CERTSinside

Free Questions for 156-585 by certsinside

Shared by Richmond on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What acceleration mode utilizes multi-core processing to assist with traffic processing?

Options:

A- CoreXL

B- SecureXL

C- HyperThreading

D- Traffic Warping

Answer:

C

Question 2

Question Type: MultipleChoice

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?

Options:

A- Passive Streaming Library

B- Protections

C- Protocol Parsers

D- Context Management

Answer:

A

Question 3

Question Type: **MultipleChoice**

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?

Options:

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

Question 4

Question Type: **MultipleChoice**

What is the correct syntax to set all debug flags for Unified Policy related issues?

Options:

A- fw ctl debug -m UP all

B- fw ctl debug -m up all

C- fw ctl kdebug -m UP all

D- fw ctl debug -m fw all

Answer:

A

Question 5

Question Type: MultipleChoice

To check the current status of hyper-threading, which command would you execute in expert mode?

Options:

A- cat /proc/hypert_status

B- cat /proc/smt_status

C- cat /proc/hypert_stat

D- cat /proc/smt_stat

Answer:

B

Question 6

Question Type: MultipleChoice

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.

Options:

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

Question 7

Question Type: **MultipleChoice**

What is the most efficient way to view large fw monitor captures and run filters on the file?

Options:

A- wireshark

B- CLISH

C- CLI

D- snoop

Answer:

A

Question 8

Question Type: MultipleChoice

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?

Options:

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

Question 9

Question Type: MultipleChoice

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?

Options:

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

Question 10

Question Type: **MultipleChoice**

Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

Options:

A- cpstat

B- CPstat

C- CPview

D- fwstat

Answer:

A

To Get Premium Files for 156-585 Visit

https://www.p2pexams.com/products/156-585

For More Free Questions Visit

https://www.p2pexams.com/checkpoint/pdf/156-585

20%
DISCOUNT