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

Check Point Certified Troubleshooting Expert

Pass CheckPoint 156-585 Exam with 100% Guarantee

QUESTION 1

What process monitors, terminates, and restarts critical Check Point processes as necessary?

A. CPWD

B. CPM

C. FWD

D. FWM

Correct Answer: A

"The Check Point WatchDog (cpwd) is a process that invokes and monitors critical processes such as Check Point daemons on the local computer, and attempts to restart them if they fail." https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_CLI_ReferenceGuide/Topics-CLIG/MDSG/cpwd_admin.htm

QUESTION 2

RAD is initiated when Application Control and URL Filtering blades are active on the Security Gateway What is the purpose of the following RAD configuration file SFWDIR/conf/rad_settings.C?

A. This file contains the location information tor Application Control and/or URL Filtering entitlements

B. This file contains the information on how the Security Gateway reaches the Security Managers RAD service for Application Control and URL Filtering

C. This file contains RAD proxy settings

D. This file contains all the host name settings for the online application detection engine

Correct Answer: B

QUESTION 3

URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync- request forwarded from if a sync-request is required\\'\\'

A. RAD Kernel Space

B. URLF Kernel Client

C. URLF Online Service

D. RAD User Space

Correct Answer: B

QUESTION 4

Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. core dump

B. CPMIL dump

C. fw monitor

D. tcpdump

Correct Answer: A

QUESTION 5

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

Correct Answer: D

QUESTION 6

What table does the command "fwaccel conns" pull information from?

A. fwxl_conns

B. SecureXLCon

C. cphwd_db

D. sxl_connections

Correct Answer: A

QUESTION 7

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 8

What are the four ways to insert an FW Monitor into the firewall kernel chain?

A. Relative position using location, relative position using alias, absolute position, all positions

B. Absolute position using location, absolute position using alias, relative position, all positions

C. Absolute position using location, relative position using alias, general position, all positions

D. Relative position using geolocation, relative position using inertial navigation, absolute position, all positions

Correct Answer: A

Page 22: relative position using a number relative position using an alias absolute position all positions

https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/9068/FILE/How_to_use_FW_Monitor.pdf Start explanation from page 19

QUESTION 9

What file contains the RAD proxy settings?

A. rad_settings.C

B. rad_services.C

C. rad_scheme.C

D. rad_control.C

Correct Answer: A

QUESTION 10

Which process is responsible for the generation of certificates?

A. cpm

B. cpca

C. dbsync D. fwm

Correct Answer: B

QUESTION 11

When running a debug with fw monitor, which parameter will create a more verbose output?

A. -i

B. -i

C. -0

D. -d

Correct Answer: D

QUESTION 12

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 13

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 14

You are trying to establish a VPN tunnel between two Security Gateways but fail. What initial steps will you make to troubleshoot the issue

A. capture traffic on both tunnel members and collect debug of IKE and VPND daemon

B. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags, then collect debug of IKE and VPND daemon

C. collect debug of IKE and VPND daemon and collect kernel debug for fw module with vm, crypt, conn and drop flags

D. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags

Correct Answer: A

QUESTION 15

You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore you need to add a timestamp to the kernel debug and write the output to a file

What is the correct syntax for this?

A. fw ctl kdebug -T -f > filename.debug

B. fw ctl kdebug -T > filename.debug

C. fw ctl debug -T -f > filename.debug

D. fw ctl kdebug -T -f -o filename.debug

Correct Answer: C