300-206

Number: 300-206
Passing Score: 800
Time Limit: 200 min
File Version: 1.0

Cisco 300-206

Implementing Cisco Edge Network Security Solutions

Экзамен A

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 2
Cisco 300-206 Exam

Explanation:

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
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

Correct Answer: ACE

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
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.
"Pass Any Exam. Any Time." - www.actualtests.com 5
Cisco 300-206 Exam
D. It passes the first outside-to-inside packet and drops all remaining packets.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 6
Cisco 300-206 Exam

QUESTION 9
What is the CLI command to enable SNMPv3 on the Cisco Web Security Appliance?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
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
"Pass Any Exam. Any Time." - www.actualtests.com 7
Cisco 300-206 Exam
B. Security administrator
C. System administrator
D. Root Administrator
E. Exec administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
Cisco Security Manager can manage which three products? (Choose three.)

"Pass Any Exam. Any Time." - www.actualtests.com 8
Cisco 300-206 Exam

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
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)

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 9
Cisco 300-206 Exam

QUESTION 17
Which statement about the Cisco Security Manager 4.4 NAT Rediscovery feature is true?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 10
Cisco 300-206 Exam

QUESTION 20
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which two SNMPv3 features ensure that SNMP packets have been sent securely?" Choose two.

"Pass Any Exam. Any Time." - www.actualtests.com 12
Cisco 300-206 Exam

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
Which two parameters must be configured before you enable SCP on a router? (Choose two.)

"Pass Any Exam. Any Time." - www.actualtests.com 13
Cisco 300-206 Exam

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Which two options are two purposes of the packet-tracer command? (Choose two.)

"Pass Any Exam. Any Time." - www.actualtests.com 14
Cisco 300-206 Exam

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
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>

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
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.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
What are two primary purposes of Layer 2 detection in Cisco IPS networks? (Choose two.)

A. identifying Layer 2 ARP attacks
"Pass Any Exam. Any Time." - www.actualtests.com 17
Cisco 300-206 Exam
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
What is the maximum jumbo frame size for IPS standalone appliances with 1G and 10G fixed or

"Pass Any Exam. Any Time." - www.actualtests.com 18
Cisco 300-206 Exam
add-on interfaces?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 19
Cisco 300-206 Exam

QUESTION 42
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

Correct Answer: ACDG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 20
Cisco 300-206 Exam

QUESTION 45
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
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
"Pass Any Exam. Any Time." - www.actualtests.com 21
Cisco 300-206 Exam

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 48
Which two voice protocols can the Cisco ASA inspect? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
Enabling what security mechanism can prevent an attacker from gaining network topology information from CDP?

A. MACsec
B. Flex VPN
C. Control Plane Protection
"Pass Any Exam. Any Time." - www.actualtests.com 22
Cisco 300-206 Exam
D. Dynamic Arp Inspection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
Which log level provides the most detail on the Cisco Web Security Appliance?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
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
"Pass Any Exam. Any Time." - www.actualtests.com 23
Cisco 300-206 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 56
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
"Pass Any Exam. Any Time." - www.actualtests.com 24
Cisco 300-206 Exam
E. VDC group tag
F. expiry date

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
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)

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
Which command configures the SNMP server group1 to enable authentication for members of the access list east?

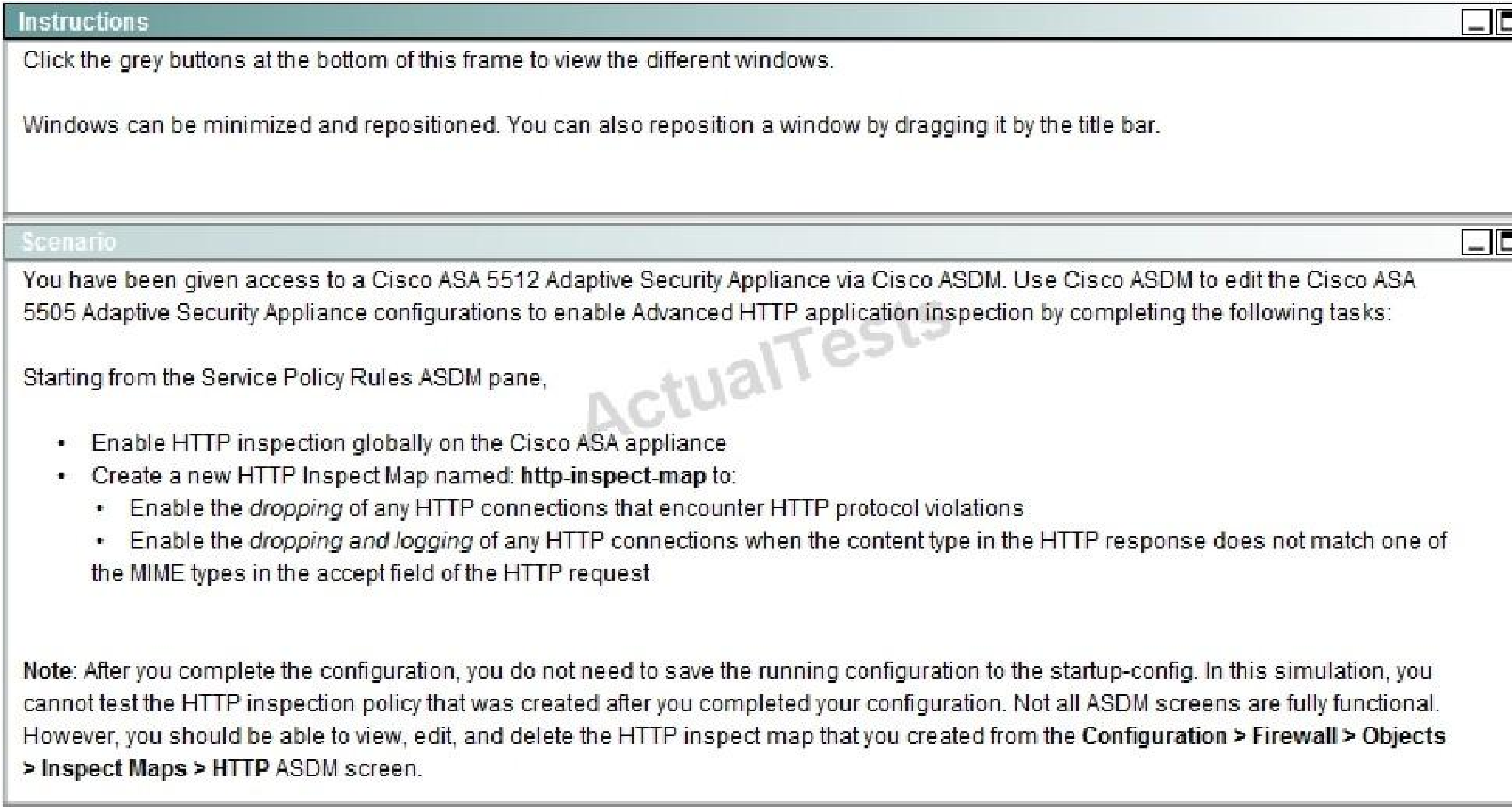
A. snmp-server group group1 v3 auth access east
B. snmp-server group1 v3 auth access east
C. snmp-server group group1 v3 east
D. snmp-server group1 v3 east access

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60

CORRECT TEXT



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

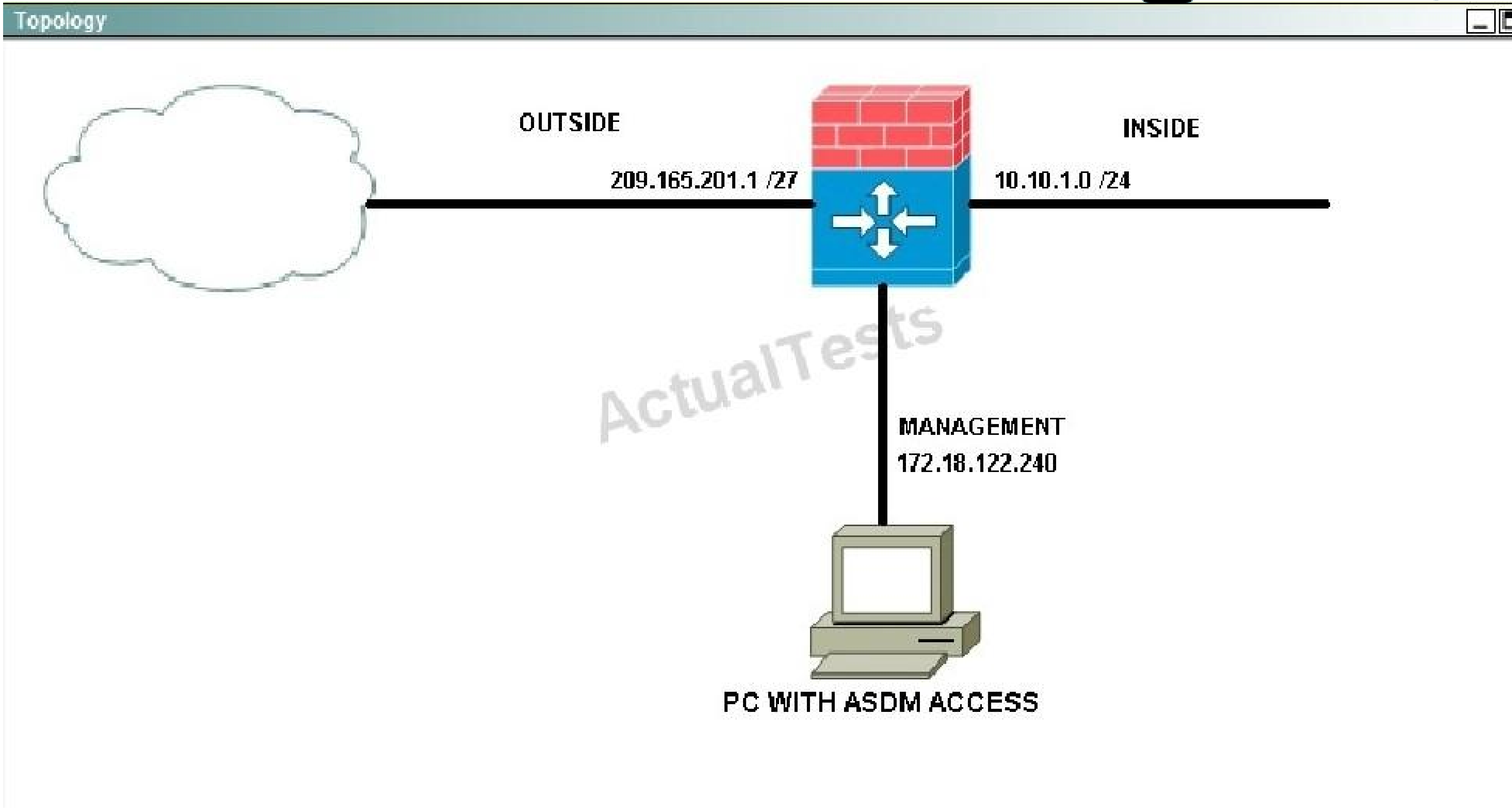
Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

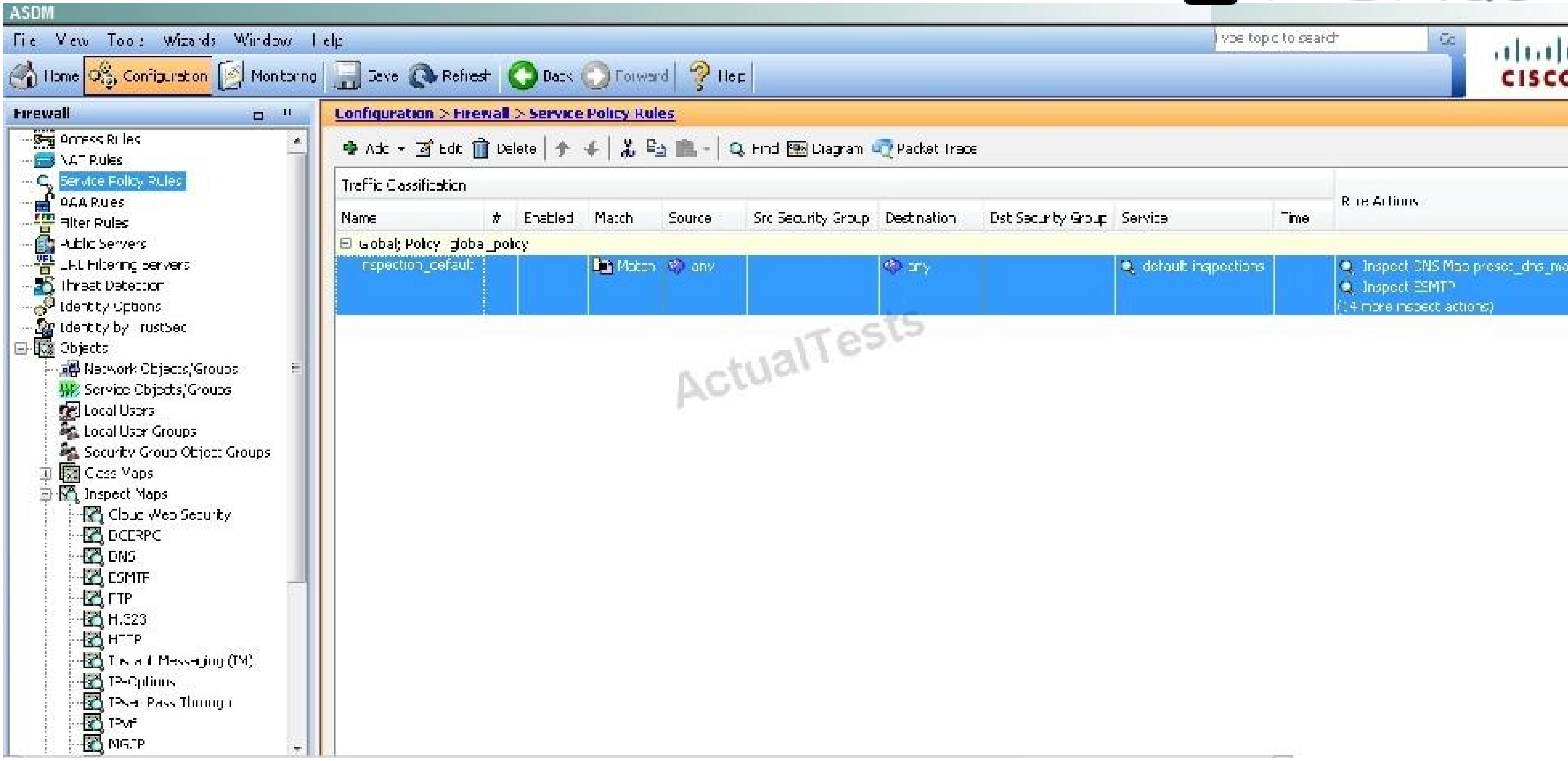
You have been given access to a Cisco ASA 5512 Adaptive Security Appliance via Cisco ASDM. Use Cisco ASDM to edit the Cisco ASA 5505 Adaptive Security Appliance configurations to enable Advanced HTTP application inspection by completing the following tasks:

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.


Topology
OUTSIDE
INSIDE
209.165.201.1 /27
10.10.1.0 /24
ActualTests
MANAGEMENT
172.18.122.240
PC WITH ASDM ACCESS



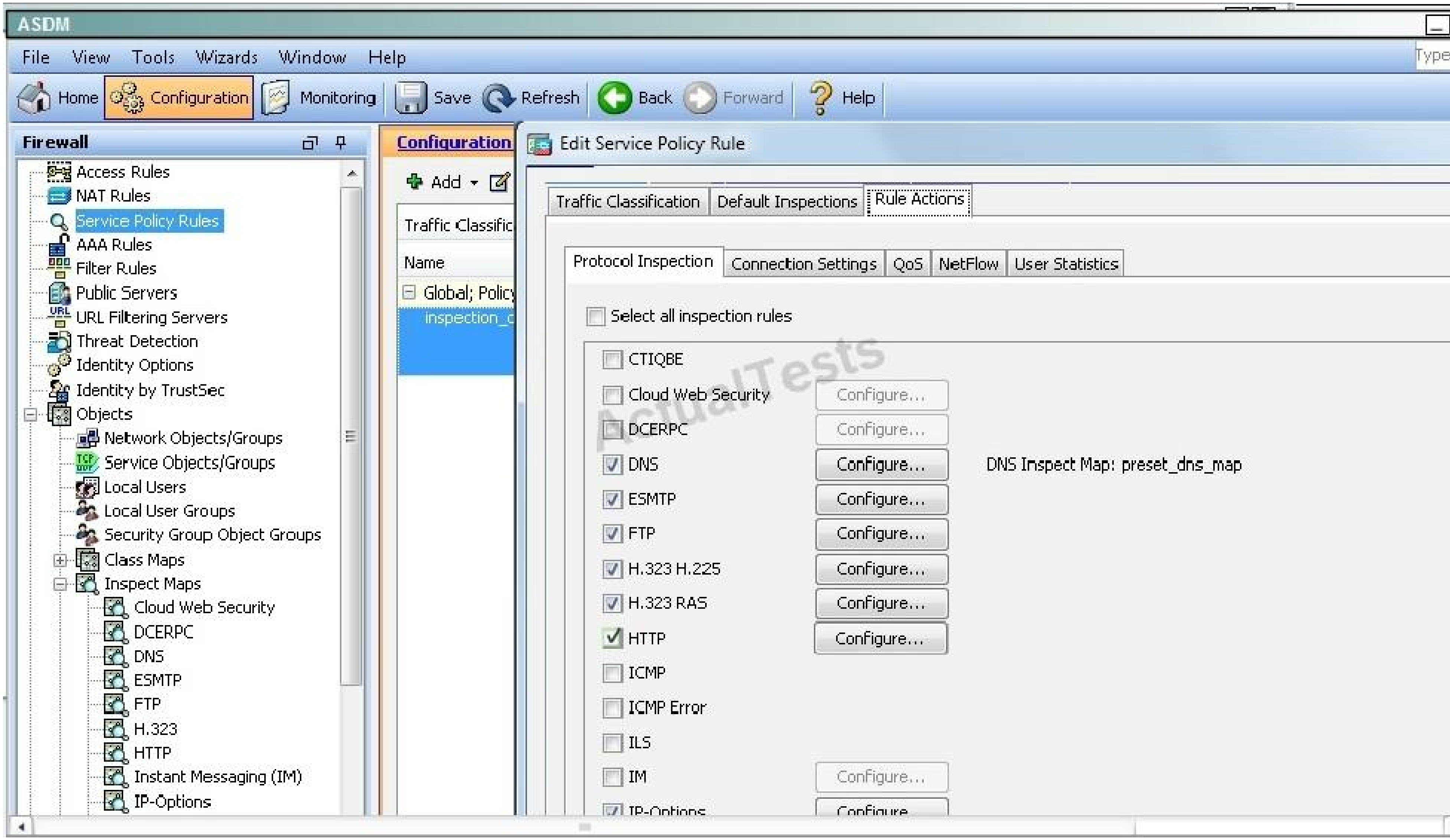
Traffic Classification										Rule Actions
Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	
Global; Policy: global_policy										
inspection_default			Match	any		any		default inspections		Inspect DNS Map preset_dns_ma Inspect ESMTP (14 more inspect actions)

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

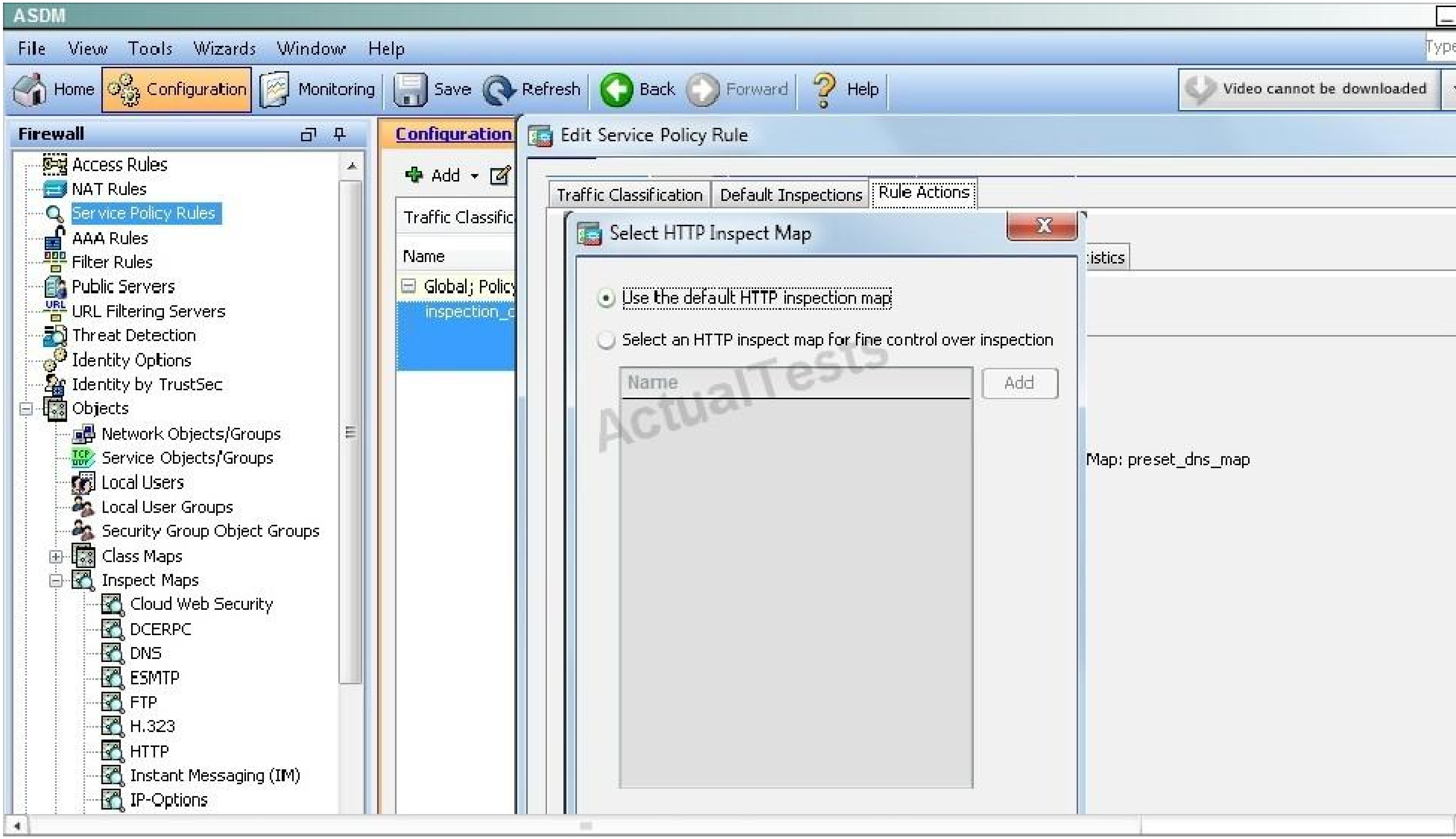
Answer: Please check the steps in explanation part below:
Explanation:
1) Click on Service Policy Rules, then Edit the default inspection rule.
2) Click on Rule Actions, then enable HTTP as shown here:



☐ Select all inspection rules

☐ CTIQBE
☐ Cloud Web Security Configure...
☐ DCERPC Configure...
☑ DNS Configure... DNS Inspect Map: preset_dns_map
☑ ESMTP Configure...
☑ FTP Configure...
☑ H.323 H.225 Configure...
☑ H.323 RAS Configure...
☑ HTTP Configure...
☐ ICMP
☐ ICMP Error
☐ ILS
☐ IM Configure...
☑ IP-Options Configure...

