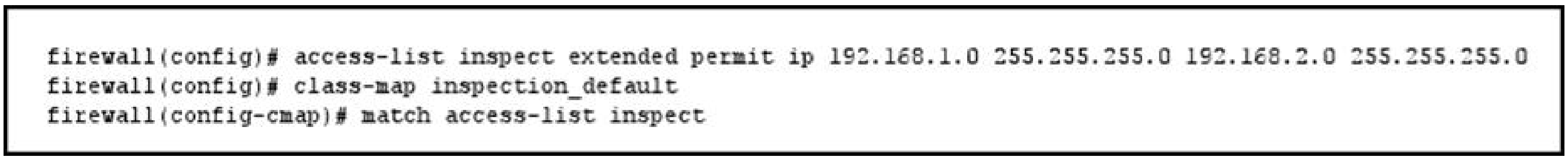
Answer: A

NEW QUESTION 256
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 258
Refer to the exhibit.



```
firewall(config)# access-list inspect extended permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
firewall(config)# class-map inspection_default
firewall(config-cmap)# match access-list inspect
```

What is the effect of this configuration?

A. The firewall will inspect IP traffic only between networks 192.168.1.0 and 192.168.2.0.
B. The firewall will inspect all IP traffic except traffic to 192.168.1.0 and 192.168.2.0.
C. The firewall will inspect traffic only if it is defined within a standard ACL.
D. The firewall will inspect all IP traffic.

Answer: A

NEW QUESTION 261
Which feature can suppress packet flooding in a network?

A. PortFast
B. BPDU guard
C. Dynamic ARP Inspection
D. storm control

Answer: D

NEW QUESTION 266
What is the default violation mode that is applied by port security?

A. restrict
B. protect
C. shutdown
D. shutdown VLAN

Answer: C

NEW QUESTION 270
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 273
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 275
What are three of the RBAC views within Cisco IOS Software? (Choose three.)

A. Admin
B. CLI
C. Root
D. Super Admin
E. Guest
F. Super

Answer: BCF

NEW QUESTION 280
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 285
Which statement about Cisco Security Manager form factors is true?

A. Cisco Security Manager Professional and Cisco Security Manager UCS Server Bundles support FWSMs.
B. Cisco Security Manager Standard and Cisco Security Manager Professional support FWSMs.
C. Only Cisco Security Manager Professional supports FWSMs.
D. Only Cisco Security Manager Standard supports FWSMs.

Answer: A

NEW QUESTION 290
Which Cisco Security Manager form factor is recommended for deployments with fewer than 25 devices?

A. only Cisco Security Manager Standard
B. only Cisco Security Manager Professional
C. only Cisco Security Manager UCS Server Bundle
D. both Cisco Security Manager Standard and Cisco Security Manager Professional

