



642-524

(Securing Networks with ASA Foundation)

Document version:1 04 11

Important Note About 642-524 PDF

techeXams' **642-524 PDF** is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Copyright

techeXams holds the copyright of this material. techeXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Question: 1

Tom works as a network administrator for the TE 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

Question: 2

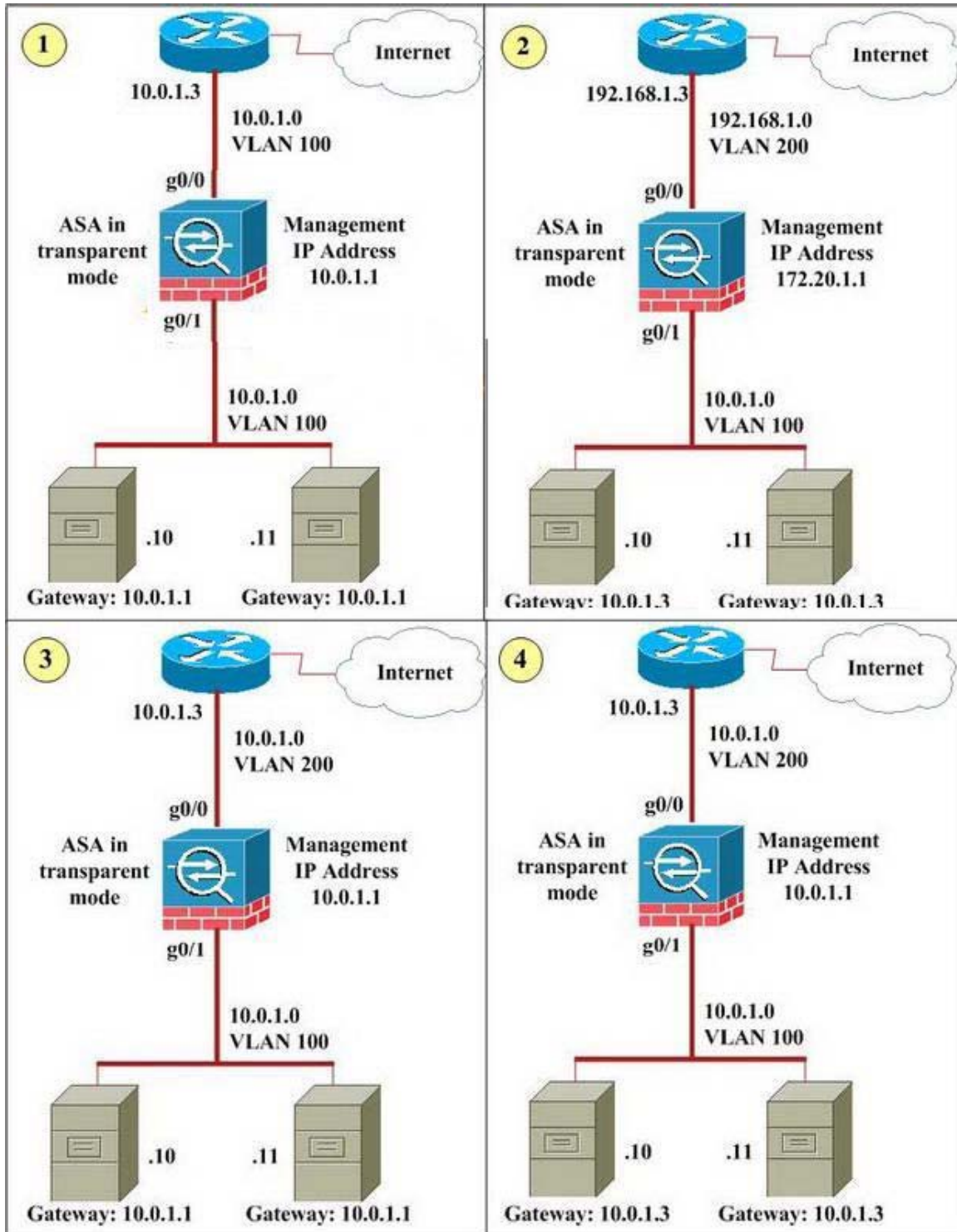
For the following commands, which one enables the DHCP server on the DMZ interface of the Cisco ASA with an address pool of 10.0.1.100-10.0.1.108 and a DNS server of 192.168.1.2?

- 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: 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: 4

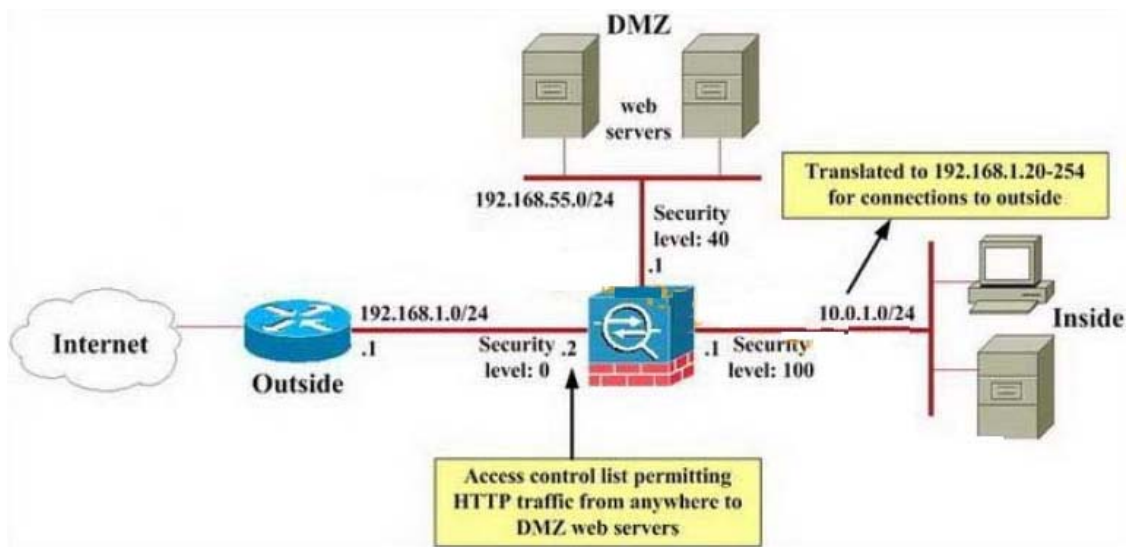
What is the effect of the per-user-override option when applied to the access-group command syntax?

- 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

Question: 5

John works as a network administrator for the TE 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

Question: 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: 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: 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

Get Full Version of Exam 642-524 PDF Q&A

techeXams presents authentic, genuine and valid study material, which promise 100% success in very first attempt. To take optimal results for 642-524 exam, you need to buy full version of 642-524 question and answer. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. So come join us and quench your thirst for knowledge.

Get complete 642-524 questions and answers by visiting URL

["http://www.techexams.ws/exams/642-524.do"](http://www.techexams.ws/exams/642-524.do)