

300-206 Dumps

Implementing Cisco Edge Network Security Solutions

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



NEW QUESTION 1

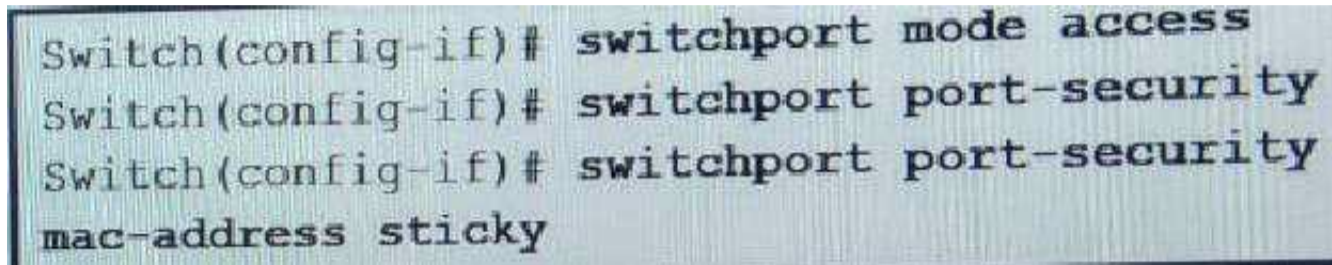
Which two user privileges does ASDM allow engineer to create? (Choose two)

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

Answer: CE

NEW QUESTION 2

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 switch port waits one minute to recover by default.
- B. Only one MAC address can be learned 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 switch port shuts down.

Answer: BE

NEW QUESTION 3

An engineer is applying best practices to stop STP unauthorized changes from the user's 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 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

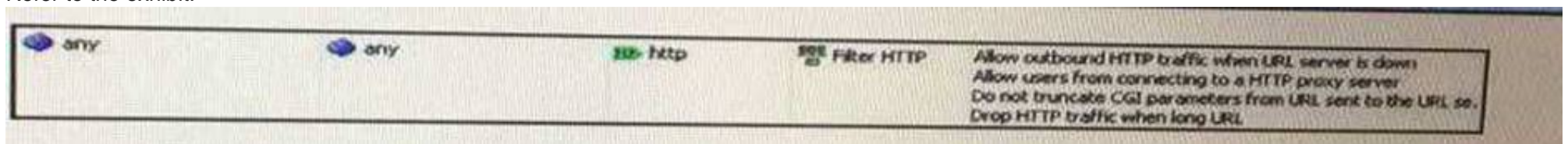
Which two main functions for application inspection on ASA are true?

- 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 balanced across the servers equally.

Answer: AB

NEW QUESTION 6

Refer to the exhibit.



```
any any http Filter HTTP
Allow outbound HTTP traffic when URL server is down
Allow users from connecting to a HTTP proxy server
Do not truncate CGI parameters from URL sent to the URL server
Drop HTTP traffic when long URL
```

Which option describes the role of the filter rule on this Cisco ASA firewall?

- A. to discard http traffic destined to a proxy server

- B. to define allowed traffic when the URL filtering server is unavailable
- C. to perform deep packet inspection on all http traffic crossing the Cisco ASA
- D. to send http traffic to a defined URL filtering server

Answer: D

NEW QUESTION 7

Which option is a consequence when an engineer changes the snmp server local engineID in router?

- A. The SNMP configuration that was created previously is invalid.
- B. The users that were created previously are invalid.
- C. The community that was created previously is invalid.
- D. The groups that were created previously are invalid

Answer: B

NEW QUESTION 8

An engineer has downloaded the database files for botnet traffic filtering on an AS

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

Answer: A

NEW QUESTION 9

Which benefit of using centralized management to manage a Cisco IronPort ESA is true?

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

Answer: D

NEW QUESTION 10

Which 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 10

An engineering team is working diligently to achieve the fastest possible throughput on a Cisco ASA deployment within the data center without sacrificing high availability or flexibility. Which type of architecture accomplishes this goal?

- A. multiple mode, transparent contexts
- B. single mode, transparent contexts
- C. multiple mode, routed contexts
- D. single mode, routed contexts

Answer: C

NEW QUESTION 15

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 20

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 22

DRAG DROP

Drag and drop the function on the left onto the matching packet capture configuration types on the right. Not all options are used.

captures inbound and outbound packets on one or more interfaces

asa_dataplane

captures traffic between an IPS module and the Cisco ASA

asp-drop

captures packets with Layer 2 to inline SGT

ethernet-type

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

captures packets dropped for a particular reason

Answer:

Explanation: Reference:

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

NEW QUESTION 23

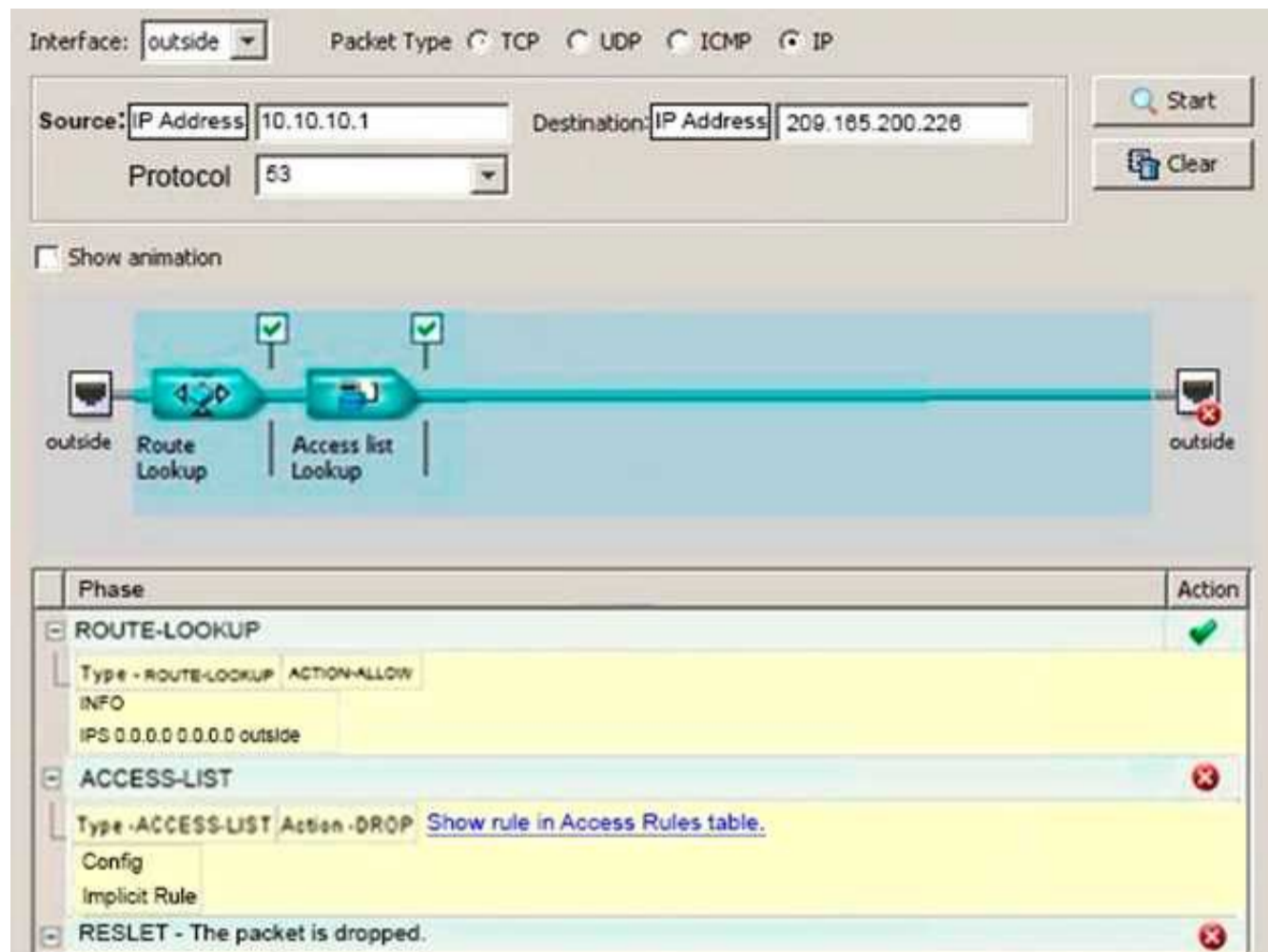
A hacker is sniffing network traffic from a Cisco Catalyst switch on a company network. Which three pieces of information can be obtained from intercepted Cisco Discovery Protocol traffic? (Choose three.)

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

Answer: DEF

NEW QUESTION 28

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 30

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 34

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 39

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?

The screenshot shows the Cisco ASDM configuration page for Firewall Identity Options. The 'Domains' table lists two domains: DC1 and DOMAIN. DC1 is associated with AD Server Group AD and has 'Disable Rules When Server Is Down' unchecked. DOMAIN is associated with AD Server Group AD1 and also has 'Disable Rules When Server Is Down' unchecked. The 'Default Domain' is set to LOCAL. The 'Active Directory Agent' section shows 'Agent Group' as RADIUS, 'Hello Timer' as 30 seconds, 'Poll Groups Timer' as 8 hours, and 'Retrieve User Information' as Full Download. The 'Error Conditions' section has four unchecked options: 'Disable Rules When Active Directory Agent Is Down', 'Remove User IP When NetBIOS Probe Fails', 'Remove User IP When User's MAC Address Is Inconsistent', and 'Track User Not Found'. The 'Users' section has 'Idle Timeout' checked and set to 60 minutes. The 'NetBIOS Logout Probe' section has 'Enable' unchecked. The 'Probe Timer' is set to 1 minute.

- 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 45

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 49

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	step 1
default rules from parent policy	step 2
mandatory rules from parent policy	step 3

Answer:

Explanation:



NEW QUESTION 50

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

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 62

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	top users by blocked transactions
threat report	top 25 attackers and top 25 vulnerable targets
user report	traffic summary by transactions
applciation report	top applications by blocked transactions
endpoint report	top operating systems by blocked transactions

Answer:

Explanation:

user report
threat report
traffic summary report
applciation report
endpoint report

NEW QUESTION 63

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 68

Which two options can be used when configuring a packet capture from the command line within the ASA using the capture command? (Choose two.)

- A. host
- B. snap-length
- C. type
- D. detail
- E. real-time

Answer: CE

NEW QUESTION 70

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 74

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 78

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 80

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 83

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 85

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

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

Answer: A

NEW QUESTION 90

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 93

Which option is a Cisco best practice when configuring traffic storm control?

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

Answer: B

NEW QUESTION 98

Which three commands can be used to harden a switch? (Choose three.)

- A. switch(config-if)# spanning-tree bpdupfilter enable
- B. switch(config)# ip dhcp snooping
- C. switch(config)# errdisable recovery interval 900
- D. switch(config-if)# spanning-tree guard root
- E. switch(config-if)# spanning-tree bpduguard disable
- F. switch(config-if)# no cdp enable

Answer: BDF

NEW QUESTION 103

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 106

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 network devices.
- 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 109

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

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

Answer: A

NEW QUESTION 112

Which statement about SNMP support on the Cisco ASA appliance is true?

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

Answer: C

NEW QUESTION 113

Which statement about Cisco ASA multicast routing support is true?

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

Answer: D

NEW QUESTION 118

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 119

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 124

A network engineer is asked to configure NetFlow to sample one of every 100 packets on a router's fa0/0 interface. Which configuration enables sampling, assuming that NetFlow is already configured and running on the router's fa0/0 interface?

- A. `flow-sampler-map flow1 mode random one-out-of 100 interface fas0/0 flow-sampler flow1`
- B. `flow monitor flow1 mode random one-out-of 100 interface fas0/0 ip flow monitor flow1`
- C. `flow-sampler-map flow1 one-out-of 100 interface fas0/0 flow-sampler flow1`
- D. `ip flow-export source fas0/0 one-out-of 100`

Answer: A

NEW QUESTION 125

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 130

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 135

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 140

To which interface on a Cisco ASA 1000V firewall should a security profile be applied when a VM sits behind it?

