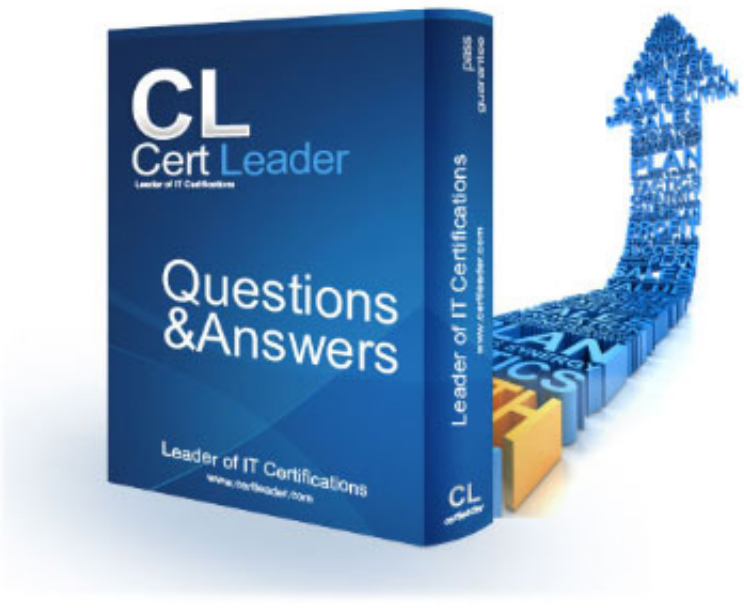
300-206 Dumps

Implementing Cisco Edge Network Security Solutions

https://www.certleader.com/300-206-dumps.html



NEW QUESTION 1
Which two user privileges does ASDM allow engineer to create? (Choose two)

A. Full access
B. admin
C. read-write
D. read-only
E. write-only

Answer: CE

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

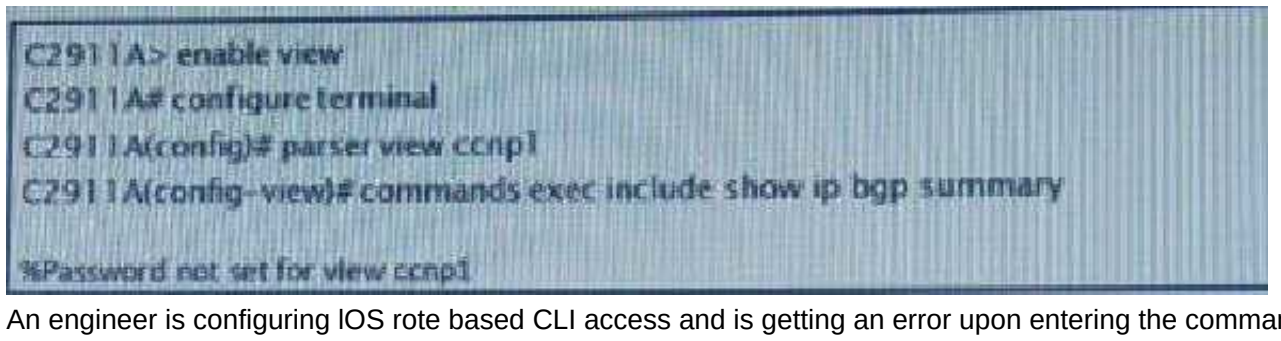
Answer: DE

NEW QUESTION 3
When you enable IP source Guard on private VLAN ports, which additional action must you take for IP Source Guard to be effective?

A. Enable DHCP snooping on the isolated VLAN
B. Enable BPDU guard on the isolated VLAN.
C. Enable BPDU guard on the primary VLAN.
D. Enable DHCP snooping on the primary VLAN.

Answer: D

NEW QUESTION 4
Refer to the exhibit.



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 5
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 6
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 7
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 8
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 9
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.

ssh 192.168.0.0 255.255.224.0 inside	Create enable password to use SSH
domain-name <domain>	Define user and password to connect via SSH
aaa authentication ssh console LOCAL	Configure authentication mode
ssh version 2	Specify SSH protocol version
enable password <password>	Allow access from the inside interface
username <username> password <password>	Configure FQDN
crypto key generate rsa modulus 2048	Generate a key pair

Answer:

Explanation:

NEW QUESTION 10
Which threat level is the default used in the Botnet Traffic Filter?

A. high
B. moderate to very-high
C. high to very-high
D. very-high

Answer: B

NEW QUESTION 10
An engineer has successfully captured data on an ASA (ip address 10.10.10.1) and wants to download the file to analyze offline. The filename is capin.
Which option must the engineer enter to accomplish this task?

A. https://10.10.10.1/admin/capture/capin
B. http://10.10.10.1/admin/capture/capin/pcap
C. https://10.10.10.1/admin/capture/capin/pcap
D. http://10.10.10.1/admin/capture/capin

Answer: C

NEW QUESTION 11
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 18
Which statement about the behavior of the Cisco ASA firewall is true?

A. The Cisco ASA is not seen as a router hop to connect devices in routed mode
B. All Cisco ASA interfaces are on different subnets in transparent mode
C. The Cisco ASA clears the running configuration when changing firewall modes
D. The Cisco ASA blocks ARP inspection packets in transparent mode

Answer: C

NEW QUESTION 21
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

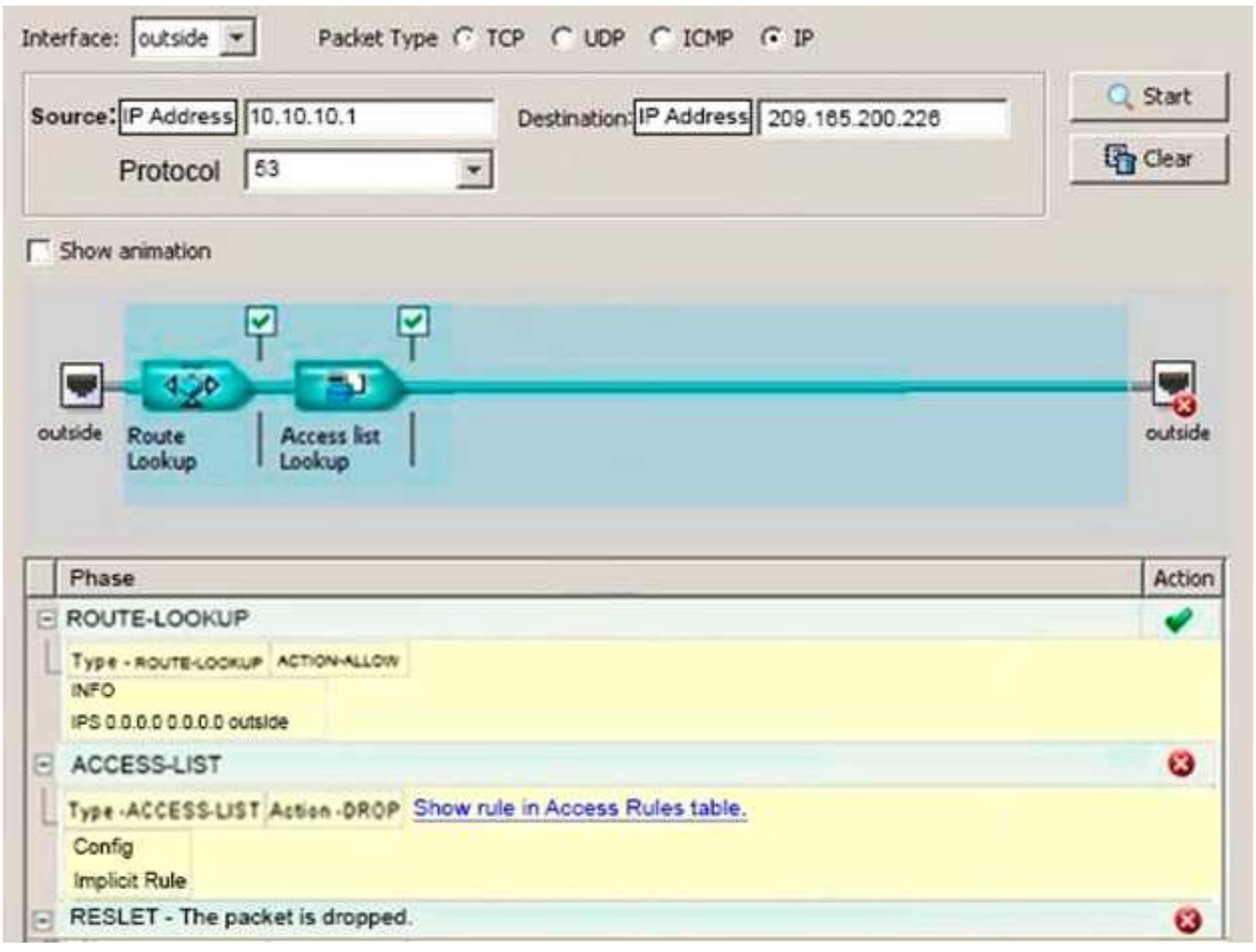
Answer: B

NEW QUESTION 25
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 26
Refer to the exhibit. The security engineer is troubleshooting internal access to the public DNS server at 209.165.200.226.



Which description of the issue is true?

A. The routes of the Cisco ASA are incorrectly identifying traffic from 10.10.10.1 on the outside interface of the firewall.
B. To accurately test DNS, the packet tracer should be run using packet type UDP and destination port 53.
C. To allow DNS, a rule specifically allowing the DNS access must be added in the rule base.
D. The engineer must verify the NAT rules of the firewall to ensure that correct NATing is taking place.

Answer: C

NEW QUESTION 29
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 31
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 33
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

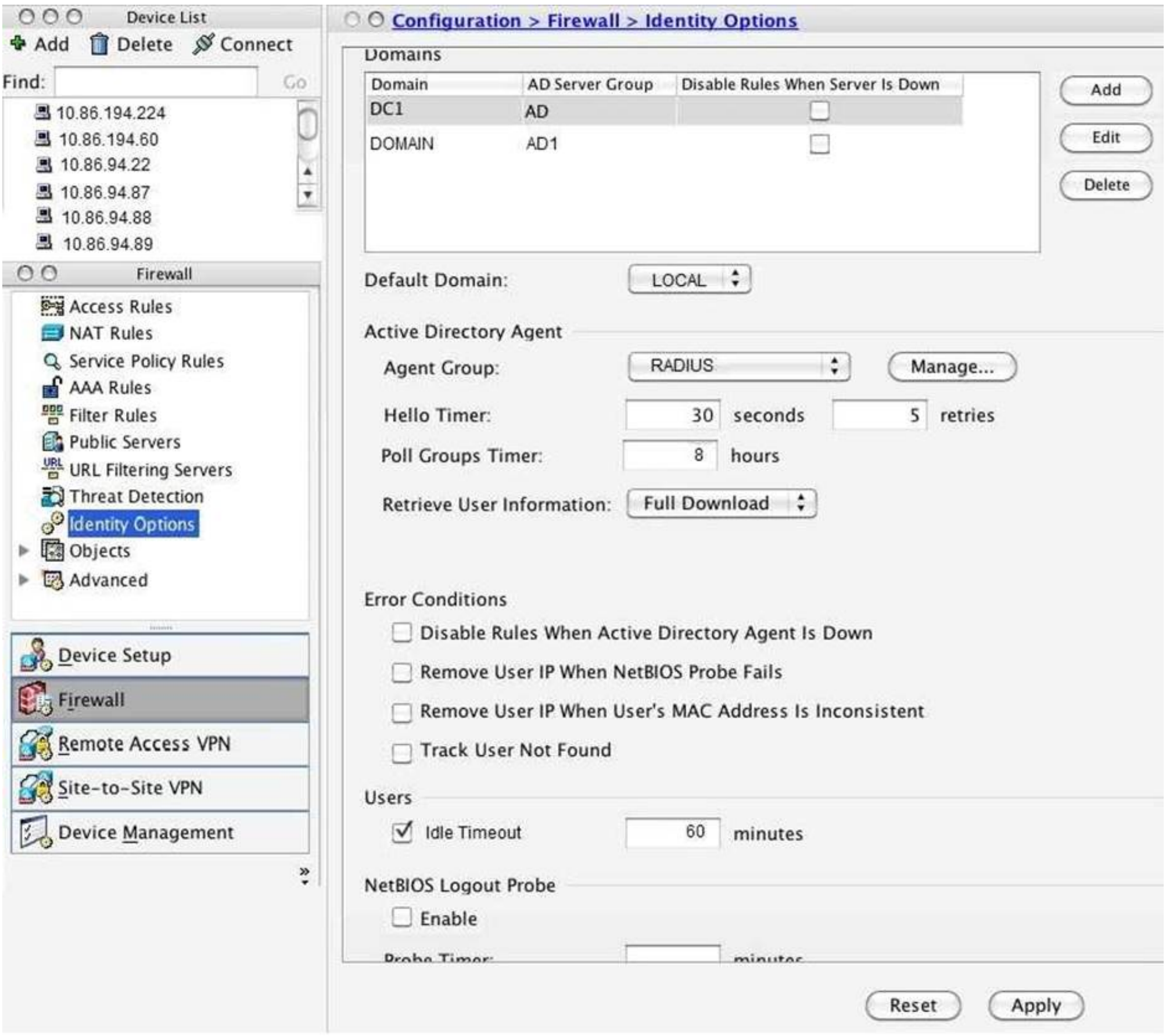
Answer: A

NEW QUESTION 38
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 40
Refer to the exhibit. An engineer has configured identify options on an ASA using ASDM. Which domain is used for a user who does not have an explicitly configured domain?



