# Checkpoint 156-510

## CheckPoint 156-510.4 Check Point NG with Application Intelligence - Management III CCSE

# Practice Test

Version 2.0

**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 of 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**

**QUESTION NO: 29**

What port does LEA use?

A. 18182
B. 18184
C. 18181
D. 18183

**Answer: B**

**QUESTION NO: 30**

On a UNIX platform what is the value given to the CPDIR environment variable?

A. /etc/fw
B. <DRIVE>:PROGRAM FILES\CHECKPOINT\CPSHARED\NG
C. $FWDIR/bin
D. /opt/CPShared//NG

**Answer: D**

**QUESTION NO: 31**

In an overlapping encryption domain topology, a SecuRemote connection may have to pass through an outer gateway to get to the destination gateway. What happens to the connection at the first gateway?

A. The gateway creates a dynamic rule to allow the connection
B. The connection is automatically passed on without being encrypted due to implied rules
C. The connection is decrypted before being passed on
D. The rulebase is checked and the gateway will pass the connection through if it is allowed

**Answer: D**

**QUESTION NO: 32**

When using SecuRemote connections to a SEP VPN, if the primary gateway goes down the connection will be maintained on the backup gateway.
True or false?

A. True

B. False

**Answer: A**

**QUESTION NO: 33**

Which command would you use to inhibit all connections to and from IP address 10.1.1.1 for 5 minutes?

A. fw sam -t 5 -I src 10.1.1.1
B. fw sam -t 5 -i any 10.1.1.1
C. fw sam -t 300 -i any 10.1.1.1
D. fw sam -i 300 -t any 10.1.1.1

**Answer: C**

**QUESTION NO: 34**

Which of the following is NOT a valid configuration statement when setting up CPMAD to monitor for Syn attacks?

A. MAD_syn_attack_mode = enable
B. MAD_syn_attack_action = alert
C. MAD_syn_attack_repititions = 100
D. MAD_syn_attack_resolution = 10
E. MAD_syn_attack_time_interval = 60

**Answer: A**

**QUESTION NO: 35**

In a Solaris platform, there are scripts that will be started automatically. When installing FW-1 it is recommended in some cases that you replace the upper case S in the script name with a lower cases.
Why is this?

A. A script will only start during boot if it starts with a lower cases
B. Solaris is case sensitive
C. The scripts with a lower case s will be started with a lower priority
D. A script will only start during boot if it starts with an upper cases.

**Answer: B,D**

**QUESTION NO: 36**

Which command opens a connection to an LDAP server, binds, and performs a search, returning one or more entries as a result?

A. fw ldapmodify
B. ldapsearch
C. fw ldapcompare
D. fw ldapfind
E. fw ldapsearch

**Answer: B**

**QUESTION NO: 37**

It would improve FW-1 performance on a Windows NT platform if the "performance boost for foreground applications" setting is increased?

A. False
B. True

**Answer: A**

**QUESTION NO: 38**

Where are MAD errors logged?

A. $FWDIR/bin/cpmad.err
B. $FWDIR/log/cpmad.err
C. $FWDIR/alert/cpmad.err
D. $FWDIR/conf/cpmad.err

**Answer: B**

**QUESTION NO: 39**

Which of the following security risks is NOT classed as an internal risk?

A. Accidental file deletion
B. Social engineering of employees
C. Disgruntled employees
D. Improper access to confidential information
E. SPAM and mail relaying

**Answer: E**

**QUESTION NO: 40**

When using IP pools in an MEP encryption environment, what is true?

A. The pools in each gateway should not use overlapping IP addresses
B. The pools in each gateway should use identical IP addresses
C. The pools should be taken from the same routable network
D. The pools should be from different routable networks

**Answer: A,D**

**QUESTION NO: 41**

On a Solaris FW-1 platform, system hardening includes disabling all unnecessary services on the operating system. What command can you use to display services that are active?

A. #grep -v "^#" /etc/inetd.conf
B. fw ctl serv
C. fw ctl pstat
D. show services

**Answer: A**

**QUESTION NO: 42**

OPSEC application communication requires SIC to be correctly set up. True or false?

A. True
B. False

**Answer: A**

**QUESTION NO: 43**

When using high availability management modules, if you synchronize configuration files what does this entail?

A. Only the changed items are synchronized
B. You are asked which sections you want to synchronize
C. The whole database is synchronized
D. Only a subsection of the database is synchronized, eg NAT rules or global properties

**Answer: C**

**QUESTION NO: 44**

Which command is used to enable the high availability feature on a gateway?

