IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **642-524**

Title : Securing Networks with ASA Foundation

Version : DEMO

1.Tom works as a network administrator for the P4S company. The primary adaptive security appliance in an active/standby failover configuration failed, so the secondary adaptive security appliance was automatically activated. Tom then fixed the problem. Now he would like to restore the primary to active status. Which one of the following commands can reactivate the primary adaptive security appliance and restore it to active status while issued on the primary adaptive security appliance?

A.failover reset

B.failover primary active

C.failover active

D.failover exec standby

Answer:C

2.For the following commands, which one enables the DHCP server on the DMZ interface of the Cisco ASA with an address pool of 10.0.1.100-10.0.1.108 and a DNS server of 192.168.1.2?

A.dhcpd address 10.0.1.100-10.0.1.108 DMZ dhcpd dns 192.168.1.2 dhcpd enable DMZ

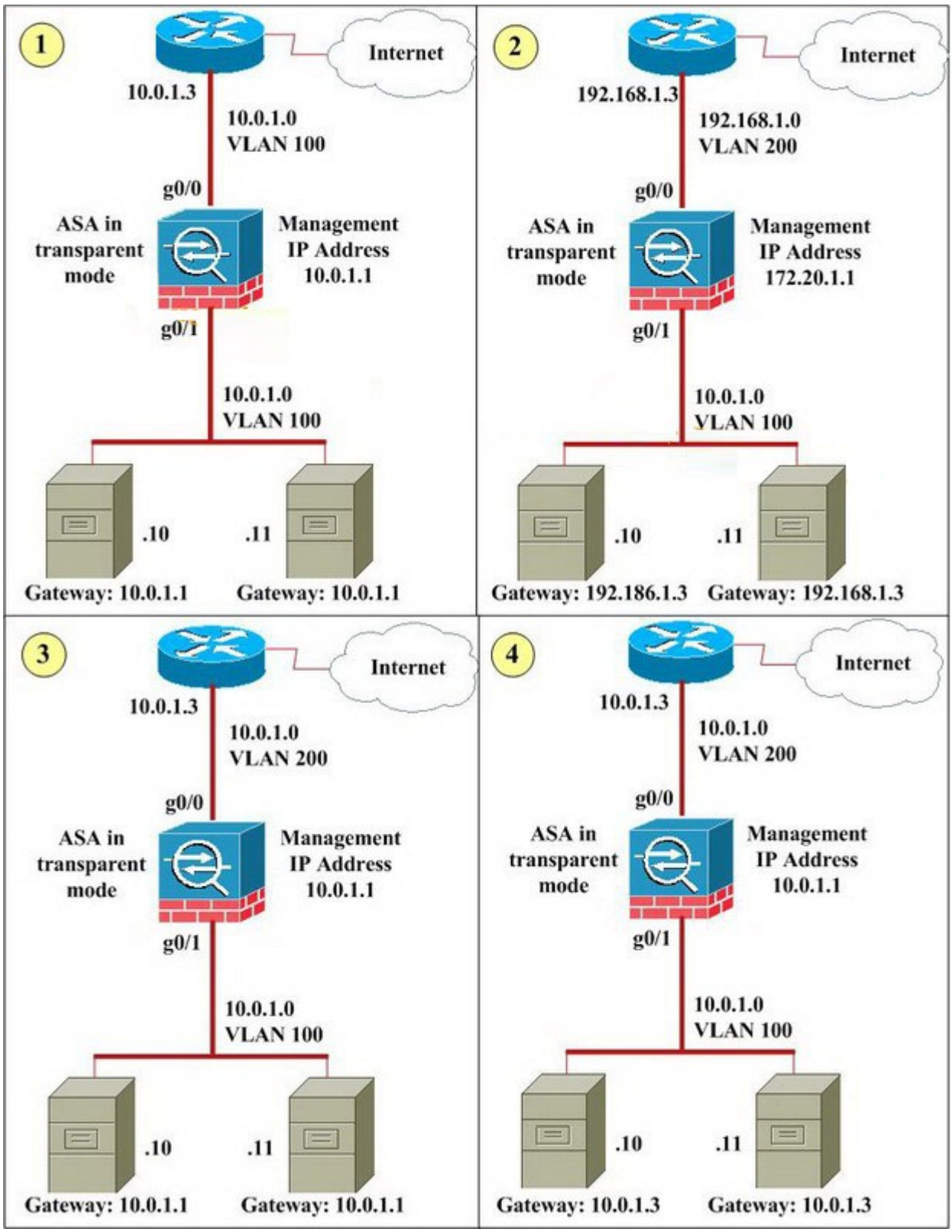
B.dhcpd address range 10.0.1.100-10.0.1.108 dhcpd dns server 192.168.1.2 dhcpd enable DMZ

C.dhcpd range 10.0.1.100-10.0.1.108 DMZ dhcpd dns server 192.168.1.2 dhcpd DMZ

D.dhcpd address range 10.0.1.100-10.0.1.108 dhcpd dns 192.168.1.2 dhcpd enable

Answer:A

3.Look at the following exhibit carefully, which one of the four diagrams displays a correctly configured network for a transparent firewall?



