CheckPoint.156-585.v2022-09-16.q47

Exam Code:	156-585
Exam Name:	Check Point Certified Troubleshooting Expert
Certification Provider:	CheckPoint
Free Question Number:	47
Version:	v2022-09-16
# of views:	1169
# of Questions views:	470
https://www.dumpsdb.com/dumps/CheckPoint/156-585/CheckPoint.156-585.v2022-09-16.q47	

NEW QUESTION: 1
Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?
A. fw monitor
B. CPMIL dump
C. core dump
D. tcpdump
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
What is the function of the Core Dump Manager utility?
A. To send crash information to an external analyzer
B. To generate a new core dump for analysis
C. To limit the number of core dump files per process as well as the total amount of disk space used by core files
D. To determine which process is slowing down the system
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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. Context Management

D. Protocol Parsers
Answer: (SHOW ANSWER)

NEW QUESTION: 4
How many captures does the command "fw monitor -p all" take?
A. The -p option takes the same number of captures, but gathers all of the data packet
B. All 15 of the inbound and outbound modules
C. 1 from every inbound and outbound module of the chain
D. All 4 points of the fw VM modules
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
What is the buffer size set by the fw ctl zdebug command?
A. 1 GB
B. 1 MB
C. 8MB
D. 8GB
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which Threat Prevention Daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?
A. ted
B. scrub
C. ctasd
D. in.msd
Answer: (SHOW ANSWER)

NEW QUESTION: 7
PostgreSQL is a powerful, open source relational database management system Check Point offers a command for viewing the database to interact with Postgres interactive shell Which command do you need to enter the PostgreSQL interactive shell?
A. mysql_client cpm postgres
B. psql_client cpm postgres
C. mysql -u root
D. psql_c!ieni postgres cpm
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Your users have some issues connecting Mobile Access VPN to the gateway. How can you debug the tunnel establishment?

A. run vpn debug truncon
B. in the file $CVPNDIR/conf/httpd.conf change the line loglevel .. To LogLevel debug and run cvpnrestart
C. in the file $VPNDIR/conf/httpd.conf the line Loglevel .. To LogLevel debug and run vpn restart
D. run fw ctl zdebug -m sslvpn all
Answer: B (LEAVE A REPLY)

NEW QUESTION: 9
What does CMI stand for in relation to the Access Control Policy?
A. Content Matching Infrastructure
B. Context Manipulation Interface
C. Context Management Infrastructure
D. Content Management Interface
Answer: (SHOW ANSWER)

NEW QUESTION: 10
What are the four ways to insert an FW Monitor into the firewallkernel chain?
A. Absolute position using location, relative position using alias, general position, all positions
B. Absolute position using location, absolute position using alias, relative position, all positions
C. Relative position using geolocation relative position using inertial navigation, absolute position all positions
D. Relative position using location, relativepositionusing alias, absolute position, all positions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
What are some measures you can take to prevent IPS false positives?
A. Use IPS only in Detect mode
B. Exclude problematic services from being protected by IPS (sip, H 323, etc)
C. Use Recommended IPS profile
D. Capture packets. Update the IPS database, and Back up custom IPS files
Answer: (SHOW ANSWER)

NEW QUESTION: 12
What table does the command "fwaccel conns" pull information from?
A. sxl_connections
B. cphwd_db
C. fwxl_conns
D. SecureXLCon
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
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. Increase debug buffer; Use fw ctl zdebug -buf 32768
C. Redirect debug output to file; Use fw ctl debug -o ./debug.elg
D. Redirect debug output to file; Use fw ctl zdebug -o ./debug.elg
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
How many captures does the command "fw monitor -p all" take?
A. The -p option takes the same number of captures, but gathers all of the data packet
B. 1 from every inbound and outbound module of the chain
C. All 15 of the inbound and outbound modules
D. All 4 points of the fw VM modules
Answer: C (LEAVE A REPLY)

NEW QUESTION: 15
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. CPview
C. cpstat
D. fwstat
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
Jenna has to create a VPN tunnel to a CISCO ASA but has to set special property to renegotiate the Phase 2 tunnel after 10 MB of transferee1 dat a. This can not be configured in the smartconsole, so how can she modify this property?
A. this cant be done anymore as GUIDBEDIT is not supported in R80 anymore
B. using GUIDBEDIT located in same directory as Smartconsole on the Windows client
C. she need to install GUIDBEDIT which can be downloaded from the Usercenter
D. she need to run GUIDBEDIT from CLISH which opens a graphical window on the smartcenter
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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. show license status
C. fwm lie print
D. fw monitor license status
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
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 doesn't match with the hash on the peer gateway generated by encrypting its pre-shared key created in Packet 1 and Packet 2
B. The authentication on Quick Mode is causing the problem
Pre-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
C. 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
D. The authentication on Phase 2 is causing the problem
Pre-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
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19

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. cp debug truncon
B. vpn debug truncon
C. fw debug truncon
D. vpn truncon debug
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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. cntawmod
B. dlpu
C. dlpda
D. cntmgr
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
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. Protocol Parsers
B. Context Management
C. Protections
D. Passive Streaming Library
Answer: (SHOW ANSWER)

