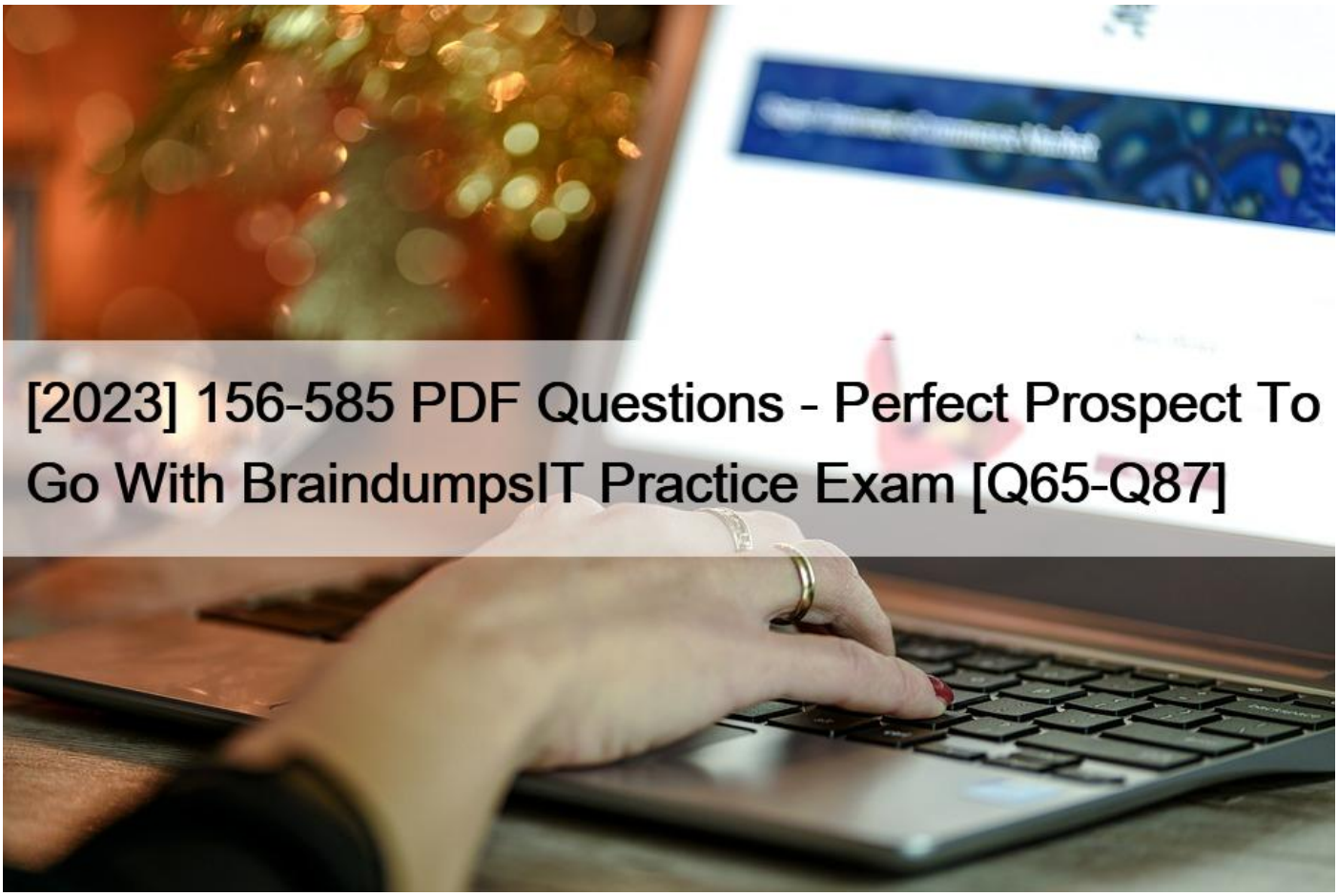
[2023 156-585 PDF Questions - Perfect Prospect To Go With BraindumpsIT Practice Exam [Q65-Q87



[2023] 156-585 PDF Questions - Perfect Prospect To Go With BraindumpsIT Practice Exam
CheckPoint 156-585 Pdf Questions - Outstanding Practice To your Exam

