156-585 Q&As

Check Point Certified Troubleshooting Expert

Pass CheckPoint 156-585 Exam with 100% Guarantee

QUESTION 1

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

Correct Answer: D

QUESTION 2

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

Correct Answer: D

QUESTION 3

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

Correct Answer: A

QUESTION 4

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

Correct Answer: C

QUESTION 5

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.

Correct Answer: B

QUESTION 6

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

What is the correct syntax for this?

A. fw ctl kdebug -T -f > filename.debug

B. fw ctl kdebug -T > filename.debug

C. fw ctl debug -T -f > filename.debug

D. fw ctl kdebug -T -f -o filename.debug

Correct Answer: C

QUESTION 7

Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application and Control Filtering?

A. rad

B. cprad

C. pepd

D. pdpd

Correct Answer: A

QUESTION 8

Vanessa is reviewing ike.elg file to troubleshoot failed site-to-site VPN connection After sending Mam Mode Packet 5 the response from the peer is PAYLOAD-MALFORMED" What is the reason for failed VPN connection?

A. The authentication on Phase 1 is causing the problem.Pre-shared key on local gateway encrypted by the hash algorithm created in Packet 3 and Packet 4 doesn\\'t match with the hash on the peer gateway generated by encrypting its preshared key

B. The authentication on Phase 2 is causing the problem Pre-shared key on local gateway encrypted by the hash algorithm created in Packets 1 and 2 doesn\\'t match with the hash on the peer gateway generated by encrypting its pre-shared key

C. The authentication on Quick Mode is causing the problem Pre-shared key on local gateway encrypted by the hash algorithm created in Packets 3 and 4 doesn\\'t match with the hash on the peer gateway generated by encrypting its preshared key

D. The authentication on Phase 1 is causing the problem Pre-shared key on local gateway encrypted by the hash algorithm doesn\\'t match with the hash on the peer gateway generated by encrypting its pre-shared key created in Packet 1 and Packet 2

Correct Answer: B

QUESTION 9

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 $FWDIR/config/db/initial

D. cat /etc/sysconfig/coredump/cdm.conf

Correct Answer: B

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk92764 [Expert@HostName]# grep cdm /config/db/initial

QUESTION 10

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?

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

Correct Answer: B

B: ids_assume_stress, 1 = IDS mechanism assumes that the Security Gateway is under stress, regardless of the actual utilization of CPU and memory. ref sk62848: How to tune the "Bypass under Load" IPS settings

QUESTION 11

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

Correct Answer: C

QUESTION 12

If IPS protections that prevent SecureXL from accelerating traffic, such as Network Quota, Fingerprint Scrambling. TTL Masking etc, have to be used, what is a recommended practice to enhance the performance of the gateway?

A. Use the IPS exception mechanism

B. Disable all such protections

C. Disable SecureXL and use CoreXL

D. Upgrade the hardware to include more Cores and Memory

Correct Answer: A

For protections that prevent SecureXL from accelerating traffic , use the IPS exception mechanism. This mechanism allows SecureXL to accelerate connections that match exception rules. For example, the Network Quota protection does not disable SecureXL templates on connections that match the protection\\'s exception rules.

QUESTION 13

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

Correct Answer: A

QUESTION 14

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

Correct Answer: A

QUESTION 15

Which of the following is NOT a valid "fwaccel" parameter?

A. stat

B. stats

C. templates

D. packets

Correct Answer: D

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk41397