



www.chinatag.com

CHINATAG

**642-501
(SECUR)**

Securing Cisco IOS Networks

Q&A
DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

Section B

QUESTION NO: 1

What command configures the amount of time CBAC will wait for a TCP session to become established before dropping the connection in the state table?

- A. ip inspect global syn-establish (seconds)
- B. ip inspect tcp global syn-time (seconds)
- C. ip inspect global tcp syn (seconds)
- D. ip inspect tcp synwait-time (seconds)

Answer: D

Explanation:

Use the IOS Firewall global configuration mode command ip inspect tcp synwait-time (seconds) command to set the CBAC timeout value for TCP session establishment. The default is 30 seconds.

QUESTION NO: 2

How do you enable the Nagle algorithm on an IOS router?

- A. ip nagle
- B. service nagle
- C. enable service nagle
- D. enable ip nagle

Answer: B

Explanation:

Use the global configuration mode command service nagle to enable the TCP congestion Nagle algorithm. The Nagle algorithm attempts to bunch traffic into fewer TCP packets, thus saving on bandwidth. This command is disabled by default.

QUESTION NO: 3

What is the router IOS command to clear all IPSEC SA's?

- A. clear crypto ipsec sa
- B. clear crypto ipsec sa all
- C. clear crypto sa
- D. clear crypto ipsec sa *

Answer: C

Explanation:

Clear all IPSEC Security Associations on a router with the clear crypto sa command.

QUESTION NO: 4

What OSI layers can CBAC filter on? Select all that apply.

- A. layer 4
- B. layer 3
- C. layer 2
- D. layer 7

Answer: A, B, D

Explanation:

Access lists can filter traffic based on layer 3 and layer 4 information, while CBAC can filter traffic based on layer 3, 4, and 7 (application layer) information.

QUESTION NO: 5

How much disk space is required to install AAA CSACS 3.0 for Windows?

- A. 900mb
- B. 100mb
- C. 250mb
- D. 500mb

Answer: C

Explanation:

Installation of CSACS 3.0 on a Windows server will need at least 250Mb of disk space for installation, more if the user database will be stored on the machine.

QUESTION NO: 6

What are the ACL number ranges for IP standard ACL's? Select all that apply.

- A. 1-99
- B. 100-199
- C. 1300-1999
- D. 800-1299

Answer: A, C

Explanation:

IP standard access lists can be numbered from 1-99 or from the expanded range of 1300-1999.

QUESTION NO: 7

Which of the following correctly applies ACL 101 inbound on an interface?

- A. ip access-class 101 inbound
- B. ip access-group 101 in
- C. ip access-list 101 in
- D. ip access-range 101 inbound
- E. ip access-group 101 inbound
- F. ip access-list 101 inbound
- G. ip access-class 101 in
- H. ip access-range 101 in

Answer: B

Explanation:

After creating an access list, you must apply it to an interface with the access-group command in interface configuration mode, and specify the direction to monitor traffic with the in or out keyword.

QUESTION NO: 8

Which of the following is NOT supported by CSACS 3.0?

- A. Radius/Tacacs+ secret keys
- B. installation on Windows NT
- C. SSL
- D. HTTP

Answer: C

Explanation:

You cannot use SSL to administratively connect to the CSACS AAA server in version 3.0, but you can in 3.1 and later.

QUESTION NO: 9

Which of the following router commands will prevent a router from giving an attacker a valid IP address via DHCP?

- A. no tcp-dhcp-servers
- B. no service dhcp
- C. no ip dhcp servers
- D. no dhcp server

Answer: B

Explanation:

The IOS command `no service dhcp` will prevent the router from responding to DHCP requests on all interfaces. You cannot disable only certain interfaces, if you need to allow this service, apply proper ACL's.

QUESTION NO: 10

By default, where does the IOS Firewall IDS engine send alarms to?

- A. CBAC
- B. Director platform
- C. CSACS
- D. DMZ
- E. syslog server

Answer: E

Explanation:

If an IDS info or attack signature is configured to generate an alarm, if no notification method is specified with the `ip audit notify` command, by default the IDS engine will send it to the syslog server.

QUESTION NO: 11

Which of the following configurations restricts telnet access to a router by requiring the password cisco?

- A. `line vty 0 4`
`login cisco`
- B. `line vty 0 4`
`set password cisco`
`login`
- C. `line vty 0 4`
`password cisco`
`login`
- D. `line vty 0 4`
`set login`
`set password cisco`

Answer: C

Explanation:

To restrict telnet access to a Cisco router, you must configure the virtual terminal lines (VTY) that telnet uses. Require a login with the `login` line configuration command (enabled on vty lines by default). You must also set a password with the `password (password)` line configuration command, or remote user telnet connections will be refused, informing them that a login is required, but no password is set.