DUMPSARENA

Check Point Certified Troubleshooting Expert

Checkpoint 156-585

Version Demo

Total Demo Questions: 10

Total Premium Questions: 75

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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 difference 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 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

QUESTION NO: 2

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

QUESTION NO: 3

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

QUESTION NO: 4

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 complies them together into unified Pattern Matchers?

A. CMI Loader

B. cpas

C. PSL - Passive Signature Loader

D. Context Loader

ANSWER: A

QUESTION NO: 5

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

QUESTION NO: 6

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

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 NO: 7

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 site. 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

B. Tunnel fails on partner site. 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.

C. Tunnel fails on Joey's site, because he misconfigured IP address of VPN peer.

D. Tunnel falls on partner site. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

ANSWER: B

QUESTION NO: 8

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

QUESTION NO: 9

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

QUESTION NO: 10

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