

Exam : Cisco 642-552

**Title : Cisco® Securing Cisco
Network Devices Exam**

Version : Demo

Important Note, Please Read Carefully

Other TestInside products

[All TestInside.com IT Exam Products](#)

Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[TestInside Testing Engine](#)

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestInside and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to <http://www.TestInside.com>
2. Log in the **Member Center**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

Feedback

If you spot a possible improvement then please let us know. We always interested in improving product quality.

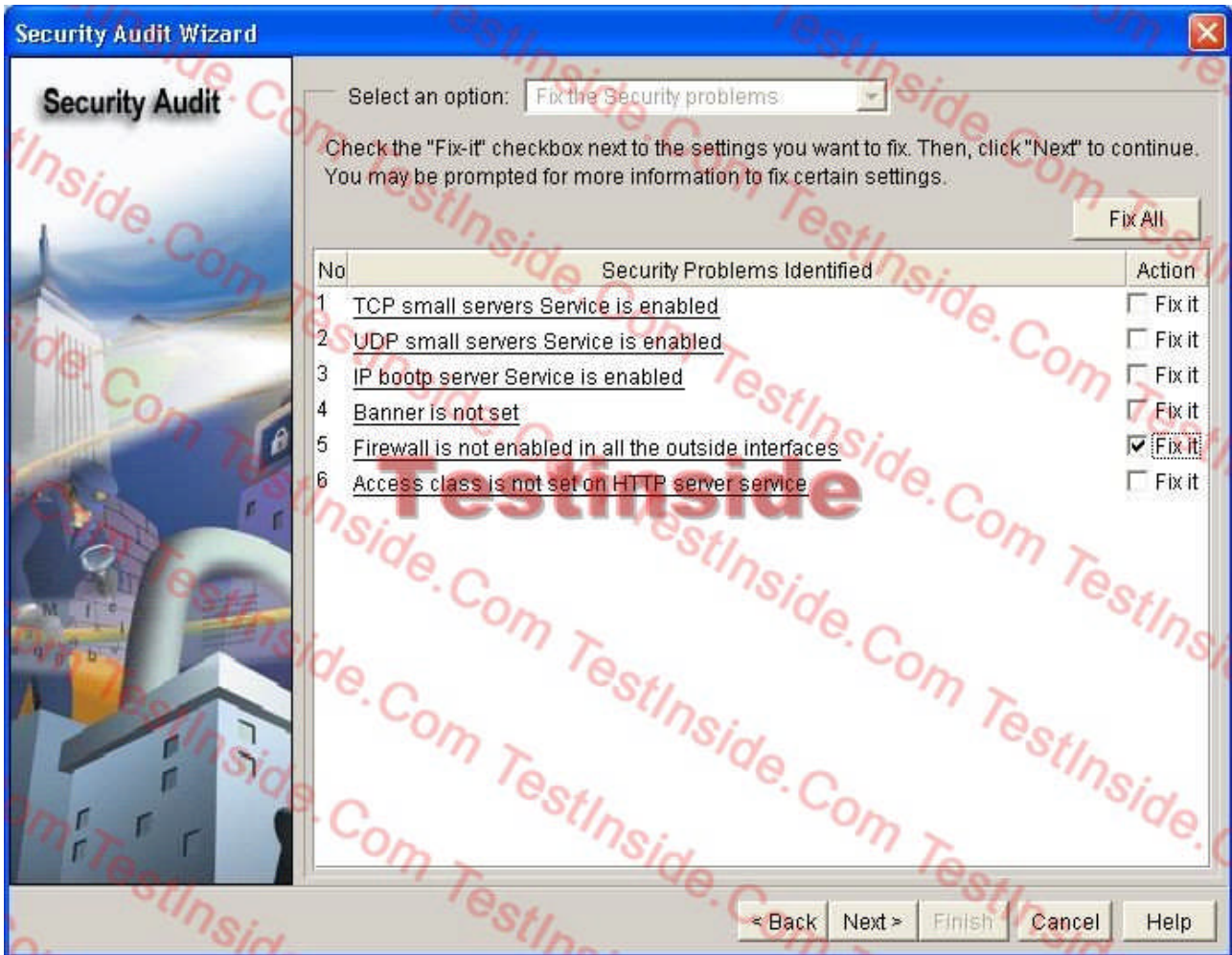
Feedback should be send to sales(at)TestInside.com. You should include the following: Exam number, version, page number, question number, and your login Account.