NEW QUESTION 65

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 66

When running a debug with fw monitor, which parameter will create a more verbose output?
* -i
* -i
* -0

* -d

NEW QUESTION 67

Which one of the following is NOT considered a Solr core partition:
* CPM_0_Revisions
* CPM_Global_A
* CPM_Gtobal_R
* CPM_0_Disabled

NEW QUESTION 68

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 69

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

NEW QUESTION 70

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 71

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 72

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 73

Vanessa is reviewing ike.elg file to troubleshoot failed site-to-site VPN connection After sending Mam Mode Packet 5 the response from the peer is PAYLOAD-MALFORMED” What is the reason for failed VPN connection?
* The authentication on Phase 1 is causing the problem.

Pre-shared key on local gateway encrypted by the hash algorithm created in Packet 3 and Packet 4 doesn’t match with the hash on the peer gateway generated by encrypting its pre-shared key
* The authentication on Phase 2 is causing the problem

Pre-shared key on local gateway encrypted by the hash algorithm created in Packets 1 and 2 doesn’t match with the hash on the peer gateway generated by encrypting its pre-shared key
* The authentication on Quick Mode is causing the problem

Pre-shared key on local gateway encrypted by the hash algorithm created in Packets 3 and 4 doesn’t match with the hash on the peer gateway generated by encrypting its pre-shared key
* The authentication on Phase 1 is causing the problem

Pre-shared key on local gateway encrypted by the hash algorithm doesn’t match with the hash on the peer gateway generated by encrypting its pre-shared key created in Packet 1 and Packet 2

NEW QUESTION 74

Which of the following is contained in the System Domain of the Postgres database?

* Saved queries for applications
* Configuration data of log servers
* Trusted GUI clients
* User modified configurations such as network objects

NEW QUESTION 75

When debugging is enabled on firewall kernel module using the ‘fw ctl debug’ command with required options, many debug messages are provided by the kernel that help the administrator to identify issues. Which of the following is true about these debug messages generated by the kernel module?
* Messages are written to a buffer and collected using ‘fw ctl kdebug’
* Messages are written to console and also /var/log/messages file
* Messages are written to /etc/dmesg file
* Messages are written to $FWDIR/log/fw.elg

NEW QUESTION 76

When a User process or program suddenly crashes, a core dump is often used to examine the problem. Which command is used to enable the core-dumping via GAIA dish?
* set core-dump enable
* set core-dump per_process
* set user-dump enable
* set core-dump total

NEW QUESTION 77

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 78

What acceleration mode utilizes multi-core processing to assist with traffic processing?
* CoreXL
* SecureXL
* HyperThreading
* Traffic Warping

NEW QUESTION 79

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 80

John works for ABC Corporation.They have enabled CoreXL on their firewall John would like to identify the cores on which the SND runs and the cores on which the firewall instance is running. Which command should John run to view the CPU role allocation?
* fw ctl affinity -v
* fwaccel stat -I
* fw ctl affinity -I
* fw ctl cores

NEW QUESTION 81

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 82

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?

NEW QUESTION 83

The management configuration stored in the Postgres database is partitioned into several relational database Domains, like – System, User, Global and Log Domains. The User Domain stores the network objects and security policies. Which of the following is stored in the Log Domain?
* Configuration data of Log Servers and saved queries for applications
* Active Logs received from Security Gateways and Management Servers
* Active and past logs received from Gateways and Servers
* Log Domain is not stored in Postgres database, it is part of Solr indexer only

NEW QUESTION 84

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

NEW QUESTION 85

Troubleshooting issues with Mobile Access requires the following:
* Standard VPN debugs, packet captures, and debugs of cvpnd’ process on Security Gateway
* Standard VPN debugs and packet captures on Security Gateway, debugs of “cvpnd’ process on Security Management

* ‘ma_vpnd’ process on Secunty Gateway
* Debug logs of FWD captured with the command – ‘fw debug fwd on TDERROR_MOBILE_ACCESS=5’

NEW QUESTION 86

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

NEW QUESTION 87

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

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.

Online Questions - Outstanding Practice To your 156-585 Exam: https://www.braindumpsit.com/156-585_real-exam.html]