NEW QUESTION: 22
What command is usedtofind out which port Multi-Portal has assigned to the Mobile Access Portal?
A. mpclient getdata mobi
B. netstat -nap | grep mobile
C. mpclient getdata sslvpn
D. netstat getdata sslvpn
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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. D Only iii
B. iii and iv only
C. i, ii, lii and iv
D. i and n only
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
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_firewall_imp/ANTIMALWARE/conf/
B. $FWDIR/log/install_manager_tmp/ANTIMALWARBlog?
C. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
D. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which of the following is contained in the System Domain of the Postgres database?
A. Trusted GUI clients
B. Configuration data of log servers
C. User modified configurations such as network objects
D. Saved queries for applications
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
What is the proper command for allowing the system to create core files?
A. >set core-dump enable
>save config
B. $FWDIR/scripts/core-dump-enable.sh
C. service core-dump start
D. # set core-dump enable
save config
Answer: (SHOW ANSWER)

NEW QUESTION: 27
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: (SHOW ANSWER)

NEW QUESTION: 28
What is the difference in debugging a S2S or C2S (using Check Point VPN Client) VPN?
A. the C2S VPN can not be debugged as it uses different protocols for the key exchange
B. the C2S client uses Browser based SSL vpn and can't be debugged
C. the C2S VPN uses a different VPN daemon and there a second VPN debug
D. there is no difference
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which of the following daemons is used for Threat Extraction?
A. scrubd
B. tex
C. tedex
D. extractd
Answer: (SHOW ANSWER)

NEW QUESTION: 30
What file contains the RAD proxy settings?
A. rad_control.C
B. rad_services.C
C. rad_scheme.C
D. rad_settings.C
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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. solr is a child process of cpm
B. fwm manages this database after initialization of the ICA
C. fwssd crashes can affect therefore not show in the list
D. cpd needs to be restarted manual to show in the list
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
The two procedures available for debugging in the firewall kernel are
i fw ctl zdebug
ii fw ctl debug/kdebug
Choose the correct statement explaining the differences in the two
A. (i) is used to debug the access control policy only, however (n) can be used to debug a unified policy
B. (i) is used to debug only issues related to dropping of traffic, however (n) can be used for any firewall issue including NATing, clustering etc.
C. (i) Is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to get an output via command line whereas (11) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line
D. (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which command(s) will turn off all vpn debug collection?
A. fw ctl debug 0
B. vpn debug -a off
C. vpn debug off and vpn debug ikeoff
D. vpn debug off
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
VPN issues may result from misconfiguration, communication failure, or incompatible default configurations between peers Which basic command syntax needs to be used fortroubleshootingSite-to-Site VPN Issues?
A. vpn truncon debug
B. vpn debug truncon
C. cp debug truncon
D. fw debug truncon
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
The customer is using Check Point appliances that were configured long ago by third-party administrators. Current policy includes different enabled IPS protections and Bypass Under Load function. Bypass Under Load is configured to disable IPS inspections of CPU and Memory usage is higher than 80%. The Customer reports that IPS protections are not working at all regardless of CPU and Memory usage.
What is the possible reason of such behavior?
A. The kernel parameter ids_tolerance_no_stress is set to 10
B. The kernel parameter ids_assume_stress is set to 1
C. The kernel parameter ids_assume_stress is set to 0
D. The kernel parameter ids_tolerance_stress is set to 10
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
Which situation triggers an IPS bypass under load on a 24-core Check Point appliance?
A. the average cpu utilization over all cores must be above the threshold for 1 second
B. any of the CPU cores is above the threshold for more than 10 seconds
C. all CPU core most be above the threshold for more than 10 seconds
D. a single CPU core must be above the threshold for more than 10 seconds, but is must be the same core during this time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
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. tcpdump -eni any <filterexpression>
B. fw monitor -pi 5 -e <filterexptession>
C. fw monitor -pi asm <filtefexpfession>
D. fw monitor -ml -pi 5 -e <filterexperession>
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
How many tiers of pattern matching can a packet pass through during IPS inspection?
A. 5
B. 2
C. 1
D. 9

Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
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. SSL VPN Daemon - sslvpnd
B. Connectra VPN Daemon - cvpnd
C. mvpnd
D. Mobile Access Daemon - MAD
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
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. show license status
B. cpstat antimalware -l subscription _status
C. fw monitor license status
D. fwm lie print
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
What is the purpose of the Hardware Diagnostics Tool?
A. Verifying the Security Management Server hardware is functioning correctly
B. Verifying that Security Gateway hardware is functioning correctly
C. Verifying that Check Point Appliance hardware is actually broken
D. Verifying that Check Point Appliance hardware is functioning correctly
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
Which of the following is NOT a valid "fwaccel" parameter?
A. stats
B. stat
C. packets
D. templates
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
What process is responsible for sending and receiving logs in the management server?
A. CPD

B. CPM
C. FWM
D. FWD
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
What are the maximum kernel debug buffer sizes, depending on the version
A. 32MB or 64MB
B. 8MB or 32MB
C. 4MB or 8MB
D. 8GB or 64GB
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
What acceleration mode utlizes multi-core processing to assist with traffic processing?
A. SecureXL
B. HyperThreading
C. CoreXL
D. Traffic Warping
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
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. the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall
B. new new console port is 19009 and a access rule ts missing
C. the license became invalig and the firewall does not start anymore
D. the upgrade process changed the interfaces and IP adresses and you have to switch cables
Answer: A (LEAVE A REPLY)

NEW QUESTION: 47
How can you start debug of the Unified Policy with all possible flags turned on?
A. fw ctl debug -m fw + UP
B. fw ctl debug -m UnifiedPolicy all
C. fw ctl debug -m UP all
D. fw ctl debug -m UP *
Answer: D (LEAVE A REPLY)