

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

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



NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

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 7

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 8

Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS. and compiles them together into unified Pattern Matchers?

- A. CMI Loader
- B. cpas
- C. PSL - Passive Signature Loader
- D. Context Loader

Answer: A

NEW QUESTION 9

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

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

Your fwm constantly crashes and is restarted by the watchdog. You can't find any coredumps related to this process, so you need to check If coredumps are enabled at all How can you achieve that?

- A. in dish run show core-dump status
- B. in expert mode run show core-dump status
- C. in dish run set core-dump status
- D. in dish run show coredumb status

Answer: D

NEW QUESTION 12

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 15

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 18

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 21

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 26

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 30

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 33

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 34

You are running R80.XX on an open server and you see a high CPU utilization on your 12 CPU cores You now want to enable Hyperthreading to get more cores to gain some performance. What is the correct way to achieve this?

- A. Hyperthreading is not supported on open servers, on on Check Point Appliances
- B. just turn on HAT in the bios of the server and boot it
- C. just turn on HAT in the bios of the server and after it has booted enable it in cpconfig
- D. in dish run set HAT on

Answer: A

NEW QUESTION 35

Check Point's PostgreSQL is partitioned into several relational database domains. Which domain contains network objects and security policies?

- A. User Domain
- B. System Domain
- C. Global Domain
- D. Log Domain

Answer: C

NEW QUESTION 38

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 39

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 40

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 43

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 47

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 50

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 51

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 52

Which of the following is contained in the System Domain of the Postgres database?

- A. Saved queries for applications
- B. Configuration data of log servers
- C. Trusted GUI clients
- D. User modified configurations such as network objects

Answer: C

NEW QUESTION 53

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 55

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 58

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 61

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 65

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 68

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 69

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 73

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. fwk ctl debug
- D. fw debug ctl

Answer: A

NEW QUESTION 76

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 80

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 85

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 88

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 90

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 93

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 (ii) is used on a Security Management Server

Answer: C

NEW QUESTION 96

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 98

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 99

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 103

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 108

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 110

.....

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