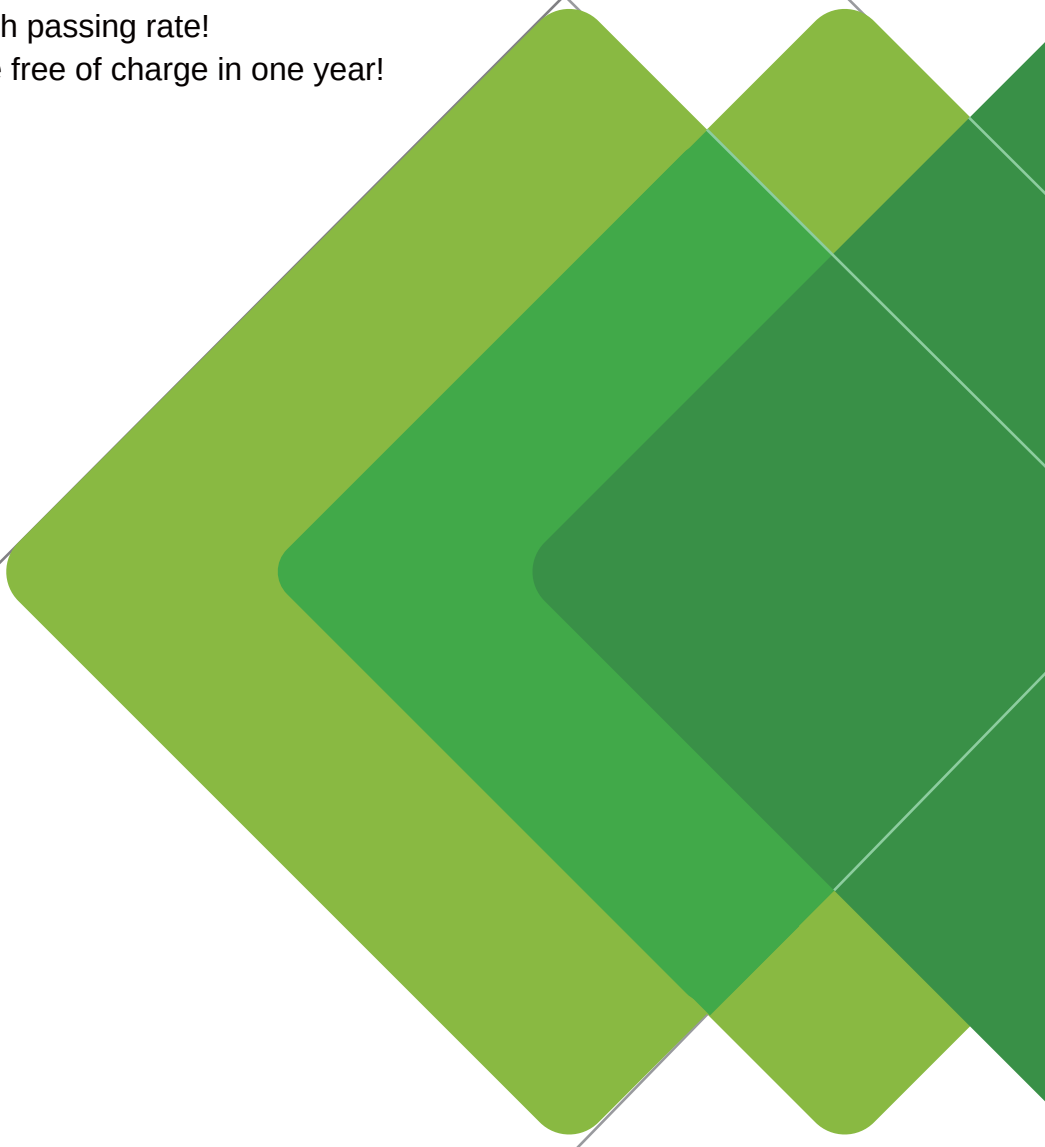
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

