Exam Questions 156-585

Check Point Certified Troubleshooting Expert

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

NEW QUESTION 1
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

Answer: D

NEW QUESTION 2
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 3
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

Answer: A

NEW QUESTION 4
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 5
For TCP connections, when a packet arrives at the Firewall Kemel out of sequence or fragmented, which layer of IPS corrects this lo allow for proper inspection?

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

Answer: D

NEW QUESTION 6
What is the main SecureXL database for tracking the acceleration status of traffic?

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

Answer: D

NEW QUESTION 7
What is the buffer size set by the fw ctl zdebug command?

A. 1 MB
B. 1 GB
C. 8MB
D. 8GB

Answer: A

NEW QUESTION 8
Which Daemon should be debugged for HTTPS Inspection related issues?

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

Answer: C

NEW QUESTION 9
Which of the following is NOT a vpn debug command used for troubleshooting?

A. fw ctl debug -m fw + conn drop vm crypt
B. vpn debug trunc
C. pclient getdata sslvpn
D. vpn debug on TDERROR_ALL_ALL=5

Answer: C

NEW QUESTION 10
If you run the command "fw monitor -e accept src=10.1.1.201 or src=172.21.101.10 or src=192.0.2.10;" from the cli sh What will be captured?

A. Packets from 10 1 1 201 going to 192.0 2.10
B. Packets destined to 172 21 101 10 from 10.1.1.101
C. Only packet going to 192.0.2.10
D. fw monitor only works in expert mode so no packets will be captured

Answer: C

NEW QUESTION 10
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 flags
D. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags

Answer: A

NEW QUESTION 12
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

Answer: A

NEW QUESTION 15
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

Answer: A

NEW QUESTION 17
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

Answer: B

NEW QUESTION 21
If the cpsemd process of SmartEvent has crashed or is having trouble coming up. then it usually indicates that .

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

Answer: C

NEW QUESTION 24
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 28
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 33
Which Threat Prevention daemon is the core Threat Emulator, engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd
B. inmsd
C. ted
D. scrub

Answer: C

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

NEW QUESTION 35
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 37
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 40
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 45
Check Point's PostgreSQL is partitioned into several relational database domains. Which domain contains network objects and security policies?

A. User Domain
B. System Domain
C. Global Domain
D. Log Domain

Answer: C

NEW QUESTION 47
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 50
You are upgrading your NOC Firewall (on a Check Point Appliance) from R77 to R80 30 but you did not touch the security policy After the upgrade you can't connect to the new R80 30 SmartConsole of the upgraded Firewall anymore What is a possible reason for this?

A. new new console port is 19009 and a access rule ts missing
B. the license became invalig and the firewall does not start anymore
C. the upgrade process changed the interfaces and IP adresses and you have to switch cables
D. the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall

Answer: D

NEW QUESTION 52
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 54
What acceleration mode utlizes multi-core processing to assist with traffic processing?

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

Answer: C

NEW QUESTION 57
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

Answer: B

NEW QUESTION 58
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 sit
B. 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 network 192.168.14.0/23

C. Tunnel fails on partner sit
D. 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 networks 192.168.14.0/24 and 192.168.15.0/24.
E. Tunnel fails on Joey's site, because he misconfigured IP address of VPN peer.
F. Tunnel falls on partner sit
G. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

Answer: B

NEW QUESTION 63
What is the simplest and most efficient way to check all dropped packets in real time?

A. fw ctl zdebug * drop in expert mode
B. Smartlog
C. cat /dev/fwTlog in expert mode
D. tail -f SFWDIR/log/fw log |grep drop in expert mode

Answer: D

NEW QUESTION 65
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 66
What process monitors, terminates, and restarts critical Check Point processes as necessary?

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

Answer: A

NEW QUESTION 71
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 74
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

Answer: C

NEW QUESTION 75
What process is responsible for sending and receiving logs in the management server?

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

Answer: A

NEW QUESTION 79
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

Answer: B

NEW QUESTION 82
The Check Pom! Firewall Kernel is the core component of the Gaia operating system and an integral part of the traffic inspection process There are two procedures available for debugging the firewall kernel Which procedure/command is used for troubleshooting packet drops and other kernel activites while using minimal resources (1 MB buffer)?

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

Answer: A

NEW QUESTION 86
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 most 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 time
D. the average cpu utilization over all cores must be above the threshold for 1 second

Answer: A

NEW QUESTION 91
What is the name of the VPN kernel process?

A. VPNK
B. VPND
C. CVPND
D. FWK

Answer: A

NEW QUESTION 92
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 95
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 98
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

Answer: D

NEW QUESTION 100
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 102
Which of the following daemons is used for Threat Extraction?

A. scrubd
B. extractd
C. tex
D. tedex

Answer: A

NEW QUESTION 106
Which one of the following is NOT considered a Solr core partition:

A. CPM_0_Revisions
B. CPM_Global_A
C. CPM_Gtobal_R
D. CPM_0_Disabled

Answer: D

NEW QUESTION 111
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

Answer: B

NEW QUESTION 116
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

Answer: C

NEW QUESTION 118
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-585 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-585 Product From:

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

Money Back Guarantee

156-585 Practice Exam Features:

* 156-585 Questions and Answers Updated Frequently

* 156-585 Practice Questions Verified by Expert Senior Certified Staff

* 156-585 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-585 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year