EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : 156-585

Title : Check Point Certified Troubleshooting Expert

Version : DEMO

1.What command is used to find out which port Multi-Portal has assigned to the Mobile Access Portal?
A. mpclient getdata sslvpn
B. netstat -nap | grep mobile
C. mpclient getdata mobi
D. netstat getdata sslvpn
Answer: A

2.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
Answer: A

3.What table does the command "fwaccel conns" pull information from?
A. fwxl_conns
B. SecureXLCon
C. cphwd_db
D. sxl_connections
Answer: C

4.What is the kernel process for Content Awareness that collects the data from the contexts received from the CMI and decides if the file is matched by a data type?
A. dlpda
B. dlpu
C. cntmgr
D. cntawmod
Answer: A

5.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
Answer: A