



642-503

(Securing Networks with Cisco Routers and Switches)

Document version:1 04 11

Important Note About 642-503 PDF

techeXams' **642-503 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

Which of these statements is correct regarding user setup on ACS 4.0?

- A. In the case of conflicting settings, the settings at the group level override the settings configured at the user level.
- B. A user can belong to more than one group.
- C. The username can contain characters such as “#” and “?”.
- D. By default, users are assigned to the default group.
- E. The ACS PAP password cannot be used as the CHAP password also.

Answer: D

Question: 2

Which two commands are used to only allow SSH traffic to the router Eth0 interface and deny other management traffic (BEEP, FTP, HTTP, HTTPS, SNMP, Telnet, TFTP) to the router interfaces? (Choose two.)

- A. interface eth0
- B. control-plane host
- C. policy-map type port-filter policy-name
- D. service-policy type port-filter input policy-name
- E. management-interface eth0 allow ssh
- F. line vty 0 5 transport input ssh

Answer: B, E

Question: 3

Exhibit:

```
aaa new-model
aaa authentication login default group tacacs
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
enable password TeSt_123
ip auth-proxy name pxy http
ip auth-proxy auth-proxy-banner
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip auth-proxy pxy
no ip http server
tacacs-server host 192.168.123.14
tacacs-server key cisco
! Output omitted
```

Refer to the exhibit. Why is the Cisco IOS Firewall authentication proxy not working?

- A. The aaa authentication auth-proxy default group tacacs+ command is missing in the configuration.
- B. The router local username and password database is not configured.
- C. Cisco IOS authentication proxy only supports RADIUS and not TACACS+.
- D. HTTP server and AAA authentication for the HTTP server is not enabled.
- E. The AAA method lists used for authentication proxy should be named "pxy" rather than "default" to match the authentication proxy rule name.

Answer: D

Question: 4

When troubleshooting site-to-site IPsec VPN on Cisco routers, you see this console message:

%CRYPTO-6-IKMP_SA_NOT_OFFERED: Remote peer %15i responded with attribute [chars] not offered or changed Which configuration should you verify?

- A. the crypto ACL
- B. the crypto map
- C. the IPsec transform set
- D. the ISAKMP policies
- E. the pre-shared key

F. the DH group

Answer: D

Question: 5

Match the ACS 4.0 component on the left to the correct function on the right.

NAFs	used to ensure that every endpoint conforms to the security policy before being granted access to the network (NAC)	Place Here
NAPs	used to send VLAN assignment information to the NAD	Place Here
RACs	used to define flexible network device restriction policies	Place Here
Posture Validation Policy	used to classify an access request and map it to a profile	Place Here

Answer:

NAFs	used to ensure that every endpoint conforms to the security policy before being granted access to the network (NAC)	Posture Validation Policy
NAPs	used to send VLAN assignment information to the NAD	RACs
RACs	used to define flexible network device restriction policies	NAFs
Posture Validation Policy	used to classify an access request and map it to a profile	NAPs

Question: 6

When verifying Cisco IOS IPS operations, when should you expect Cisco IOS IPS to start loading the signatures?

- A. immediately after you configure the ip ips sdf location flash:filename command
- B. immediately after you configure the ip ips sdf builtin command
- C. after you configure a Cisco IOS IPS rule in the global configuration
- D. after traffic reaches the interface with Cisco IOS IPS enabled
- E. when the first Cisco IOS IPS rule is enabled on an interface
- F. when the SMEs are put into active state using the ip ips name rule-name command

Answer: E

Question: 7

Exhibit:

```
R1#show ip ips all
Configured SDF Locations:
flash:/128MB.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 00:50:03 UTC Aug 22 2006
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is enabled
Total Active Signatures: 0
Total Inactive Signatures: 0
IPS Rule Configuration
IPS name test
R1#
```

Refer to the exhibit. Why is the Total Active Signatures count zero?

- A. The 128MB.sdf file in flash is corrupted.
- B. IPS is in fail-open mode.
- C. IPS is in fail-closed mode.
- D. IPS has not been enabled on an interface yet.
- E. The flash:/128MB.sdf needs to be merged with the built-in signatures first.

Answer: D

Question: 8

When configuring FPM, what should be the next step after the PHDFs have been loaded?

- A. Define a stack of protocol headers.
- B. Define a traffic policy.
- C. Define a service policy.
- D. Define a class map of type "access-control" for classifying packets.
- E. Reload the router.
- F. Save the PHDFs to startup-config.

Answer: A

Question: 9

Exhibit:

```
ip ips name MYIPS
!
interface GigabitEthernet0/1
ip address 10.1.1.16 255.255.255.0
ip ips MYIPS in
!
```

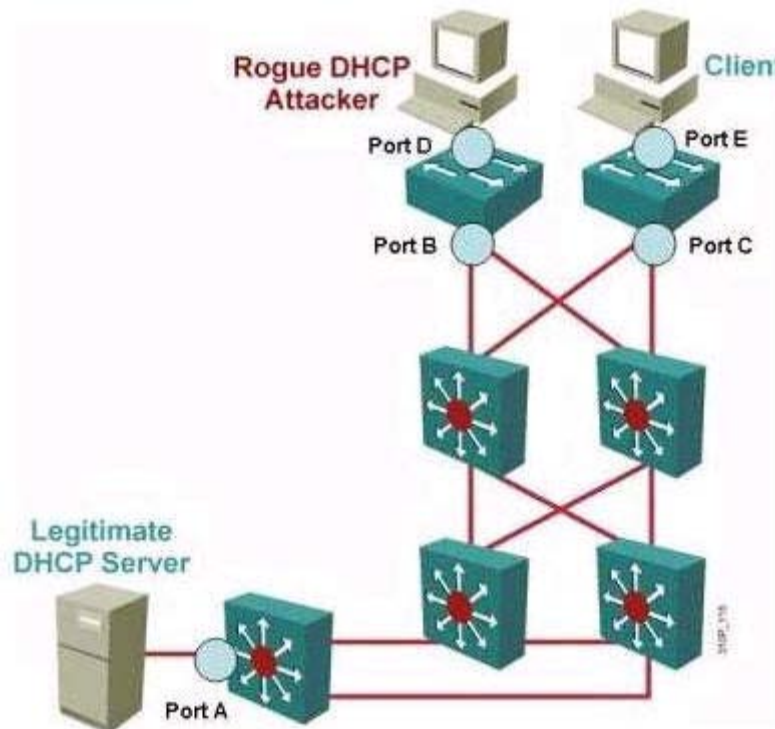
Refer to the exhibit. Which two statements are correct? (Choose two.)

- A. Cisco IOS IPS will fail-open.
- B. The basic signatures (previously known as 128MB.sdf) will be used if the built-in signatures fail to load.
- C. The built-in signatures will be used.
- D. SDEE alert messages will be enabled.
- E. syslog alert messages will be enabled.

Answer: A, C

Question: 10

Exhibit: Refer to the exhibit. When you configure DHCP snooping, which ports should be configured as trusted?



- A. port A only
- B. port E only
- C. ports B and C
- D. ports A, B, and C
- E. ports B, C, and E
- F. ports A, B, C, and E

Answer: D

Get Full Version of Exam 642-503 PDF Q&A

techeXams presents authentic, genuine and valid study material, which promise 100% success in very first attempt. To take optimal results for 642-503 exam, you need to buy full version of 642-503 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 642-503 questions and answers by visiting URL

["http://www.techexams.ws/exams/642-503.do"](http://www.techexams.ws/exams/642-503.do)