A.1

B.2

C.3

D.4

Answer:D

4.What is the effect of the per-user-override option when applied to the access-group command syntax?

A.The log option in the per-user access list overrides existing interface log options.

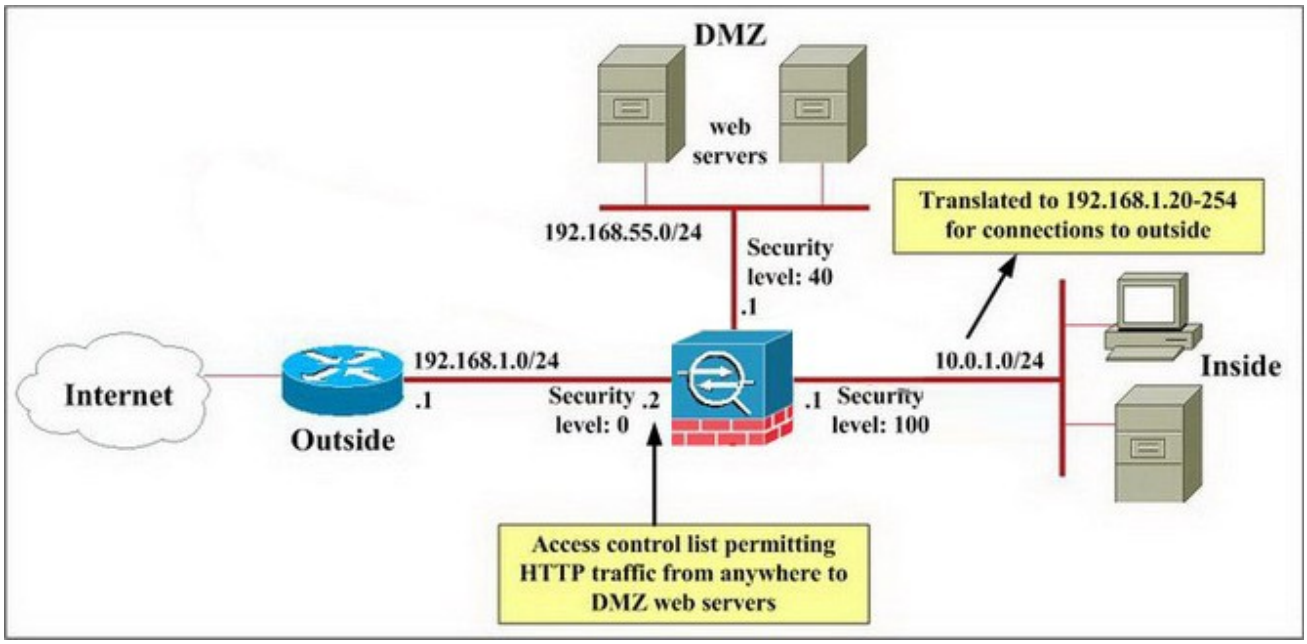
B.It allows for extended authentication on a per-user basis.

C.It allows downloadable user access lists to override the access list applied to the interface.

D.It increases security by building upon the existing access list applied to the interface. All subsequent users are also subject to the additional access list entries.

Answer:C

5.John works as a network administrator for the P4S company. According to the exhibit, the only traffic that John would like to allow through the corporate Cisco ASA adaptive security appliance is inbound HTTP to the DMZ network and all traffic from the inside network to the outside network. John also has configured the Cisco ASA adaptive security appliance, and access through it is now working as expected with one exception: contractors working on the DMZ servers have been surfing the Internet from the DMZ servers, which (unlike other Company XYZ hosts) are using public, routable IP addresses. Neither NAT statements nor access lists have been configured for the DMZ interface. What is the reason that the contractors are able to surf the Internet from the DMZ servers? (Note: The 192.168.X.X IP addresses are used to represent routable public IP addresses even though the 192.168.1.0 network is not actually a public routable network.)



A.An access list on the outside interface permits this traffic.

B.NAT control is not enabled.

C.The DMZ servers are using the same global pool of addresses that is being used by the inside hosts.

D.HTTP inspection is not enabled.

Answer:B

6.In order to recover the Cisco ASA password, which operation mode should you enter?

A.configure

B.unprivileged

C.privileged

D.monitor

Answer:D

7.Which three statements correctly describe protocol inspection on the Cisco ASA adaptive security appliance? (Choose three.)

A.For the security appliance to inspect packets for signs of malicious application misuse, you must enable advanced (application layer) protocol inspection.

B.If you want to enable inspection globally for a protocol that is not inspected by default or if you want to globally disable inspection for a protocol, you can edit the default global policy.

C.The protocol inspection feature of the security appliance securely opens and closes negotiated ports and IP addresses for legitimate client-server connections through the security appliance.

D.If inspection for a protocol is not enabled, traffic for that protocol may be blocked.