A. cpharun
B. cphastart
C. cpstartha
D. fw hastart

**Answer: B**

**QUESTION NO: 45**

What is the function of a UFP server?

A. It provides QoS facilities
B. It provides a virus checking capability
C. It supports a user database
D. It maintains a list of URL's to be checked against by FW-1

**Answer: D**

**QUESTION NO: 46**

How do you make a secondary management module function as a primary?

A. On the primary management module select Policy>management high availability, then select "change to standby"
B. On the secondary management module select Policy>management high availability, then select "change to active"

C. Perform "fw hamprim" on the secondary management module

D. Open the Policy editor GUI onto the secondary management module, select "Change to active"

**Answer: A,D**

**QUESTION NO: 47**

What is the name given to the globally unique ID associated with an entry in an LDAP sever?

A. Domain name

B. Distinguished name

C. Global property

D. Distinguished number

**Answer: B**

**QUESTION NO: 48**

In a fully overlapping encryption domain assigned to two gateways, SecuRemote tries to connect to both gateways. What is true about what happens next?

A. SecuRemote will use the first gateway to respond

B. SecuRemote will prefer its primary gateway if both respond

C. SecuRemote will choose the gateway closest to the server

D. SecuRemote will chose the gateway with the lowest cost

**Answer: A**

**QUESTION NO: 49**

What is the recommended ratio between the CPMAD values for resolution and time_interval?

A. 1:4

B. 1:10

C. 1:5

D. 1:2

**Answer: B**

**QUESTION NO: 50**

Which of the following are supported in conjunction with a load sharing SEP configuration?

A. None of these
B. FWZ encryption
C. FlloodGate-1
D. All of these

**Answer: A**

**QUESTION NO: 51**

The -u option on fwd designates that this enforcement module allows SecuRemote connections. This option is on by default, true or false?

A. False
B. True

**Answer: B**

**QUESTION NO: 52**

IP pools can be used in MEP configurations for what purpose?

A. To allow multiple connections from one client
B. To ensure that valid addresses are assigned to clients
C. To reserve connections for clients
D. To prevent asymmetric routing issues

**Answer: D**

**QUESTION NO: 53**

In a high availability management module situation, in normal circumstances what is true?

A. The primary module is limited to read only access, a secondary can grant read/write access
B. The primary and secondary modules can both grant read/write access
C. The primary and secondary modules are both limited to read only access once initialized
D. The primary module can grant read/write access, a secondary is limited tot read only access

**Answer: D**

**QUESTION NO: 54**

When displaying FW-1 statistics using the "fw ctl pstat" command, you may see negative values for kernel memory. What is true about this?

A. There is a memory fault
B. FW-1 is currently not active
C. This does not indicate a problem
D. Memory is being over utilized

**Answer: C**

**QUESTION NO: 55**

To get the most efficient operation, you should place the rules most often matched at the bottom of the rulebase, and the rules least often matched at the top. True or false?

A. False
B. True

**Answer: A**

**QUESTION NO: 56**

Which default ports are used by LDAP?

A. Port 636 for a standard connection
B. Port 389 for a standard connection
C. Port 389 for a SSL connection
D. Port 636 for a SSL connection

**Answer: B,D**

**QUESTION NO: 57**

What is the default value for the timeout on cached users, applied when using an LDAP server as a user database?

A. 300 secs
B. 0 secs (ie no caching)

C. 600 secs
D. 900 secs

**Answer: D**

**QUESTION NO: 58**

Which two CPMAD parameters are directly used to determine if an attack is taking place?

A. Resolution
B. Action
C. Time_interval
D. Repetitions
E. Mode

**Answer: C,D**

**QUESTION NO: 59**

In a load sharing SEP configuration, what mechanism is used to ensure that each gateway sees all the traffic it needs to?

A. The gateway cluster IP address is used
B. The receiving gateway forwards the packets to the others
C. All packets are broadcast
D. Each gateways is sent the packets separately

**Answer: A**

**QUESTION NO: 60**

Which is the correct format on a Windows platform to enable debug mode in fwd on an enforcement module only server?

A. fwd -d -n
B. fwd -d
C. fw d -d -n
D. fw d -d

**Answer: D**

**QUESTION NO: 61**

When configuring an MEP VPN facility, you would specify a backup gateway in the VPN screen of the gateway properties window. What could be the reason for the backup gateway not being available in the drop down list?

A. The backup gateway is already a backup to another gateway
B. The backup gateway is not running VPN-1
C. The backup gateway is not defined as an internal object on this gateway
D. The backup gateway is not defined as an external object on this gateway

**Answer: C**

**QUESTION NO: 62**

In a high availability management module environment, each management module can function as an individual certificate authority. True or false?

A. True
B. False

**Answer: B**

**QUESTION NO: 63**

Which three files can be generated by a Unix core dump?

A. vmunix.
B. vmcore.
C. unixdump
D. core

**Answer: A,B,D**

**QUESTION NO: 64**

What is NOT true when using MEP encryption topologies?

A. Gateways must use the same FW-1 build level
B. Gateways must use the same management module
C. You must use a distributed installation of VPN-1/FW-1
D. Gateways must run identical policies

**Answer: D**

**QUESTION NO: 65**

What is another name for an LDAP server?

A. Account server
B. DN Unit
C. User server
D. Account unit

**Answer: D**

**QUESTION NO: 66**

Exhibit missing.

Please look at the exhibit, which is a sample output from a "fw ctl pstat" command. How many NAT operations have there been in an outgoing direction?

A. 20760405
B. 340
C. 312
D. 523

**Answer: C**

**QUESTION NO: 67**

Which file would you modify in order to enable and configure CPMAD?

A. $FWDIR/bin/cpmad_config.conf
B. $FWDIR/conf/cpmad.conf
C. $FWDIR/conf/cpmad_config.conf
D. $FWDIR//cpmad/config.conf

**Answer: C**

**QUESTION NO: 68**

For most efficient rulebase operation, which of the following objects would it be preferable to use if you have many contiguous addresses to translate using static NAT? Assume you could validly use any of them.

A. Network
B. Workstation
C. Range

**Answer: A**

**QUESTION NO: 69**

Where would it be best to locate a CVP server?

A. On an internal user lan network
B. On a firewalled gateway
C. On a separate isolated segment or DMZ
D. On a remote network

**Answer: C**

**QUESTION NO: 70**

What is the result of not configuring CPMAD with enough memory?

A. Some attacks will not be detected
B. It will automatically grab more memory
C. It will automatically flush out old events to create more memory
D. It will exit

**Answer: D**

**QUESTION NO: 71**

In a SEP HA environment not using load sharing, the external interfaces of each cluster member must have the same IP address. True or false?

A. False
B. True

**Answer: B**

**QUESTION NO: 72**

Which command would you use to copy a user database file into VPN-1/FW-1?

A. dbimport <filename>
B. fwm dbimport -s "o=city,c=country"
C. fwm dbexport <filename>
D. fwm dbimport -f <filename>

**Answer: D**

**QUESTION NO: 73**

When would you need to import the Checkpoint schema into an LDAP server?

A. If you use the severs management interface to update the LDAP database
B. Never, the LDAP standard caters for it
C. If you use Policy Editor to update the LDAP database
D. Always, when you use an LDAP server

**Answer: C**

**QUESTION NO: 74**

Which is designated the primary management module?

A. It is selected by priority numbers (1 is the highest priority)
B. The last management module installed
C. The first management module installed
D. It is chosen at random

**Answer: C**

**QUESTION NO: 75**

You do not need LDAP schema checking enabled if you want to use policy editor user manager to add a new LDAP user. True or false?

A. False
B. True

**Answer: A**

**QUESTION NO: 76**

On a Windows NT FW-1 system, how would you increase the amount of memory allocated to the kernel to 5MBytes?

A. Set the value of HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\FW1\Parameters\Memory to 5000000
B. Type "# zap -s _fwhmem $FWDIR/modules/fwmod.o 5000000"
C. Type "set fw:fwhmem=5000000"
D. Type"# echo "fwhmem?W500000" | adb -w /stand/vmnt"

**Answer: A**

**QUESTION NO: 77**

A collection of gateways that are synchronized in a VPN topology are called a ___________?

A. MEP
B. Gateway group
C. Gateway cluster
D. Gateway pool

**Answer: C**

**QUESTION NO: 78**

When using LDAP what may be a reason for a users password to be rejected?

A. The password does not contain a numeric character
B. The user is defined differently in the VPN-1/FW-1 user database
C. than in the LDAP server
D. The user is defined in both VPN-1/FW-1 and the LDAP server
E. The password is also used by someone else

**Answer: B**

**QUESTION NO: 79**

Which API is used by applications to write to the VPN-1/FW-1 log database?

A. ELA
B. EAL
C. LEA
D. LAA

**Answer: A**

**QUESTION NO: 80**

When are the statistics provided by the fw ctl pstat command reset?

A. After restarting FW-1
B. Whenever you purge the log file
C. On a reboot
D. On entering the command "fw ctl clear"

**Answer: A,C**

**QUESTION NO: 81**

You need to set the environment variable $FWDIR before running cpifno.
True or false?

A. True
B. False

**Answer: A**

**QUESTION NO: 82**

FW-1 does not support multi level proper subset encryption domains.
True or false?

A. False
B. True

**Answer: A**

**QUESTION NO: 83**

What is true about conflicting configuration parameters between a gateway cluster and a gateway defined as a member of that cluster?

A. Some gateway parameters override cluster parameters
B. Some cluster parameters override gateway parameters
C. The cluster configuration is overridden by the primary gateway parameters
D. All the gateway parameters remain intact

**Answer: B**

**QUESTION NO: 84**

If you are troubleshooting a SMTP security server problem, which file could be useful?

A. smtp.dmp
B. smtpd.log
C. asmtpd.log
D. cvp.conf

**Answer: C**

**QUESTION NO: 85**

Please look at the exhibit, which is a sample output from a "fw ctl pstat" command. There is a memory utilization problem here. True or false?

A. False
B. True

**Answer: A**

**QUESTION NO: 86**

Which is NOT a group of files that can be synchronized in a HA management environment?

A. Configuration database files
B. Install files
C. Fetch files
D. log files

**Answer: D**

**QUESTION NO: 87**

When SEP gateways are said to be synchronized, what exactly is synchronized between them?

A. Rulebase
B. User database
C. Objects database
D. State tables

**Answer: D**

**QUESTION NO: 88**

On which module(s) does CPMAD run?

A. An external server
B. The management module
C. The Checkpoint GUI
D. The enforcement module

**Answer: B**

**QUESTION NO: 89**

How many LDAP servers are supported by VPN-1/FW-1?

A. 1
B. 2, one primary and one backup
C. Unlimited
D. Up to 4

**Answer: C**

**QUESTION NO: 90**

When debugging a Unix based management server you could use the fwd -d command. True or false?

A. False

B. True

**Answer: A**

**QUESTION NO: 91**

Asymmetric routing can be a problem in which type of encryption domain topology?

A. Partial overlapping

B. Fully overlapping domains in gateways using hide mode NAT for all connections

C. none overlapped backup domains with internal links between the two

D. Proper subset

**Answer: C**

**QUESTION NO: 92**

What is the function of the "fw hastat <target>" command?

A. It forces failover of high availability gateways

B. It starts HA on high availability capable gateways

C. It provides operational status of high availability gateways

D. It is an invalid command, you should use cphaprob instead

**Answer: C**

**QUESTION NO: 93**

When you are logged into the active management server and viewing the high availability management screen, what icon is displayed if there is a recommendation or error that FW-1 wishes to bring to your attention?

A. A lightbulb

B. A red question mark

C. A red hash

D. A green tick

**Answer: A**

**QUESTION NO: 94**

Which of the following platforms cannot support CPMAD?

A. Win2000
B. None of these
C. Nokia IP530
D. Solaris
E. Win NT
F. Linux

**Answer: B**

**QUESTION NO: 95**

How would you perform a manual synchronization in a HA management module environment?

A. On the primary login and click on the "synchronize me" button of the HA management manager window
B. Perform the "fw hamansync" command
C. On the secondary login and click on the "synchronize me" button of the HA management manager window
D. On the primary use Policy editor > Policy > Management high availability > click on the "synchronize" button

**Answer: C,D**

**QUESTION NO: 96**

When starting FW-1 debugging, you may want to send all the output to a buffer, what command(s) would you use to do this?

A. fw ctl buffer -debug
B. fw ctl buf
fw ctl debug
C. fw ctl -b debug
D. fw ctl debug -buf

**Answer: D**

**QUESTION NO: 97**

On a Windows NT platform, the specified state of the OS memory strategy can impact the performance of FW-1. What is the default state for this?

A. Maximize throughput for network applications
B. Maximize throughput for file sharing
C. Maximize throughput for video applications
D. Maximize throughput for disk access

**Answer: B**

**QUESTION NO: 98**

In an LDAP database two entries cannot have the same common name (CN). True or false?

A. False
B. True

**Answer: A**

**QUESTION NO: 99**

If you want to receive debug information for HTTP or FTP security servers when debugging the firewall daemon, you must use the "fw debug fwd on" command. True or false?