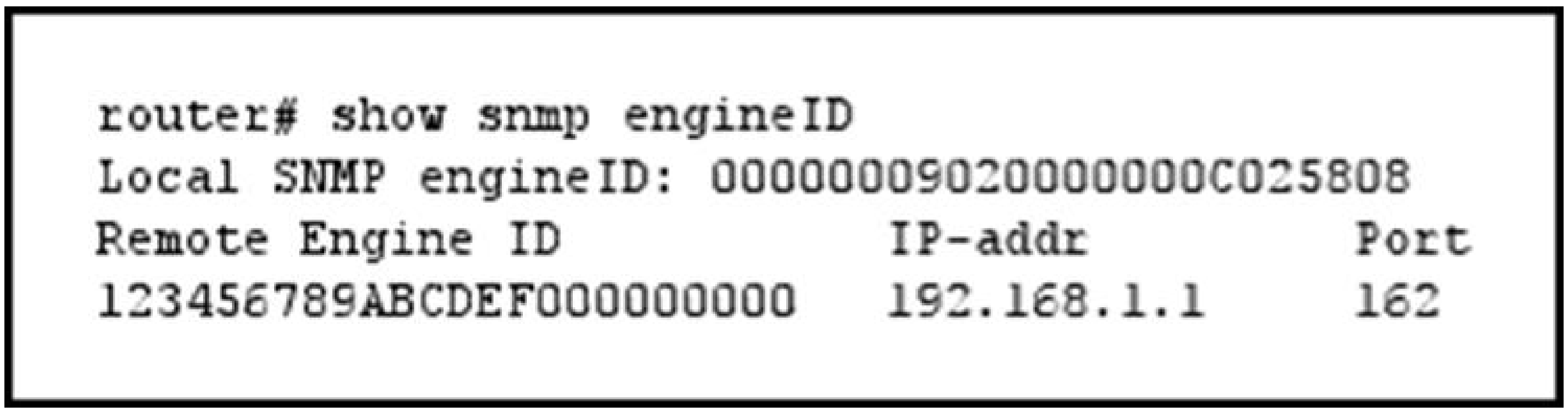
Answer: A

NEW QUESTION 295
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 297
Refer to the exhibit.



```
router# show snmp engineID
Local SNMP engineID: 00000009020000000C025808
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.

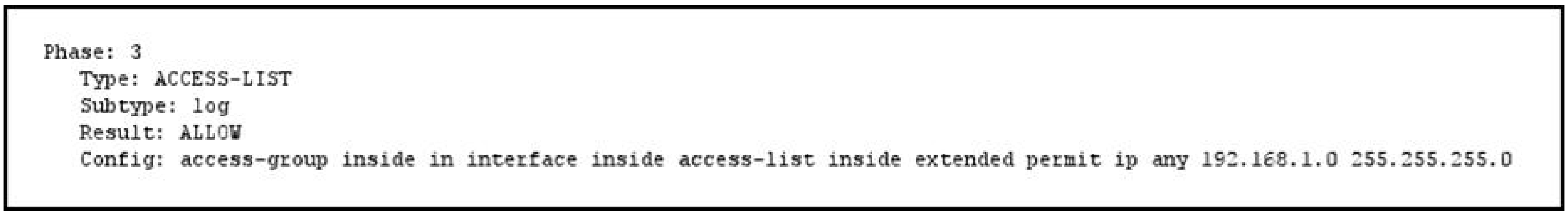
Answer: BD

NEW QUESTION 301
To which port does a firewall send secure logging messages?

A. TCP/1500
B. UDP/1500
C. TCP/500
D. UDP/500

Answer: A

NEW QUESTION 303
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 306
A Cisco ASA is configured in multiple context mode and has two user-defined contexts-- Context_A and Context_B. From which context are device logging messages sent?

A. Admin
B. Context_A
C. Context_B
D. System

Answer: A

NEW QUESTION 308
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 309
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 312
In a Cisco ASAv failover deployment, which interface is preconfigured as the failover interface?

A. GigabitEthernet0/2
B. GigabitEthernet0/4
C. GigabitEthernet0/6
D. GigabitEthernet0/8

Answer: D

NEW QUESTION 313
Which VTP mode supports private VLANs on a switch?

A. transparent

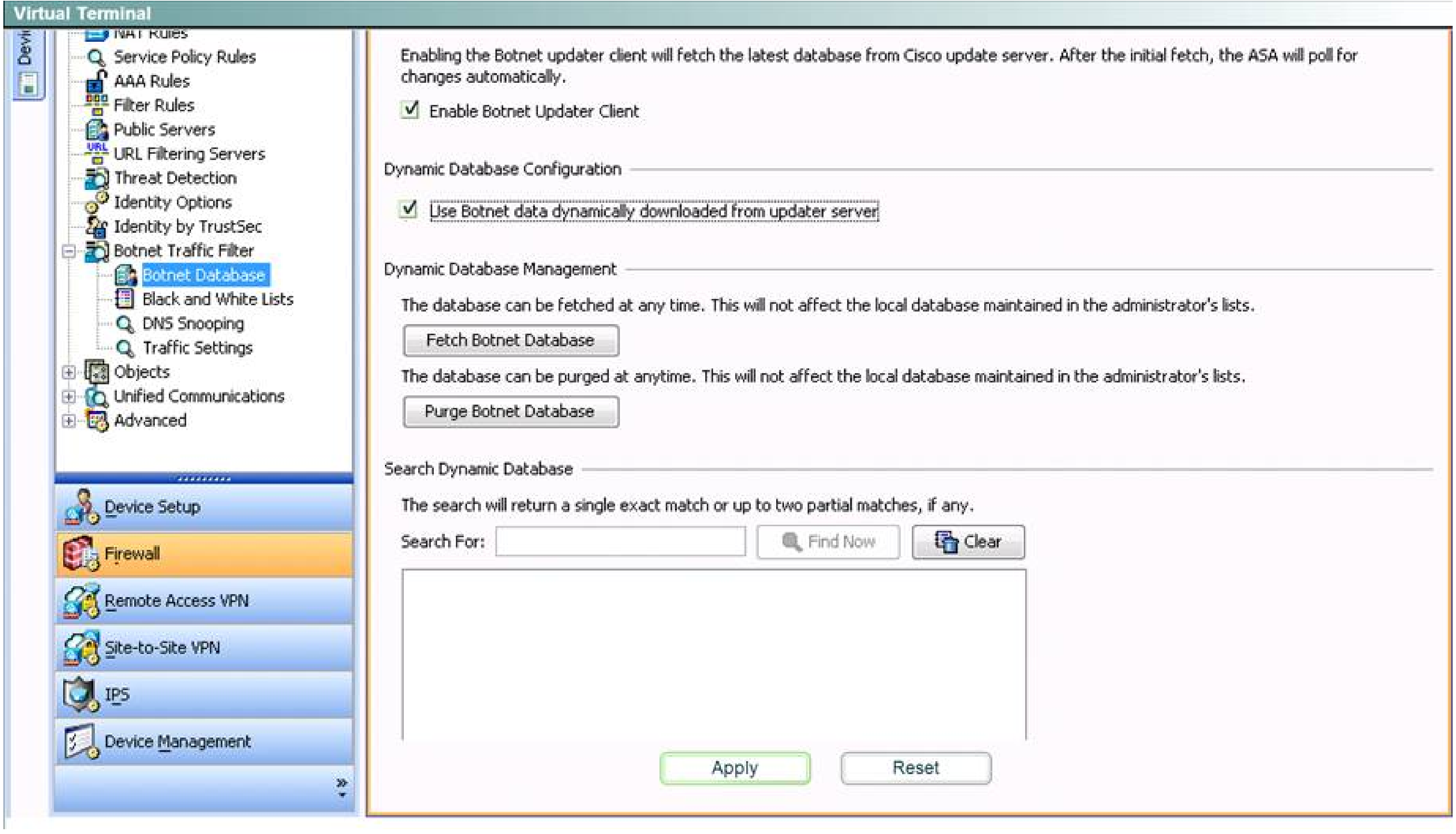
B. server
C. client
D. off

Answer: A

NEW QUESTION 318
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:



Enabling the Botnet updater client will fetch the latest database from Cisco update server. After the initial fetch, the ASA will poll for changes automatically.

☑ Enable Botnet Updater Client

Dynamic Database Configuration

☑ Use Botnet data dynamically downloaded from updater server

Dynamic Database Management

The database can be fetched at any time. This will not affect the local database maintained in the administrator's lists.

Fetch Botnet Database

The database can be purged at anytime. This will not affect the local database maintained in the administrator's lists.

Purge Botnet Database

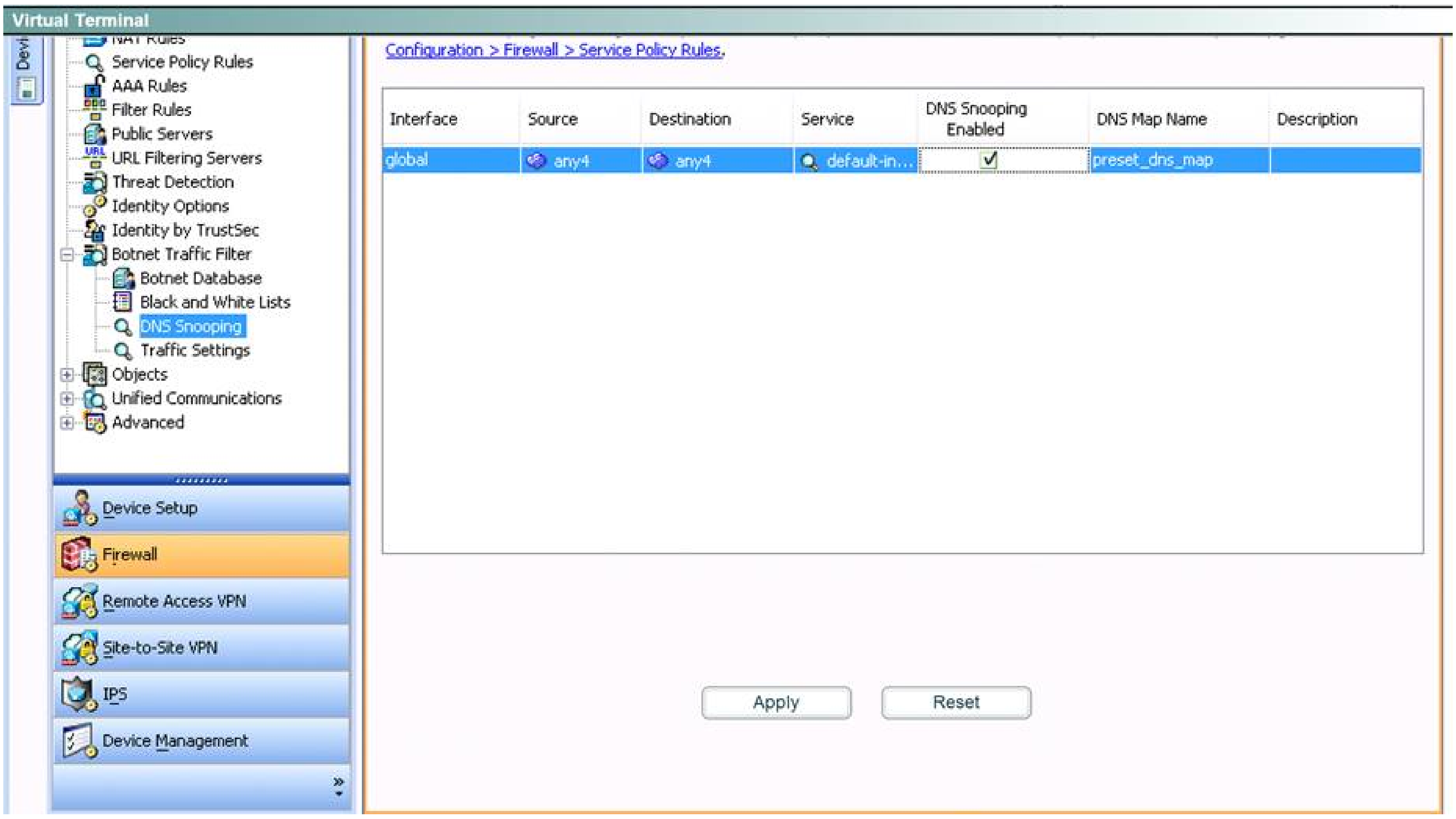
Search Dynamic Database

The search will return a single exact match or up to two partial matches, if any.

Search For: Find Now Clear

Apply Reset

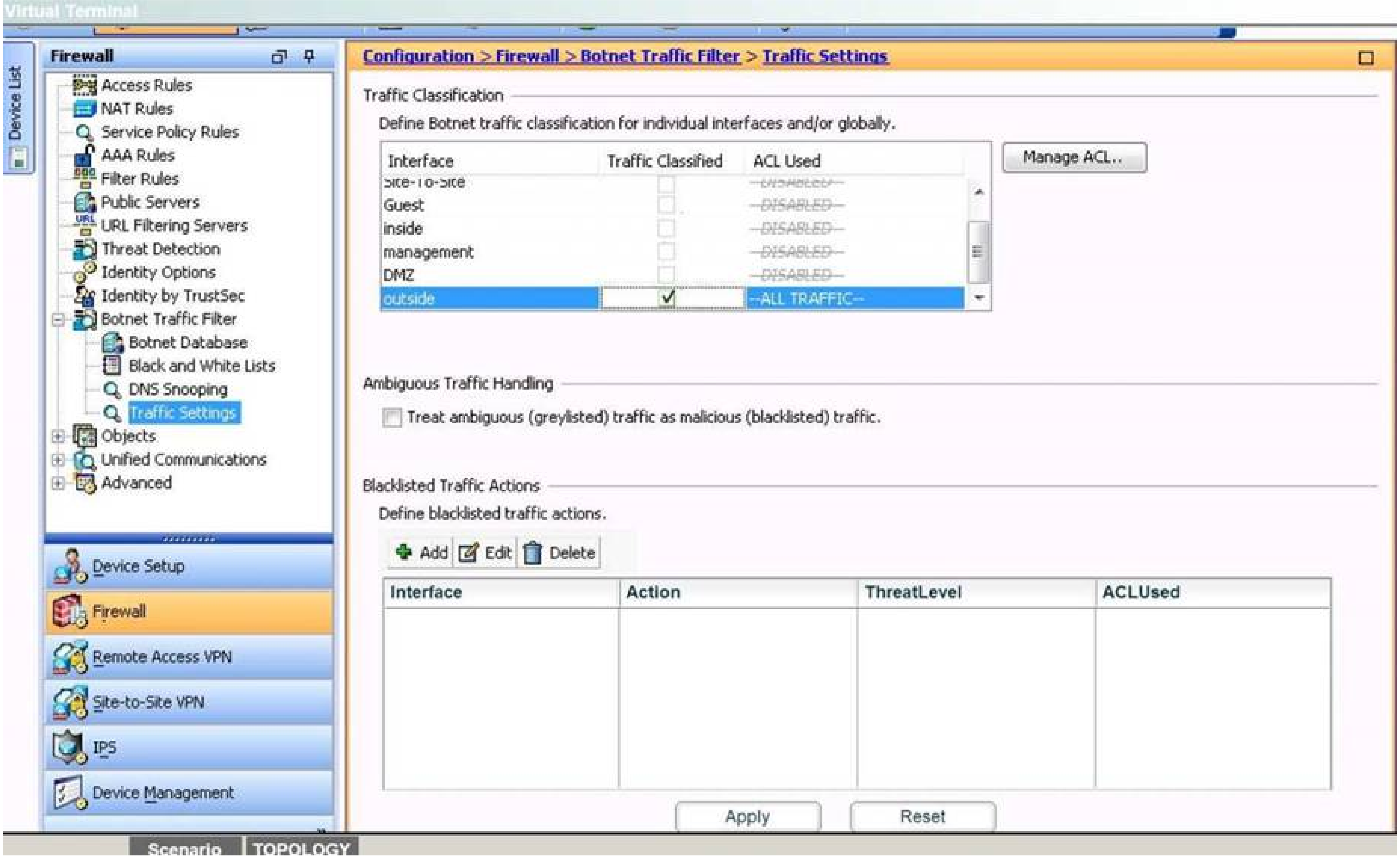
Click Yes to send the commands when prompted.
Then, click on the box on the DNS Snooping page as shown below and hit apply:



Configuration > Firewall > Service Policy Rules.

