Exam Questions 156-585

Check Point Certified Troubleshooting Expert

https://www.2passeasy.com/dumps/156-585/

NEW QUESTION 1
How can you start debug of the Unified Policy with all possible flags turned on?

A. fw ctl debug -m UP all
B. fw ctl debug -m UnifiedPolicy all
C. fw ctl debug -m fw + UP
D. fw ctl debug -m UP *

Answer: D

NEW QUESTION 2
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 packet
E. Update the IPS database, and Back up custom IPS files

Answer: A

NEW QUESTION 3
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_lmp/ANTIMALWARE/conf/
C. $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/
D. $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

Answer: A

NEW QUESTION 4
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

Answer: A

NEW QUESTION 5
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
ii. Memory management information
iv Other Processor and OS flags / information

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

Answer: C

NEW QUESTION 6
Which command is most useful for debugging the fwaccel module?

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

Answer: C

NEW QUESTION 7
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

Answer: A

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 8
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

Answer: C

NEW QUESTION 9
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

Answer: A

NEW QUESTION 10
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 SFWDIR/conf/rad_settings.C?

A. This file contains the location information tor 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 Filtering
C. This file contains RAD proxy settings
D. This file contains all the host name settings for the online application detection engine

Answer: B

NEW QUESTION 10
Which Daemon should be debugged for HTTPS Inspection related issues?

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

Answer: C

NEW QUESTION 12
Your fwm constantly crashes and is restarted by the watchdog. You can't find any coredumps related to this process, so you need to check If coredumps are enabled at all How can you achieve that?

A. in dish run show core-dump status
B. in expert mode run show core-dump status
C. in dish run set core-dump status
D. in dish run show coredumb status

Answer: D

NEW QUESTION 13
Which process is responsible for the generation of certificates?

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

Answer: B

NEW QUESTION 15
What is the kernel process for Content Awareness that collects the data from the contexts received from the CMI and decides if the file is matched by a data type?

A. dlpda
B. dlpu
C. cntmgr
D. cntawmod

Answer: D

NEW QUESTION 16
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

Answer: D

NEW QUESTION 18
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

Answer: A

NEW QUESTION 22
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

Answer: D

NEW QUESTION 27
What is NOT a benefit of the fw ctl zdebug command?

A. Cannot be used to debug additional modules
B. Collect debug messages from the kernel
C. Clean the buffer
D. Automatically allocate a 1MB buffer

Answer: A

NEW QUESTION 32
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 Management
C. 'ma_vpnd' process on Secunty Gateway
D. Debug logs of FWD captured with the command - 'fw debug fwd on TDERROR_MOBILE_ACCESS=5'

Answer: A

NEW QUESTION 35
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 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 has booted enable it in cpconfig
D. in dish run set HAT on

Answer: A

NEW QUESTION 37
During firewall kernel debug with fw ctl zdebug you received less information than 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 to file; Use fw ctl zdebug –o ./debug.elg
C. Increase debug buffer; Use fw ctl zdebug –buf 32768
D. Redirect debug output to file; Use fw ctl debug –o ./debug.elg

Answer: A

NEW QUESTION 39
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

Answer: C

NEW QUESTION 44
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

Answer: D

NEW QUESTION 46
PostgreSQL is a 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_c!ieni postgres cpm
D. mysql -u root

Answer: A

NEW QUESTION 50
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

Answer: A

NEW QUESTION 54
Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. core dump
B. CPMIL dump
C. fw monitor
D. tcpdump

Answer: A

NEW QUESTION 56
What acceleration mode utilizes multi-core processing to assist with traffic processing?

A. CoreXL
B. SecureXL
C. HyperThreading
D. Traffic Warping

Answer: C

NEW QUESTION 58
Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0,

choose the correct answer.

A. fw monitor –po -0x1ffffe0
B. fw monitor –p0 ox1ffffe0
C. fw monitor –po 1ffffe0
D. fw monitor –p0 –ox1ffffe0

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminG

NEW QUESTION 63
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

Answer: C

NEW QUESTION 65
Vanessa is reviewing ike.elg file to troubleshoot failed site-to-site VPN connection After sending Mam Mode Packet 5 the response from the peer is PAYLOAD-MALFORMED"
What is the reason for failed VPN connection?

A. The authentication on Phase 1 is causing the problem.Pre-shared key on local gateway encrypted by the hash algorithm created in Packet 3 and Packet 4 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
B. The authentication on Phase 2 is causing the problemPre-shared key on local gateway encrypted by the hash algorithm created in Packets 1 and 2 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
C. The authentication on Quick Mode is causing the problemPre-shared key on local gateway encrypted by the hash algorithm created in Packets 3 and 4 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
D. The authentication on Phase 1 is causing the problemPre-shared key on local gateway encrypted by the hash algorithm doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key created in Packet 1 and Packet 2

Answer: B

NEW 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

Answer: C

NEW QUESTION 73
URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required"

A. RAD Kernel Space
B. URLF Kernel Client
C. URLF Online Service
D. RAD User Space

Answer: B

NEW QUESTION 76
What table does the command "fwaccel conns" pull information from?

A. fwxl_conns
B. SecureXLCon
C. cphwd_db
D. sxl_connections

Answer: A

NEW QUESTION 79
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 zdebug' because of 1024KB buffer size
B. Divide debug information into smaller files Use "fw ctl kdebug -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

Answer: C

NEW QUESTION 81
What is the correct syntax to turn a VPN debug on and create new empty debug files?

A. vpn debug truncon
B. vpndebug trunc on
C. vpn kdebug on
D. vpn debug trunkon

Answer: D

NEW QUESTION 84
Check Point Access Control Daemons contains several daemons for Software Blades and features Which Daemon is used for Application & Control URL Filtering?

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

Answer: C

NEW QUESTION 89
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 differences 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 linewhereas (11) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line
B. (i) is used to debug the access control policy only, however (n) can be used to debug a unified policy
C. (i) is used to debug only issues related to dropping of traffic, however (n) can be used for any firewall issue including NATing, clustering etc.
D. (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server

Answer: C

NEW QUESTION 90
What table does command “fwaccel conns” pull information from?

A. fwxl_conns
B. SecureXLCon
C. cphwd_db
D. sxl_connections

Answer: A

NEW QUESTION 94
What command sets a specific interface as not accelerated?

A. noaccel-s<interface1>
B. fwaccel exempt state <interface1>
C. nonaccel -s <interface1>
D. fwaccel -n <intetface1 >

Answer: C

NEW QUESTION 97
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

Answer: B

NEW QUESTION 101
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 -I
C. fw ctl affinity -I
D. fw ctl cores

Answer: C

NEW QUESTION 103

......