

**Cisco 300-206**



## **Implementing Cisco Edge Network Security Solutions**

**Version: 4.0**

**QUESTION NO: 1**

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**

**Explanation:**

**QUESTION NO: 2**

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**

**Explanation:**

**QUESTION NO: 3**

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**

**Explanation:**

**QUESTION NO: 4**

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

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

**Answer: A**

**Explanation:**

**QUESTION NO: 5**

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**

**Explanation:**

**QUESTION NO: 6**

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**

**Explanation:**

**QUESTION NO: 7**

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**

**Explanation:**

**QUESTION NO: 8**

What is the default behavior of NAT control on Cisco ASA Software Version 8.3?

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

**Answer: A**

**Explanation:**

**QUESTION NO: 9**

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: A,C,D**

**Explanation:**

**QUESTION NO: 10**

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: B,D,F**

**Explanation:**

**QUESTION NO: 11**

What are three features of the Cisco ASA 1000V? (Choose three.)

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

**Answer: A,C,E**

**Explanation:**

**QUESTION NO: 12**

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**

**Explanation:**

### **QUESTION NO: 13**

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**

**Explanation:**

### **QUESTION NO: 14**

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

- A.** sslconfig
- B.** sslciphers
- C.** tlsconfig
- D.** certconfig

**Answer: A**

**Explanation:**

**QUESTION NO: 15**

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

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

**Answer: A**

**Explanation:**

**QUESTION NO: 16**

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: A,B,D**

**Explanation:**

**QUESTION NO: 17**

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**

**Explanation:**

**QUESTION NO: 18**

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**

**Explanation:**

**QUESTION NO: 19**

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: A,B,C**

**Explanation:**

**QUESTION NO: 20**

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: A,B,C**

**Explanation:**

#### **QUESTION NO: 21**

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: A,C**

**Explanation:**

#### **QUESTION NO: 22**

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**

**Explanation:**

**QUESTION NO: 23**

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**

**Explanation:**

**QUESTION NO: 24**

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**

**Explanation:**

**QUESTION NO: 25**

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**

**Explanation:**

**QUESTION NO: 26**

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**

**Explanation:**

**QUESTION NO: 27**

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: A,B,C**

**Explanation:**

**QUESTION NO: 28**

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**

**Explanation:**

#### **QUESTION NO: 29**

What is the default log level on the Cisco Web Security Appliance?

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

**Answer: C**

**Explanation:**

#### **QUESTION NO: 30**

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**

**Explanation:**

#### **QUESTION NO: 31**

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

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

**Answer: B,C**

**Explanation:**

#### **QUESTION NO: 32**

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: A,C,D**

**Explanation:**

#### **QUESTION NO: 33**

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: B,D,E**

**Explanation:**

#### **QUESTION NO: 34**

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: A,B**

**Explanation:**

#### **QUESTION NO: 35**

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**

**Explanation:**

#### **QUESTION NO: 36**

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**

**Explanation:**

#### **QUESTION NO: 37**

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: C,D**

**Explanation:**

#### **QUESTION NO: 38**

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

- A. enable logging  
show logging
- B. logging enable  
show logging
- C. enable logging int e0/1  
view logging
- D. logging enable  
logging view config

**Answer: B**

**Explanation:**

#### **QUESTION NO: 39**

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**

**Explanation:**

**QUESTION NO: 40**

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 2  
console logging critical\_messages
- B. logging list critical\_messages level 2  
logging console critical\_messages
- C. logging list critical\_messages level 2  
logging console enable critical\_messages
- D. logging list enable critical\_messages level 2  
console logging critical\_messages

**Answer: B**

**Explanation:**

**QUESTION NO: 41**

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 mac-address 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. The configuration will not automatically be saved to NVRAM.
- C. Only MAC addresses with the 5th most significant bit of the address (the 'sticky' bit) set to 1 will be learned.
- D. If configured on a trunk port without the 'vlan' keyword, it will apply to all vlans.
- E. If configured on a trunk port without the 'vlan' keyword, it will apply only to the native vlan.