Interface	Source	Destination	Service	DNS Snooping Enabled	DNS Map Name	Description
global	any4	any4	default-in...	☑	preset_dns_map	

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



Configuration > Firewall > Botnet Traffic Filter > Traffic Settings

Traffic Classification

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

Interface	Traffic Classified	ACL Used
Site-To-Site	□	~~DISABLED~~
Guest	□	~~DISABLED~~
inside	□	~~DISABLED~~
management	□	~~DISABLED~~
DMZ	□	~~DISABLED~~
outside	☑	--ALL TRAFFIC--

Ambiguous Traffic Handling

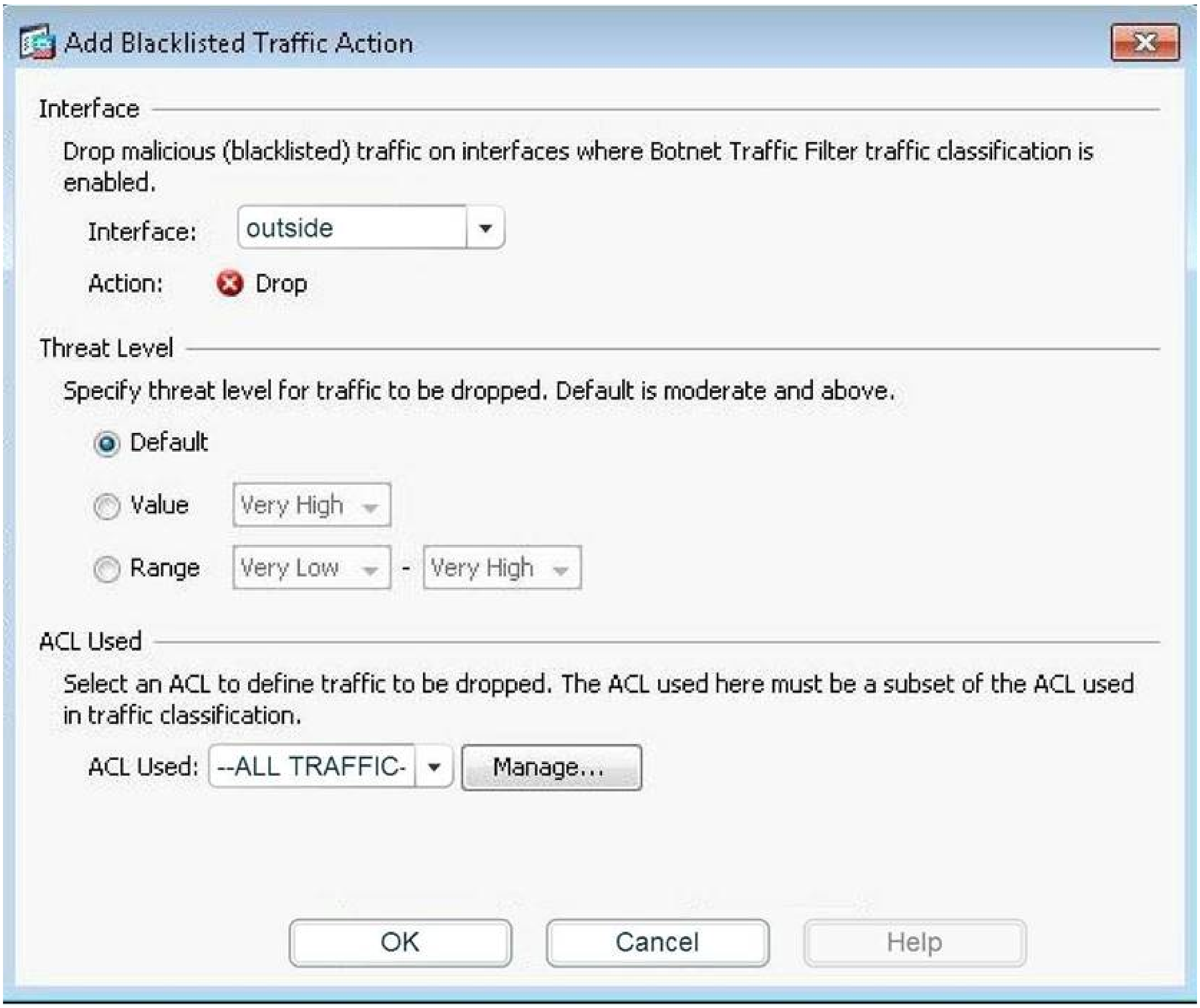
□ Treat ambiguous (greylisted) traffic as malicious (blacklisted) traffic.

Blacklisted Traffic Actions

Define blacklisted traffic actions.

Interface	Action	ThreatLevel	ACLUsed

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



Add Blacklisted Traffic Action

Interface

Drop malicious (blacklisted) traffic on interfaces where Botnet Traffic Filter traffic classification is enabled.

Interface: outside

Action: Drop

Threat Level

Specify threat level for traffic to be dropped. Default is moderate and above.

● Default

○ Value Very High

○ Range Very Low - Very High

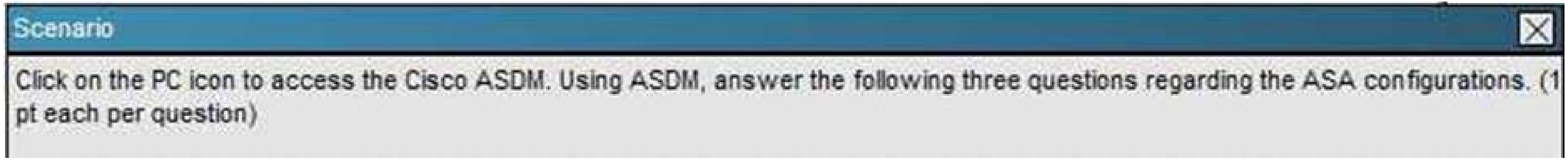
ACL Used

Select an ACL to define traffic to be dropped. The ACL used here must be a subset of the ACL used in traffic classification.

ACL Used: --ALL TRAFFIC-

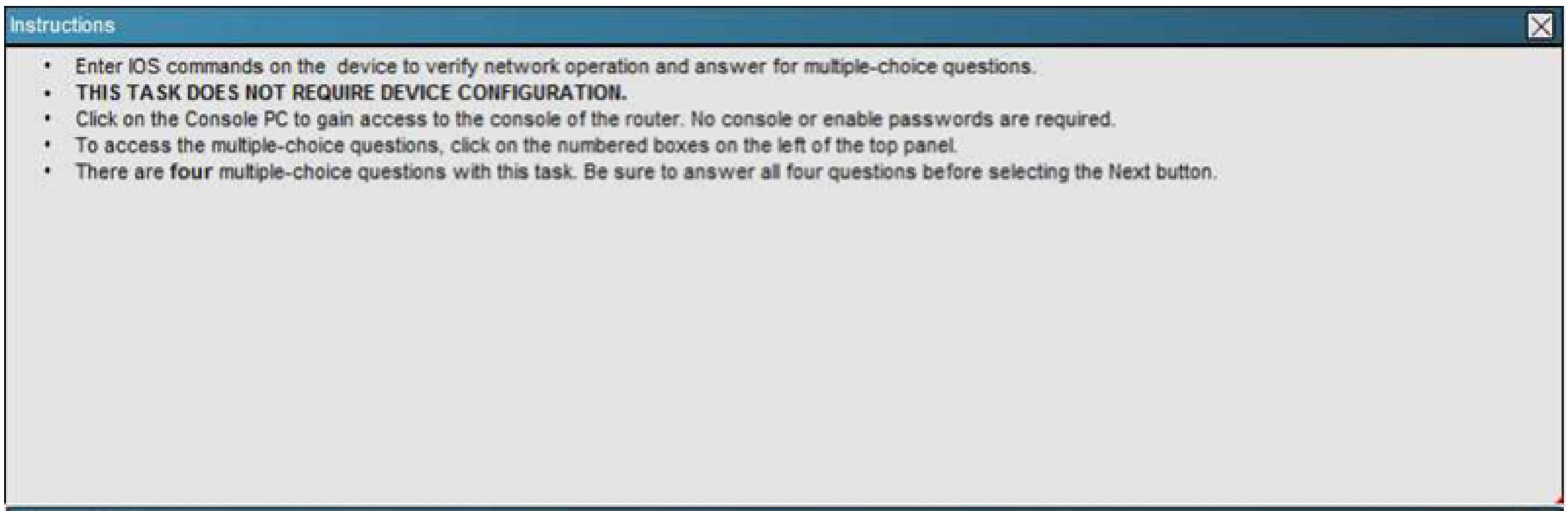
Click OK. Then Apply. Then Send when prompted.
Then verify that all is working according to the instructions given in the question.

NEW QUESTION 322



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.

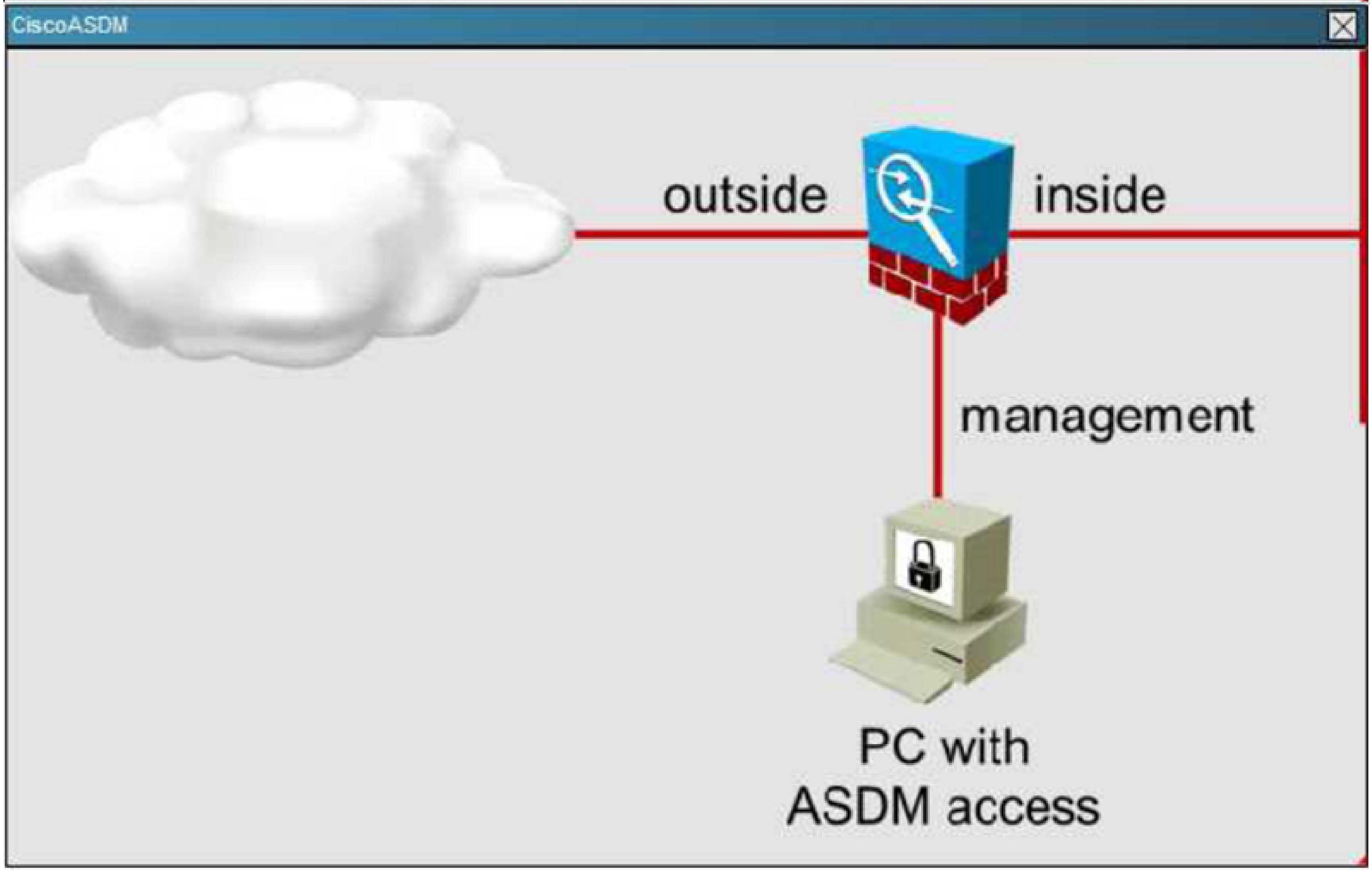
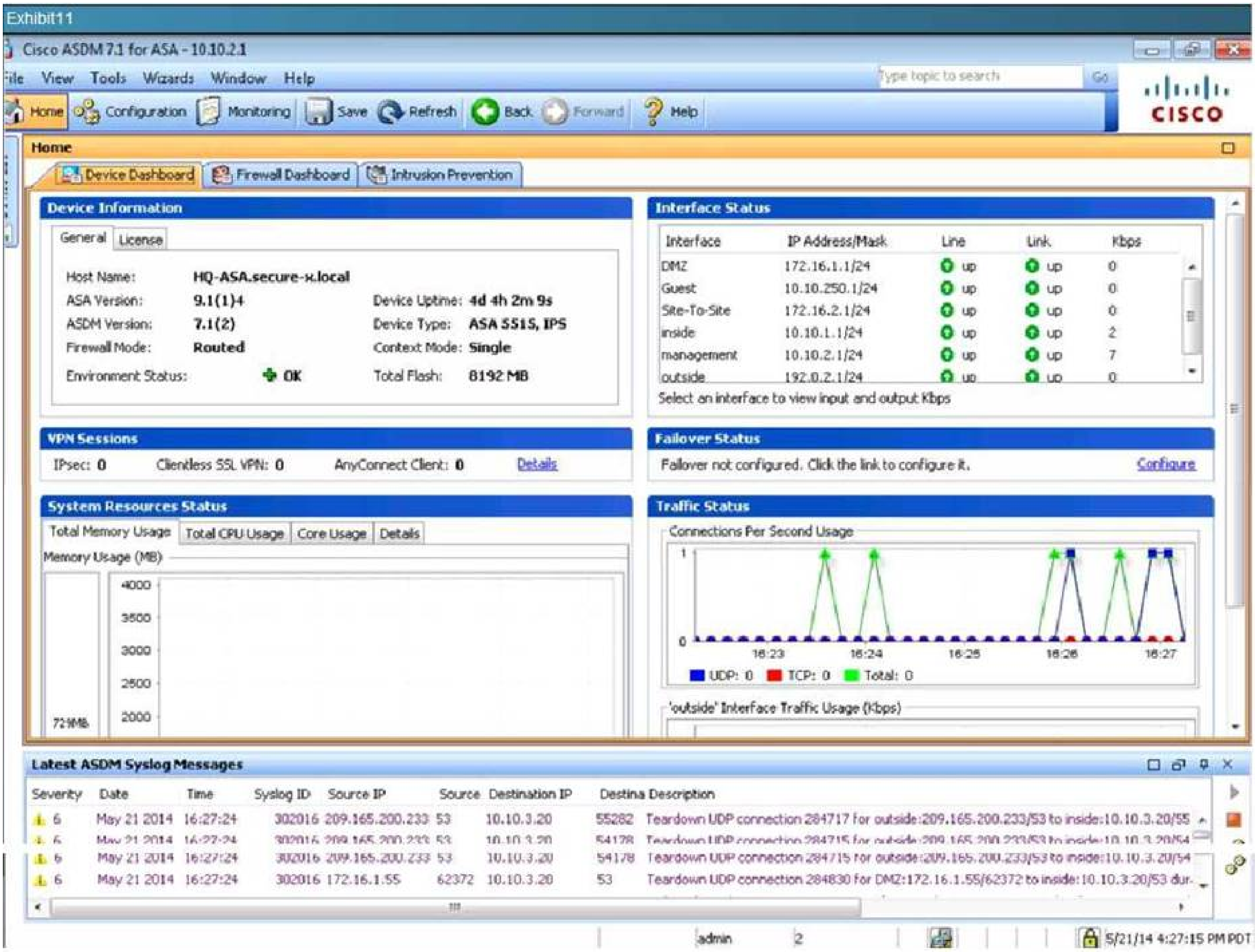


Exhibit11



Device Information

Host Name: HQ-ASA.secure-x.local
ASA Version: 9.1(1)4
ASDM Version: 7.1(2)
Firewall Mode: Routed
Environment Status: OK
Device Uptime: 4d 4h 2m 9s
Device Type: ASA 5515, IPS
Context Mode: Single
Total Flash: 8192 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
DMZ	172.16.1.1/24	up	up	0
Guest	10.10.250.1/24	up	up	0
Site-To-Site	172.16.2.1/24	up	up	0
inside	10.10.1.1/24	up	up	2
management	10.10.2.1/24	up	up	7
outside	192.0.2.1/24	up	up	0

VPN Sessions

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

Failover Status

Failover not configured. Click the link to configure it.

System Resources Status

Traffic Status

UDP: 0 TCP: 0 Total: 0

Latest ASDM Syslog Messages