Answer:B C D

8.Observe the following commands, which one verifies that NAT is working normally and displays active NAT translations?

A.show ip nat all

B.show running-configuration nat

C.show xlate

D.show nat translation

Answer:C

9.Multimedia applications transmit requests on TCP, get responses on UDP or TCP, use dynamic ports, and use the same port for source and destination, so they can pose challenges to a firewall. Which three items are true about how the Cisco ASA adaptive security appliance handles multimedia applications? (Choose three.)

A.It dynamically opens and closes UDP ports for secure multimedia connections, so you do not need to open a large range of ports.

B.It supports SIP with NAT but not with PAT.

C.It supports multimedia with or without NAT.

D.It supports RTSP, H.323, Skinny, and CTIQBE.

Answer:A C D

10.What is the result if the WebVPN url-entry parameter is disabled?

A.The end user is unable to access pre-defined URLs.

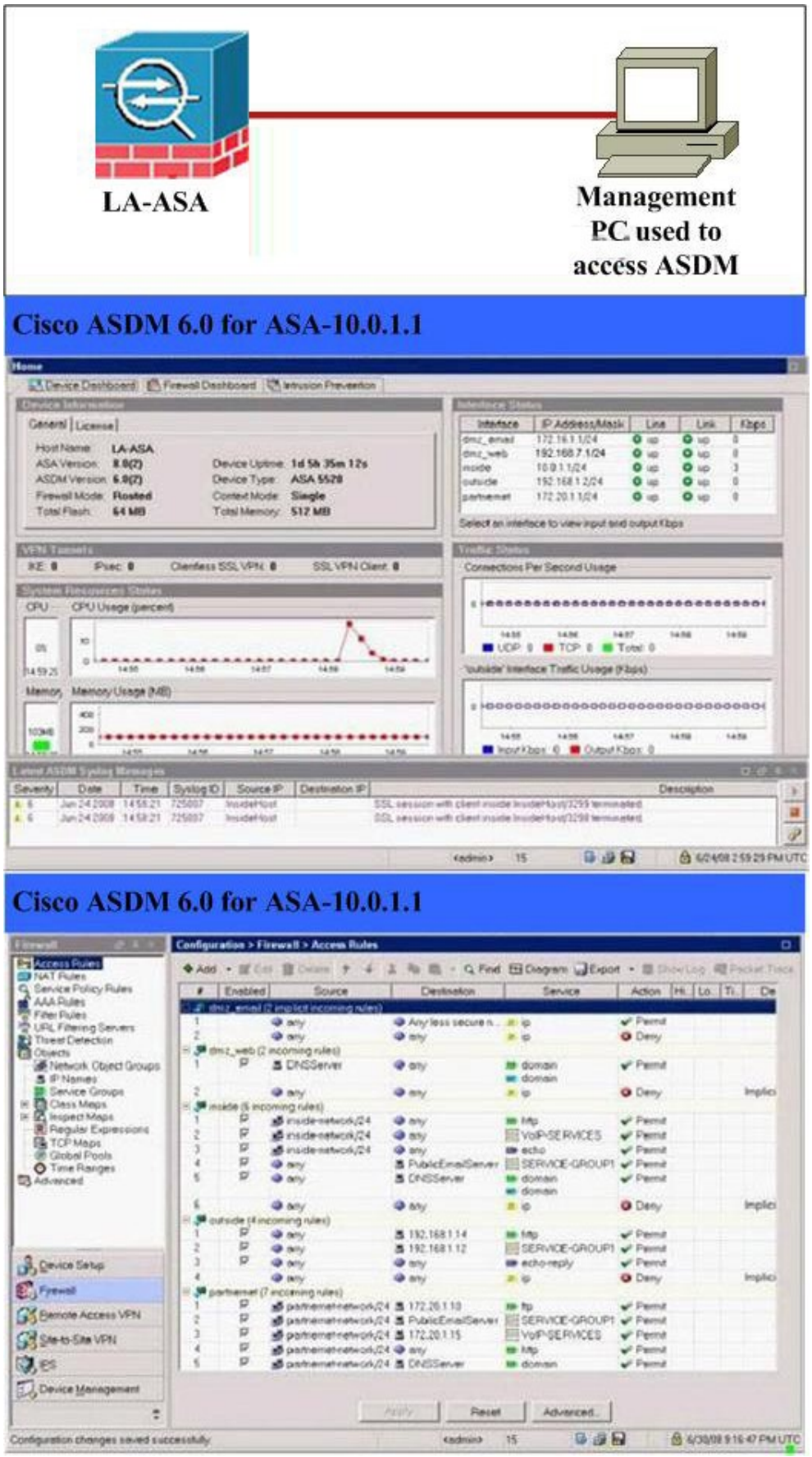
B.The end user is unable to access any CIFS shares or URLs.

C.The end user is able to access CIFS shares but not URLs.

D.The end user is able to access pre-defined URLs.