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

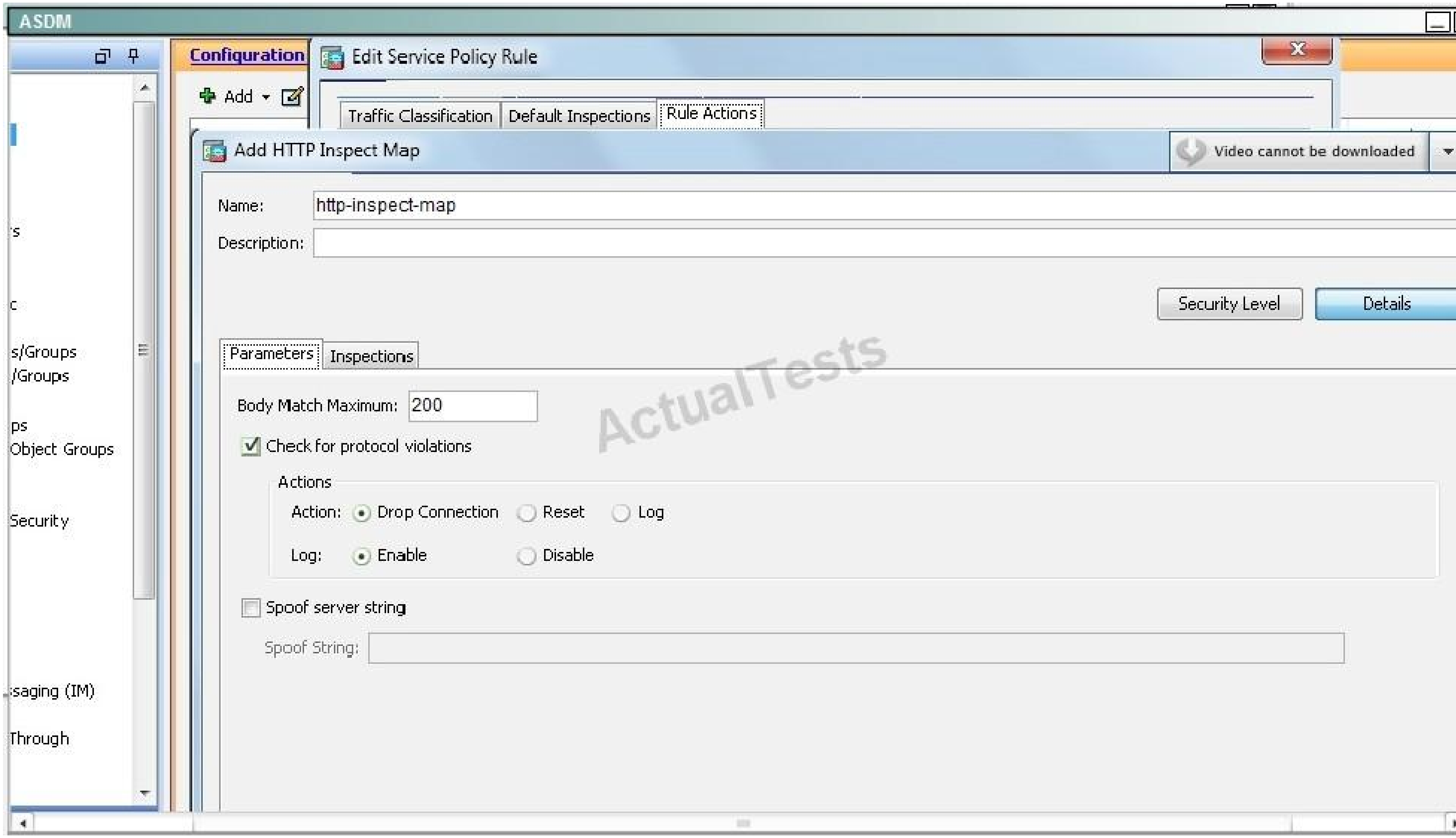


Select HTTP Inspect Map

● Use the default HTTP inspection map

○ Select an HTTP inspect map for fine control over inspection

4) Create the new map in ASDM like shown:



Name: http-inspect-map

Description:

Body Match Maximum: 200

☑ Check for protocol violations

Actions

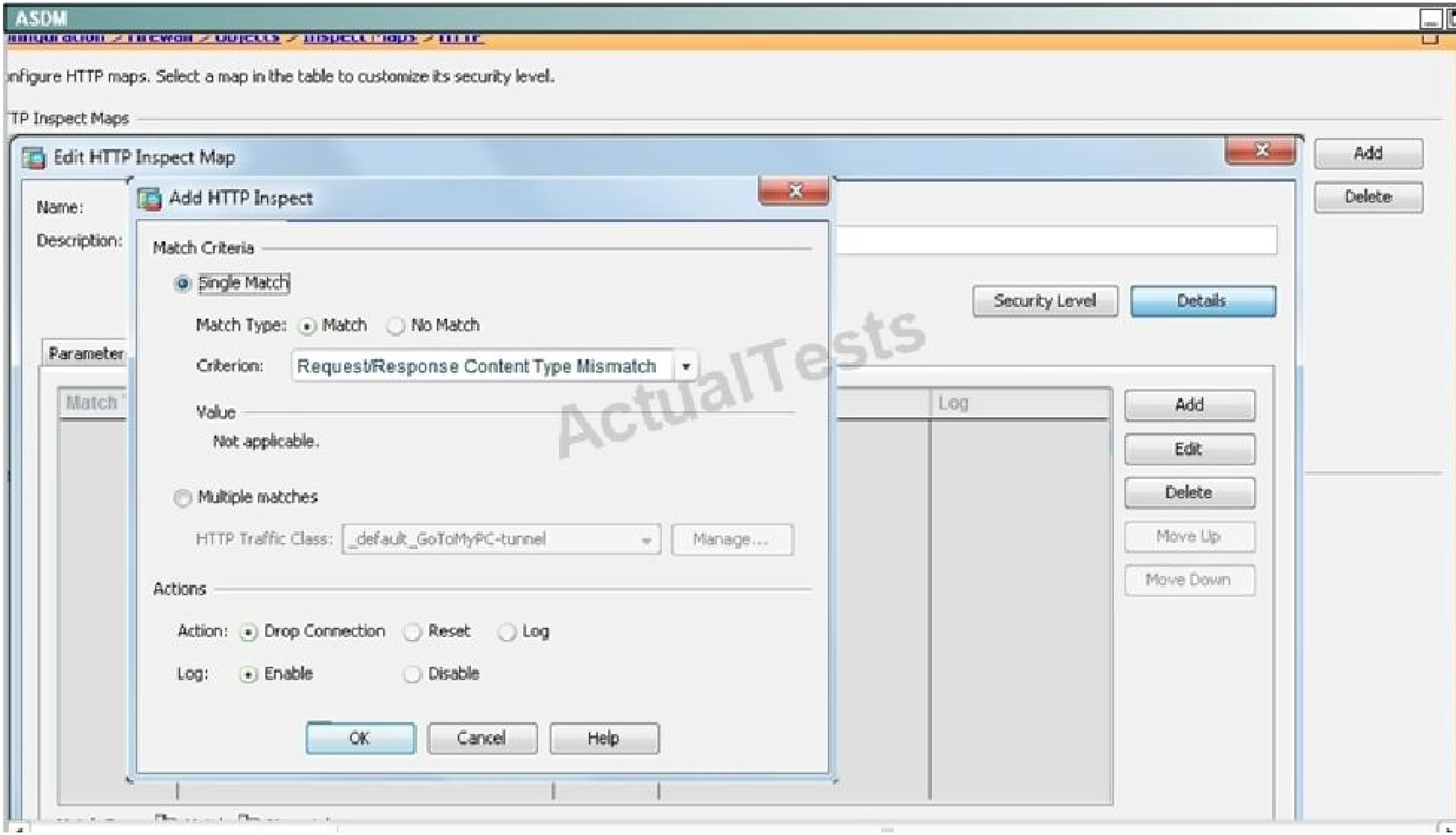
Action: ● Drop Connection ○ Reset ○ Log

Log: ● Enable ○ Disable

□ Spoof server string

Spoof String:

5) Edit the policy as shown:



nfigure HTTP maps. Select a map in the table to customize its security level.

Add HTTP Inspect

Match Criteria

● Single Match

Match Type: ● Match ○ No Match

Criterion: Request/Response Content Type Mismatch

Value

Not applicable.

○ Multiple matches

HTTP Traffic Class: _default_GoToMyPC-tunnel

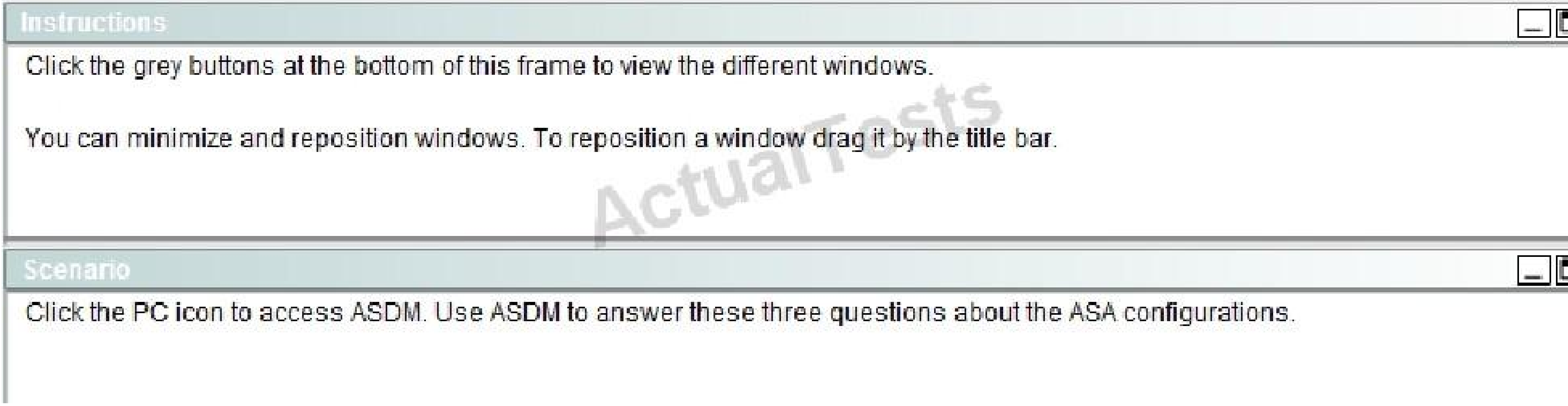
Actions

Action: ● Drop Connection ○ Reset ○ Log

Log: ● Enable ○ Disable

6) Hit OK

QUESTION 61



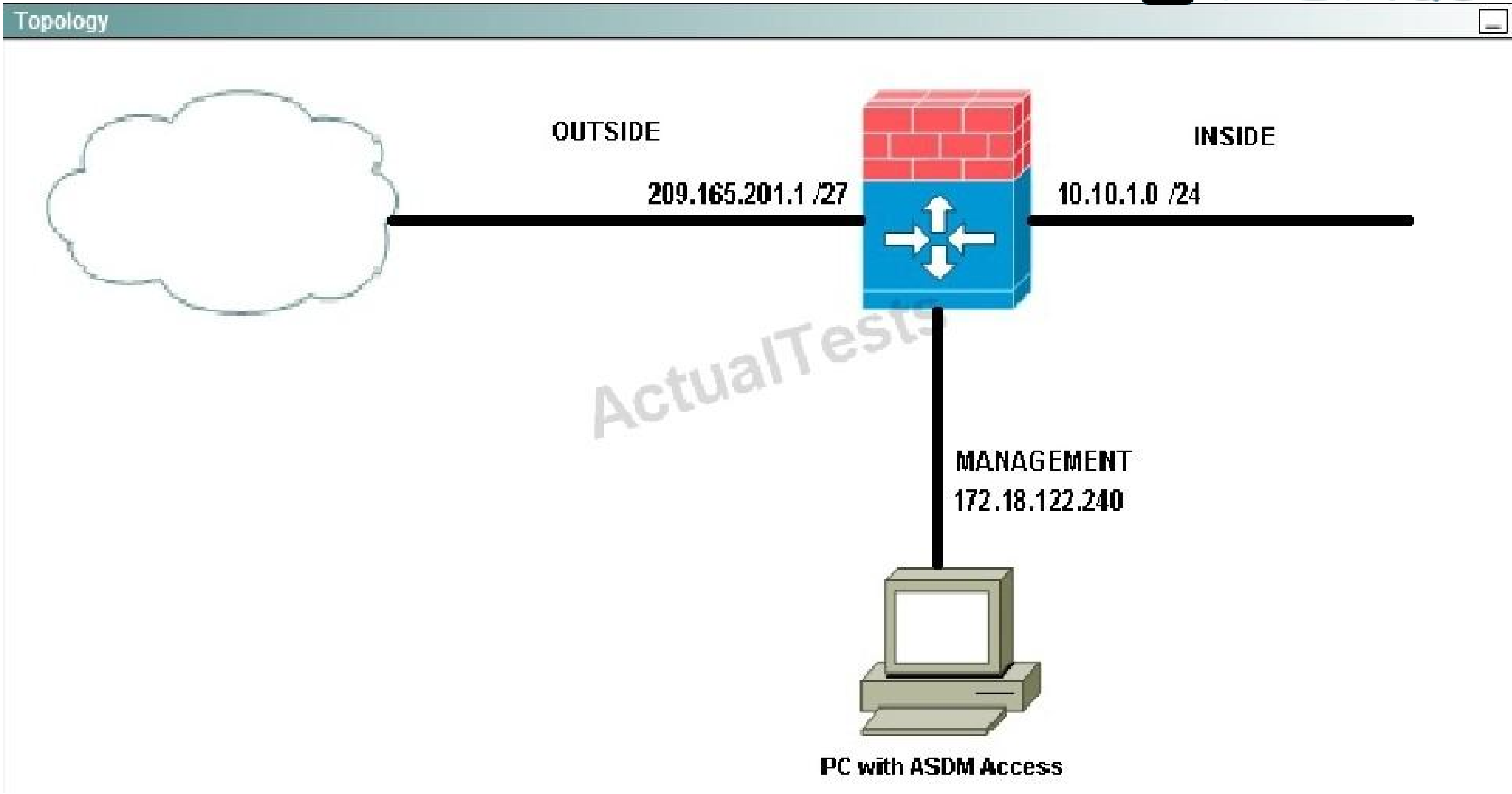
Instructions

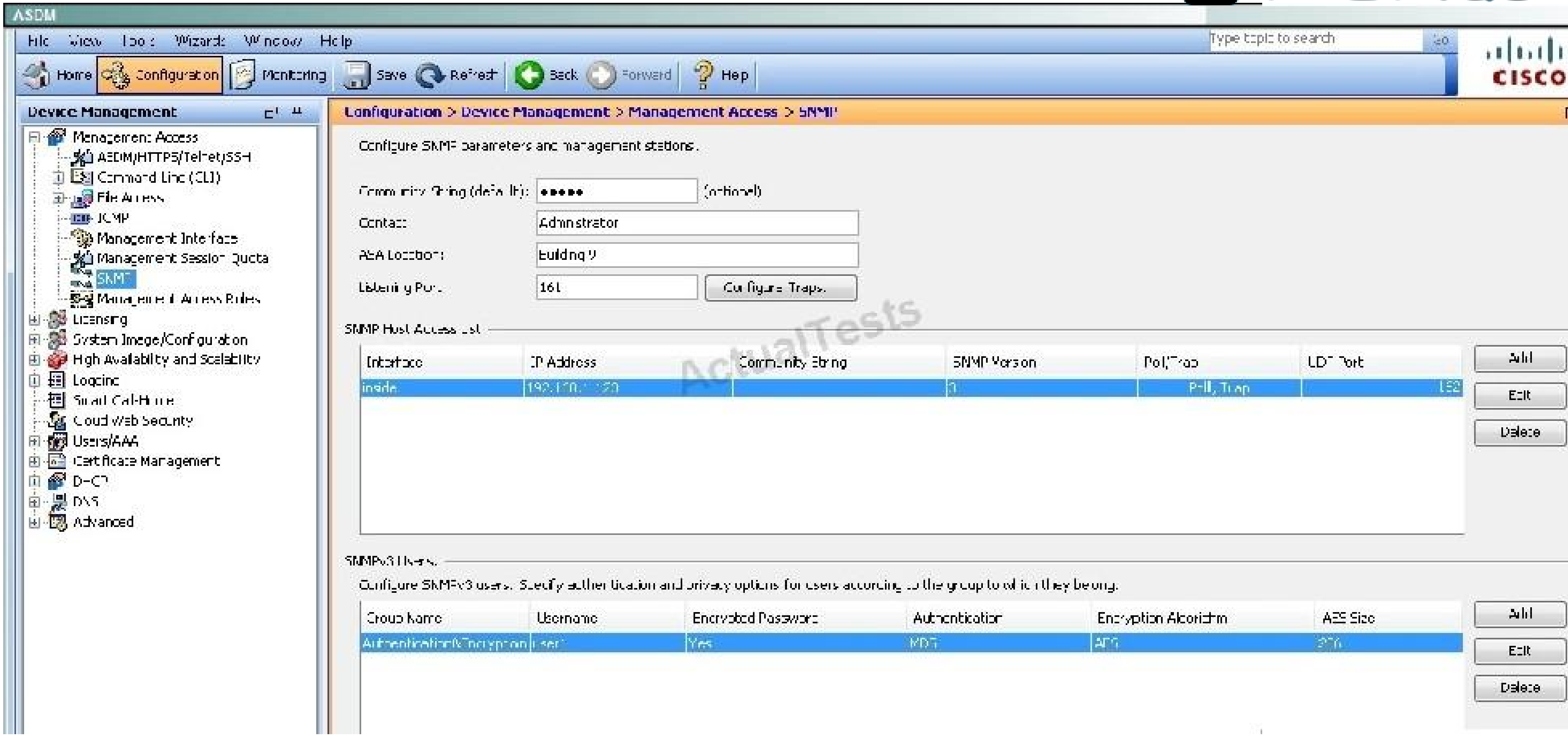
Click the grey buttons at the bottom of this frame to view the different windows.

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.


Topology
OUTSIDE
209.165.201.1 /27
INSIDE
10.10.1.0 /24
MANAGEMENT
172.18.122.240
PC with ASDM Access



Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

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

Contact: Administrator

ASA Location: Building 9

Listening Port: 161 Configure Traps...

SNMP Host Access List

Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.120		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

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.

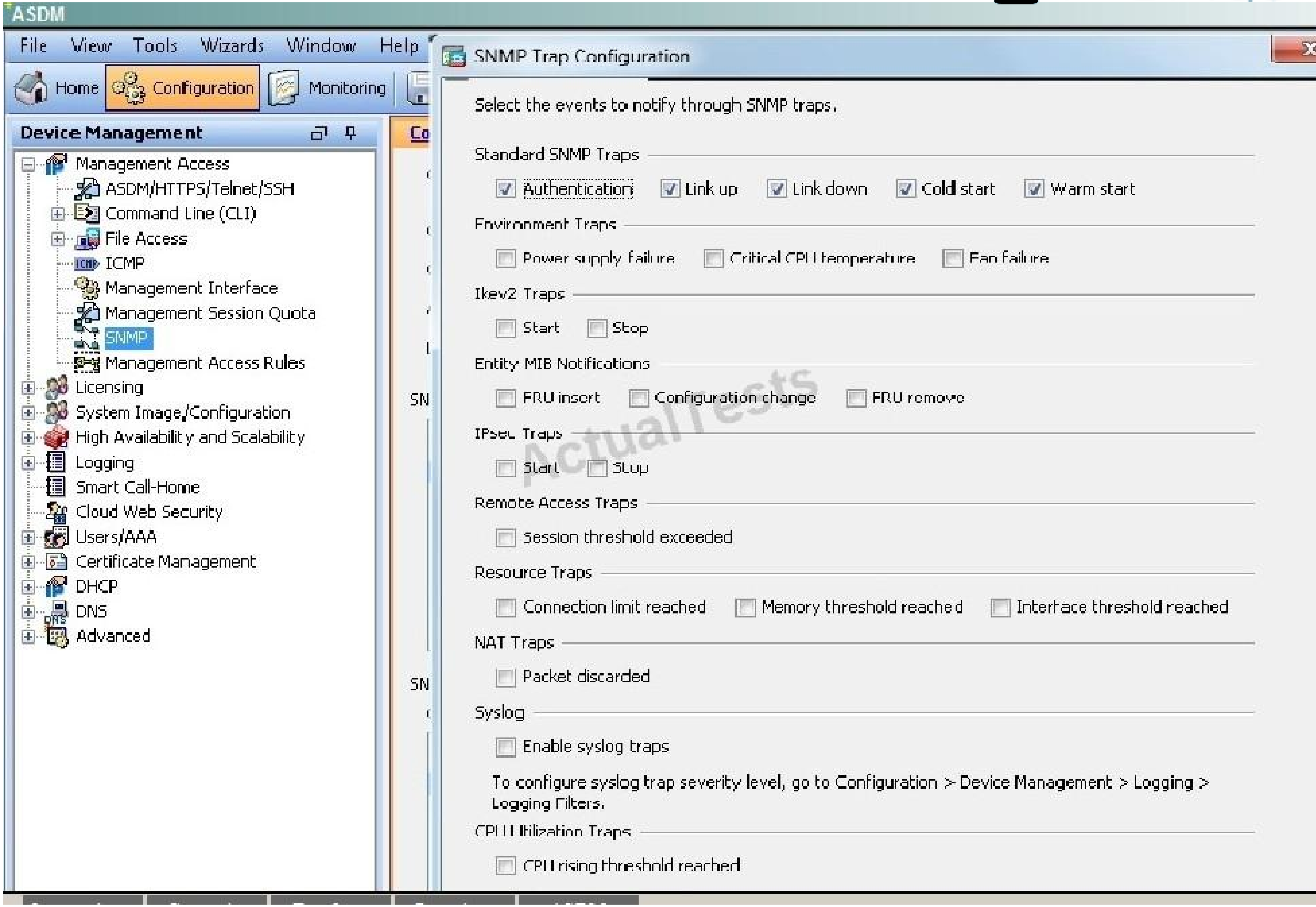
D. SNMPv3 is enabled by default and SNMP v1 and 2c are disabled by default.

E. SNMPv3 is more secure because it uses SSH as the transport mechanism.

Correct Answer: C

Section: (none)
Explanation

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



SNMP Trap Configuration

Select the events to notify through SNMP traps.

Standard SNMP Traps

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

Environment Traps

□ Power supply failure □ Critical CPU temperature □ Fan failure

Ikev2 Traps

□ Start □ Stop

Entity MIB Notifications

□ FRU insert □ Configuration change □ FRU remove

IPsec Traps

□ Start □ Stop

Remote Access Traps

□ Session threshold exceeded

Resource Traps

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

NAT Traps

□ Packet discarded

Syslog

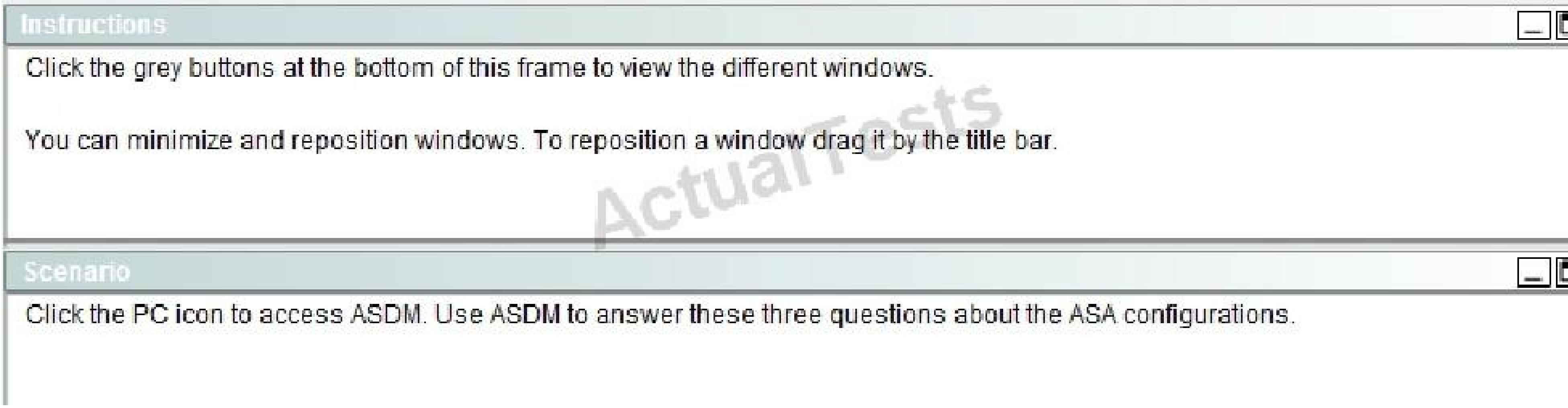
□ Enable syslog traps

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

CPU Utilization Traps

□ CPU rising threshold reached

QUESTION 62



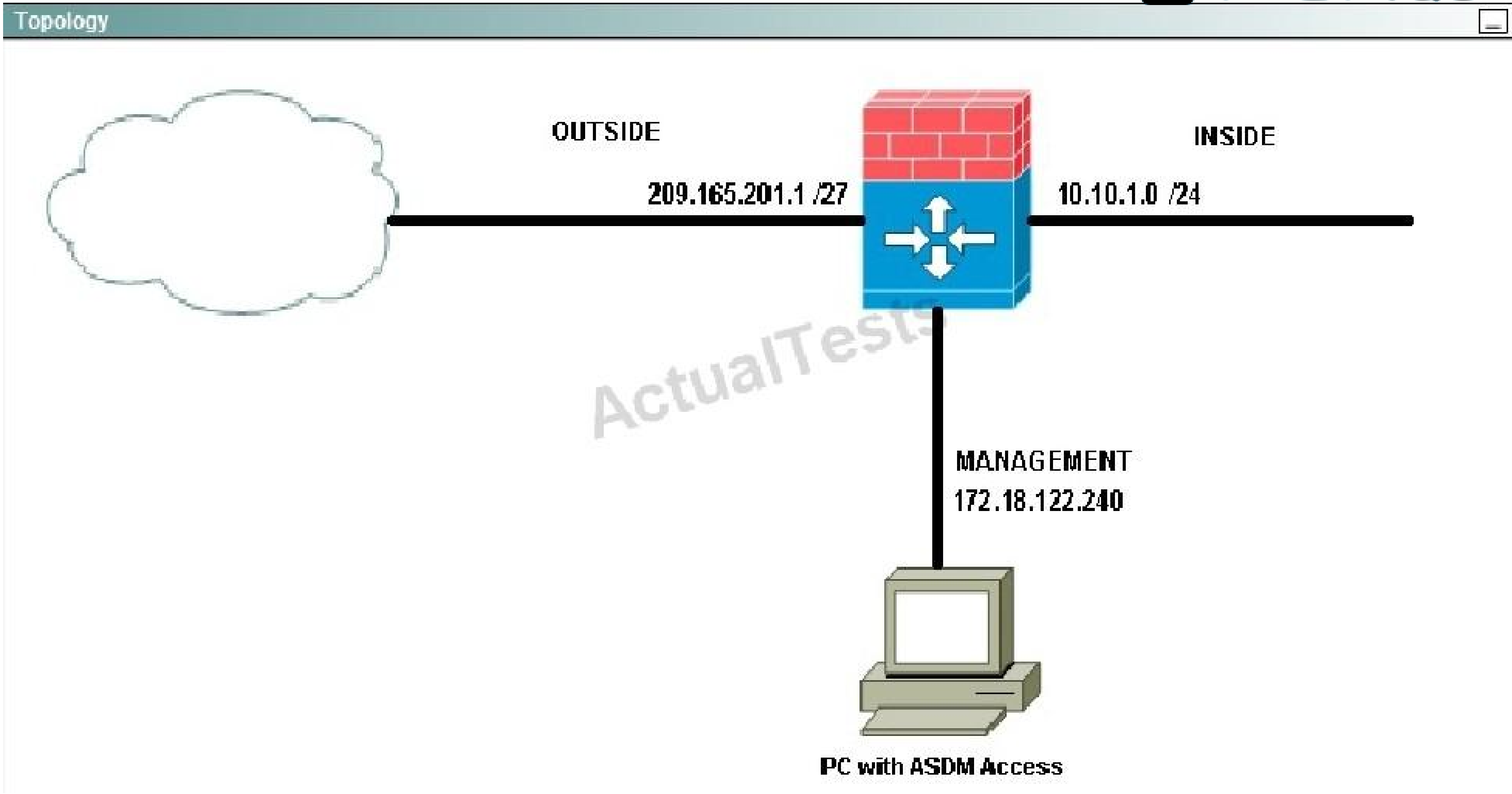
Instructions

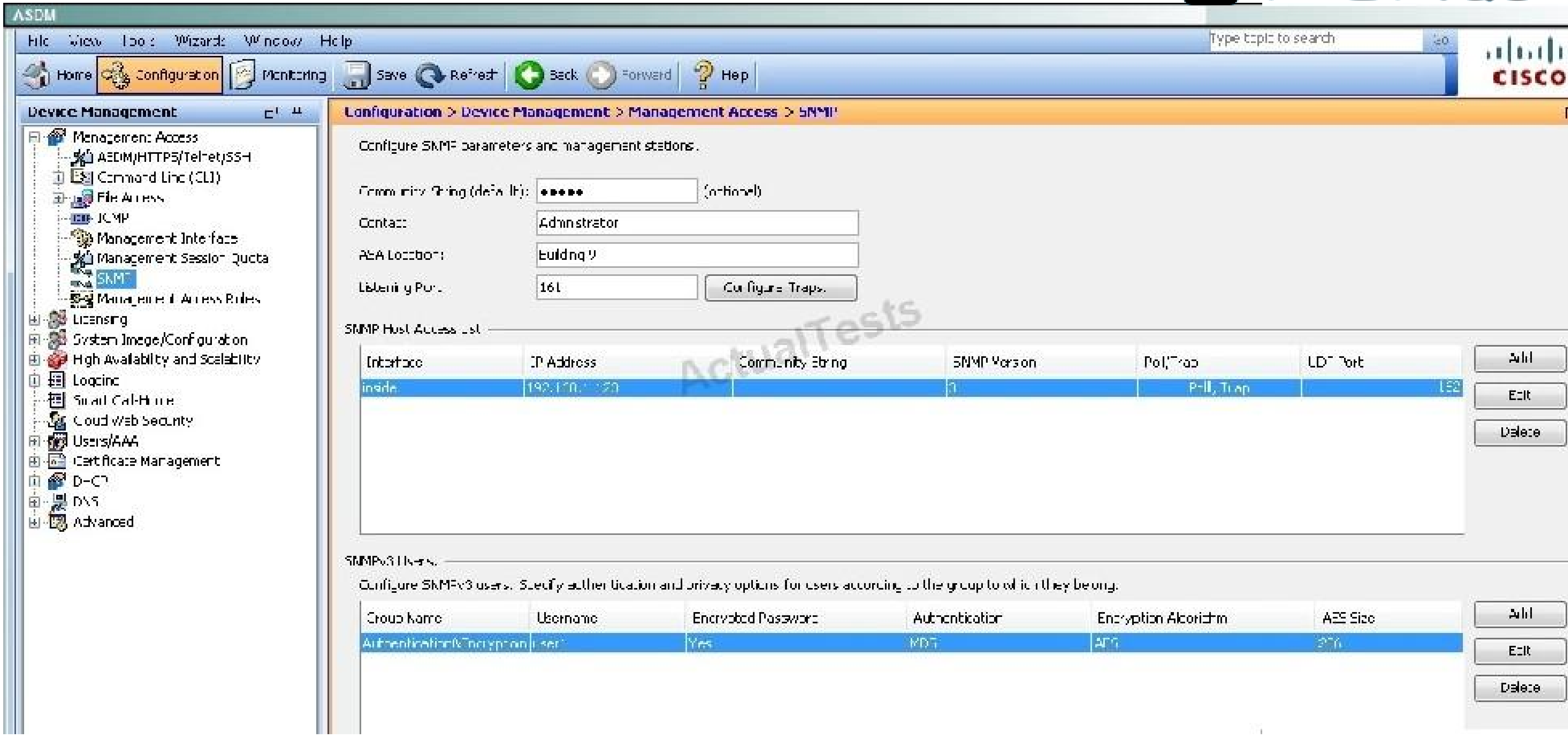
Click the grey buttons at the bottom of this frame to view the different windows.

