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
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 3
Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application & Control Filtering?

A. rad
B. cprad
C. pepd
D. pdpd

Answer: A

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
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
What is connect about the Resource Advisor (RAD) service on the Security Gateways?

A. RAD has a kernel module that looks up the kernel cache, notifies client about hits and misses and forwards a-sync requests to RAD user space module which is responsible for online categorization
B. RAD is completely loaded as a kernel module that looks up URL in cache and if not found connects online for categorization There is no user space involvement in this process
C. RAD functions completely in user space The Pattern Matter (PM) module of the CMI looks up for URLs in the cache and if not found, contact the RAD process in user space to do online categorization
D. RAD is not a separate module, it is an integrated function of the 'fw1 kernel module and does all operations in the kernel space

Answer: C

NEW QUESTION 8
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

Answer: A

NEW QUESTION 9
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 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 is the most efficient way to view large fw monitor captures and run filters on the file?

A. wireshark
B. CLISH
C. CLI
D. snoop

Answer: A

NEW QUESTION 19
What are four main database domains?

A. System, Global, Log, Event
B. System, User, Host, Network
C. Local, Global, User, VPN
D. System, User, Global, Log

Answer: D

NEW QUESTION 23
Some users from your organization have been reporting some connection problems with CIFS since this morning You suspect an IPS issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS chain module (position 4 in the chain) to check If the packets pass the IPS. What command do you need to run?

A. fw monitor -ml -pi 5 -e <filterexperession>
B. fw monitor -pi 5 -e <filterexptession>
C. tcpdump -eni any <filterexpression>
D. fw monitor -pi asm <filtefexpfession>

Answer: C

NEW QUESTION 25
What is NOT a benefit of the fw ctl zdebug command?

A. Cannot be used to debug additional modules
B. Collect debug messages from the kernel
C. Clean the buffer
D. Automatically allocate a 1MB buffer

Answer: A

NEW QUESTION 28
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 33
The Check Point Firewall Kernel is the core component of the Gala operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

A. fw ctl debug/kdebug
B. fw ctl zdebug
C. fw debug/kdebug
D. fw debug/kdebug ctl

Answer: B

NEW QUESTION 36
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 41
Some users from your organization have been reported some connection problems with CIFS since this morning. You suspect an IPS Issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS module (position 4 in the chain) to check if the packets pass the IPS. What command do you need to run?

A. fw monitor -ml -pl 5 -e <filterexpression>
B. fw monitor -pi 5 -e <filterexpression>
C. tcpdump -eni any <filterexpression>
D. fw monitor -pl asm <filterexpression>

Answer: A

NEW QUESTION 46
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 48
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 51
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 54
When a User process or program suddenly crashes, a core dump is often used to examine the problem. Which command is used to enable the core-dumping via GAIA dish?

A. set core-dump enable
B. set core-dump per_process
C. set user-dump enable
D. set core-dump total

Answer: A

NEW QUESTION 55
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 57
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 61
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 62
What acceleration mode utilizes multi-core processing to assist with traffic processing?

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

Answer: C

NEW QUESTION 64
Vanessa is reviewing ike.elg file to troubleshoot failed site-to-site VPN connection After sending Mam Mode Packet 5 the response from the peer is PAYLOAD-MALFORMED"
What is the reason for failed VPN connection?

A. The authentication on Phase 1 is causing the problem.Pre-shared key on local gateway encrypted by the hash algorithm created in Packet 3 and Packet 4 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
B. The authentication on Phase 2 is causing the problemPre-shared key on local gateway encrypted by the hash algorithm created in Packets 1 and 2 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
C. The authentication on Quick Mode is causing the problemPre-shared key on local gateway encrypted by the hash algorithm created in Packets 3 and 4 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key
D. The authentication on Phase 1 is causing the problemPre-shared key on local gateway encrypted by the hash algorithm doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key created in Packet 1 and Packet 2

Answer: B

NEW QUESTION 65
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 66
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 67
What process monitors, terminates, and restarts critical Check Point processes as necessary?

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

Answer: A

NEW QUESTION 71
Which Threat Prevention Daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd
B. in.msd
C. ted
D. scrub

Answer: C

NEW QUESTION 73
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 75
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 76
What is the best way to resolve an issue caused by a frozen process?

A. Reboot the machine
B. Restart the process
C. Kill the process
D. Power off the machine

Answer: B

NEW QUESTION 80
The Check Pom! Firewall Kernel is the core component of the Gaia operating system and an integral part of the traffic inspection process There are two procedures available for debugging the firewall kernel Which procedure/command is used for troubleshooting packet drops and other kernel activites while using minimal resources (1 MB buffer)?

A. fw ctl zdebug
B. fw ctl debug/kdebug
C. fwk ctl debug
D. fw debug ctl

Answer: A

NEW QUESTION 83
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 86
How can you increase the ring buffer size to 1024 descriptors?

A. set interface eth0 rx-ringsize 1024
B. fw ctl int rx_ringsize 1024
C. echo rx_ringsize=1024>>/etc/sysconfig/sysctl.conf
D. dbedit>modify properties firewall_properties rx_ringsize 1024

Answer: A

NEW QUESTION 87
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 92
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 94
What is the name of the VPN kernel process?

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

Answer: A

NEW QUESTION 96
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 101
What is the benefit of running "vpn debug trunc over "vpn debug on"?

A. "vpn debug trunc" purges ike.elg and vpnd elg and creates limestarnp while starting ike debug and vpn debug
B. "vpn debug trunc* truncates the capture hence the output contains minimal capture
C. "vpn debug trunc* provides verbose capture
D. No advantage one over the other

Answer: A

NEW QUESTION 102
What table does command “fwaccel conns” pull information from?

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

Answer: A

NEW QUESTION 103
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

Answer: D

NEW QUESTION 107
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 111
What file contains the RAD proxy settings?

A. rad_settings.C
B. rad_services.C
C. rad_scheme.C
D. rad_control.C

Answer: A

NEW QUESTION 112
......