- A. outside
- B. inside
- C. management
- D. DMZ

Answer: B

NEW QUESTION 141

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

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

Answer: D

NEW QUESTION 146

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 network devices.
- 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 148

Which tool provides the necessary information to determine hardware lifecycle and compliance details for deployed network devices?

- A. Prime Infrastructure
- B. Prime Assurance
- C. Prime Network Registrar
- D. Prime Network Analysis Module

Answer: A

NEW QUESTION 153

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 156

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 159

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 160

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 162

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 164

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 165

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 169

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 174

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 176

Which option describes the purpose of the input parameter when you use the packet-tracer command on a Cisco device?

- A. to provide detailed packet-trace information
- B. to specify the source interface for the packet trace
- C. to display the trace capture in XML format
- D. to specify the protocol type for the packet trace

Answer: B

NEW QUESTION 179

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

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

Answer: B

NEW QUESTION 183

Which five options are valid logging destinations for the Cisco ASA? (Choose five.)

- A. AAA server
- B. Cisco ASDM
- C. buffer
- D. SNMP traps
- E. LDAP server
- F. email
- G. TCP-based secure syslog server

Answer: BCDFG

NEW QUESTION 185

When configuring security contexts on the Cisco ASA, which three resource class limits can be set using a rate limit? (Choose three.)

- A. address translation rate
- B. Cisco ASDM session rate
- C. connections rate
- D. MAC-address learning rate (when in transparent mode)
- E. syslog messages rate
- F. stateful packet inspections rate

Answer: CEF

NEW QUESTION 190

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 191

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

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

Answer: C

NEW QUESTION 193

Enabling what security mechanism can prevent an attacker from gaining network topology information from CDP?

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

Answer: A

NEW QUESTION 196

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 198

Which threat-detection feature is used to keep track of suspected attackers who create connections to too many hosts or ports?

- A. complex threat detection
- B. scanning threat detection
- C. basic threat detection
- D. advanced threat detection

Answer: B

NEW QUESTION 199

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 200

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 203

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 205

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 policies.
- D. It enables NAT policy rediscovery while leaving existing shared policies unchanged.

Answer: D

NEW QUESTION 210

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 213

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 214

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 217

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 221

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 223

What is the maximum jumbo frame size for IPS standalone appliances with 1G and 10G fixed or add-on interfaces?

- A. 1024 bytes
- B. 1518 bytes
- C. 2156 bytes
- D. 9216 bytes

Answer: D

NEW QUESTION 228

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 232

An administrator is deploying port-security to restrict traffic from certain ports to specific MAC addresses. Which two considerations must an administrator take into account when using the switchport port-security macaddress sticky command? (Choose two.)

- A. The configuration will be updated with MAC addresses from traffic seen ingressing the port. The configuration will automatically be saved to NVRAM if no other changes to the configuration have been made.
- B. The configuration will be updated with MAC addresses from traffic seen ingressing the port.
- C. The configuration will not automatically be saved to NVRAM.
- D. Only MAC addresses with the 5th most significant bit of the address (the 'sticky' bit) set to 1 will be learned.
- E. If configured on a trunk port without the 'vlan' keyword, it will apply to all vlans.
- F. If configured on a trunk port without the 'vlan' keyword, it will apply only to the native vlan.

Answer: BE

NEW QUESTION 234

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 238

Instructions

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

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

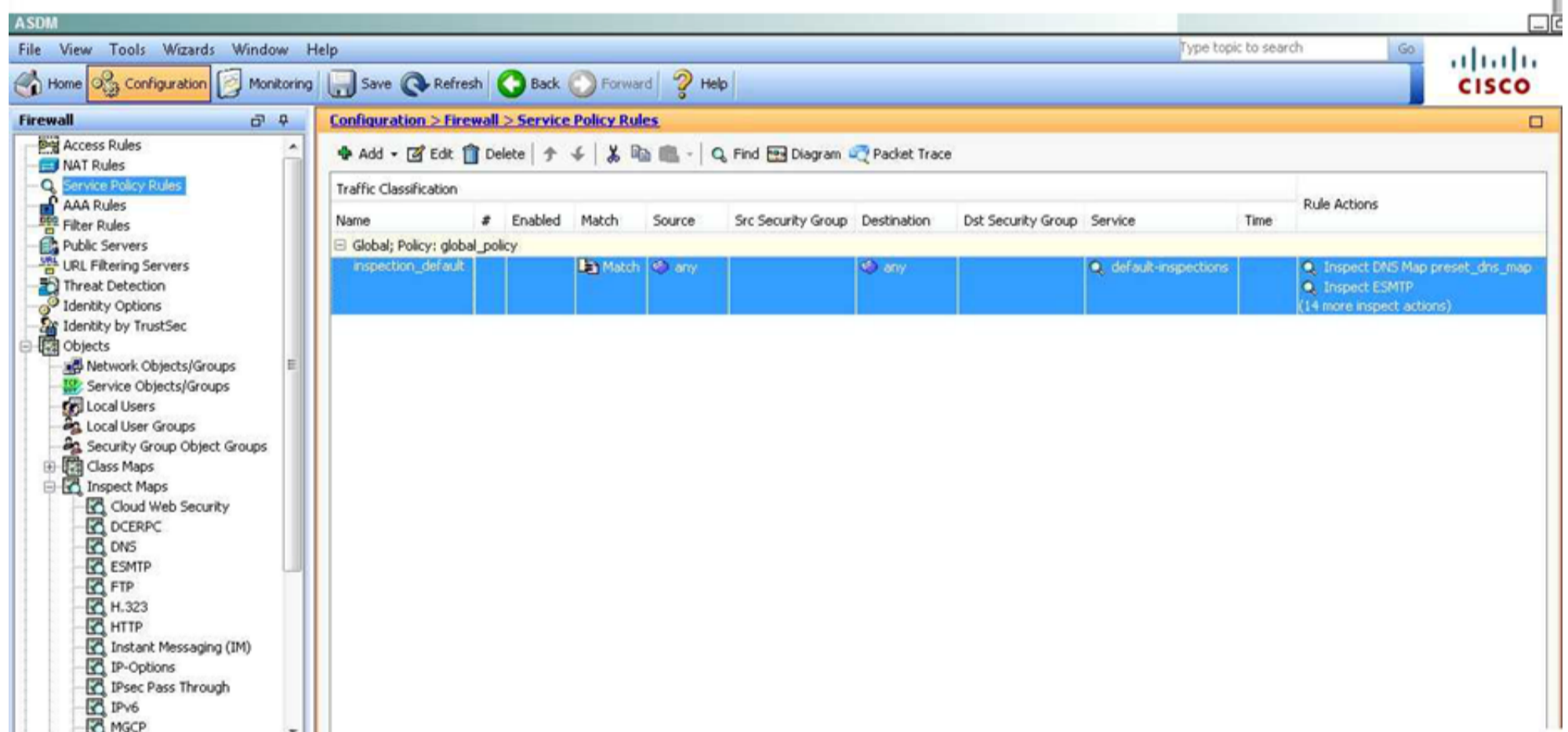
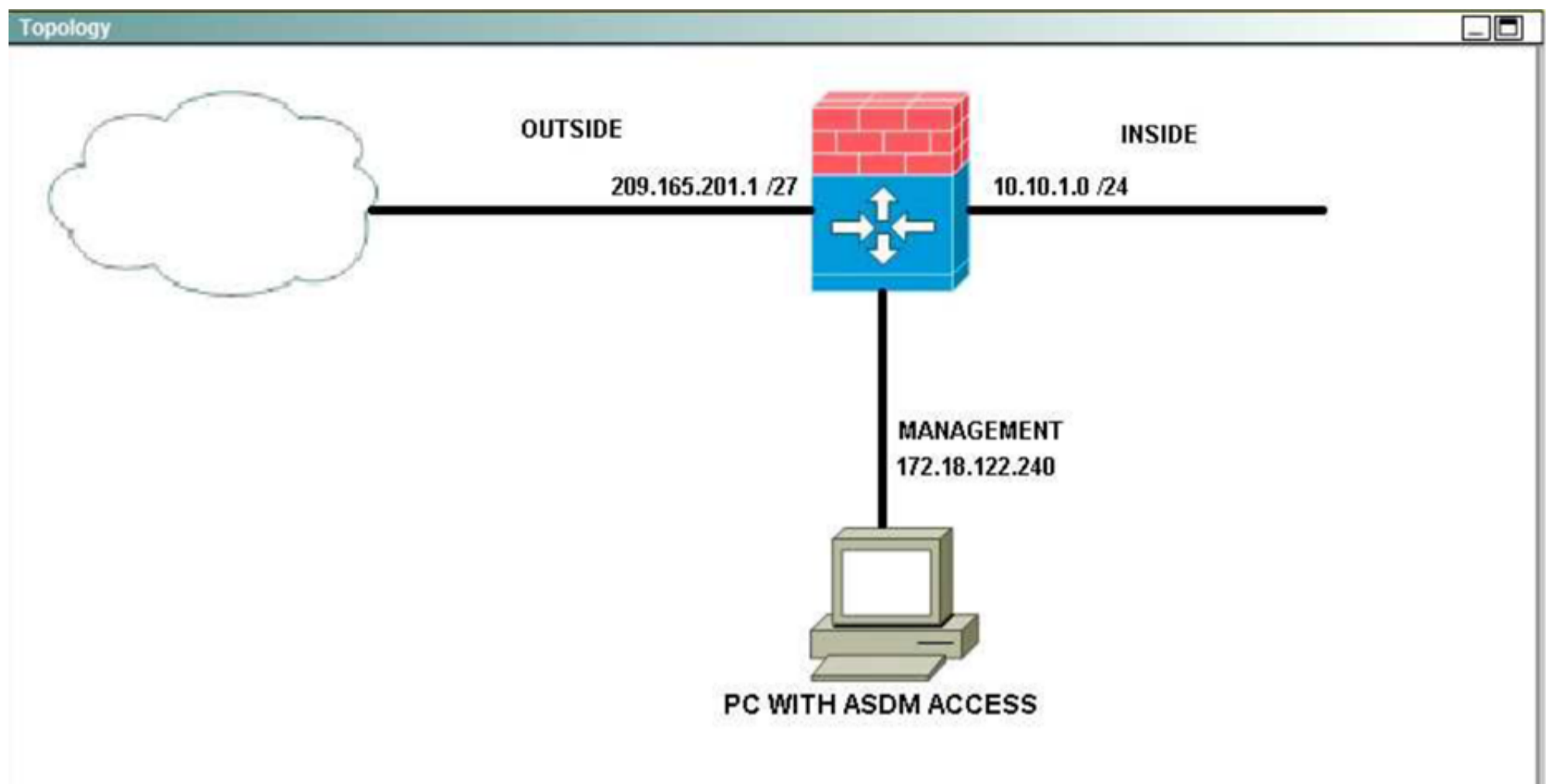
Scenario

You have been given access to a Cisco ASA 5512 Adaptive Security Appliance via Cisco ASDM. Use Cisco ASDM to edit the Cisco ASA 5505 Adaptive Security Appliance configurations to enable Advanced HTTP application inspection by completing the following tasks:

Starting from the Service Policy Rules ASDM pane,

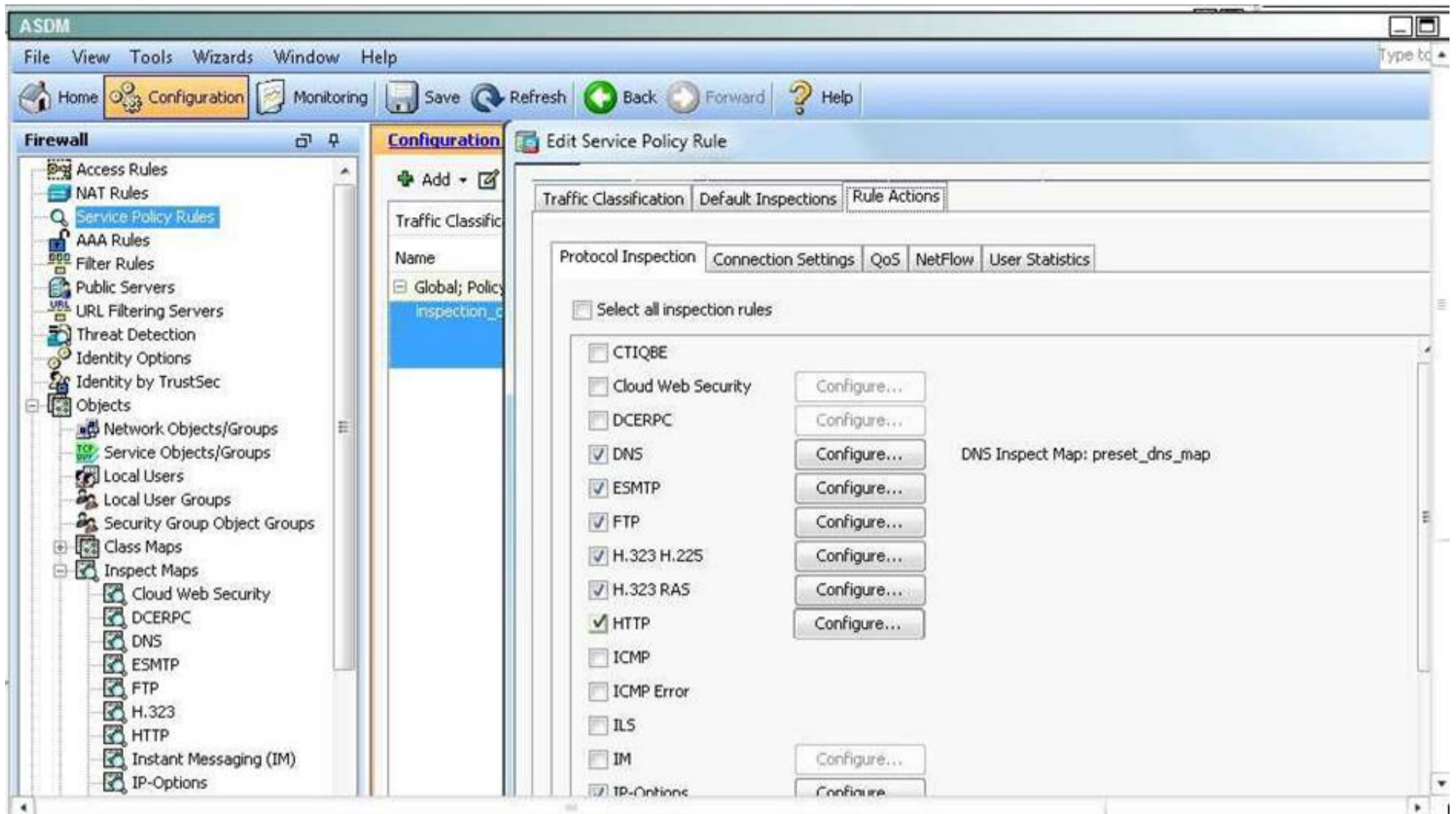
- Enable HTTP inspection globally on the Cisco ASA appliance
- Create a new HTTP Inspect Map named: **http-inspect-map** to:
 - Enable the *dropping* of any HTTP connections that encounter HTTP protocol violations
 - Enable the *dropping and logging* of any HTTP connections when the content type in the HTTP response does not match one of the MIME types in the accept field of the HTTP request

Note: After you complete the configuration, you do not need to save the running configuration to the startup-config. In this simulation, you cannot test the HTTP inspection policy that was created after you completed your configuration. Not all ASDM screens are fully functional. However, you should be able to view, edit, and delete the HTTP inspect map that you created from the **Configuration > Firewall > Objects > Inspect Maps > HTTP** ASDM screen.

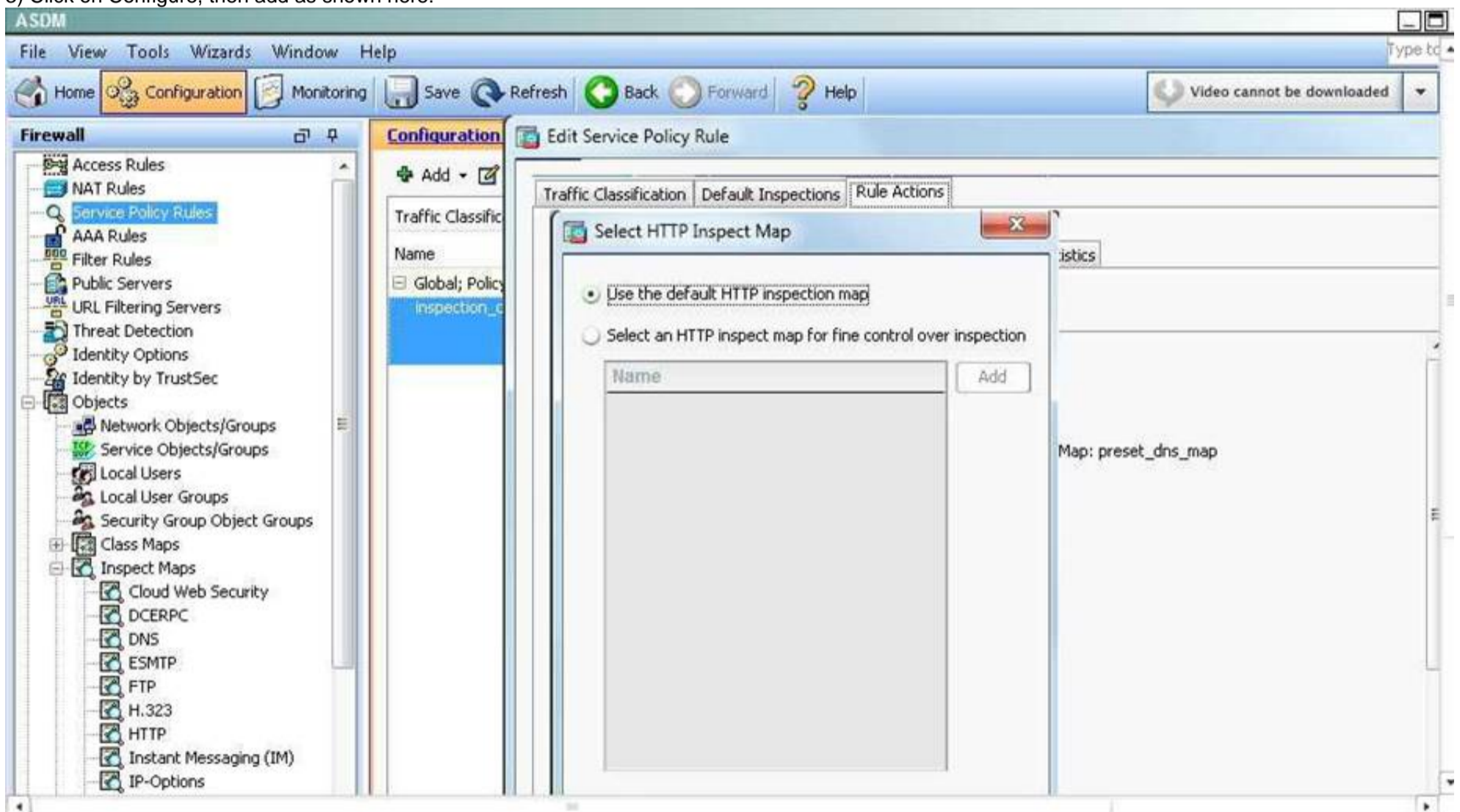


Answer:

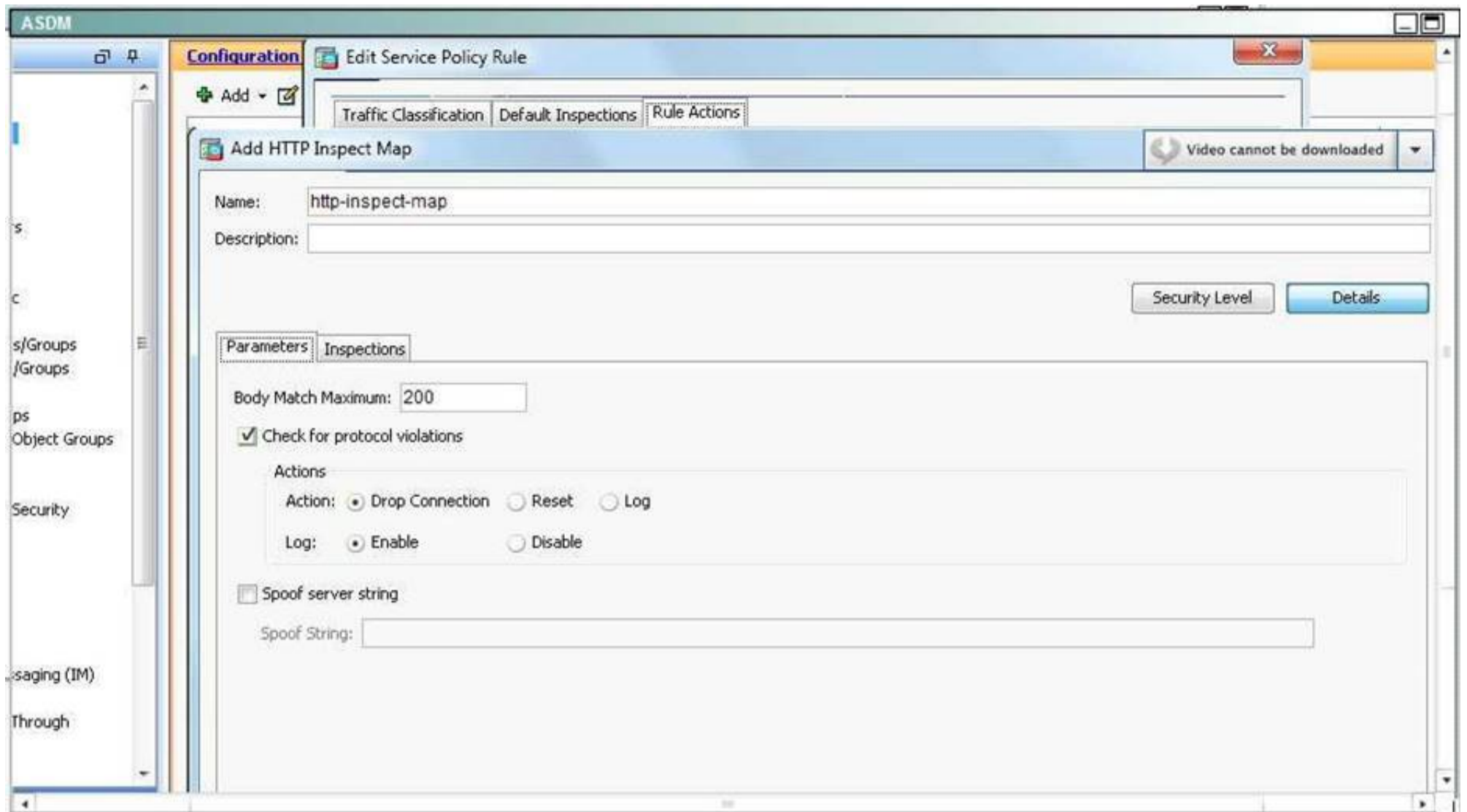
Explanation: 1) Click on Service Policy Rules, then Edit the default inspection rule.
2) Click on Rule Actions, then enable HTTP as shown here:



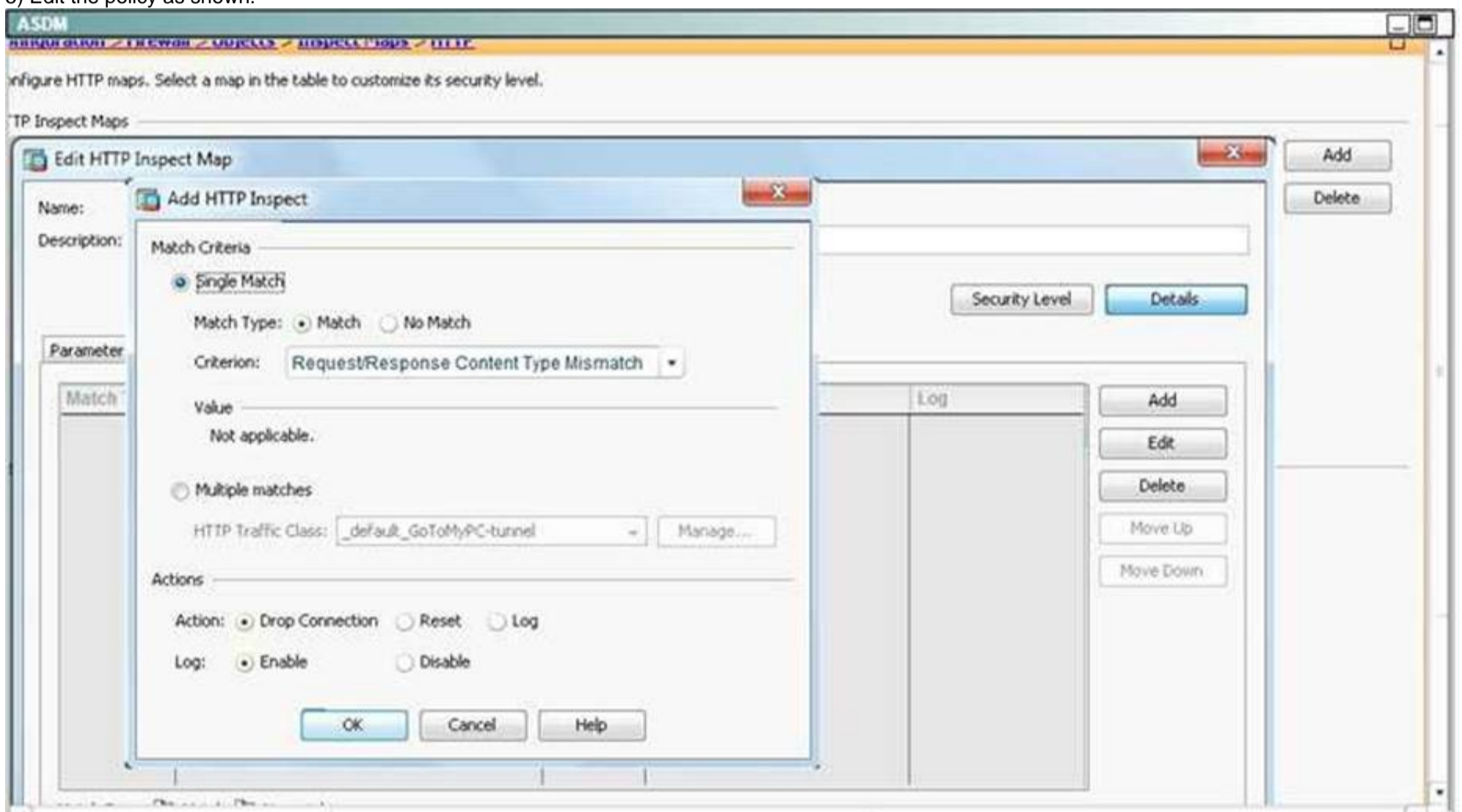
3) Click on Configure, then add as shown here:



4) Create the new map in ASDM like shown:

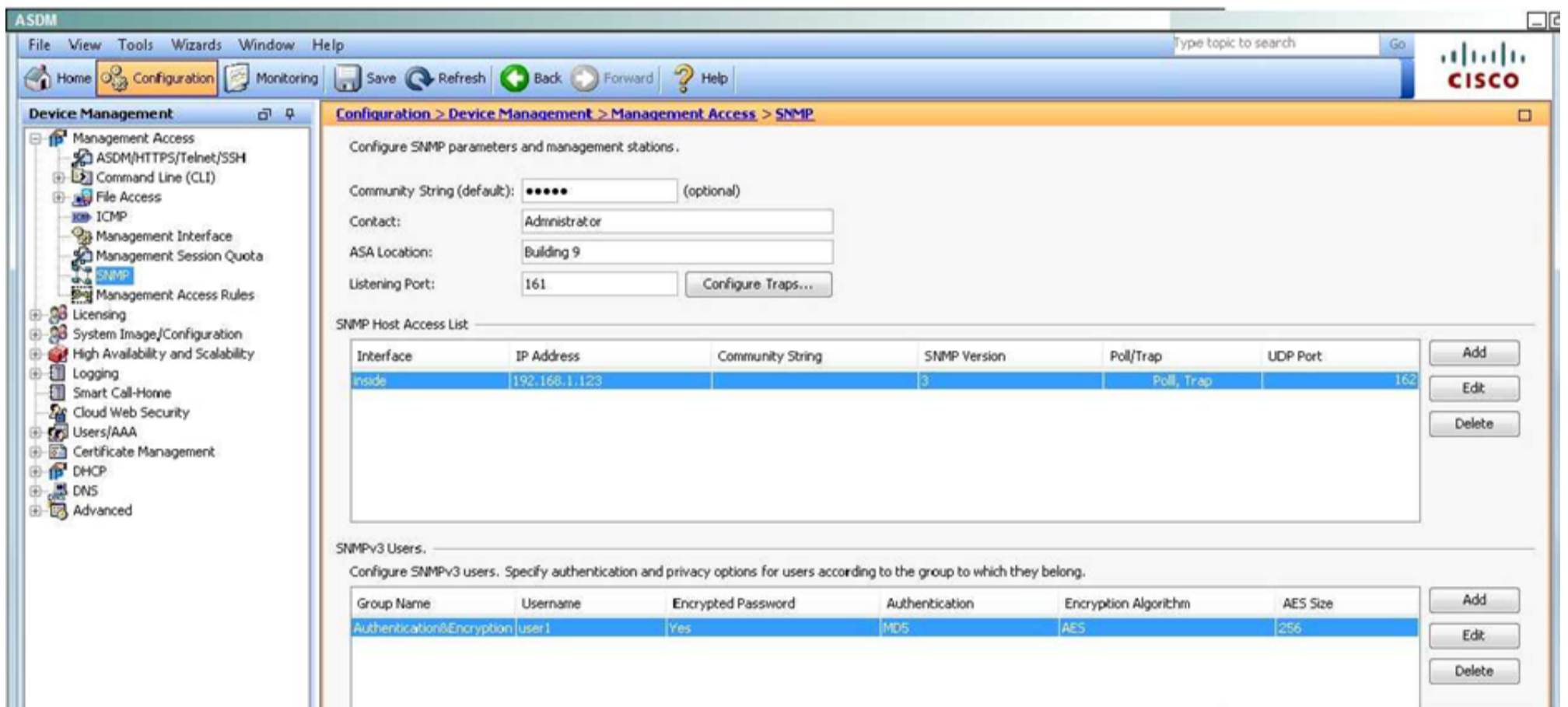
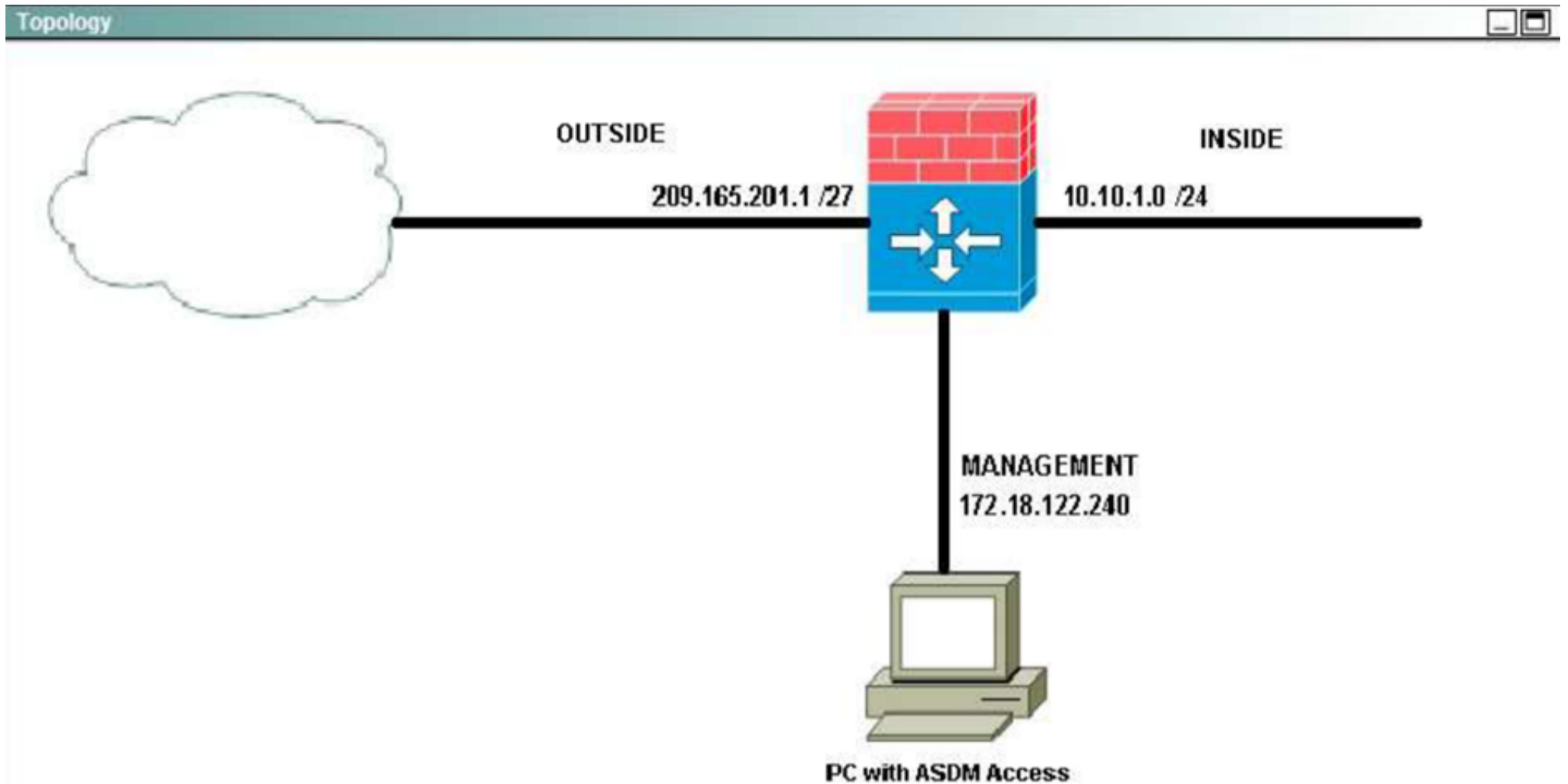


5) Edit the policy as shown:



6) Hit OK

NEW QUESTION 243

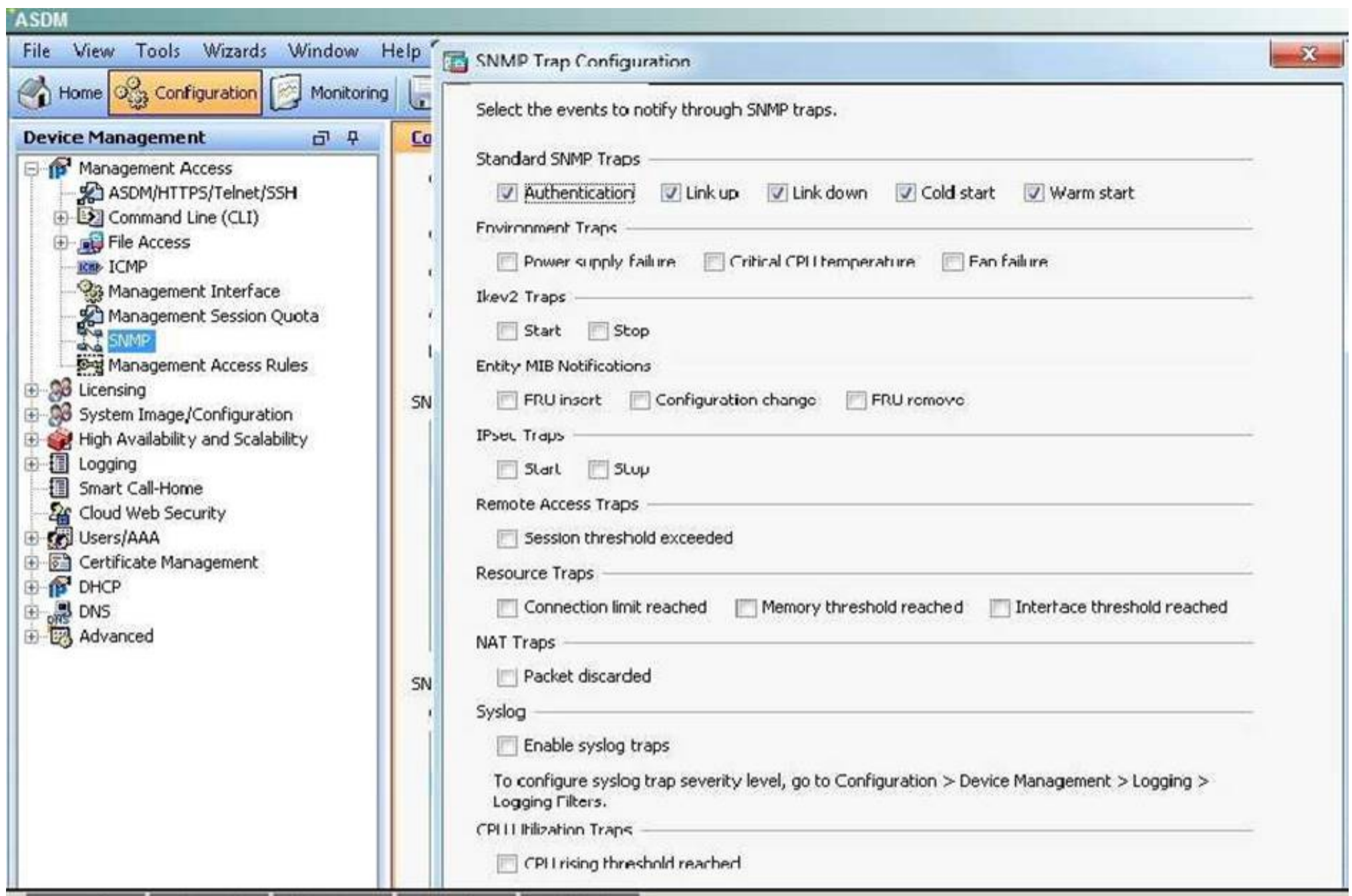


Which statement about how the Cisco ASA supports SNMP is true?

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

Answer: C

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



NEW QUESTION 248

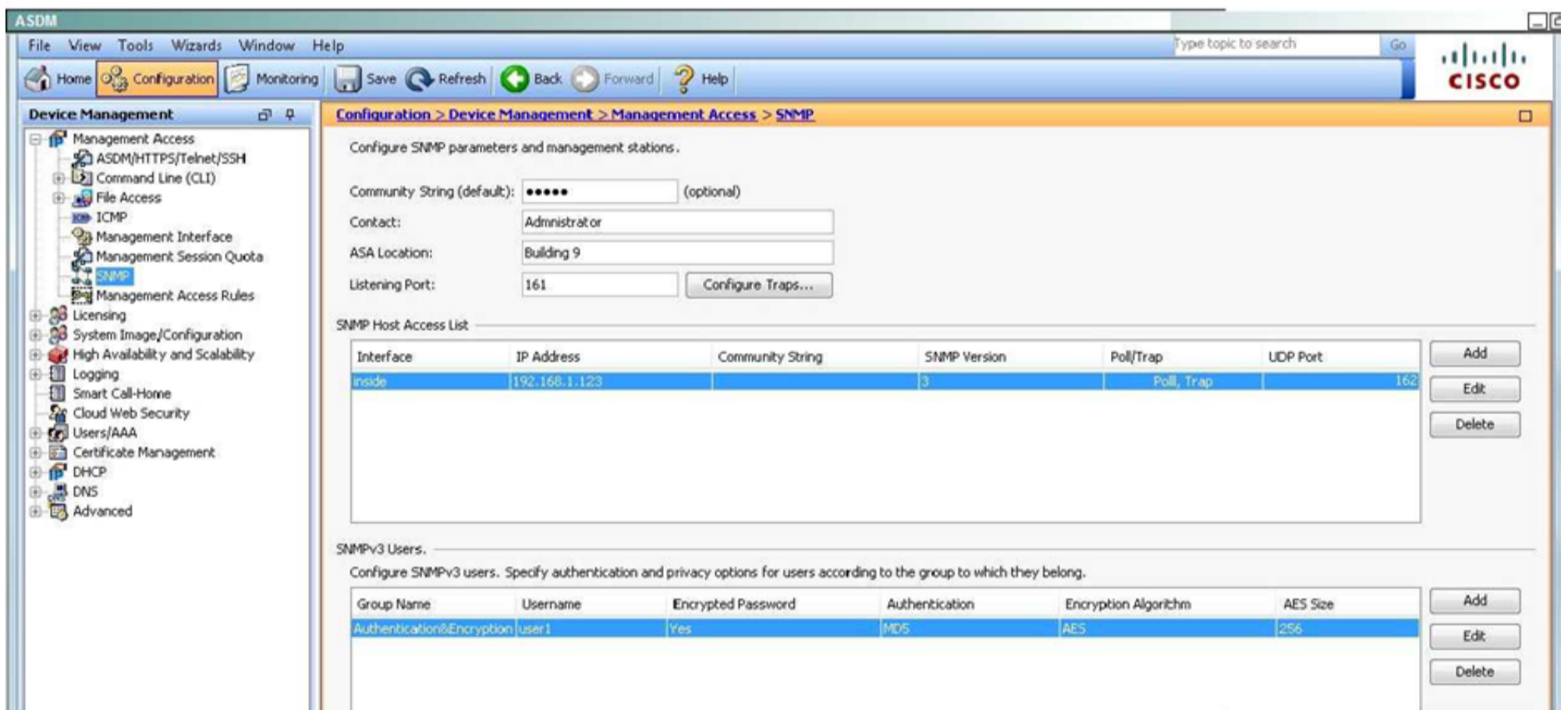
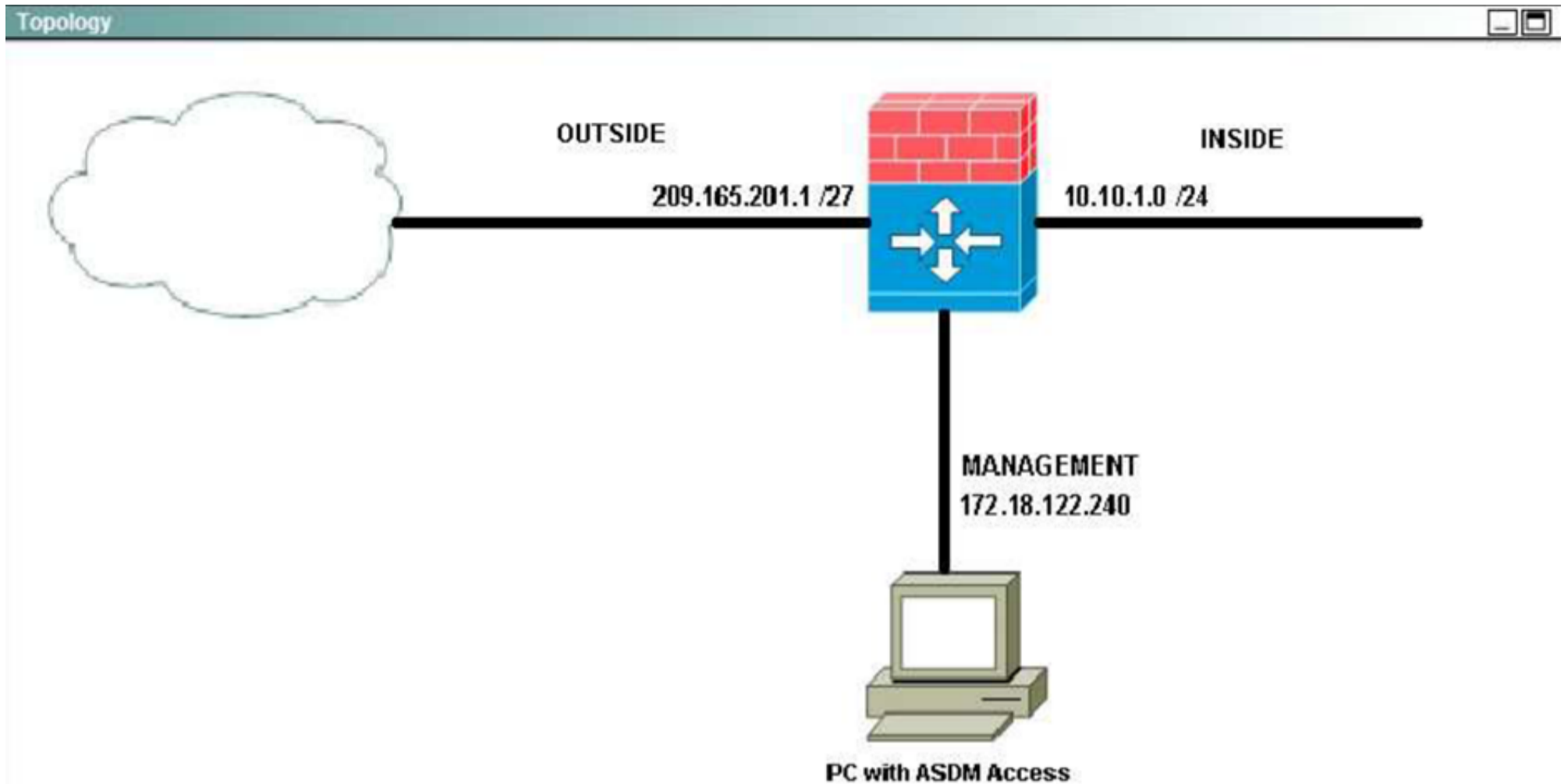
Instructions

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.

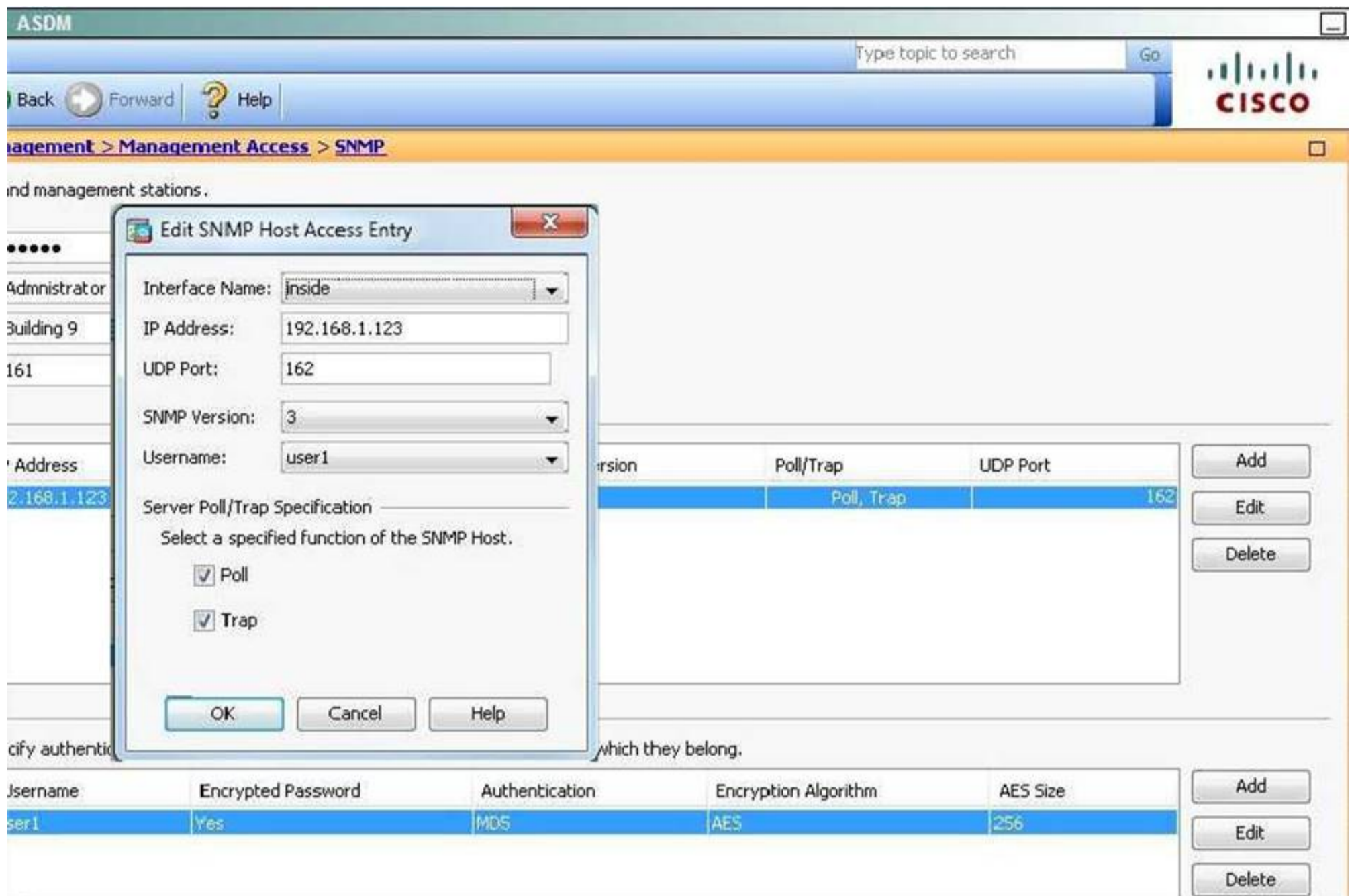


An SNMP host is an IP address to which SNMP notifications and traps are sent. To configure SNMFV3 hosts, which option must you configure in addition to the target IP address?

