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.passapply.com/156-585.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

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

QUESTION 3

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

Correct Answer: D

CPM_0_Active - Contains SMC_User Damain, system domain information from both public data and private session CPM_0_Revision - contains revision and public data CPM_Global_A - Contains CP_Data log, APPI, IPS, global domain information for both public data and private session CPM_Global_R - Contail Global revision and pubic data CPM_0_Log - Contains Log data Solr has 2 of these cores CPM_Global_M - contains statuses of SmarView New revision are transfer from active core to revision core once a day at midnight

Reference: http://dkcheckpoint.blogspot.com/2019/12/check-point-certified-security-master.html

QUESTION 4

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 5

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 compiles them together into unified Pattern Matchers?

A. CMI Loader

B. cpas

C. PSL - Passive Signature Loader

D. Context Loader

Correct Answer: A