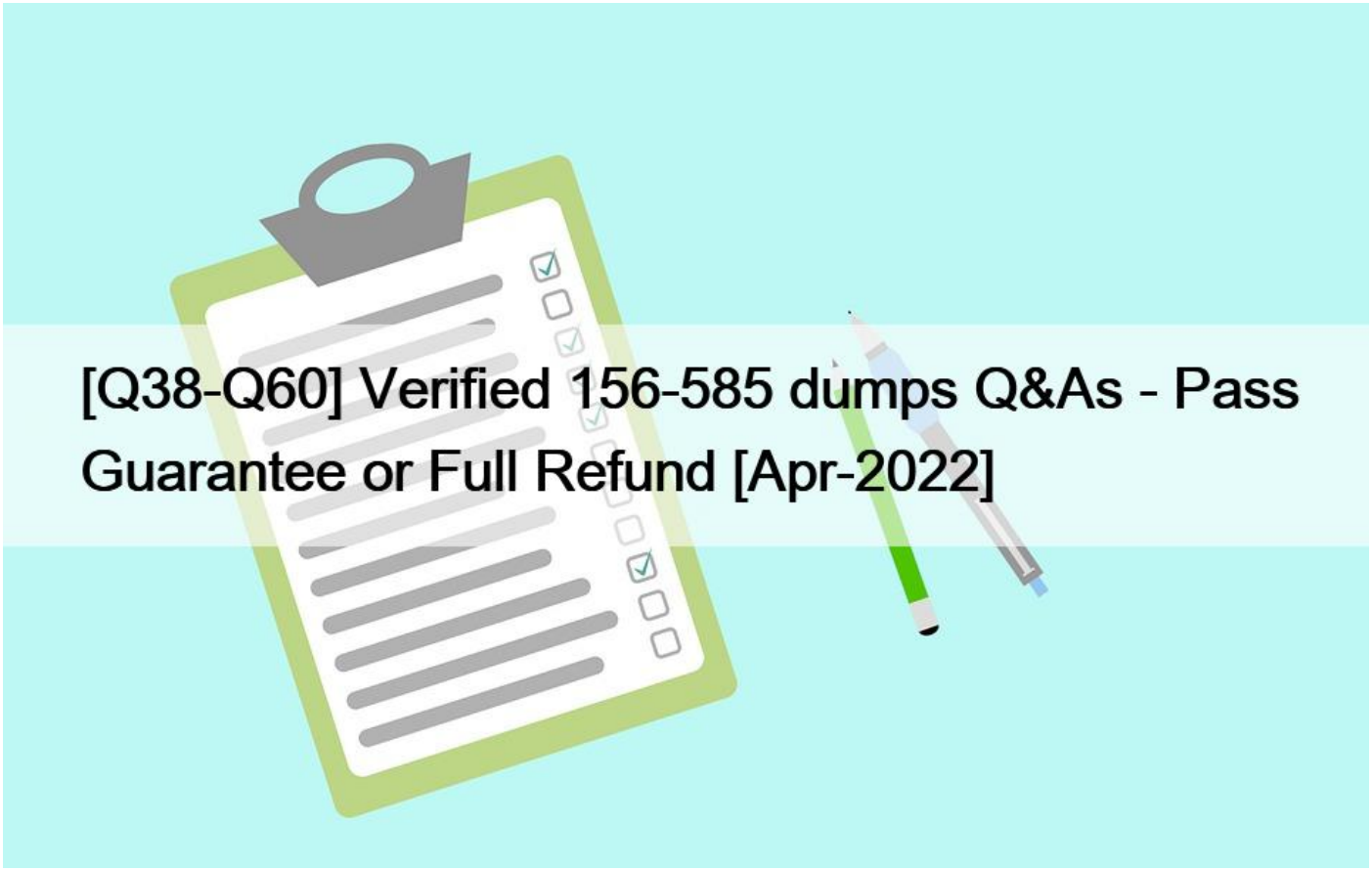
[Q38-Q60 Verified 156-585 dumps Q&As - Pass Guarantee or Full Refund [Apr-2022



Verified 156-585 dumps Q&As - Pass Guarantee or Full Refund [Apr-2022]
156-585 PDF Dumps | Apr 10, 2022 Recently Updated Questions

What is the Exam fee for the CheckPoint 156-585 Exam

The CheckPoint 156-585 exam costs $200, which is the current standard cost for the ISC2 certification exams. The CheckPoint 156-585 Exam will be administered via computer at Pearson Vue testing centers throughout the world. Discount is available for ISC2 members at the time of purchase.

