

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

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



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

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_imp/ANTIMALWARE/conf/
- C. \$FWDIR/conf/install_firewall_imp/ANTIMALWARE/conf/
- D. \$FWDIR/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

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
- iii 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 6

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 7

What components make up the Context Management Infrastructure?

- A. CMI Loader and Pattern Matcher
- B. CPMI and FW Loader
- C. CPX and FWM
- D. CPM and SOLR

Answer: A

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

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 10

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 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 13

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 16

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. dlpd
- C. cntmgr
- D. cntawmod

Answer: D

NEW QUESTION 21

If you run the command "fw monitor -e accept src=10.1.1.201 or src=172.21.101.10 or src=192.0.2.10;" from the cli sh What will be captured?

- A. Packets from 10 1 1 201 going to 192.0 2.10
- B. Packets destined to 172 21 101 10 from 10.1.1.101

- C. Only packet going to 192.0.2.10
- D. fw monitor only works in expert mode so no packets will be captured

Answer: C

NEW QUESTION 25

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 27

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

Answer: C

NEW QUESTION 30

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 34

The management configuration stored in the Postgres database is partitioned into several relational database Domains, like - System, User, Global and Log Domains. The User Domain stores the network objects and security policies. Which of the following is stored in the Log Domain?

- A. Configuration data of Log Servers and saved queries for applications
- B. Active Logs received from Security Gateways and Management Servers
- C. Active and past logs received from Gateways and Servers
- D. Log Domain is not stored in Postgres database, it is part of Solr indexer only

Answer: D

NEW QUESTION 38

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 Gateway
- C. Multi-Domain Server, SmartEvent Server
- D. Management Server
- E. Log Server
- F. LDAP Server, Web Server
- G. Management server Log server, Gateway server
- H. Security server

Answer: A

NEW QUESTION 43

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

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 50

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 53

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 57

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 SFWDIR/config/db/initial
- D. cat /etc/sysconfig/coredump/cdm conf

Answer: C

NEW QUESTION 60

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 65

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 invalid and the firewall does not start anymore
- C. the upgrade process changed the interfaces and IP addresses 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 70

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 72

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 74

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 78

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 79

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 81

Joey is configuring a site-to-site VPN with his business partner. On Joey’s site he has a Check Point R80.10 Gateway and his partner uses Cisco ASA 5540 as a gateway.

Joey’s VPN domain on the Check Point Gateway object is manually configured with a group object that contains two network objects:

VPN_Domain3 = 192.168.14.0/24 VPN_Domain4 = 192.168.15.0/24

Partner’s site ACL as viewed from “show run”

access-list JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.14.0 255.255.255.0

access-list JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.15.0 255.255.255.0 When they try to establish VPN tunnel, it fails. What is the most likely cause of the failure given the information provided?

- A. Tunnel falls on partner sit
- B. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation.Check Point continues to present its own encryption domain as 192.168.14.0/24 and 192.168.15.0/24, but the peer expects the one network 192.168.14.0/23
- C. Tunnel falls on partner sit
- D. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation.Check Point continues to present its own encryption domain as 192.168.14.0/23, but the peer expects the two distinct networks 192.168.14.0/24 and 192.168.15.0/24.
- E. Tunnel fails on Joey’s site, because he misconfigured IP address of VPN peer.
- F. Tunnel falls on partner sit
- G. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

Answer: B

NEW QUESTION 85

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 86

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 91

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 92

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 93

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 95

The Check Point 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 activities while using minimal resources (1 MB buffer)?

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

Answer: A

NEW QUESTION 98

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 must 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 it 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 103

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 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 (ii) 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
- B. (i) is used to debug the access control policy only, however (ii) can be used to debug a unified policy
- C. (i) is used to debug only issues related to dropping of traffic, however (ii) can be used for any firewall issue including NATing, clustering etc.

D. (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server

Answer: C

NEW QUESTION 108

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

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

Answer: A

NEW QUESTION 111

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 114

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 cant be debugged

Answer: D

NEW QUESTION 118

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 121

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 123

Which of the following daemons is used for Threat Extraction?

- A. scrubd
- B. extractd
- C. tex
- D. tedex

Answer: A

NEW QUESTION 128

Which of the following inputs is suitable for debugging HTTPS inspection issues?

- A. vpn debug cptls on
- B. fw ctl debug -m fw + conn drop cptls
- C. fw diag debug tls enable
- D. fw debug tls on TDERROR_ALL_ALL=5

Answer: B

NEW QUESTION 132

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 135

.....

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