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.leads4pass.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

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: B

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk92764 [Expert@HostName]# grep cdm /config/db/initial

QUESTION 2

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 3

VPN\\'s allow traffic to pass through the Internet securely by encrypting the traffic as it enters the VPN tunnel and then decrypting the exists. Which process is responsible for Mobile VPN connections?

A. cvpnd

B. vpnd

C. vpnk

D. fwk

Correct Answer: C

QUESTION 4

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 line whereas

(ii) 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

(ii) can be used to debug a unified policy

C. (i) is used to debug only issues related to dropping of 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: A

According to the study material, this should be A:

The Zdebug has a 1 MB buffer, cleans the buffer, enable flags and collects debug messages from the kernel for you.

According to C, it is used for drop traffic, this is completely false

You can set modules on it as well, such as CCP, cluster, fw, drop etc.

Debug requires more configuration to be effective, but gives you more opportunities to play with, therefore, A is the correct answer.

QUESTION 5

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