```
Severity Date        Time     Syslog ID Source IP       Source Destination IP Destina Description
6        May 21 2014 16:27:24 302016    209.165.200.233 53     10.10.3.20     55282   Teardown UDP connection 284717 for outside:209.165.200.233/53 to inside:10.10.3.20/55
6        May 21 2014 16:27:24 302016    209.165.200.233 53     10.10.3.20     54178   Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6        May 21 2014 16:27:24 302016    172.16.1.55     62372  10.10.3.20     53      Teardown UDP connection 284830 for DMZ:172.16.1.55/62372 to inside:10.10.3:20/53 dur.
```

In your role as network security administrator, you have installed syslog server software on a server whose IP address is 10.10.2.40. According to the exhibits, why isn't the syslog server receiving any syslog messages?

A. Logging is not enabled globally on the Cisco ASA.
B. The syslog server has failed.
C. There have not been any events with a severity level of seven.
D. The Cisco ASA is not configured to log messages to the syslog server at that IP address.

Answer: B

Explanation: By process of elimination, we know that the other answers choices are not correct so that only leaves us with the server must have failed. We can see from the following screen shots, that events are being generated with severity level of debugging and below, The 10.10.2.40 IP address has been configured as a syslog server, and that logging has been enabled globally:

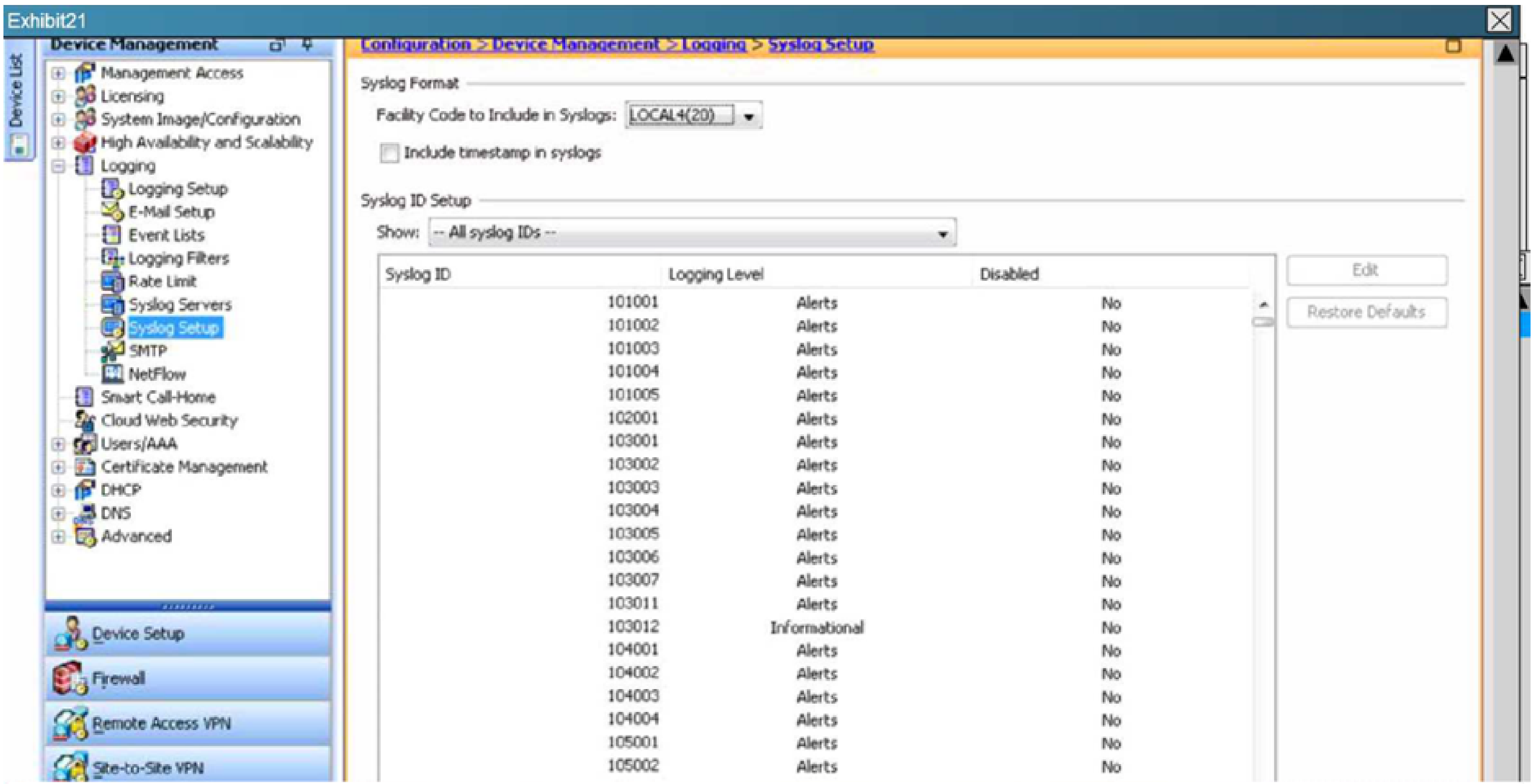


Exhibit21

Configuration > Device Management > Logging > Syslog Setup

Syslog Format

Facility Code to Include in Syslogs: LOCAL4(20)

□ Include timestamp in syslogs

Syslog ID Setup

Show: -- All syslog IDs --

Syslog ID	Logging Level	Disabled
101001	Alerts	No
101002	Alerts	No
101003	Alerts	No
101004	Alerts	No
101005	Alerts	No
102001	Alerts	No
103001	Alerts	No
103002	Alerts	No
103003	Alerts	No
103004	Alerts	No
103005	Alerts	No
103006	Alerts	No
103007	Alerts	No
103011	Alerts	No
103012	Informational	No
104001	Alerts	No
104002	Alerts	No
104003	Alerts	No
104004	Alerts	No
105001	Alerts	No
105002	Alerts	No

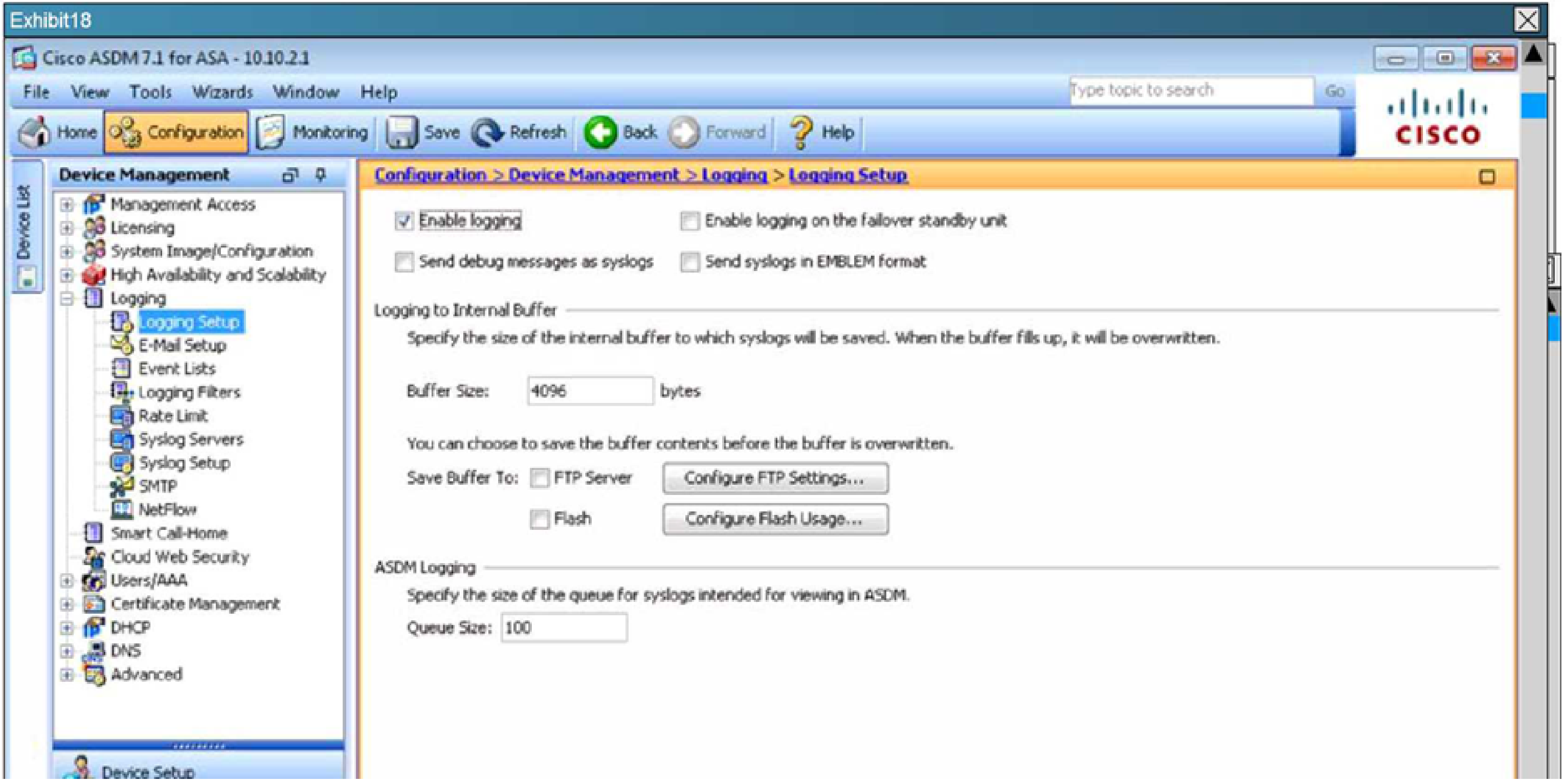


Exhibit18

Configuration > Device Management > Logging > Logging Setup

☑ Enable logging □ Enable logging on the failover standby unit

□ Send debug messages as syslogs □ Send syslogs in EMBLEM format

Logging to Internal Buffer

Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.

Buffer Size: 4096 bytes

You can choose to save the buffer contents before the buffer is overwritten.

Save Buffer To: □ FTP Server Configure FTP Settings...

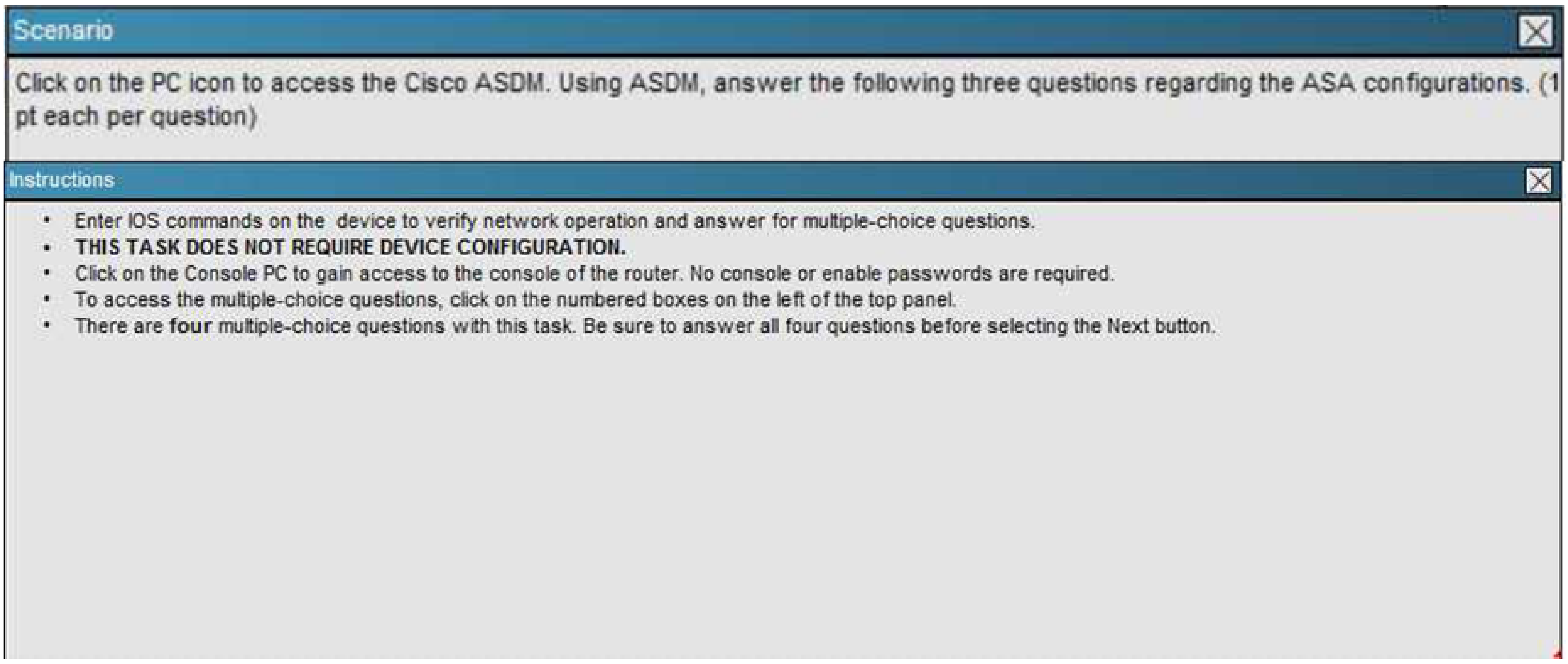
□ Flash Configure Flash Usage...

ASDM Logging

Specify the size of the queue for syslogs intended for viewing in ASDM.

Queue Size: 100

NEW QUESTION 326



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.

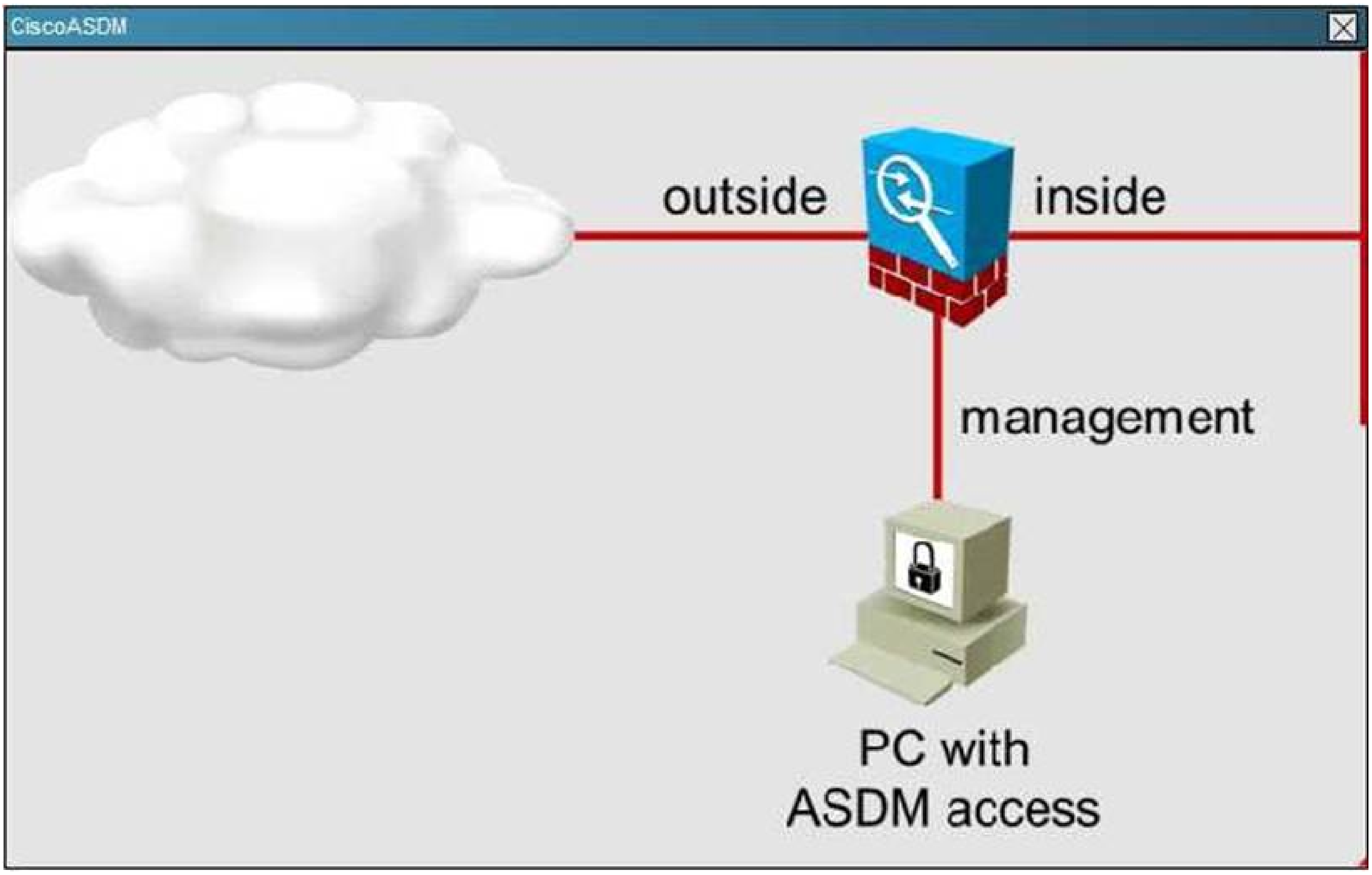
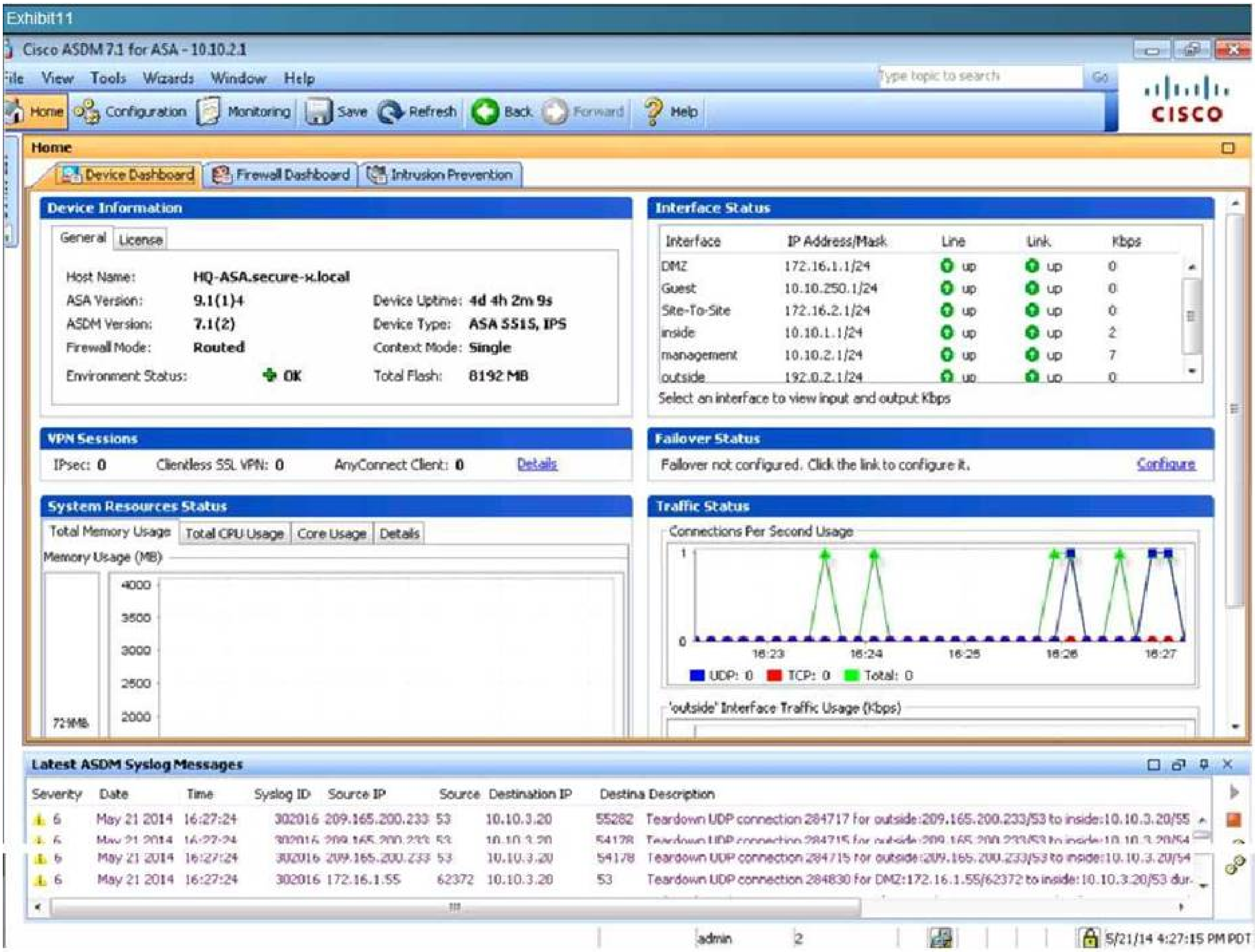


Exhibit11



Cisco ASDM 7.1 for ASA - 10.10.2.1

Device Information

General | License

Host Name: HQ-ASA.secure-x.local
ASA Version: 9.1(1)4
ASDM Version: 7.1(2)
Firewall Mode: Routed
Environment Status: OK
Device Uptime: 4d 4h 2m 9s
Device Type: ASA 5515, IPS
Context Mode: Single
Total Flash: 8192 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
DMZ	172.16.1.1/24	up	up	0
Guest	10.10.250.1/24	up	up	0
Site-To-Site	172.16.2.1/24	up	up	0
inside	10.10.1.1/24	up	up	2
management	10.10.2.1/24	up	up	7
