156-585.VCEplus.premium.exam.75q - DEMO

Number: 156-585
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam A

QUESTION 1

What are some measures you can take to prevent IPS false positives?

A. Exclude problematic services from being protected by IPS (sip, H.323, etc.)
B. Use IPS only in Detect mode
C. Use Recommended IPS profile
D. Capture packets, Update the IPS database, and Back up custom IPS files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 VPN issues may result from misconfiguration, communication failure, or incompatible default configurations between peers. Which basic command syntax needs to be used for troubleshooting Site-to-Site VPN issues?

A. vpn debug truncon
B. fw debug truncon
C. cp debug truncon
D. vpn truncon debug

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 What are the maximum kernel debug buffer sizes, depending on the version?

A. 8MB or 32MB
B. 8GB or 64GB
C. 4MB or 8MB
D. 32MB or 64MB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which daemon governs the Mobile Access VPN blade and works with VPND to create Mobile Access VPN connections? It also handles interactions between HTTPS and the Multi-Portal Daemon.

A. Connectra VPN Daemon - cvpnd
B. Mobile Access Daemon - MAD
C. mvpnd
D. SSL VPN Daemon - sslvpnd

Correct Answer: A
Section: (none)

Explanation
Explanation/Reference:

QUESTION 5 What does CMI stand for in relation to the Access Control Policy?

A. Content Matching Infrastructure
B. Content Management Interface
C. Context Management Infrastructure
D. Context Manipulation Interface

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
You are trying to establish a VPN tunnel between two Security Gateways but fail. What initial steps will you make to troubleshoot the issue?

A. capture traffic on both tunnel members and collect debug of IKE and VPND daemon
B. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags, then collect debug of IKE and VPND daemon
C. collect debug of IKE and VPND daemon and collect kernel debug for fw module with vm, crypt, conn and drop flagsD. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
An administrator receives reports about issues with log indexing and text searching regarding an existing Management Server. In trying to find a solution she wants to check if the process responsible for this feature is running correctly. What is true about the related process?

A. fwm manages this database after initialization of the ICA
B. cpd needs to be restarted manual to show in the list
C. fwssd crashes can affect therefore not show in the list
D. solr is a child process of cpm

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
When debugging is enabled on firewall kernel module using the ‘fw ctl debug’ command with required options, many debug messages are provided by the kernel that help the administrator to identify issues. Which of the following is true about these debug messages generated by the kernel module?

A. Messages are written to a buffer and collected using ‘fw ctl kdebug’
B. Messages are written to console and also /var/log/messages file
C. Messages are written to /etc/dmesg file
D. Messages are written to $FWDIR/log/fw.elg

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 How can you increase the ring buffer size to 1024 descriptors?

A. set interface eth0 rx-ringsize 1024
B. fw ctl int rx_ringsize 1024
C. echo rx_ringsize=1024>>/etc/sysconfig/sysctl.conf
D. dbedit>modify properties firewall_properties rx_ringsize 1024

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 What are four main database domains?

A. System, Global, Log, Event
B. System, User, Host, Network
C. Local, Global, User, VPN
D. System, User, Global, Log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 During firewall kernel debug with fw ctl zdebug you received less information that expected. You noticed that a lot of messages were lost since the time the debug was started. What should you do to resolve this issue?

A. Increase debug buffer; Use fw ctl debug -buf 32768
B. Redirect debug output file; Use fw ctl zdebug -o ./debug.elg
C. Increase debug buffer; Use fw ctl zdebug -buf 32768
D. Redirect debug output file; Use fw ctl debug -o ./debug.elg

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 Where do Protocol parsers register themselves for IPS?

A. Passive Streaming Library
B. Other handlers register to Protocol parser
C. Protections database

D. Context Management Infrastructure

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 Which command can be run in Expert mode to verify the core dump settings?

A. grep cdm /config/db/coredump
B. grep cdm /config/db/initial
C. grep $FWDIR/config/db/initial
D. cat /etc/sysconfig/coredump/cdm.conf

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
The two procedures available for debugging in the firewall kernel are:
i. fw ctl zdebug ii. fw ctl debug/kdebug

Choose the correct statement explaining the difference in the two.

