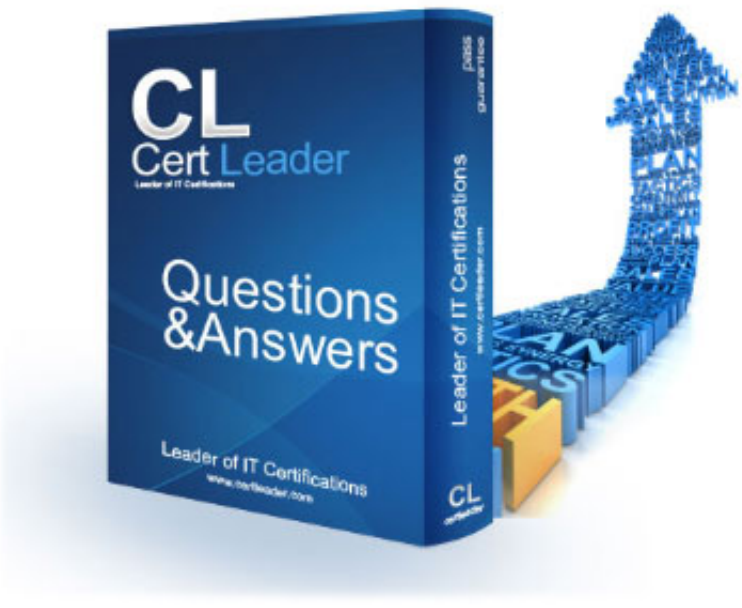
156-585 Dumps

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 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 3
What is 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 daemon 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 can't be debugged

Answer: D

NEW QUESTION 4
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 5
RAD is initiated when Application Control and URL Filtering blades are active on the Security Gateway What is the purpose of the following RAD configuration file SFWDIR/conf/rad_settings.C?

A. This file contains the location information tor Application Control and/or URL Filtering entitlements
B. This file contains the information on how the Security Gateway reaches the Security Managers RAD service for Application Control and URL Filtering
C. This file contains RAD proxy settings
D. This file contains all the host name settings for the online application detection engine

Answer: B

NEW QUESTION 6
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 7
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore you need to add a timestamp to the kernel debug and write the output to a file What is the correct syntax for this?

A. fw ctl kdebug -T -f > filename.debug
B. fw ctl kdebug -T > filename.debug
C. fw ctl debug -T -f > filename.debug
D. fw ctl kdebug -T -f -o filename.debug

Answer: C

NEW QUESTION 8
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 9
Which process is responsible for the generation of certificates?

A. cpm
B. cpca
C. dbsync
D. fwm

Answer: B

NEW QUESTION 10
If you run the command "fw monitor -e accept src=10.1.1.201 or src=172.21.101.10 or src=192.0.2.10;" from the cli sh What will be captured?

A. Packets from 10 1 1 201 going to 192.0 2.10
B. Packets destined to 172 21 101 10 from 10.1.1.101
C. Only packet going to 192.0.2.10
D. fw monitor only works in expert mode so no packets will be captured

Answer: C

NEW QUESTION 10
Some users from your organization have been reporting some connection problems with CIFS since this morning You suspect an IPS issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS chain module (position 4 in the chain) to check If the packets pass the IPS. What command do you need to run?

A. fw monitor -ml -pi 5 -e <filterexperession>
B. fw monitor -pi 5 -e <filterexptession>
C. tcpdump -eni any <filterexpression>
D. fw monitor -pi asm <filtefexpfession>

Answer: C

NEW QUESTION 11
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 16
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 18
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 20
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 21
Which Threat Prevention daemon is the core Threat Emulator, engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd
B. inmsd
C. ted
D. scrub

Answer: C

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

NEW QUESTION 26
Check Point Threat Prevention policies can contain multiple policy layers and each layer consists of its own Rule Base Which Threat Prevention daemon is used for Anti-virus?

A. in.emaild.mta
B. in.msd
C. ctasd
D. in emaild

Answer: D

NEW QUESTION 28
Check Point's PostgreSQL is partitioned into several relational database domains. Which domain contains network objects and security policies?

A. User Domain
B. System Domain
C. Global Domain
D. Log Domain

Answer: C

NEW QUESTION 31
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 36
Which kernel process is used by Content Awareness to collect the data from contexts?

A. dlpda
B. PDP
C. cpemd
D. CMI

Answer: D

NEW QUESTION 41
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 42
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 43
What is the simplest and most efficient way to check all dropped packets in real time?

A. fw ctl zdebug * drop in expert mode
B. Smartlog
C. cat /dev/fwTlog in expert mode
D. tail -f SFWDIR/log/fw log |grep drop in expert mode

Answer: D

NEW QUESTION 46
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"

A. RAD Kernel Space
B. URLF Kernel Client
C. URLF Online Service
D. RAD User Space

Answer: B

NEW QUESTION 47
What is the best way to resolve an issue caused by a frozen process?

A. Reboot the machine
B. Restart the process
C. Kill the process
D. Power off the machine

Answer: B

NEW QUESTION 51
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?

A. Passive Streaming Library
B. Protections
C. Protocol Parsers
D. Context Management

Answer: A

NEW QUESTION 54
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 57
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?

A. Messages are written to a buffer and collected using 'fw ctl kdebug'
B. Messages are written to console and also /var/log/messages file
C. Messages are written to /etc/dmesg file

D. Messages are written to $FWDIR/log/fw.elg

Answer: B

NEW QUESTION 60
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

A. (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 linewhereas (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
B. (i) is used to debug the access control policy only, however (n) can be used to debug a unified policy
C. (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.
D. (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server

Answer: C

NEW QUESTION 61
What table does command “fwaccel conns” pull information from?

A. fwxl_conns
B. SecureXLCon
C. cphwd_db
D. sxl_connections

Answer: A

NEW QUESTION 66
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 71
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 75
Which of the following inputs is suitable for debugging HTTPS inspection issues?

A. vpn debug cptls on
B. fw ctl debug –m fw + conn drop cptls
C. fw diag debug tls enable
D. fw debug tls on TDERROR_ALL_ALL=5

Answer: B

NEW QUESTION 78
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 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?

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

C. fw ctl affinity -l
D. fw ctl cores

Answer: C

NEW QUESTION 85
.....

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