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.


Topology
OUTSIDE
209.165.201.1 /27
INSIDE
10.10.1.0 /24
MANAGEMENT
172.18.122.240
PC with ASDM Access



Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

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

Contact: Administrator

ASA Location: Building 9

Listening Port: 161 Configure Traps...

SNMP Host Access List

Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.120		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

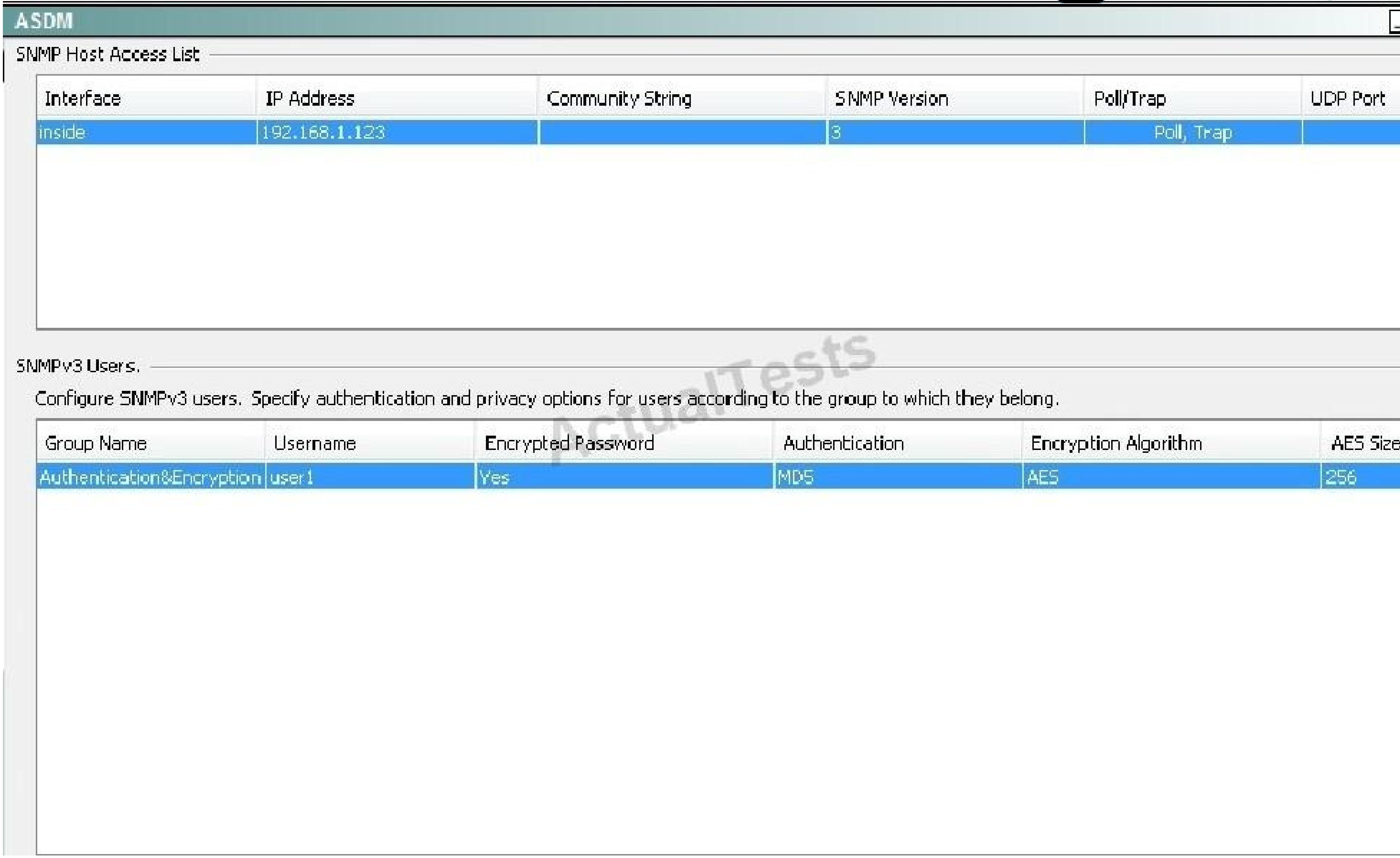
Cisco 300-206 Exam

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, andAES (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

Correct Answer: A
Section: (none)
Explanation

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



SNMP Host Access List

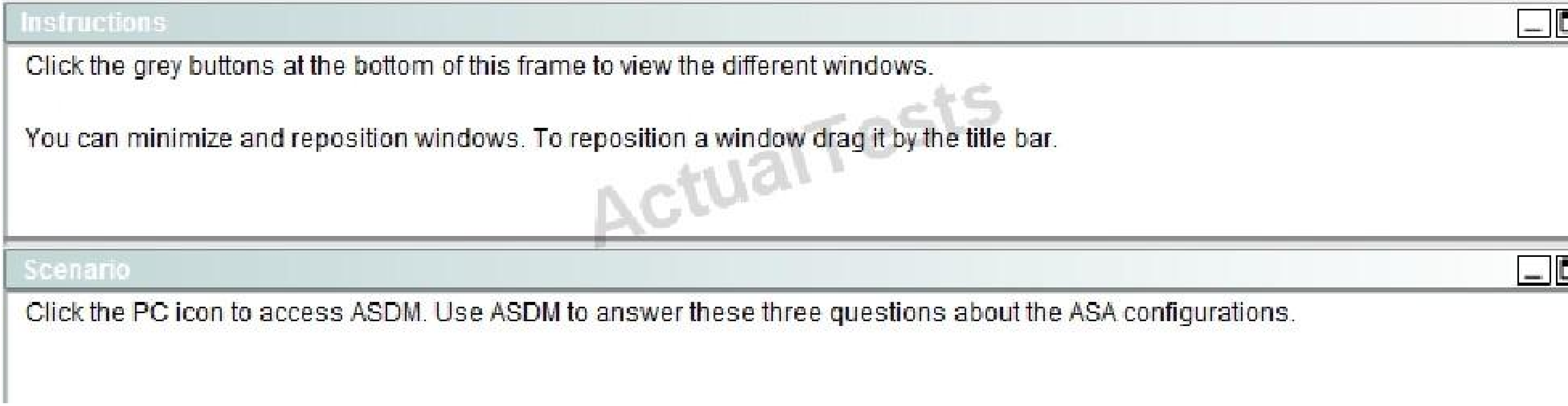
Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.123		3	Poll, Trap	

SNMPv3 Users.

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

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

QUESTION 63



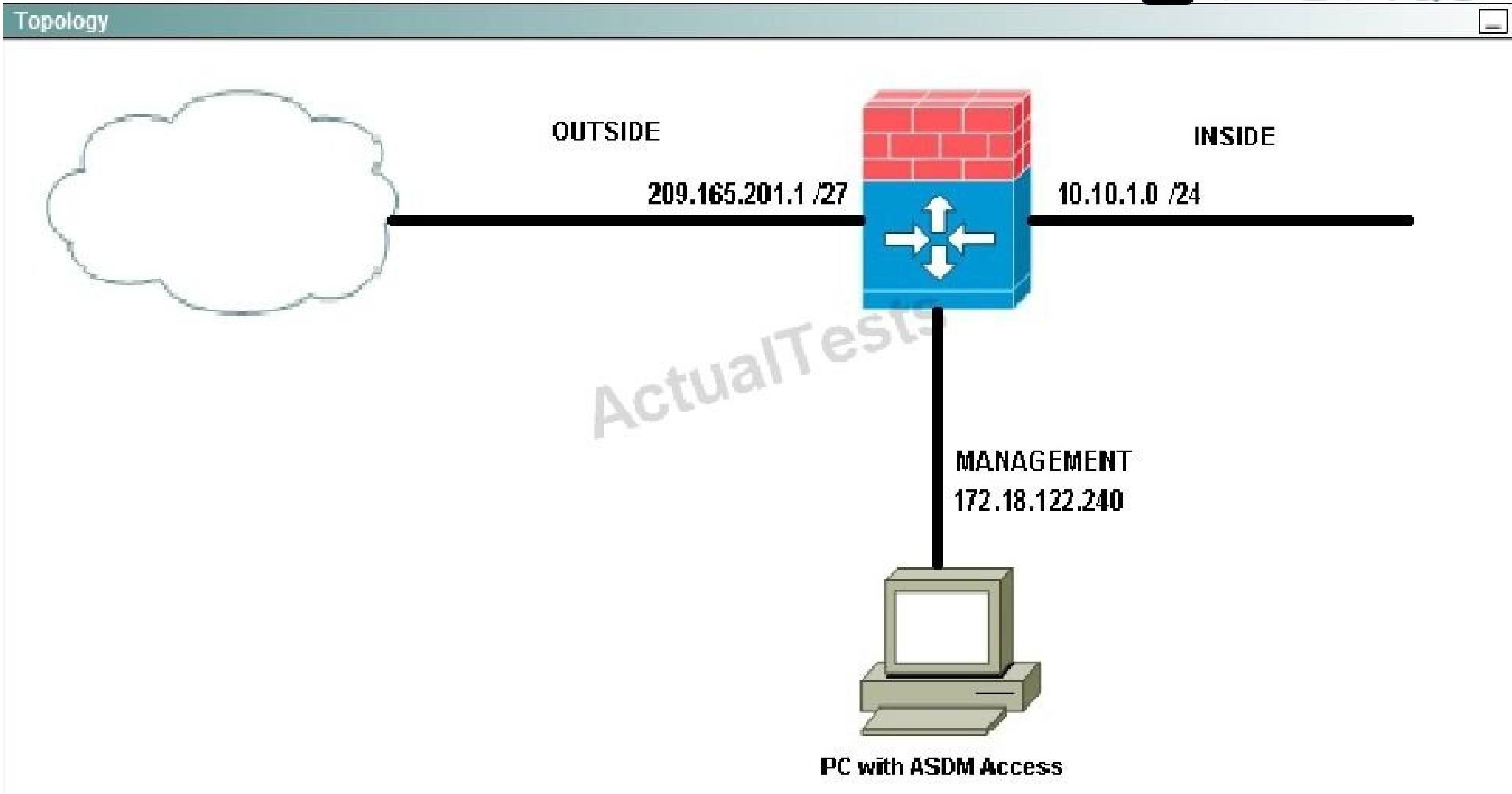
Instructions

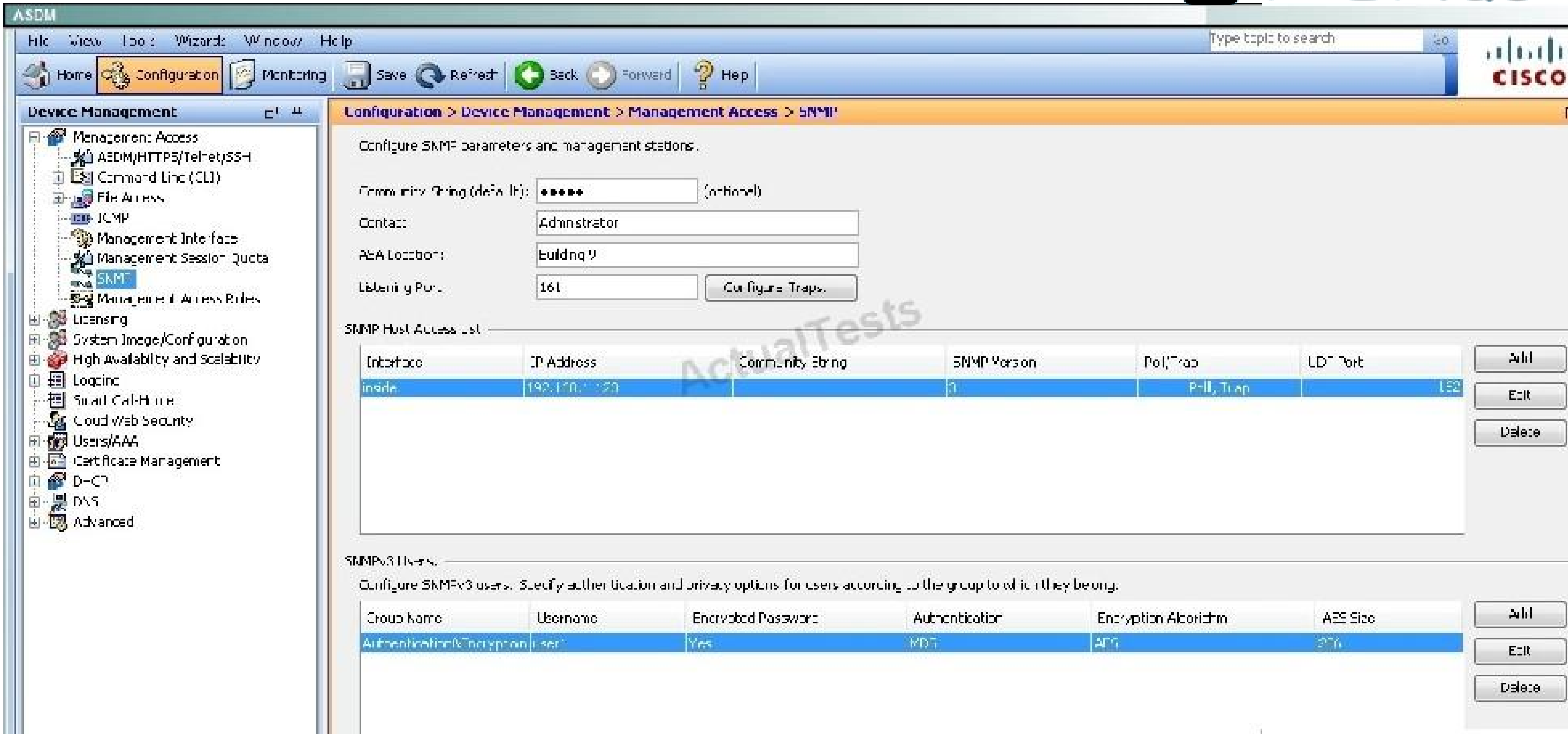
Click the grey buttons at the bottom of this frame to view the different windows.

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.


Topology
OUTSIDE
209.165.201.1 /27
INSIDE
10.10.1.0 /24
MANAGEMENT
172.18.122.240
PC with ASDM Access



Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

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

Contact: Administrator

ASA Location: Building 9

Listening Port: 161 Configure Traps...

SNMP Host Access List

Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.120		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

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.

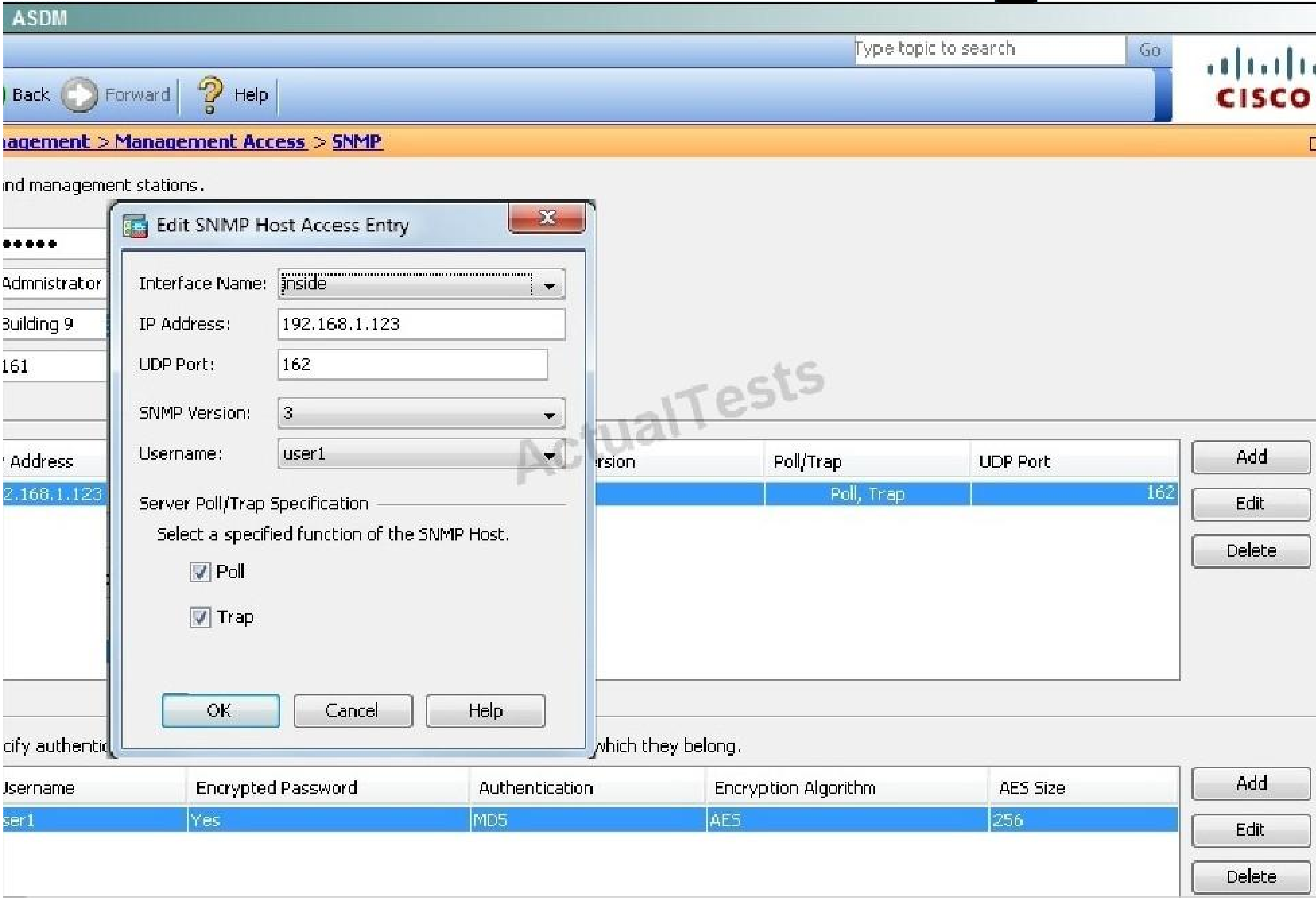
Correct Answer: B

Section: (none)

Explanation

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

"Pass Any Exam. Any Time." - www.actualtests.com 33
Cisco 300-206 Exam



agement > Management Access > SNMP

nd management stations.

••••••

Administrator

Building 9

161

Edit SNMP Host Access Entry

Interface Name: inside

IP Address: 192.168.1.123

UDP Port: 162

SNMP Version: 3

Username: user1

Server Poll/Trap Specification

Select a specified function of the SNMP Host.

☑ Poll

☑ Trap

Address	rsion	Poll/Trap	UDP Port
2.168.1.123		Poll, Trap	162

cify authenti… which they belong.

Jsername	Encrypted Password	Authentication	Encryption Algorithm	AES Size
ser1	Yes	MD5	AES	256

QUESTION 64
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
On an ASA running version 9.0, which command is used to nest objects in a pre-existing group?

A. object-group
B. network group-object
C. object-group network
"Pass Any Exam. Any Time." - www.actualtests.com 34
Cisco 300-206 Exam
D. group-object

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 66
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
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
"Pass Any Exam. Any Time." - www.actualtests.com 35
Cisco 300-206 Exam
D. domain context 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
You are a security engineer at a large multinational retailer. Your Chief Information Officer recently attended a security conference and has asked you to secure the network infrastructure from VLAN hopping.

"Pass Any Exam. Any Time." - www.actualtests.com 36
Cisco 300-206 Exam

Which statement describes how VLAN hopping can be avoided?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
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. Also configure the Firewall Operators group to have privilege level 6 access.
B. 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.
Configure level 15 access to be assigned to members of the Firewall Admins group.
C. 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.
Configure level 15 access to be assigned to members of the Firewall Admins group.
D. Active Directory Group membership cannot be used as a determining factor for accessing the Cisco ASA CLI.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 73
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
Which two configurations are necessary to enable password-less SSH login to an IOS router? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
Which two features does Cisco Security Manager provide? (Choose two.)

A. Configuration and policy deployment before device discovery
B. Health and performance monitoring
"Pass Any Exam. Any Time." - www.actualtests.com 38
Cisco 300-206 Exam
C. Event management and alerting
D. Command line menu for troubleshooting
E. Ticketing management and tracking

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 77
When it is configured in accordance to Cisco best practices, the switchport port-security maximum command can mitigate which two types of Layer 2 attacks? (Choose two.)

A. rogue DHCP servers
B. ARP attacks
C. DHCP starvation

D. MAC spoofing
E. CAM attacks
F. IP spoofing

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

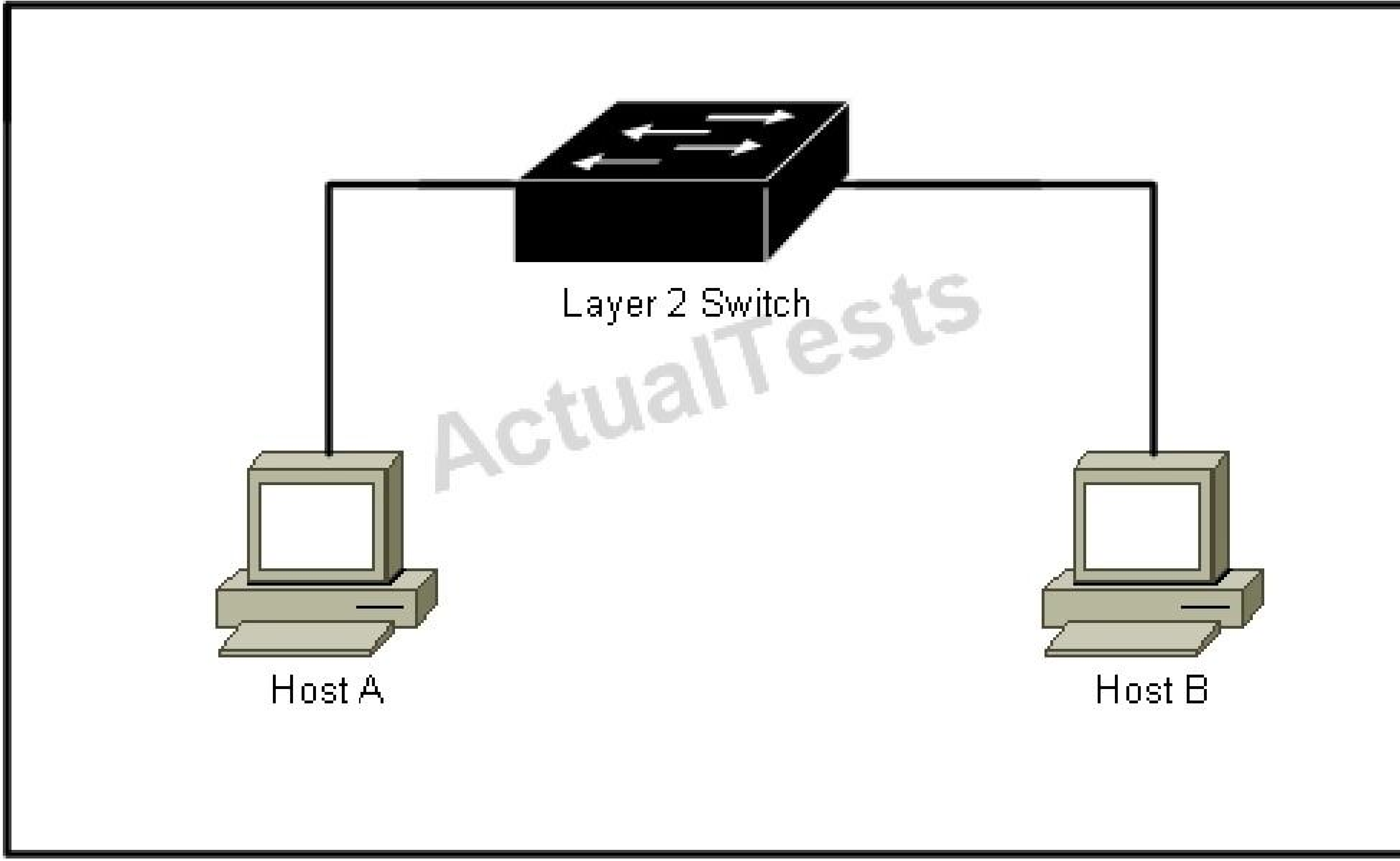
QUESTION 78
When configured in accordance to Cisco best practices, the ip verify source command can mitigate which two types of Layer 2 attacks? (Choose two.)

A. rogue DHCP servers
B. ARP attacks
C. DHCP starvation
D. MAC spoofing
E. CAM attacks
F. IP spoofing
"Pass Any Exam. Any Time." - www.actualtests.com 43
Cisco 300-206 Exam

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
Refer to the exhibit.



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

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
Which security operations management best practice should be followed to enable appropriate network access for administrators?

"Pass Any Exam. Any Time." - www.actualtests.com 44
Cisco 300-206 Exam

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 81
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82
Which three options correctly identify the Cisco ASA1000V Cloud Firewall? (Choose three.)

