

156-585 Dumps

Check Point Certified Troubleshooting Expert

<https://www.certleader.com/156-585-dumps.html>



NEW QUESTION 1

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 2

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 3

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 4

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: D

NEW QUESTION 5

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 6

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 7

Select the technology that does the following actions

- provides reassembly via streaming for TCP
- handles packet reordering and congestion
- handles payload overlap
- provides consistent stream of data to protocol parsers

- A. Passive Streaming Library

- B. Context Management
- C. Pre-Protocol Parser
- D. fwtcpstream

Answer: A

NEW QUESTION 8

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 for 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 9

Which Daemon should be debugged for HTTPS Inspection related issues?

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

Answer: C

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

Which process is responsible for the generation of certificates?

- A. cpm
- B. cpcap
- C. dbsync
- D. fwm

Answer: B

NEW QUESTION 11

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 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 18

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 20

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 22

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 24

Troubleshooting issues with Mobile Access requires the following:

- A. Standard VPN debugs, packet captures, and debugs of cvpnd' process on Security Gateway
- B. Standard VPN debugs and packet captures on Security Gateway, debugs of "cvpnd" process on Security Management
- C. 'ma_vpnd' process on Security Gateway
- D. Debug logs of FWD captured with the command - 'fw debug fwd on TDERROR_MOBILE_ACCESS=5'

Answer: A

NEW QUESTION 27

The Check Point Firewall Kernel is the core component of the Gaia 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 32

How many captures does the command "fw monitor -p all" take?

- A. All 15 of the inbound and outbound modules
- B. All 4 points of the fw VM modules
- C. 1 from every inbound and outbound module of the chain
- D. The -p option takes the same number of captures, but gathers all of the data packet

Answer: C

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, only 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 37

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 39

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 42

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 47

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 49

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 52

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 56

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 60

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 68

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 73

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 77

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 82

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 84

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 85

What is the name of the VPN kernel process?

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

Answer: A

NEW QUESTION 88

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 93

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 95

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 100

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 102

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 104

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 156-585 Exam with Our Prep Materials Via below:

<https://www.certleader.com/156-585-dumps.html>