Free Questions for 156-585 by vceexamstest

Shared by Patel on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which Threat Prevention Daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?

Options:

A- ctasd

B- in.msd

C- ted

D- scrub

Answer:

C

Question 2

Question Type: MultipleChoice

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 but you can't afford to fill up all the remaining disk space and you only have 10 GB free for saving the debugs. What is the correct syntax for this?

Options:

A- fw ctl kdebug -T -f -m 10 -s 1000000 -o debugfilename

B- fw ctl kdebug -T -f -m 10 -s 1000000 > debugfilename

C- fw ctl kdebug -T -m 10 -s 1000000 -o debugfilename

D- fw ctl debug -T -f -m 10 -s 1000000 -o debugfilename

Answer:

D

Question 3

Question Type: **MultipleChoice**

Which kernel process is used by Content Awareness to collect the data from contexts?

Options:

A- dlpda

B- PDP

C- cpemd

D- CMI

Answer:

D

Question 4

Question Type: MultipleChoice

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?

Options:

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 5

Question Type: MultipleChoice

The Check Point Firewall Kernel is the core component of the Gala operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

Options:

A- fw ctl debug/kdebug

B- fw ctl zdebug

C- fw debug/kdebug

D- fw debug/kdebug ctl

Answer:

B

Question 6

Question Type: MultipleChoice

What is the difference in debugging a S2S or C2S (using Check Point VPN Client) VPN?

Options:

A- there is no difference

B- the C2S VPN uses a different VPN daemon and there a second VPN debug

C- the C2S VPN can not be debugged as it uses different protocols for the key exchange

D- the C2S client uses Browser based SSL vpn and can't be debugged

Answer:

D

Question 7

Question Type: MultipleChoice

What is the best way to resolve an issue caused by a frozen process?

Options:

A- Reboot the machine

B- Restart the process

C- Kill the process

D- Power off the machine

Answer:

B

Question 8

Question Type: MultipleChoice

What is the best way to resolve an issue caused by a frozen process?

Options:

A- Reboot the machine

B- Restart the process

C- Kill the process

D- Power off the machine

Answer:

B

Question 9

Question Type: MultipleChoice

What table does command "fwaccel conns" pull information from?

Options:

A- fwxl_conns

B- SecureXLCon

C- cphwd_db

D- sxl_connections

Answer:

A

Question 10

Question Type: MultipleChoice

The Check Point Firewall Kernel is the core component of the Gala operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

Options:

A- fw ctl debug/kdebug

B- fw ctl zdebug

C- fw debug/kdebug

D- fw debug/kdebug ctl

Answer:

B

Question 11

Question Type: MultipleChoice

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

Options:

A- rad

B- cprad

C- pepd

D- pdpd

Answer:

A

Question 12

Question Type: MultipleChoice

What is the proper command for allowing the system to create core files?

Options:

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