Answer:D

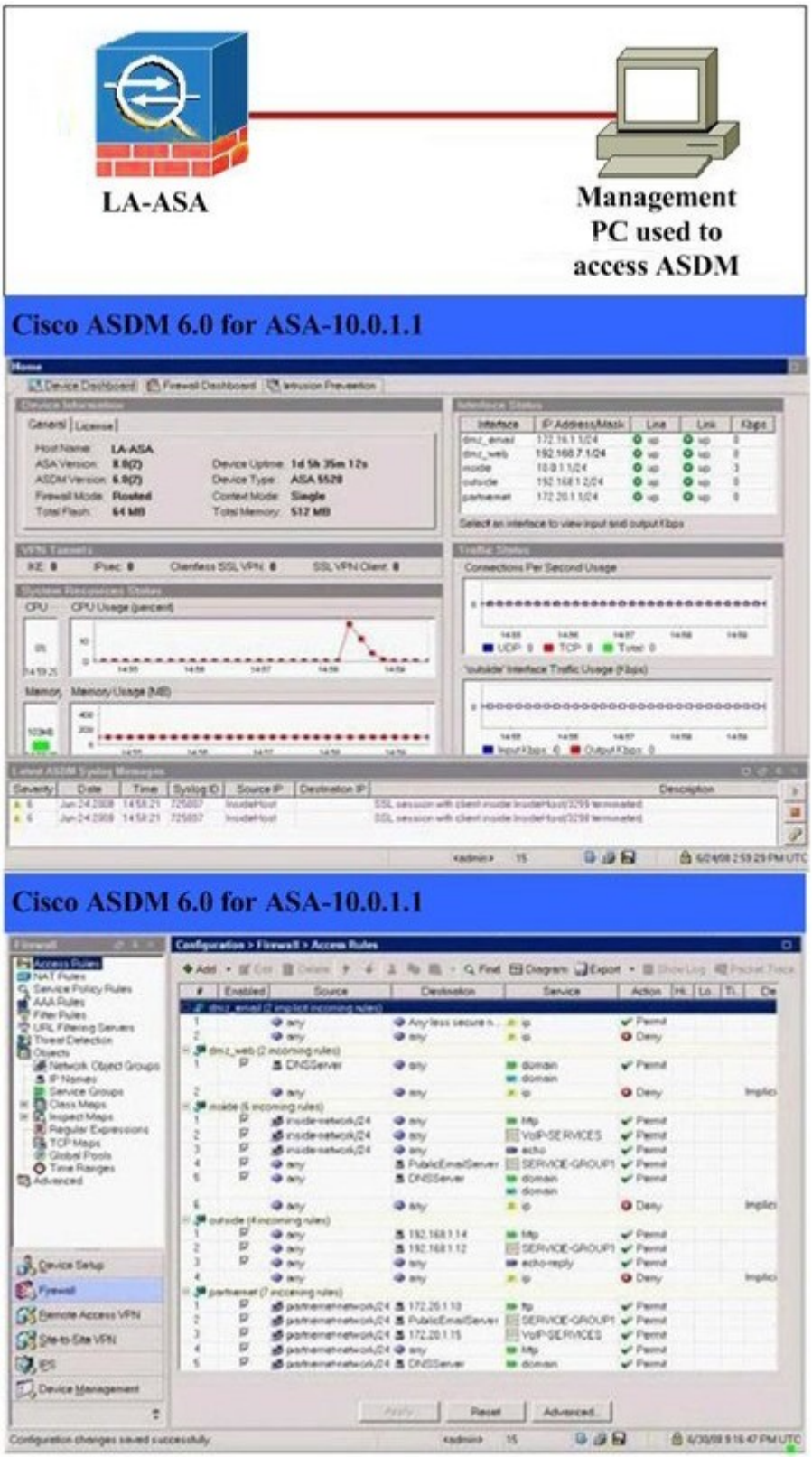
11.You work as a network engineer at Pass4sure.com, you are asked to examine the current Modular Policy Framework configurations on the LA-ASA Adaptive Security Appliances using the Cisco Adaptive Security Device Manager (ASDM) utility. You need to answer the multiple-choice questions in this simulation by use of the appropriate Cisco ASDM configuration screens. A host on the partnernet network attempts to use FTP to download a file from InsideHost,which resides on the inside interface of the security appliance.What does the security appliance do with the traffic from the partnernet host?



