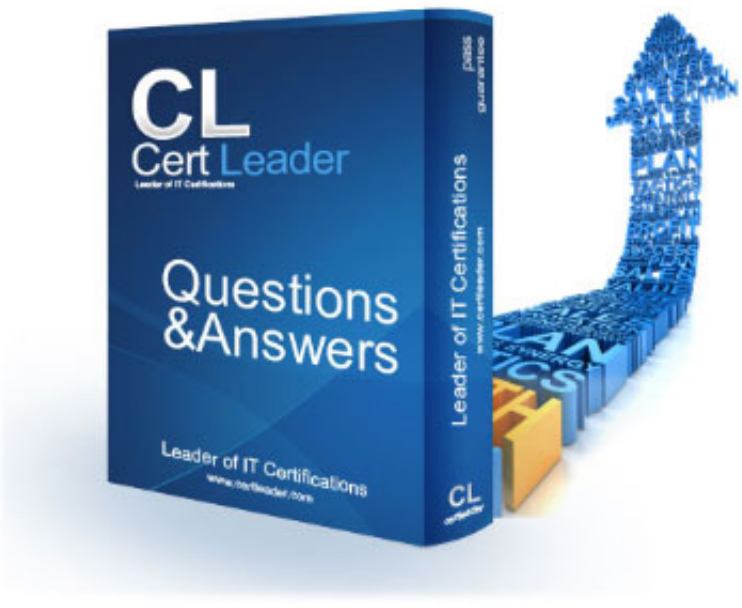
156-585 Dumps

Check Point Certified Troubleshooting Expert

https://www.certleader.com/156-585-dumps.html



NEW QUESTION 1
Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

A. cpstat
B. CPstat
C. CPview
D. fwstat

Answer: A

NEW QUESTION 2
How can you start debug of the Unified Policy with all possible flags turned on?

A. fw ctl debug -m UP all
B. fw ctl debug -m UnifiedPolicy all
C. fw ctl debug -m fw + UP
D. fw ctl debug -m UP *

Answer: D

NEW QUESTION 3
Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
C. $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/
D. $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

Answer: A

NEW QUESTION 4
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?

A. $FWDIR/lib/fwmonltor.def
B. $FWDIR/conf/fwmonltor.def
C. $FWDIR/lib/tcpip.def
D. $FWDIR/lib/fw.monitor

Answer: A

NEW QUESTION 5
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

A. i, ii, lii and iv
B. i and n only
C. iii and iv only
D. D Only iii

Answer: C

NEW QUESTION 6
How many tiers of pattern matching can a packet pass through during IPS inspection?

A. 2
B. 1
C. 5
D. 9

Answer: A

NEW QUESTION 7
What does SIM handle?

A. Accelerating packets
B. FW kernel to SXL kernel hand off
C. OPSEC connects to SecureXL
D. Hardware communication to the accelerator

Answer:

D

NEW QUESTION 8
What is the main SecureXL database for tracking the acceleration status of traffic?

A. cphwd_db
B. cphwd_tmp1
C. cphwd_dev_conn_table
D. cphwd_dev_identity_table

Answer: D

NEW QUESTION 9
What components make up the Context Management Infrastructure?

A. CMI Loader and Pattern Matcher
B. CPMI and FW Loader
C. CPX and FWM
D. CPM and SOLR

Answer: A

NEW QUESTION 10
Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS. and compiles them together into unified Pattern Matchers?

A. CMI Loader
B. cpas
C. PSL - Passive Signature Loader
D. Context Loader

Answer: A

NEW QUESTION 10
Select the technology that does the following actions
- provides reassembly via streaming for TCP
- handles packet reordering and congestion
- handles payload overlap
- provides consistent stream of data to protocol parsers

A. Passive Streaming Library
B. Context Management
C. Pre-Protocol Parser
D. fwtcpstream

Answer: A

NEW QUESTION 13
What is the buffer size set by the fw ctl zdebug command?

A. 1 MB
B. 1 GB
C. 8MB
D. 8GB

Answer: A

NEW QUESTION 16
Which command is used to write a kernel debug to a file?

A. fw ctl debug -T -f > debug.txt
B. fw ctl kdebug -T -l > debug.txt
C. fw ctl debug -S -t > debug.txt
D. fw ctl kdebug -T -f > debug.txt

Answer: D

NEW QUESTION 18
Which of the following is NOT a vpn debug command used for troubleshooting?

A. fw ctl debug -m fw + conn drop vm crypt
B. vpn debug trunc
C. pclient getdata sslvpn
D. vpn debug on TDERROR_ALL_ALL=5

Answer:

C

NEW QUESTION 19
You are trying to establish a VPN tunnel between two Security Gateways but fail. What initial steps will you make to troubleshoot the issue

A. capture traffic on both tunnel members and collect debug of IKE and VPND daemon
B. 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
C. collect debug of IKE and VPND daemon and collect kernel debug for fw module with vm, crypt, conn and drop flags
D. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags

Answer: A

NEW QUESTION 24
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?