A. True
B. False

**Answer: B**

**QUESTION NO: 100**

What are the three types of overlapping encryption domains?

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

**Answer: A,B,D**

**QUESTION NO: 101**

When using the cphaprob command to list the interfaces on the local machine and their status, which form would you use?

A. cphaprob -I
B. cphaprob if
C. cphaprob ports
D. cphaprob list if

**Answer: B**

**QUESTION NO: 102**

If you have previously started debugging on the firewall, how would you cancel debugging?

A. fw ctl debug 0
B. fw ctl debug can
C. fw ctl debug stop
D. fw ctl dbstop

**Answer: A**

**QUESTION NO: 103**

In a fully overlapping encryption domain, a SecuRemote client will encrypt with the first gateway to reply. All subsequent connections will remain with that gateway for a set period. How long is that period?

A. 60 secs
B. 5 mins
C. 10 mins
D. 30 secs

**Answer: A**

**QUESTION NO: 104**

Which is NOT a valid entity in the LDAP tree structure?

A. OU
B. C

C. CN
D. CU

**Answer: D**

**QUESTION NO: 105**

Checkpoint provides several command line utilities to assist with the integration of LDAP servers. Which of the following is NOT one of them?

A. ldapsearch
B. ldapcompare
C. ldapmodify
D. ldapfind

**Answer: D**

**QUESTION NO: 106**

If you have a Unix core dump, in which directory will the dump be created?

A. In the directory from which the executable that caused the dump is running
B. In the directory given by the command "# find / -name core"
C. In a directory named /dump
D. in the root directory

**Answer: A,B**

**QUESTION NO: 107**

What command would you use to check the current status of high availability gateways within a cluster?

A. cphaprob list
B. cphaprob report
C. cphaprob state
D. cphaprob register

**Answer: C**

**QUESTION NO: 108**

If you run the "fw debug fwd on" command, where is the output directed to?

A. The kernel buffer
B. The screen
C. To a file called $FWDIR/log/fwd.elg
D. To a file called $FWDIR/conf/fwd_output.log

**Answer: C**

**QUESTION NO: 109**

On a Unix system, what is the output from the command "# file core"

A. The size of the file named core
B. A textual listing of the contents of the file named core
C. The name of the executable that generated the core dump
D. The location of the file named core

**Answer: C**

**QUESTION NO: 110**

What is true about high availability management modules?

A. Primary and secondary modules can be on different platforms, but must run the same build of FW1
B. Primary and Secondary modules must be on the same platform
C. The active primary module cannot be manually switched to secondary
D. They are only supported on distributed installations

**Answer: B,D**

**QUESTION NO: 111**

Which command would you use to enable debugging of IKE only?

A. fw debug ikeon
B. fwm debug ikeon
C. vpn debug ikeon
D. vpn debug on ikeon

**Answer: C**

**QUESTION NO: 112**

In a proper subset encryption domain, to which gateway will SecuRemote attempt to create an encrypted connection?

A. SecuRemote will chose the gateway with the lowest cost
B. SecuRemote will prefer its primary gateway if both respond
C. SecuRemote will choose the gateway closest to the server
D. SecuRemote will use the first gateway to respond

**Answer: C**

**QUESTION NO: 113**

Which type of overlapping encryption domain can be described as one domain being entirely contained within another domain?

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

**Answer: C**

**QUESTION NO: 114**

Where can a User Authority Server be installed?

A. A Windows machine with just a FW-1 enforcement module installed
B. A Solaris machine with just a FW-1 management module installed
C. A Solaris or Windows machine with any FW-1 module installed
D. A Windows Domain Controller

**Answer: C,D**

**QUESTION NO: 115**

If VPN-1/FW-1 has a blue screen crash on a Windows NT platform, there is an extra file you should include in those sent to Checkpoint for analysis. Which is that extra file?

A. WINNT\system.dmp
B. WINNT\user.dmp
C. WINNT\memory.dmp
D. WINNT\core.dmp

**Answer: C**

**Explanation:**
The description and format of the event log differs from the format that is displayed when the computer is writing the Memory.dmp file, but the majority of the information is the same. Below is an example of the event log:
Event ID: 1001 Source: Save Dump Description: The computer has rebooted from a bugcheck. The bugcheck was : 0xc000021a (0xe1270188, 0x00000001, 0x00000000, 0x00000000). Microsoft Windows NT (v15.1381). A dump was saved in: C:\WINNT\MEMORY.DMP.

