[Jan-2023 Use Real 156-585 Dumps Free Sample Questions and Practice Test Engine [Q60-Q74

[Jan-2023] Use Real 156-585 Dumps Free Sample Questions and Practice Test Engine
Pass CheckPoint 156-585 exam - questions - convert Tets Engine to PDF

QUESTION 60

You have configured IPS Bypass Under Load function with additional kernel parameters ids_tolerance_no_stress=15 and ids_tolerance_stress-15 For configuration you used the *fw ctl set’ command After reboot you noticed that these parameters returned to their default values What do you need to do to make this configuration work immediately and stay permanent?
* Set these parameters again with “fw ctl set” and edit appropriate parameters in $FWDIR/boot/modules/ fwkern.conf
* Use script $FWDIR/bin IpsSetBypass.sh to set these parameters
* Set these parameters again with “fw ctl set” and save configuration with “save config”
* Edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf
Explanation

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

QUESTION 61

When a User Mode process suddenly crashes it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash?

i Program Counter

ii Stack Pointer

ii. Memory management information

iv Other Processor and OS flags / information
* i, ii, lii and iv
* i and n only
* iii and iv only
* D Only iii

QUESTION 62

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?
* using GUIDBEDIT located in same directoryas Smartconsole on the Windows client
* she need to install GUIDBEDIT which can be downloaded from the Usercenter
* she need to run GUIDBEDIT from CLISH which opens a graphical window on the smartcenter
* this cant be done anymore as GUIDBEDIT is not supported in R80 anymore

QUESTION 63

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.
* 5, 6, 7, 1, 3, 2, 4
* 5, 6, 2, 4, 1, 7, 3
* 5, 6, 4, 1, 7, 2, 3
* 5, 6, 3, 1, 2, 4, 7

QUESTION 64

John has renewed his NGTX License but he gets an error (contract for Anti-Bot expired). He wants to check the subscription status on the CU of the gateway, what command can he use for this?
* cpstat antimalware -I subscription _status
* fw monitor license status
* fwm lie print
* show license status

QUESTION 65

What is the proper command for allowing the system to create core files?
* $FWDIR/scripts/core-dump-enable.sh
* # set core-dump enable

save config
* service core-dump start
* >set core-dump enable

>save config

QUESTION 66

What command is usually used for general firewall kernel debugging andwhatis the sizeofthe buffer that isautomaticallyenabled whenusingthe command?
* fw ctl debug, buffer sizeis 1024 KB
* fw ell zdebug. buffer size is 32768 KB
* fw dl zdebug, buffer size is 1 MB
* fw ctl kdeoug. buffer sizeis 32000 KB

QUESTION 67

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

QUESTION 68

Which kernel process is used by Content Awareness to collect the data from contexts?
* dlpda
* PDP
* cpemd
* CMI

QUESTION 69

What are the four ways to insert an FW Monitor into the firewallkernel chain?
* Relative position using location, relativepositionusing alias, absolute position, all positions
* Absolute position using location, absolute position using alias, relative position, all positions

* Absolute position using location, relative position using alias, general position, all positions
* Relative position using geolocation relative position using inertial navigation, absolute position all positions

QUESTION 70

Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?
* $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
* $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
* $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/
* $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

QUESTION 71

You are trying to establish a VPN tunnel between two Security Gateways but fail. What initial steps will you make to troubleshoot the issue
* capture traffic on both tunnel members and collect debug of IKE and VPND daemon
* 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
* collect debug of IKE and VPND daemon and collect kernel debug for fw module with vm, crypt, conn and drop flags
* capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags

QUESTION 72

You need to runa 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?
* fw ctl kdebug -T -f > filename debug
* fw ctl kdebug -T > filename debug
* fw ctl debug -T -f > filename debug
* fw ctl kdebug -T -f -o filename debug

QUESTION 73

Which daemon governs the Mobile Access VPN blade and works with VPND to create Mobile Access VPN connections? It also handles interactions between HTTPS and the Multi-Portal Daemon.
* Connectra VPN Daemon – cvpnd
* Mobile Access Daemon – MAD
* mvpnd
* SSL VPN Daemon – sslvpnd

QUESTION 74

Where will the usermode core files be located?
* /var/log/dump/usermode
* /var/suroot
* SFWDlR/var’log/dump/usermode
* SCPDIR/var/log/dump/usermode

Best Solution to prepare CheckPoint 156-585 Exam:

Even if you have a lot of experience in the security field, you will still need to take the CheckPoint 156-585 exam to become certified. It is vital that you become certified as a CheckPoint 156-585 professional, even if this is your first IT certification because it will ensure that you are well-prepared for any position within the industry. It is also easier to find a job without this certification because there are enough people who have earned their certifications online or from other companies.

You can study from the sources like the Official CheckPoint 156-585 Exam Guide, Online Test Simulator like **CheckPoint 156-585 exam dumps**, Sample Question Papers, video from YouTube, or other free videos, etc. for the preparation for the CheckPoint 156-585 certification exam effectively. It helps you to test your knowledge and ability before you sit for the Checkpoint 156-585 exam. Desired information for the preparation of CheckPoint 156-585 exam is presented by the most experienced and renowned expert and professional team who treat the subject in a perfect and comprehensive way. Guarantee to pass CheckPoint 156-585 exam by the integrated study.

Pass Your 156-585 Exam Easily - Real 156-585 Practice Dump Updated Jan 18, 2023:
https://www.vceprep.com/156-585-latest-vce-prep.html]