A. operates at Layer 2
B. operates at Layer 3
C. secures tenant edge traffic
D. secures intraswitch traffic
E. secures data center edge traffic
F. replaces Cisco VSG
G. complements Cisco VSG
H. requires Cisco VSG

Correct Answer: BCG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
"Pass Any Exam. Any Time." - www.actualtests.com 45
Cisco 300-206 Exam
Which two SNMPv3 features ensure that SNMP packets have been sent securely? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
Which two statements about zone-based firewalls are true? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
An attacker has gained physical access to a password protected router. Which command will prevent access to the startup-config in NVRAM?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
"Pass Any Exam. Any Time." - www.actualtests.com 46
Cisco 300-206 Exam
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
Which configuration keyword will configure SNMPv3 with authentication but no encryption?

A. Auth
B. Priv
C. No auth
D. Auth priv

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
Which product can manage licenses, updates, and a single signature policy for 15 separate IPS

"Pass Any Exam. Any Time." - www.actualtests.com 47
Cisco 300-206 Exam
appliances?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
Which three statements about private VLANs are true? (Choose three.)

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

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
When you set a Cisco IOS Router as an SSH server, which command specifies the RSA public key of the remote peer when you set the SSH server to perform RSA-based authentication?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 48
Cisco 300-206 Exam

QUESTION 92
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 93
Which type of object group will allow configuration for both TCP 80 and TCP 443?

A. service
B. network
C. time range
D. user group

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

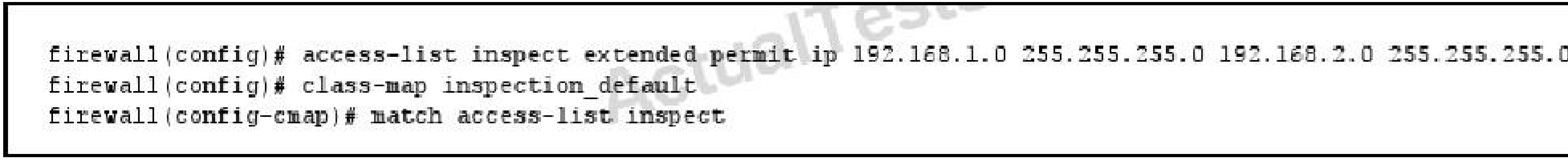
QUESTION 94
When you configure a Botnet Traffic Filter on a Cisco firewall, what are two optional tasks? (Choose two.)

A. Enable the use of dynamic databases.
B. Add static entries to the database.
C. Enable DNS snooping.
D. Enable traffic classification and actions.
E. Block traffic manually based on its syslog information.
"Pass Any Exam. Any Time." - www.actualtests.com 49
Cisco 300-206 Exam

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95



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

Refer to the exhibit. What is the effect of this configuration?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
At which layer does Dynamic ARP Inspection validate packets?

A. Layer 2
B. Layer 3
"Pass Any Exam. Any Time." - www.actualtests.com 50
Cisco 300-206 Exam
C. Layer 4
D. Layer 7

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
Which feature can suppress packet flooding in a network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99
What is the default violation mode that is applied by port security?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 100
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
"Pass Any Exam. Any Time." - www.actualtests.com 51
Cisco 300-206 Exam
D. Secure Shell
E. SNMP

Correct Answer: AB
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 101
At which layer does MACsec provide encryption?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
What are two enhancements of SSHv2 over SSHv1? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 103
What is the result of the default ip ssh server authenticate user command?

A. It enables the public key, keyboard, and password authentication methods.

B. It enables the public key authentication method only.

C. It enables the keyboard authentication method only.

D. It enables the password authentication method only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 104
What are three of the RBAC views within Cisco IOS Software? (Choose three.)

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

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
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

Correct Answer: E

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 106
What are two high-level task areas in a Cisco Prime Infrastructure life-cycle workflow? (Choose two.)

A. Design
"Pass Any Exam. Any Time." - www.actualtests.com 53
Cisco 300-206 Exam
B. Operate
C. Maintain
D. Log
E. Evaluate

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 107
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.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 108
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 109
Which Cisco Security Manager form factor is recommended for deployments with fewer than 25 devices?

"Pass Any Exam. Any Time." - www.actualtests.com 54
Cisco 300-206 Exam

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 110
Which two TCP ports must be open on the Cisco Security Manager server to allow the server to communicate with the Cisco Security Manager client? (Choose two.)

A. 1741
B. 443

C. 80
D. 1740
E. 8080

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 111
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 112
Which function in the Cisco ADSM ACL Manager pane allows an administrator to search for a specfic element?

"Pass Any Exam. Any Time." - www.actualtests.com 55
Cisco 300-206 Exam

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

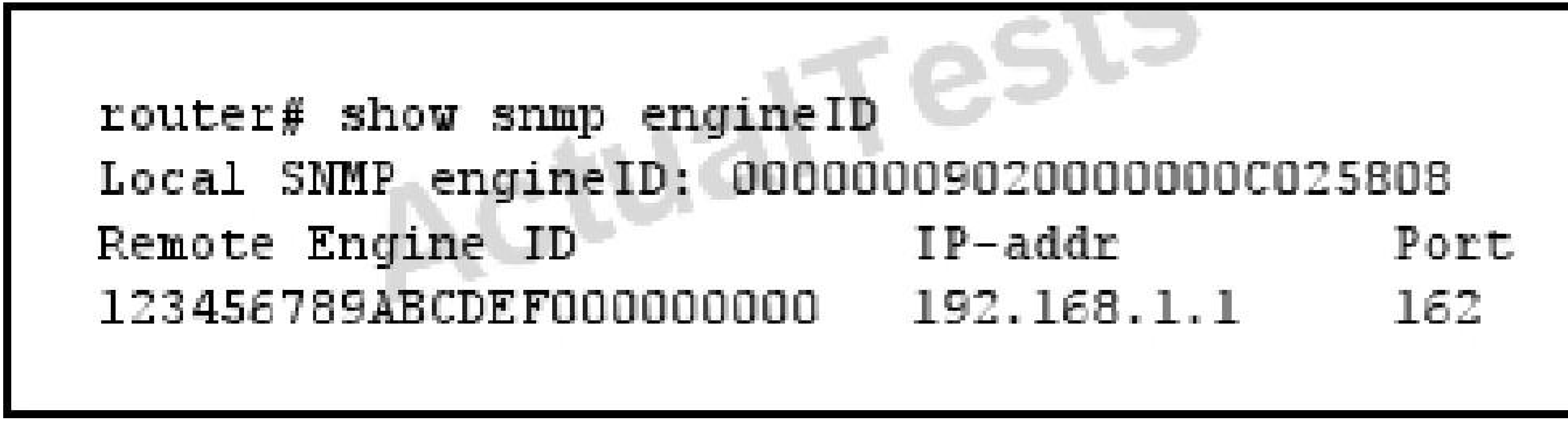
QUESTION 113
Which two router commands enable NetFlow on an interface? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 114



```
router# show snmp engineID
Local SNMP engineID: 00000009020000000C025808
Remote Engine ID               IP-addr         Port
123456789ABCDEF000000000   192.168.1.1     162
```

Refer to the exhibit. 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 56
Cisco 300-206 Exam

QUESTION 115
To which port does a firewall send secure logging messages?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 116
What is a required attribute to configure NTP authentication on a Cisco ASA?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
Which function does DNSSEC provide in a DNS infrastructure?

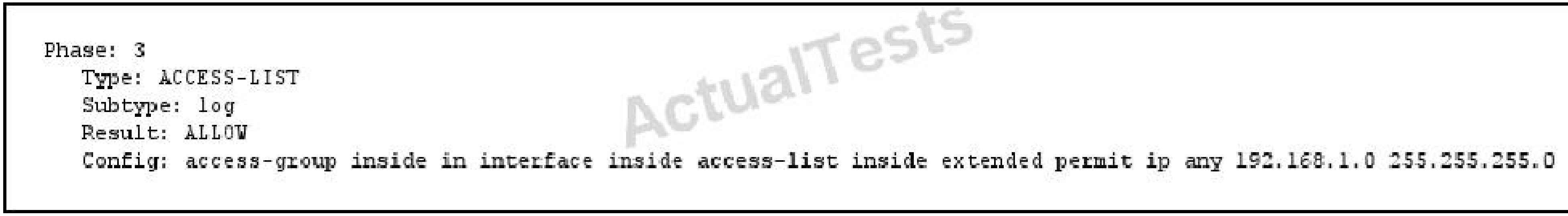
A. It authenticates stored information.
B. It authorizes stored information.
C. It encrypts stored information.
D. It logs stored security information.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 57
Cisco 300-206 Exam

QUESTION 118



```
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
```

Refer to the exhibit. 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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

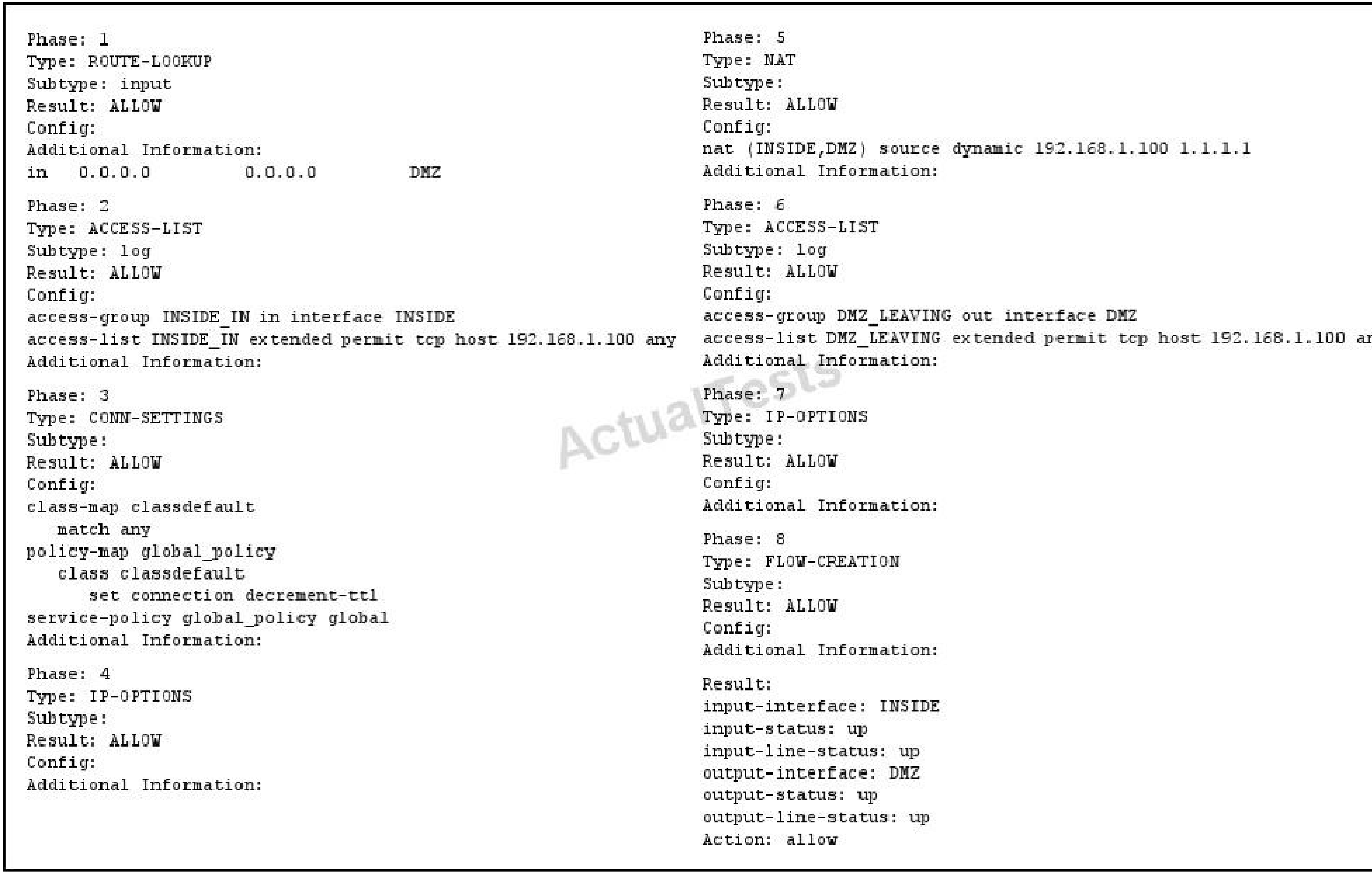
QUESTION 120
What can an administrator do to simultaneously capture and trace packets in a Cisco ASA?

A. Install a Cisco ASA virtual appliance.
B. Use the trace option of the capture command.
C. Use the trace option of the packet-tracer command.
D. Install a switch with a code that supports capturing, and configure a trunk to the Cisco ASA.
"Pass Any Exam. Any Time." - www.actualtests.com 58
Cisco 300-206 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 121



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

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

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

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

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

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

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

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 122
At which firewall severity level will debugs appear on a Cisco ASA?

A. 7
B. 6
C. 5
D. 4
"Pass Any Exam. Any Time." - www.actualtests.com 59
Cisco 300-206 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

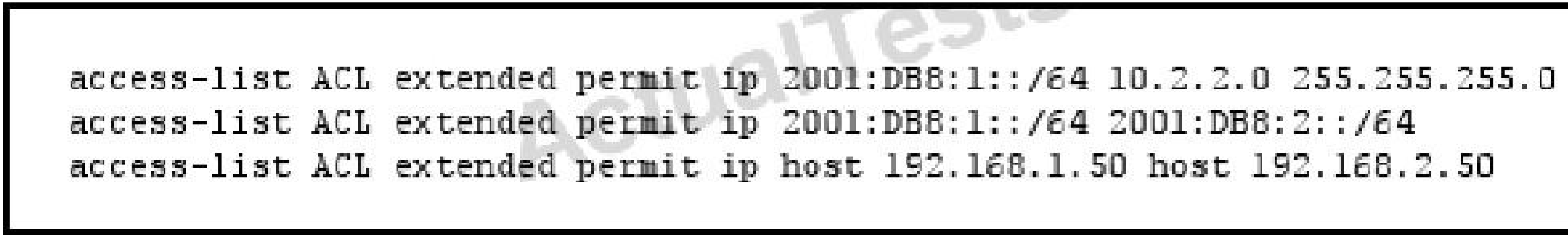
QUESTION 123
A Cisco ASA is configured in multiple context mode and has two user-defined contexts--Context_A and Context_B. From which context are device logging messages sent?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124



```
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
```

Cisco 300-206 Exam
Refer to the exhibit. Which type of ACL is shown in this configuration?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
CORRECT TEXT

You are the network security engineer for the Secure-X network. The company has recently detected Increase of traffic to malware Infected destinations. The Chief Security Officer deduced that some PCs in the internal networks are infected with malware and communicate with malware infected destinations.

The CSO has tasked you with enable Botnet traffic filter on the Cisco ASA to detect and deny further connection attempts from infected PCs to malware destinations. You are also required to test your configurations by initiating connections through the Cisco ASA and then display and observe the Real-Time Log Viewer in ASDM.

To successfully complete this activity, you must perform the following tasks:

* Download the dynamic database and enable use of it.

· Enable the ASA to download of the dynamic database

· Enable the ASA to download of the dynamic database.

· Enable DNS snooping for existing DNS inspection service policy rules..

· Enable Botnet Traffic Filter classification on the outside interface for All Traffic.

· Configure the Botnet Traffic Filter to drop blacklisted traffic on the outside interface. Use the default Threat Level settings

NOTE: The database files are stored in running memory; they are not stored in flash memory.

NOTE: DNS is enabled on the inside interface and set to the HQ-SRV (10.10.3.20).

NOTE: Not all ASDM screens are active for this exercise.

· Verify that the ASA indeed drops traffic to blacklisted destinations by doing the following:

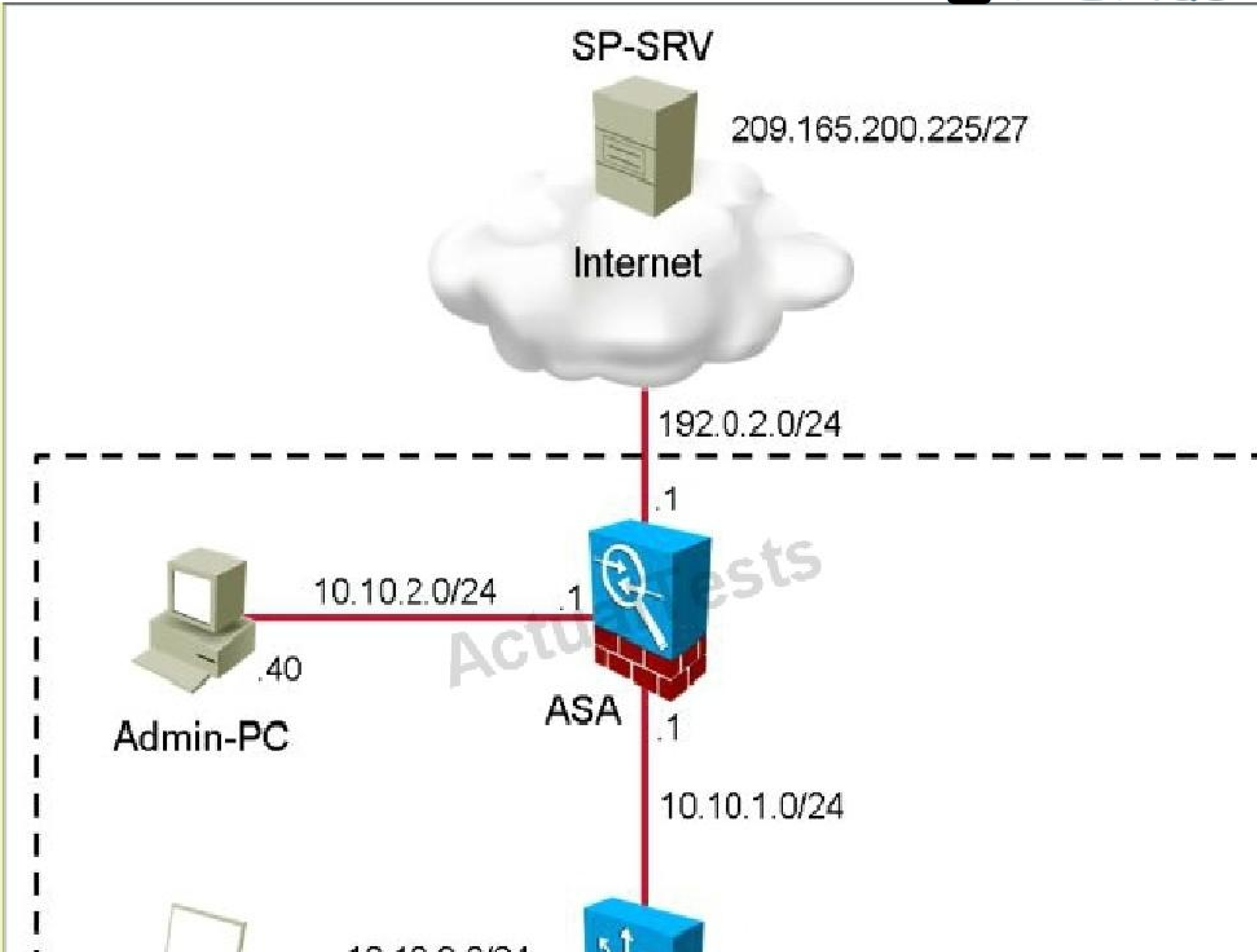
· From the Employee PC, navigate to http://www.google.com to make sure that access to the Internet is working.

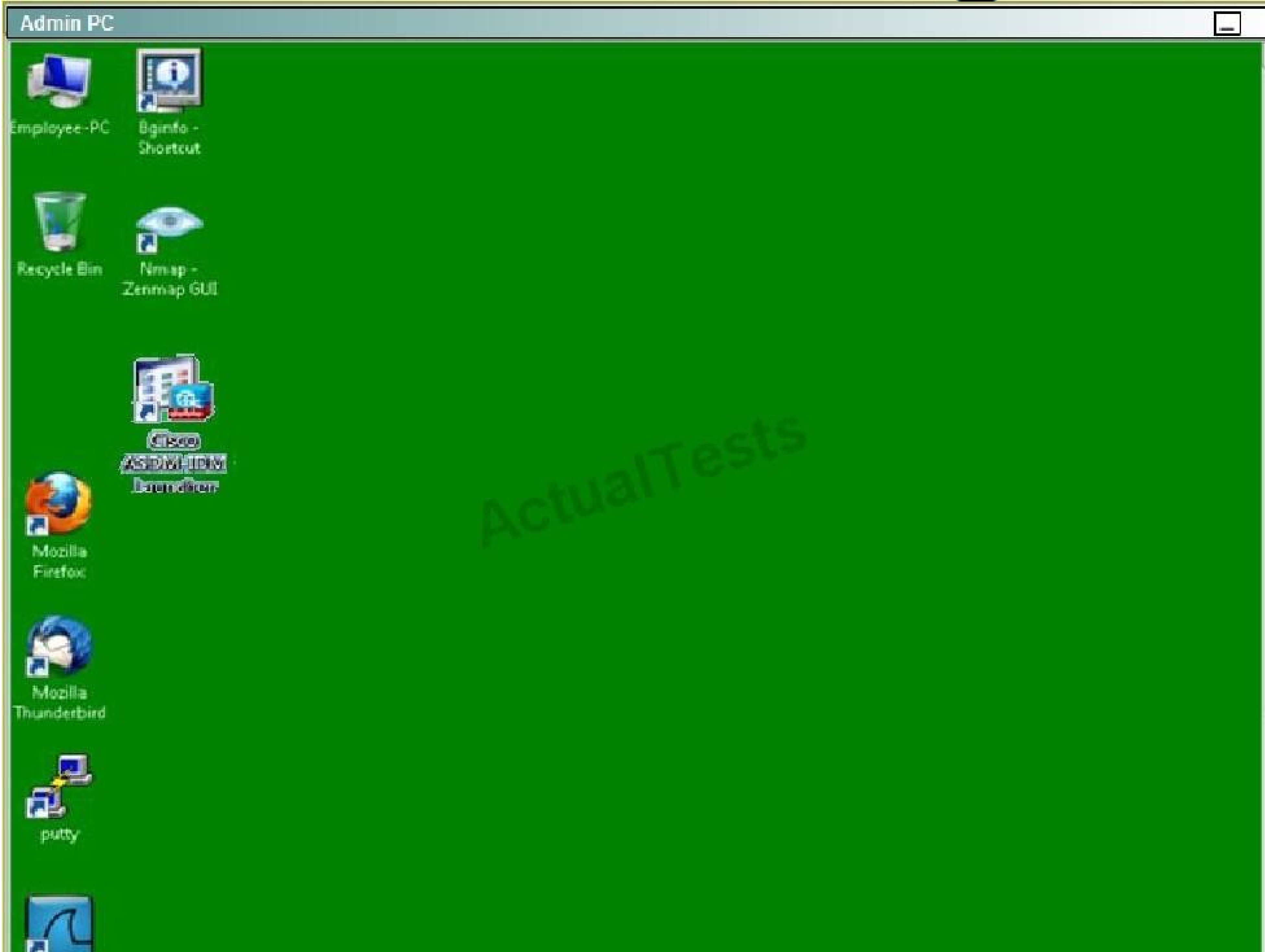
· From the Employee PC, navigate to http://bot-sparta.no-ip.org. This destination is classified as malware destination by the Cisco SIO database.

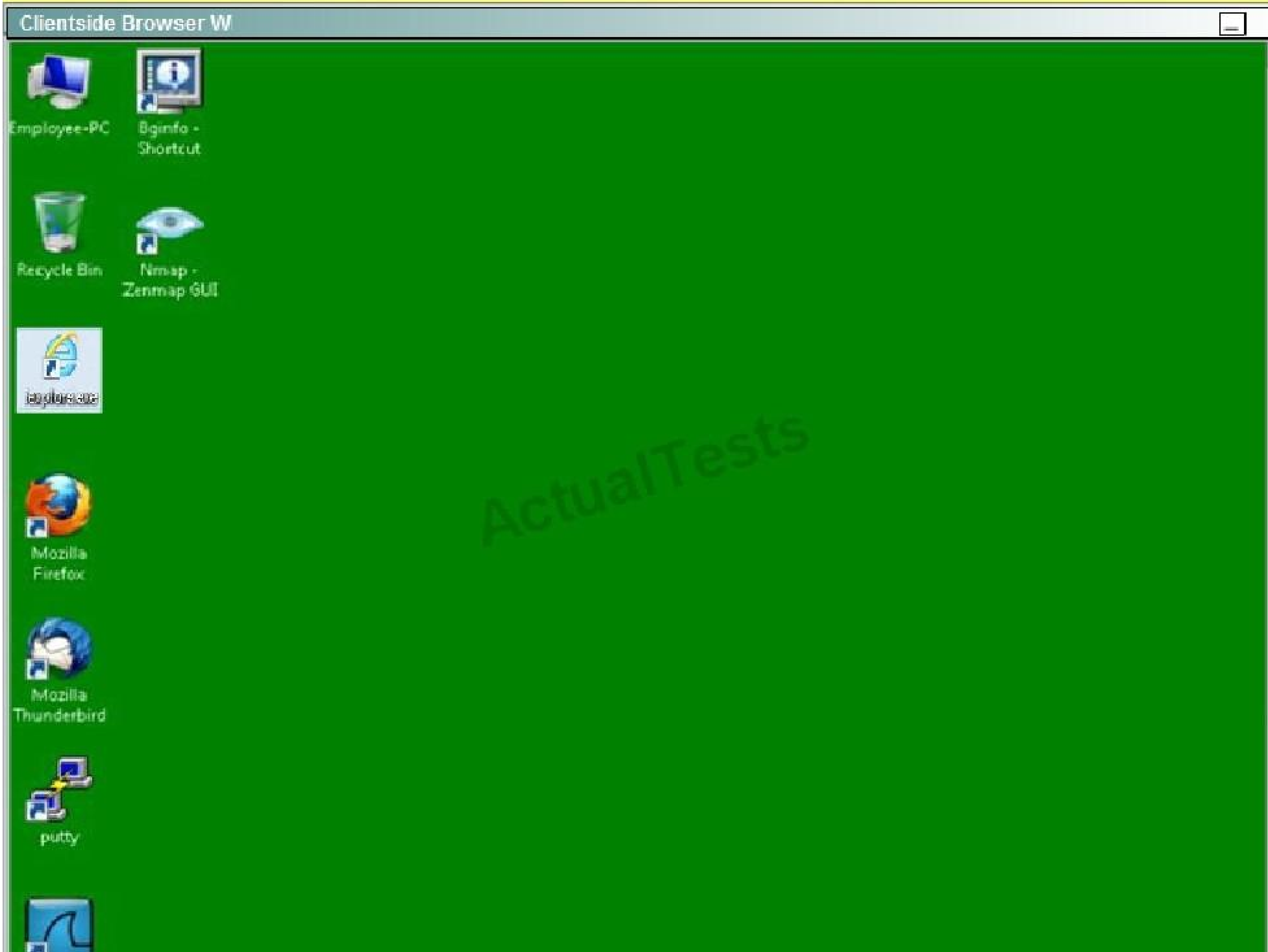
· From the Employee PC, navigate to http://superzarabotok-gid.ru/. This destination is classified as malware destination by the Cisco SIO database.