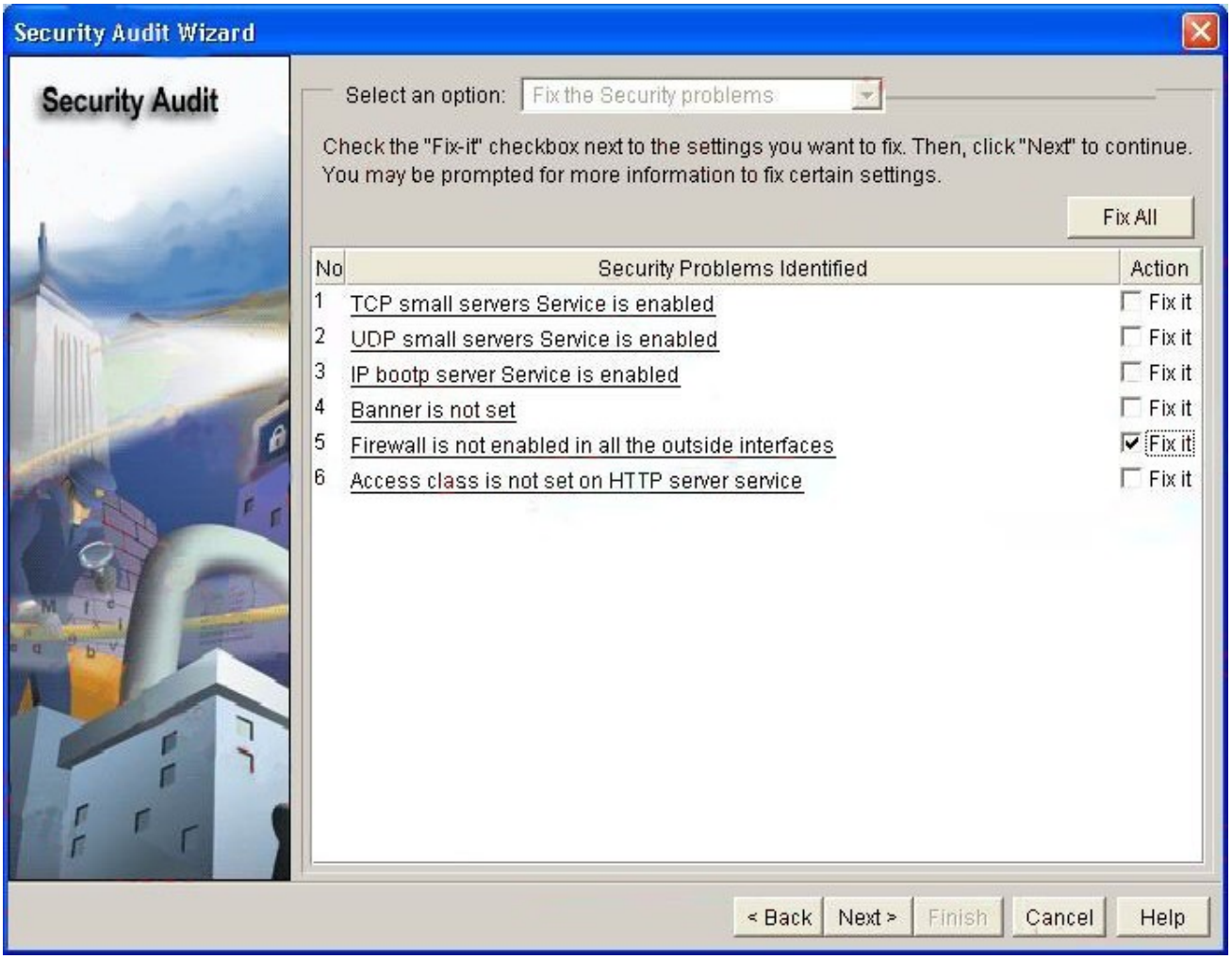


Exam : **642-552**

Title : Cisco Securing Cisco Network Devices Exam

Version : Demo

1. Referring to the Cisco SDM Security Audit Wizard screen shown, what will happen if you check the Fix it box for Firewall is not enabled in all the outside interfaces then click the Next button?



A. All outside access through the outside interfaces will immediately be blocked by an ACL.
B. SDM will prompt you to configure an ACL to block access through the outside interfaces.
C. SDM will take you to the Advanced Firewall Wizard.
D. SDM will perform a one-step lockdown to lock down the outside interfaces.
E. SDM will take you to the Edit Firewall Policy/ACL screen where you can configure an ACL to block access through the outside interfaces.
Answer: C

2. Which of these two ways does Cisco recommend that you use to mitigate maintenance-related threats? (Choose two.)
A. Maintain a stock of critical spares for emergency use.
B. Ensure that all cabling is Category 6.
C. Always follow electrostatic discharge procedures when replacing or working with internal router and switch device components.
D. Always wear an electrostatic wrist band when handling cabling, including fiber-optic cabling.
E. Always employ certified maintenance technicians to maintain mission-critical equipment and cabling.
Answer: AC