outside	192.0.2.1/24	up	up	0

Select an interface to view input and output Kbps

VPN Sessions

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

Failover Status

Failover not configured. Click the link to configure it. Configure

System Resources Status

Total Memory Usage | Total CPU Usage | Core Usage | Details

Traffic Status

Connections Per Second Usage
1
0
16:23
16:24
16:25
16:26
16:27
UDP: 0
TCP: 0
Total: 0
'outside' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	55282	Teardown UDP connection 284717 for outside:209.165.200.233/53 to inside:10.10.3.20/55
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6	May 21 2014	16:27:24	302016	172.16.1.55	62372	10.10.3.20	53	Teardown UDP connection 284830 for DMZ:172.16.1.55/62372 to inside:10.10.3.20/53 dur-

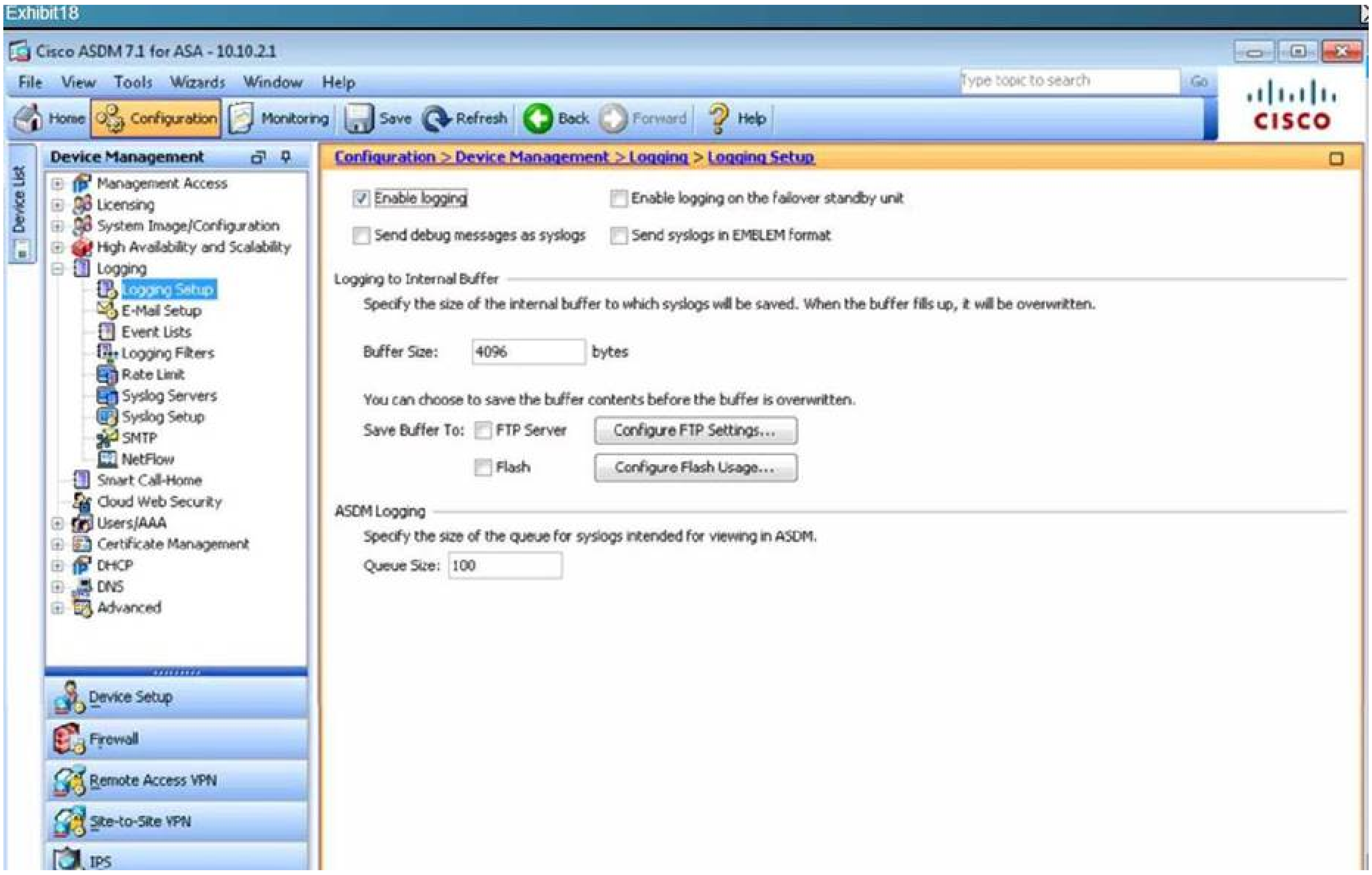
admin 2 5/21/14 4:27:15 PM PDT

Which statement is true of the logging configuration on the Cisco ASA?

A. The contents of the internal buffer will be saved to an FTP server before the buffer is overwritten.
B. The contents of the internal buffer will be saved to flash memory before the buffer is overwritten.
C. System log messages with a severity level of six and higher will be logged to the internal buffer.
D. System log messages with a severity level of six and lower will be logged to the internal buffer.

Answer: C

Explanation:



Configuration > Device Management > Logging > Logging Setup

☑ Enable logging
□ Enable logging on the failover standby unit
□ Send debug messages as syslogs
□ Send syslogs in EMBLEM format

Logging to Internal Buffer

Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.

Buffer Size: 4096 bytes

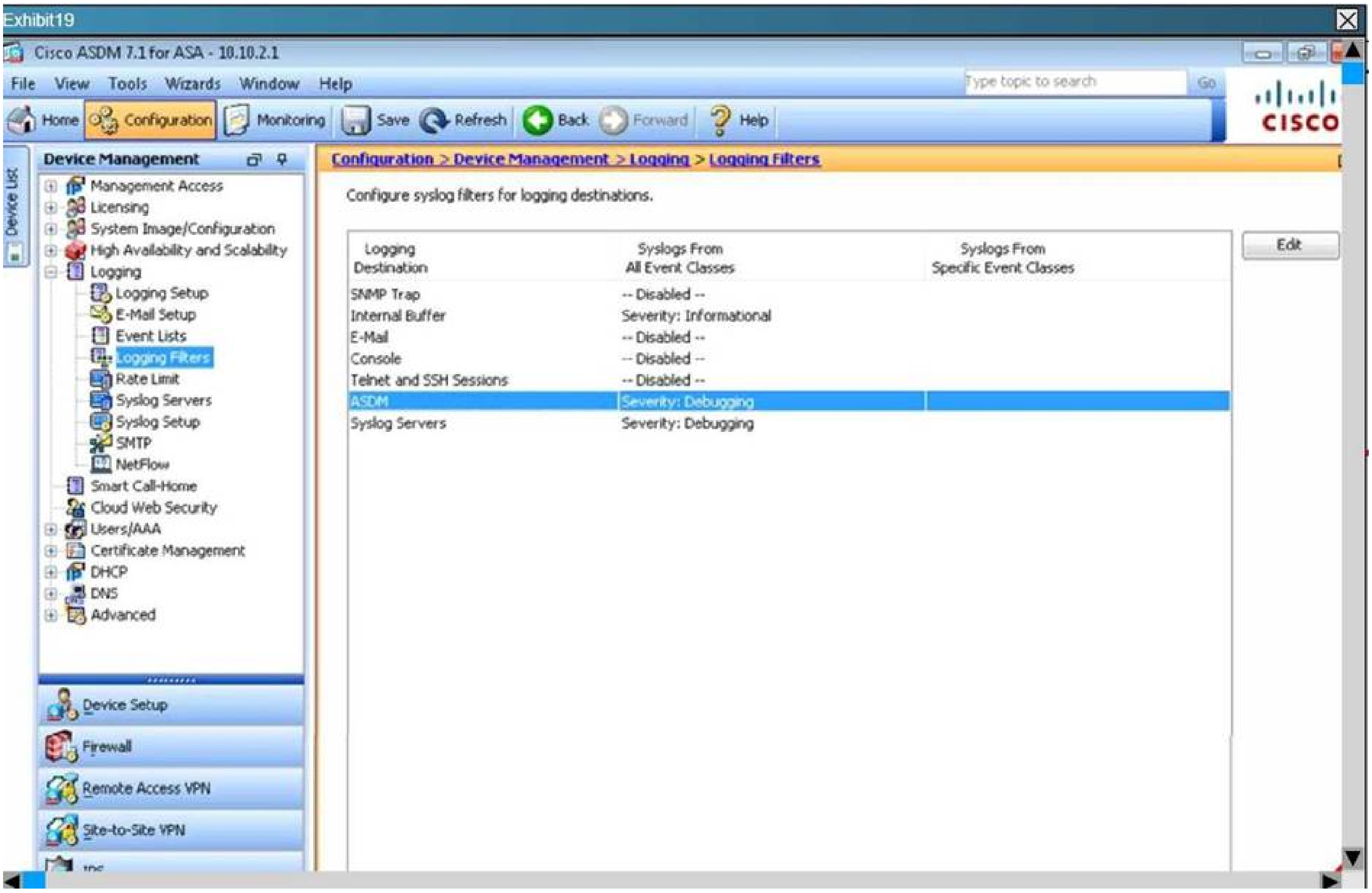
You can choose to save the buffer contents before the buffer is overwritten.

Save Buffer To: □ FTP Server [Configure FTP Settings...]
□ Flash [Configure Flash Usage...]

ASDM Logging

Specify the size of the queue for syslogs intended for viewing in ASDM.

Queue Size: 100



Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	Severity: Informational	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH Sessions	-- Disabled --	
ASDM	Severity: Debugging	
Syslog Servers	Severity: Debugging	

NEW QUESTION 329
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 333
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 335
Where do you apply a control plane services policy to implement Management Plane Protection on a Cisco Router?

A. Control-plane router
B. Control-plane host
C. Control-plane interface management 0/0
D. Control-plane service policy

Answer: B

Explanation:
http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/htsecmpp.html

NEW QUESTION 336
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 339
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 344
How much storage is allotted to maintain system,configuration , and image files on the Cisco ASA 1000V during OVF template file deployment?

A. 1GB
B. 5GB
C. 2GB
D. 10GB

Answer: C

NEW QUESTION 349

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 351
When access rule properties are configured within ASDM, which traffic direction type is required by global and management access rule?

A. Any
B. Both in and out
C. In
D. Out

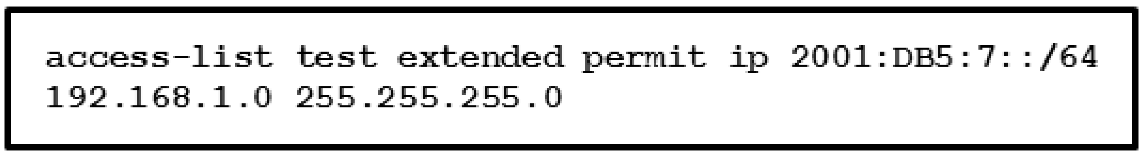
Answer: C

NEW QUESTION 352
Which option is a different type of secondary VLAN?

A. Transparent
B. Promiscuous
C. Virtual
D. Community

Answer: D

NEW QUESTION 357
Refer to the exhibit.



