156-585 Q&As

Check Point Certified Troubleshooting Expert

Pass CheckPoint 156-585 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/156-585.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

QUESTION 2

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: A

fw ctl zdebug is only for drops and fw ctl debug/kdebug are more detailed and flexible

QUESTION 3

Which command can be run in Expert mode lo verify the core dump settings?

A. grep cdm /config/db/coredump

B. grep cdm /config/db/initial

C. grep SFWDIR/config/db/initial

D. cat /etc/sysconfig/coredump/cdm conf

Correct Answer: C

QUESTION 4

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

QUESTION 5

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

Correct Answer: A

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/Content/Topics-PTG/CLI/fw-monitor.htm

QUESTION 6

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

Correct Answer: C

QUESTION 7

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

QUESTION 8

Which is the correct "fw monitor" syntax for creating a capture file for loading it into WireShark?

A. fw monitor -e "accept;" >> Output.cap

B. This cannot be accomplished as it is not supported with R80.10

C. fw monitor -e "accept;" -file Output.cap

D. fw monitor -e "accept;" -o Output.cap

Correct Answer: D

QUESTION 9

Which of the following inputs is suitable for debugging HTTPS inspection issues?

A. vpn debug cptls on

B. fw ctl debug ? fw + conn drop cptls

C. fw diag debug tls enable

D. fw debug tls on TDERROR_ALL_ALL=5

Correct Answer: B

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk108202

QUESTION 10

Where will the usermode core files be located?

A. /var/log/dump/usermode

B. /var/suroot

C. SFWDIR/var\\'log/dump/usermode

D. SCPDIR/var/log/dump/usermode

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk92764

QUESTION 11

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

QUESTION 12

Some users from your organization have been reporting 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 chain 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 -pi 5 -e

B. fw monitor -pi 5 -e

C. tcpdump -eni any

D. fw monitor -pi asm

Correct Answer: C

QUESTION 13

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 dish?

A. set core-dump enable

B. set core-dump per_process

C. set user-dump enable

D. set core-dump total

Correct Answer: A

QUESTION 14

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

QUESTION 15

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