A. (i) Is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to get an output via command line whereas (ii) is useful when there is a need for detailed debugging and requires additional steps to set thebuffer and get an output via command line
B. (i) is used to debug the access control policy only, however (ii) can be used to debug a unified policy
C. (i) is used to debug only issues related to dropping traffic, however (ii) can be used for any firewall issue including NATing, clustering etc.D. (i) is used on a Security Gateway, whereas (ii) is used on a Security Management Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
If the cpsemd process of SmartEvent has crashed or is having trouble to coming up, then it usually indicates that _______________.

A. Postgres database is down
B. Cpd daemon is unable to connect to the log server
C. The SmartEvent core on the Solr indexer has been deleted
D. The logged in administrator does not have permissions to run SmartEvent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
What process is responsible for sending and receiving logs in the management server?
A. FWD

B. CPM
C. FWM
D. CPD

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 If IPS protections that prevent SecureXL from accelerating traffic, such as Network Quota, Fingerprint Scrambling, TTL Masking etc, have to be used, what is recommended practice to enhance the performance of the gateway?

A. Use the IPS exception mechanism
B. Disable all such protections
C. Disable SecureXL and use CoreXL
D. Upgrade the hardware to include more Cores and Memory

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18 What is the best way to resolve an issue caused by a frozen process?

A. Reboot the machine
B. Restart the process
C. Kill the process
D. Power off the machine

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 What is the difference in debugging a S2S or C2S (using Check Point VPN Client) VPN?

A. there is no difference
B. the C2S VPN uses a different VPN daemon and there a second VPN debug
C. the C2S VPN can not be debugged as it uses different protocols for the key exchangeD. the C2S client uses Browser based SSL vpn and can’t be debugged

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which one of the following is NOT considered a Solr core partition?
A. CPM_0_Revisions

B. CPM_Global_A
C. CPM_Global_R
D. CPM_0_Disabled

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 What process monitors, terminates, and restarts critical Check Point processes as necessary?

A. CPWD
B. CPM
C. FWD
D. FWM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
The Check Point Firewall Kernel is the core component of the Gala operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

A. fw ctl debug/kdebug
B. fw ctl zdebug
C. fw debug/kdebug
D. fw debug/kdebug ctl

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
B. $CPDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
C. $FWDIR/conf/install_firewall_tmp/ANTIMALWARE/conf/
D. $FWDIR/log/install_manager_tmp/ANTIMALWARE/log/

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 24 How many captures does the command “fw monitor -p all” take?

A. All 15 of the inbound and outbound modules
B. All 4 points of the VM modules
C. 1 from every inbound and outbound module of the chain
D. The -p option takes the same number of captures, but gathers all of the data packet

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25 Which Daemon should be debugged for HTTPS Inspection related issues?

A. FWD
B. HTTPD
C. WSTLSD
D. VPND

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
John works for ABC Corporation. They have enabled CoreXL on their firewall. John would like to identify the cores on which the SND runs and the cores on which the firewall Instance is running. Which command should John run to view the CPU role allocation?

A. fw ctl affinity -v
B. fwaccel stat -l
C. fw ctl affinity -l
D. fw ctl cores

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Joey is configuring a site-to-site VPN with his business partner. On Joey's site he has a Check Point R80.10 Gateway and his partner uses Cisco ASA 5540 as a gateway. Joey's
VPN domain on the Check Point Gateway object is manually configured with a group object that contains two network objects:
VPN_Domain3 = 192.168.14.0/24
VPN_Domain4 = 192.168.15.0/24
Partner's site ACL as viewed from "show run"
access-list JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.14.0 255.255.255.0 access-list
JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.15.0 255.255.255.0

When they try to establish VPN tunnel, it fails. What is the most likely cause of the failure given the information provided?

A. Tunnel falls on partner site. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation. Check Point continues to present its own encryption domain as 192.168.14.0/24 and 192.168.15.0/24, but the peer expects the one network192.168.14.0/23
B. Tunnel fails on partner site. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation. Check Point continues to present its own encryption domain as 192.168.14.0/23, but the peer expects the two distinct networks192.168.14.0/24 and 192.168.15.0/24.

C. Tunnel fails on Joey's site, because he misconfigured IP address of VPN peer.
D. Tunnel falls on partner site. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 What are the main components of Check Point's Security Management architecture?

A. Management server, management database, log server, automation server
B. Management server, Security Gateway, Multi-Domain Server, SmartEvent Server
C. Management server, Log Server, LDAP Server, Web Server
D. Management server, Log Server, Gateway server, Security server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 What are the four ways to insert an FW Monitor into the firewall kernel chain?