```
access-list test extended permit ip 2001:DB5:7::/64
192.168.1.0 255.255.255.0
```

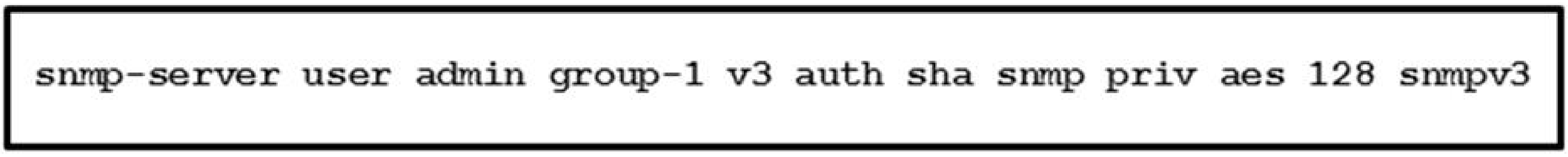
Which statement about this access list is true?

A. This access list does not work without 6to4 NAT
B. IPv6 to IPv4 traffic permitted on the Cisco ASA by default
C. This access list is valid and works without additional configuration
D. This access list is not valid and does not work at all
E. We can pass only IPv6 to IPv6 and IPv4 to IPv4 traffic

Answer: A

Explanation:
ASA 9.0(1) code introduced the Unified ACL for IPv4 and IPv6. ACLs now support IPv4 and IPv6 addresses. You can even specify a mix of IPv4 and IPv6 addresses for the source and destination. The any keyword was changed to represent IPv4 and IPv6 traffic. The any4 and any6 keywords were added to represent IPv4-only and IPv6-only traffic, respectively. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs.

NEW QUESTION 360
Refer to the exhibit.



