CheckPoint 156-587 CCTE Practice Questions

Shared by Kemp on 24-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You want to fully investigate the VPN establishment, what will you do?

Options:

A- vpn debug and use IKEview
B- debug FWD because VPND Is child process
C- use vpn tu command and use option 8 to start debug
D- use kernel debug with fw ctl debug -m VPN all

Answer:

A

Question 2

Question Type: MultipleChoice

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?

Options:

A- fw ctl debug, buffer size is 1024 KB
B- fw ctl zdebug, buffer size is 1 MB
C- fw ctl kdebug, buffer size is 32000 KB
D- fw ctl zdebug, buffer size is 32768 KB

Answer:

D

Question 3

Question Type: MultipleChoice

Which of the following daemons is used for Threat Extraction?

Options:

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

Answer:

A

Question 4

Question Type: MultipleChoice

During firewall kernel debug with fw ctl zdebug you received less information that 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?

Options:

A- Increase debug buffer Use fw ctl debug -buf 32768
B- Redirect debug output to file; Use fw ctl debug -o /debug.elg
C- Redirect debug output to file; Use fw ctl zdebug -o /debug.elg
D- Increase debug buffer; Use fw ctl zdebug -buf 32768

Answer:

A

Question 5

Question Type: MultipleChoice

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

Options:

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

Answer:

D

Explanation:

One possible solution to solve the issue of having a very large file that is difficult to open and analyze with standard text editors is to divide the debug information into smaller files. This can be done by using thefw ctl kdebugcommand with the-f,-o,-m, and-soptions. The-foption means to write the debug output to a file instead of the screen. The-ooption specifies the name of the output file. The-moption sets the maximum number of files to be created. The-soption sets the maximum size of each file in KB. For example, the commandfw ctl kdebug -f -o debug -m 25 -s 1024will create up to 25 files named debug.0, debug.1, ..., debug.24, each with a maximum size of 1024KB. This way, the debug information can be split into more manageable chunks that can be opened and analyzed more easily with standard text editors.

1: How to use ''fw ctl kdebug'' command

2: How to debug Check Point firewalls

3: Check Point CLI Reference Card

Question 6

Question Type: MultipleChoice

You need to monitor traffic pre-inbound and before the VPN module in a Security Gateway. How would you achieve this using fw monitor?

Options:

A- fw monitor -p all
B- fw monitor -pi -vpn
C- fw monitor -pi +vpn
D- RAD is completely loaded as a kernel module that looks up URL in cache and if not found connects online for categorization There is no user space involvement in this process

Answer:

B

Explanation:

The fw monitor command is a powerful troubleshooting tool in Check Point Gateways that captures packets at various points in the processing chain. The question asks how to capture traffic pre-inbound (before inbound processing, i.e., at the ''i'' inspection point) and before the VPN module (before VPN decryption or processing).

The fw monitor syntax allows specifying inspection points using options like -pi (pre-inbound) and module names (e.g., -vpn for the VPN module). The correct syntax to capture traffic before a specific module is -pi -<module>, where the module name is prefixed with a minus sign to indicate ''before'' the module.

Option A: Incorrect. fw monitor -p all captures packets at all inspection points in the chain, which includes pre-inbound, post-inbound, pre-outbound, and post-outbound points, as well as points around all modules. This is too broad and does not specifically target pre-inbound and before the VPN module.

Option B: Correct. fw monitor -pi -vpn captures packets at the pre-inbound inspection point (''i'') and before the VPN module (-vpn). The -pi specifies the pre-inbound point, and -vpn ensures the capture occurs before VPN processing (e.g., decryption).

Option C: Incorrect. fw monitor -pi +vpn would capture packets at the pre-inbound point but after the VPN module (+vpn indicates after the module), which contradicts the requirement to capture before the VPN module.

Option D: Incorrect. This option is a duplicate of Option C in the provided question, likely a typographical error. Even if corrected, +vpn is incorrect for the same reason as Option C.

The Check Point R81.20 Gaia Administration Guide explains the fw monitor command and its options, including how to specify inspection points and module positions. The CCTE R81.20 course includes hands-on labs for using fw monitor to troubleshoot packet flow, emphasizing precise inspection point selection.

For precise details, refer to:

Check Point R81.20 Gaia Administration Guide, section on ''fw monitor'' (available via Check Point Support Center).

CCTE R81.20 Courseware, which covers advanced packet capture techniques with fw monitor (available through authorized training partners).

Question 7

Question Type: MultipleChoice

When URL category is not found in the kernel cache, what action will GW do?

Options:

A- RAD In user space will forward request to the cloud
B- GW will update kernel cache during next policy install
C- RAD in kernel space will forward request to the cloud
D- RAD forwards this request to CMI which is the brain of inspection

Answer:

A

Question 8

Question Type: MultipleChoice

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

Options:

A- iii and iv only
B- i and ii only
C- i, ii, iii and iv

D- Only lii

Answer:

C

Explanation:

A core dump file is essentially a snapshot of the process's memory at the time of the crash. This snapshot includes crucial information that can help diagnose the cause of the crash. Here's why all the options are relevant:

i. Program Counter: This register stores the address of the next instruction the CPU was supposed to execute. It pinpoints exactly where in the code the crash occurred.

ii. Stack Pointer: This register points to the top of the call stack, which shows the sequence of function calls that led to the crash. This helps trace the program's execution flow before the crash.

iii. Memory management information: This includes details about the process's memory allocations, which can reveal issues like memory leaks or invalid memory access attempts.

iv. Other Processor and OS flags/information: This encompasses various registers and system information that provide context about the state of the processor and operating system at the time of the crash.

By analyzing this information within the core dump, you can often identify the root cause of the crash, such as a segmentation fault, null pointer dereference, or stack overflow.

Check Point Troubleshooting Reference:

While core dumps are a general concept in operating systems, Check Point's documentation touches upon them in the context of troubleshooting specific processes like fwd (firewall) or cpd (Check Point daemon). The fw ctl zdebug command, for example, can be used to trigger a core dump of the fwd process for debugging purposes.

Question 9

Question Type: MultipleChoice

What cli command is run on the GW to verify communication to the identity Collector?

Options:

A- pdp connections idc
B- pep connections idc
C- show idc connections
D- fwd connected

Answer:

A

Question 10

Question Type: MultipleChoice

When debugging is enabled on firewall kernel module using the fw ctl debug' command with required options, many debug messages are provided by the kernel that help the administrator to identify

Issues. Which of the following is true about these debug messages generated by the kernel module?

Options:

A- Messages are written to /etc/dmesg file
B- Messages are written to a buffer and collected using 'fw ctl kdebug
C- Messages are written to SFWDIR
D- Messages are written to console and also /var/log/messages file

Answer:

B