A.Sends it to the Cisco ASA Advanced Inspection and Prevention(AIP)-Security Services

Module(SSM)for inspection before forwarding it to its destination
B.Sends it to the Cisco ASA 5500 Series Content Security and Control(CSC)SSM for inspection before forwarding it to its destination
C.Forwards it directly to its destination
D.Forwards it directly to its destination unless the connection limit is already met
Answer:D

12.You work as a network engineer at Pass4sure.com, you are asked to examine the current Modular Policy Framework configurations on the LA-ASA Adaptive Security Appliances using the Cisco Adaptive Security Device Manager (ASDM) utility. You need to answer the multiple-choice questions in this simulation by use of the appropriate Cisco ASDM configuration screens. Which traffic does the security appliance inspect globally(regardless of the interface on which the traffic enters the security appliance)?(Choose 3)



A.HTTP

B.DNS

C.GTP

D.H.323 H.225

Answer:A B D

13.You work as a network engineer at Pass4sure.com, you are asked to examine the current Modular Policy Framework configurations on the LA-ASA Adaptive Security Appliances using the Cisco Adaptive Security Device Manager (ASDM) utility. You need to answer the multiple-choice questions in this simulation by use of the appropriate Cisco ASDM configuration screens. A host on the partnernet network makes a VoIP call to 172.20.1.15,which is statically mapped to an IP phone on the inside network.What does the security appliance do with the VoIP traffic between host 172.20.1.15 and the host on the partnernet network?

A.Sends it to the AIP-SSM for inspection before forwarding it to its destination

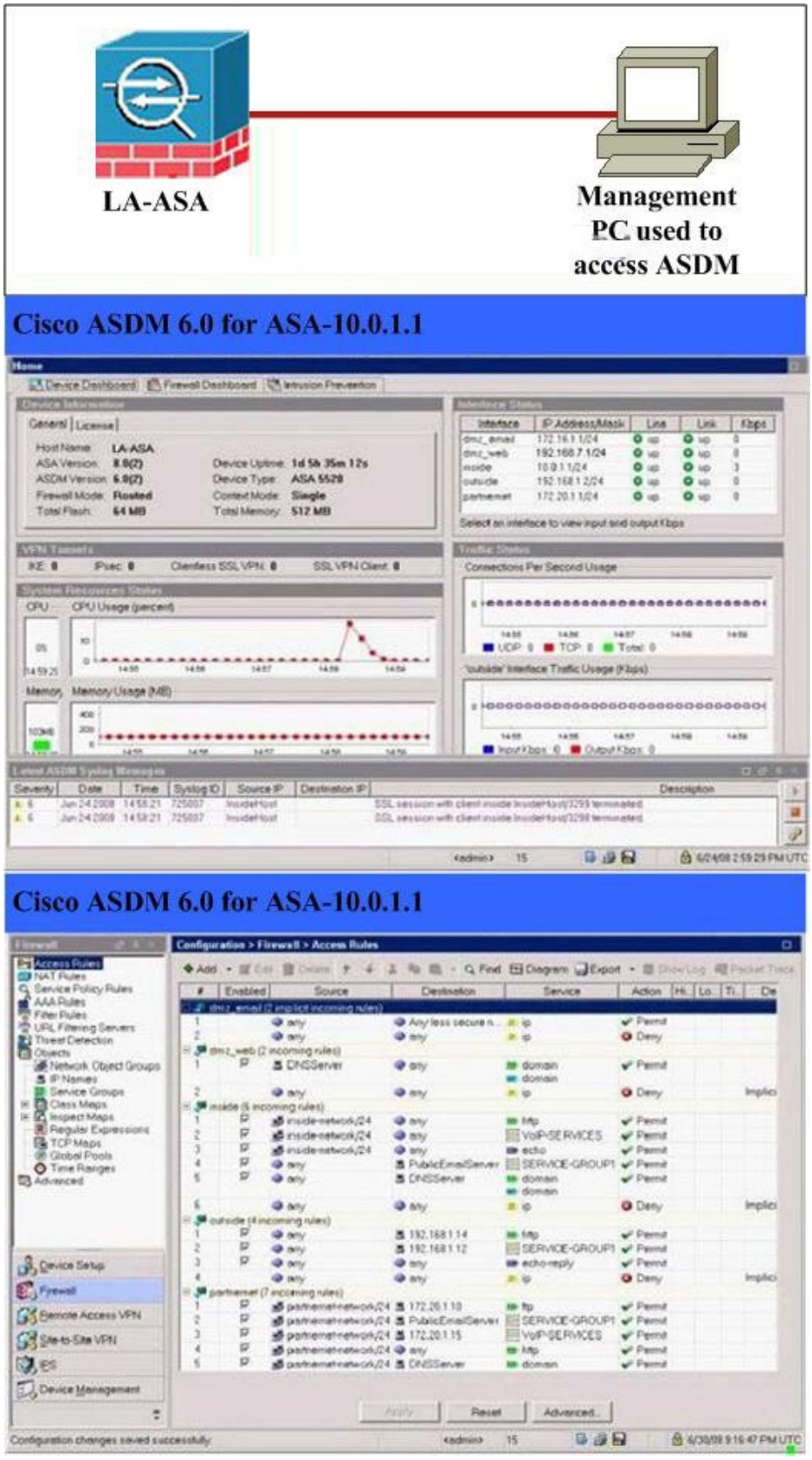
B.Sends it to the CSC-SSM for inspection before forwarding it to its destination

C.Forwards it directly to its destination unless the connection limit is already met

D.Applies low latency queuing as it exits the partnernet interface

Answer:D

14.You work as a network engineer at Pass4sure.com, you are asked to examine the current Modular Policy Framework configurations on the LA-ASA Adaptive Security Appliances using the Cisco Adaptive Security Device Manager (ASDM) utility. You need to answer the multiple-choice questions in this simulation by use of the appropriate Cisco ASDM configuration screens. A host on the outside network sends e-mail to the public e-mail server.What does the security appliance do with the traffic from the outside host?

