

Cisco 642-524

**642-524 Securing Networks with ASA Foundation
(SNAF)**

Practice Test

Version 1.7

QUESTION NO: 1

Tom works as a network administrator. 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

QUESTION NO: 2

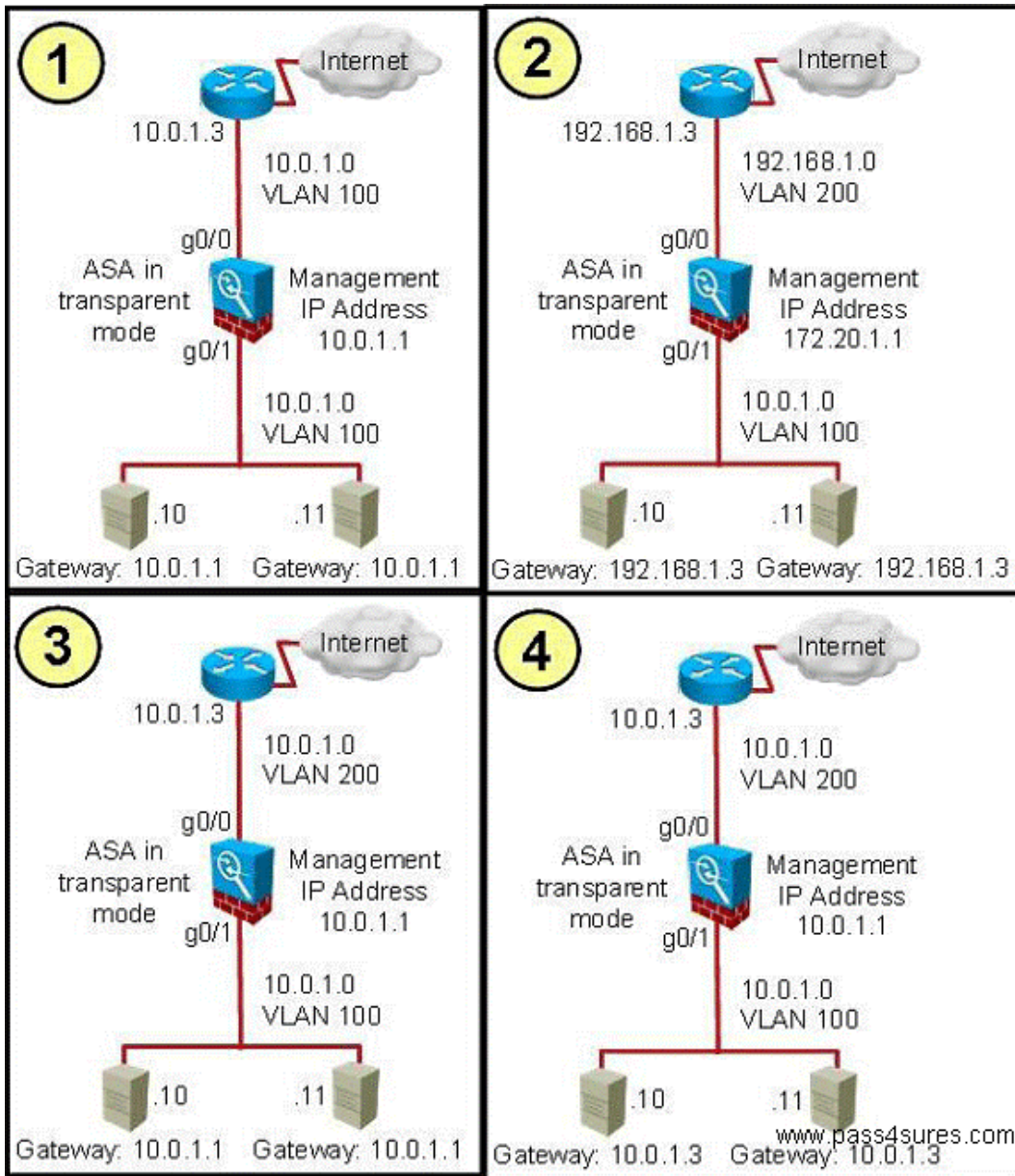
For the following commands, which one enables the DHCP server on the DMZ interface of the Cisco ASA with an address pool of 10.0.1.100-10.0.1.108 and a DNS server of 192.168.1.2?