A. Relative position using location, relative position using alias, absolute position, all positions
B. Absolute position using location, absolute position using alias, relative position, all positions
C. Absolute position using location, relative position using alias, general position, all positions
D. Relative position using geolocation, relative position using inertial navigation, absolute position, all positions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 Which kernel process is used by Content Awareness to collect the data from contexts?

A. dlpda
B. PDP
C. cpemd
D. CMI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore, you need to add a timestamp to the kernel debug and write the output to a file but you can't afford to fill up all the remaining disk space and you only have 10 GB free for saving the debugs. What is the correct syntax for this?

A. fw ctl kdebug -T -f -m 10 -s 1000000 -o debugfilename
B. fw ctl kdebug -T -f -m 10 -s 1000000 > debugfilename
C. fw ctl kdebug -T -m 10 -s 1000000 -o debugfilename
D. fw ctl debug -T -f -m 10 -s 1000000 -o debugfilename

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
You have configured IPS Bypass Under Load function with additional kernel parameters: ids_tolerance_no_stress=15 and ids_tolerance_stress=15. For configuration you used the "fw ctl set" command. After reboot you noticed that these parameters returned to their default values. What do you need to do to make this configuration work immediately and stay permanent?

A. Set these parameters again with "fw ctl set" and edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf
B. Use script $FWDIR/bin/ IpsSetBypass.sh to set these parameters
C. Set these parameters again with "fw ctl set' and save configuration with "save config"D. Edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33 Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

A. cpstat
B. CPstat
C. CPview
D. fwstat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34 You are running R80.XX on an open server and you see a high CPU utilization on your 12 CPU cores. You now want to enable Hyperthreading to get more cores to gain some performance. What is the correct way to achieve this?

A. Hyperthreading is not supported on open servers, on Check Point Appliances
B. Just turn on HAT in the bios of the server and boot it
C. Just turn on HAT in the bios of the server and after it was booted enable it in cpconfigD. in clish run set HAT on

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 35
The customer is using Check Point appliances that were configured long ago by third-party administrators. Current policy includes different enabled IPS protections and Bypass Under Load function. Bypass Under Load is configured to disable IPS inspections of CPU and Memory usage is higher than 80%. The Customer reports that IPS protections are not working at all regardless of CPU and Memory usage. What is the possible reason of such behavior?

A. The kernel parameter ids_assume_stress is set to 0
B. The kernel parameter ids_assume_stress is set to 1
C. The kernel parameter ids_tolerance_no_stress is set to 10
D. The kernel parameter ids_tolerance_stress is set to 10

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 What is the benefit of running “vpn debug trunc” over
“vpn debug on”?

A. “vpn debug trunc” purges ike.elg and vpnd.elg and creates timestamp while starting ike debug and vpn debug B.
“vpn debug trunc” truncates the capture hence the output contains minimal capture
C. “vpn debug trunc” provides verbose capture
D. No advantage one over other

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
In Security Management High Availability, if the primary and secondary managements, running the same version of R80.x, are in a state of ‘Collision’, how can this be resolved?

A. Administrator should manually synchronize the servers using SmartConsole
B. The Collision state does not happen in R80.x as the synchronizing automatically on every publish action
C. Reset the SIC of the secondary management server
D. Run the command ‘fw send synch force’ on the primary server and ‘fw get sync quiet’ on the secondary server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 After kernel debug with “fw ctl debug” you received a huge amount of information. It was saved in a very large file that is difficult to open and analyze with standard text editors. Suggest a solution to solve this issue.

A. Use “fw ctl debug” because of 1024KB buffer size
B. Divide debug information into smaller files. Use “fw ctl debug -f -o “filename” -m 25 -s “1024”
C. Reduce debug buffer to 1024KB and run debug for several times
D. Use Check Point InfoView utility to analyze debug output

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 39 What is the most efficient way to view large fw monitor captures and run filters on the file?

A. wireshark
B. CLISH
C. CLI
D. snoop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
What does SIM handle?

A. Accelerating packets
B. FW kernel to SXL kernel hand off
C. OPSEC connects to SecureXL
D. Hardware communication to the accelerator

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 Which process is responsible for the generation of certificates?

