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.pass4itsure.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

Jenna has to create a VPN tunnel to a CISCO ASA but has to set special property to renegotiate the Phase 2 tunnel after 10 MB of transferee1 data. This can not be configured in the smartconsole, so how can she modify this property?

A. using GUIDBEDIT located in same directory as Smartconsole on the Windows client

B. she need to install GUIDBEDIT which can be downloaded from the Usercenter

C. she need to run GUIDBEDIT from CLISH which opens a graphical window on the smartcenter

D. this cant be done anymore as GUIDBEDIT is not supported in R80 anymore

Correct Answer: C

QUESTION 3

When debugging is enabled on firewall kernel module using the `fw ctl debug\\' command with required options, many debug messages are provided by the kernel that help the administrator to identify issues. Which of the following is true about these debug messages generated by the kernel module?

A. Messages are written to a buffer and collected using `fw ctl kdebug\\'

B. Messages are written to console and also /var/log/messages file

C. Messages are written to /etc/dmesg file

D. Messages are written to $FWDIR/log/fw.elg

Correct Answer: B

QUESTION 4

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

Correct Answer: C

QUESTION 5

The management configuration stored in the Postgres database is partitioned into several relational database Domains, like - System, User, Global and Log Domains. The User Domain stores the network objects and security policies. Which of the following is stored in the Log Domain?

A. Configuration data of Log Servers and saved queries for applications

B. Active Logs received from Security Gateways and Management Servers

C. Active and past logs received from Gateways and Servers

D. Log Domain is not stored in Postgres database, it is part of Solr indexer only

Correct Answer: D