· From Admin PC, launch ASDM to display and observe the Real-Time Log Viewer.

You have completed this exercise when you have configured and successfully tested Botnet traffic filter on the Cisco ASA.


SP-SRV
209.165.200.225/27
Internet
192.0.2.0/24
.1
10.10.2.0/24
.1
.40
Admin-PC
ASA
.1
10.10.1.0/24


Admin PC
Employee-PC
Bginfo - Shortcut
Recycle Bin
Nmap - Zenmap GUI
Cisco ASDM-IDM Launcher
Mozilla Firefox
Mozilla Thunderbird
putty

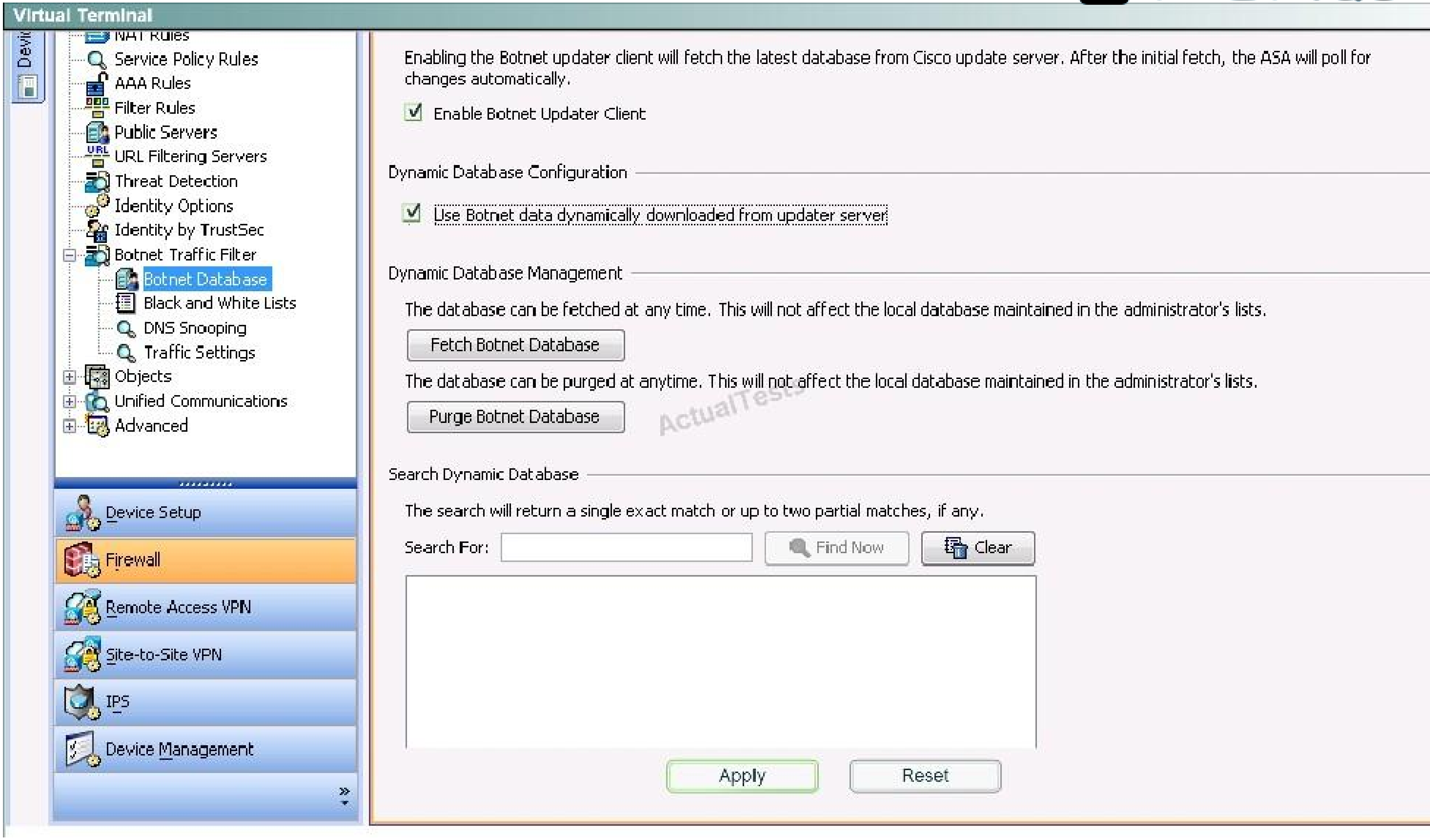

Clientside Browser W
Employee-PC
Bginfo - Shortcut
Recycle Bin
Nmap - Zenmap GUI
iexplore.exe
Mozilla Firefox
Mozilla Thunderbird
putty

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: See the explanation for detailed answer to this sim question.
Explanation:
First, click on both boxes on the Botnet Database as shown below and hit apply:

"Pass Any Exam. Any Time." - www.actualtests.com 67
Cisco 300-206 Exam



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

☑ Enable Botnet Updater Client

Dynamic Database Configuration

☑ Use Botnet data dynamically downloaded from updater server

Dynamic Database Management

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

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

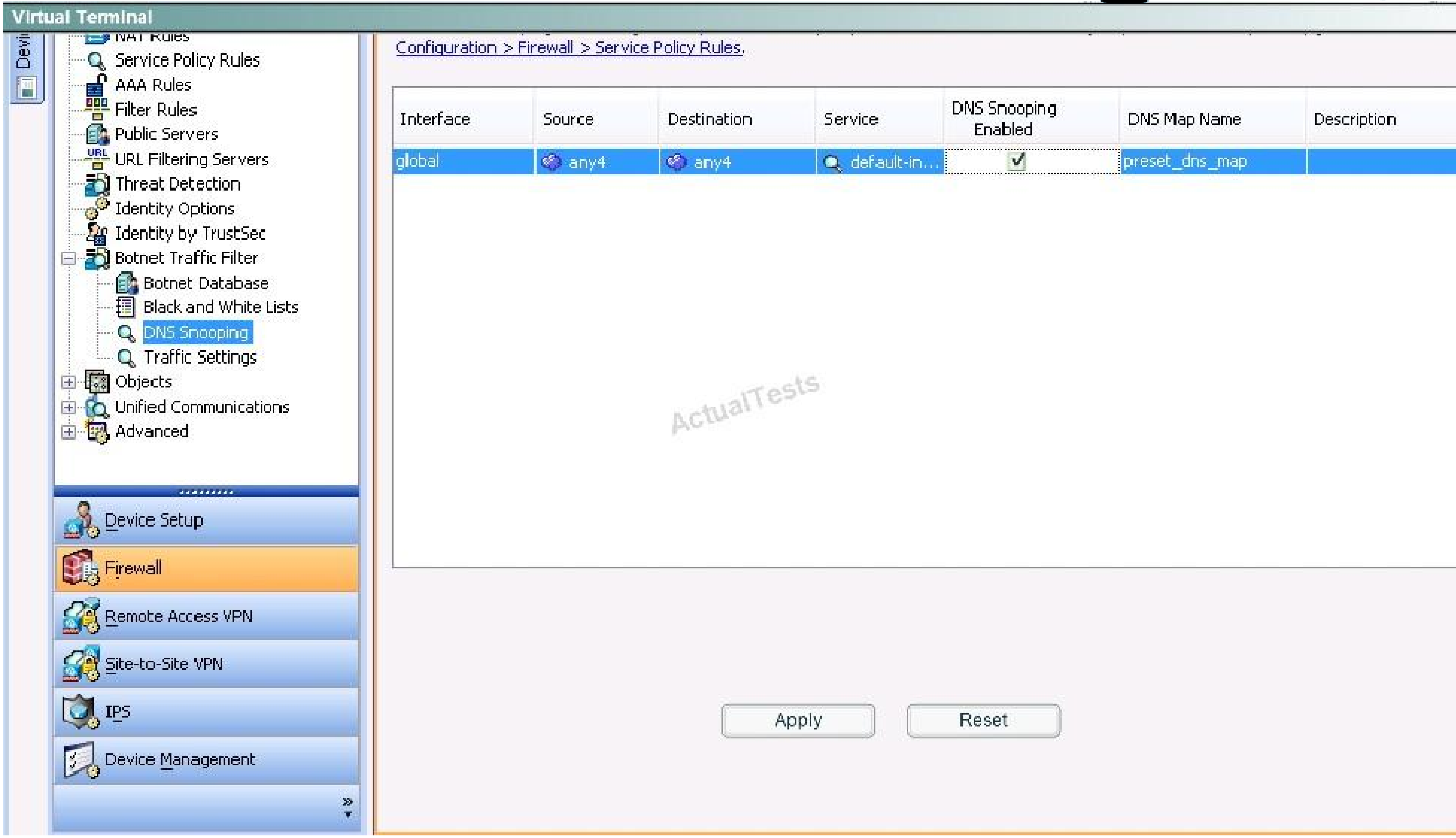
Search Dynamic Database

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

Search For:

Click Yes to send the commands when prompted.

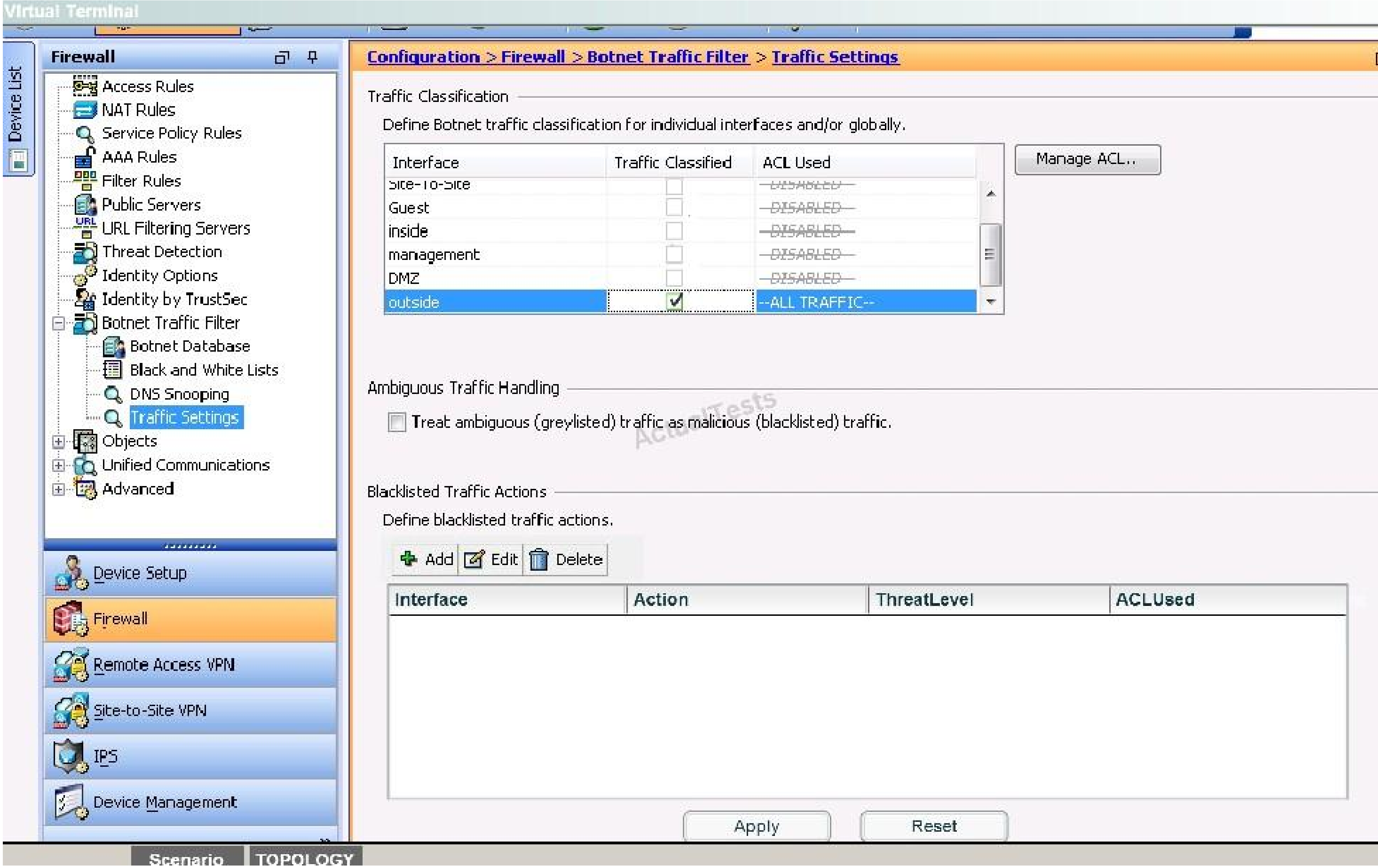
Then, click on the box on the DNS Snooping page as shown below and hit apply:



Configuration > Firewall > Service Policy Rules.

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

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



Configuration > Firewall > Botnet Traffic Filter > Traffic Settings

Traffic Classification

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

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

Ambiguous Traffic Handling

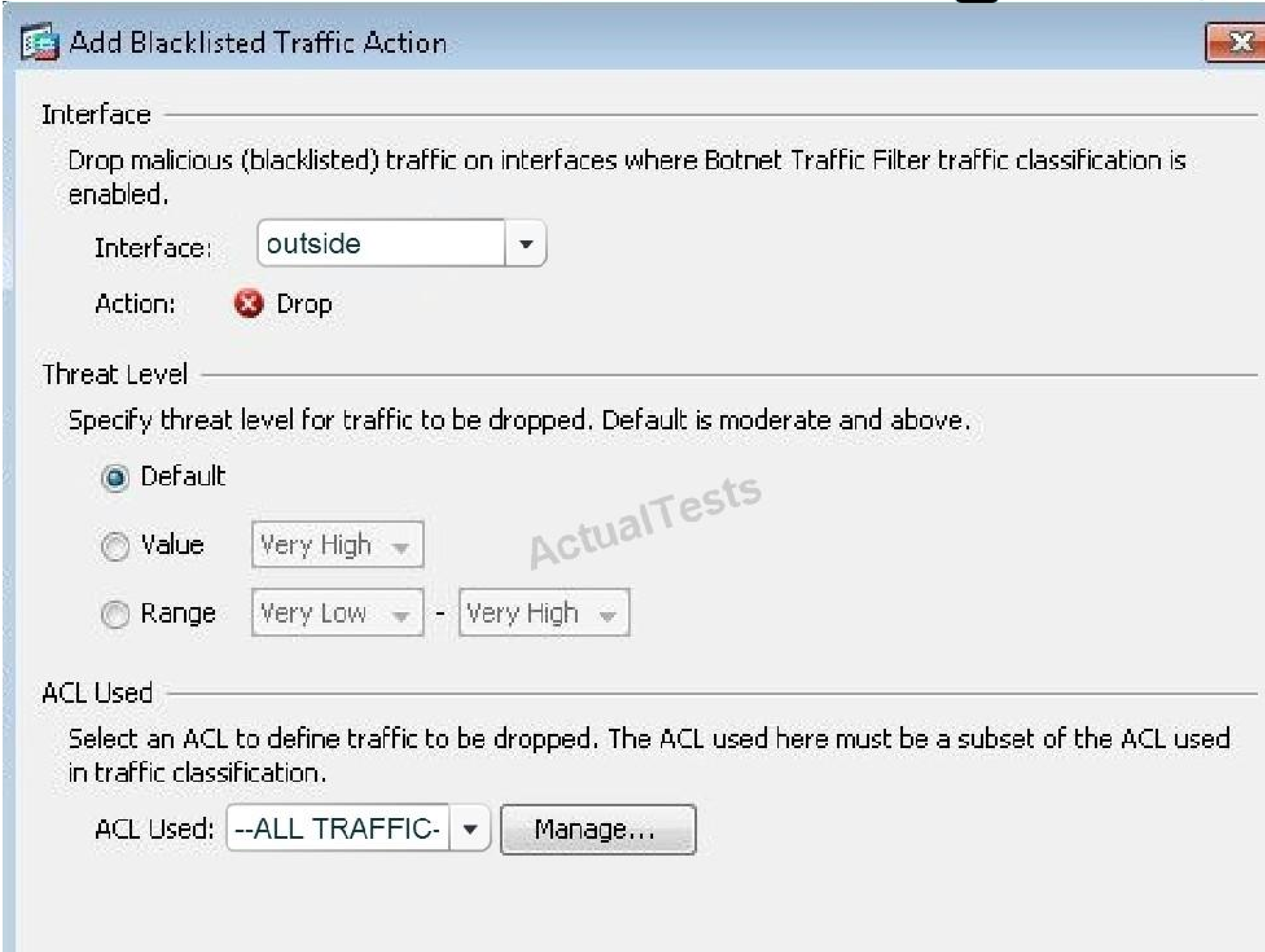
☐ Treat ambiguous (greylisted) traffic as malicious (blacklisted) traffic.

Blacklisted Traffic Actions

Define blacklisted traffic actions.

Interface	Action	ThreatLevel	ACLUsed

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



Add Blacklisted Traffic Action

Interface

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

Interface: outside

Action: Drop

Threat Level

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

● Default

○ Value Very High

○ Range Very Low - Very High

ACL Used

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

ACL Used: --ALL TRAFFIC-

Click OK. Then Apply. Then Send when prompted.

Then verify that all is working according to the instructions given in the question.

QUESTION 126
CORRECT TEXT

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 ASA. You must configure the Cisco ASA such that the source IP addresses of all internal hosts are translated to a single IP address (using different ports) when the internal hosts access the Internet.

To successfully complete this activity, you must perform the following tasks:

· Use the Cisco ASDM GUI on the Admin PC to configure dynamic network object NAT with PAT using the following parameters:

· Network object name: Internal-Networks

· IP subnet: 10.10.0.0/16

· Translated IP address: 192.0.2.100

· Source interface: inside

· Destination interface: outside

NOTE: The object (TRANSLATED-INSIDE-HOSTS) for this translated IP address has already been created for your use in this activity.

NOTE: Not all ASDM screens are active for this exercise.

NOTE: Login credentials are not needed for this simulation.

· In the Cisco ASDM, display and view the auto-generated NAT rule.

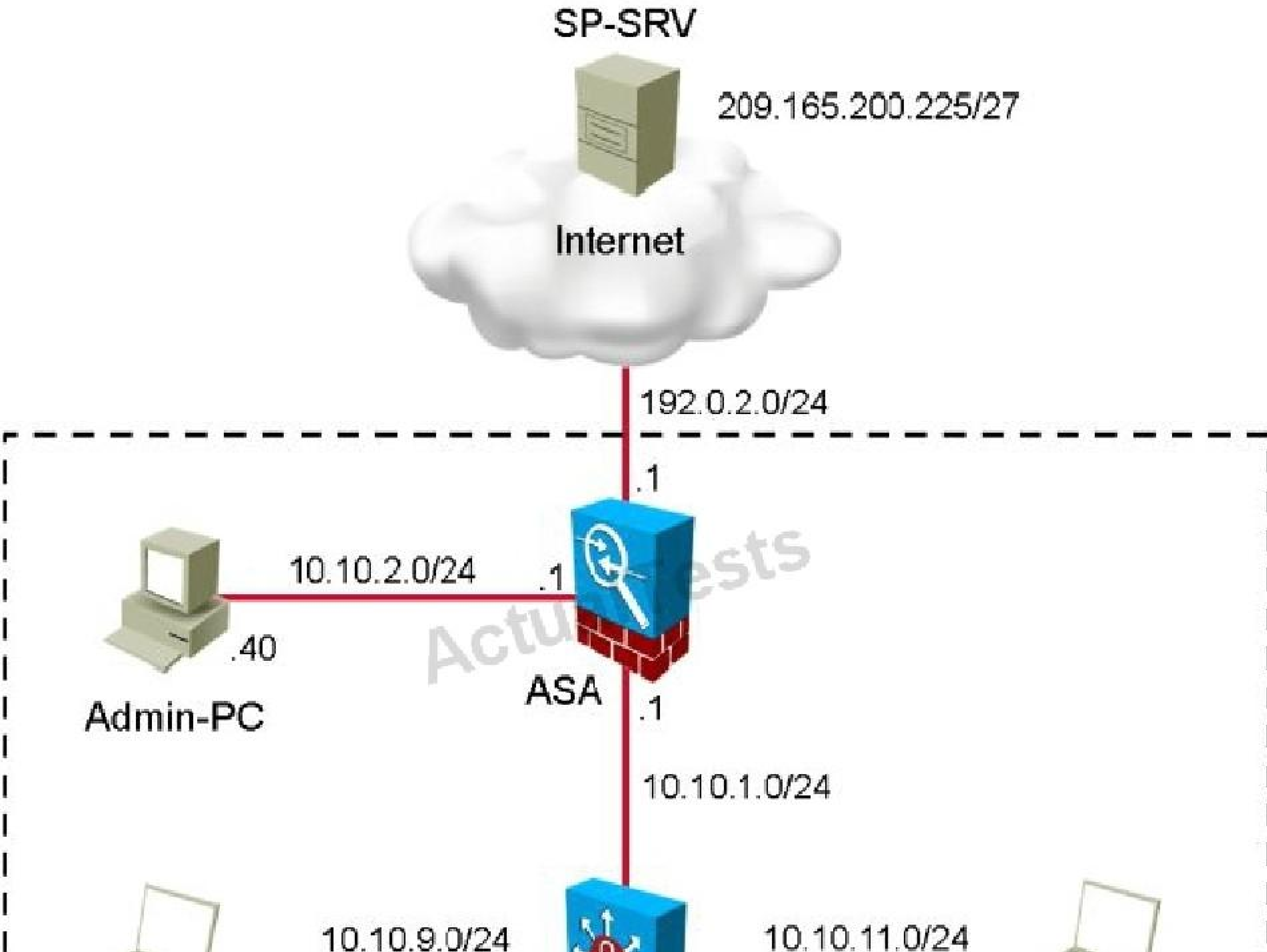
· From the Employee PC, generate traffic to SP-SRV by opening a browser and navigating to http://sp-srv.sp.public.

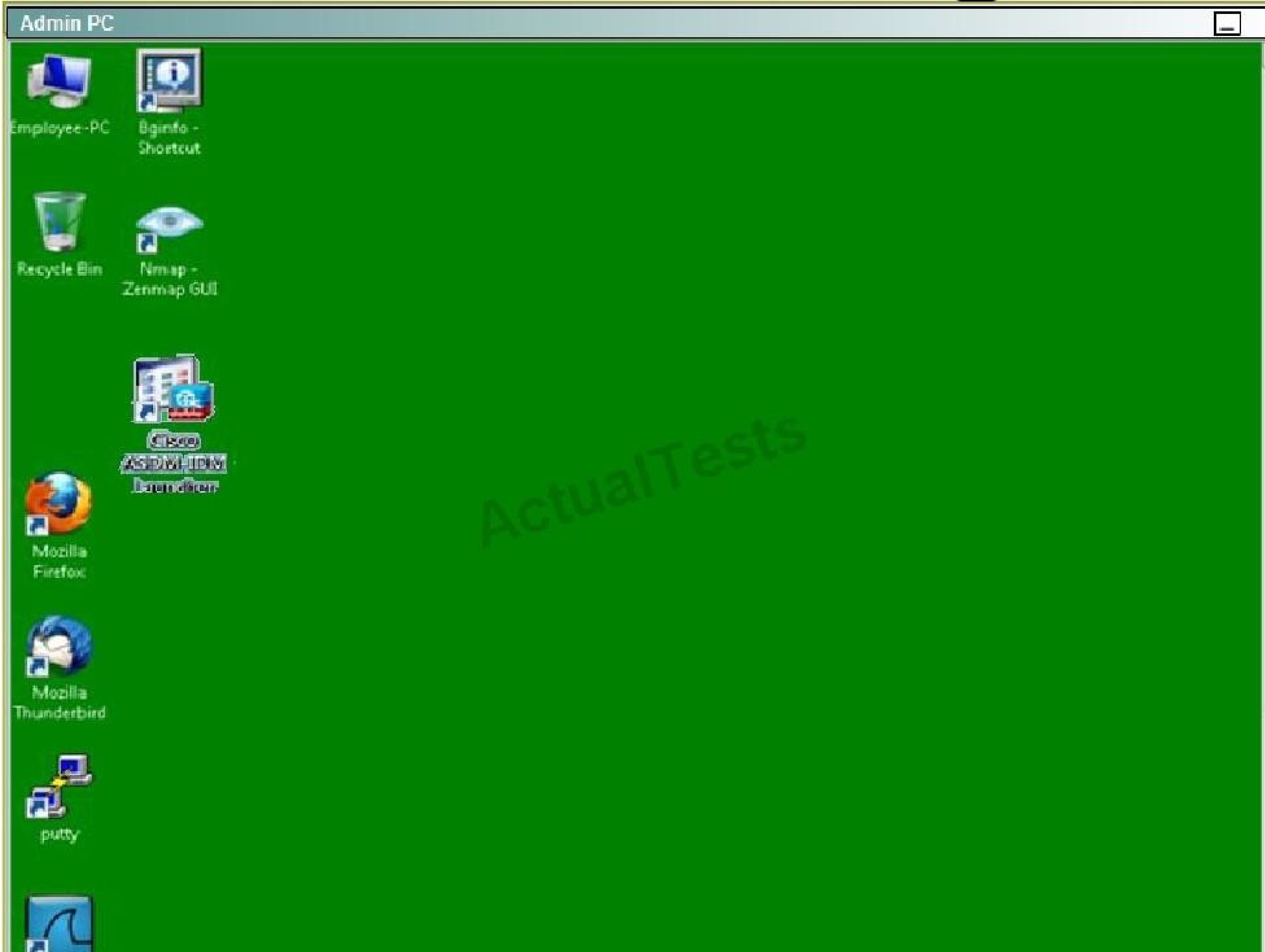
· From the Guest PC, generate traffic to SP-SRV by opening a browser and navigating to http://sp-srv.sp.public.