Our experts will answer your mail promptly.

Explanations

This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact sales(at)TestInside.com.

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

11. The figure contains a sample configuration using Cisco IOS commands. Which Cisco IOS command or setting does the configuration need to get SSH to work?

```
Router# config t
Router(config)# ip domain-name cisco.com
Router(config)# crypto key zeroize rsa
Router(config)# ip ssh timeout 120
Router(config)# ip ssh authentication-retries 4
Router(config)# line vty 0 4
Router(config)# no transport input telnet
Router(config)# transport input ssh
Router(config)# end
Router#
```

- A. add the transport input telnet ssh Cisco IOS command after the line vty 0 4 Cisco IOS command
- B. add the transport output ssh Cisco IOS command after the line vty 0 4 Cisco IOS command
- C. set the SSH timeout value using the ip ssh timeout 60 Cisco IOS command
- D. add the crypto key generate rsa general-keys modulus 1024 Cisco IOS command
- E. set the SSH retries value using the ip ssh authentication-retries 3 Cisco IOS command

Answer: D

12. Network administrators have just configured SSH on their target router and have now discovered that an intruder has been using this router to perform a variety of malicious attacks. What have they most likely forgotten to do and which Cisco IOS commands do they need to use to fix this problem on their target router?

- A. forgot to reset the encryption keys using the crypto key zeroize rsa Cisco IOS global configuration command
- B. forgot to close port 23 and they need to issue the no transport input telnet Cisco IOS global configuration command
- C. forgot to disable vty inbound Telnet sessions and they need to issue the line vty 0 4 and the no transport input telnet Cisco IOS line configuration commands
- D. forgot to restrict access to the Telnet service on port 23 using ACLs and they need to issue the access-list 90 deny any log Cisco IOS global configuration command, and the line vty 0 4 and access-class 90 in Cisco IOS line configuration commands

Answer: C

13. Which security log messaging method is the most common message logging facility and why?

- A. SNMP traps, because the router can act as an SNMP agent and forward SNMP traps to an external SNMP server
- B. buffered logging, because log messages are stored in router memory and events are cleared whenever

the router is rebooted

- C. console logging, because security messages are not stored and do not take up valuable storage space on network servers
- D. syslog, because this method is capable of providing long-term log storage capabilities and supporting a central location for all router messages
- E. logging all events to the Cisco Incident Control System to correlate events and provide recommended mitigation actions

Answer: D

14. What is a syslog configuration oversight that makes system event logs hard to interpret and what can be done to fix this oversight?

- A. The system time does not get set on the router, making it difficult to know when events occurred. Recommend that an NTP facility be used to ensure that all the routers operate at the correct time.
- B. Third-party flash memory gets installed and doesn't provide easily understandable error or failure codes. Only Cisco-authorized memory modules should be installed in Cisco devices.
- C. The syslog message stream does not get encrypted and invalid syslog messages get sent to the syslog server. Encrypt the syslog messages.
- D. The syslog messages filter rules did not get configured on the router, resulting in too many unimportant messages. Configure syslog messages filter rules so that low-severity messages are blocked from being sent to the syslog server and are logged locally on the router.

Answer: A

15. What are two security risks on 802.11 WLANs that implement WEP using a static 40-bit key with open authentication? (Choose two.)

- A. The IV is transmitted as plaintext, and an attacker can sniff the WLAN to see the IV.
- B. The challenge packet sent by the wireless AP is sent unencrypted.
- C. The response packet sent by the wireless client is sent unencrypted.
- D. WEP uses a weak-block cipher such as the Data Encryption Algorithm.
- E. One-way authentication only where the wireless client does not authenticate the wireless-access point.

Answer: AE

Testinside

Testinside.com was founded in 2002. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially [Adobe](#), [Apple](#), [Citrix](#), [Comptia](#), [EMC](#), [HP](#), [Juniper](#), [LPI](#), [Nortel](#), [Oracle](#), [SUN](#), [Vmware](#) and so on. And help you pass any IT Certification exams at the first try.

English	<u>http://www.testinside.com</u>
Chinese (Traditional)	<u>http:// www.testinside.net</u>
Chinese (Simplified)	<u>http:// www.testinside.cn</u>