- 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 253

Which security operations management best practice should be followed to enable appropriate network access for administrators?

- A. Provide full network access from dedicated network administration systems
- B. Configure the same management account on every network device
- C. Dedicate a separate physical or logical plane for management traffic
- D. Configure switches as terminal servers for secure device access

Answer: C

NEW QUESTION 258

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 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 264

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 267

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

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 274

Which ASA feature is used to keep track of suspected attackers who create connections to too many hosts or ports?

- A. complex threat detection
- B. scanning threat detection
- C. basic threat detection
- D. advanced threat detection

Answer: B

NEW QUESTION 278

What is the default behavior of an access list on a Cisco ASA?

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

Answer: C

NEW QUESTION 279

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 282

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 286

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

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

Answer: B

NEW QUESTION 290

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 access.
- B. Also configure 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 group.
- 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 group.
- 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 ASA CLI.

Answer: B

NEW QUESTION 291

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 293

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 username username password password CLI command.
- D. enable_15 / (no password)
- E. cisco / cisco

Answer: D

NEW QUESTION 296

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 300

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 305

You are the administrator of a multicontext transparent-mode Cisco ASA that uses a shared interface that belongs to more than one context. Because the same interface will be used within all three contexts, which statement describes how you will ensure that return traffic will reach the correct context?

- A. Interfaces may not be shared between contexts in routed mode.
- B. Configure a unique MAC address per context with the no mac-address auto command.
- C. Configure a unique MAC address per context with the mac-address auto command.
- D. Use static routes on the Cisco ASA to ensure that traffic reaches the correct context.

Answer: C

NEW QUESTION 310

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 314

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 315

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 318

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 323

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 324

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 329

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 330

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 334

Which Cisco TrustSec role does a Cisco ASA firewall serve within an identity architecture?

- A. Access Requester
- B. Policy Decision Point
- C. Policy Information Point
- D. Policy Administration Point
- E. Policy Enforcement Point

Answer: E

NEW QUESTION 339

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 342

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 345

Which command enables the HTTP server daemon for Cisco ASDM access?

- A. http server enable
- B. http server enable 443
- C. crypto key generate rsa modulus 1024
- D. no http server enable

Answer: A

NEW QUESTION 350

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 355

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 358

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 362

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 363

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: 5 Type: NAT Subtype: Result: ALLOW Config: nat (INSIDE,DMZ) source dynamic 192.168.1.100 1.1.1.1 Additional Information:
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: 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: 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: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information:
Phase: 4 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 373

At which firewall severity level will debugs appear on a Cisco ASA?

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

Answer: A

NEW QUESTION 377

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

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

Answer: A

NEW QUESTION 379

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 380

Which Layer 2 security feature validates ARP packets?

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

Answer: A

NEW QUESTION 383

Which VTP mode supports private VLANs on a switch?

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

Answer: A

NEW QUESTION 388

Which technology can be deployed with a Cisco ASA 1000V to segregate Layer 2 access within a virtual cloud environment?

- A. Cisco Nexus 1000V
- B. Cisco VSG
- C. WSVA
- D. ESVA

Answer: A

NEW QUESTION 392

Refer to the exhibit.

```
access-list ACL extended permit ip 2001:DB8:1::/64 10.2.2.0 255.255.255.0
access-list ACL extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
access-list ACL extended permit ip host 192.168.1.50 host 192.168.2.50
```

Which type of ACL is shown in this configuration?

- A. IPv4
- B. IPv6
- C. unified
- D. IDFW

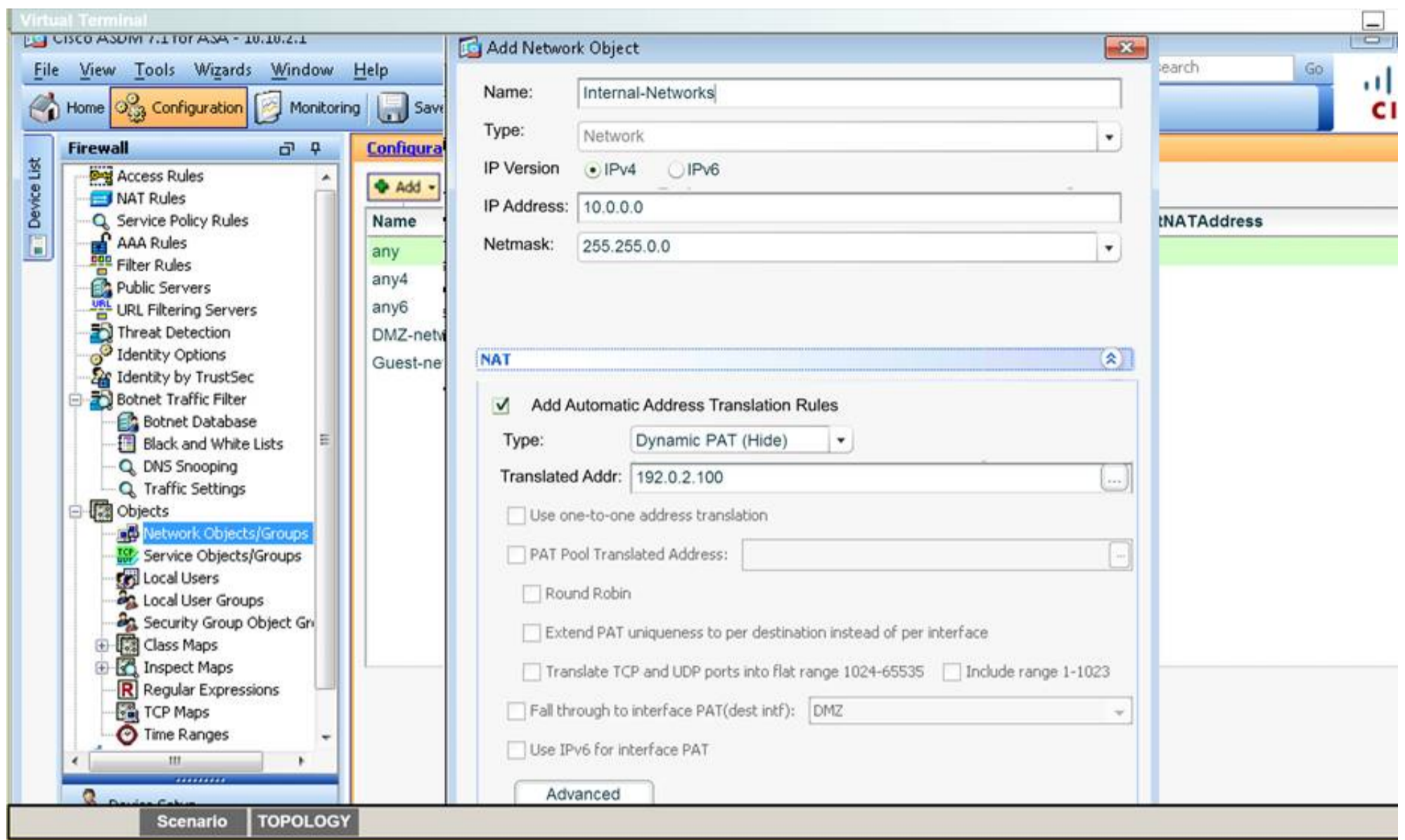
Answer: C

NEW QUESTION 393

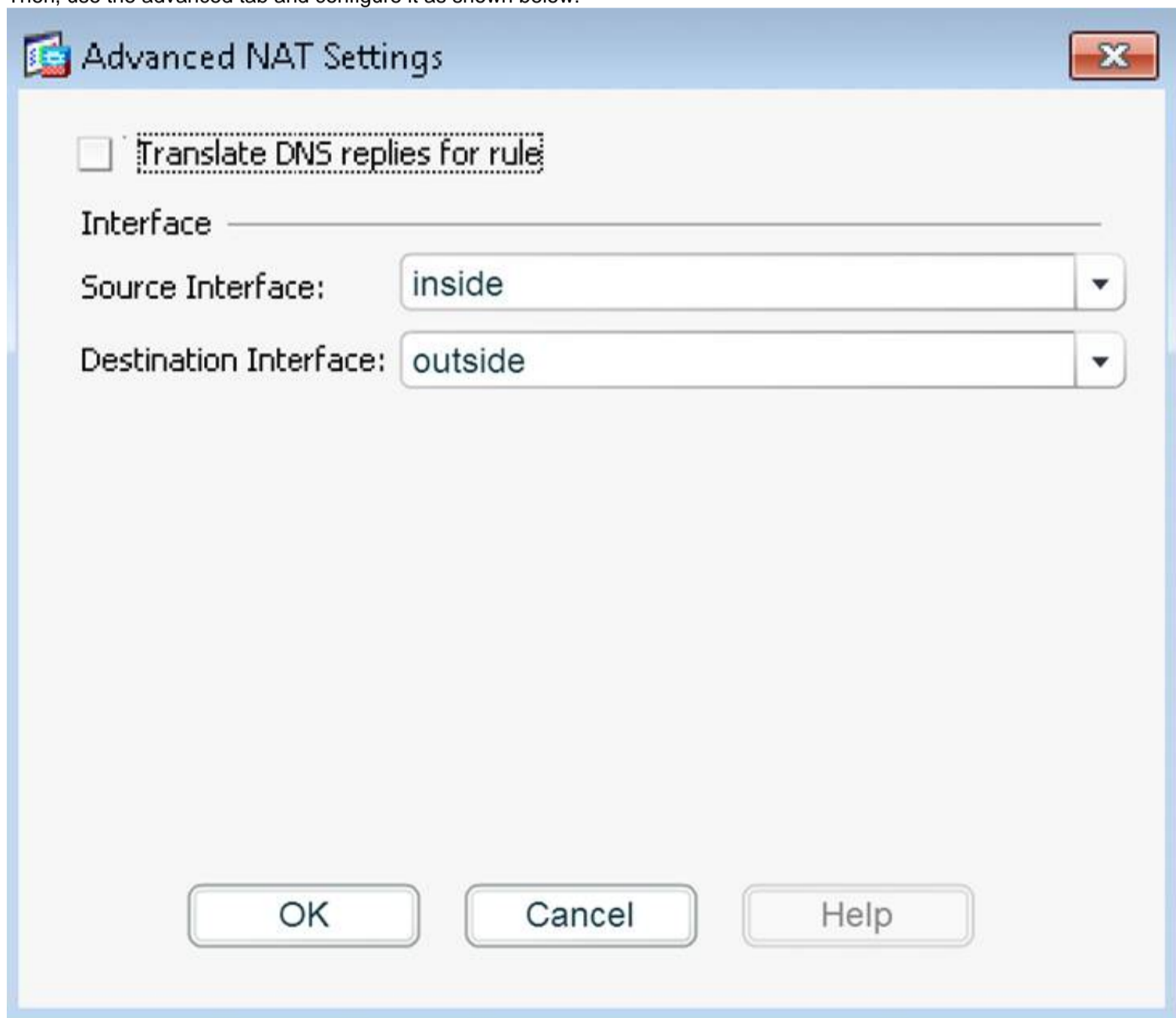
You are a network security engineer for the Secure-X network. You have been tasked with implementing dynamic network object NAT with PAT on a Cisco AS

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 396

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.