A. Use the IPS exception mechanism
B. Disable all such protections
C. Disable SecureXL and use CoreXL
D. Upgrade the hardware to include more Cores and Memory

Answer: C

NEW QUESTION 25
What is NOT a benefit of the fw ctl zdebug command?

A. Cannot be used to debug additional modules
B. Collect debug messages from the kernel
C. Clean the buffer
D. Automatically allocate a 1MB buffer

Answer: A

NEW QUESTION 30
Troubleshooting issues with Mobile Access requires the following:

A. Standard VPN debugs, packet captures, and debugs of cvpnd' process on Security Gateway
B. Standard VPN debugs and packet captures on Security Gateway, debugs of "cvpnd' process on Security Management
C. 'ma_vpnd' process on Secunty Gateway
D. Debug logs of FWD captured with the command - 'fw debug fwd on TDERROR_MOBILE_ACCESS=5'

Answer: A

NEW QUESTION 33
What is the correct syntax to set all debug flags for Unified Policy related issues?

A. fw ctl debug -m UP all
B. fw ctl debug -m up all
C. fw ctl kdebug -m UP all
D. fw ctl debug -m fw all

Answer: A

NEW QUESTION 37
What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .cap
B. .exe
C. .tgz
D. .pcap

Answer: A

NEW QUESTION 39
The Check Point Firewall Kernel is the core component of the Gala operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

A. fw ctl debug/kdebug
B. fw ctl zdebug
C. fw debug/kdebug
D. fw debug/kdebug ctl

Answer: B

NEW QUESTION 42
What are the main components of Check Point's Security Management architecture?

A. Management server, management database, log server, automation server
B. Management server, Security Gatewa
C. Multi-Domain Server, SmartEvent Server
D. Management Serve
E. Log Serve
F. LDAP Server, Web Server
G. Management server Log server, Gateway serve
H. Security server

Answer: A

NEW QUESTION 44
How many captures does the command "fw monitor -p all" take?

A. All 15 of the inbound and outbound modules
B. All 4 points of the fw VM modules
C. 1 from every inbound and outbound module of the chain
D. The -p option takes the same number of captures, but gathers all of the data packet

Answer: C

NEW QUESTION 49
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?

A. Increase debug buffer; Use fw ctl debug –buf 32768
B. Redirect debug output to file; Use fw ctl zdebug –o ./debug.elg
C. Increase debug buffer; Use fw ctl zdebug –buf 32768
D. Redirect debug output to file; Use fw ctl debug –o ./debug.elg

Answer: A

NEW QUESTION 51
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?

A. cpstat antimalware -f subscription_status
B. fw monitor license status
C. fwm lie print
D. show license status

Answer: A

NEW QUESTION 55
Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. core dump
B. CPMIL dump
C. fw monitor
D. tcpdump

Answer: A

NEW QUESTION 58
Your users have some issues connecting Mobile Access VPN to the gateway. How can you debug the tunnel establishment?

A. in the file $CVPNDIR/conf/httpd.conf change the line loglevel .. To LogLevel debug and run cvpnrestart
B. run vpn debug truncon
C. run fw ctl zdebug -m sslvpn all
D. in the file $VPNDIR/conf/httpd.conf the line Loglevel .. To LogLevel debug and run vpn restart

Answer: A

NEW QUESTION 59
Where will the usermode core files be located?

A. /var/log/dump/usermode
B. /var/suroot
C. SFWDIR/var'log/dump/usermode
D. SCPDIR/var/log/dump/usermode

Answer: A

NEW QUESTION 62
Which is the correct “fw monitor” syntax for creating a capture file for loading it into WireShark?

A. fw monitor -e “accept<FILTER EXPRESSION>;” >> Output.cap
B. This cannot be accomplished as it is not supported with R80.10
C. fw monitor -e “accept<FILTER EXPRESSION>;” -file Output.cap
D. fw monitor -e “accept<FILTER EXPRESSION>;” -o Output.cap

Answer: D

NEW QUESTION 67
What is the function of the Core Dump Manager utility?

A. To generate a new core dump for analysis
B. To limit the number of core dump files per process as well as the total amount of disk space used by core files
C. To determine which process is slowing down the system
D. To send crash information to an external analyzer

Answer: B

NEW QUESTION 69
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?

A. Tunnel falls on partner sit
B. 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
C. Tunnel fails on partner sit
D. 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.
E. Tunnel fails on Joey’s site, because he misconfigured IP address of VPN peer.
F. Tunnel falls on partner sit
G. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

Answer: B

NEW QUESTION 71
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?