3. Which method of mitigating packet-sniffer attacks is the most effective?
A. implement two-factor authentication
B. deploy a switched Ethernet network infrastructure
C. use software and hardware to detect the use of sniffers
D. deploy network-level cryptography using IPsec, secure services, and secure protocols
Answer: D

4. A malicious program is disguised as another useful program; consequently, when the user executes the program,files get erased and then the malicious program spreads itself using emails as the delivery mechanism. Which type of attack best describes how this scenario got started?
A. DoS
B. worm
C. virus
D. trojan horse
E. DDoS
Answer: D

5. What is the key function of a comprehensive security policy?
A. informing staff of their obligatory requirements for protecting technology and information assets
B. detailing the way security needs will be met at corporate and department levels
C. recommending that Cisco IPS sensors be implemented at the network edge
D. detailing how to block malicious network attacks
Answer: A

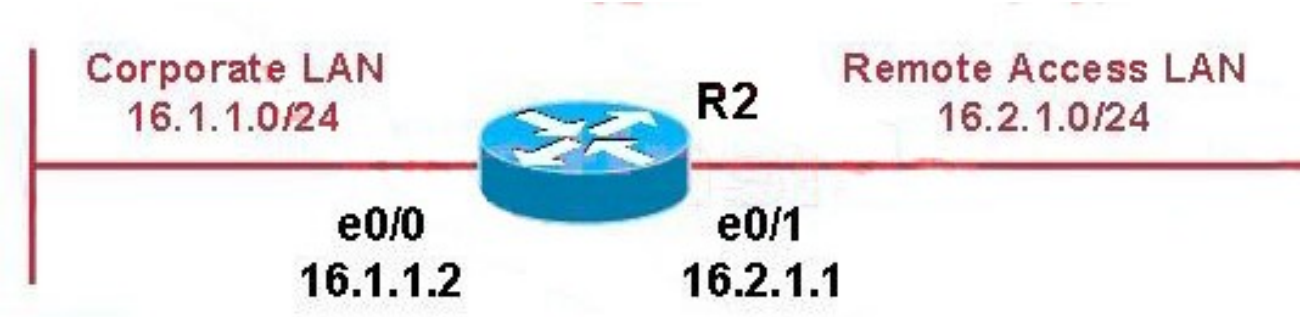
6. Which building blocks make up the Adaptive Threat Defense phase of Cisco SDN strategy?
A. VoIP services, NAC services, Cisco IBNS
B. network foundation protection, NIDS services, adaptive threat mitigation services
C. firewall services, intrusion prevention, secure connectivity
D. firewall services, IPS and network antivirus services, network intelligence
E. Anti-X defense, NAC services, network foundation protection
Answer: D

7. Why is TACACS+ the preferred AAA protocol to use with Cisco device authentication?
A. TACACS+ encryption algorithm is more recent than other AAA protocols
B. TACACS+ has a more robust programming interface than other AAA protocols
C. TACACS+ was initially developed as open-source software
D. TACACS+ provides true AAA functional separation and encrypts the entire body of the packet
E. TACACS+ maintains authentication information in the local database of each Cisco IOS router
F. TACACS+ combines authentication and authorization to provide more robust functionalities
Answer: D

8. Which method does a Cisco router use for protocol type IP packet filtering?
A. inspection rules
B. standard ACLs

C. security policies
D. extended ACLs
Answer: D

9. Referring to the network diagram shown, which ACL entry will block any Telnet Client traffic from the Corporate LAN to any Telnet Servers on the Remote Access LAN?



A. access-list 190 deny tcp any eq 23 16.2.1.0 0.0.0.255
B. access-list 190 deny tcp 16.1.1.0 0.0.0.255 eq 23 16.2.1.0 0.0.0.255 eq 23
C. access-list 190 deny tcp any 16.1.1.0 0.0.0.255 eq 23
D. access-list 190 deny tcp any 16.2.1.0 0.0.0.255 eq 23
E. access-list 190 deny tcp 16.2.1.0 0.0.0.255 eq 23 16.1.1.0 0.0.0.255 eq 23
Answer: D

10. What two tasks should be done before configuring SSH server operations on Cisco routers? (Choose two.)
A. Upgrade routers to run a Cisco IOS Release 12.1(1)P image.
B. Upgrade routers to run a Cisco IOS Release 12.1(3)T image or later with the IPsec feature set.
C. Ensure routers are configured for external ODBC authentication.
D. Ensure routers are configured for local authentication or AAA for username and password authentication.
E. Upgrade routers to run a Cisco IOS Release 11.1(3)T image or later with the IPsec feature set.
Answer: BD