```
snmp-server user admin group-1 v3 auth sha snmp priv aes 128 snmpv3
```

This command is used to configure the SNMP server on a Cisco router. Which option is the encryption password for the SNMP server?

A. sha
B. snmp
C. group-1
D. snmpv3

Answer: D

NEW QUESTION 361
How much storage is allotted to maintain system, configuration, and image files on the Cisco ASA 1000V during OVF template file deployment?

A. 1GB
B. 5GB
C. 2GB

D. 10GB

Answer: C

NEW QUESTION 363
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 368
Which option lists cloud deployment models?

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

Answer: D

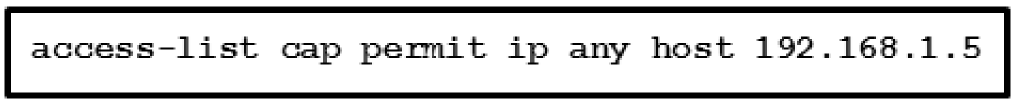
Explanation:
https://www.ibm.com/developerworks/community/blogs/722f6200-f4ca-4eb3- 9d64- 8d2b58b2d4e8/
entry/4_Types_of_Cloud_Computing_Deployment_Model_You_Need_to_K now1?lang=en

NEW QUESTION 372
Which statement about traffic storm control behavior is true?

A. Traffic storm control cannot determine if the packet is unicast or broadcast.
B. If you enable broadcast and multicast traffic storm control and the combined broadcast and multicast traffic exceeds the level within a 1 second traffic storm interval, storm control drops all broadcast and multicast traffic until the end of the storm interval
C. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet isunicast or broadcast.
D. Traffic storm control monitors incoming traffic levels over a 10 second traffic storm control interval

Answer: B

NEW QUESTION 377
Refer to the exhibit.