A. DOMAIN1
B. PIXTEST
C. NetBIOS domain name configured on the Active Directory domain controller
D. LOCAL domain name for all locally defined users and groups

Answer: D

NEW QUESTION 42
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

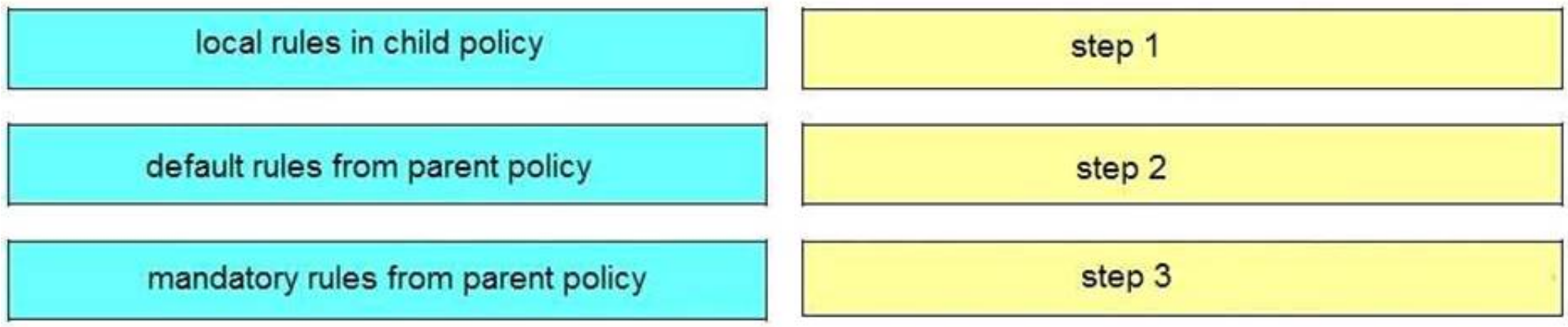
NEW QUESTION 44
With the crypto key generate rsa command, how many bits minimum must the RSA key size be to enable SSH2 on a router?

A. 512 bits
B. 768 bits
C. 1024 bits

D. 2048 bits

Answer: B

NEW QUESTION 46
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 49
An engineer is configuring MACsec encryption. Which two components does Cisco TrustSec NDAC MACsec support? (Choose two.)

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

Answer: BE

NEW QUESTION 54
A web server has been configured to operate on port 1521. The web server traffic is passing through an ASA with default application inspection configured. Which application inspection affects the web server traffic?

A. HTTP
B. MSCP
C. HTTPS
D. SQL *Net

Answer: D

NEW QUESTION 59
An engineer is examining the configuration of an IOS device and notices that though SSH is configured properly, the ip ssh version 2 command is not explicitly configured. How does the device behave in regards to SSH connections?

A. only SSHv2 is allowed.
B. SSHv1 and SSHv2 are denied.
C. SSHv1 and SSHv2 are allowed.
D. only SSHv1 is allowed.

Answer: D

NEW QUESTION 62
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 67
An engineer is hardening the management plane for an AS

A. Which protocol is affected by this hardening?
B. BGP
C. IKE
D. ICMP
E. ARP

Answer: C

NEW QUESTION 70
An engineer is trying to configure Dynamic ARP Inspection. Which feature must be enabled first?

A. DHCP snooping
B. Cisco Discovery Protocol
C. port security
D. IP Source Guard

Answer: A

NEW QUESTION 75
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 80
DRAG DROP
Drag and drop the syslog message examples on the left onto the message security level on the right.

ASA-1-130827	inforrnational message
ASA-2-639214	warning message
ASA-4-415698	alert message
ASA-6-259266	critical message

Answer:

Explanation:

NEW QUESTION 83
Private VLANs have been configured in the data center. Which type of Private VLAN port would allow a new server to communicate with all other interfaces?

A. isolated
B. community
C. private
D. promiscuous
E. shared

Answer: D

NEW QUESTION 88
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 92
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 95
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 the administrator assign to the user?

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

Answer: B

NEW QUESTION 97
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 101
How many interfaces can a Cisco ASA bridge group support and how many bridge groups can a Cisco ASA appliance support?

A. up to 2 interfaces per bridge group and up to 4 bridge groups per Cisco ASA appliance
B. up to 2 interfaces per bridge group and up to 8 bridge groups per Cisco ASA appliance
C. up to 4 interfaces per bridge group and up to 4 bridge groups per Cisco ASA appliance
D. up to 4 interfaces per bridge group and up to 8 bridge groups per Cisco ASA appliance
E. up to 8 interfaces per bridge group and up to 4 bridge groups per Cisco ASA appliance
F. up to 8 interfaces per bridge group and up to 8 bridge groups per Cisco ASA appliance

Answer: D

NEW QUESTION 102
Which addresses are considered "ambiguous addresses" and are put on the greylist by the Cisco ASA botnet traffic filter feature?

A. addresses that are unknown
B. addresses that are on the greylist identified by the dynamic database
C. addresses that are blacklisted by the dynamic database but also are identified by the static whitelist
D. addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist

Answer: D

NEW QUESTION 105
For which purpose is the Cisco ASA CLI command aaa authentication match used?

A. Enable authentication for SSH and Telnet connections to the Cisco ASA appliance.
B. Enable authentication for console connections to the Cisco ASA appliance.
C. Enable authentication for connections through the Cisco ASA appliance.
D. Enable authentication for IPsec VPN connections to the Cisco ASA appliance.
E. Enable authentication for SSL VPN connections to the Cisco ASA appliance.
F. Enable authentication for Cisco ASDM connections to the Cisco ASA appliance.

Answer: C

NEW QUESTION 107
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 110
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 113
Which three logging methods are supported by Cisco routers? (Choose three.)

A. console logging
B. TACACS+ logging
C. terminal logging
D. syslog logging
E. ACL logging
F. RADIUS logging

Answer: ACD

NEW QUESTION 115
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 120
A Cisco ASA is configured for TLS proxy. When should the security appliance force remote IP phones connecting to the phone proxy through the internet to be in secured mode?

A. When the Cisco Unified Communications Manager cluster is in non-secure mode
B. When the Cisco Unified Communications Manager cluster is in secure mode only
C. When the Cisco Unified Communications Manager is not part of a cluster
D. When the Cisco ASA is configured for IPSec VPN

Answer: A

NEW QUESTION 122
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 125
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 126
Which component does Cisco ASDM require on the host Cisco ASA 5500 Series or Cisco PIX security appliance?

A. a DES or 3DES license
B. a NAT policy server
C. a SQL database
D. a Kerberos key
E. a digital certificate

Answer: A

NEW QUESTION 129
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 132
Which three compliance and audit report types are available in Cisco Prime Infrastructure? (Choose three.)

A. Service
B. Change Audit
C. Vendor Advisory
D. TAC Service Request
E. Validated Design
F. Smart Business Architecture

Answer: ABC

NEW QUESTION 137

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 142
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 144
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 147
When troubleshooting redundant interface operations on the Cisco ASA, which configuration should be verified?

A. The nameif configuration on the member physical interfaces are identical.
B. The MAC address configuration on the member physical interfaces are identical.
C. The active interface is sending periodic hellos to the standby interface.
D. The IP address configuration on the logical redundant interface is correct.
E. The duplex and speed configuration on the logical redundant interface are correct.

Answer: D

NEW QUESTION 148
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 153
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 155
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 157
Which two options are two 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 inject virtual packets into the data path
D. to debug packet drops in a production network
E. to correct dropped packets in a production network

Answer: CD

NEW QUESTION 160
By default, not all services in the default inspection class are inspected. Which Cisco ASA CLI command do you use to determine which inspect actions are applied to the default inspection class?

A. show policy-map global_policy
B. show policy-map inspection_default
C. show class-map inspection_default
D. show class-map default-inspection-traffic
E. show service-policy global

Answer: E

NEW QUESTION 165
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 170
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 171
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 176
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 178
Which two voice protocols can the Cisco ASA inspect? (Choose two.)

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

Answer: AD

NEW QUESTION 180
Which log level provides the most detail on the Cisco Web Security Appliance?

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

Answer: C

NEW QUESTION 182
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 186
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 191
Which two VPN types can you monitor and control with Cisco Prime Security Manager? (Choose two.)

A. AnyConnect SSL
B. site-to-site
C. clientless SSL
D. IPsec remote-access

Answer: AD

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_1.pdf

NEW QUESTION 192
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 196
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 200
Which three options are hardening techniques for Cisco IOS routers? (Choose three.)

A. limiting access to infrastructure with access control lists
B. enabling service password recovery
C. using SSH whenever possible
D. encrypting the service password
E. using Telnet whenever possible
F. enabling DHCP snooping

Answer: ACD

NEW QUESTION 204
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 209
When a Cisco ASA is configured in multicontext mode, which command is used to change between contexts?

A. changeto config context
B. changeto context
C. changeto/config context change
D. changeto/config context 2

Answer: B

NEW QUESTION 213
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 216
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 219
Which Cisco product provides a GUI-based device management tool to configure Cisco access routers?

A. Cisco ASDM
B. Cisco CP Express
C. Cisco ASA 5500
D. Cisco CP

Answer: D

NEW QUESTION 223
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 224
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 226
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 229
What are two reasons for implementing NIPS at enterprise Internet edges? (Choose two.)

A. Internet edges typically have a lower volume of traffic and threats are easier to detect.
B. Internet edges typically have a higher volume of traffic and threats are more difficult to detect.
C. Internet edges provide connectivity to the Internet and other external networks.
D. Internet edges are exposed to a larger array of threats.
E. NIPS is more optimally designed for enterprise Internet edges than for internal network configurations.

