



www.chinatag.com

CHINATAG

CheckPoint 156-510

VPN-1/FireWall-1 Management III – NG
CCSE

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.

QUESTION NO: 1

You can tell if CPMAD is enabled because you see the message

"FireWall-1: Starting cpmad (Malicious Activity Detection)"

when you perform a fwstart. True or false?

- A. False
- B. True

Answer: A

QUESTION NO: 2

When installing FW-1 on a Windows NT platform, what state should IP forwarding be in for correct FW-1 operation?

- A. Enabled
- B. Disabled

Answer: A

QUESTION NO: 3

What is true about detecting "blocked connection port scanning"?

- A. It requires less memory than general port scanning
- B. It is less secure than general port scanning
- C. It is more secure than general port scanning
- D. It requires more memory than general port scanning

Answer: A, B

QUESTION NO: 4

In a load sharing MEP environment accessed by secuRemote. What is true about gateway selection?

- A. SecuRemote will choose the gateway closest to the server
- B. SecuRemote will use the first gateway to respond
- C. SecuRemote will chose the gateway randomly

D. SecuRemote will prefer its primary gateway if both respond

Answer: C

QUESTION NO: 5

Which two types of overlapping encryption domains are supported by FW-1?

- A. Partial overlap
- B. Full overlap
- C. Proper subset
- D. Partial subset

Answer: B, C

QUESTION NO: 6

What does LDAP stand for?

- A. Link level Direct Access Process
- B. Layered Directory Administration Protocol
- C. Layer Dependent Administration process
- D. Lightweight Directory Access Protocol

Answer: D

QUESTION NO: 7

By default a Windows NT platform enables both TCP/IP and IPX. What does FW-1 do with any IPX traffic?

- A. Logs it, then drops it
- B. Allows it through without being inspected
- C. Drops all traffic regardless
- D. Inspects the traffic and decide whether to allow it through

Answer: B

QUESTION NO: 8

When using IP pools for MEP VPN access, where would you specify the pool to be used for a particular gateway?

- A. The NAT screen of the gateway's properties configuration
- B. The ADVANCED screen of the gateway's properties configuration
- C. The VPN screen of the gateway's properties screen
- D. The TOPOLOGY screen of the gateway's properties configuration

Answer: A

QUESTION NO: 9

What is the maximum limit to the number of secondary management modules allowed?

- A. No limit
- B. 4
- C. 2
- D. 1
- E. 8

Answer: A

QUESTION NO: 10

What is a land attack?

- A. It causes incomplete TCP connections
- B. It involves gaining access by imitating an authorized IP address
- C. It involves scanning for ports on an IP address that will allow access
- D. It causes a server to send packets to itself

Answer: D

QUESTION NO: 11

If CPMAD terminates, how can you restart it?

- A. By using the GUI log client
- B. It automatically starts itself
- C. By using fw cpmadstart
- D. By using fwstop/fwstart

Answer: D

QUESTION NO: 12

What is true when using SEP high availability encryption topologies?

- A. Gateways must use the same FW-1 build level
- B. All of these
- C. You must use a distributed installation of VPN-1/FW-1
- D. Gateways must use the same platform and OS
- E. Gateways must run identical policies

Answer: B

QUESTION NO: 13

In a resilient MEP topology, what mechanism can be used by SecuRemote to determine that the primary gateway is still available?

- A. TCP Ping
- B. TCP keepalives
- C. RDP status queries
- D. UDP ping

Answer: C

QUESTION NO: 14

Which are two network related conditions required by high availability in SEP VPN's?

- A. The gateways must be synchronized
- B. Traffic must be redirected correctly to the backup gateway when the primary gateway fails
- C. The gateways must use identical MAC addresses
- D. NTP (network time protocol) must be configured between both gateways

Answer: A, B

QUESTION NO: 15

How much memory is reserved for the VPN-1/FW-1 kernel on a Nokia platform?

- A. 5 MB
- B. 15 MB
- C. 3 MB
- D. 10 MB

Answer: A

QUESTION NO: 16

Which of the following should be disabled in a Windows NT platform when installing FW-1?

- A. WINS
- B. RPC
- C. NetBIOS
- D. All of them
- E. DHCP relay

Answer: D

QUESTION NO: 17

CPMAD will try to connect to the LEA server a number of times before giving up. What are the default values for the number of connection attempts and the time interval between them?

- A. 20 times with 30secs between attempts
- B. 10 times with 60secs between attempts
- C. 5 times with 60secs between attempts
- D. 10 times with 10secs between attempts

Answer: B

QUESTION NO: 18

When making changes to users in an LDAP server using the policy editor user manager, when will the changes take effect?

- A. After the user database is downloaded
- B. When you log out of policy editor
- C. After a policy download
- D. When cache times out

Answer: A, C, D

QUESTION NO: 19

Addresses allocated from an IP pool remain allocated for a configurable period, even after all connections to that address are closed. What is the default time before the address is returned to the pool?

- A. 120 mins
- B. 180mins
- C. 30 mins
- D. 60 mins

Answer: D

QUESTION NO: 20

How often will SecuRemote check for the availability of a VPN gateway by default?

- A. 60 secs
- B. 120 secs
- C. 30 secs
- D. 90 secs

Answer: A

QUESTION NO: 21

What does the -all option on the fw tab command specify?

- A. Display table information pertaining to all targets
- B. Display every table for the target
- C. Nothing, it is invalid, it should be -a
- D. Display every entry in the table

Answer: A

QUESTION NO: 22

If you are running CPMAD on a Solaris machine, and you see the following messages:

"Connection broken while communicating with localhost for ssl_opsec"

and

"Connection broken while communicating with localhost for fwn1_opsec".

What is the problem?

- A. There is already an instance of CPMAD running
- B. CPMAD is wrongly configured
- C. Nothing is wrong
- D. The machine is not a management module

Answer: C

QUESTION NO: 23

When using SecuRemote connections to an MEP VPN, if the primary gateway goes down the connection will be maintained on the backup gateway.

True or false?

- A. True
- B. False

Answer: B

QUESTION NO: 24

Please look at the exhibit, which is a sample output from a "fw ctl pstat" command.

What is the amount of memory allocated for the use by such entities as the state tables?

- A. 3072000 bytes
- B. 103246 bytes
- C. 62857216 bytes
- D. 4171460 bytes

Answer: D

QUESTION NO: 25

When configuring CPMAD, the global clean interval time setting overrides the individual time interval setting for a particular attack. True or false?

- A. True
- B. False

Answer: B

QUESTION NO: 26

Which VPN-1/FW-1 feature is designed to scan the log file, and alert the administrator to a suspicious sequence of events?

- A. Management module
- B. Anti spoof
- C. CPMAD
- D. FW-1 alerts

Answer: C

QUESTION NO: 27

What is necessary before you can delete an organization from an LDAP server?

- A. The branch of the tree must be empty
- B. You must take the LDAP server offline
- C. There must be no active users associated with that organization
- D. There are no specific requirements other than the correct access rights

Answer: A

QUESTION NO: 28

On a Windows platform, you can enable VPN and IKE logging by setting an environment variable. What is the command to do that?

- A. Setenv VPN_DEBUG 1
- B. Setenv VPN_DEBUG 0
- C. Set VPN_DEBUG=0
- D. Set VPN_DEBUG=1

Answer: D