```
access-list cap permit ip any host 192.168.1.5
```

Which option describes the expected result of the capture ACL?

A. The capture is applied, but we cannot see any packets in the capture
B. The capture does not get applied and we get an error about mixed policy.
C. The capture is applied and we can see the packets in the capture
D. The capture is not applied because we must have a host IP as the source

Answer: B

NEW QUESTION 382
When a traffic storm threshold occurs on a port, into which state can traffic storm control put the port?

A. Disabled
B. Err-disabled
C. Disconnected
D. Blocked
E. Connected

Answer: B

NEW QUESTION 387
Which Layer 2 security feature prevents traffic on a LAN from being disrupted by a broadcast,multicat, or unicast storm on one physical interface?

A. Bridge protocol Data Unit Guard
B. Storm Control
C. Embedded event monitoring
D. Access control lists

Answer: B

NEW QUESTION 392
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 394
Which information is NOT replicated to the secondary Cisco ASA adaptive security appliance in an active/ standby configuration with stateful failover links ?

A. TCP sessions
B. DHCP lease
C. NAT translations
D. Routing tables

Answer: B

NEW QUESTION 396
Which Cisco prime Infrastructure features allows you to assign templates to a group of wireless LAN controllers with similar configuration requirements?

A. Lightweight access point configuration template
B. Composite template
C. Controller configuration group
D. Shared policy object

Answer: C

NEW QUESTION 397
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 399
A security engineer must evaluate Cisco Security Manager. Which two options are benefits of using Cisco Security Manager to manage security? (Choose two)

A. Configuration of access control plane policies on multiple Cisco ASA firewalls at once
B. automatic software upgrades on multiple firewall devices
C. ability to console into each firewall from centralized management
D. configuration of ACLs on multiple Cisco VSG firewalls at once
E. configuration of IPS signatures on multiple Firepower sensors at once

Answer: BE

Explanation:
automatic software upgrades on multiple firewall devices configuraion of IPS signatures on multiple Firepower sensors at once

NEW QUESTION 404
When configuring packet-tracer command from CLI, what is the first option that you set?

A. source IP address
B. destination IP address
C. interface
D. protocol (ip, tcp, udp)

Answer: C

NEW QUESTION 406
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 410
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 413
Which statement about traffic zoning in cisco ASA?

A. you can create a maximum of 512 zones
B. you can add failover interface to zone
C. an interface can be member of more than one zone
D. you can up to eight interface per zone

Answer: D

NEW QUESTION 414
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 416
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 417
Which two attacks are common at Layer 2? (Choose two)

A. teardrop attack
B. MAC spoofing
C. DHCP spoofing
D. ICMP attacks
E. packet sniffing

Answer: BC

NEW QUESTION 418
Within Cisco Prime Infrastructure, which configuration Archive task will allow you to specify when to copy the running configuration to the startup configuration?

A. Schedule Deploy
B. Schedule Overwrite
C. Schedule Archive
D. Schedule Rollback

Answer: B

Explanation: You can schedule to have Prime Infrastructure copy the running configuration to the startup configuration by choosing Inventory > Device

Configuration Archive, then clicking Schedule Overwrite .
http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/user/guide/pi_ug/ chgdevconfig.html#82530

NEW QUESTION 423
A network engineer must manage and push configurations to a Cisco networking environment, in which 10 Cisco ASA with IPS modules reside. Which solution accomplishes this task?

A. Cisco Adaptive Security Device Manager to push configurations to each of the IPS units
B. FireSIGHT manager to bundle and push configurations to the IPS units installed on an SSD within the Cisco ASA 5500 Series ASA
C. Cisco Security Manager 4.5 or later and pushing configuration bundles to each of the IPS units
D. Cisco IPS Manager Express and pushing configurations to the IPS units

Answer: B

NEW QUESTION 427
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 428
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 433
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 437
Which is the minimum RSA crypto key generate for SSH2?

A. 512
B. 768
C. 1024
D. 2048

Answer: B

NEW QUESTION 439
About User identity with domain in the exhibit, if user is not in domain, what identity will be?

A. local
B. default

Answer: A

Explanation: ASA Identity Firewall:

The default domain is used for all users and user groups when a domain has not been explicitly configured for those users or groups. When a default domain is not specified, the default domain for users and groups is LOCAL. Additionally, the Identity Firewall uses the LOCAL domain for all
locally defined user groups or locally defined users (users who log in and authenticate by using a VPN or web portal).

NEW QUESTION 442
Control plane thresholding limit for which protocols?

A. ICMP
B. BGP
C. ARP

Answer: B

Explanation: The queue-thresholding feature policy supports the following TCP/UDP-based protocols:
Bgp,dns,ftp,http,igmp,snmp,ssh,syslog,telnet,Tftp,host-protocols

NEW QUESTION 446
About snmp v3 encryption, which option we have to use?

A. priv
B. auth
C. encrypted

Answer: A

Explanation: -Configure snmp group:snmp-server group [groupname {v1 | v2c | v3{auth | noauth | priv}}] [read readview] [write writeview] [notify notifyview] [access access-list]
-Configure snmp user: snmp-server user username group-name [remote host [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access [ipv6 nacl] [priv {des | 3des | aes
{128 | 192 |256}} privpassword] {acl-number | acl-name}]
encrypet if the password are encrypted ex. insert password not in plain text for auth.

NEW QUESTION 449
ASA in transparent mode for which traffic default route is required?

A. trusted
B. untrusted
C. Internet
D. inside
E. management

Answer: E

Explanation: In transparent mode, the default route, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from
more than one bridge group network, you need to specify a regular static route that identifies the network from which you expect management traffic.

NEW QUESTION 453
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 456
You moved your servers from physical to virtual infrastructure, how to defend it ?

A. Cisco V
B. Cisco ASA 1000V
C. VXLAN
D. VSG

Answer: BD

Explanation: Cisco VSG and the ASA 1000V provide complementary functionalities. The VSG provides virtual machine
context-aware and zone-based security capabilities. The ASA 1000V provides tenant edge security and default gateway functionalities. Together, they provide a trusted and comprehensive virtual and cloud security Portfolio.

From: https://www.cisco.com/c/en/us/products/switches/virtual-security-gateway/index.html

NEW QUESTION 459
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 461
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

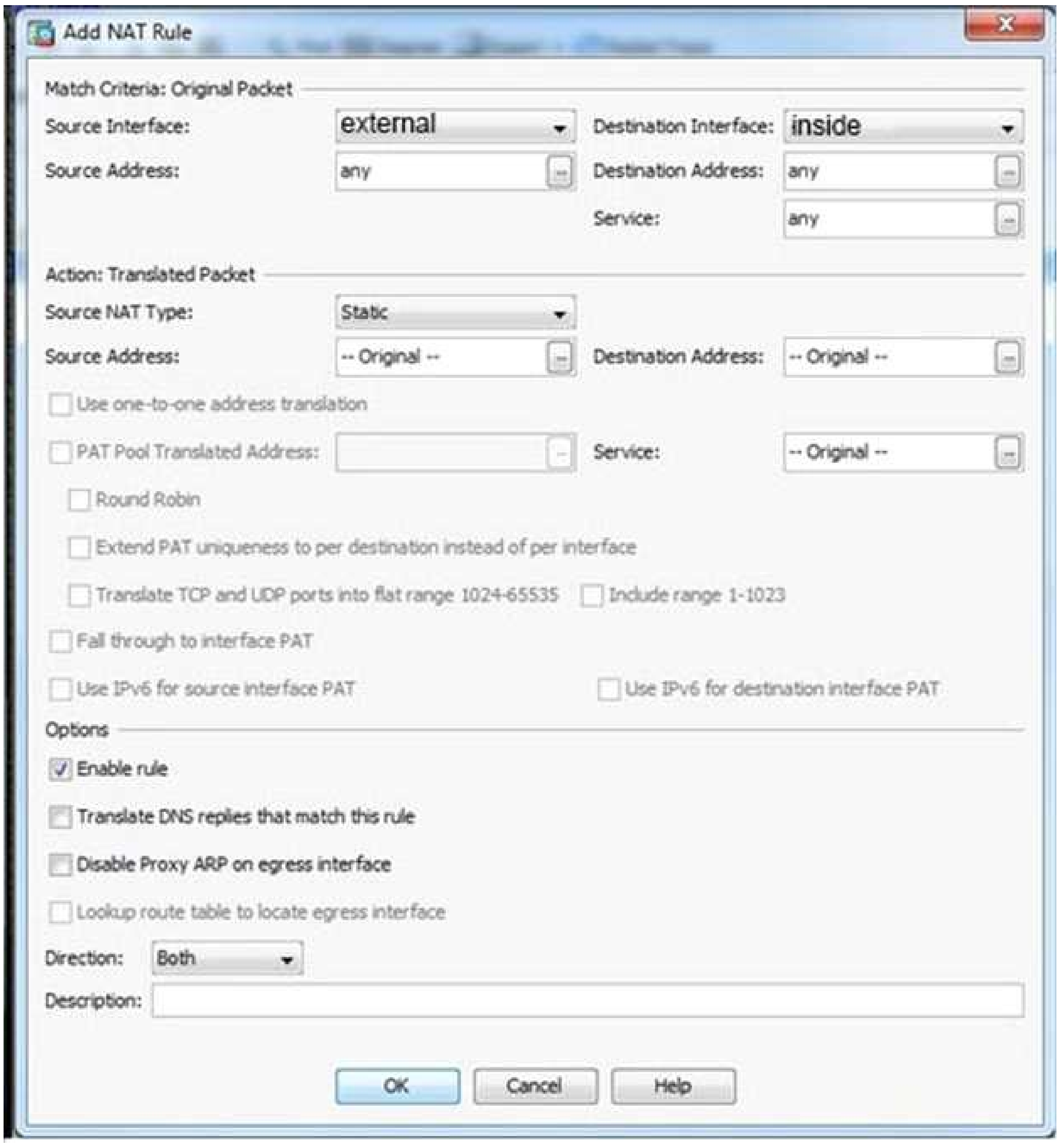
Explanation: Reference:
https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next- generationfirewalls/
product_data_sheet0900aecd8073cbbf.html

NEW QUESTION 462
You must restrict the interface on which management traffic can be received by the routers on your network.
Which feature do you enable?

A. MPP
B. extended ACL on all of the interfaces
C. CPP with a port filter
D. AAA

Answer: A

NEW QUESTION 464
DRAG DROP



Add NAT Rule

Match Criteria: Original Packet

Source Interface: external
Destination Interface: inside
Source Address: any
Destination Address: any
Service: any

Action: Translated Packet

Source NAT Type: Static
Source Address: -- Original --
Destination Address: -- Original --

□ Use one-to-one address translation

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

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

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

□ Fall through to interface PAT

□ Use IPv6 for source interface PAT □ Use IPv6 for destination interface PAT

Options

☑ Enable rule

□ Translate DNS replies that match this rule

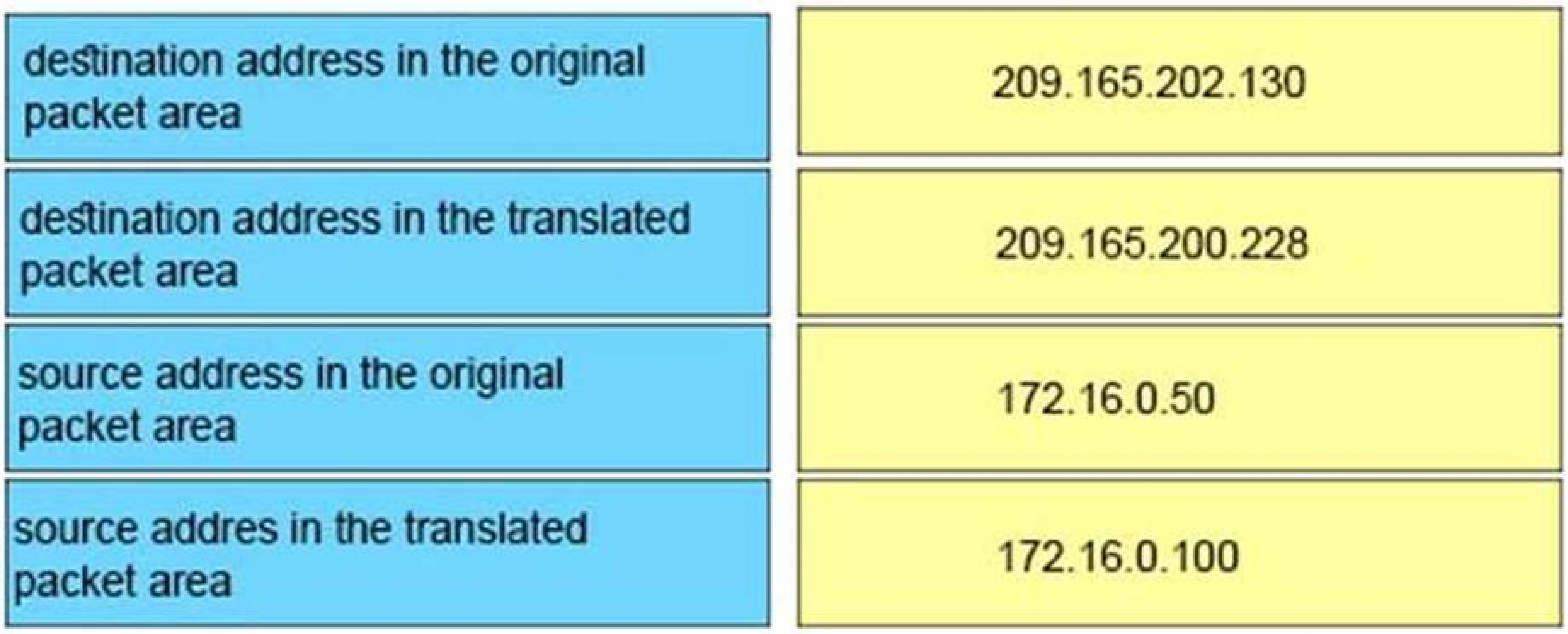
□ Disable Proxy ARP on egress interface

□ Lookup route table to locate egress interface

Direction: Both

Description:

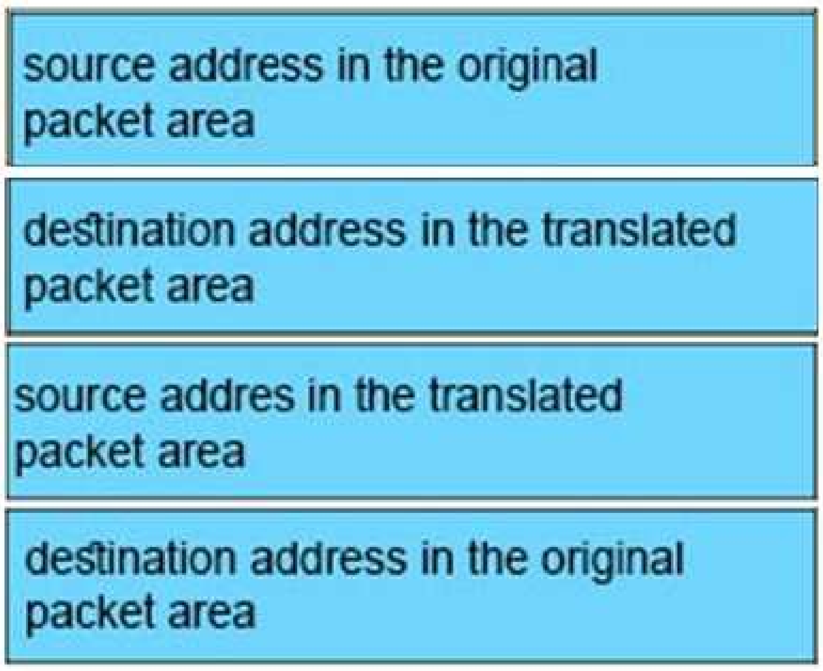
Refer to the exhibit. You have a business partner who has a host IP address of 209.165.202.130. You have a host object that has an IP address of 172.16.0.100. You need to create a NAT rule that allows 209.165.202.130 to connect over the Internet to 172.16.0.100 by using an object that has a public IP address of 209.165.200.228. The partner IP address must be translated to an internal IP address of 172.16.0.50 for security reasons. Drag and drop the NAT criteria options from the left onto the correct host objects on the right.



destination address in the original packet area	209.165.202.130
destination address in the translated packet area	209.165.200.228
source address in the original packet area	172.16.0.50
source addres in the translated packet area	172.16.0.100

Answer:

Explanation:



source address in the original packet area

destination address in the translated packet area

source addres in the translated packet area

destination address in the original packet area

NEW QUESTION 469

......