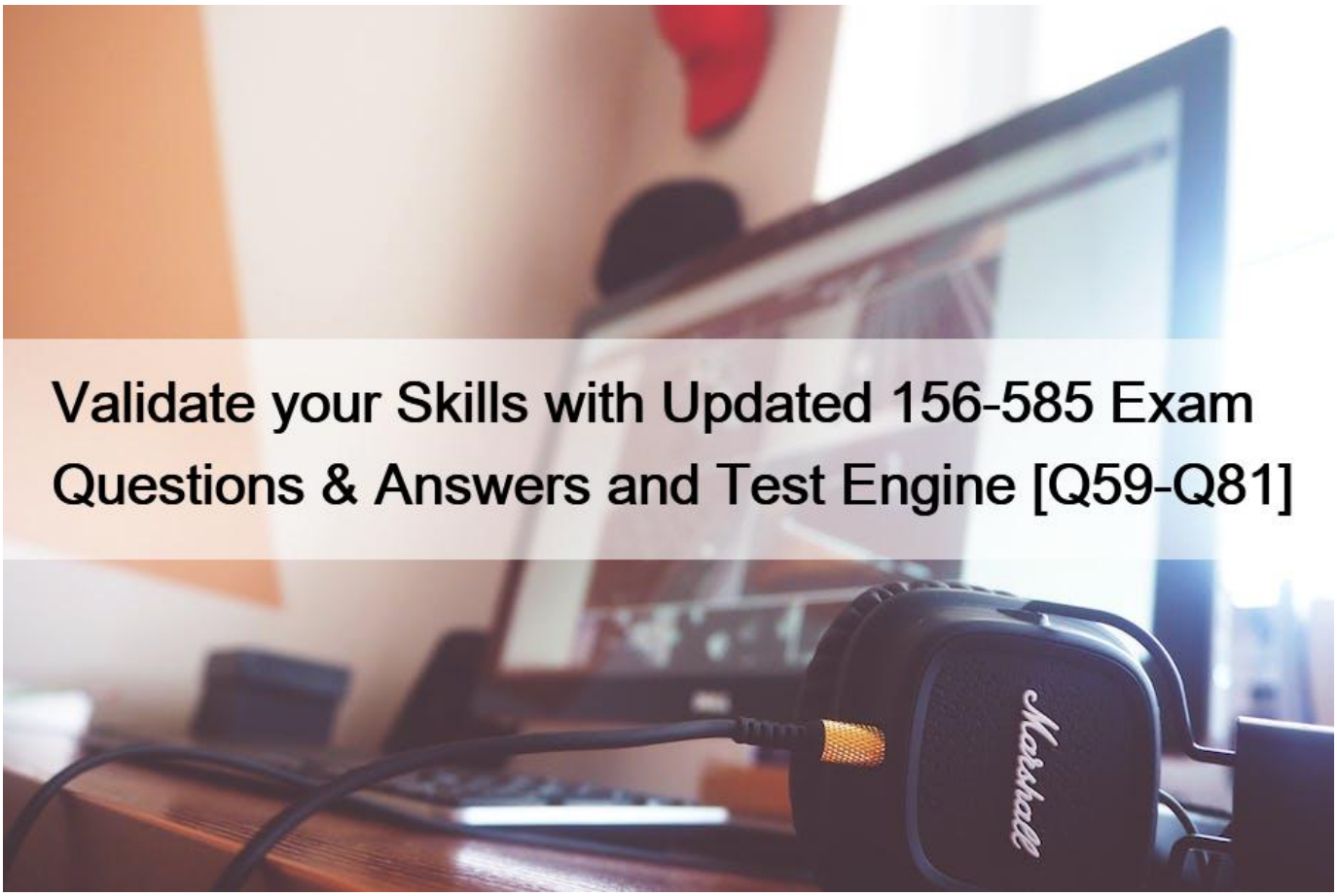
Validate your Skills with Updated 156-585 Exam Questions & Answers and Test Engine [Q59-Q81



Validate your Skills with Updated 156-585 Exam Questions & Answers and Test Engine
Tested & Approved 156-585 Study Materials Download Free Updated 116 Questions

The Check Point Certified Troubleshooting Expert (CCTE) certification is aimed at security professionals who are responsible for troubleshooting complex security issues in large-scale networks. Check Point Certified Troubleshooting Expert certification is designed to validate the skills and expertise of security professionals in areas such as network and VPN troubleshooting, firewall configuration, and advanced threat analysis.