Reference: Microsoft Knowledge Base Article - 192463, Gathering Blue Screen Information After Memory Dump in Windows 2000 or Windows NT

**QUESTION NO: 116**

In the following DN, which part is the root?
CN= John Doe, ou= Sales, o= Acme Corp, C= US

A. Acme Corp
B. John Doe
C. Sales
D. US

**Answer: D**

**QUESTION NO: 117**

Which files are useful in the case of a Windows NT Dr. Watson error?

A. WINNT\memory.dmp
B. WINNT\drwtsn32.log
C. WINNT\system.dmp
D. WINNT\user.dmp

**Answer: A,B,D**

**QUESTION NO: 118**

Why is a sniffer a security risk?

A. It can create a DOS attack
B. It can cause a firewall to crash
C. It can emulate an authorized workstation
D. It can record traffic, which may include clear text passwords

**Answer: D**

**QUESTION NO: 119**

When exporting a user database using the "fw dbexport" command. What is the default file used?

A. $FWDIR/user/def_file
B. $FWDIR/conf/user_def_file
C. $FWDIR/bin/user_def_file
D. $FWDIR/conf/user_export_file

**Answer: B**

**QUESTION NO: 120**

How can you analyze a file captured by the fw monitor utility?

A. Snoop
B. Snort
C. Spock
D. Sniff

**Answer: A**

**QUESTION NO: 121**

What is the name of the protocol analyzer that ships with WindowsNT/SMS?

A. Tcpdump
B. Network monitor
C. Snoop
D. Sniffer

**Answer: B**

**QUESTION NO: 122**

From where would you enable load sharing in an MEP configuration?

A. Global properties > VPN-1 Net > Advanced then select "enable load sharing in MEP configuration"
B. Global properties > Remote Access > Advanced then select "enable load sharing in MEP configuration"
C. Cluster properties > general tab >, select "enable load sharing in MEP configuration"
D. Global properties > VPN-1 Pro > Advanced then select "enable load sharing in MEP configuration"

**Answer: D**

**QUESTION NO: 123**

How would FW-1 communicate securely with an LDAP server?

A. SIC
B. Certificates
C. RDP
D. SSL

**Answer: D**

**QUESTION NO: 124**

What is meant by a promiscuous mode network capture tool?

A. It can run on any platform
B. It can monitor all traffic on the network not just that intended
C. for the adapter in the device
D. It can put traffic onto the network
E. It can emulate any other device on the network

**Answer: B**

**QUESTION NO: 125**

Which parameter would you use on the "fw dbexport" command in order to specify that exported users are to be added under the "o=Acme Corp, c=US" branch?

A. -s "o=Acme Corp, c=US"
B. -a "o=Acme Corp, c=US"
C. -k "o=Acme Corp, c=US"
D. -b "o=Acme Corp, c=US"

**Answer: A**

**QUESTION NO: 126**

What is not included in the output of the "fw ctl pstat" command?

A. System memory statistics
B. Policy name
C. Encryption statistics
D. Hash memory statistics
E. Translation statistics

**Answer: B**

**QUESTION NO: 127**

What is the name of the traffic capture tool that is available on Unix platforms?

A. Network monitor
B. Snoop
C. Sniffer
D. Tcpdump

**Answer: B**

**QUESTION NO: 128**

When initially setting up high availability, where would you enable the high availability services?

A. The cpconfig utility
B. The fwstart script
C. The management server global properties screen
D. The gateway cluster properties screen

**Answer: A**

**QUESTION NO: 129**

What is true about hardening the operating system of a firewall gateway?

A. It is only necessary on a Solaris platform
B. It is necessary on both Solaris and NT platforms
C. It is not necessary
D. It is only necessary on an NT platform

**Answer: B**

**QUESTION NO: 130**

What command would you use to initiate a packet capture on a Unix machine?

A. snoop -o filename
B. tcpdump -i filename
C. snoop -i filename
D. tcpdump -o filename

**Answer: A**

**QUESTION NO: 131**

If you use the -a option in the "fw dbexport" command to export a subset of the possible user attributes. What happens if you import the exported file back into the FW-1 user database using the "fw import" command?

A. The database is merged with the subset database
B. You will get a warning, stating that you may delete part of your database
C. The process will error with no change to the original database
D. The database is overwritten with the subset database

**Answer: D**

**QUESTION NO: 132**

How do you remake a connection between a management server and a firewall module, if not using backward compatibility?