**Answer: B,E**

**Explanation:**

**QUESTION NO: 42**

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**

**Explanation:**

#### **QUESTION NO: 43**

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: A,B**

**Explanation:**

#### **QUESTION NO: 44**

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**

**Explanation:**

#### **QUESTION NO: 45**

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

- A. identifying Layer 2 ARP attacks

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

**Answer: A,D**

**Explanation:**

#### **QUESTION NO: 46**

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

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

**Answer: B**

**Explanation:**

#### **QUESTION NO: 47**

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: B,C**

**Explanation:**

#### **QUESTION NO: 48**

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**

**Explanation:**

#### **QUESTION NO: 49**

Which two statements about Cisco IDS are true? (Choose two.)

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

**Answer: B,C**

**Explanation:**

#### **QUESTION NO: 50**

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: C,D**

**Explanation:**

**QUESTION NO: 51**

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: A,C,D,G**

**Explanation:**

**QUESTION NO: 52**

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**

**Explanation:**

**QUESTION NO: 53**

Which two device types can Cisco Prime Security Manager manage in Multiple Device mode? (Choose two.)

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

**Answer: B,D**

**Explanation:**

**QUESTION NO: 54**

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

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

**Answer: C**

**Explanation:**

**QUESTION NO: 55**

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**

**Explanation:**

**QUESTION NO: 56**

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**

**Explanation:**

**QUESTION NO: 57**

Which two voice protocols can the Cisco ASA inspect? (Choose two.)

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

**Answer: A,D**

**Explanation:**

**QUESTION NO: 58**

You have explicitly added the line deny ipv6 any log to the end of an IPv6 ACL on a router interface. Which two ICMPv6 packet types must you explicitly allow to enable traffic to traverse the interface? (Choose two.)

- A. router solicitation
- B. router advertisement
- C. neighbor solicitation
- D. neighbor advertisement
- E. redirect

**Answer: C,D**

**Explanation:**

**QUESTION NO: 59**

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**

**Explanation:**

**QUESTION NO: 60**

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

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

**Answer: C**

**Explanation:**

**QUESTION NO: 61**

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**

**Explanation:**

**QUESTION NO: 62**

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**

**Explanation:**

**QUESTION NO: 63**

Which two statements about Cisco IOS Firewall are true? (Choose two.)

- A. It provides stateful packet inspection.
- B. It provides faster processing of packets than Cisco ASA devices provide.
- C. It provides protocol-conformance checks against traffic.
- D. It eliminates the need to secure routers and switches throughout the network.
- E. It eliminates the need to secure host machines throughout the network.

