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.geekcert.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

Some users from your organization have been reported 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 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 -pl 5 -e

B. fw monitor -pi 5 -e

C. tcpdump -eni any

D. fw monitor -pl asm

Correct Answer: A

QUESTION 2

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

QUESTION 3

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

Correct Answer: C

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk97638

QUESTION 4

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 5

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

Correct Answer: D