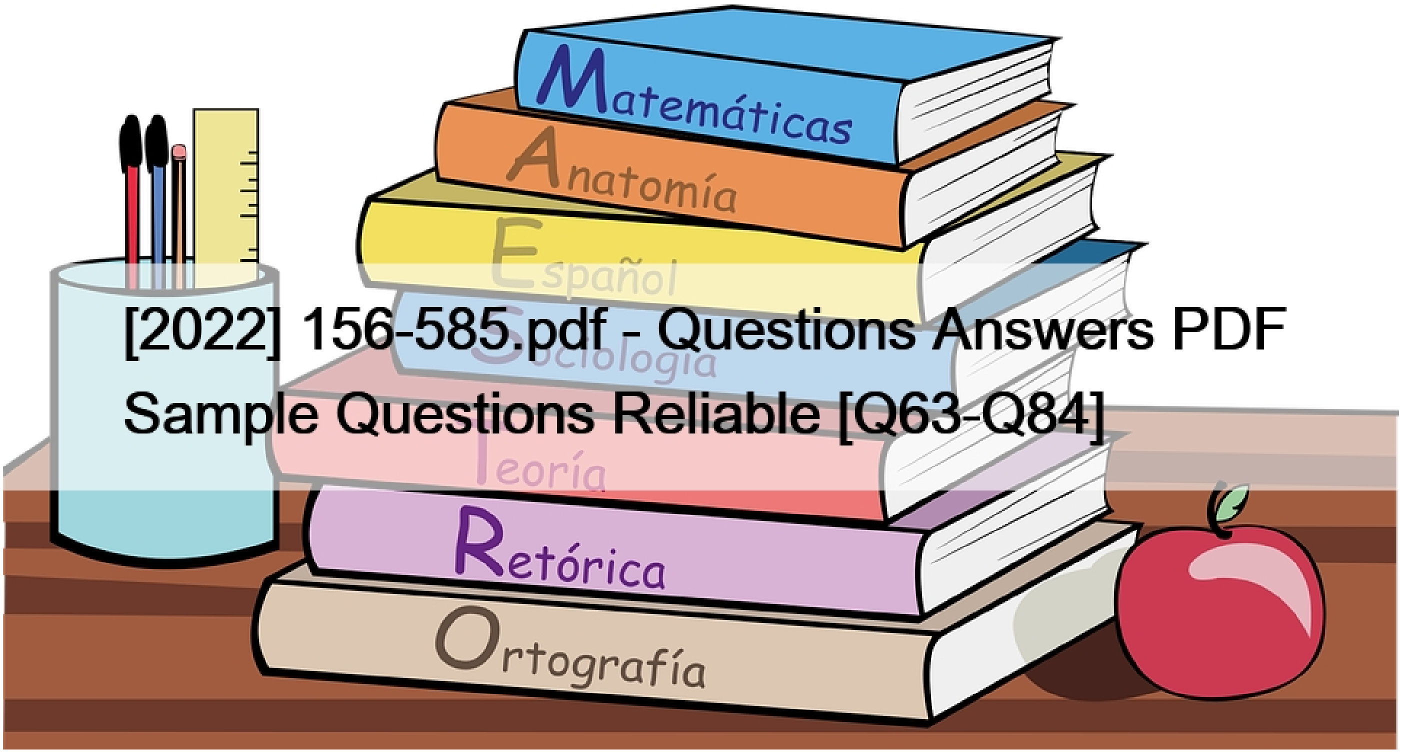
[2022 156-585.pdf - Questions Answers PDF Sample Questions Reliable [Q63-Q84


Matemáticas
Anatomía
Español
Sociología
Teoría
Retórica
Ortografía
[2022] 156-585.pdf - Questions Answers PDF Sample Questions Reliable [Q63-Q84]

[2022] 156-585.pdf - Questions Answers PDF Sample Questions Reliable
CheckPoint 156-585 Dumps PDF Are going to be The Best Score

NEW QUESTION 63

What are the main components of Check Point&#8217;s Security Management architecture?
* Management server management database, log server, automation server
* Management server, Security Gateway. Multi-Domain Server, SmartEvent Server
* Management Server. Log Server. LDAP Server, Web Server
* Management server Log server, Gateway server. Security server

NEW QUESTION 64

What are four main database domains?
* System, User, Global, Log
* System, User, Host, Network
* System, Global, Log, Event
* Local, Global, User, VPN

NEW QUESTION 65

What table does the command &#8220;fwaccel conns&#8221; pull information from?

* fwxl_conns
* SecureXLCon
* cphwd_db
* sxl_connections

NEW QUESTION 66

Which command is used to write a kernel debug to a file?
* fw ctl debug -T -f > debug.txt
* fw ctl kdebug -T -l > debug.txt
* fw ctl debug -S -t > debug.txt
* fw ctl kdebug -T -f > debug.txt

NEW QUESTION 67

What is the buffer size set by the fw ctl zdebug command?
* 1 GB
* 1 MB
* 8GB
* 8MB

NEW QUESTION 68

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?
* Use the IPS exception mechanism
* Disable all such protections
* Disable SecureXL and use CoreXL
* Upgrade the hardware to include more Cores and Memory

NEW QUESTION 69

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 70

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 71

What does SIM handle?
* Accelerating packets
* FW kernel to SXL kernel hand off
* OPSEC connects to SecureXL
* Hardware communication to the accelerator

NEW QUESTION 72

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

NEW QUESTION 73

What is the name of the VPN kernel process?
* VPNK
* VPND
* CVPND
* FWK

NEW QUESTION 74

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

NEW QUESTION 75

During firewall kernel debug with fw ctl zdebug you received less information than expected. You noticed that a lot of messages were lost since the time the debug was started. What should you do to resolve this issue?
* Increase debug buffer; Use fw ctl debug -buf 32768
* Redirect debug output to file; Use fw ctl zdebug -o ./debug.elg
* Increase debug buffer; Use fw ctl zdebug -buf 32768
* Redirect debug output to file; Use fw ctl debug -o ./debug.elg

NEW QUESTION 76

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 77

What is the kernel process for Content Awareness that collects the data from the contexts received from the CMI and decides if the file is matched by a data type?

* dlpda
* dlpu
* cntmgr
* cntawmod

NEW QUESTION 78

What process is responsible for sending and receiving logs in the management server?

* FWD
* CPM
* FWM
* CPD

NEW QUESTION 79

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

* there is no difference
* the C2S VPN uses a different VPN daemon and there a second VPN debug
* the C2S VPN can not be debugged as it uses different protocols for the key exchange
* the C2S client uses Browser based SSL vpn and can&#8217;t be debugged

NEW QUESTION 80

You are upgrading your NOC Firewall (on a Check Point Appliance) from R77 to R80 30 but you did not touch thesecuritypolicy After the upgrade you can&#8217;t connect to the new R80 30 SmartConsole of the upgraded Firewall anymore What is a possible reason for this?

* new new console port is 19009 and a access rule ts missing
* the license became invalig and the firewall does not start anymore
* the upgrade process changed the interfaces and IP adresses and you have to switch cables
* the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall

NEW QUESTION 81

Check Point&#8217;s PostgreSQL is partitioned into several relational database domains. Which domain contains network objects and security policies?

* User Domain
* System Domain
* Global Domain
* Log Domain

NEW QUESTION 82

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

* ctasd

* in.msd
* ted
* scrub

NEW QUESTION 83

How can you start debug of the Unified Policy with all possible flags turned on?
* fw ctl debug -m UP all
* fw ctl debug -m UnifiedPolicy all
* fw ctl debug -m fw + UP
* fw ctl debug -m UP *

NEW QUESTION 84

After kernel debug with &#8220;fw ctl debug&#8221; you received a huge amount of information It was saved in a very large file that is difficult to open and analyze with standard text editors Suggest a solution to solve this issue.
* Use &#8220;fw ctl zdebug&#8217; because of 1024KB buffer size
* Divide debug information into smaller files Use &#8220;fw ctl kdebug -f -o &#8220;filename&#8221; -m 25 &#8211; s &#8220;1024&#8221;
* Reduce debug buffer to 1024KB and run debug for several times
* Use Check Point InfoView utility to analyze debug output

Can I cancel my CheckPoint 156-585 exam or retake it?

No, you cannot cancel your CheckPoint 156-585 exam, but you are allowed to take this exam up to three times per year. Temporarily, you will be unable to take this exam again for three months. The exponent is based on the time between your attempt at this exam. Authenticity is ensured by the ISC2 policy. No, if you fail the CheckPoint 156-585 exam twice in a row, or three times in a row, then you will have to wait three months before being allowed to take this specific exam again. This is for any person who has failed the CheckPoint 156-585 exam in a non-recurring fashion within a total of five years. If you change roles within your company, then you will have to wait three years from the last time you took this test. Reasons for this might include; you changed departments, moved to a new company, or retired.
This certification will be added to all of your background checks in order to verify your credibility in the IT industry. If you fail this exam, then this will become a significant weakness in your resume when applying for higher rank positions within the security space. This is more of a career limiter than it is a job blocker; however, there is no way of knowing what your potential employer will think of you and your ability to do the job. Final decisions rest with the employer. So get in touch with the **CheckPoint 156-585 exam dumps** to get success in this exam.

Use 156-585 Exam Dumps (2022 PDF Dumps) To Have Reliable 156-585 Test Engine:
https://www.examslabs.com/CheckPoint/CCTE/best-156-585-exam-dumps.html]