A. Reboot
B. Bounce the management server
C. Remake the SIC connection
D. Remake the putkey association

**Answer: C**

**QUESTION NO: 133**

What is true about the following command?

snoop -i filename | more

A. The file named "filename" contains raw captured traffic
B. It analyses captured traffic
C. It will continue the display until it ends
D. It captures traffic

**Answer: A,B**

**QUESTION NO: 134**

When configuring automatic synchronization for HA management modules, which is NOT a valid trigger for the synchronization to take place?

A. When the policy is installed
B. When the policy is saved
C. Regularly after a specified period
D. When you log off the GUI client

**Answer: D**

**QUESTION NO: 135**

To create synchronization between gateways in NG, which file do you need to edit?

A. conf.sync
B. sync.conf
C. None
D. rulebases.fws

**Answer: C**

**QUESTION NO: 136**

When a primary gateway cluster member fails another will take over.
When the primary recovers what is true?

A. The action depends on the configuration of the ClusterXL screen of the cluster properties
B. The primary always resumes primary function
C. The action depends on the configuration of the Cluster member gateway general properties
D. The primary will become a lower priority and not resume its primary function

**Answer: A**

**QUESTION NO: 137**

When exporting a checkpoint user database for importation to an LDAP server, what format should the output file take?

A. LDAP
B. Binary
C. LDIF
D. HTTP

**Answer: C**

**QUESTION NO: 138**

Which of the following are termed CPMAD global parameters?

A. MAD_Memory
B. MAD_syn_attack_action
C. MAD_number_of_connection_attempts
D. MAD_anti_spoofing_mode
AC

**Answer: A,C**

**QUESTION NO: 139**

What is true about the effects of configuring a high MAD_clean_interval in CPMAD?

A. It reduces CPU utilization
B. It increases CPU utilization
C. It decreases memory usage
D. It increases memory usage

**Answer: A,D**

**QUESTION NO: 140**

What is the meaning of the "collision" status when seen against a secondary management module?

A. Synchronization was attempted from both primary and secondary at the same time
B. The primary management module database lags behind the secondary
C. Both the primary and secondary management module have independently updated databases since the last synchronization
D. Synchronization has failed due to network problems

**Answer: C**

**QUESTION NO: 141**

If you want to use information from a cpinfo file produced by a Windows platform, you first need to perform a series of operations to extract the file concerned. True or false?

A. False
B. True

**Answer: A**

**QUESTION NO: 142**

What command would you use on a Solaris machine to increase the amount of memory allocated to the kernel to approximately 16Mbytes?

A. set fw:fwhmem=0x16
B. set fw:fwhmem=0x10
C. set fw:fwhmem=0x1000000
D. set fw:fwhmem=0x16000000

**Answer: C**

**Explanation:**
If this value is too low, or if you get "memory exhausted" errors, perform the following steps to increase the FireWall's memory. In this example, we change the memory to 5 MB (The values are in HEX notation). The default value is 3 MB. UNIX === 1. Stop the FireWall; fwstop 2. Perform the following commands, depending on the platform: Solaris: Add to /etc/system "set fw:fwhmem = 0x500000" and reboot

**QUESTION NO: 143**

How would you specify the primary member of a gateway cluster?

A. On the gateway cluster properties screen select "cluster members", then arrange priority sequence using the increase and decrease priority buttons
B. On the gateway cluster properties screen select "cluster members", then select priority number (1 is the highest)
C. On the member gateway properties general screen arrange priority sequence using the increase and decrease priority buttons
D. On the member gateway properties general screen select priority number (1 is the highest)

**Answer: A**

**QUESTION NO: 144**

Which debug option will gather information regarding the accept or drop action performed on traffic?

A. ioctl
B. packet
C. driver
D. kbuf

**Answer: B**

**QUESTION NO: 145**

Which of the following files is held on a management module and cotains the whole rulebase?

A. rulebases_5_0.C
B. objects.C

C. objects_5_0.C
D. rulebases_5_0.fws

**Answer: D**

**QUESTION NO: 146**

In the peer status area of the high availability management module screen of the active server, there are defined status levels that can apply to a peer module. Which status implies that a secondary module has a later version of the database than the primary?

A. Advanced
B. Lagging
C. Collision
D. Never Synchronized

**Answer: A**

**QUESTION NO: 147 CORRECT TEXT**

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

Answer: D

**QUESTION NO: 148**

To configure a fully overlapping encryption domain, what type of group(s) do you need to configure?

A. A group containing both gateways and all the networks they protect
B. A group containing both gateways only
C. A group containing all the networks that both gateways protect
D. Two groups, one containing both gateways and the networks that one protects. The other containing both gateways and the networks the other protects.

**Answer: A**

**QUESTION NO: 149**

What is the approximate memory requirement of a simple (I.e. not authenticated or encrypted) connection in VPN-1/FW-1?

A. 3 Kbytes
B. 70 bytes
C. 10 bytes
D. 1 Kbytes

**Answer: B**

**QUESTION NO: 150**

If you want to run the cpinfo utility to gather diagnostic information for a problematic enforcement module in a distributed system, what is true?

A. You should run cpinfo on the enforcement module only
B. You should run cpinfo on all the modules in the distributed system
C. You should run cpinfo on both the management and enforcement modules
D. You should run cpinfo on the management module only

**Answer: C**

**QUESTION NO: 151 CORRECT TEXT**

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

Answer: B, C

**QUESTION NO: 152**

Which is NOT a valid log file maintained on the SecuRemote client?

A. sr_watchdog_tde.log
B. sr_service_<serial number>.log
C. sr_background_tde.log
D. sr_gui_tde.log

**Answer: C**

**QUESTION NO: 153**

Which debug option will gather information about input/output control messages, such as loading of FW-1 or kernel to daemon communications?

A. kbuf
B. ioctl
C. misc
D. driver

**Answer: B**

**QUESTION NO: 154**

It is not possible to use two gateways running a standalone installation in an MEP environment. True or false?

A. False
B. True

**Answer: B**

**QUESTION NO: 155**

How would you use a policy editor gui in local mode when using FW-1 NG FP-2?

A. Enter *local in the "management server" box of the GUI login screen
B. Check the "demo mode" box of the GUI login screen
C. Enter demo_mode in the "management server" box of the GUI login screen
D. Enter *local in the "user name" box of the GUI login screen

**Answer: A,B**

**QUESTION NO: 156**

How would you restart CPMAD on a firewall?

A. $FWDIR/conf/fwstart
B. $FWDIR/bin/cpmad
C. $FWDIR/cpmad/fwstart
D. $FWDIR/bin/fwstart

**Answer: D**

**QUESTION NO: 157**

What is used by FW-1 to create a SIC certificate?

A. External CA
B. Putkey
C. LDAP
D. Internal CA

**Answer: D**

**QUESTION NO: 158**

How would you find more information about the "fw tab" options?

A. fw tab help
B. fw tab -h
C. fw tab -?
D. fw tab options -h

**Answer: B**

**QUESTION NO: 159**

What is contained in the rulebases.fws file?

A. Auditing information
B. All rulebases
C. All rulebases plus auditing information
D. Only the rulebase from the last load

**Answer: B**

**QUESTION NO: 160**

When using management high availability, you can synchronize from the primary or secondary management server. True or false?

A. False
B. True

**Answer: A**

**QUESTION NO: 161**

On a SecuRemote client, in which directory are the log files located?

A. $CPDIR/log
B. $SCDIR/log
C. $SRDIR/log
D. $FWDIR/log

**Answer: C**

**QUESTION NO: 162**

If you were having problems with a CVP server, you may want to capture traffic to and from the server. What could you do to get this information?

A. Run "fw monitor" for port 18182 on the interface connected to the management server
B. Run "fw monitor" for port 18182 on the interface connected to the CVP server
C. Run "fw monitor" for port 18181 on the interface connected to the management server
D. Run "fw monitor" for port 18181 on the interface connected to the CVP server

**Answer: D**

**QUESTION NO: 163**

When using backward compatibility, what is true?

A. It restricts inter-module communications to the putkey method
B. It allows the management of 4.1 gateways
C. It restricts inter-module communication to the SIC method
D. It allows the use of the old putkey function

**Answer: B,D**

**QUESTION NO: 164**

Why would you disable NetBEUI on a FW-1 Windows Platform?

A. It can cause FW-1 to crash

B. It clashes with internal FW-1 protocols
C. It is an inefficient protocol
D. It is a security risk

**Answer: D**

**QUESTION NO: 165**

What does "resolver_ttl" do in relation to SecuRemote configuration?

A. Specifies the interval in seconds between RDP status queries
B. Specifies that RDP status queries are sent automatically
C. Specifies the number of seconds that a Securemote client waits for a reply to a RDP status query
D. Controls the time to live when accessing a DNS server

**Answer: C**