**Answer: A,C**

**Explanation:**

**QUESTION NO: 64**

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: A,B**

**Explanation:**

**QUESTION NO: 65**

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

- A. domain
- B. password
- C. ACE tag
- D. user roles
- E. VDC group tag

F. expiry date

**Answer: B,D,F**

**Explanation:**

#### **QUESTION NO: 66**

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**

**Explanation:**

#### **QUESTION NO: 67**

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**

**Explanation:**

#### **QUESTION NO: 68**

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**

**Explanation:**

## QUESTION NO: 69 CORRECT TEXT

**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.

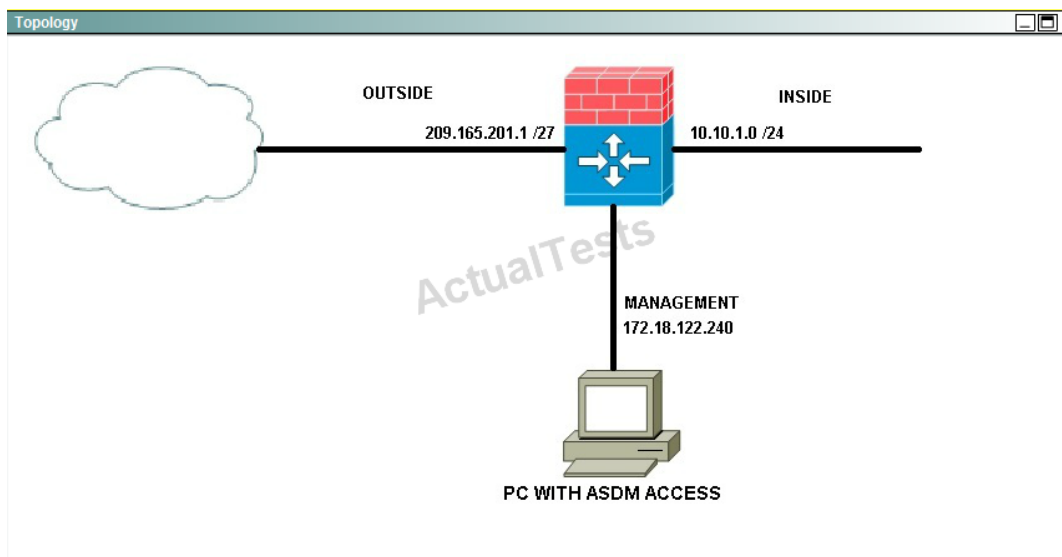
**Scenario**

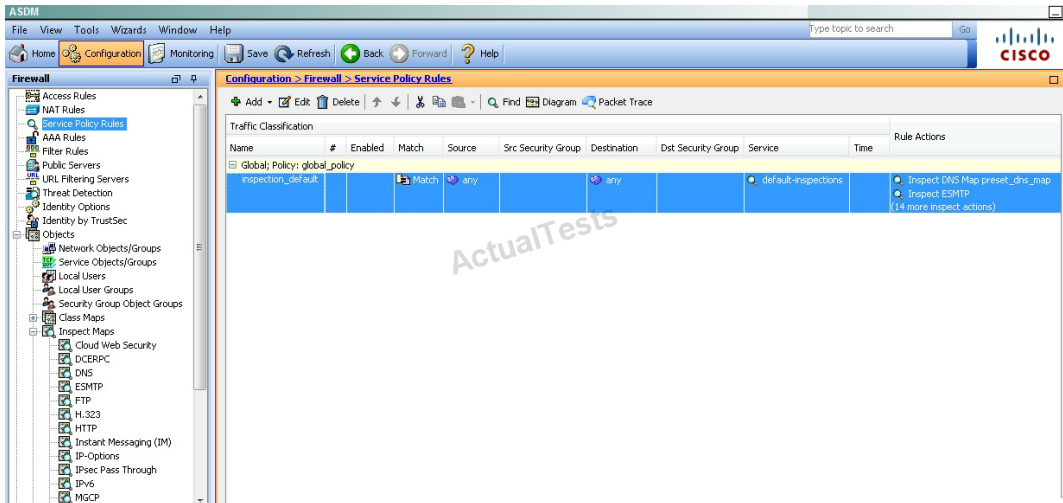
You have been given access to a Cisco ASA 5512 Adaptive Security Appliance via Cisco ASDM. Use Cisco ASDM to edit the Cisco ASA 5505 Adaptive Security Appliance configurations to enable Advanced HTTP application inspection by completing the following tasks:

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.

