Vendor: CheckPoint

Exam Code:156-585

Exam Name: Check Point Certified Troubleshooting Expert

Version: Demo

QUESTION 1

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 2

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 3

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

Correct Answer: C

QUESTION 4

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 5

If you run the command "fw monitor -e accept src=10.1.1.201 or src=172.21.101.10 or src=192.0.2.10;" from the cli sh What will be captured?

A. Packets from 10 1 1 201 going to 192.0 2.10

B. Packets destined to 172 21 101 10 from 10.1.1.101

C. Only packet going to 192.0.2.10

D. fw monitor only works in expert mode so no packets will be captured

Correct Answer: C

QUESTION 6

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

Correct Answer: C

QUESTION 7

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

Correct Answer: A

QUESTION 8

Where will the usermode core files be located?

A. /var/log/dump/usermode

B. /var/suroot

C. SFWDlR/var\\'log/dump/usermode

D. SCPDIR/var/log/dump/usermode

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk92764

QUESTION 9

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

Correct Answer: A

QUESTION 10

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 11

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 differences 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 of 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

Correct Answer: A

According to the study material, this should be A:

The Zdebug has a 1 MB buffer, cleans the buffer, enable flags and collects debug messages from the kernel for you.

According to C, it is used for drop traffic, this is completely false

You can set modules on it as well, such as CCP, cluster, fw, drop etc.

Debug requires more configuration to be effective, but gives you more opportunities to play with, therefore, A is the correct answer.

QUESTION 12

Which is the correct "fw monitor" syntax for creating a capture file for loading it into WireShark?

A. fw monitor -e "accept;" >> Output.cap

B. This cannot be accomplished as it is not supported with R80.10

C. fw monitor -e "accept;" -file Output.cap

D. fw monitor -e "accept;" -o Output.cap

Correct Answer: D