156-585$^{\text{Q\&As}}$

Check Point Certified Troubleshooting Expert

Pass CheckPoint 156-585 Exam with 100% Guarantee

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

QUESTION 1

Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application and Control Filtering?

A. rad

B. cprad

C. pepd

D. pdpd

Correct Answer: A

QUESTION 2

John works for ABC Corporation. They have enabled CoreXL on their firewall John would like to identify the cores on which the SND runs and the cores on which the firewall instance is running. Which command should John run to view the CPU role allocation?

A. fw ctl affinity -v

B. fwaccel stat -l

C. fw ctl affinity -l

D. fw ctl cores

Correct Answer: C

QUESTION 3

What is the function of the Core Dump Manager utility?

A. To generate a new core dump for analysis

B. To limit the number of core dump files per process as well as the total amount of disk space used by core files

C. To determine which process is slowing down the system

D. To send crash information to an external analyzer

Correct Answer: B

QUESTION 4

Which command(s) will turn off all vpn debug collection?

A. vpn debug off

B. vpn debug -a off

C. vpn debug off and vpn debug ikeoff

D. fw ctl debug 0

Correct Answer: C

QUESTION 5

What are the maximum kernel debug buffer sizes, depending on the version

A. 8MB or 32MB

B. 8GB or 64GB

C. 4MB or 8MB

D. 32MB or 64MB

Correct Answer: A

QUESTION 6

Your users have some issues connecting Mobile Access VPN to the gateway. How can you debug the tunnel establishment?

A. in the file $CVPNDIR/conf/httpd.conf change the line loglevel .. To LogLevel debug and run cvpnrestart

B. run vpn debug truncon

C. run fw ctl zdebug -m sslvpn all

D. in the file $VPNDIR/conf/httpd.conf the line Loglevel .. To LogLevel debug and run vpn restart

Correct Answer: A

QUESTION 7

How many captures does the command "fw monitor -p all" take?

A. All 15 of the inbound and outbound modules

B. All 4 points of the fw VM modules

C. 1 from every inbound and outbound module of the chain

D. The -p option takes the same number of captures, but gathers all of the data packet

Correct Answer: C

QUESTION 8

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

QUESTION 9

Which command is most useful for debugging the fwaccel module?

A. fw zdebug

B. securexl debug

C. fwaccel dbg

D. fw debug

Correct Answer: C

QUESTION 10

What is the purpose of the Hardware Diagnostics Tool?

A. Verifying that Check Point Appliance hardware is functioning correctly

B. Verifying the Security Management Server hardware is functioning correctly

C. Verifying that Security Gateway hardware is functioning correctly

D. Verifying that Check Point Appliance hardware is actually broken

Correct Answer: B

QUESTION 11

Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/

B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/

C. $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/

D. $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

Correct Answer: A

QUESTION 12

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

QUESTION 13

If IPS protections that prevent SecureXL from accelerating traffic, such as Network Quota, Fingerprint Scrambling. TTL Masking etc, have to be used, what is a recommended practice to enhance the performance of the gateway?

A. Use the IPS exception mechanism

B. Disable all such protections

C. Disable SecureXL and use CoreXL

D. Upgrade the hardware to include more Cores and Memory

Correct Answer: A

For protections that prevent SecureXL from accelerating traffic , use the IPS exception mechanism. This mechanism allows SecureXL to accelerate connections that match exception rules. For example, the Network Quota protection does not disable SecureXL templates on connections that match the protection\\'s exception rules.

QUESTION 14

Which daemon governs the Mobile Access VPN blade and works with VPND to create Mobile Access VPN connections? It also handles interactions between HTTPS and the Multi-Portal Daemon.

A. Connectra VPN Daemon - cvpnd

B. Mobile Access Daemon - MAD

C. mvpnd

D. SSL VPN Daemon - sslvpnd

Correct Answer: A

QUESTION 15

What is the correct syntax to set all debug flags for Unified Policy related issues?

A. fw ctl debug -m UP all

B. fw ctl debug -m up all

C. fw ctl kdebug -m UP all

D. fw ctl debug -m fw all

Correct Answer: A