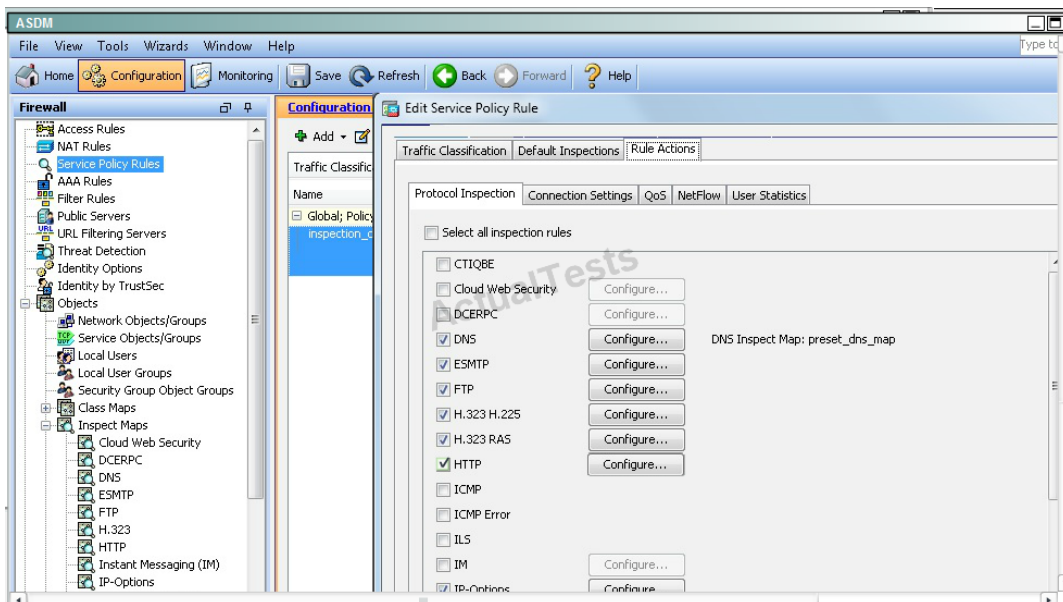




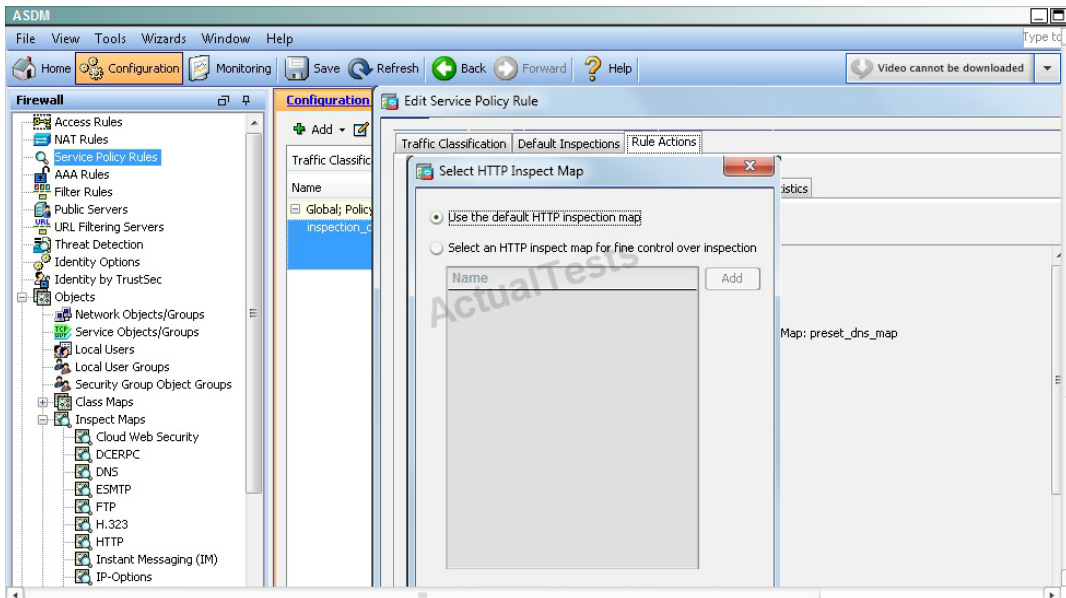
Answer: Please check the steps in explanation part below:

### Explanation:

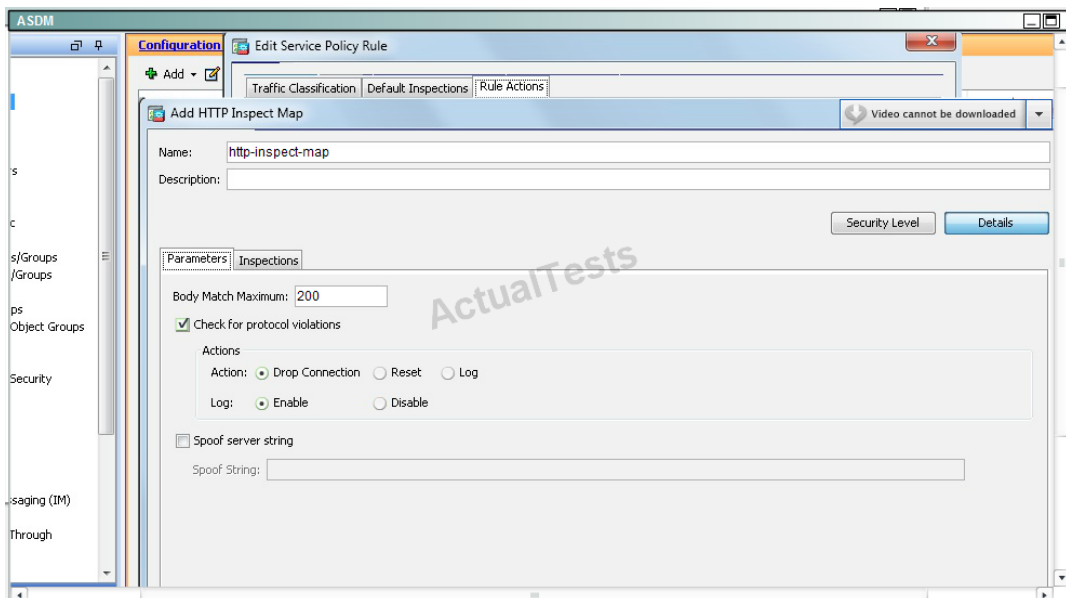
- 1) Click on Service Policy Rules, then Edit the default inspection rule.
- 2) Click on Rule Actions, then enable HTTP as shown here:



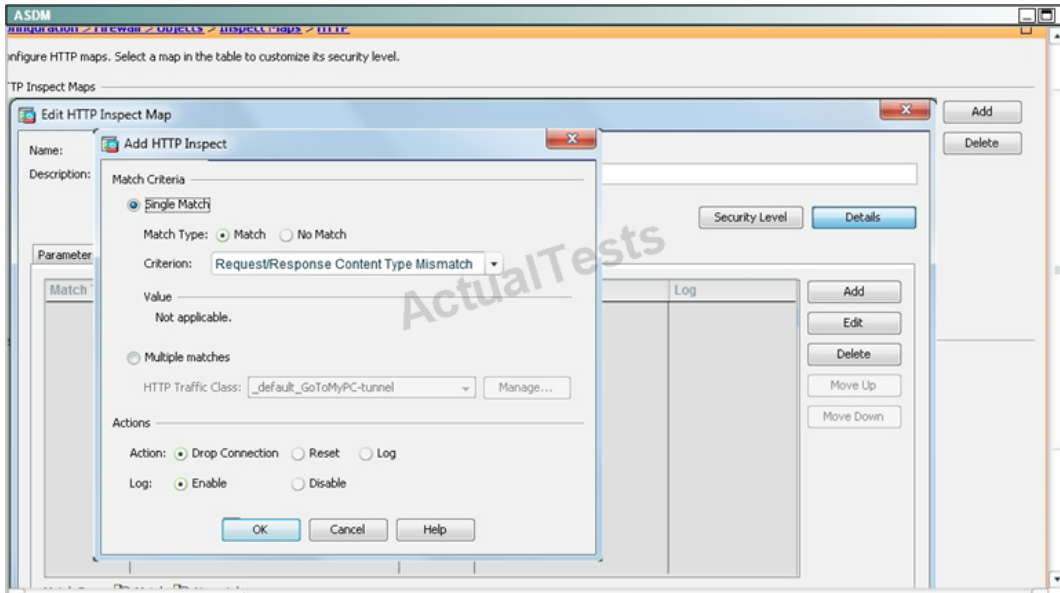
- 3) Click on Configure, then add as shown here:



4) Create the new map in ASDM like shown:



5) Edit the policy as shown:



6) Hit OK

## QUESTION NO: 70

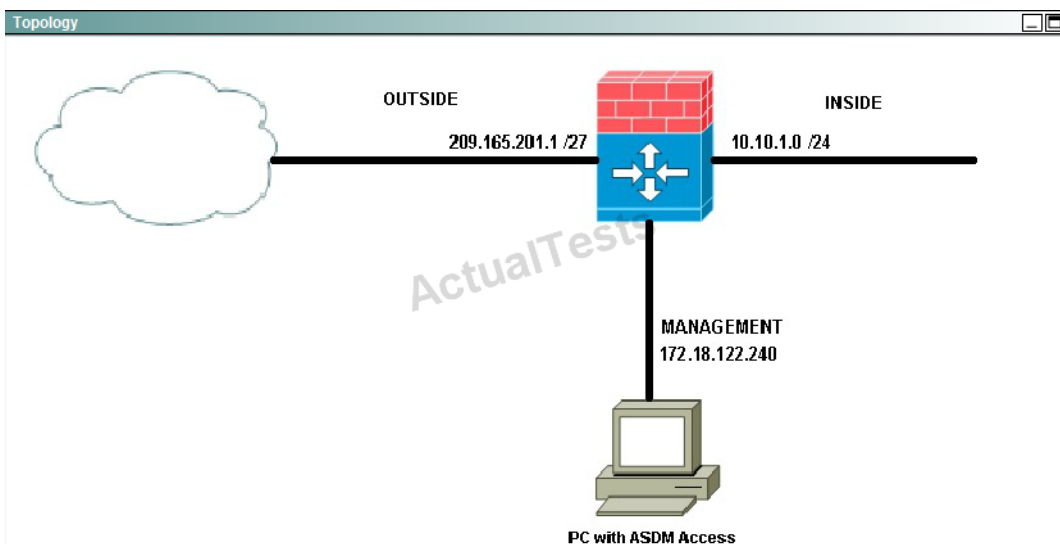
**Instructions**

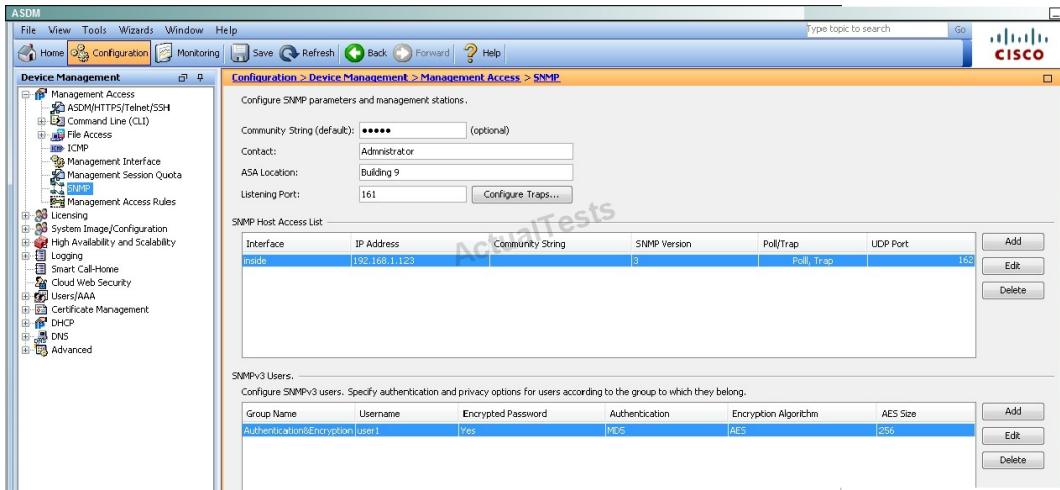
Click the grey buttons at the bottom of this frame to view the different windows.

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.





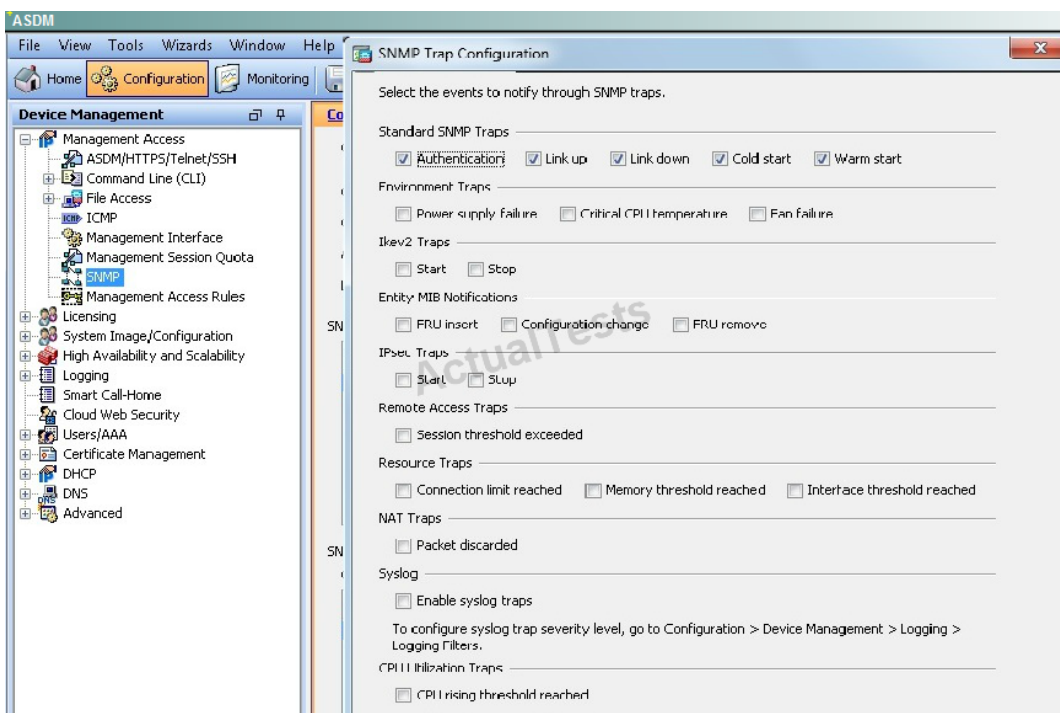
Which statement about how the Cisco ASA supports SNMP is true?

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

**Answer: C**

**Explanation:**

This can be verified by this ASDM screen shot:



## QUESTION NO: 71

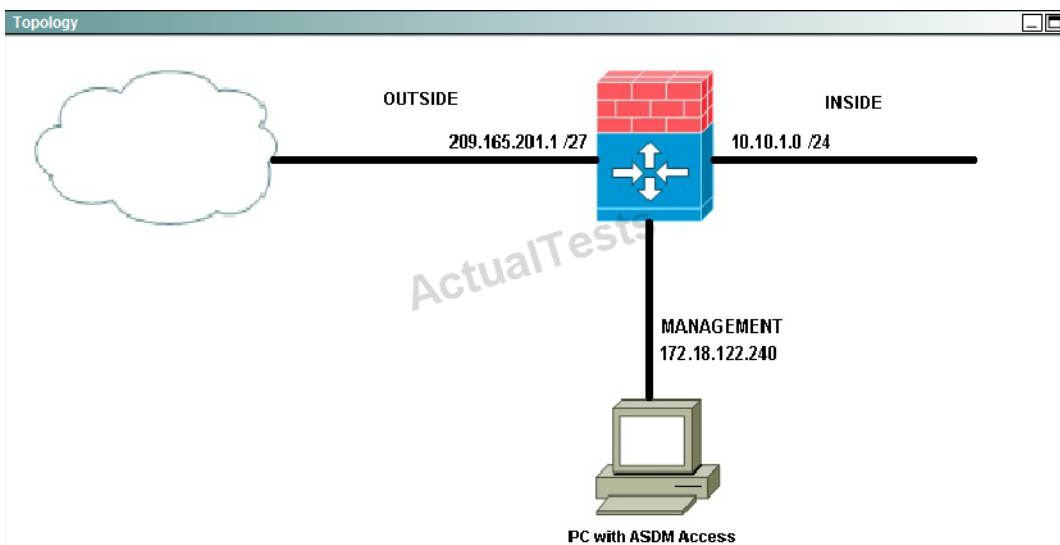
**Instructions**

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.



**ASDM**

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Type topic to search Go

**Device Management**

- Management Access
  - ASDM/HTTPS/Telnet/SSH
  - Command Line (CLI)
  - File Access
  - ICMP
  - Management Interface
  - Management Session Quota
  - SNMP
  - Management Access Rules
- Licensing
- System Image/Configuration
- High Availability and Scalability
- Logging
- Smart Call-Home
- Cloud Web Security
- Users/AAA
- Certificate Management
- DHCP
- DNS
- Advanced

**Configuration > Device Management > Management Access > SNMP**

Configure SNMP parameters and management stations.

Community String (default):  (optional)

Contact:

ASA Location:

Listening Port:

**SNMP Host Access List**

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

**SNMPv3 Users**

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

| Group Name                | Username | Encrypted Password | Authentication | Encryption Algorithm | AES Size |
|---------------------------|----------|--------------------|----------------|----------------------|----------|
| Authentication/Encryption | user1    | Yes                | MD5            | AES                  | 256      |

SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SHA. The encryption algorithm options are DES, 3DES, and AES (which is available in 128, 192, and 256 versions). When you create a user, with which option must you associate it?

- A. an SNMP group
- B. at least one interface
- C. the SNMP inspection in the global\_policy
- D. at least two interfaces

**Answer: A**

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

The screenshot shows the ASDM interface with two main configuration sections:

**SNMP Host Access List**

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

**SNMPv3 Users**

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

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

## QUESTION NO: 72

The screenshot shows two windows from the ASDM interface:

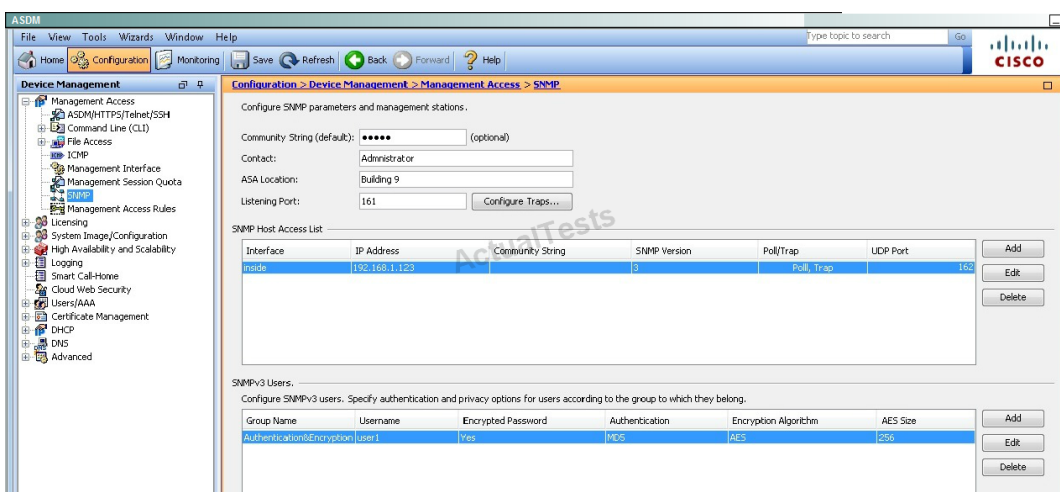
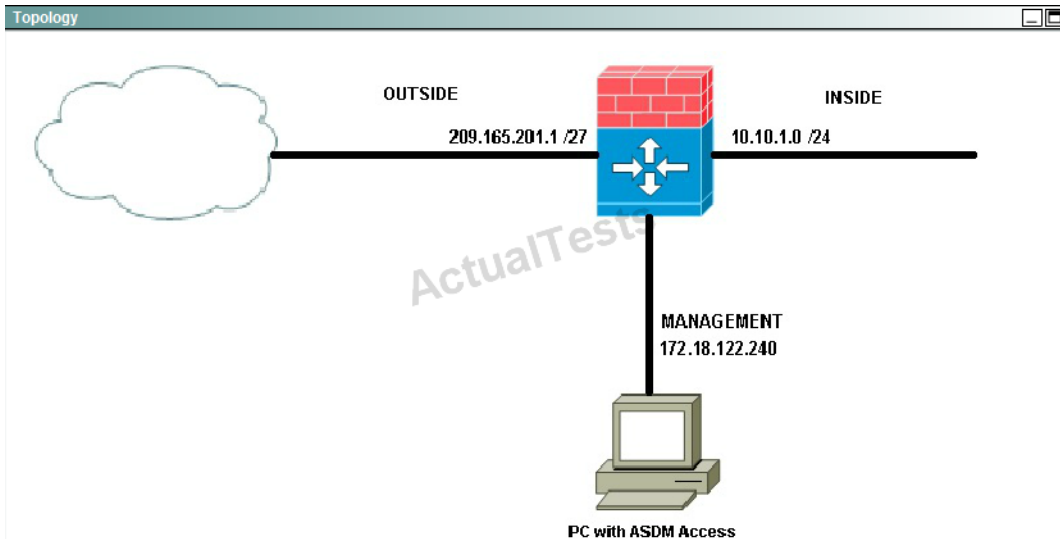
**Instructions**

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 SNMFFV3 hosts, which option must you configure in addition to the target IP address?

- A. the Cisco ASA as a DHCP server, so the SNMFFV3 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:

ASDM

Type topic to search Go

Back Forward ? Help

Management > Management Access > SNMP

and management stations.

Administrator

Building 9

161

Address

2.168.1.123

2.168.1.123

Server Poll/Trap Specification

Select a specified function of the SNMP Host.

☒ Poll

☒ Trap

OK Cancel Help

which they belong.

| Username | Encrypted Password | Authentication | Encryption Algorithm | AES Size |
|----------|--------------------|----------------|----------------------|----------|
| per1     | Yes                | MD5            | AES                  | 256      |

Add Edit Delete

Interface Name: inside

IP Address: 192.168.1.123

UDP Port: 162

SNMP Version: 3

Username: user1

| Version | Poll/Trap  | UDP Port |
|---------|------------|----------|
|         | Poll, Trap | 162      |

Add Edit Delete