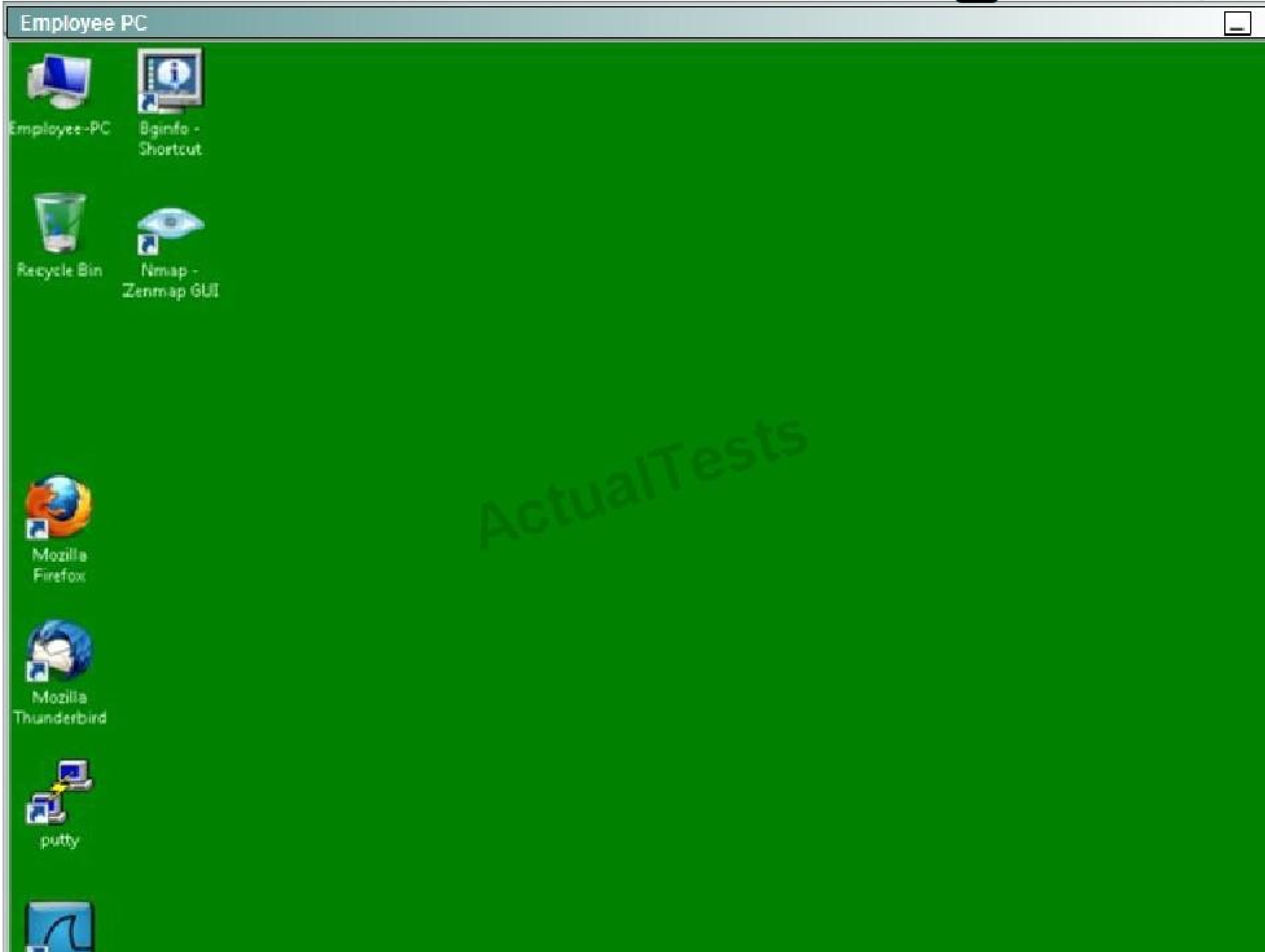
· At the CLI of the Cisco ASA, display your NAT configuration. You should see the configured policy and statistics for translated packets.

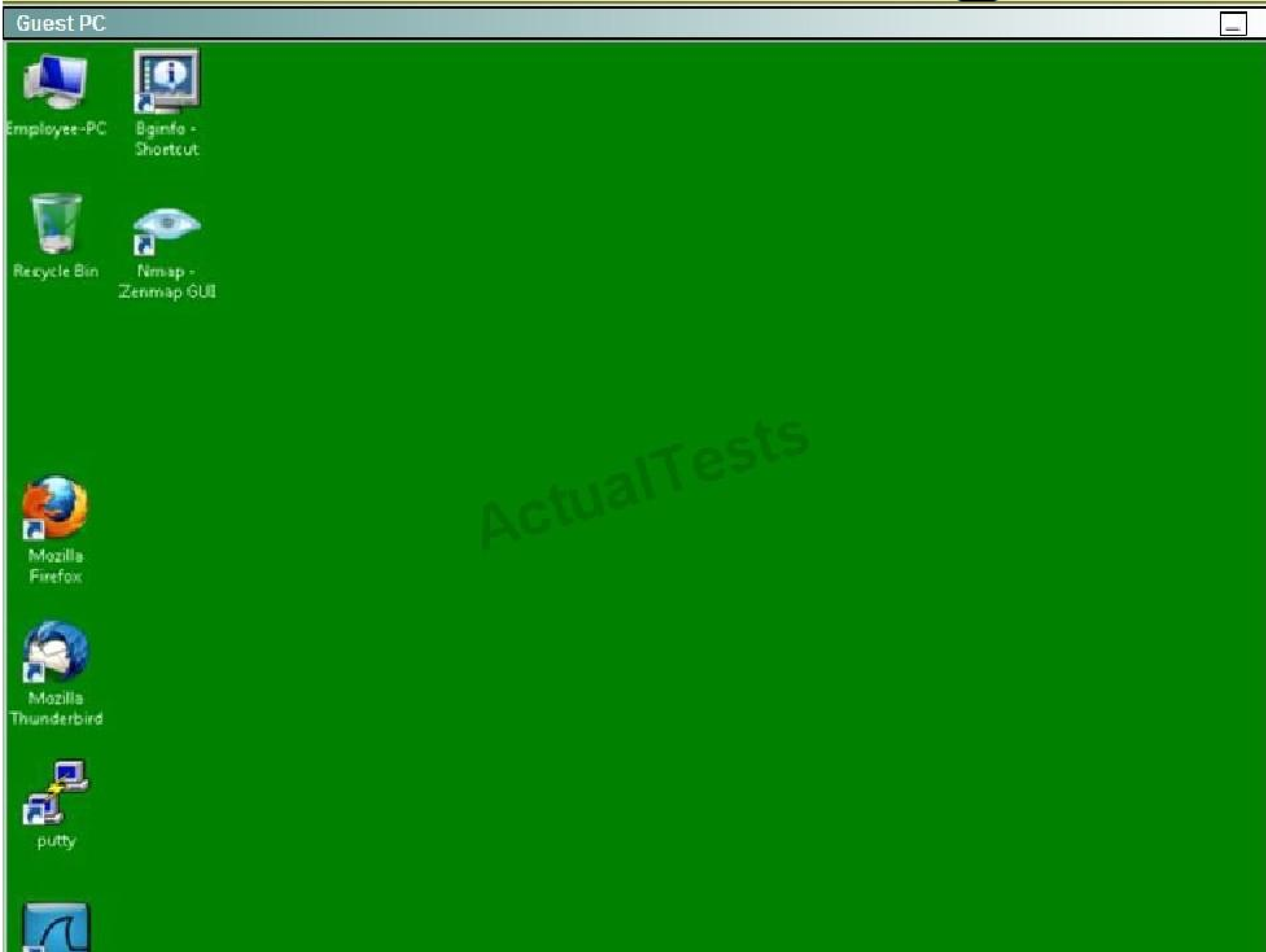
· At the CLI of the Cisco ASA, display the translation table. You should see dynamic translations for the Employee PC and the Guest PC. Both inside IP addresses translate to the same IP address, but using different ports.

You have completed this exercise when you have configured and successfully tested dynamic network object NAT with PAT.


SP-SRV
209.165.200.225/27
Internet
192.0.2.0/24
.1
10.10.2.0/24
.1
.40
Admin-PC
ASA
.1
10.10.1.0/24
10.10.9.0/24
10.10.11.0/24


Admin PC
Employee-PC
Bginfo - Shortcut
Recycle Bin
Nmap - Zenmap GUI
Cisco ASDM-IDM Launcher
Mozilla Firefox
Mozilla Thunderbird
putty

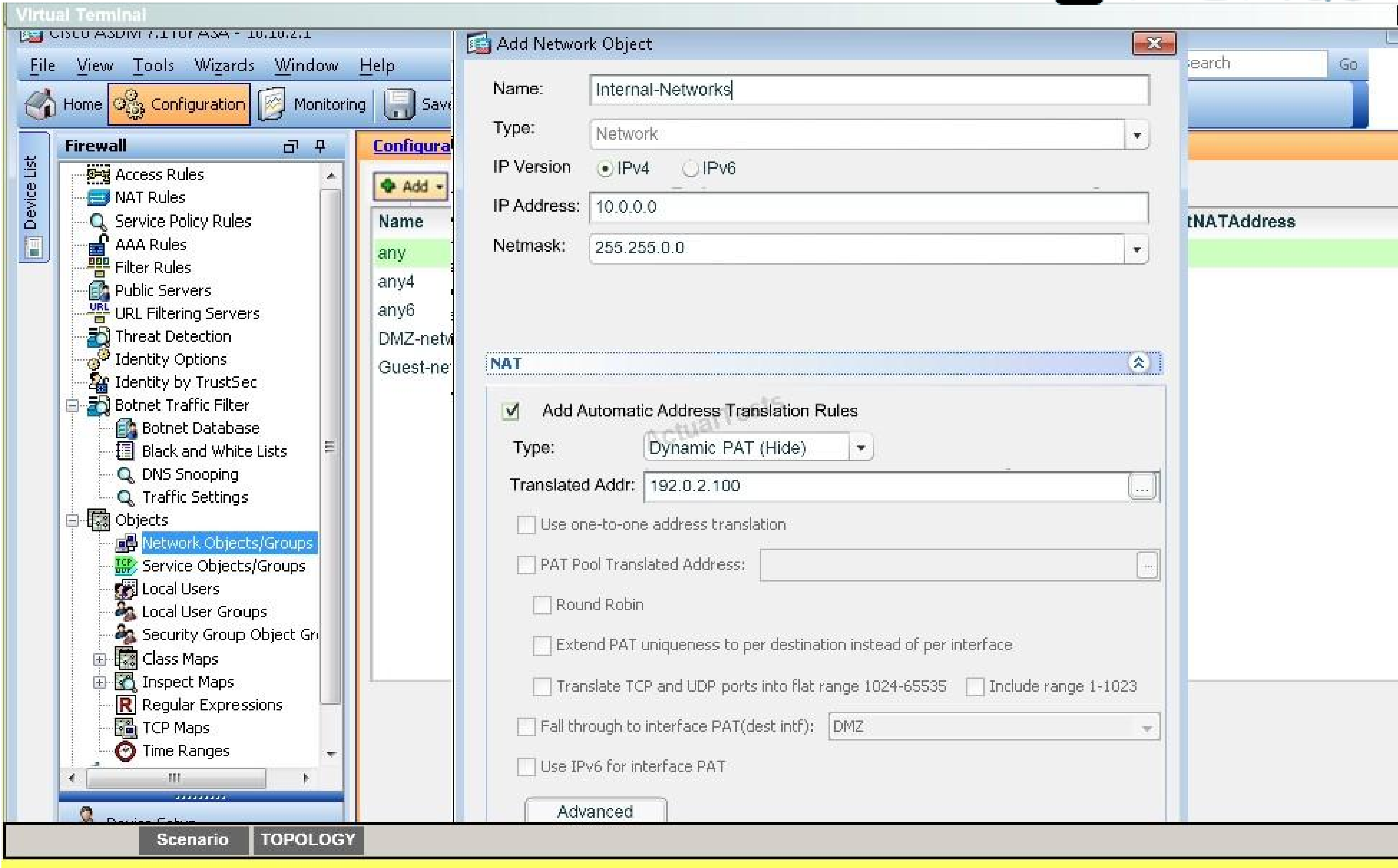

Employee PC
_
Employee-PC
Bginfo - Shortcut
Recycle Bin
Nmap - Zenmap GUI
Mozilla Firefox
Mozilla Thunderbird
putty


Guest PC
Employee-PC
Bginfo - Shortcut
Recycle Bin
Nmap - Zenmap GUI
Mozilla Firefox
Mozilla Thunderbird
putty

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: See the explanation for detailed answer to this sim question.
Explanation:
First, click on Add Network Objects on the Network Objects/Groups tab and fill in the information as shown below:



Add Network Object

Name: Internal-Networks

Type: Network

IP Version ● IPv4 ○ IPv6

IP Address: 10.0.0.0

Netmask: 255.255.0.0

NAT

☑ Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: 192.0.2.100

□ Use one-to-one address translation

□ PAT Pool Translated Address:

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

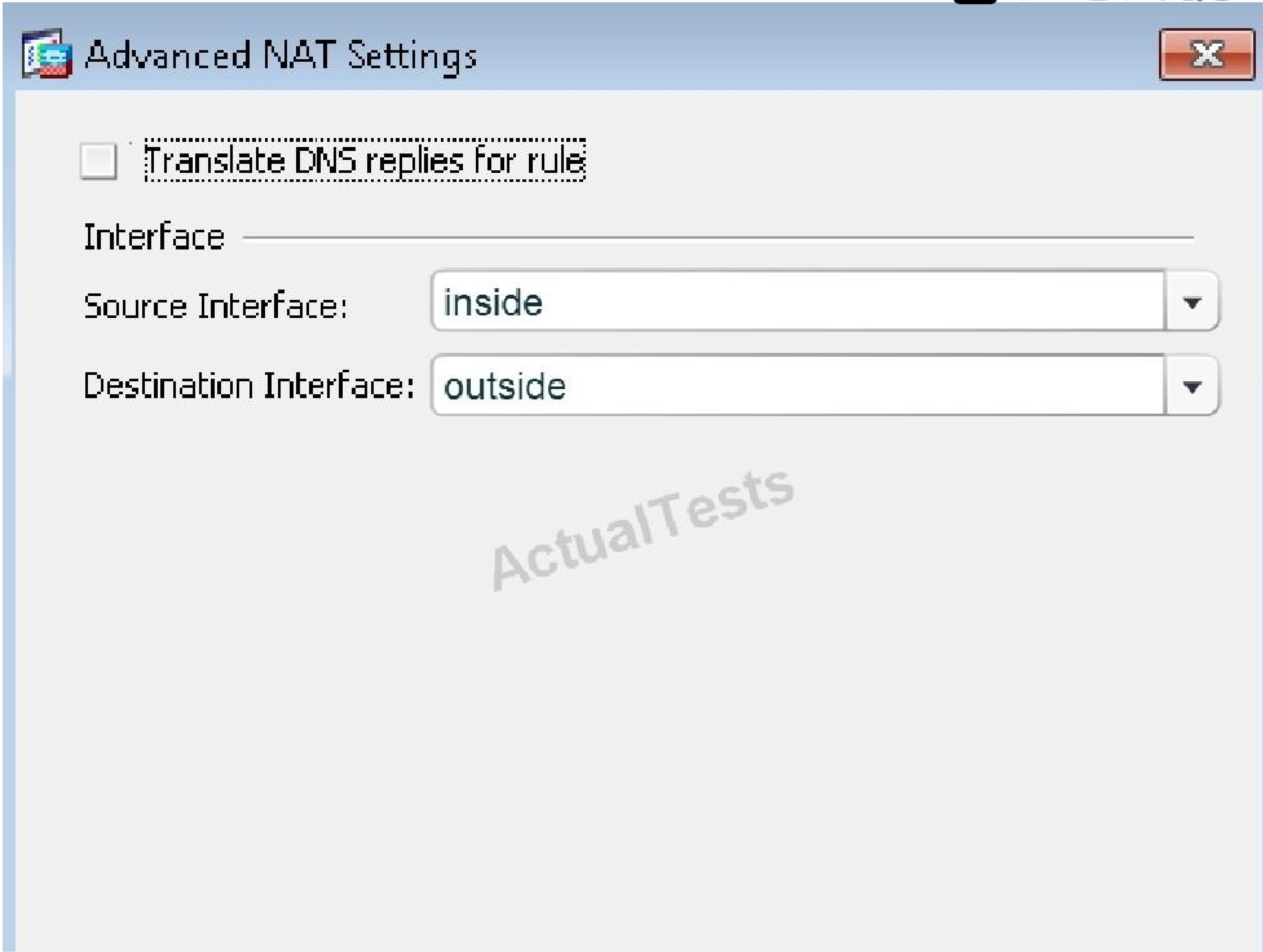
□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

□ Fall through to interface PAT(dest intf): DMZ

□ Use IPv6 for interface PAT

Advanced

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



Advanced NAT Settings

☐ Translate DNS replies for rule

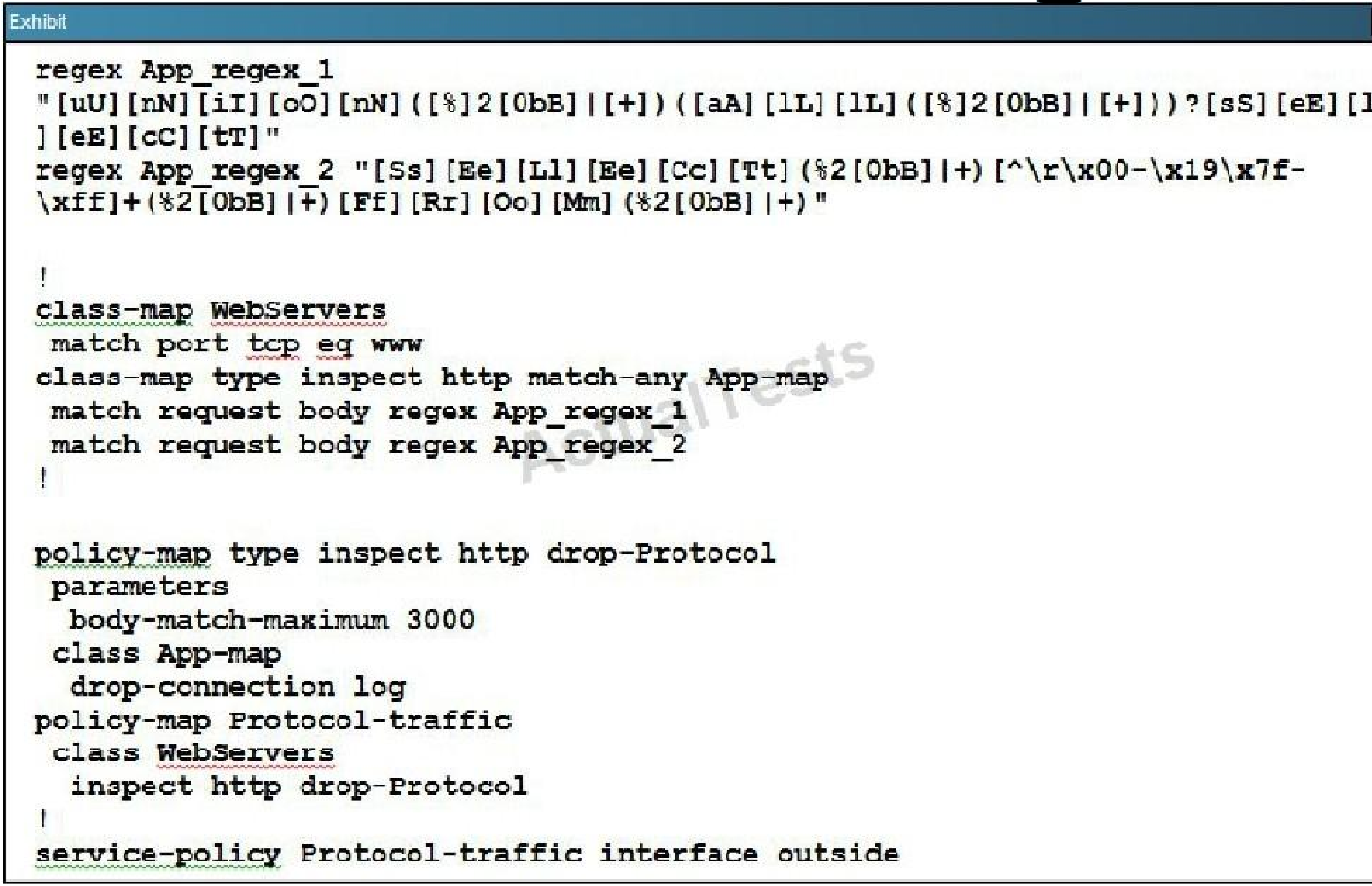
Interface

Source Interface: inside

Destination Interface: outside

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

QUESTION 127
"Pass Any Exam. Any Time." - www.actualtests.com 74
Cisco 300-206 Exam



Exhibit

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

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

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

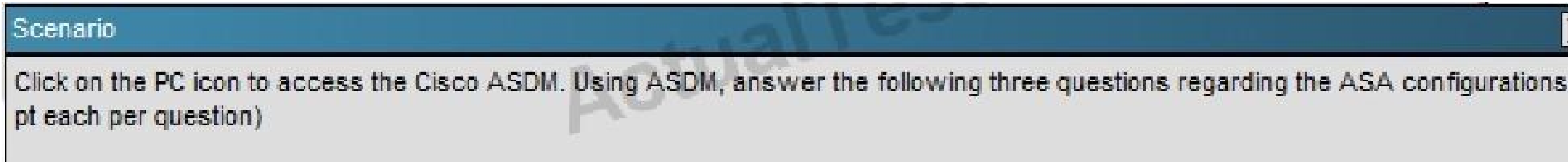
Refer to the exhibit. What type of attack is being mitigated on the Cisco ASA appliance?

A. HTTP and POST flood attack
B. HTTP Compromised-Key Attack
C. HTTP Shockwave Flash exploit
D. HTTP SQL injection attack

Correct Answer: D
Section: (none)
Explanation

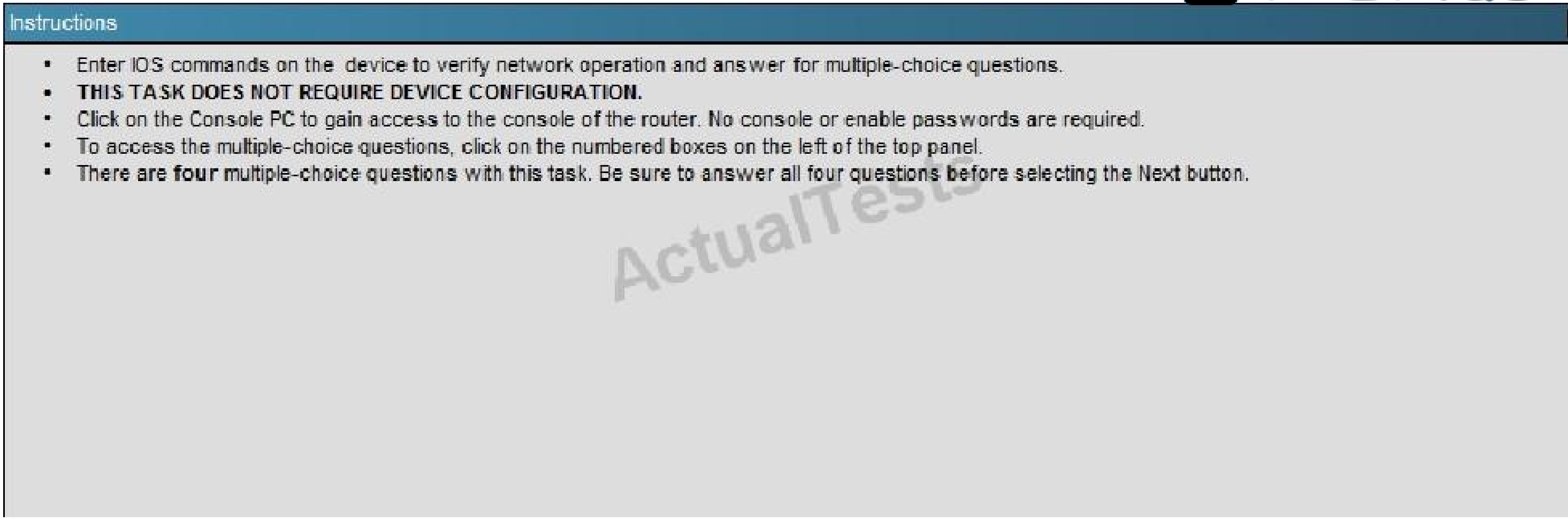
Explanation/Reference:
Explanation:

QUESTION 128



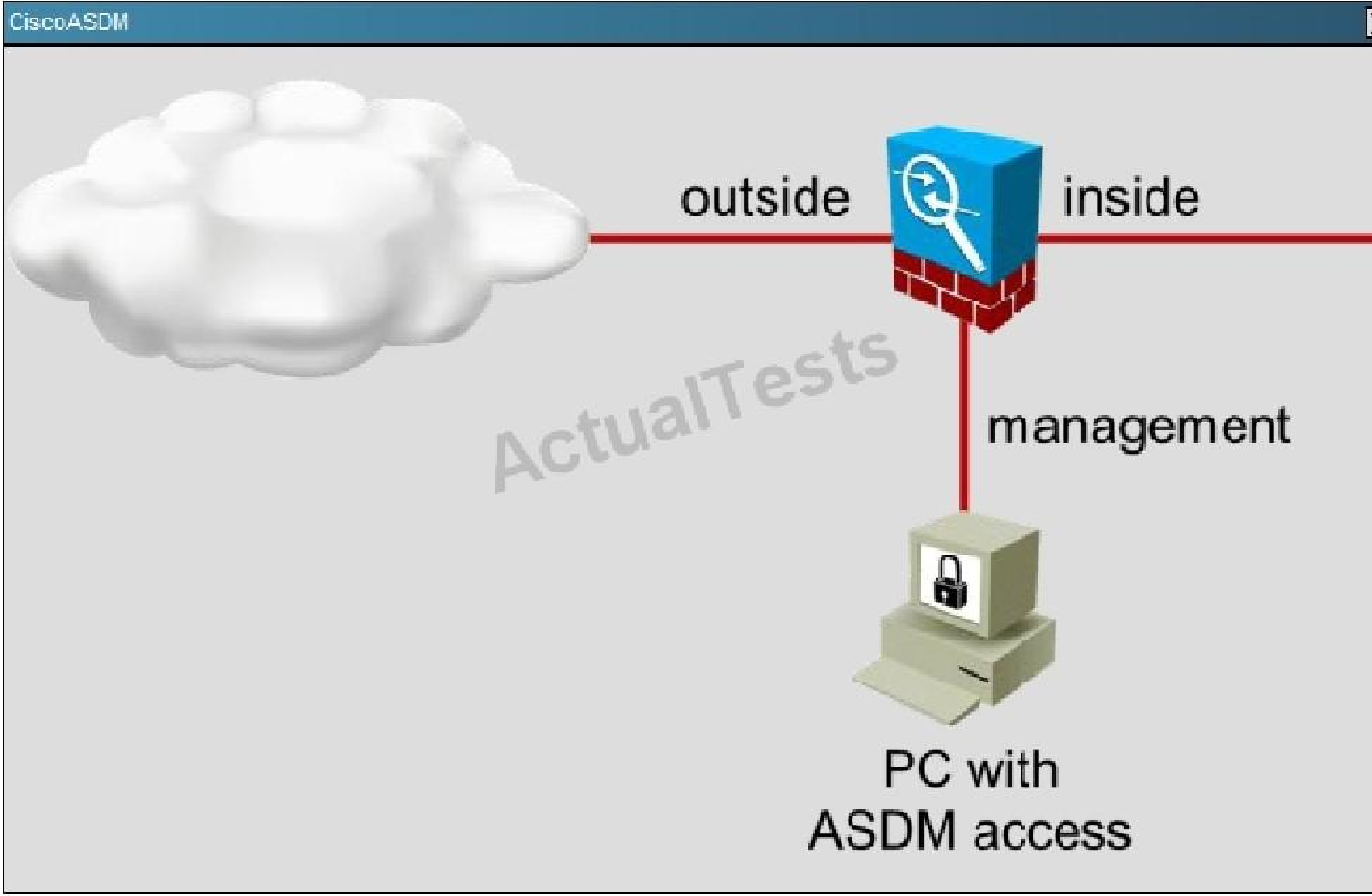
Scenario

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



Instructions

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


CiscoASDM
outside
inside
management
PC with
ASDM access

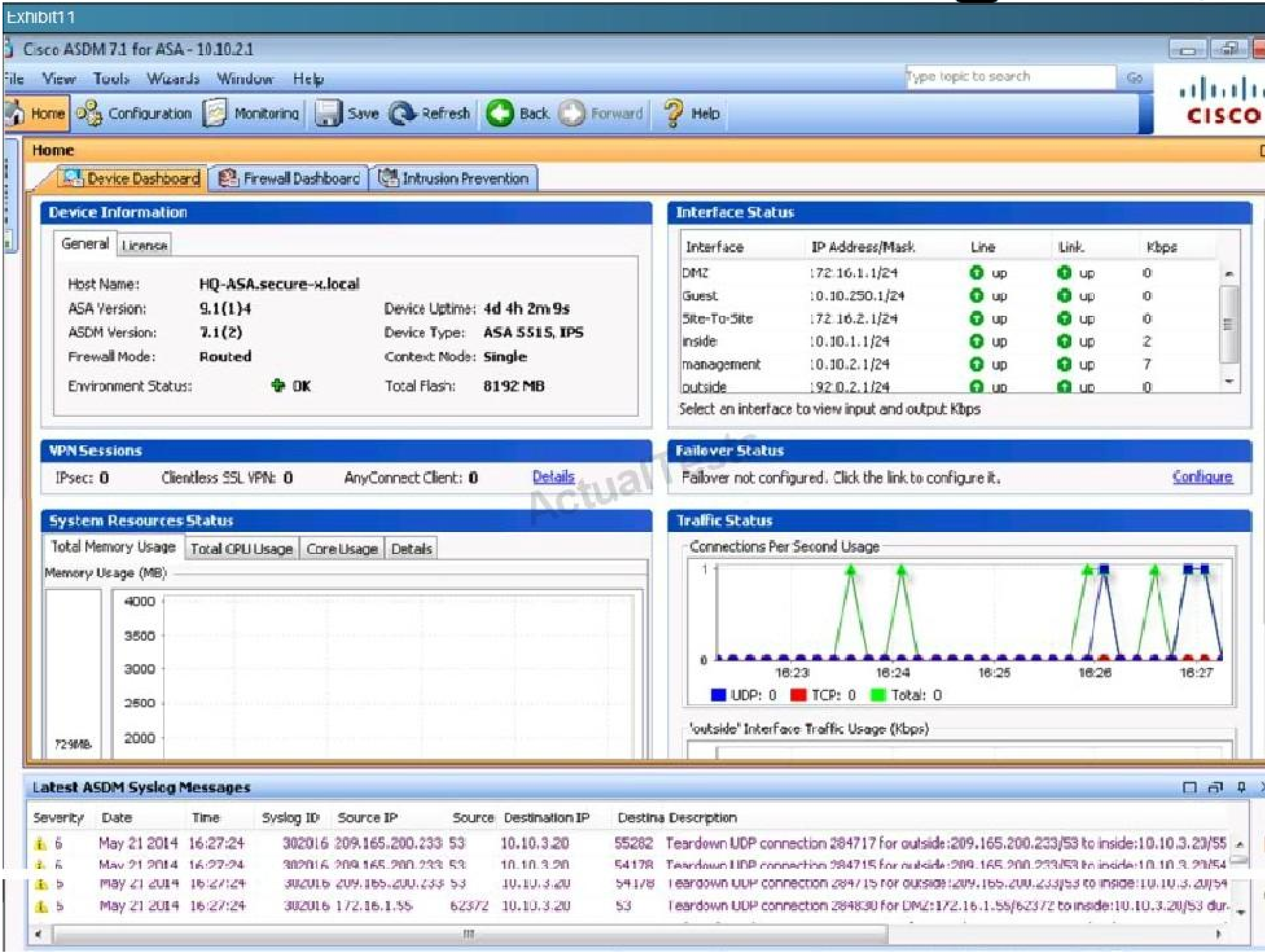


Exhibit11

Cisco ASDM 7.1 for ASA - 10.10.2.1

File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device Dashboard Firewall Dashboard Intrusion Prevention

Device Information

General | License

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

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

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

Failover Status

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

System Resources Status

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

Traffic Status

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	55282	Teardown UDP connection 284717 for outside:209.165.200.233/53 to inside:10.10.3.23/55
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.23/54
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6	May 21 2014	16:27:24	302016	172.16.1.55	62372	10.10.3.20	53	Teardown UDP connection 284830 for DMZ:172.16.1.55/62372 to inside:10.10.3.20/53 dur.

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

A. Logging is not enabled globally on the Cisco ASA.

B. The syslog server has failed.

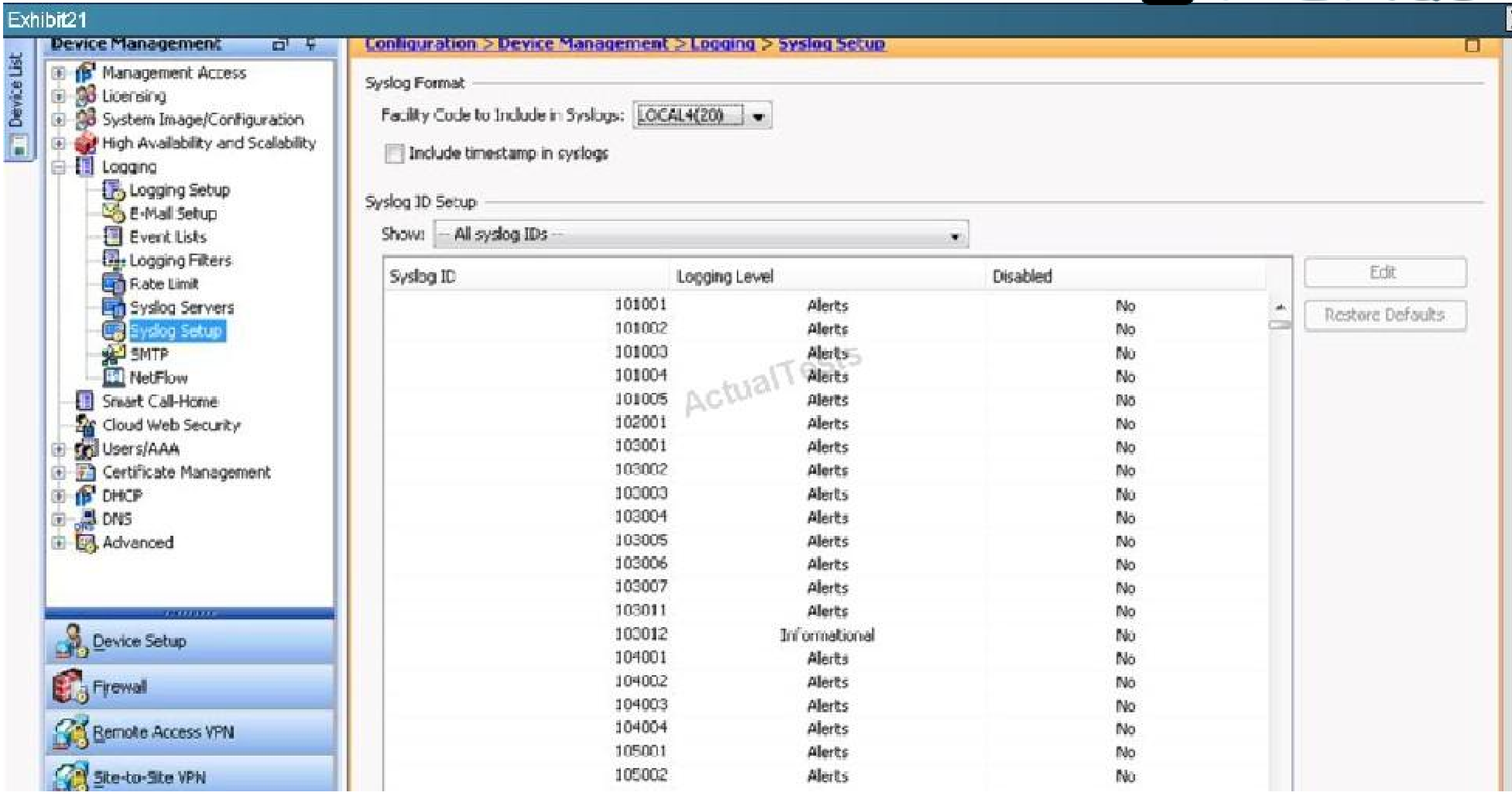
C. There have not been any events with a severity level of seven.
"Pass Any Exam. Any Time." - www.actualtests.com 76
Cisco 300-206 Exam

D. The Cisco ASA is not configured to log messages to the syslog server at that IP address.

Correct Answer: B
Section: (none)
Explanation

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

Exhibit21



Configuration > Device Management > Logging > Syslog Setup

Syslog Format

Facility Code to Include in Syslogs: LOCAL4(20)

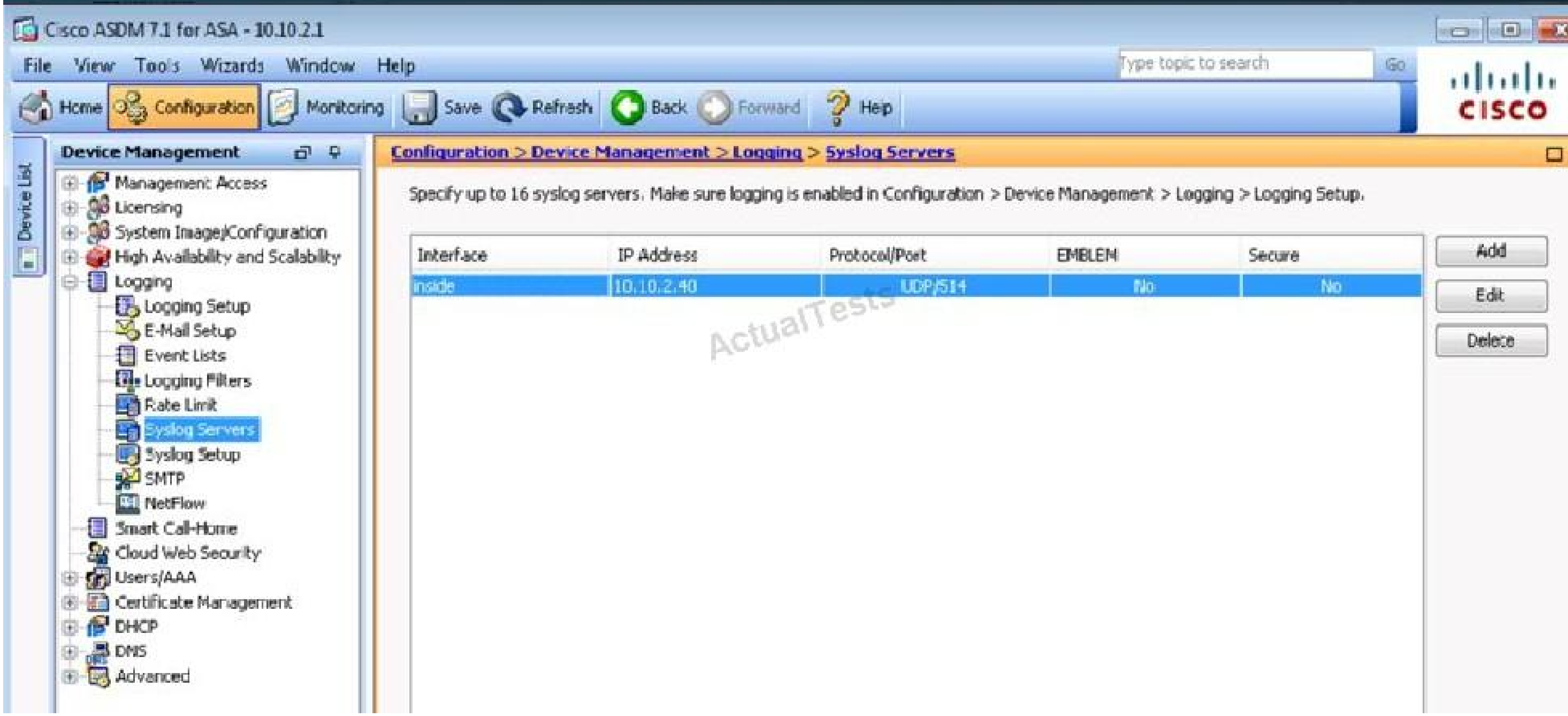
□ Include timestamp in syslogs

Syslog ID Setup

Show: -- All syslog IDs --

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

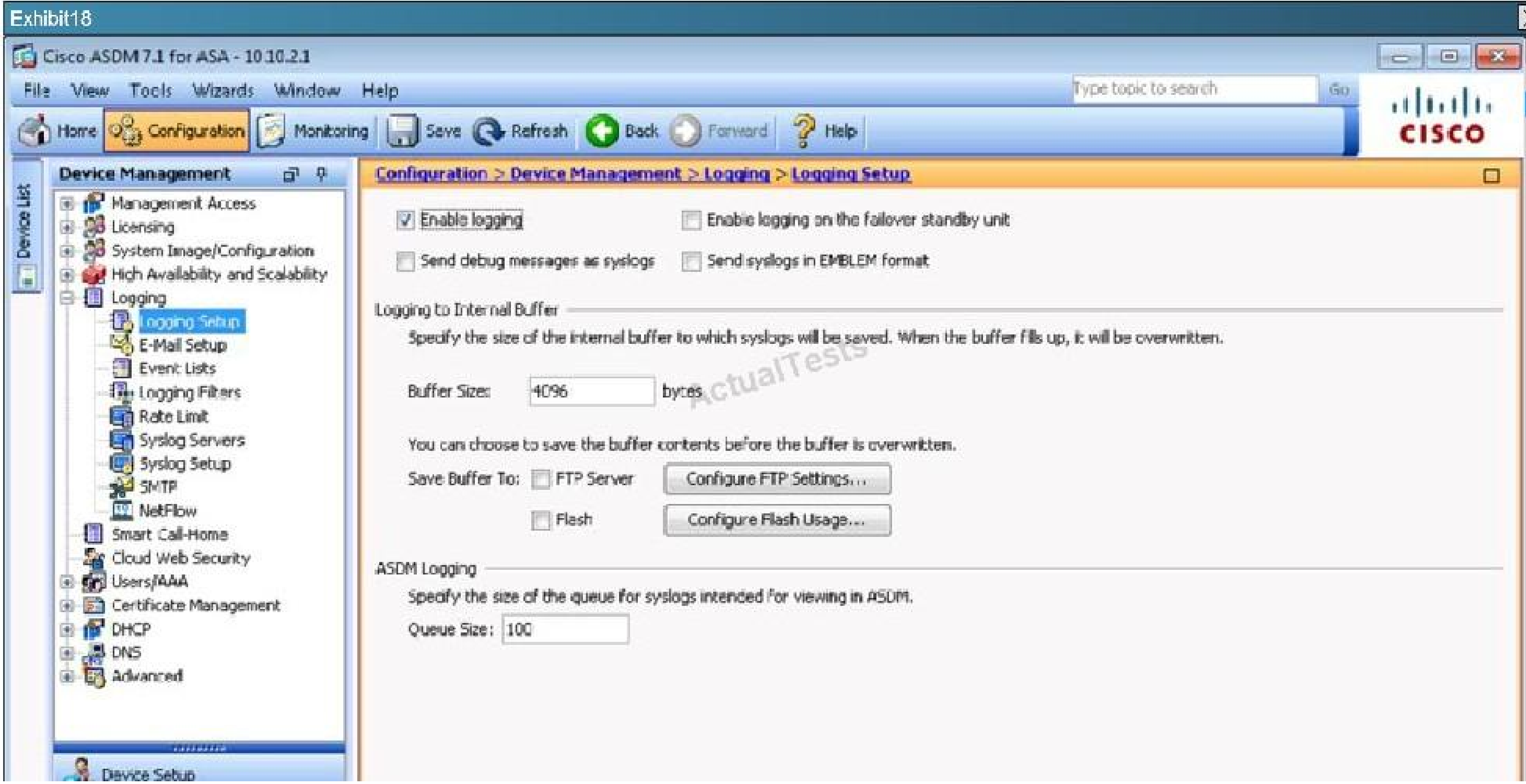
Exhibit20



Configuration > Device Management > Logging > Syslog Servers

Specify up to 16 syslog servers. Make sure logging is enabled in Configuration > Device Management > Logging > Logging Setup.

Interface	IP Address	Protocol/Port	EMBLEM	Secure
inside	10.10.2.40	UDP/514	No	No



Configuration > Device Management > Logging > Logging Setup

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

Logging to Internal Buffer

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

Buffer Size: 4096 bytes

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

Save Buffer To: ☐ FTP Server

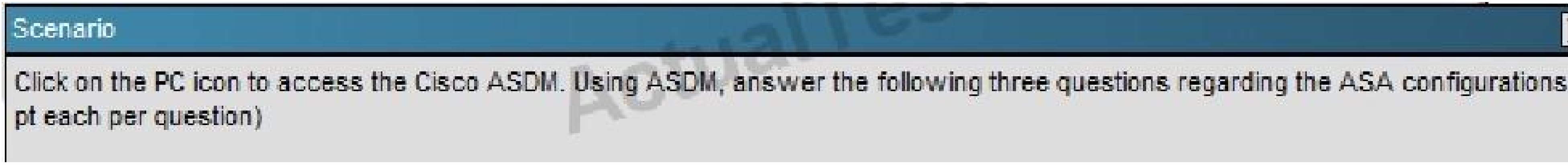
☐ Flash

ASDM Logging

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

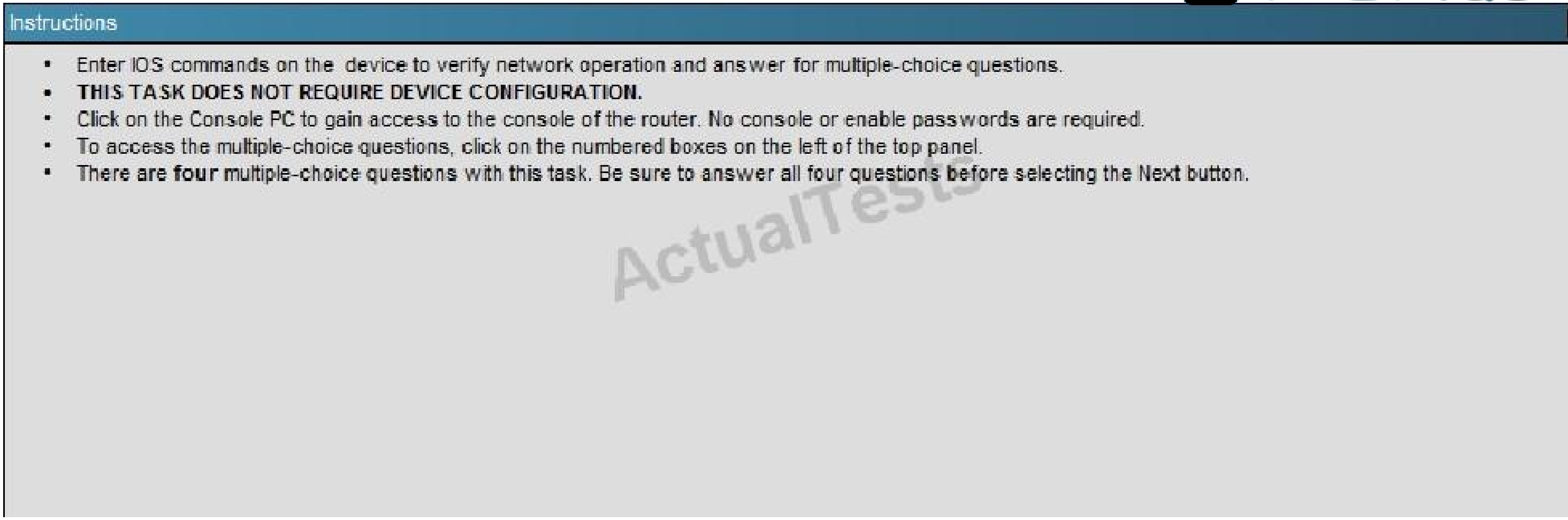
Queue Size: 100

QUESTION 129



Scenario

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



Instructions

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

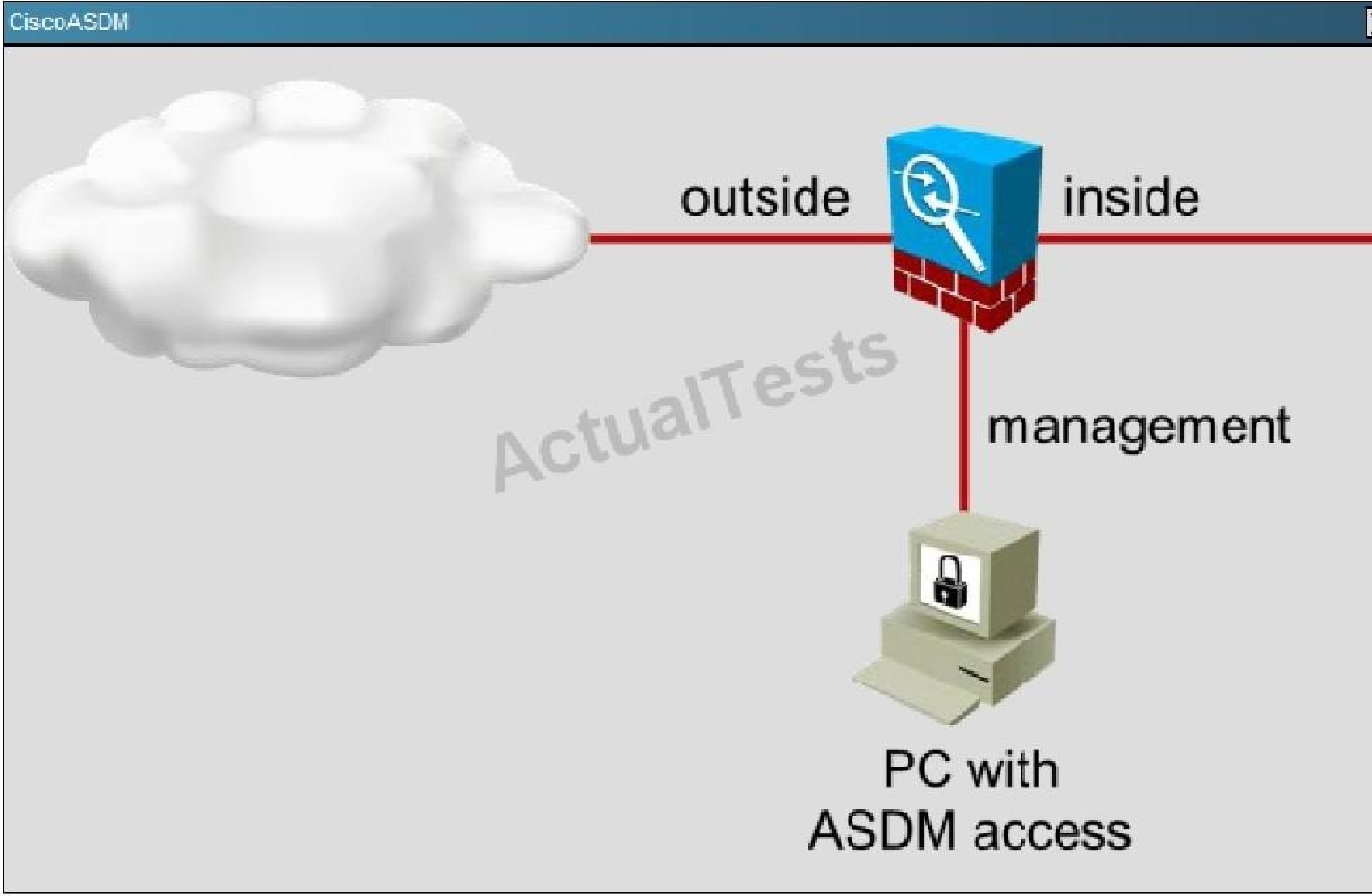
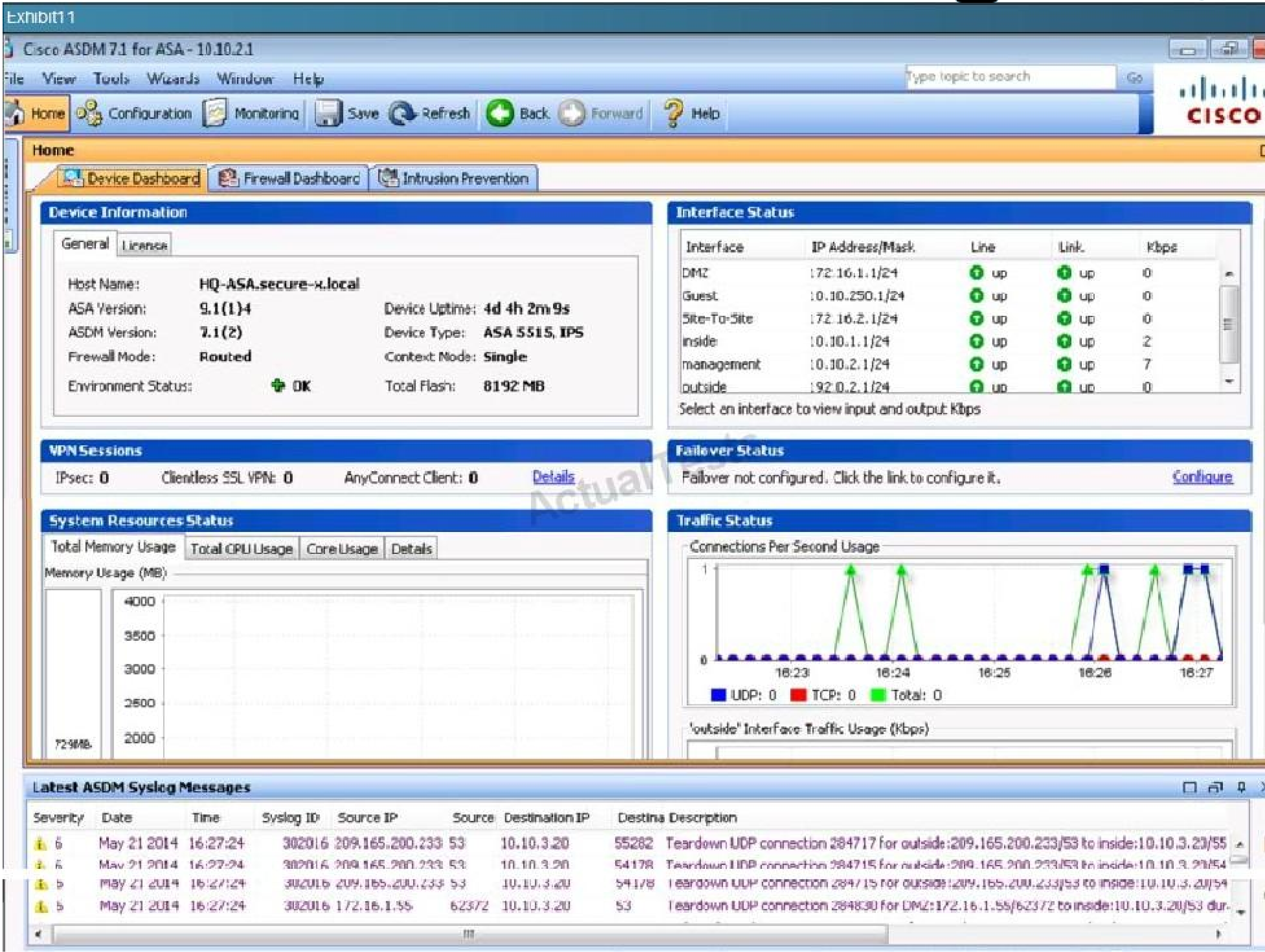

CiscoASDM
outside
inside
management
PC with
ASDM access

Exhibit11



Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
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

Traffic Status

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

Latest ASDM Syslog Messages

```
Severity  Date         Time      Syslog ID  Source IP        Source  Destination IP  Destina  Description
6         May 21 2014  16:27:24  302016     209.165.200.233  53      10.10.3.20      55282    Teardown UDP connection 284717 for outside:209.165.200.233/53 to inside:10.10.3.23/55
6         May 21 2014  16:27:24  302016     209.165.200.233  53      10.10.3.20      54178    Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.23/54
6         May 21 2014  16:27:24  302016     209.165.200.233  53      10.10.3.20      54178    Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6         May 21 2014  16:27:24  302016     172.16.1.55      62372   10.10.3.20      53       Teardown UDP connection 284830 for DMZ:172.16.1.55/62372 to inside:10.10.3.20/53 dur-
```

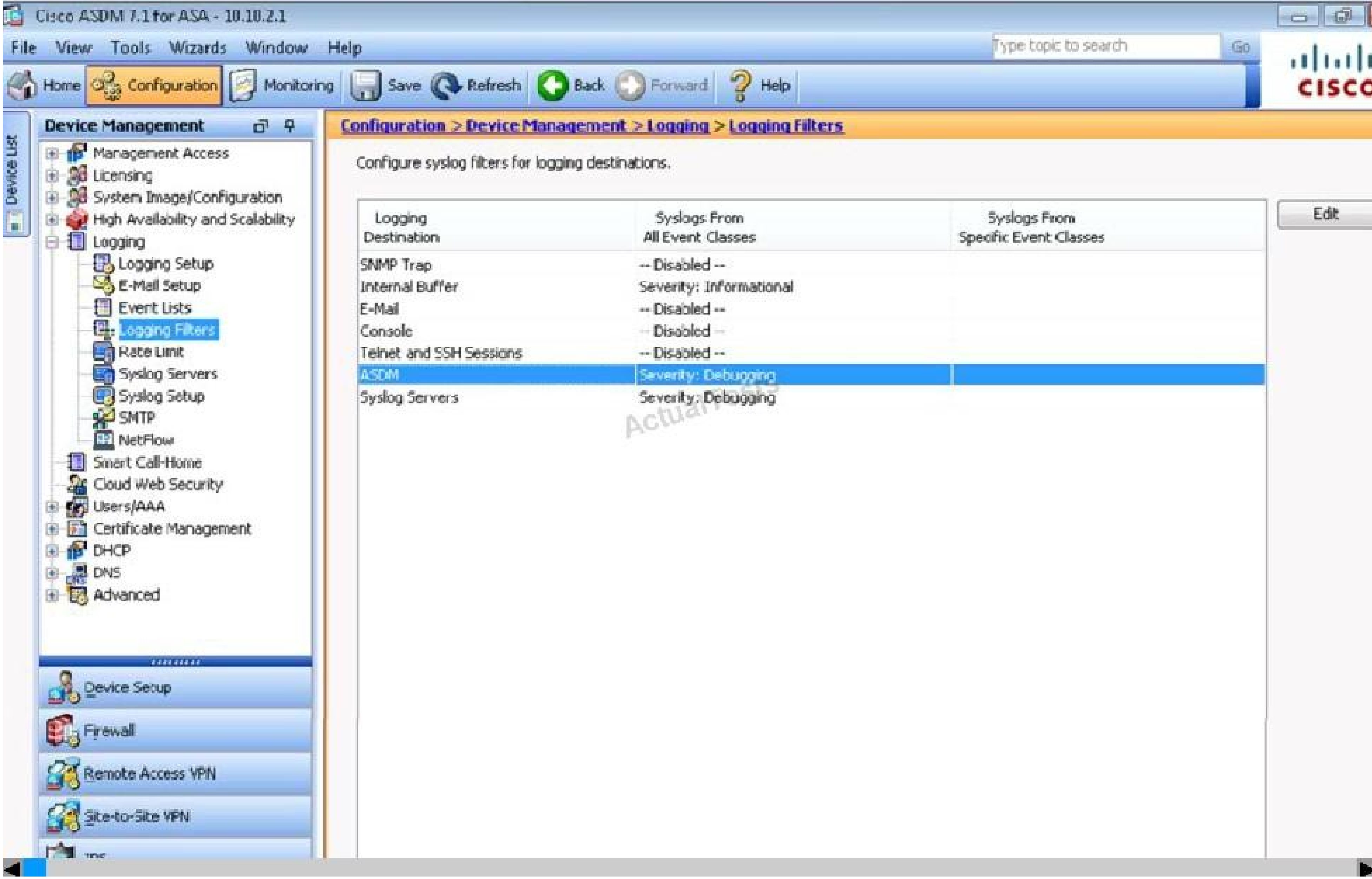
According to the logging configuration on the Cisco ASA, what will happen if syslog server 10.10.2.40 fails?

A. New connections through the ASA will be blocked and debug system logs will be sent to the internal buffer.
B. New connections through the ASA will be blocked and informational system logs will be sent to the internal buffer.
"Pass Any Exam. Any Time." - www.actualtests.com 79
Cisco 300-206 Exam
C. New connections through the ASA will be blocked and system logs will be sent to server 10.10.2.41.
D. New connections through the ASA will be allowed and system logs will be sent to server 10.10.2.41.
E. New connections through the ASA will be allowed and informational system logs will be sent to the internal buffer.
F. New connections through the ASA will be allowed and debug system logs will be sent to the internal buffer.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is shown by the following screen shot:

Exhibit19

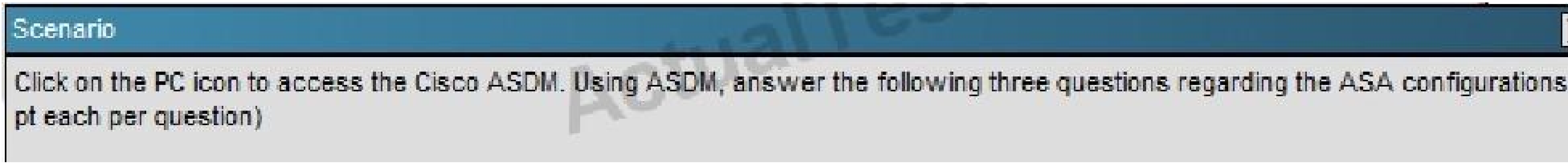


Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

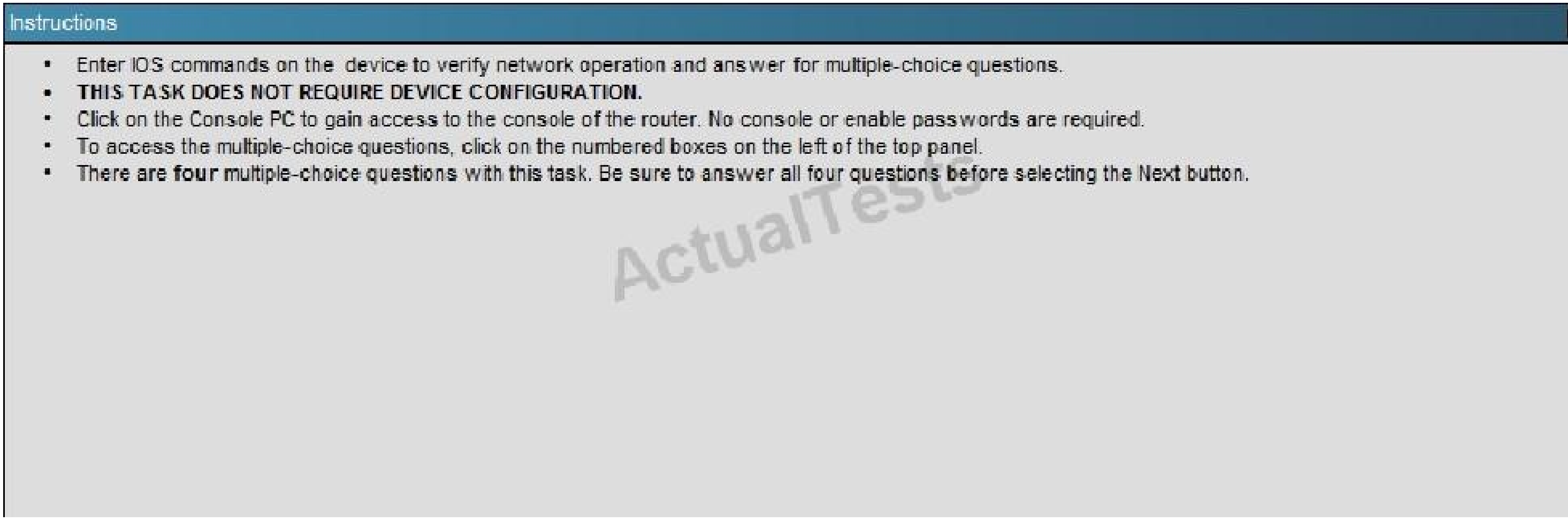
Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	Severity: Informational	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH Sessions	-- Disabled --	
ASDM	Severity: Debugging	
Syslog Servers	Severity: Debugging	

QUESTION 130



Scenario

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



Instructions

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

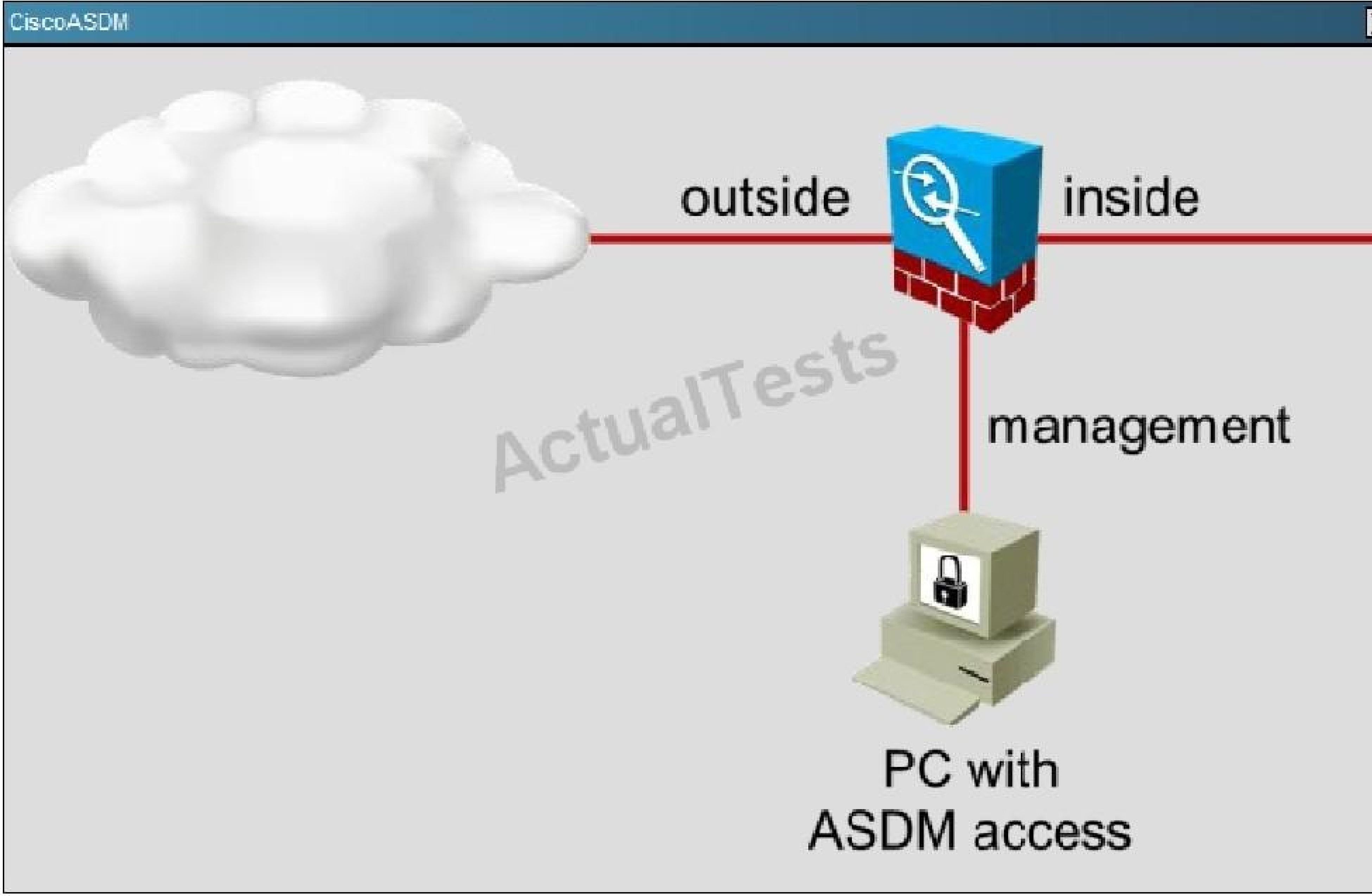
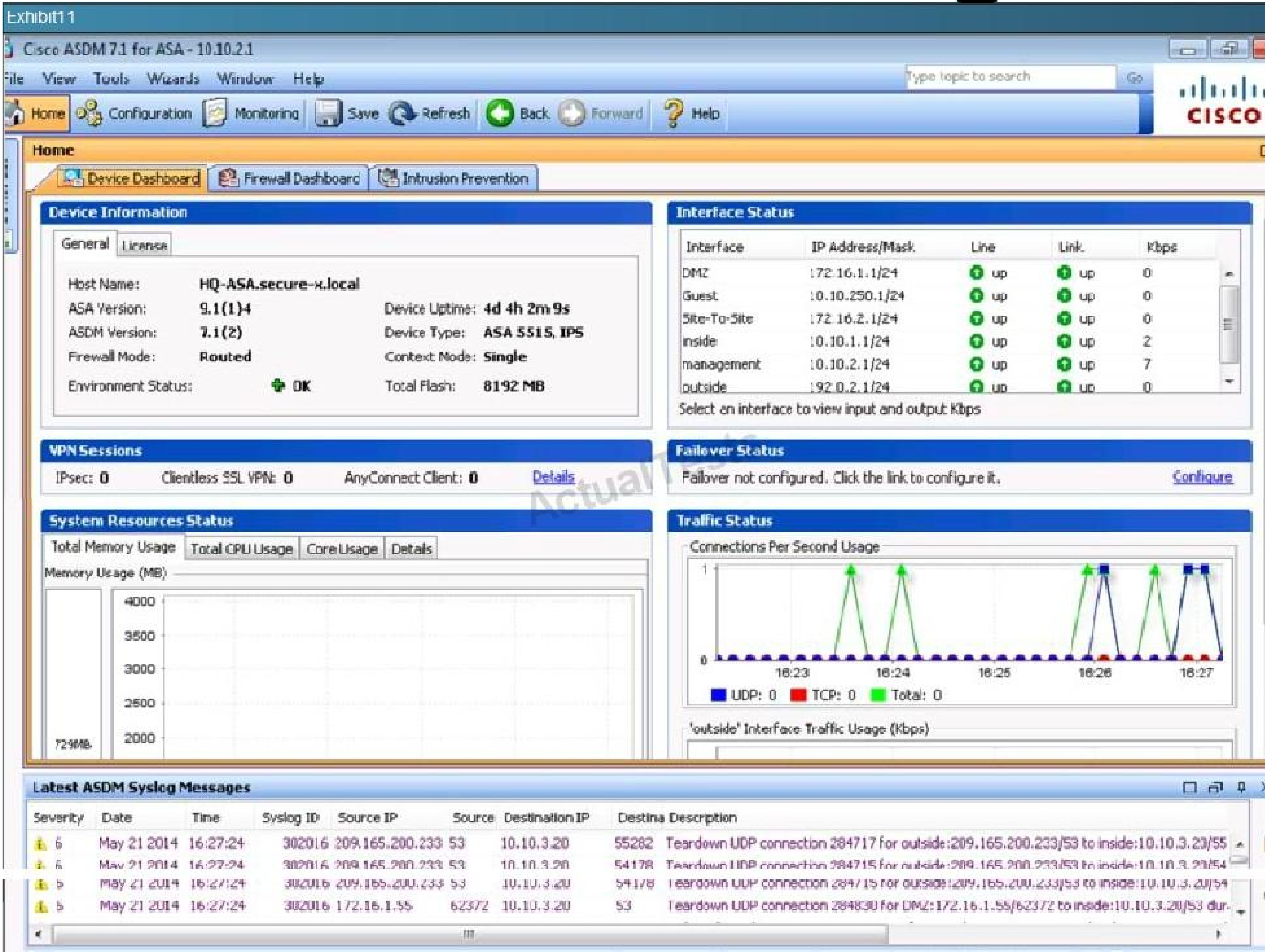

CiscoASDM
outside
inside
management
PC with
ASDM access

Exhibit11



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

Traffic Status

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

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	55282	Teardown UDP connection 284717 for outside:209.165.200.233/53 to inside:10.10.3.23/55
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.23/54
6	May 21 2014	16:27:24	302016	209.165.200.233	53	10.10.3.20	54178	Teardown UDP connection 284715 for outside:209.165.200.233/53 to inside:10.10.3.20/54
6	May 21 2014	16:27:24	302016	172.16.1.55	62372	10.10.3.20	53	Teardown UDP connection 284830 for DMZ:172.16.1.55/62372 to inside:10.10.3.20/53 dur...

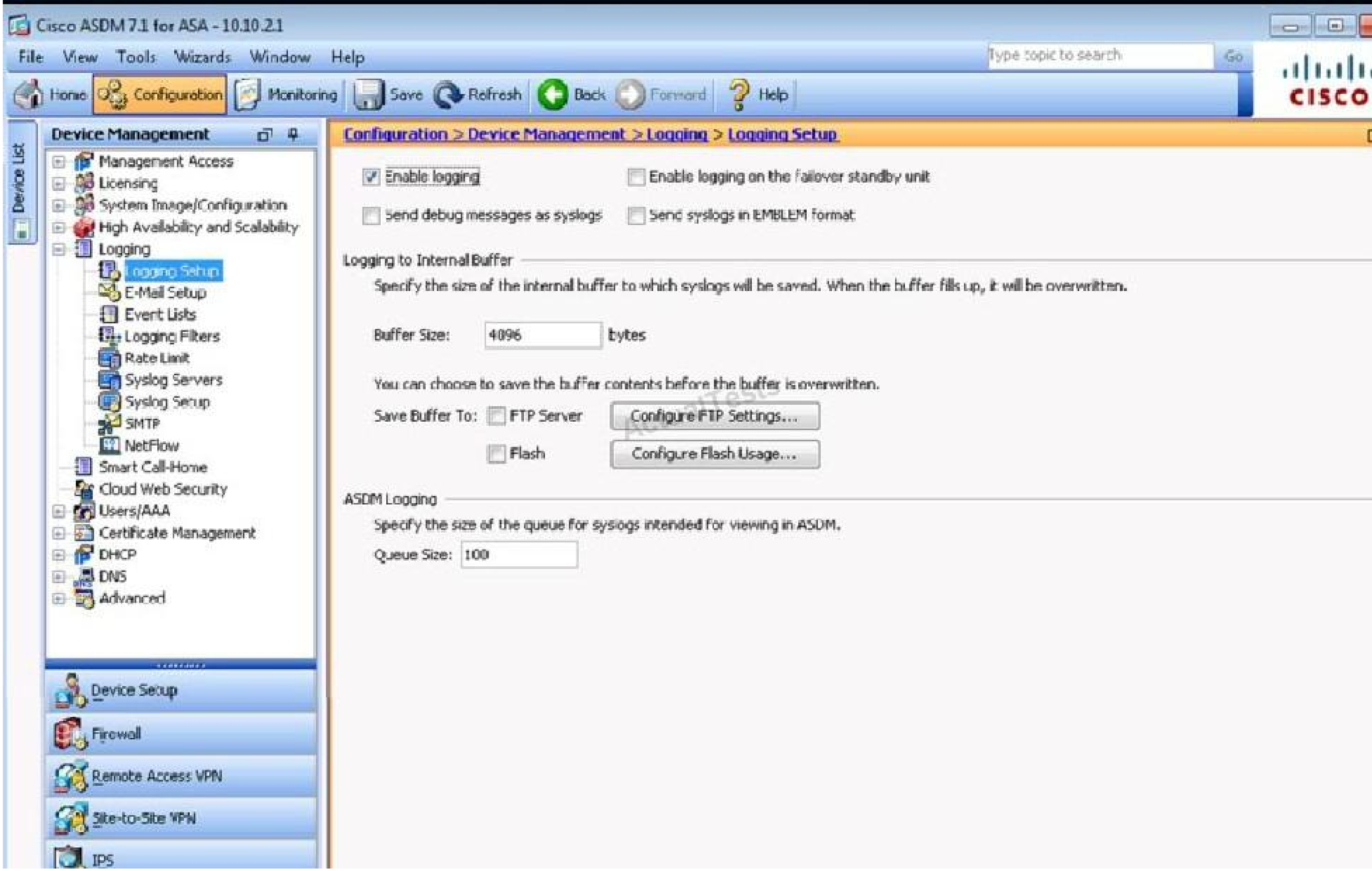
"Pass Any Exam. Any Time." - www.actualtests.com 81
Cisco 300-206 Exam
Which statement is true of the logging configuration on the Cisco ASA?

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Exhibit18



Configuration > Device Management > Logging > Logging Setup

☑ Enable logging　　□ Enable logging on the failover standby unit

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

Logging to Internal Buffer

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

Buffer Size: 4096 bytes

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

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

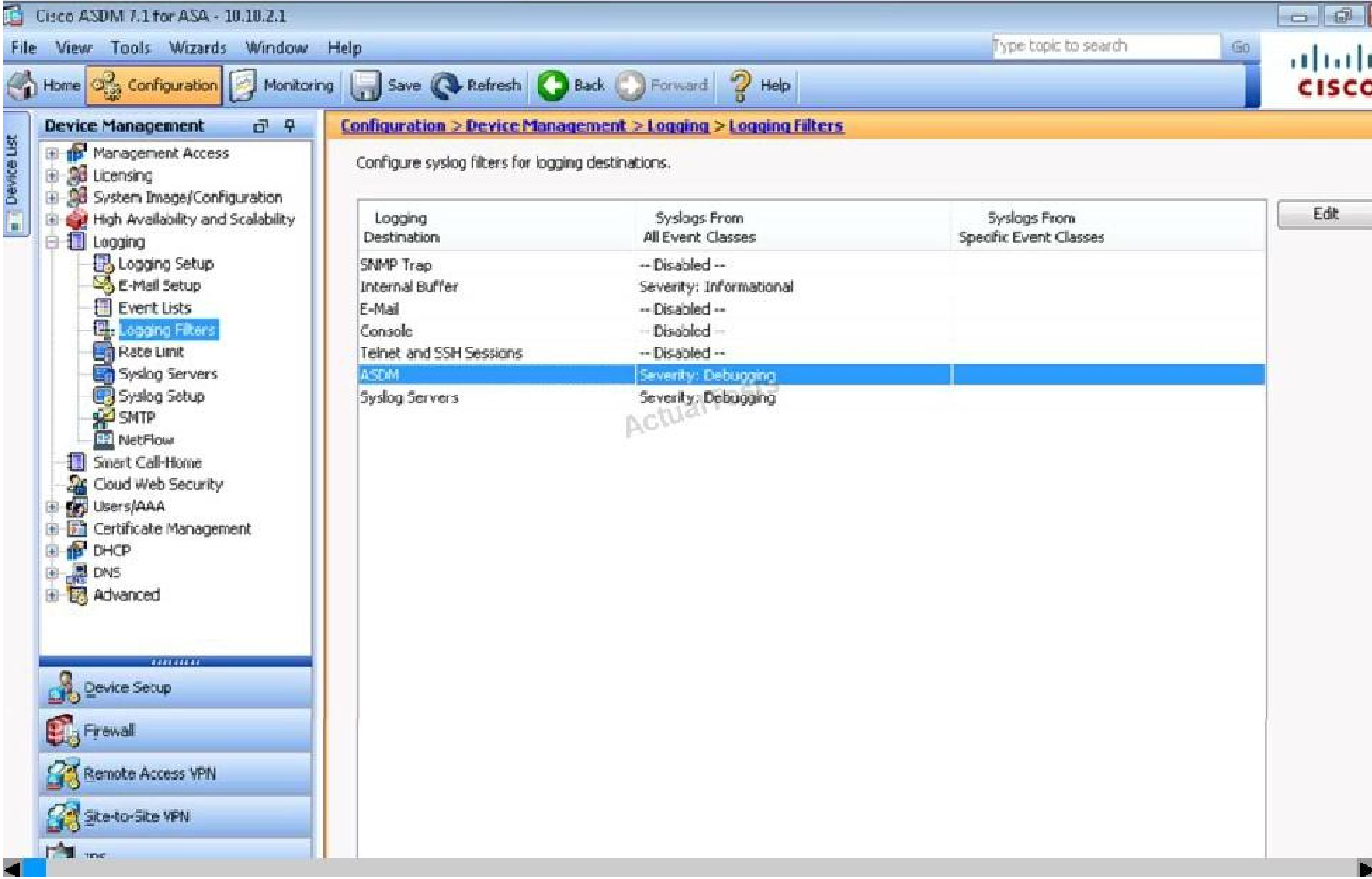
□ Flash　[Configure Flash Usage...]

ASDM Logging

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

Queue Size: 100

Exhibit19



Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

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

QUESTION 131
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
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
"Pass Any Exam. Any Time." - www.actualtests.com 21
Cisco 300-206 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
Which two voice protocols can the Cisco ASA inspect? (Choose two.)

A. MGCP
B. IAX
C. Skype

D. CTIQBE

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 134
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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 135
Enabling what security mechanism can prevent an attacker from gaining network topology information from CDP?

A. MACsec
B. Flex VPN
C. Control Plane Protection
"Pass Any Exam. Any Time." - www.actualtests.com 22
Cisco 300-206 Exam
D. Dynamic Arp Inspection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: