Exam Questions 156-585

Check Point Certified Troubleshooting Expert

https://www.2passeasy.com/dumps/156-585/

NEW QUESTION 1
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 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
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_manager_tmp/ANTIMALWARE/conf/
B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
C. $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/
D. $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

Answer: A

NEW QUESTION 4
James is using the same filter expression in fw monitor for CITRIX very often and instead of typing this all the time he wants to add it as a macro to the fw monitor definition file. What's the name and location of this file?

A. $FWDIR/lib/fwmonltor.def
B. $FWDIR/conf/fwmonltor.def
C. $FWDIR/lib/tcpip.def
D. $FWDIR/lib/fw.monitor

Answer: A

NEW QUESTION 5
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 6
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 7
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 8

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 9
What is the main SecureXL database for tracking the acceleration status of traffic?

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

Answer: D

NEW QUESTION 10
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 10
Which Daemon should be debugged for HTTPS Inspection related issues?

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

Answer: C

NEW QUESTION 12
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 data. This can not be configured in the smartconsole, so how can she modify this property?

A. using GUIDBEDIT located in same directory as Smartconsole on the Windows client
B. she need to install GUIDBEDIT which can be downloaded from the Usercenter
C. she need to run GUIDBEDIT from CLISH which opens a graphical window on the smartcenter
D. this cant be done anymore as GUIDBEDIT is not supported in R80 anymore

Answer: C

NEW 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

Answer: C

NEW QUESTION 17
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

Answer: D

NEW QUESTION 19
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

Answer: D

NEW QUESTION 23
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 25
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_assume_stress is set to 0
B. The kernel parameter ids_assume_stress is set to 1
C. The kernel parameter ids_tolerance_no_stress is set to 10
D. The kernel parameter ids_tolerance_stress is set to 10

Answer: D

NEW QUESTION 28
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 32
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 35
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 40
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 41
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 44
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. psql_client cpm postgres
B. mysql_client cpm postgres
C. psql_c!ieni postgres cpm
D. mysql -u root

Answer: A

NEW QUESTION 47
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 48
In Security Management High Availability, if the primary and secondary managements, running the same version of R80.x, are in a state of ‘Collision’, how can this be resolved?

A. Administrator should manually synchronize the servers using SmartConsole
B. The Collision state does not happen in R80.x as the synchronizing automatically on every publish action
C. Reset the SIC of the secondary management server
D. Run the command ‘fw send synch force’ on the primary server and ‘fw get sync quiet’ on the secondary server

Answer: A

NEW QUESTION 52
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 55
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 59
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 63
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 67
What is the function of the Core Dump Manager utility?

A. To generate a new core dump for analysis
B. To limit the number of core dump files per process as well as the total amount of disk space used by core files
C. To determine which process is slowing down the system
D. To send crash information to an external analyzer

Answer: B

NEW QUESTION 72
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 73
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 78
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 82
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

Answer: B

NEW QUESTION 84
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 86
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 90
After kernel debug with "fw ctl debug" you received a huge amount of information It was saved in a very large file that is difficult to open and analyze with standard text editors Suggest a solution to solve this issue.

A. Use "fw ctl zdebug' because of 1024KB buffer size
B. Divide debug information into smaller files Use "fw ctl kdebug -f -o "filename" -m 25 - s "1024"
C. Reduce debug buffer to 1024KB and run debug for several times
D. Use Check Point InfoView utility to analyze debug output

Answer: C

NEW QUESTION 93
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 96
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 101
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 103
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 107
What is the name of the VPN kernel process?

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

Answer: A

NEW QUESTION 112
Check Point Access Control Daemons contains several daemons for Software Blades and features Which Daemon is used for Application & Control URL Filtering?

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

Answer: C

NEW QUESTION 114
What table does command “fwaccel conns” pull information from?

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

Answer: A

NEW QUESTION 116
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 119
What command sets a specific interface as not accelerated?

A. noaccel-s<interface1>
B. fwaccel exempt state <interface1>
C. nonaccel -s <interface1>
D. fwaccel -n <intetface1 >

Answer: C

NEW QUESTION 123
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 125
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 127
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 129

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 -I
C. fw ctl affinity -I
D. fw ctl cores

Answer: C

NEW QUESTION 131
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-585 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-585 Product From:

https://www.2passeasy.com/dumps/156-585/

Money Back Guarantee

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