A. cpm
B. cpca
C. dbsync
D. fwm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
How does the URL Filtering Categorization occur in the kernel?
1. RAD provides the status of the search to the client.
2. The a-sync request is forwarded to the RAD User space via the RAD kernel for online categorization.
3. The online detection service responds with categories and the kernel cache is updated.
4. The kernel cache notifies the RAD kernel of hits and misses.
5. URL lookup initiated by the client.
6. URL lookup occurs in the kernel cache.
7. The client sends an a-sync request back to RAD If the URL was not found.

A. 5, 6, 7, 1, 3, 2, 4
B. 5, 6, 2, 4, 1, 7, 3 C. 5, 6, 4, 1, 7, 2, 3
D. 5, 6, 3, 1, 2, 4, 7

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 43 Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS, and complies them together into unified Pattern Matchers?

A. CMI Loader
B. cpas
C. PSL - Passive Signature Loader
D. Context Loader

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 What is the function of the Core Dump Manager utility?

A. To generate a new core dump for analysis
B. To limit the number of core dump files per process as well as the total amount of disk space used by core files
C. To determine which process is slowing down the system
D. To send crash information to an external analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 To check the current status of hyper-threading, which command would you execute in expert mode?

A. cat /proc/hypert_status
B. cat /proc/smt_status
C. cat /proc/hypert_stat
D. cat /proc/smt_stat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following daemons is used for Threat Extraction?
A. scrubd
B. extractd
C. tex
D. tedex

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47 What is the correct syntax to set all debug flags for Unified Policy related issues?

A. fw ctl debug -m UP all
B. fw ctl debug -m up all
C. fw ctl kdebug -m UP all
D. fw ctl debug -m fw all

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Some users from your organization have been reported some connection problems with CIFS since this morning. You suspect an IPS Issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS module (position 4 in the chain) to check if the packets pass the IPS. What command do you need to run?

A. fw monitor -ml -pl 5 -e <filterexpression>
B. fw monitor -pi 5 -e <filterexpression>
C. tcpdump -eni any <filterexpression>
D. fw monitor -pl asm <filterexpression>

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
For TCP connections, when a packet arrives at the Firewall Kernel out of sequence or fragmented, which layer of IPS corrects this to allow for proper inspection?

A. Passive Streaming Library
B. Protections
C. Protocol Parsers
D. Context Management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
What acceleration mode utilizes multi-core processing to assist with traffic processing?

A. CoreXL
B. SecureXL

C. HyperThreading
D. Traffic Warping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 How many tiers of pattern matching can a packet pass through during IPS inspection?

A. 2
B. 1
C. 5
D. 9

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52 James is using the same filter expression in fw monitor for CITRIX very often and instead of typing this all the time he wants to add it as a macro to the fw monitor definition file. What’s the name and location of this file?

A. $FWDIR/lib/fwmonltor.def
B. $FWDIR/conf/fwmonltor.def
C. $FWDIR/lib/tcpip.def
D. $FWDIR/lib/fw.monitor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 What command is used to find out which port Multi-Portal has assigned to the Mobile Access Portal?

A. mpclient getdata sslvpn
B. netstat -nap | grep mobile
C. mpclient getdata mobi
D. netstat getdata sslvpn

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 54 What file contains the RAD proxy settings?

A. rad_settings.C
B. rad_services.C

C. rad_scheme.C
D. rad_control.C

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55 Your users have some issues connecting Mobile Access VPN to the gateway. How can you debug the tunnel establishment?

A. in the file $CVPNDIR/conf/httpd.conf change the line loglevel .. To LogLevel debug and run cvpnrestart
B. run vpn debug truncon
C. run fw ctl zdebug -m sslvpn all
D. in the file $VPNDIR/conf/httpd.conf the line Loglevel .. To LogLevel debug and run vpn restart

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which Threat Prevention Daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd
B. in.msd
C. ted
D. scrub

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
John has renewed his NGTX License but he gets an error (contract for Anti-Bot expired). He wants to check the subscription status on the CLI of the gateway, what command can he use for this?

A. cpstat antimalware -f subscription_status
B. fw monitor license status
C. fwm lic print
D. show license status

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 58 When a User Mode process suddenly crashes, it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash? i. Program Counter ii. Stack Pointer
iii. Memory management information iv. Other
Processor and OS flags / information

A. i, ii, iii and iv
B. i and ii only
C. iii and iv only
D. Only iii

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59 What file extension should be used with fw monitor to allow the output file to be imported and read in WireShark?

A. .cap
B. .exe
C. .tgz
D. .pcap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 Which situation triggers an IPS bypass under load on a 24-core Check Point appliance?

A. any of the CPU cores is above the threshold for more than 10 seconds
B. all CPU core must be above the threshold for more than 10 seconds
C. a single CPU core must be above the threshold for more than 10 seconds, but is must be the same core during this timeD. the average CPU utilization over all cores must be above the threshold for 1 second

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61 What table does command “fwaccel conns” pull information from?

A. fwxl_conns
B. SecureXLCon
C. cphwd_db
D. sxl_connections
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
RAD is initiated when Application Control and URL Filtering blades are active on the Security Gateway. What is the purpose of the following RAD configuration file $FWDIR/cong/rad_settings.C?

A. This file contains the location information for Application Control and/or URL Filtering entitlements
B. This file contains the information on how the Security Gateway reaches the Security Managers RAD service for Application Control and URL FilteringC. This file contains RAD proxy settings
D. This file contains all the host name settings for the online application detection engine

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63 What is the proper command for allowing the system to create core files?

A. $FWDIR/scripts/core-dump-enable.sh
B. # set core-dump enable# save config
C. service core-dump start
D. >set core-dump enable
>save config

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64 Which command is used to write a kernel debug to a file?

A. fw ctl debug -T -f > debug.txt
B. fw ctl kdebug -T -l > debug.txt
C. fw ctl debug -S -t > debug.txt
D. fw ctl kdebug -T -f > debug.txt

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65 Which command is most useful for debugging the fwaccel module?

A. fw zdebug
B. securexl debug
C. fwaccel dbg
D. fw debug

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66

Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application & Control Filtering?

A. rad
B. cprad
C. pepd
D. pdpd

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67 What is the main SecureXL database for tracking acceleration status of traffic?

A. cphwd_db
B. cphwd_tmp1
C. cphwd_dev_conn_table
D. cphwd_dev_identity_table

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68 Which command(s) will turn off all vpn debug collection?

A. vpn debug off
B. vpn debug -a off
C. vpn debug off and vpn debug ikeoff
D. fw ctl debug 0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69 Which of the following is contained in the System Domain of the Postgres database?

A. Saved queries for applications
B. Configuration data of log servers
C. Trusted GUI clients
D. User modified configurations such as network objects

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70 Which is the correct “fw monitor” syntax for creating a capture file for loading it into WireShark?

A. fw monitor -e “accept<FILTER EXPRESSION>;” >> Output.cap
B. This cannot be accomplished as it is not supported with R80.10
C. fw monitor -e “accept<FILTER EXPRESSION>;” -file Output.cap
D. fw monitor -e “accept<FILTER EXPRESSION>;” -o Output.cap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
PostgreSQL is powerful, open source relational database management system. Check Point offers a command for viewing the database to interact with Postgres interactive shell. Which command do you need to enter the PostgreSQL interactive shell?

A. psql_client cpm postgres
B. mysql_client cpm postgres
C. psql_client postgres cpm
D. mysql -u root

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
When a User process or program suddenly crashes, a core dump is often used to examine the problem. Which command is used to enable the core-dumping via GAIA clish?

A. set core-dump enable
B. set core-dump per_process
C. set user-dump enable
D. set core-dump total

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
What components make up the Context Management Infrastructure?
A. CMI Loader and Pattern Matcher
B. CPMI and FW Loader
C. CPX and FWM
D. CPM and SOLR

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74 You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore, you need to add a timestamp to the kernel debug and write the output to a file. What is the correct syntax for this?

A. fw ctl kdebug -T -f > filename.debug
B. fw ctl kdebug -T > filename.debug
C. fw ctl debug -T -f > filename.debug
D. fw ctl kdebug -T -f -o filename.debug

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75 Troubleshooting issues with Mobile Access requires the following:

A. Standard VPN debugs, packet captures, and debugs of ‘cvpnd’ process on Security Gateway
B. Standard VPN debugs and packet captures on Security Gateway, debugs of ‘cvpnd’ process on Security ManagementC. ‘ma_vpnd’ process on Security Gateway
D. Debug logs of FWD captured with the command - ‘fw debug fwd on TDERROR_MOBILE_ACCESS=5’

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: