CheckPoint

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

NEW QUESTION 1
What is the proper command for allowing the system to create core files?

A. $FWDIR/scripts/core-dump-enable.sh
B. # set core-dump enable# save config
C. service core-dump start
D. >set core-dump enable>save config

Answer: D

NEW QUESTION 2
Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

A. cpstat
B. CPstat
C. CPview
D. fwstat

Answer: A

NEW QUESTION 3
How can you start debug of the Unified Policy with all possible flags turned on?

A. fw ctl debug -m UP all
B. fw ctl debug -m UnifiedPolicy all
C. fw ctl debug -m fw + UP
D. fw ctl debug -m UP *

Answer: D

NEW QUESTION 4
When a User Mode process suddenly crashes it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash?
i Program Counter ii Stack Pointer
ii. Memory management information
iv Other Processor and OS flags / information

A. i, ii, Iii and iv
B. i and n only
C. iii and iv only
D. D Only iii

Answer: C

NEW QUESTION 5
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 6
What does CMI stand for in relation to the Access Control Policy?

A. Content Matching Infrastructure
B. Content Management Interface
C. Context Management Infrastructure
D. Context Manipulation Interface

Answer: C

NEW QUESTION 7
What is 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 daemon 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 can’t be debugged

Answer: D

NEW QUESTION 8
What is the buffer size set by the fw ctl zdebug command?

A. 1 MB
B. 1 GB
C. 8MB
D. 8GB

Answer: A

NEW QUESTION 9
Which Daemon should be debugged for HTTPS Inspection related issues?

A. FWD
B. HTTPD
C. WSTLSO
D. VPND

Answer: C

NEW QUESTION 10
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 10
Which process is responsible for the generation of certificates?

A. cpm
B. cpca
C. dbsync
D. fwm

Answer: B

NEW 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

Answer: A

NEW QUESTION 15
What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .cap
B. .exe
C. .tgz
D. .pcap

Answer: A

NEW QUESTION 18
If the cpsemd process of SmartEvent has crashed or is having trouble coming up. then it usually indicates that .

A. Postgres database ts down
B. Cpd daemon is unable to connect to the log server
C. The SmartEvent core on the Solr mdexer has been deleted
D. The logged in administrator does not have permissions to run SmartEvent

Answer: C

NEW QUESTION 23
What are the main components of Check Point's Security Management architecture?

A. Management server, management database, log server, automation server
B. Management server, Security Gatewa
C. Multi-Domain Server, SmartEvent Server
D. Management Serve
E. Log Serve
F. LDAP Server, Web Server
G. Management server Log server, Gateway serve
H. Security server

Answer: A

NEW QUESTION 28
How does the URL Filtering Categorization occur in the kernel?
* 1. RAD provides the status of the search to the client.
* 2. The a-sync request is forwarded to the RAD User space via the RAD kernel for online categorization.
* 3. The online detection service responds with categories and the kernel cache is updated.
* 4. The kernel cache notifies the RAD kernel of hits and misses.
* 5. URL lookup initiated by the client.
* 6. URL lookup occurs in the kernel cache.
* 7. The client sends an a-sync request back to RAD If the URL was not found.

A. 5, 6, 7, 1, 3, 2, 4
B. 5, 6, 2, 4, 1, 7, 3
C. 5, 6, 4, 1, 7, 2, 3
D. 5, 6, 3, 1, 2, 4, 7

Answer: C

NEW QUESTION 33
Check Point Threat Prevention policies can contain multiple policy layers and each layer consists of its own Rule Base Which Threat Prevention daemon is used for Anti-virus?

A. in.emaild.mta
B. in.msd
C. ctasd
D. in emaild

Answer: D

NEW QUESTION 38
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 but you can’t afford to fill up all the remaining disk space and you only have 10 GB free for saving the debugs. What is the correct syntax for this?

A. fw ctl kdebug -T -f -m 10 -s 1000000 -o debugfilename
B. fw ctl kdebug -T -f -m 10 -s 1000000 > debugfilename
C. fw ctl kdebug -T -m 10 -s 1000000 -o debugfilename
D. fw ctl debug -T -f -m 10 -s 1000000 -o debugfilename

Answer: D

NEW QUESTION 43
John has renewed his NGTX License but he gets an error (contract for Anti-Bot expired). He wants to check the subscription status on the CU of the gateway, what command can he use for this?

A. cpstat antimalware -f subscription_status
B. fw monitor license status
C. fwm lie print
D. show license status

Answer: A

NEW QUESTION 47
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

Answer: A

NEW QUESTION 52
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 57
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 58
Which is the correct “fw monitor” syntax for creating a capture file for loading it into WireShark?

A. fw monitor -e “accept<FILTER EXPRESSION>;” >> Output.cap
B. This cannot be accomplished as it is not supported with R80.10
C. fw monitor -e “accept<FILTER EXPRESSION>;” -file Output.cap
D. fw monitor -e “accept<FILTER EXPRESSION>;” -o Output.cap

Answer: D

NEW QUESTION 61
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

NEW QUESTION 62
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 67
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 72
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 73
When debugging is enabled on firewall kernel module using the ‘fw ctl debug’ command with required options, many debug messages are provided by the kernel that help the administrator to identify issues. Which of the following is true about these debug messages generated by the kernel module?

A. Messages are written to a buffer and collected using ‘fw ctl kdebug’
B. Messages are written to console and also /var/log/messages file
C. Messages are written to /etc/dmesg file
D. Messages are written to $FWDIR/log/fw.elg

Answer: B

NEW QUESTION 78
What is the name of the VPN kernel process?

A. VPNK
B. VPND
C. CVPND
D. FWK

Answer: A

NEW QUESTION 81
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 84
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 87
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

Answer: A

NEW QUESTION 92
Which one of the following is NOT considered a Solr core partition:

A. CPM_0_Revisions
B. CPM_Global_A
C. CPM_Gtobal_R
D. CPM_0_Disabled

Answer: D

NEW QUESTION 97
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 98
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

Answer: C

NEW QUESTION 101
......