A. 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
B. The authentication on Phase 2 is causing the problemPre-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
C. The authentication on Quick Mode is causing the problemPre-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
D. The authentication on Phase 1 is causing the problemPre-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

Answer: B

NEW QUESTION 76
Which command(s) will turn off all vpn debug collection?

A. vpn debug off
B. vpn debug -a off
C. vpn debug off and vpn debug ikeoff
D. fw ctl debug 0

Answer: C

NEW QUESTION 79
Which command can be run in Expert mode to verify the core dump settings?

A. grep cdm /config/db/coredump
B. grep cdm /config/db/initial
C. grep $FWDIR/config/db/initial
D. cat /etc/sysconfig/coredump/cdm.conf

Answer: C

NEW QUESTION 82
Where do Protocol parsers register themselves for IPS?

A. Passive Streaming Library
B. Other handlers register to Protocol parser
C. Protections database
D. Context Management Infrastructure

Answer: A

NEW QUESTION 84
After kernel debug with "fw ctl debug" 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.

A. Use "fw ctl zdebug' because of 1024KB buffer size
B. Divide debug information into smaller files Use "fw ctl kdebug -f -o "filename" -m 25 - s "1024"
C. Reduce debug buffer to 1024KB and run debug for several times
D. Use Check Point InfoView utility to analyze debug output

Answer: C

NEW QUESTION 89
What is the purpose of the Hardware Diagnostics Tool?

A. Verifying that Check Point Appliance hardware is functioning correctly
B. Verifying the Security Management Server hardware is functioning correctly
C. Verifying that Security Gateway hardware is functioning correctly
D. Verifying that Check Point Appliance hardware is actually broken

Answer: B

NEW QUESTION 92
How can you increase the ring buffer size to 1024 descriptors?

A. set interface eth0 rx-ringsize 1024
B. fw ctl int rx_ringsize 1024
C. echo rx_ringsize=1024>>/etc/sysconfig/sysctl.conf
D. dbedit>modify properties firewall_properties rx_ringsize 1024

Answer: A

NEW QUESTION 93
Which situation triggers an IPS bypass under load on a 24-core Check Point appliance?

A. any of the CPU cores is above the threshold for more than 10 seconds
B. all CPU core most be above the threshold for more than 10 seconds
C. a single CPU core must be above the threshold for more than 10 seconds, but is must be the same core during this time
D. the average cpu utilization over all cores must be above the threshold for 1 second

Answer: A

NEW QUESTION 94
What is the name of the VPN kernel process?

A. VPNK
B. VPND
C. CVPND
D. FWK

Answer: A

NEW QUESTION 96
When running a debug with fw monitor, which parameter will create a more verbose output?

A. -i
B. -i
C. -0
D. -d

Answer: D

NEW QUESTION 101
What is the correct syntax to turn a VPN debug on and create new empty debug files?

A. vpn debug truncon
B. vpndebug trunc on
C. vpn kdebug on
D. vpn debug trunkon

Answer: D

NEW QUESTION 102
What is the benefit of running "vpn debug trunc over "vpn debug on"?

A. "vpn debug trunc" purges ike.elg and vpnd elg and creates limestarnp while starting ike debug and vpn debug
B. "vpn debug trunc* truncates the capture hence the output contains minimal capture
C. "vpn debug trunc* provides verbose capture
D. No advantage one over the other

Answer: A

NEW QUESTION 105
What are the four ways to insert an FW Monitor into the firewall kernel chain?

A. Relative position using location, relative position using alias, absolute position, all positions
B. Absolute position using location, absolute position using alias, relative position, all positions
C. Absolute position using location, relative position using alias, general position, all positions
D. Relative position using geolocation, relative position using inertial navigation, absolute position, all positions

Answer: D

NEW QUESTION 106
the difference in debugging a S2S or C2S (using Check Point VPN Client) VPN?

A. there is no difference
B. the C2S VPN uses a different VPN deamon and there a second VPN debug
C. the C2S VPN can not be debugged as it uses different protocols for the key exchange
D. the C2S client uses Browser based SSL vpn and cant be debugged

Answer: D

NEW QUESTION 107
What file contains the RAD proxy settings?

A. rad_settings.C
B. rad_services.C
C. rad_scheme.C
D. rad_control.C

Answer: A

NEW QUESTION 108
Which of the following daemons is used for Threat Extraction?

A. scrubd
B. extractd
C. tex
D. tedex

Answer: A

NEW QUESTION 112
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?

A. fwm manages this database after initialization of the ICA
B. cpd needs to be restarted manual to show in the list
C. fwssd crashes can affect therefore not show in the list
D. solr is a child process of cpm

Answer: D

NEW QUESTION 116
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?

A. fw ctl affinity -v
B. fwaccel stat -l
C. fw ctl affinity -l

D. fw ctl cores

Answer: C

NEW QUESTION 118

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 156-585 Exam with Our Prep Materials Via below:

https://www.certleader.com/156-585-dumps.html