NEW QUESTION 38

Which command can be run in Expert mode lo verify the core dump settings?
* grep cdm /config/db/coredump
* grep cdm /config/db/initial
* grep SFWDlR/config/db/initial
* cat /etc/sysconfig/coredump/cdm conf

NEW QUESTION 39

Which command is most useful for debugging the fwaccel module?
* fw zdebug
* securexl debug
* fwaccel dbg
* fw debug

NEW QUESTION 40

Which Threat Prevention daemon is the core Threat Emulator, engine and responsible for emulation files and communications with Threat Cloud?
* ctasd
* inmsd
* ted
* scrub

Explanation

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

NEW QUESTION 41

Which of the following is NOT a valid “fwaccel” parameter?
* stat
* stats
* templates
* packets

NEW QUESTION 42

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?
* The kernel parameter ids_assume_stress is set to 0
* The kernel parameter ids_assume_stress is set to 1
* The kernel parameter ids_tolerance_no_stress is set to 10
* The kernel parameter ids_tolerance_stress is set to 10

NEW QUESTION 43

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

NEW QUESTION 44

How many captures does the command “fw monitor -p all” take?
* All 15 of the inbound and outbound modules
* All 4 points of the fw VM modules
* 1 from every inbound and outbound module of the chain
* The -p option takes the same number of captures, but gathers all of the data packet

NEW QUESTION 45

For TCP connections, when a packet arrives at the Firewall Kernel out of sequence or fragmented, which layer of IPS corrects this to allow for proper inspection?
* Passive Streaming Library
* Protections
* Protocol Parsers
* Context Management

NEW QUESTION 46

To check the current status of hyper-threading, which command would you execute in expert mode?
* cat /proc/hypert_status
* cat /proc/smt_status
* cat /proc/hypert_stat
* cat /proc/smt_stat

NEW QUESTION 47

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

NEW QUESTION 48

Which command(s) will turn off all vpn debug collection?
* vpn debug off
* vpn debug -a off
* vpn debug off and vpn debug ikeoff
* fw ctl debug 0

NEW QUESTION 49

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

NEW QUESTION 50

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?
* Administrator should manually synchronize the servers using SmartConsole
* The Collision state does not happen in R80.x as the synchronizing automatically on every publish action
* Reset the SIC of the secondary management server
* Run the command ‘fw send synch force’ on the primary server and ‘fw get sync quiet’ on the secondary server

NEW QUESTION 51

Where do Protocol parsers register themselves for IPS?
* Passive Streaming Library
* Other handlers register to Protocol parser
* Protections database
* Context Management Infrastructure

NEW QUESTION 52

What components make up the Context Management Infrastructure?
* CMI Loader and Pattern Matcher
* CPMI and FW Loader
* CPX and FWM
* CPM and SOLR

NEW QUESTION 53

Which of the following is NOT a vpn debug command used for troubleshooting?
* fw ctl debug -m fw + conn drop vm crypt
* vpn debug trunc
* pclient getdata sslvpn
* vpn debug on TDERROR_ALL_ALL=5

NEW QUESTION 54

Which of the following inputs is suitable for debugging HTTPS inspection issues?
* vpn debug cptls on
* fw ctl debug -m fw + conn drop cptls
* fw diag debug tls enable
* fw debug tls on TDERROR_ALL_ALL=5

NEW QUESTION 55

PostgreSQL is a powerful, open source relational database management system Check Point offers a command for viewing the database to interact with Postgres interactive shell Which command do you need to enter the PostgreSQL interactive shell?
* psql_client cpm postgres

* mysql_client cpm postgres
* psql_c!ieni postgres cpm
* mysql -u root

NEW QUESTION 56

What is the simplest and most efficient way to check all dropped packets in real time?
* fw ctl zdebug * drop in expert mode
* Smartlog
* cat /dev/fwTlog in expert mode
* tail -f SFWDIR/log/fw log |grep drop in expert mode

NEW QUESTION 57

James is using the same filter expression in fw monitor for CITRIX very often and instead of typing this all the time he wants to add it as a macro to the fw monitor definition file. What’s the name and location of this file?
* $FWDIR/lib/fwmonltor.def
* $FWDIR/conf/fwmonltor.def
* $FWDIR/lib/tcpip.def
* $FWDIR/lib/fw.monitor

NEW QUESTION 58

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
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk62848&partition=Advanced&product=IPS

NEW QUESTION 59

What is the main SecureXL database for trackingthe acceleration status of traffic?
* cphwd_db
* cphwd_tmp1
* cphwd_dev_conn_table
* cphwd_dev_identity_table

NEW QUESTION 60

Which process is responsible for the generation of certificates?
* cpm
* cpca
* dbsync
* fwm

156-585 Exam Questions – Valid 156-585 Dumps Pdf: https://www.vceprep.com/156-585-latest-vce-prep.html]