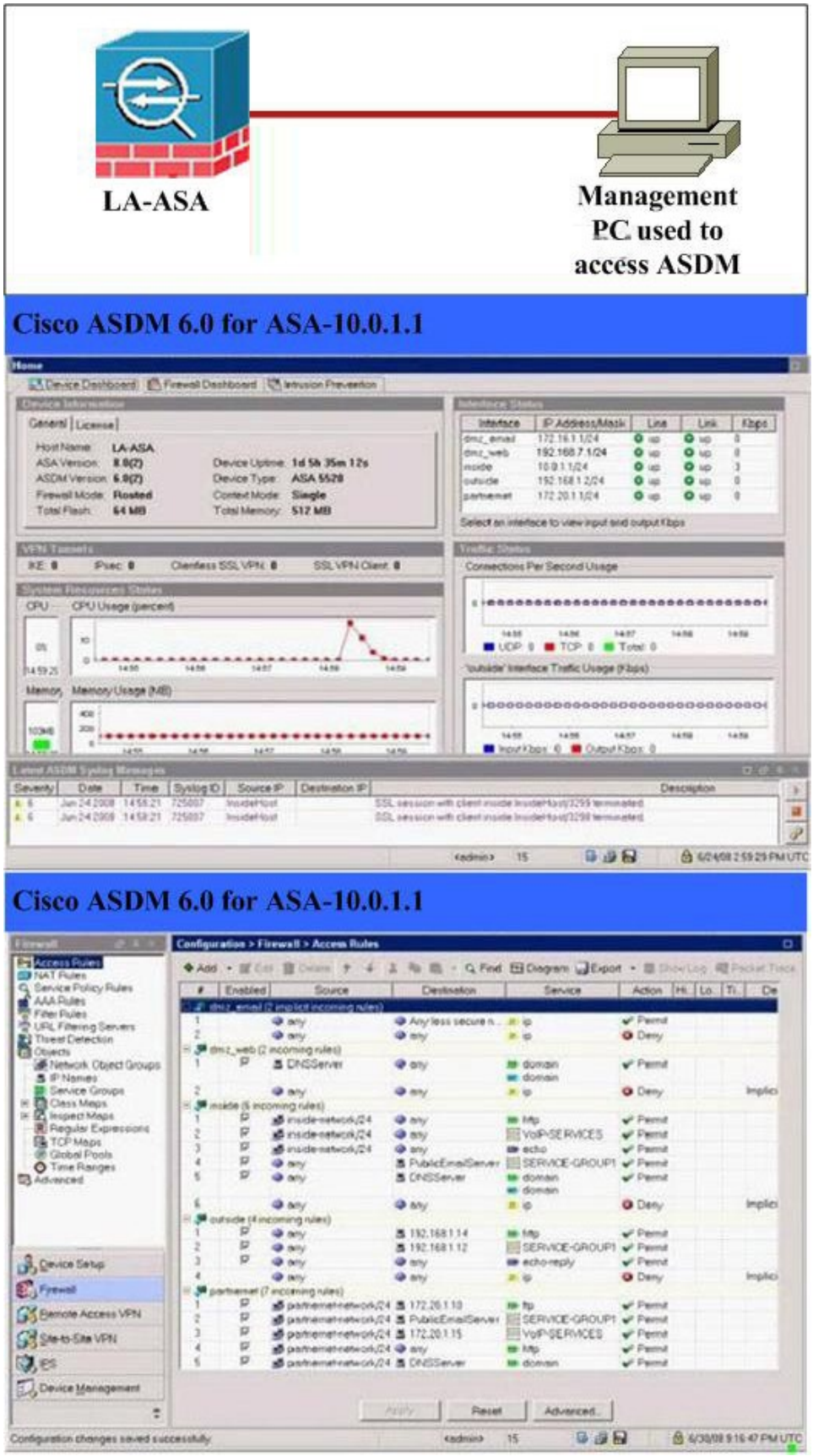


A.Sends it to the AIP-SSM for inspection before forwarding it to its destination
B.Sends it to the CSC-SSM for inspection before forwarding it to its destination
C.Forwards it directly to its destination

D.Forwards it directly to its destination unless the connection limit is already met

Answer:A

15.You work as a network engineer at Pass4sure.com, you are asked to examine the current Modular Policy Framework configurations on the LA-ASA Adaptive Security Appliances using the Cisco Adaptive Security Device Manager (ASDM) utility. You need to answer the multiple-choice questions in this simulation by use of the appropriate Cisco ASDM configuration screens. A host on the partnernet network attempts to access the public web server via HTTP.What does the security appliance do with traffic from the partnernet?