- 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

QUESTION NO: 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

QUESTION NO: 4

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

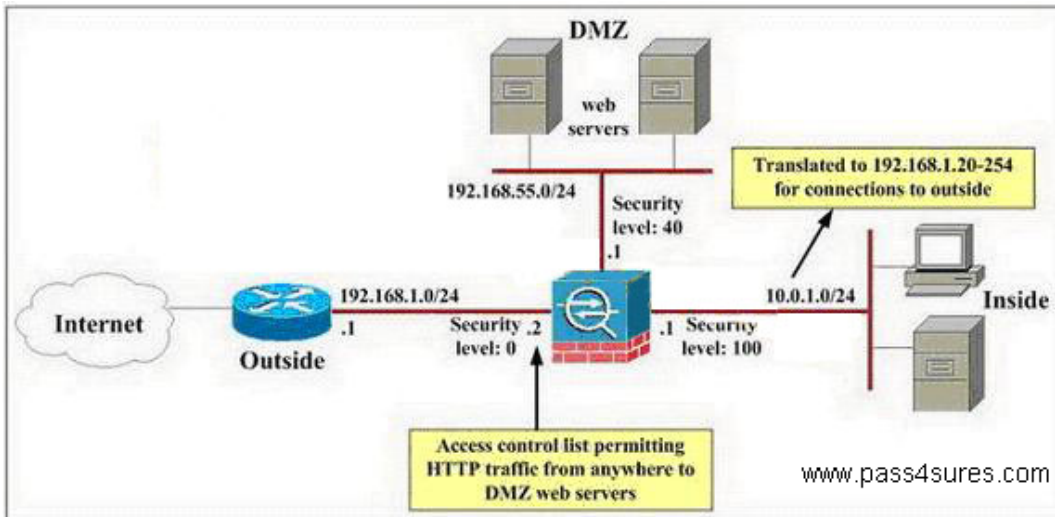
- A. The log option in the per-user access list overrides existing interface log options.
- B. It allows for extended authentication on a per-user basis.
- C. Allows downloadable user access lists to override the access list applied to the interface.

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

QUESTION NO: 5

John works as a network administrator .



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.XIP 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 10

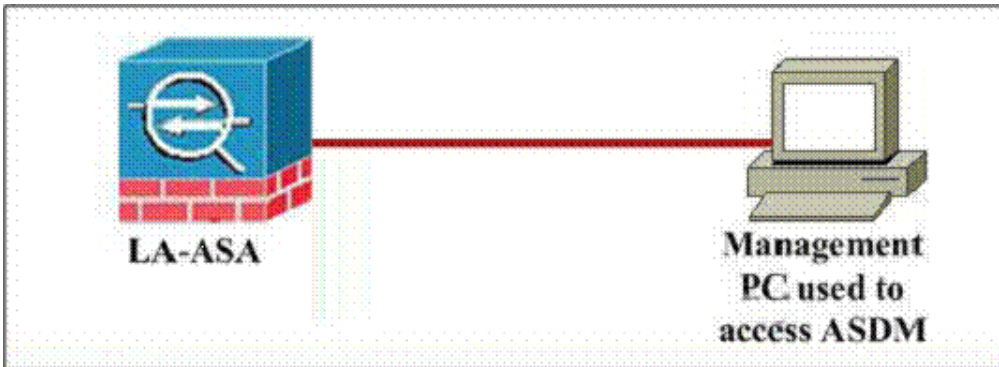
What is the result if the WebVPN url-entry parameter is disabled?

- 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

QUESTION NO: 11

You work as a network engineer, 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.



Cisco ASDM 6.0 for ASA-10.0.1.1

This screenshot shows the main dashboard of the Cisco ASDM 6.0 interface. It includes several panels:

- System Information:** Host Name: LA-ASA, Device Uptime: 1d 5h 35m 12s, Device Type: ASA 5520, ASDM Version: 6.0(2), Firewall Mode: Routed, Control Mode: Single, Total Flash: 64 MB, Total Memory: 512 MB.
- Interface Table:**

Interface	IP Address/Mask	Link	Up	Down	Fltgs
enc_ether1	172.26.1.1/24	up	up	up	0
enc_ether2	192.168.7.1/24	up	up	up	0
inside	10.0.1.1/24	up	up	up	0
outside	192.168.1.1/24	up	up	up	0
partnetnet	172.25.1.1/24	up	up	up	0
- Performance Graphs:** CPU usage (0-100%), Memory usage (0-1024 MB), and various traffic usage graphs for interfaces.
- Event Log:** Shows system messages such as 'SSL session with client mode ipsec@host: 10.0.1.1 terminated'.

Cisco ASDM 6.0 for ASA-10.0.1.1

This screenshot shows the 'Access Rules' configuration page in Cisco ASDM 6.0. The table below represents the data visible in the interface:

#	Enabled	Source	Destination	Service	Action	Hit	Log	RT	Ch
1	<input checked="" type="checkbox"/>	any	Any less secure n...	ip	Permit				
2	<input checked="" type="checkbox"/>	any	any	ip	Deny				
1	<input checked="" type="checkbox"/>	enc_ether2 (incoming)	any	domain	Permit				
2	<input checked="" type="checkbox"/>	any	any	ip	Deny				Implicit
1	<input checked="" type="checkbox"/>	inside (incoming)	any	any	Permit				
2	<input checked="" type="checkbox"/>	inside-network/24	any	any	Permit				
3	<input checked="" type="checkbox"/>	inside-network/24	any	any	Permit				
4	<input checked="" type="checkbox"/>	any	Public-Host/Server	any	Permit				
5	<input checked="" type="checkbox"/>	any	CHOCServer	domain	Permit				
6	<input checked="" type="checkbox"/>	any	any	ip	Deny				Implicit
1	<input checked="" type="checkbox"/>	outside (incoming)	192.168.1.1	any	Permit				
2	<input checked="" type="checkbox"/>	any	192.168.1.2	any	Permit				
3	<input checked="" type="checkbox"/>	any	any	any	Permit				
4	<input checked="" type="checkbox"/>	any	any	ip	Deny				Implicit
1	<input checked="" type="checkbox"/>	partnetnet-network/24	172.25.1.10	any	Permit				
2	<input checked="" type="checkbox"/>	partnetnet-network/24	Public-Host/Server	any	Permit				
3	<input checked="" type="checkbox"/>	partnetnet-network/24	172.20.1.15	any	Permit				
4	<input checked="" type="checkbox"/>	partnetnet-network/24	any	any	Permit				
5	<input checked="" type="checkbox"/>	partnetnet-network/24	CHOCServer	domain	Permit				

A host on the partnetnet 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 partnetnet 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

QUESTION NO: 12

You work as a network engineer, 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.



LA-ASA



Management PC used to access ASDM

Cisco ASDM 6.0 for ASA-10.0.1.1

The screenshot shows the Cisco ASDM 6.0 interface for a Cisco ASA device. The 'General' tab is active, displaying system information:

- Host Name: LA-ASA
- ASA Version: 8.8(2)
- ASDM Version: 6.8(2)
- Firewall Mode: Hosted
- Total Flash: 64 MB
- Device Uptime: 1d 5h 35m 12s
- Device Type: ASA 5528
- Control Mode: Single
- Total Memory: 517 MB

The 'Interfaces' table shows the following:

Interface	IP Address/Mask	Line	Link	Up	Flaps
dmz_email	172.16.1.124	up	up	0	0
dmz_web	192.168.7.124	up	up	0	0
inside	10.8.1.124	up	up	0	0
outside	192.168.1.254	up	up	0	0
porternet1	172.20.1.124	up	up	0	0

Below the interface table, there are two graphs: 'CPU Usage (percent)' and 'Memory Usage (MB)'. To the right, there are two bar charts: 'Connection Pairs Second Usage' and 'Inbound Interface Traffic Usage (Kbps)'. At the bottom, a log table shows recent events related to SSL sessions.

Cisco ASDM 6.0 for ASA-10.0.1.1

The screenshot shows the 'Access Rules' configuration page in Cisco ASDM 6.0. The left sidebar shows the navigation tree with 'Access Rules' selected. The main area displays a table of rules:

#	Enabled	Source	Destination	Service	Action	Ht	Lo	Tp	De
1	<input checked="" type="checkbox"/>	any	Any host (secured)	ip	Permit				
2	<input checked="" type="checkbox"/>	any	any	ip	Deny				
dmz_web (2 outgoing rules)									
1	<input checked="" type="checkbox"/>	any	any	domain	Permit				
2	<input checked="" type="checkbox"/>	any	any	domain	Deny				Implic
inside (3 outgoing rules)									
1	<input checked="" type="checkbox"/>	inside-network/24	any	ftp	Permit				
2	<input checked="" type="checkbox"/>	inside-network/24	any	Voice-IPSEC	Permit				
3	<input checked="" type="checkbox"/>	inside-network/24	any	echo	Permit				
4	<input checked="" type="checkbox"/>	any	PublicEmailServer	SERVICE-GROUP1	Permit				
5	<input checked="" type="checkbox"/>	any	DNSServer	domain	Permit				
6	<input checked="" type="checkbox"/>	any	any	ip	Deny				Implic
outside (4 incoming rules)									
1	<input checked="" type="checkbox"/>	any	192.168.1.14	ftp	Permit				
2	<input checked="" type="checkbox"/>	any	192.168.1.12	SERVICE-GROUP1	Permit				
3	<input checked="" type="checkbox"/>	any	any	echosrc	Permit				
4	<input checked="" type="checkbox"/>	any	any	ip	Deny				Implic
porternet1 (2 outgoing rules)									
1	<input checked="" type="checkbox"/>	porternet-network/24	172.16.1.12	ftp	Permit				
2	<input checked="" type="checkbox"/>	porternet-network/24	PublicEmailServer	SERVICE-GROUP1	Permit				
3	<input checked="" type="checkbox"/>	porternet-network/24	172.20.1.15	Voice-SERVICES	Permit				
4	<input checked="" type="checkbox"/>	porternet-network/24	any	ftp	Permit				
5	<input checked="" type="checkbox"/>	porternet-network/24	DNSServer	domain	Permit				

At the bottom of the screen, there is a watermark: 'www.pass4sures.com'.

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.323H.225

Answer: A,B,D

QUESTION NO: 13

You work as a network engineer, 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.