To pass the CheckPoint 156-585 Exam, candidates must have a thorough understanding of Check Point products and technologies, as well as hands-on experience in troubleshooting complex issues. They must also have the ability to analyze and diagnose network problems, configure and manage Check Point products, and deploy security policies effectively. Additionally, candidates must have good communication skills and the ability to work under pressure to solve critical security issues.

NEW QUESTION 59

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 60

What are the maximum kernel debug buffer sizes, depending on the version
* 8MB or 32MB
* 8GB or 64GB
* 4MB or 8MB
* 32MB or 64MB

NEW QUESTION 61

You are running R80.XX on an open server and you see a high CPU utilization on your 12 CPU cores You now want to enable Hyperthreading to get more cores to gain some performance. What is the correct way to achieve this?
* Hyperthreading is not supported on open servers, on on Check Point Appliances
* just turn on HAT in the bios of the server and boot it
* just turn on HAT in the bios of the server and after it has booted enable it in cpconfig
* in dish run set HAT on

NEW QUESTION 62

What table does command “fwaccel conns” pull information from?
* fwxl_conns
* SecureXLCon
* cphwd_db
* sxl_connections

NEW QUESTION 63

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?
* 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
* 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.
* Tunnel fails on Joey’s site, because he misconfigured IP address of VPN peer.
* Tunnel falls on partner site. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

NEW QUESTION 64

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’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 65

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 66

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 67

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 68

What is the benefit of running “vpn debug trunc over “vpn debug on”?
* “vpn debug trunc” purges ike.elg and vpnd elg and creates limestarnp while starting ike debug and vpn debug
* “vpn debug trunc*truncates the capture hence the output contains minimal capture
* “vpn debug trunc* provides verbose capture
* No advantage one over the other

NEW QUESTION 69

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 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

URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required”
* RAD Kernel Space
* URLF Kernel Client
* URLF Online Service
* RAD User Space

NEW QUESTION 72

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

NEW QUESTION 73

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 74

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

* 1 MB
* 8GB
* 8MB

NEW QUESTION 75

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 76

Which Daemon should be debugged for HTTPS Inspection related issues?
* FWD
* HTTPD
* WSTLSO
* VPND

NEW QUESTION 77

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
* (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 (11) 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
* (i) is used to debug the access control policy only, however (n) can be used to debug a unified policy
* (i) is used to debug only issues related to dropping of traffic, however (n) can be used for any firewall issue including NATing, clustering etc.
* (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server

NEW QUESTION 78

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

NEW QUESTION 79

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 80

What is the purpose of the Hardware Diagnostics Tool?
* Verifying that Check Point Appliance hardware is functioning correctly
* Verifying the Security Management Server hardware is functioning correctly
* Verifying that Security Gateway hardware is functioning correctly
* Verifying that Check Point Appliance hardware is actually broken

NEW QUESTION 81

An administrator receives reports about issues with log indexing and text searching regarding an existing Management Server. In trying to find a solution she wants to check if the process responsible for this feature is running correctly. What is true about the related process?
* fwm manages this database after initialization of the ICA
* cpd needs to be restarted manual to show in the list
* fwssd crashes can affect therefore not show in the list
* solr is a child process of cpm

Who cannot take the CheckPoint 156-585 Certification Exam?

You cannot take this certification exam if you have a Record of Arrest or Conviction for a Felony, or if you have been terminated from any certified position within your organization within the last three years. Also, you may not have passed the CheckPoint 156-585 exam within the past two years. Request to take the exam again after you have had time to brush up on your skills.

Regular Free Updates 156-585 Dumps Real Exam Questions Test Engine: https://www.dumpleader.com/156-585_exam.html]