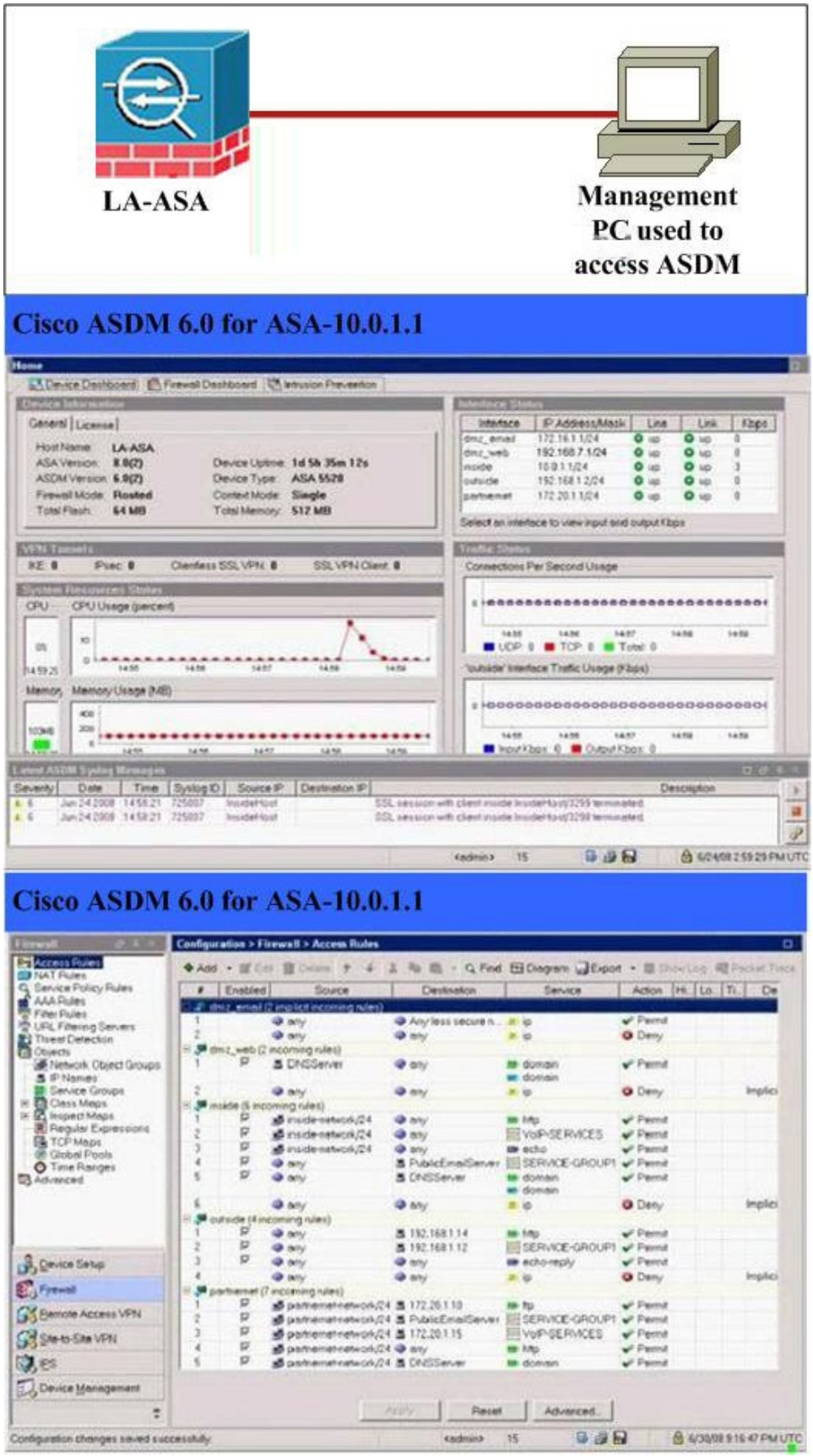
A.Sends it to the AIP-SSM for inspection before forwarding it to its destination
B.Sends it to the CSC-SSM for inspection before forwarding it to its destination

C.Forwards it directly to its destination

D.Forwards it directly to its destination unless the connection limit is already met

Answer:C

16.You work as a network engineer at Pass4sure.com, you are asked to examine the current Modular Policy Framework configurations on the LA-ASA Adaptive Security Appliances using the Cisco Adaptive Security Device Manager (ASDM) utility. You need to answer the multiple-choice questions in this simulation by use of the appropriate Cisco ASDM configuration screens. A host on the outside network makes a VoIP call to a host on the inside network.What does the security appliance do with the traffic from the host on the outside network?