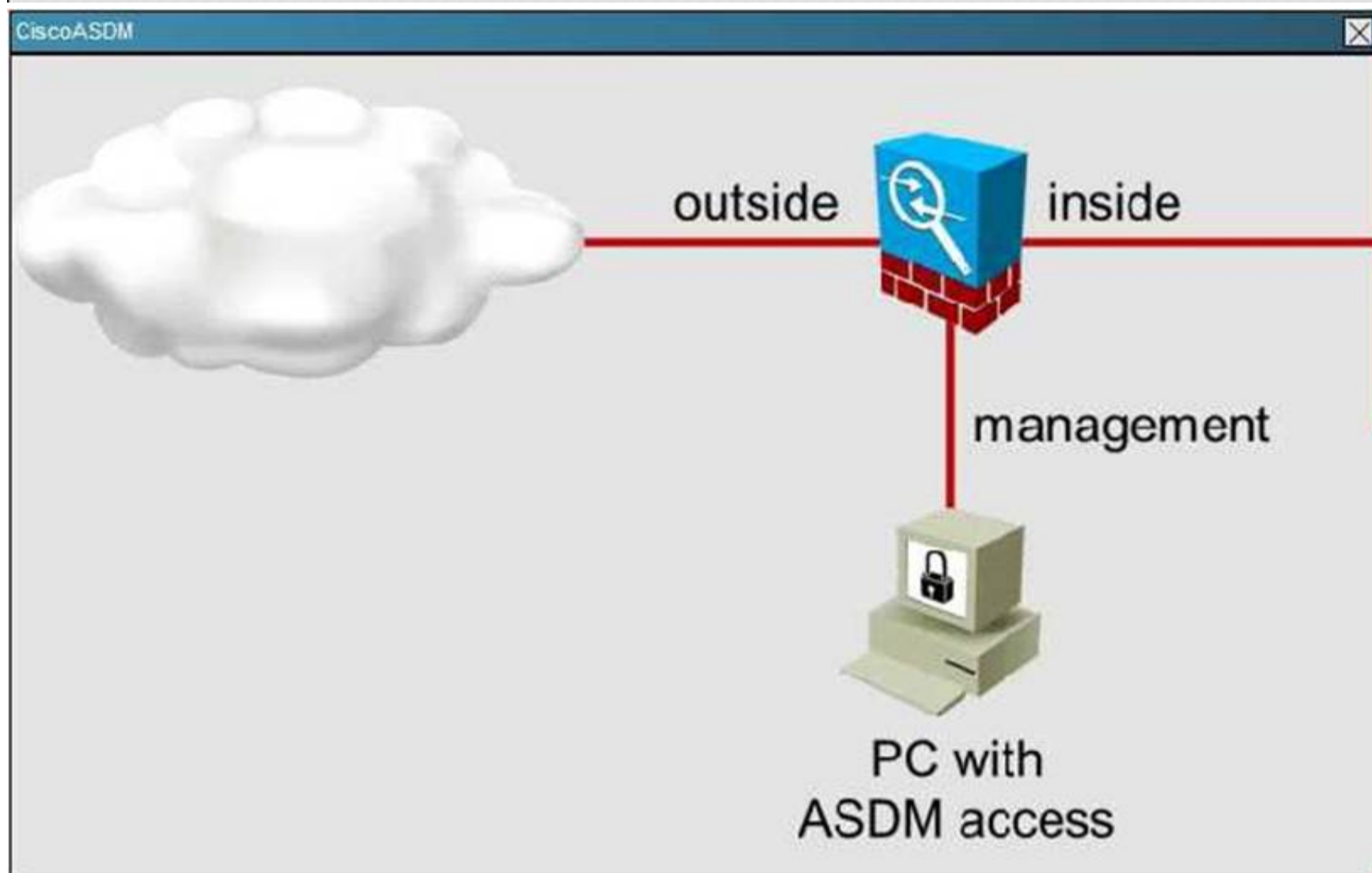


Exhibit11

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard Intrusion Prevention

Device Information

General License

Host Name: **HQ-ASA.secure-x.local**

ASA Version: **9.1(1)4** Device Uptime: **4d 4h 2m 9s**

ASDM Version: **7.1(2)** Device Type: **ASA 5515, IPS**

Firewall Mode: **Routed** Context Mode: **Single**

Environment Status: **OK** 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

Memory Usage (MB)

4000
3500
3000
2500
2000

729MB

Traffic Status

Connections Per Second Usage

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	Destination	Description
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	55282	Tear down 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	Tear down 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	Tear down 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	Tear down UDP connection 284830 for DMZ:172.16.1.55/62372 to inside:10.10.3.20/53 dur

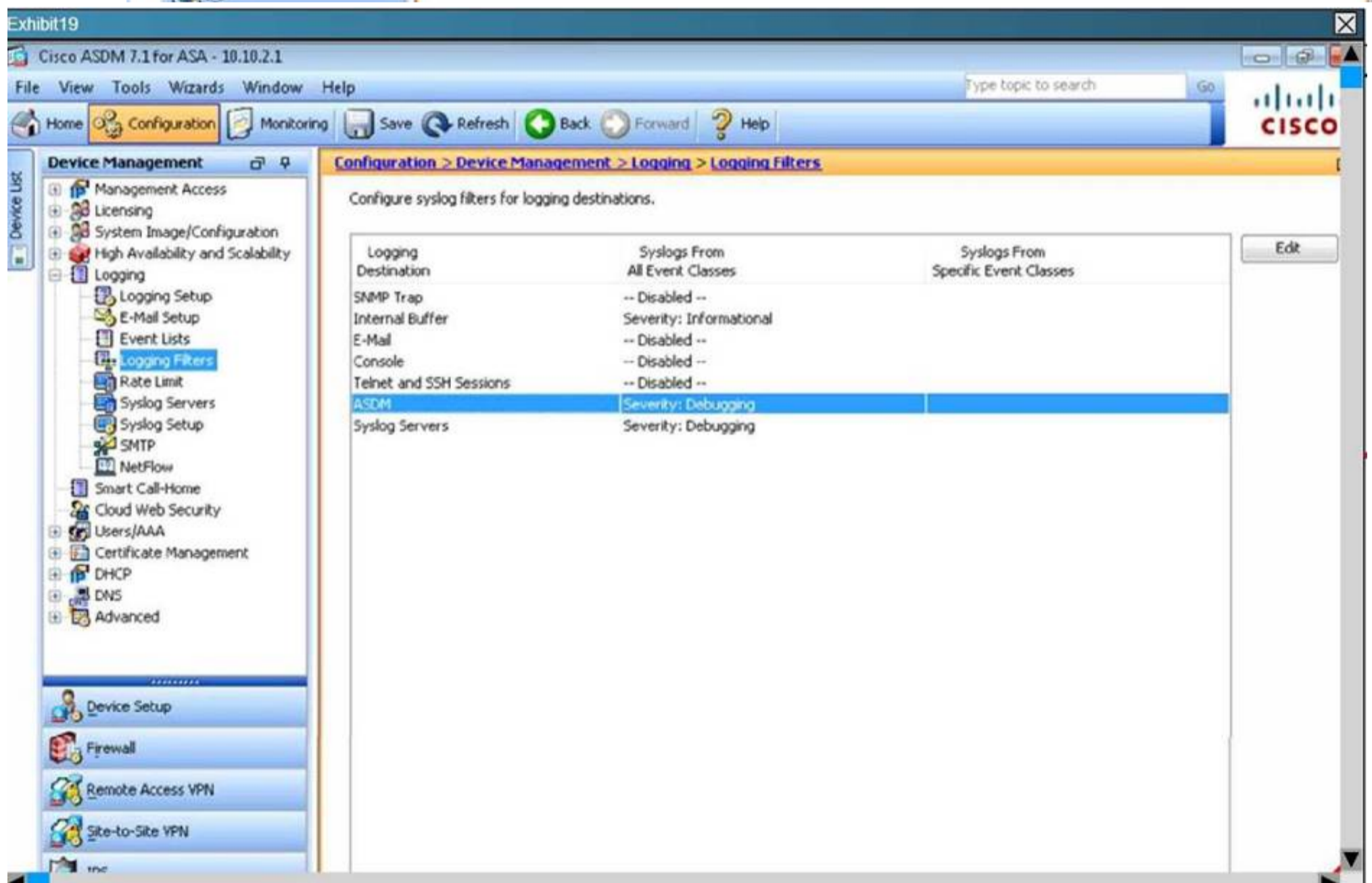
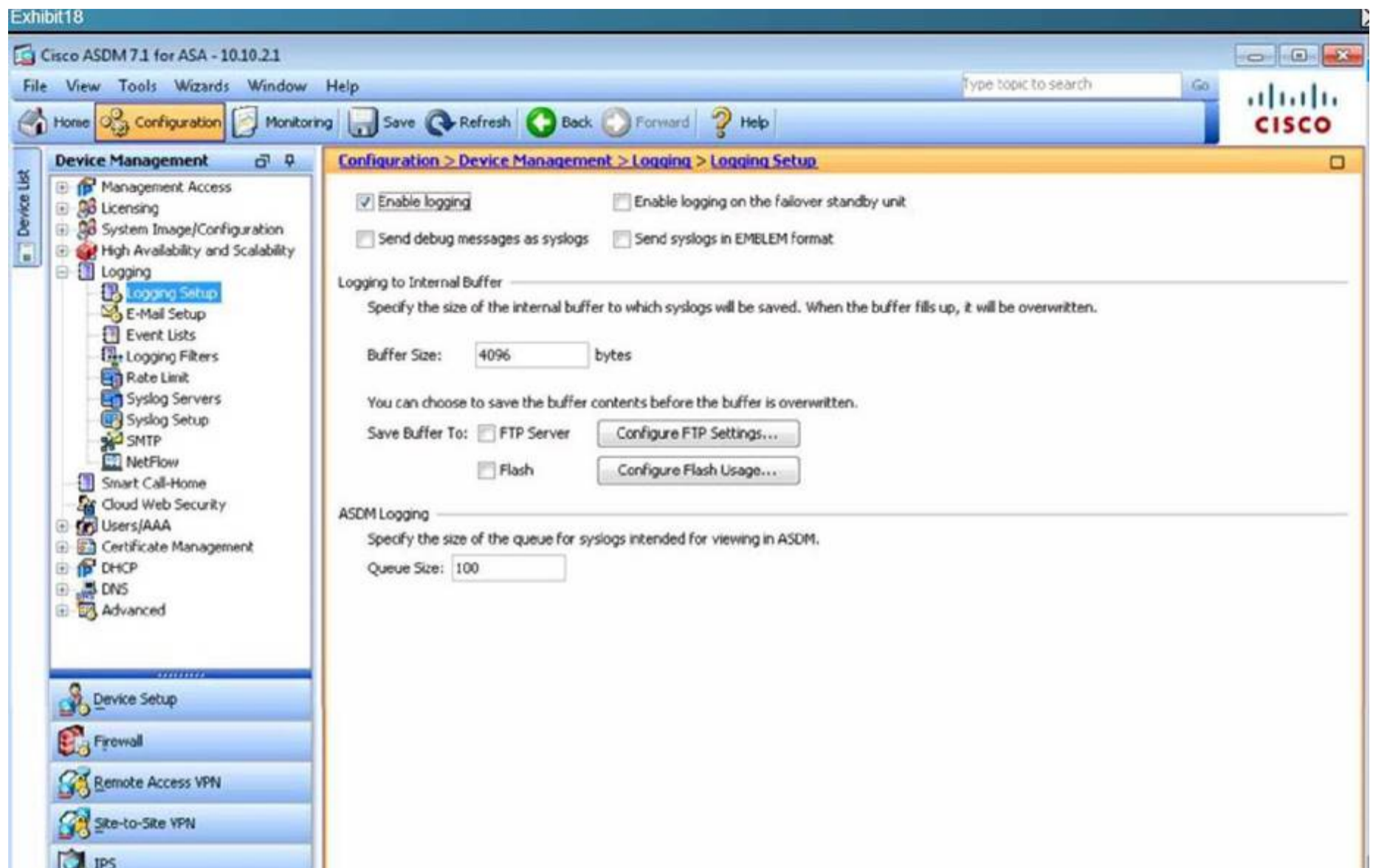
admin 2 5/21/14 4:27:15 PM PDT

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:



NEW QUESTION 399

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.html

NEW QUESTION 404

Which URL downloads a copy of packet-capture named "security" residing on a Cisco ASA adaptive security appliance with IP 10.10.100.11?

