CheckPoint

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

NEW QUESTION 1
What are some measures you can take to prevent IPS false positives?

A. Exclude problematic services from being protected by IPS (sip, H 323, etc)
B. Use IPS only in Detect mode
C. Use Recommended IPS profile
D. Capture packet
E. Update the IPS database, and Back up custom IPS files

Answer: A

NEW QUESTION 2
Which command is most useful for debugging the fwaccel module?

A. fw zdebug
B. securexl debug
C. fwaccel dbg
D. fw debug

Answer: C

NEW QUESTION 3
How many tiers of pattern matching can a packet pass through during IPS inspection?

A. 2
B. 1
C. 5
D. 9

Answer: A

NEW QUESTION 4
You have configured IPS Bypass Under Load function with additional kernel parameters ids_tolerance_no_stress=15 and ids_tolerance_stress-15 For configuration you used the *fw ctl set' command After reboot you noticed that these parameters returned to their default values What do you need to do to make this configuration work immediately and stay permanent?

A. Set these parameters again with “fw ctl set” and edit appropriate parameters in $FWDIR/boot/modules/ fwkern.conf
B. Use script $FWDIR/bin IpsSetBypass.sh to set these parameters
C. Set these parameters again with “fw ctl set” and save configuration with “save config”
D. Edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf

Answer: A

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 5
For TCP connections, when a packet arrives at the Firewall Kemel out of sequence or fragmented, which layer of IPS corrects this lo allow for proper inspection?

A. Passive Streaming Library
B. Protections
C. Protocol Parsers
D. Context Management

Answer: D

NEW QUESTION 6
What does SIM handle?

A. Accelerating packets
B. FW kernel to SXL kernel hand off
C. OPSEC connects to SecureXL
D. Hardware communication to the accelerator

Answer: D

NEW QUESTION 7
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

Answer: B

NEW QUESTION 8
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

Answer: C

NEW QUESTION 9
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

Answer: C

NEW QUESTION 10
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

Answer: A

NEW QUESTION 10
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

Answer: A

NEW QUESTION 15
Which of the following is NOT a valid "fwaccel" parameter?

A. stat
B. stats
C. templates
D. packets

Answer: D

NEW QUESTION 19
During firewall kernel debug with fw ctl zdebug you received less information than expected. You noticed that a lot of messages were lost since the time the debug was started. What should you do to resolve this issue?

A. Increase debug buffer; Use fw ctl debug –buf 32768
B. Redirect debug output to file; Use fw ctl zdebug –o ./debug.elg
C. Increase debug buffer; Use fw ctl zdebug –buf 32768
D. Redirect debug output to file; Use fw ctl debug –o ./debug.elg

Answer: A

NEW QUESTION 21
You are upgrading your NOC Firewall (on a Check Point Appliance) from R77 to R80 30 but you did not touch the security policy After the upgrade you can't connect to the new R80 30 SmartConsole of the upgraded Firewall anymore What is a possible reason for this?

A. new new console port is 19009 and a access rule ts missing
B. the license became invalig and the firewall does not start anymore
C. the upgrade process changed the interfaces and IP adresses and you have to switch cables
D. the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall

Answer: D

NEW QUESTION 23
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

Answer: A

NEW QUESTION 27
Where will the usermode core files be located?

A. /var/log/dump/usermode
B. /var/suroot
C. SFWDIR/var'log/dump/usermode
D. SCPDIR/var/log/dump/usermode

Answer: A

NEW QUESTION 30
What command is usually used for general firewall kernel debugging and what is the size of the buffer that is automatically enabled when using the command?

A. fw ctl debug, buffer size is 1024 KB
B. fw ell zdebu
C. buffer size is 32768 KB
D. fw dl zdebug, buffer size is 1 MB
E. fw ctl kdeou
F. buffer size is 32000 KB

Answer: D

NEW QUESTION 31
Which kernel process is used by Content Awareness to collect the data from contexts?

A. dlpda
B. PDP
C. cpemd
D. CMI

Answer: D

NEW QUESTION 36
What acceleration mode utlizes multi-core processing to assist with traffic processing?

A. CoreXL
B. SecureXL
C. HyperThreading
D. Traffic Warping

Answer: C

NEW QUESTION 40
Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0, choose the correct answer.

A. fw monitor –po -0x1ffffe0
B. fw monitor –p0 ox1ffffe0
C. fw monitor –po 1ffffe0
D. fw monitor –p0 –ox1ffffe0

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminG

NEW QUESTION 41
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

Answer: C

NEW QUESTION 43
Which command can be run in Expert mode to verify the core dump settings?

A. grep cdm /config/db/coredump
B. grep cdm /config/db/initial
C. grep $FWDIR/config/db/initial
D. cat /etc/sysconfig/coredump/cdm.conf

Answer: C

NEW QUESTION 48
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: D

NEW QUESTION 50
What table does the command "fwaccel conns" pull information from?

A. fwxl_conns
B. SecureXLCon
C. cphwd_db
D. sxl_connections

Answer: A

NEW QUESTION 52
What process is responsible for sending and receiving logs in the management server?

A. FWD
B. CPM
C. FWM
D. CPD

Answer: A

NEW QUESTION 57
For TCP connections, when a packet arrives at the Firewall Kernel out of sequence or fragmented, which layer of IPS corrects this to allow for proper inspection?

A. Passive Streaming Library
B. Protections
C. Protocol Parsers
D. Context Management

Answer: A

NEW QUESTION 62
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

Answer: C

NEW QUESTION 64
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

Answer: B

NEW QUESTION 67
Which situation triggers an IPS bypass under load on a 24-core Check Point appliance?

A. any of the CPU cores is above the threshold for more than 10 seconds

B. all CPU core most be above the threshold for more than 10 seconds
C. a single CPU core must be above the threshold for more than 10 seconds, but is must be the same core during this time
D. the average cpu utilization over all cores must be above the threshold for 1 second

Answer: A

NEW QUESTION 70
When running a debug with fw monitor, which parameter will create a more verbose output?

A. -i
B. -i
C. -0
D. -d

Answer: D

NEW QUESTION 72
What is the correct syntax to turn a VPN debug on and create new empty debug files?

A. vpn debug truncon
B. vpndebug trunc on
C. vpn kdebug on
D. vpn debug trunkon

Answer: D

NEW QUESTION 75
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: D

NEW QUESTION 79
the difference in debugging a S2S or C2S (using Check Point VPN Client) VPN?

A. there is no difference
B. the C2S VPN uses a different VPN deamon and there a second VPN debug
C. the C2S VPN can not be debugged as it uses different protocols for the key exchange
D. the C2S client uses Browser based SSL vpn and cant be debugged

Answer: D

NEW QUESTION 80
To check the current status of hyper-threading, which command would you execute in expert mode?

A. cat /proc/hypert_status
B. cat /proc/smt_status
C. cat /proc/hypert_stat
D. cat /proc/smt_stat

Answer: B

NEW QUESTION 85
What is the main SecureXL database for tracking acceleration status of traffic?

A. cphwd_db
B. cphwd_tmp1
C. cphwd_dev_conn_table
D. cphwd_dev_identity_table

Answer: B

NEW QUESTION 89
An administrator receives reports about issues with log indexing and text searching regarding an existing Management Server. In trying to find a solution she wants to check if the process responsible for this feature is running correctly. What is true about the related process?

A. fwm manages this database after initialization of the ICA
B. cpd needs to be restarted manual to show in the list
C. fwssd crashes can affect therefore not show in the list
D. solr is a child process of cpm

Answer: D

NEW QUESTION 92

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

156-585 Practice Exam Features:

* 156-585 Questions and Answers Updated Frequently

* 156-585 Practice Questions Verified by Expert Senior Certified Staff

* 156-585 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-585 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year