Answer: CD

NEW QUESTION 233
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 234
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

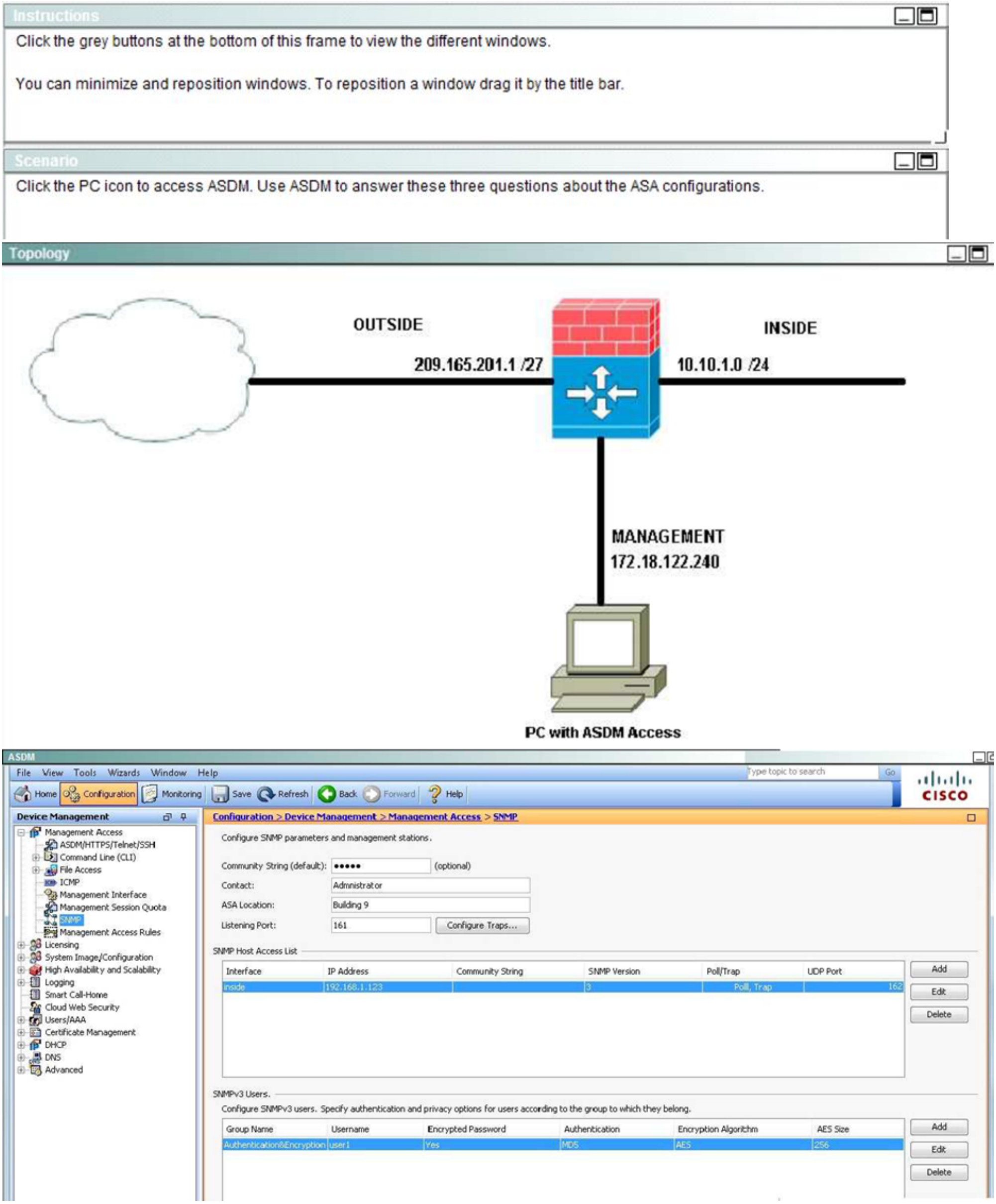
Answer: B

NEW QUESTION 239
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 241

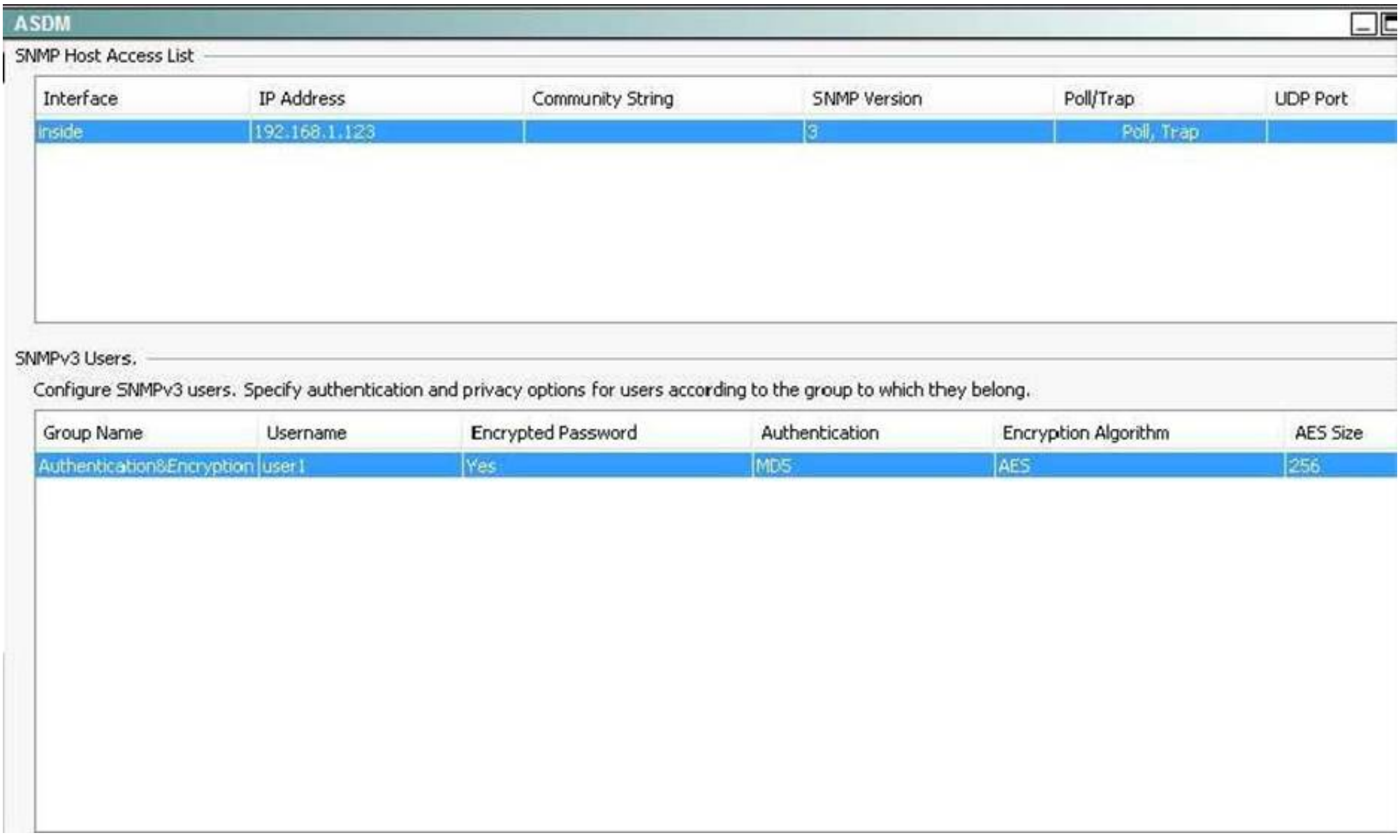


SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SH

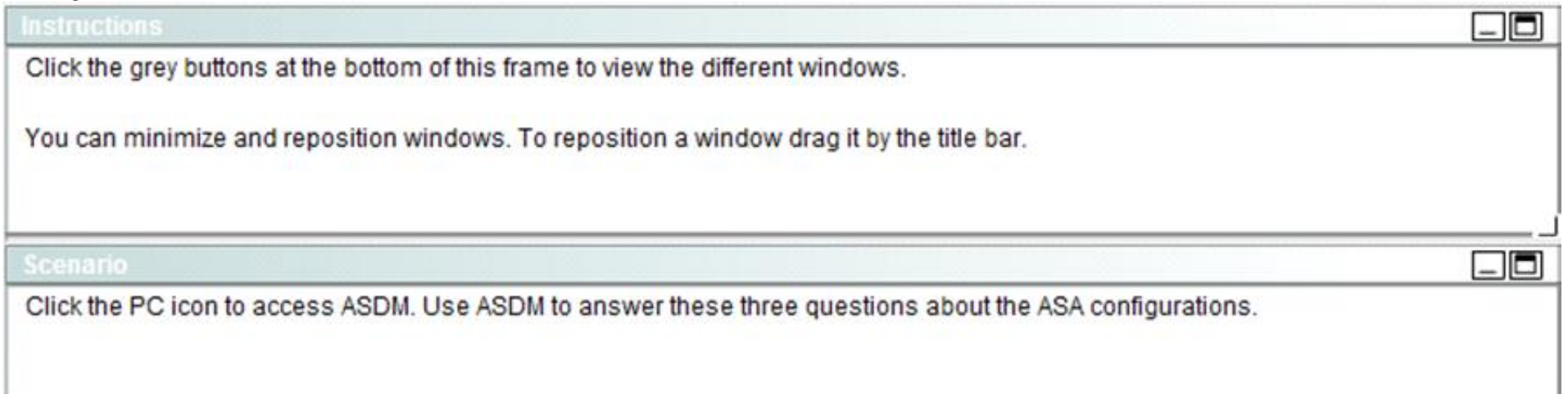
A. The encryption algorithm options are DES, 3DES, andAES (which is available in 128,192, and 256 versions). When you create a user, with which option must you associate it?
B. an SNMP group
C. at least one interface
D. the SNMP inspection in the global_policy
E. at least two interfaces

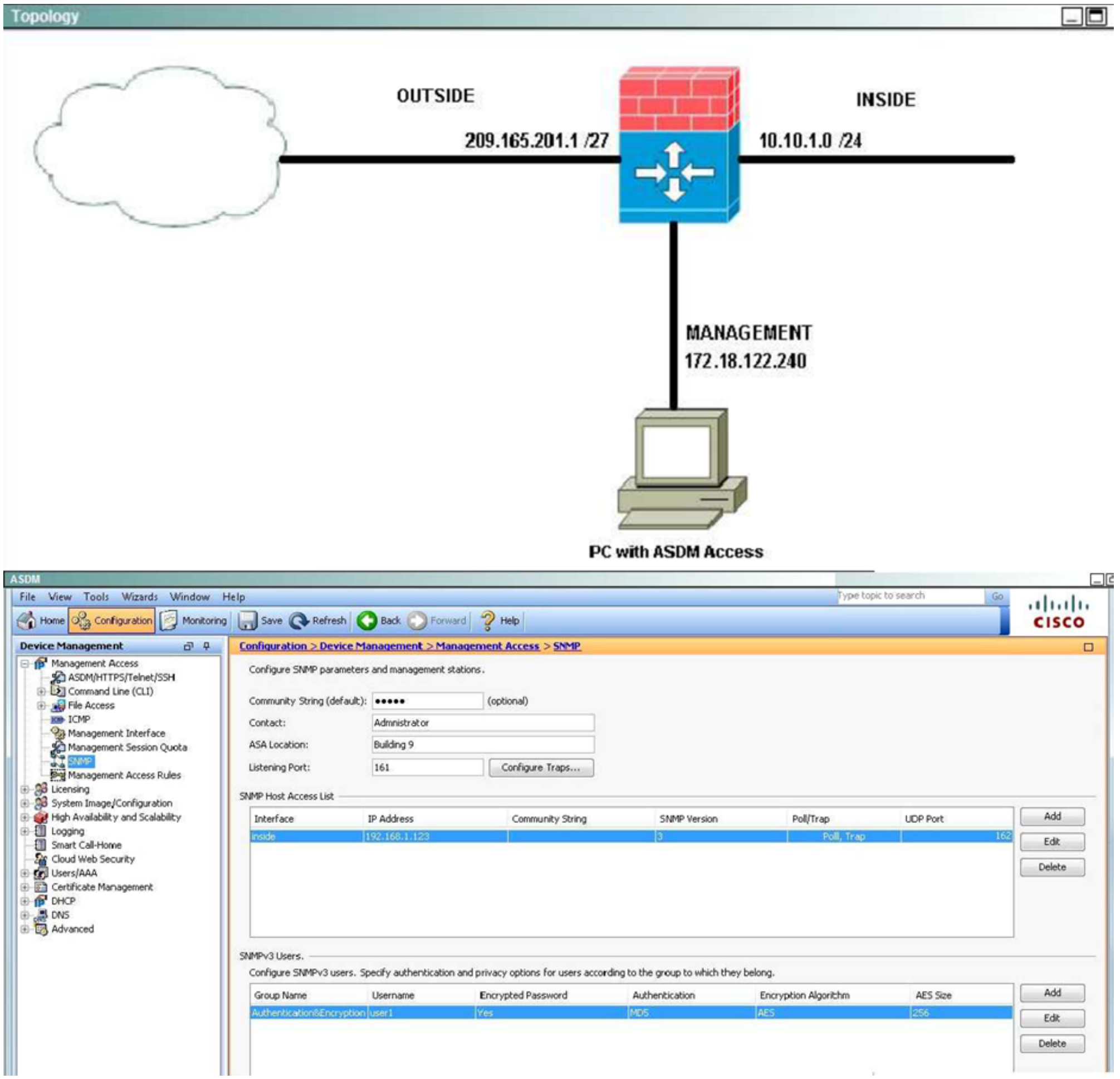
Answer: A

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



NEW QUESTION 244



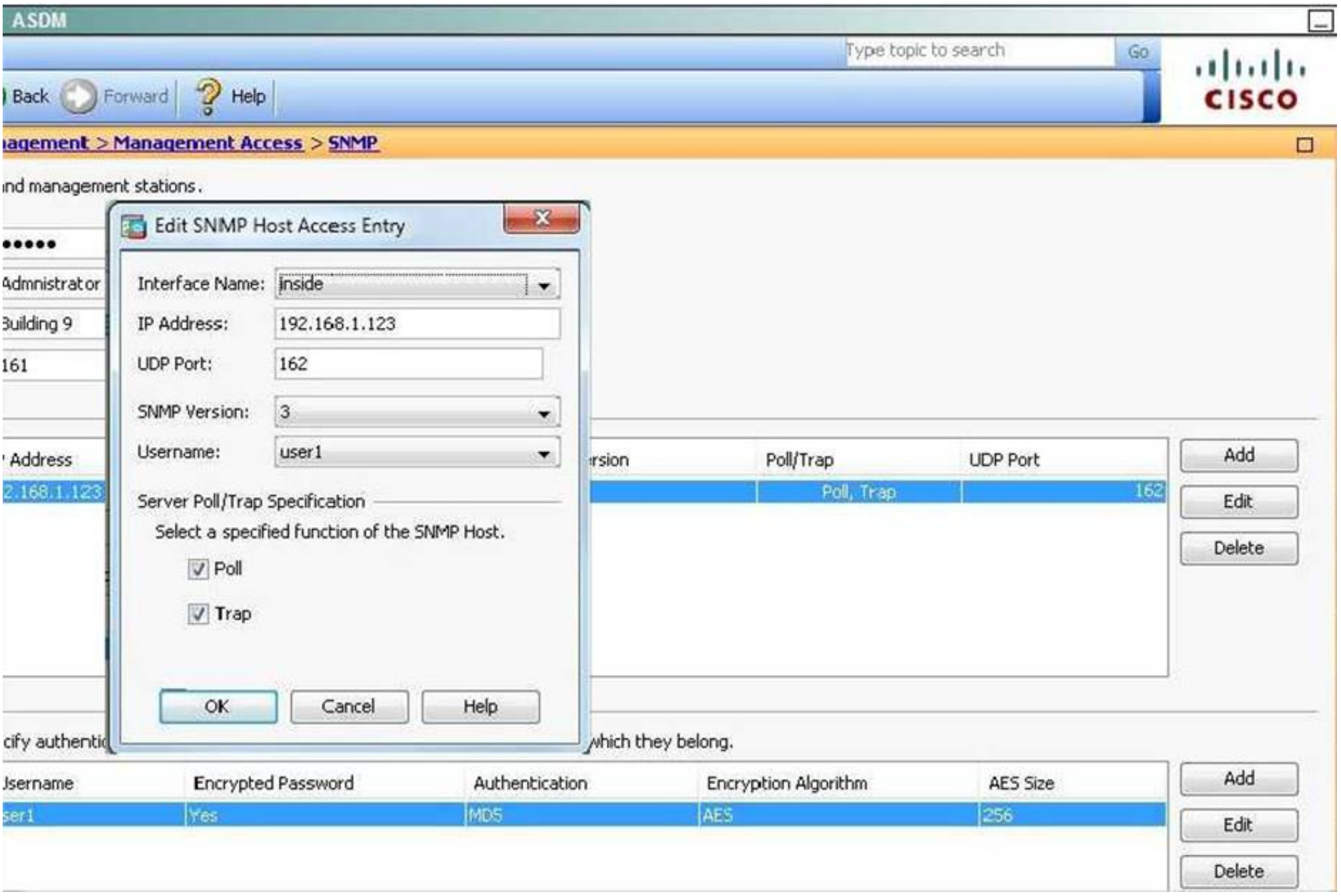


An SNMP host is an IP address to which SNMP notifications and traps are sent. To configure SNMFV3 hosts, which option must you configure in addition to the target IP address?

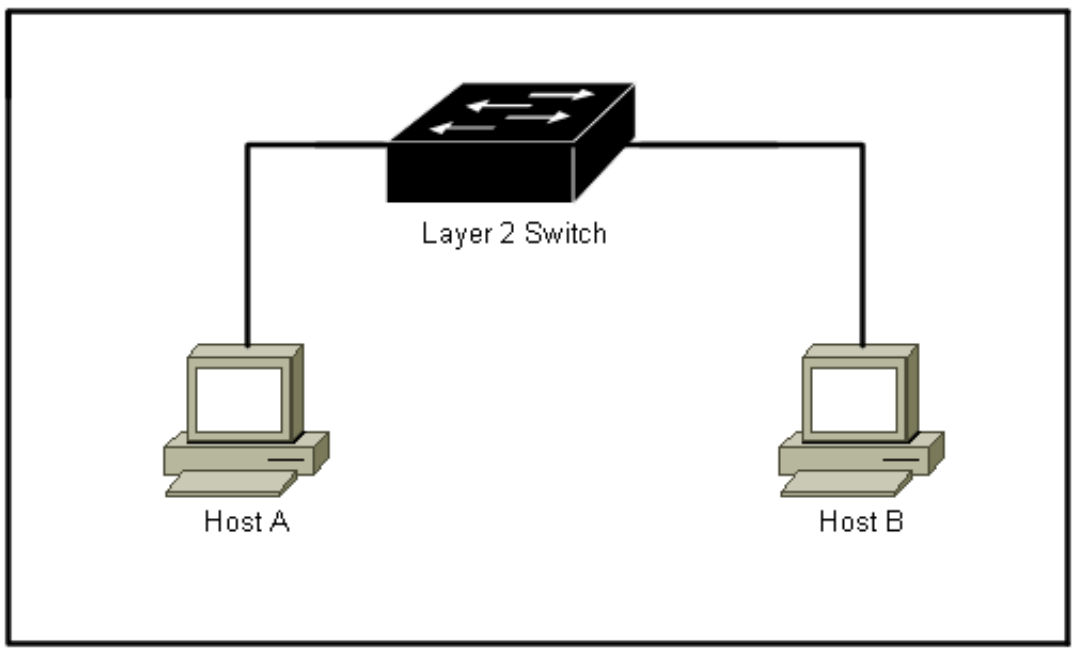
A. the Cisco ASA as a DHCP server, so the SNMFV3 host can obtain an IP address
B. a username, because traps are only sent to a configured user
C. SSH, so the user can connect to the Cisco ASA
D. the Cisco ASA with a dedicated interface only for SNMP, to process the SNMP host traffic.

Answer: B

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



NEW QUESTION 249
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 252
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 254
Which two statements about zone-based firewalls are true? (Choose two.)

A. More than one interface can be assigned to the same zone.
B. Only one interface can be in a given zone.
C. An interface can only be in one zone.
D. An interface can be a member of multiple zones.
E. Every device interface must be a member of a zone.

Answer: AC

NEW QUESTION 258
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 262
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 267
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 271
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 272
Which three statements about private VLANs are true? (Choose three.)

A. Isolated ports can talk to promiscuous and community ports.
B. Promiscuous ports can talk to isolated and community ports.
C. Private VLANs run over VLAN Trunking Protocol in client mode.
D. Private VLANS run over VLAN Trunking Protocol in transparent mode.
E. Community ports can talk to each other as well as the promiscuous port.
F. Primary, secondary, and tertiary VLANs are required for private VLAN implementation.

Answer: BDE

NEW QUESTION 276
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 278
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 283
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 287
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 292
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 295
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 300
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 304
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 306
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 309
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 312
In which two modes is zone-based firewall high availability available? (Choose two.)

A. IPv4 only
B. IPv6 only
C. IPv4 and IPv6
D. routed mode only
E. transparent mode only
F. both transparent and routed modes

Answer: CD

NEW QUESTION 317
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 321
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 325
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 329
At which layer does Dynamic ARP Inspection validate packets?

A. Layer 2
B. Layer 3
C. Layer 4
D. Layer 7

Answer: A

NEW QUESTION 331
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 336
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 337
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 339
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 344
Which two TCP ports must be open on the Cisco Security Manager server to allow the server to communicate with the Cisco Security Manager client? (Choose two.)

A. 1741
B. 443
C. 80
D. 1740
E. 8080

Answer: AB

NEW QUESTION 348
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 349
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 352
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 357
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 359
Which function does DNSSEC provide in a DNS infrastructure?

A. It authenticates stored information.
B. It authorizes stored information.
C. It encrypts stored information.
D. It logs stored security information.

Answer: A

NEW QUESTION 364
Which utility can you use to troubleshoot and determine the timeline of packet changes in a data path within a Cisco firewall?

A. packet tracer
B. ping
C. traceroute
D. SNMP walk

Answer: A

NEW QUESTION 368
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 372
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 374
In which way are management packets classified on a firewall that operates in multiple context mode?

A. by their interface IP address
B. by the routing table
C. by NAT
D. by their MAC addresses

Answer: A

NEW QUESTION 375
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 379

If you disable PortFast on switch ports that are connected to a Cisco ASA and globally turn on BPDU filtering, what is the effect on the switch ports?

A. The switch ports are prevented from going into an err-disable state if a BPDU is received.
B. The switch ports are prevented from going into an err-disable state if a BPDU is sent.
C. The switch ports are prevented from going into an err-disable state if a BPDU is received and sent.
D. The switch ports are prevented from forming a trunk.

Answer: C

NEW QUESTION 380
What are the three types of private VLAN ports? (Choose three.)

A. promiscuous
B. isolated
C. community
D. primary
E. secondary
F. trunk

Answer: ABC

NEW QUESTION 383
Which VTP mode supports private VLANs on a switch?

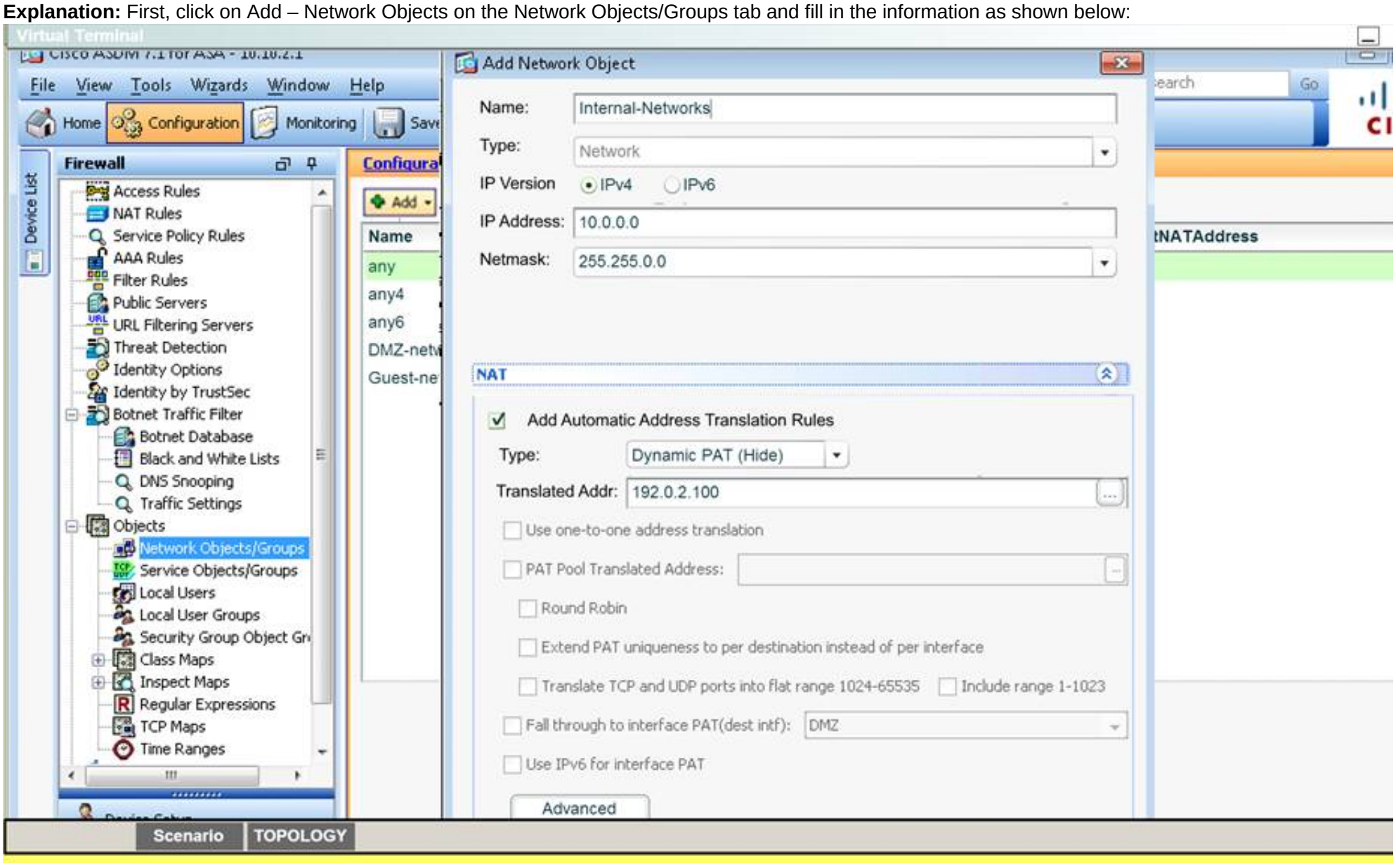
A. transparent
B. server
C. client
D. off

Answer: A

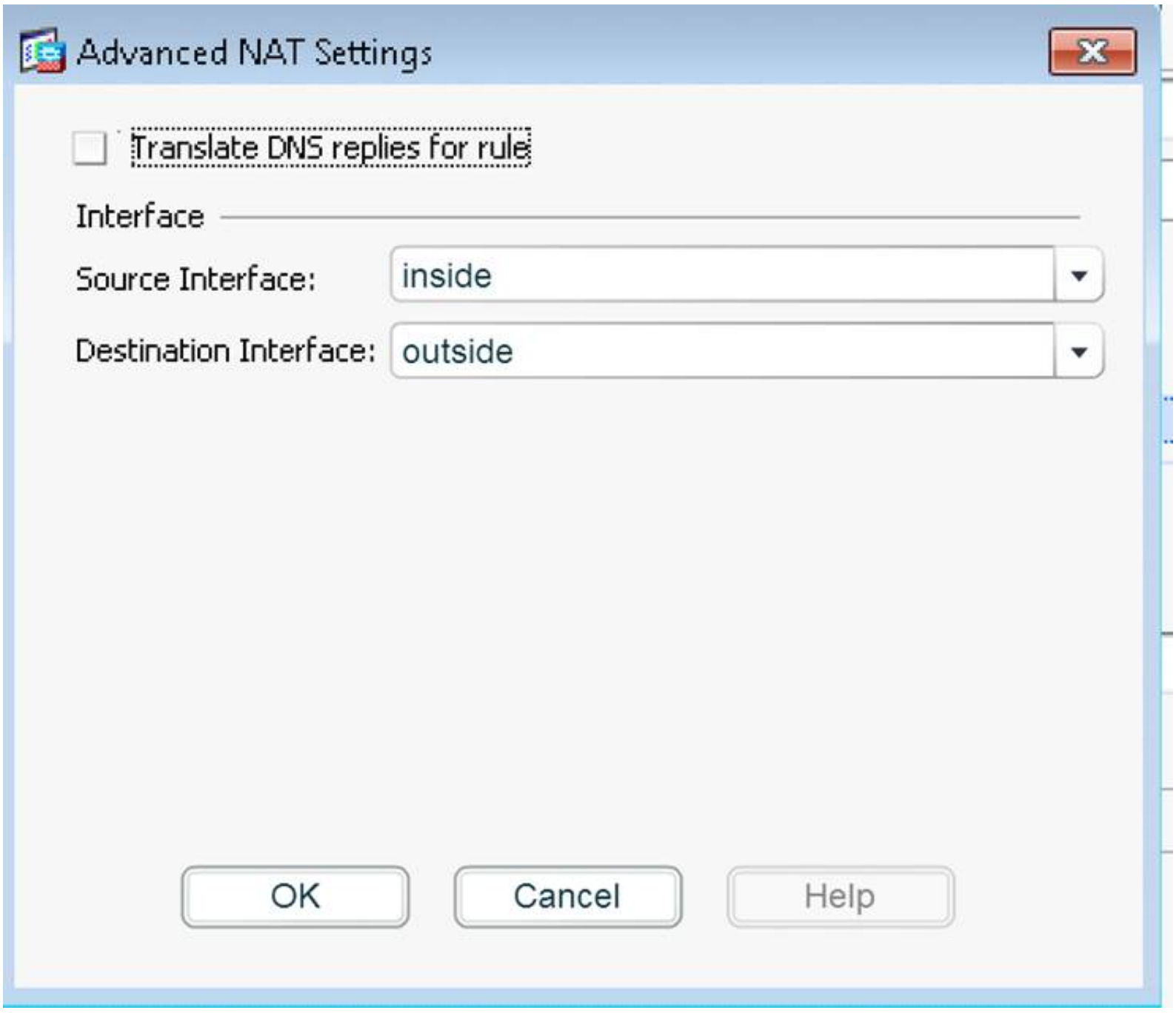
NEW QUESTION 384
You are a network security engineer for the Secure-X network. You have been tasked with implementing dynamic network object NAT with PAT on a Cisco AS

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 387
Refer to the exhibit.

Exhibit

```
regex App_regex_1
"[uU][nN][iI][oO][nN]([%]2[0bB]|[+])([aA][lL][lL]([%]2[0bB]|[+]))?[sS][eE][lL
][eE][cC][tT]"
regex App_regex_2 "[Ss][Ee][Ll][Ee][Cc][Tt](%2[0bB]|+)[^\r\x00-\x19\x7f-
\xff]+(%2[0bB]|+)[Ff][Rr][Oo][Mm](%2[0bB]|+)"

!
class-map WebServers
 match port tcp eq www
class-map type inspect http match-any App-map
 match request body regex App_regex_1
 match request body regex App_regex_2
!

policy-map type inspect http drop-Protocol
 parameters
  body-match-maximum 3000
 class App-map
  drop-connection log
policy-map Protocol-traffic
 class WebServers
  inspect http drop-Protocol
!
service-policy Protocol-traffic interface outside
```

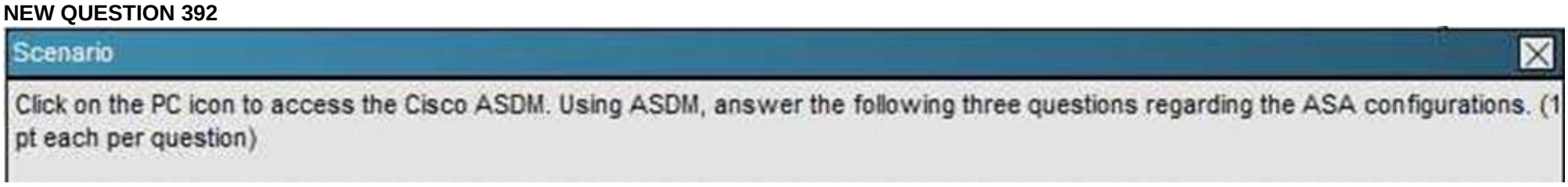
What type of attack is being mitigated on the Cisco ASA appliance?

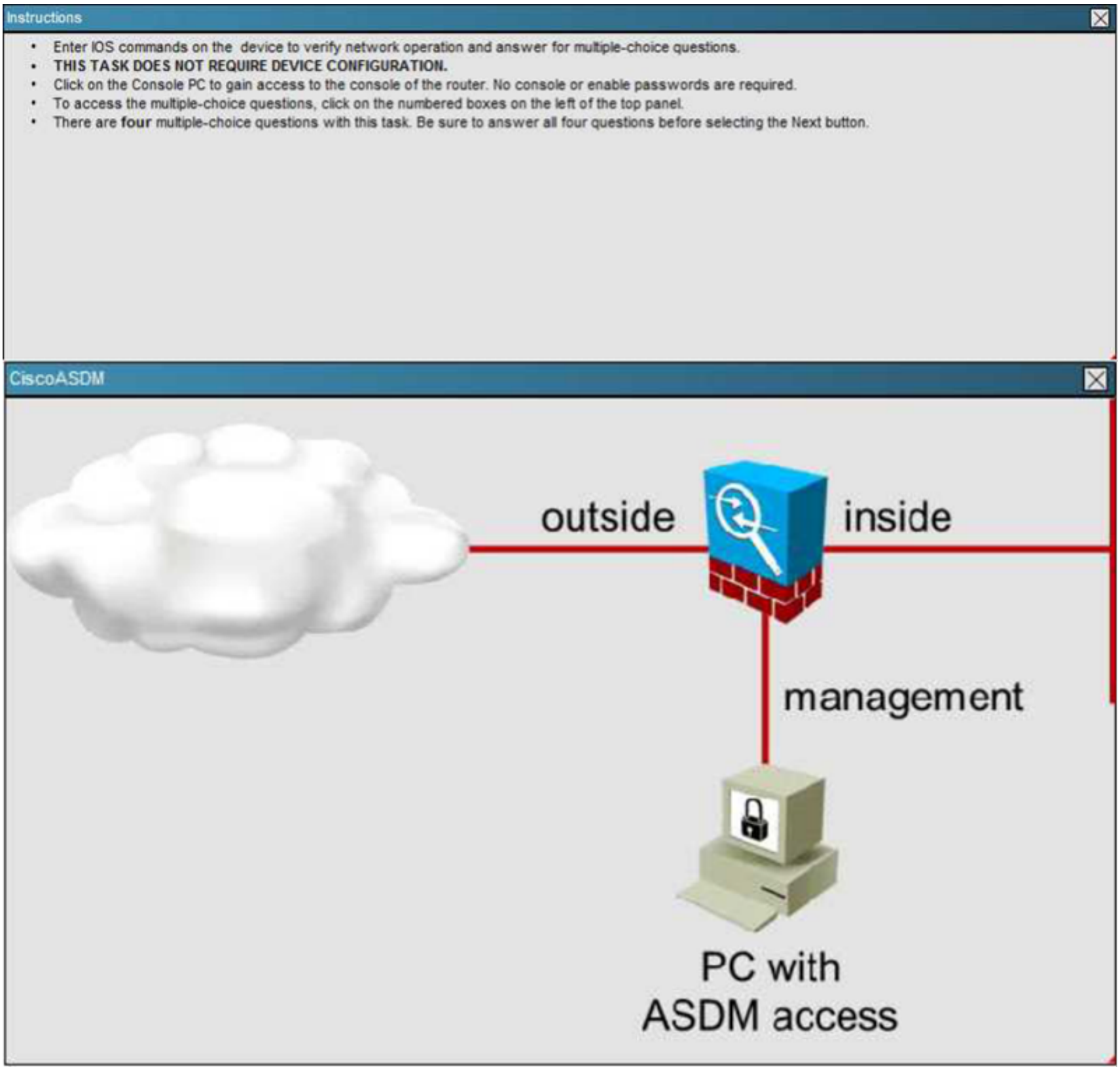
A. HTTP and POST flood attack
B. HTTP Compromised-Key Attack

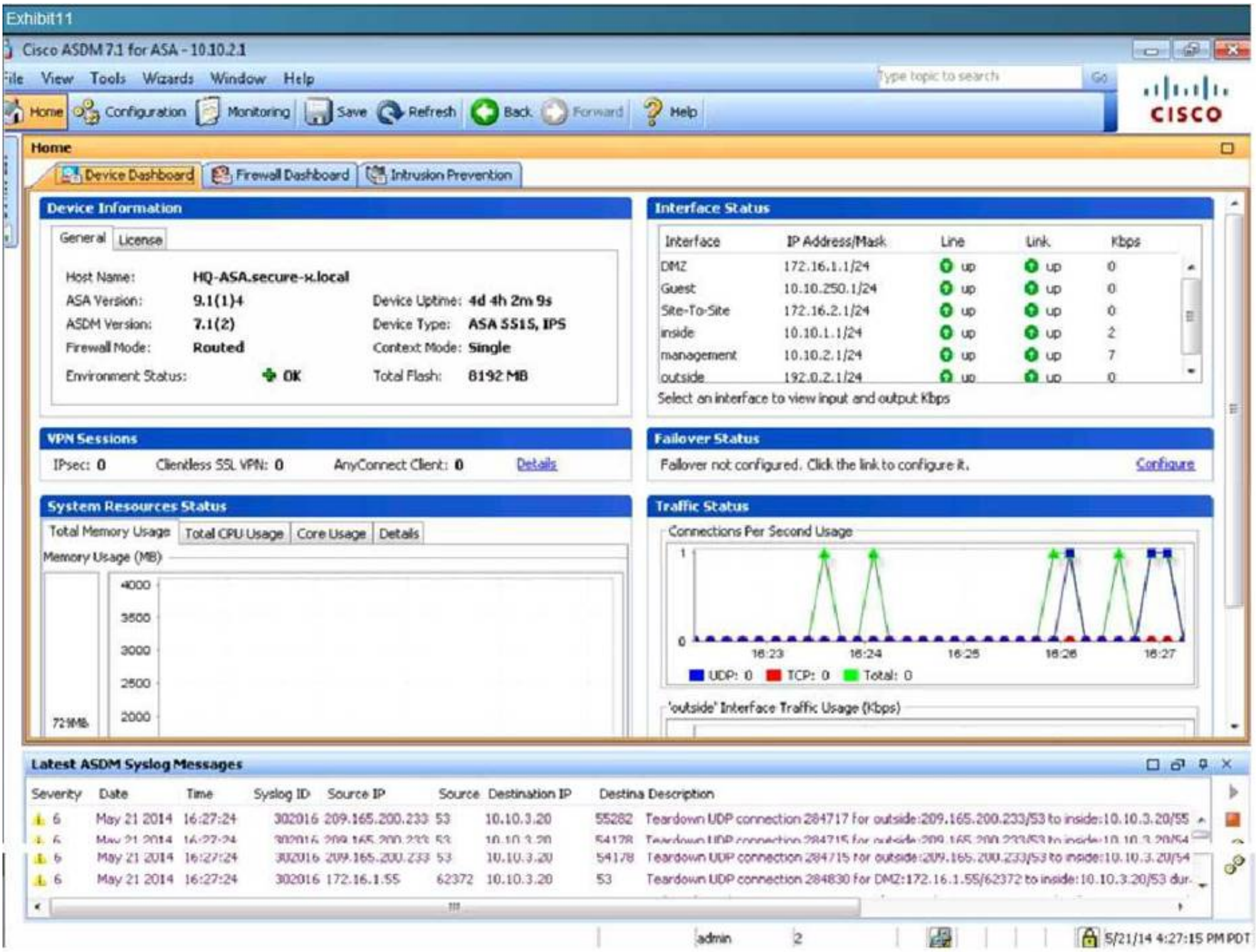
C. HTTP Shockwave Flash exploit
D. HTTP SQL injection attack

Answer: D

NEW QUESTION 392







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

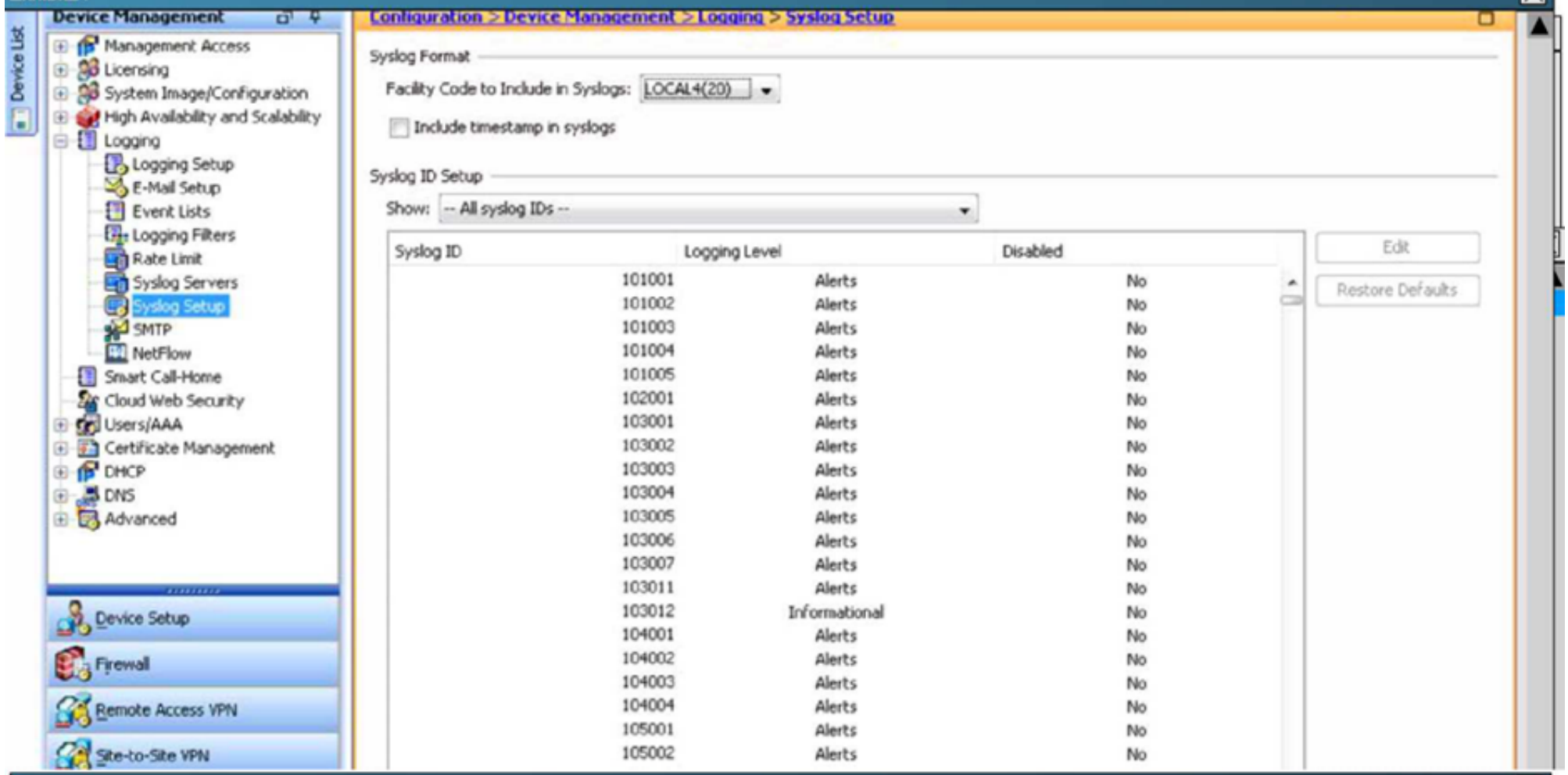
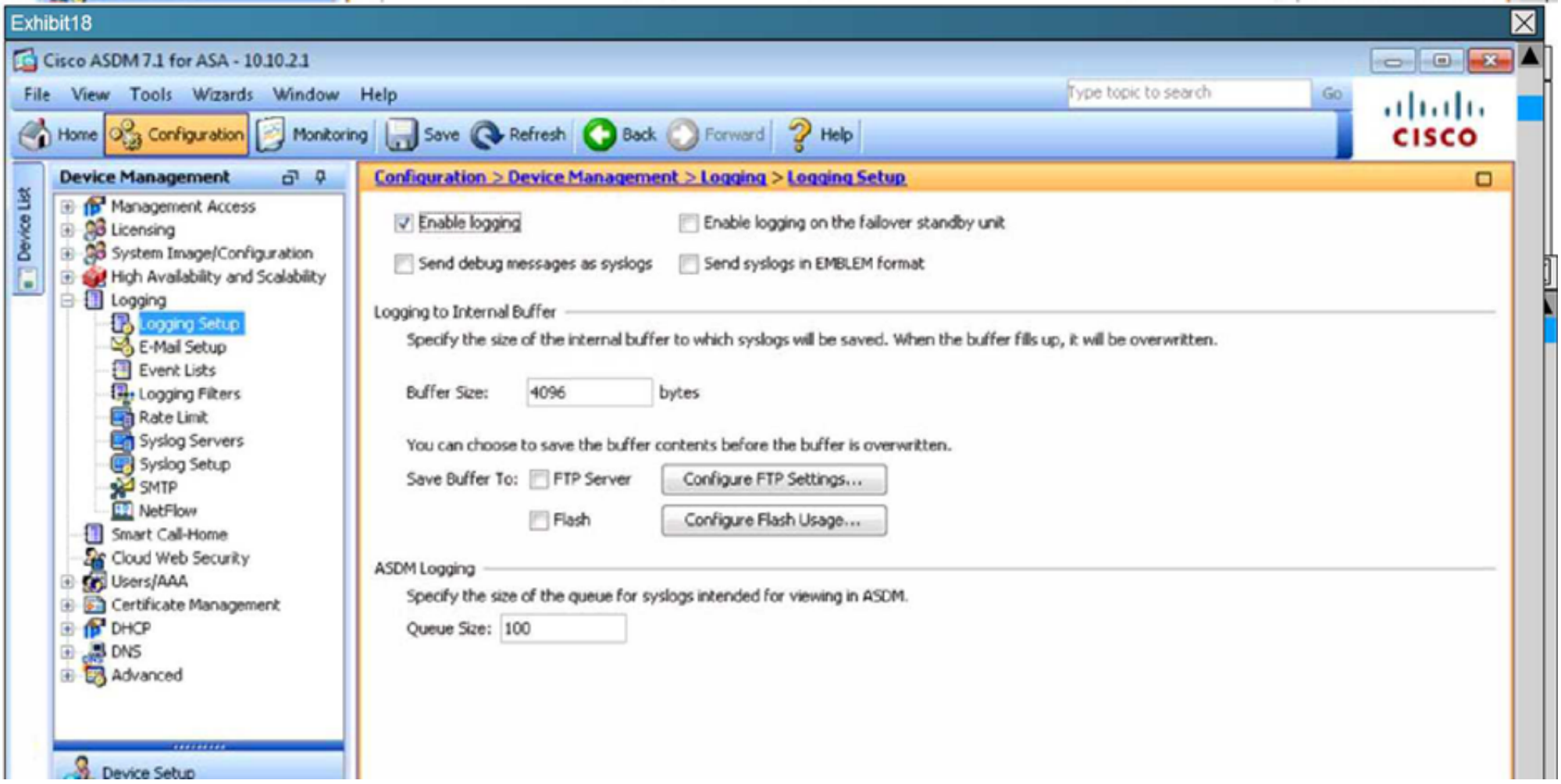


Exhibit18



NEW QUESTION 393

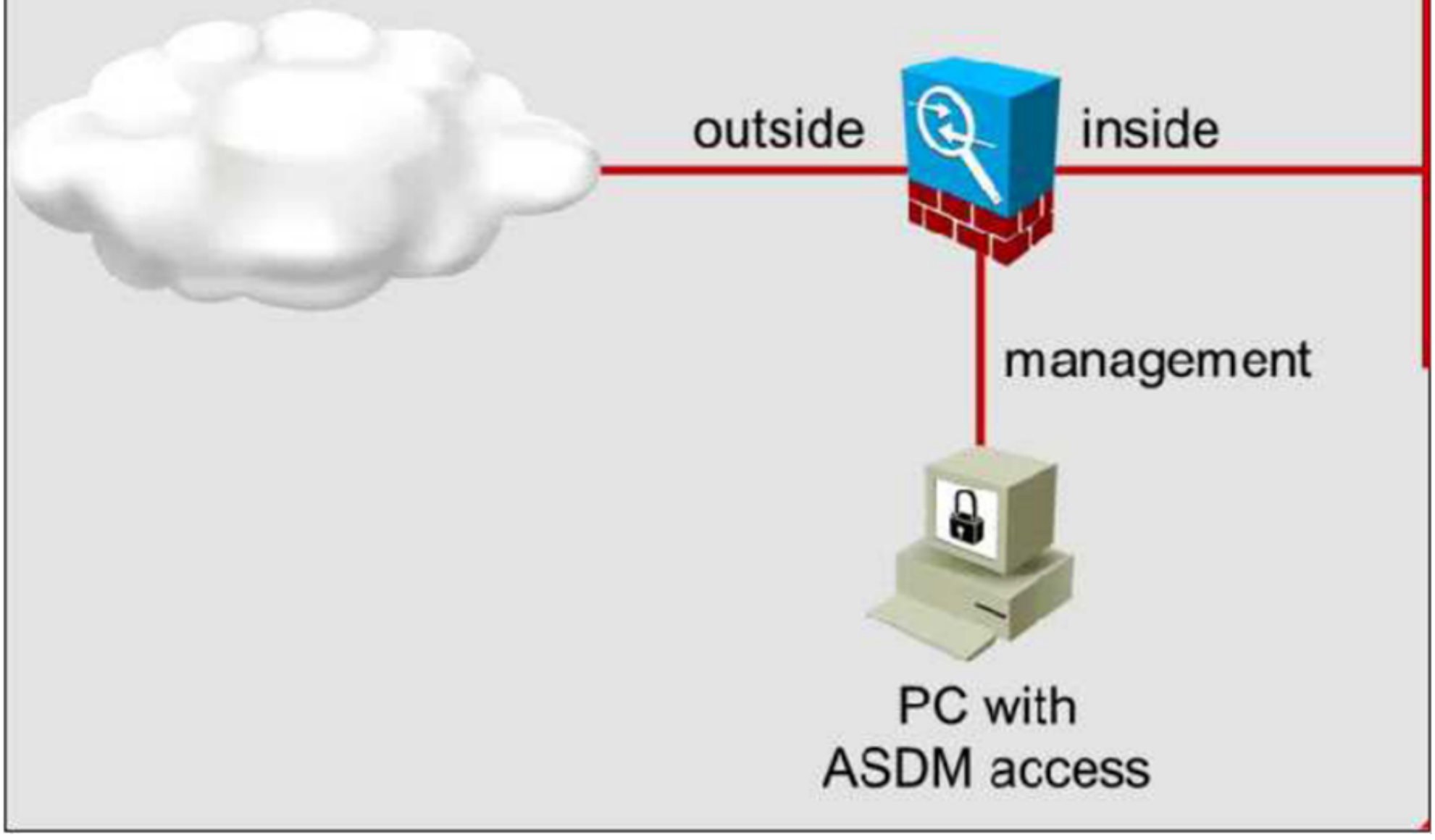
Scenario

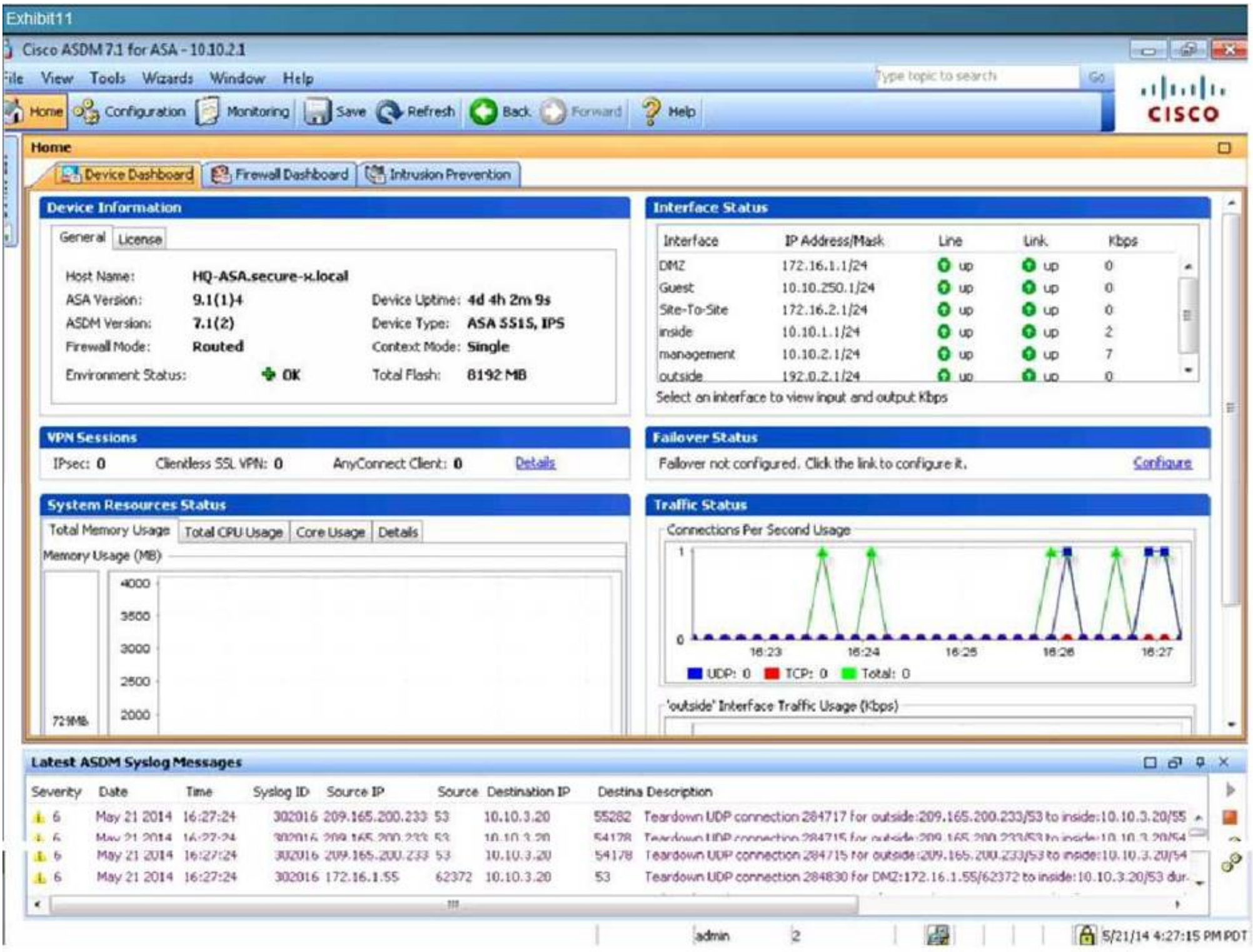
Click on the PC icon to access the Cisco ASDM. Using ASDM, answer the following three questions regarding the ASA configurations. (1 pt each per question)

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



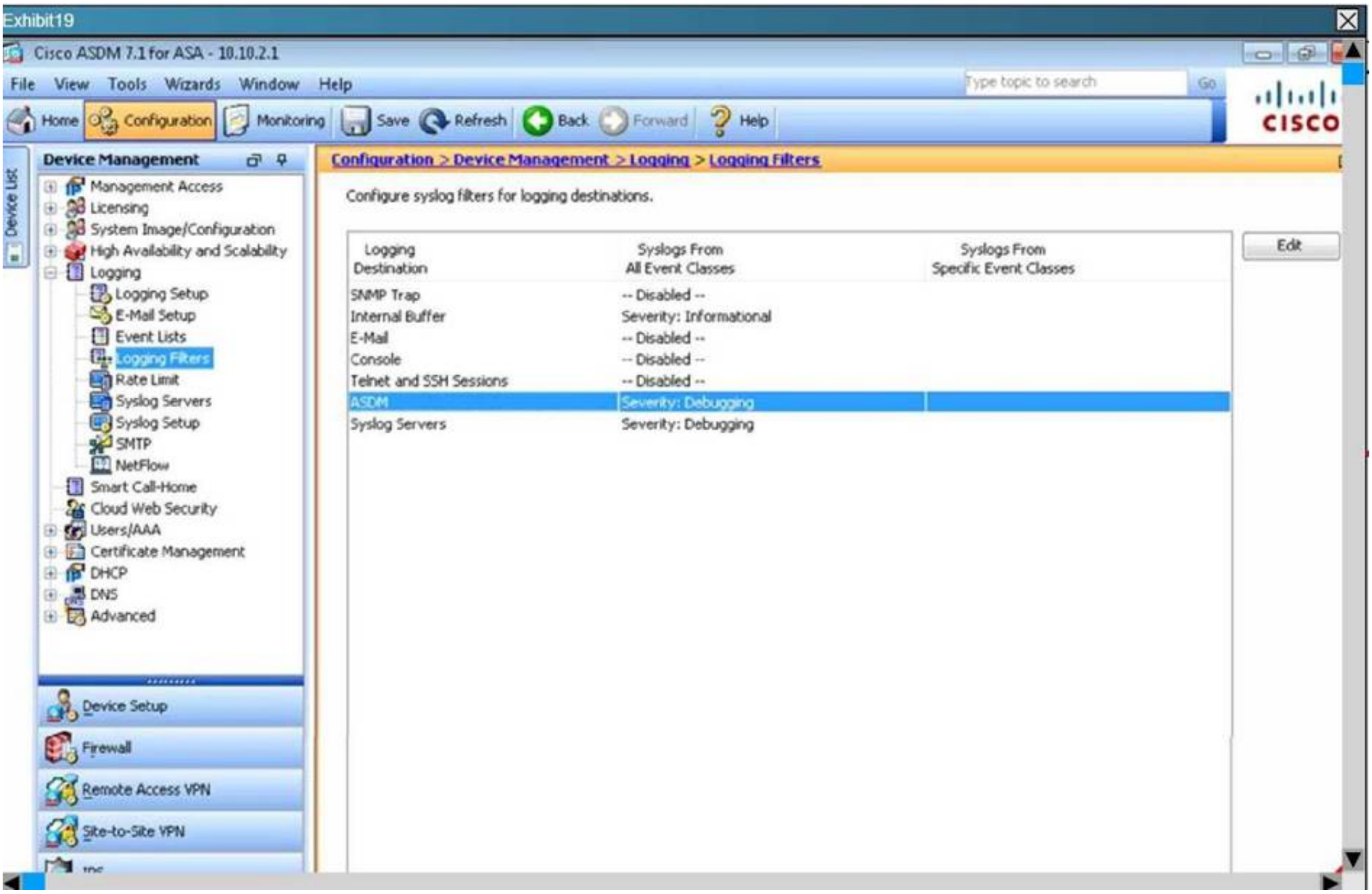


According to the logging configuration on the Cisco ASA, what will happen if syslog server 10.10.2.40 fails?

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 396
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 399
Which two option are protocol and tools are used by management plane when using cisco ASA general management plane hardening ?

A. Unicast Reverse Path Forwarding
B. NetFlow
C. Routing Protocol Authentication
D. Threat detection
E. Syslog
F. ICMP unreachables
G. Cisco URL Filtering

Answer: BE

Explanation:
http://www.cisco.com/web/about/security/intelligence/firewall-best-practices.html

NEW QUESTION 400
Which option describes the enhancements that SNMPv3 adds over 1 and 2 versions?

A. Predefined events that generate message from the SNMP agent to the NMS
B. Addition of authentication and privacy options
C. Cleartext transmission of data between SNMP server and SNMP agent

D. Addition of the ability to predefine events using traps
E. Pooling of devices using GET-NEXT requests
F. Use of the object identifier

Answer: B

Explanation:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html

NEW QUESTION 402
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 403
What is the best description of a unified ACL on a Cisco Firewall

A. An Ipv4 ACL with Ipv4 support
B. An ACL the support EtherType in additional Ipv6
C. An ACL with both Ipv4 and Ipv6 functionality
D. An Ipv6 ACL with Ipv4 backward compatitiblity

Answer: C

Explanation:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/i ntro_intro.html

NEW QUESTION 407
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 409
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 413
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 416
Which option is a different type of secondary VLAN?

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

Answer: D

NEW QUESTION 420
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 425
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 427
Which command is the first that you enter to check whether or not ASDM is installed on the ASA?

A. Show ip
B. Show running-config asdm
C. Show running-config boot
D. Show version
E. Show route

Answer: B

NEW QUESTION 432
Which option is the Cisco ASA on-box graphical management solution?

A. SSH
B. ASDM
C. Console
D. CSM

Answer: B

NEW QUESTION 434
At which layer does MACsecprovide encryption?

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

Answer: B

NEW QUESTION 439
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 444
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 449
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 450
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 455
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 456
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 457
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 462
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 463
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 464
Which activity is performed by the switch when Dynamic ARP inspection is configured?

A. It intercepts all ARP requests and responses on untrusted ports.
B. It forwards ARP packets that it receives on trusted ports, nust still checks them.
C. It drops ARP packets for MAC addresses that are not present in the DHCP snooping database table.
D. It bypasses all validation checks for MAC addresses that are present in the DHCP snooping database table.

Answer: A

Explanation:
DAI Intercepts all ARP requests and responses on untrusted ports. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/
dynarp.html#wp1082194

NEW QUESTION 465
When creating a cluster of Cisco ASA firewalls, which feature is configured on the cluster, instead of being applied to each Cisco ASA unit?

A. OSPF routing
B. URL filtering
C. HTTPS inspection
D. resource management

Answer: B

NEW QUESTION 467
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 469
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 470
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 472
An engineer is configuring MACsec encryption. 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: BC

NEW QUESTION 474
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 477
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 482
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 484
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 487
An engineer must implement secure device management on a Cisco ASA. Which two actions are required? (Choose two)

A. enable logging
B. enable Telnet
C. enable SSH
D. disable login timeouts
E. configure SNMPv3

Answer: CE

Explanation: Management plane: The management plane manages traffic that is sent to the Cisco firewall device and is composed of applications and protocols such as SSH and Simple Network Management Protocol (SNMP), the more secure version for SNMP is SNMPv3. http://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html

NEW QUESTION 490
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 491
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 495
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 498
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

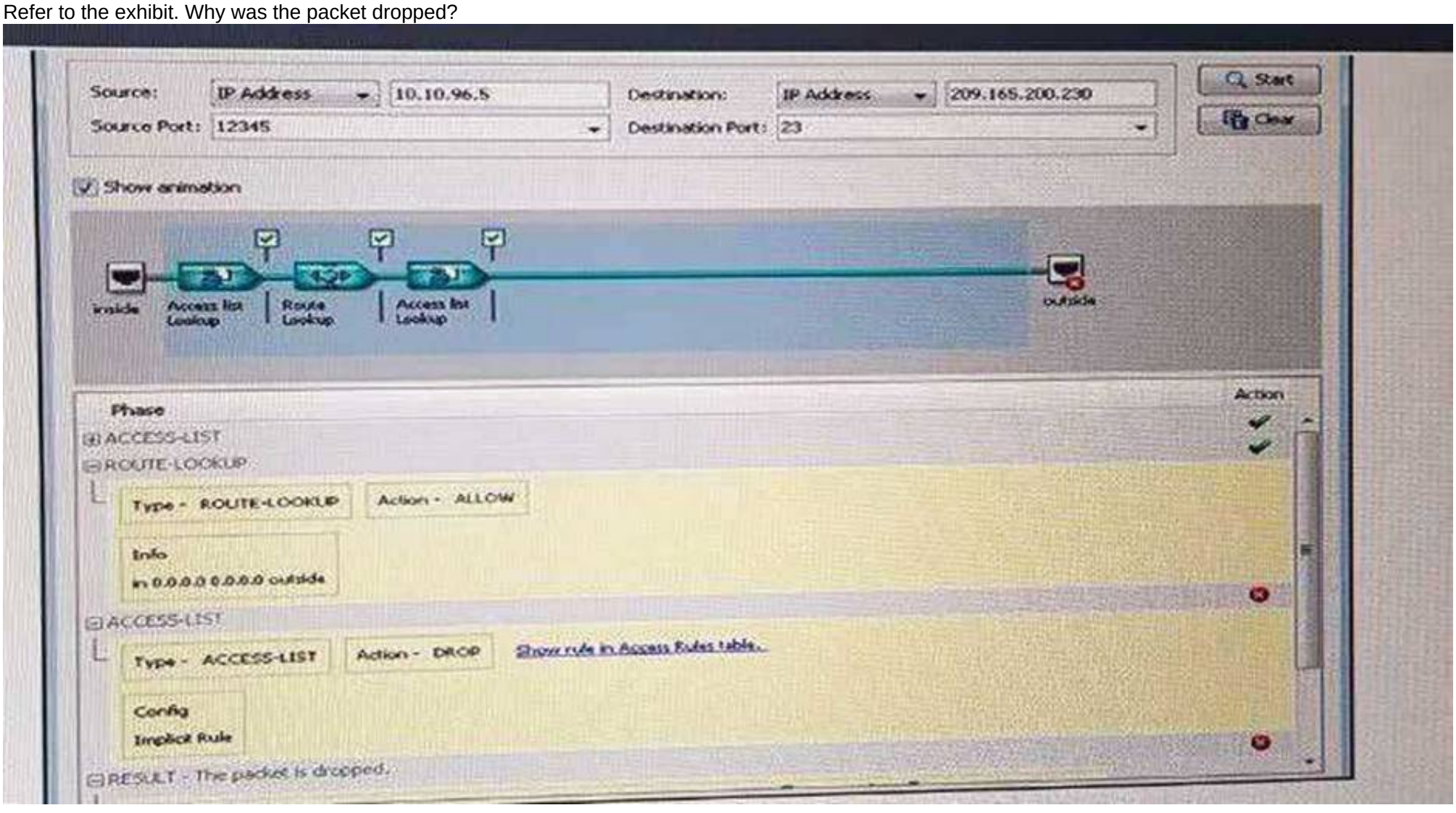
NEW QUESTION 502
Which hypervisor technology is supported by Cisco ASA 1000V Cloud Firewall?

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 504
Refer to the exhibit. Why was the packet dropped?

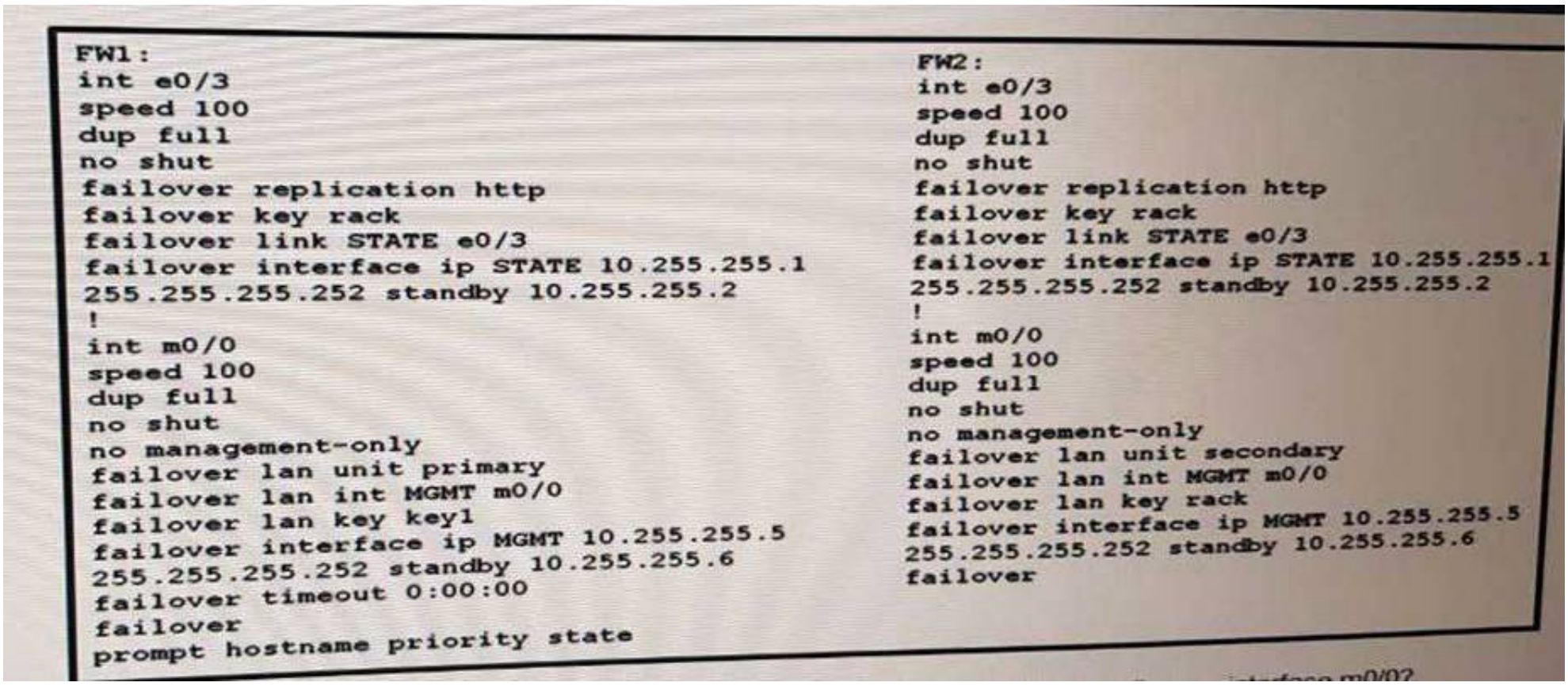


(this exhibit is packet capture with traffic destination to port 23 and being drop by access-list)

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 505
Refer to the exhibit.



Which Information Is passed between the active and standby Cisco ASA firewalls over interface m0/0?

A. TCP connection status
B. network link status
C. ARP table
D. SIP signaling session

Answer: A

NEW QUESTION 506
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 508
Which is the minimum RSA crypto key generate for SSH2?

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

Answer: B

NEW QUESTION 509
Which command change secure HTTP port from 443 to 444?

A. IP http secure-port 444
B. IP http secure-server
C. http server enable 444
D. IP http server-secure

Answer: C

Explanation: The ip http secure-port command can set the HTTPS port number from the default value of 443, if required.
http://www.ciscopress.com/articles/article.asp?p=2246945&seqNum=2

NEW QUESTION 513
How does the DAI works? (Choose two)

A. DAI relies on DHCP snooping.
B. It is applied on configured untrusted interfaces
C. IP address binding stored in trusted database
D. User-configured ARP ACLs

Answer: AB

NEW QUESTION 518

Which two options are available with cisco security manager (more of benefits of using cisco security manager?

A. Open simultaneous connections to each FW
B. Upgrade operating system
C. Upgrade IPS signatures
D. Automatic software upgrade

Answer: CD

NEW QUESTION 523
What mean following command arp outside 10.1.1.1 0009.xxxx.2100?

A. create static arp entry
B. create virtual arp entry
C. It manually assign host to access outside

Answer: A

NEW QUESTION 527
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 529
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 531
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 535
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 538
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 539
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 544
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**

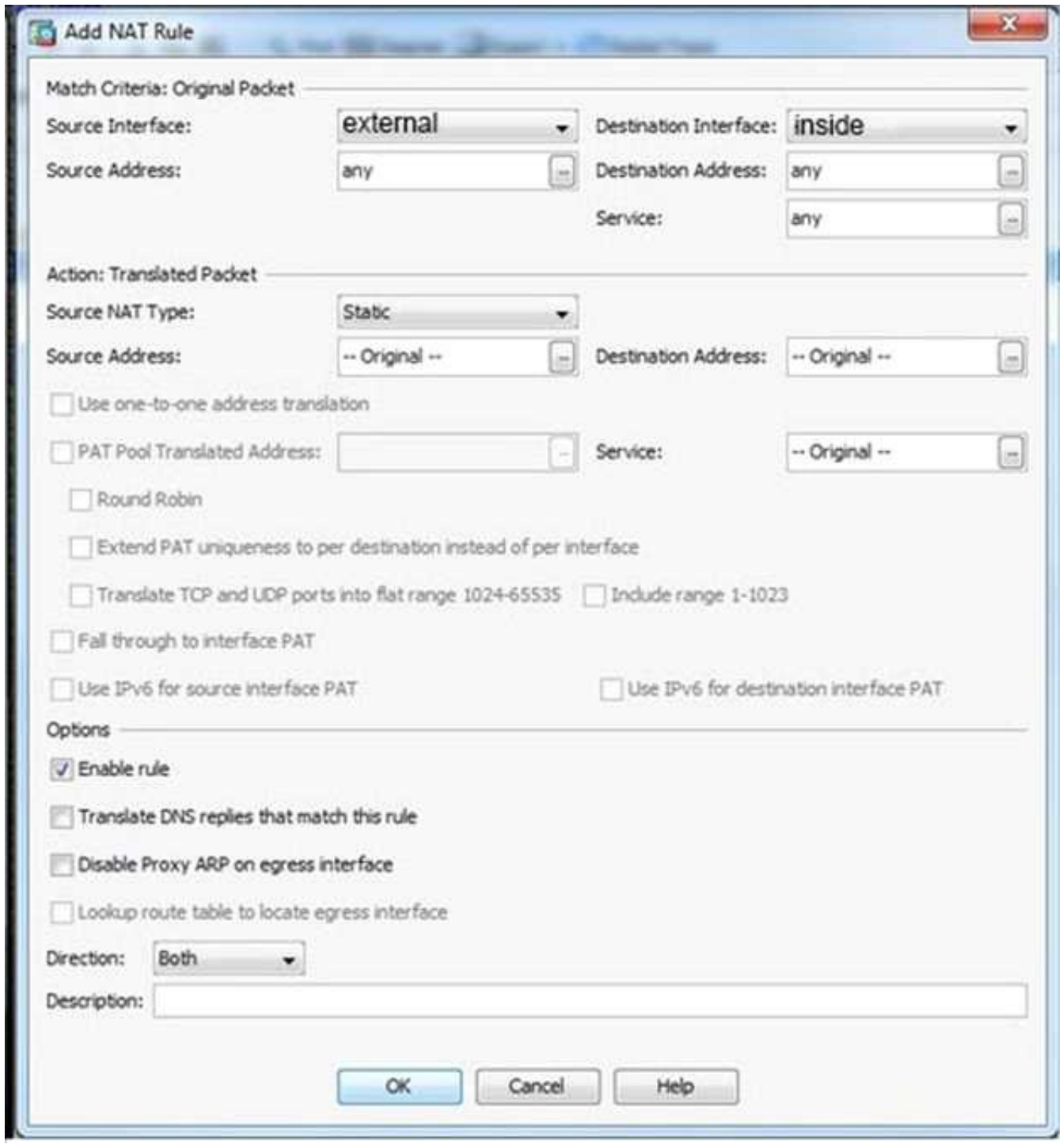
( )%ASA-7-102398 **Debugging**

NEW QUESTION 547
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 548
DRAG DROP



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 552

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-206 Exam with Our Prep Materials Via below:

https://www.certleader.com/300-206-dumps.html