- A. <https://10.10.10.11/security.pcap/download>
- B. <https://10.10.10.11/asa/security/pcap>
- C. <https://10.10.10.11/capture/security.pcap>
- D. <https://10.10.10.11/capture/security/pcap>

Answer: D

NEW QUESTION 408

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 413

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 compatibility

Answer: C

Explanation:

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

NEW QUESTION 415

Which options lists cloud deployment modes?

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

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_Know?lang=en

NEW QUESTION 419

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 422

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 424

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 428

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 432

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 435

Which action is needed to set up SSH on the Cisco ASA firewall?

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

Answer: C

NEW QUESTION 440

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 442

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 is unicast or broadcast.
- D. Traffic storm control monitors incoming traffic levels over a 10 second traffic storm control interval

Answer: B

NEW QUESTION 443

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

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

Answer: B

NEW QUESTION 448

Refer to the exhibit.

```
capture udp match tcp host 10.10.0.12 any eq 80
```

What traffic is being captured by the Cisco ASA adaptive security appliance?

- A. UDP traffic sourced from host 10.10.0.12 on port 80
- B. TCP traffic destined to host 10.10.0.12 on port 80
- C. TCP traffic sourced from host 10.10.0.12 on port 80
- D. UDP traffic destined to host 10.10.0.12 on port 80

Answer: C

NEW QUESTION 450

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 452

Which Layer 2 security feature prevents traffic on a LAN from being disrupted by a broadcast, multicast, 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 455

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 458

Which Cisco prime Infrastructure feature 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 463

Which information does the ASA fail to replicate to the secondary Cisco ASA adaptive security appliance in an active/standby configuration with stateful and failover links?

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

Answer: C

NEW QUESTION 466

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 469

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, must 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 474

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 479

Which two option are main challenges for public cloud data center?

- A. deployment cost
- B. tenant isolation
- C. disaster recovery
- D. system scalability

E. network visibility

Answer: BE

NEW QUESTION 483

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 488

Which statement describes what the arp outside 1.1.1.1 0192.7gid.0020 command accomplishes?

- A. enable ARP inspection for host 1.1.1.1
- B. configures proxy ARP for host 1.1.1.1
- C. assigns virtual MAC address for host 1.1.1.1
- D. creates static ARP entry for host 1.1.1.1 .

Answer: D

Explanation: That command adds a static ARP entry to allow ARP responses from the host at 1.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface <http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/fwmode.html#wp1224694>

NEW QUESTION 490

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 492

Which device can be managed by the Cisco Prime Security Manager?

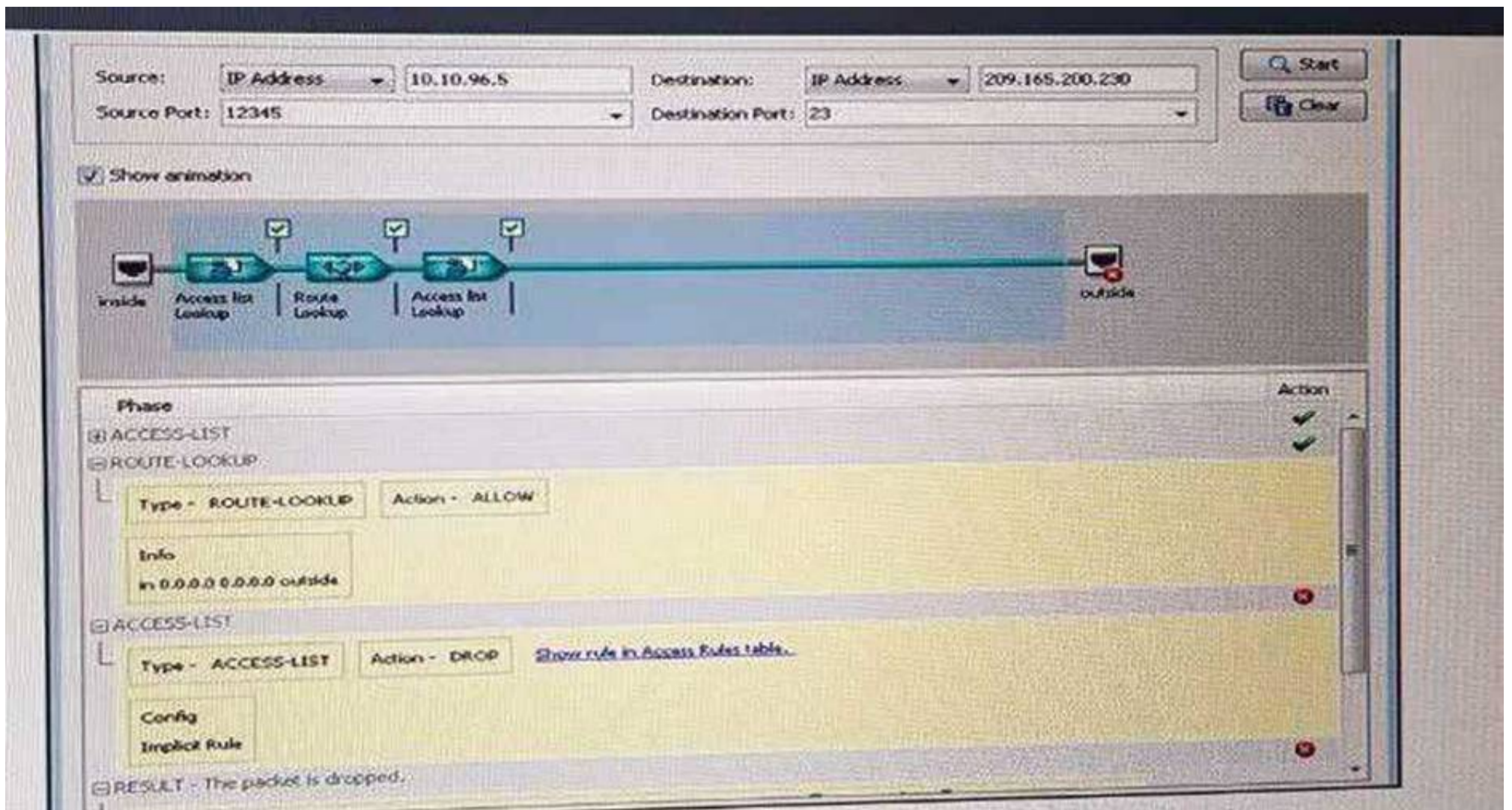
- A. ASA CX
- B. ISR G2
- C. Nexus
- D. UCM

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 495

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 497

DRAG DROP

Match the following to its exact description

Authorization	defined guideline instruction for operators to follow
Change Management	configuration priviledge levels on device etc
Access-control	network group roles, which action to be performed by which group
Operation policy	controlled access to devices
Segregated of duty	track changes timeline action
Accounting	processes to manage changes in envrionment etc

Answer:

Explanation: Authorization – configuration priviledge levels on device etc
 Change Management – processes to manage changes in envrionment etc
 Access-control – controlled access to devices
 Operation policy – defined guideline instruction for operators to follow
 Segregated of duty – network group roles, which action to be performed by which group etc
 Accounting – track changes timeline action

NEW QUESTION 502

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 505

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 508

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 509

Best practices for hardening of management plane have been implemented on an ASA (or IOS router). Which protocols will be affected?

- A. BGP
- B. ICMP
- C. ARP
- D. HTTP

Answer: B

NEW QUESTION 514

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 517

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 521

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 522

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 523

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 528

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 533

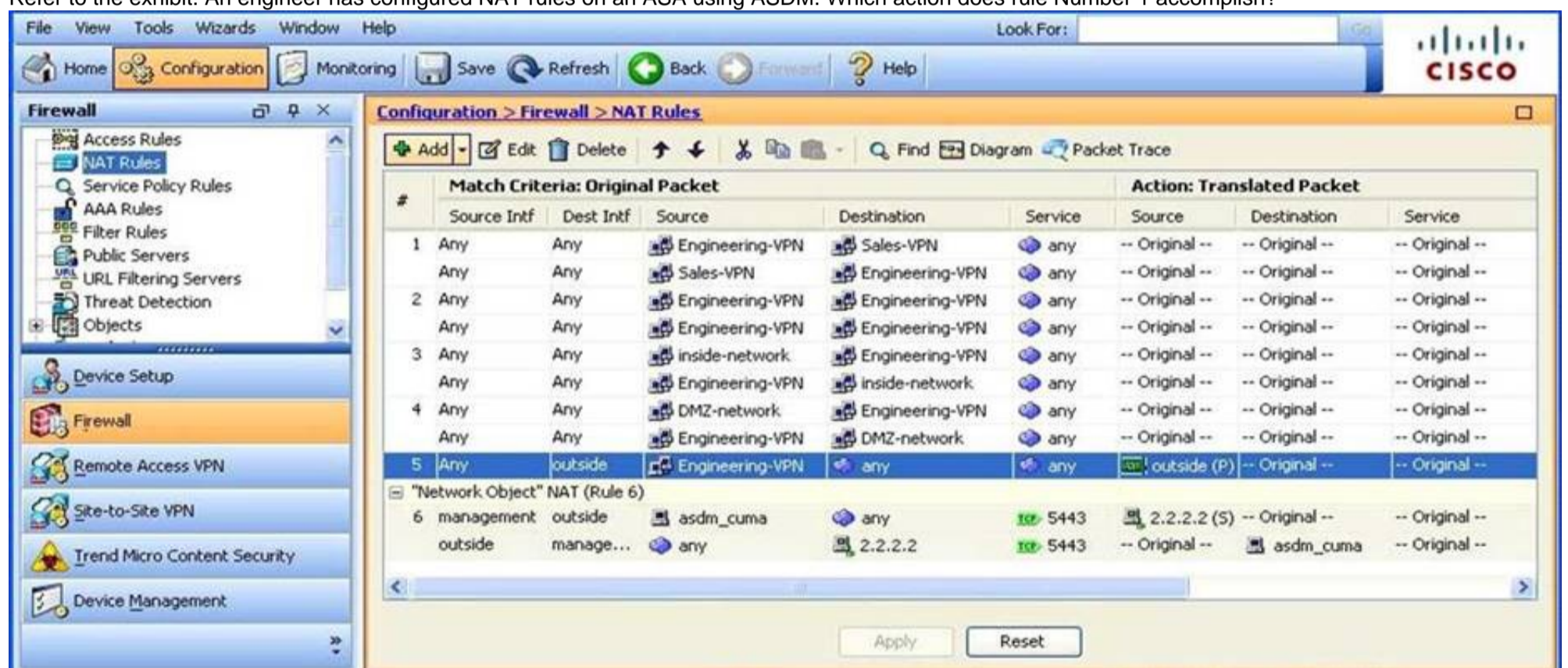
You must restrict the interface on which management traffic can be received by the routers on your network. Which feature do you enable?

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

Answer: A

NEW QUESTION 538

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



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

Answer: C

NEW QUESTION 543

Which two types of addresses can be blocked by configuring botnet traffic filtering on an ASA? (Choose two.)

- A. spyware
- B. instant messaging
- C. P2P
- D. games
- E. ads

Answer: AE

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/special/botnet/guide/asa-botnet.html>

NEW QUESTION 547

.....

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>