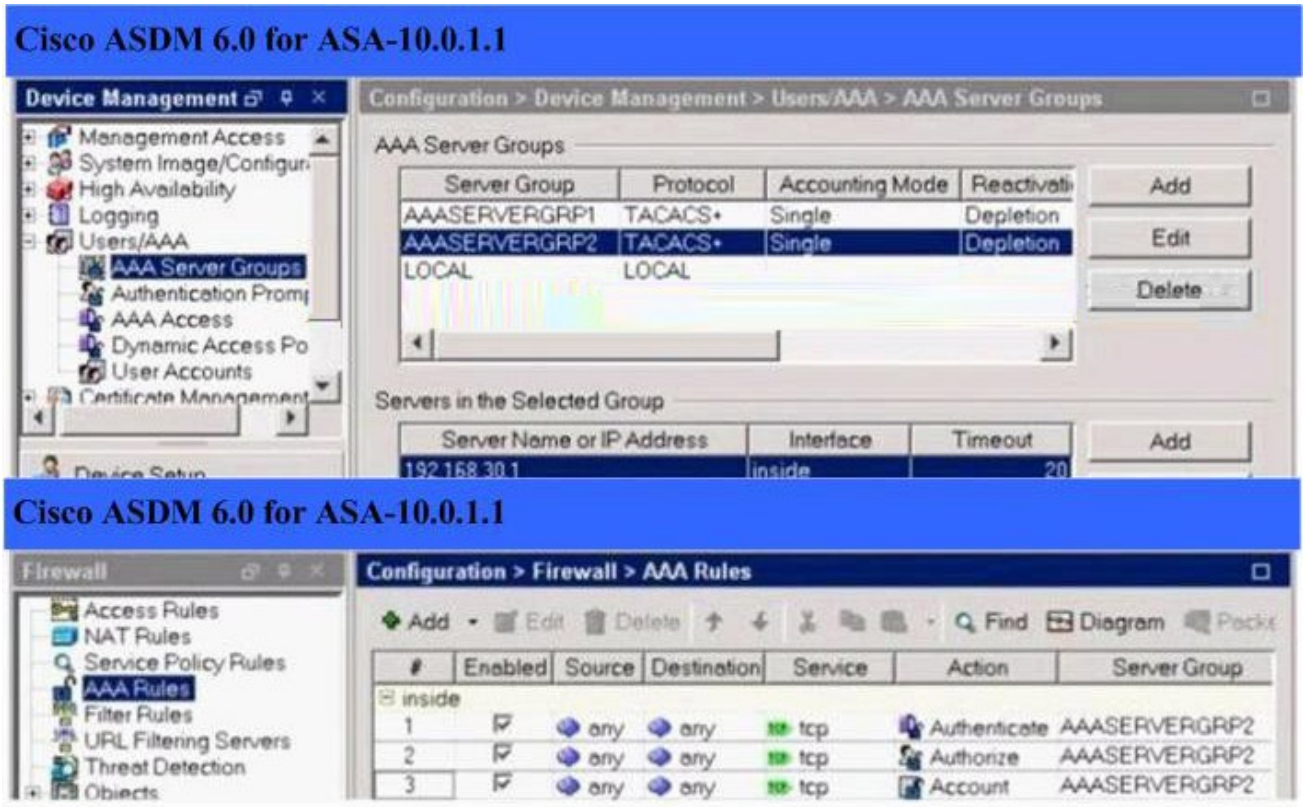
A.Sends it to the AIP-SSM for inspection before forwarding it to its destination
B.Sends it to the CSC-SSM for inspection before forwarding it to its destination

C.Forwards it directly to its destination
D.Drops it
Answer:D

17.Which three tunneling protocols and methods are supported by the Cisco VPN Client? (Choose three.)
A.IPsec over TCP
B.IPsec over UDP
C.ESP
D.AH
Answer:A B C

18.Which two options are correct about the impacts of this configuration? (Choose two.) class-map INBOUND_HTTP_TRAFFIC match access-list TOINSIDEHOST class-map OUTBOUND_HTTP_TRAFFIC match access-list TOOUTSIDEHOST policy-map MYPOLICY class INBOUND_HTTP_TRAFFIC inspect http set connection conn-max 100 policy-map MYOTHERPOLICY class OUTBOUND_HTTP_TRAFFIC inspect http service-policy MYOTHERPOLICY interface inside service-policy MYPOLICY interface outside
A.Traffic that matches access control list TOINSIDEHOST is subject to HTTP inspection and maximum connection limits.
B.Traffic that enters the security appliance through the inside interface is subject to HTTP inspection.
C.Traffic that enters the security appliance through the outside interface and matches access control list TOINSIDEHOST is subject to HTTP inspection and maximum connection limits.
D.Traffic that enters the security appliance through the inside interface and matches access control list TOOUTSIDEHOST is subject to HTTP inspection.
Answer:C D

19.Take the following configuration shown in the exhibit carefully, what traffic will be logged to the AAA server?



A.Only authenticated and authorized console connection information will be logged in the accounting database.

B.All outbound TCP connection information will be logged in the accounting database.

C.No information will be logged. This is not a valid configuration because TACACS+ connection information cannot be captured and logged.

D.All connection information will be logged in the accounting database.

Answer:B