156-585 Q&As

Check Point Certified Troubleshooting Expert

Pass CheckPoint 156-585 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/156-585.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

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

Correct Answer: A

QUESTION 2

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

Correct Answer: A

QUESTION 3

Some users from your organization have been reported 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 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 -pl 5 -e

B. fw monitor -pi 5 -e

C. tcpdump -eni any

D. fw monitor -pl asm

Correct Answer: A

QUESTION 4

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

Correct Answer: D

QUESTION 5

PostgreSQL is a powerful, open source relational database management system Check Point offers a command for viewing the database to interact with Postgres interactive shell Which command do you need to enter the PostgreSQL interactive shell?

A. psql_client cpm postgres

B. mysql_client cpm postgres

C. psql_c!ieni postgres cpm

D. mysql -u root

Correct Answer: A

QUESTION 6

Which process is responsible for the generation of certificates?

A. cpm

B. cpca

C. dbsync D. fwm

Correct Answer: B

QUESTION 7

What acceleration mode utilizes multi-core processing to assist with traffic processing?

A. CoreXL

B. SecureXL

C. HyperThreading

D. Traffic Warping

Correct Answer: C

QUESTION 8

In Security Management High Availability, if the primary and secondary managements, running the same version of R80.x, are in a state of `Collision\\', how can this be resolved?

A. Administrator should manually synchronize the servers using SmartConsole

B. The Collision state does not happen in R80.x as the synchronizing automatically on every publish action

C. Reset the SIC of the secondary management server

D. Run the command `fw send synch force\\' on the primary server and `fw get sync quiet\\' on the secondary server

Correct Answer: A

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

Correct Answer: A

QUESTION 10

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

Correct Answer: C

QUESTION 11

What is the most efficient way to view large fw monitor captures and run filters on the file?

A. wireshark

B. CLISH

C. CLI

D. snoop

Correct Answer: A

QUESTION 12

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

Correct Answer: A

fw ctl zdebug is only for drops and fw ctl debug/kdebug are more detailed and flexible

QUESTION 13

VPN\\'s allow traffic to pass through the Internet securely by encrypting the traffic as it enters the VPN tunnel and then decrypting the exists. Which process is responsible for Mobile VPN connections?

A. cvpnd

B. vpnd

C. vpnk

D. fwk

Correct Answer: C

QUESTION 14

VPN issues may result from misconfiguration, communication failure, or incompatible default configurations between peers Which basic command syntax needs to be used for troubleshooting Site-to-Site VPN Issues?

A. vpn debug truncon

B. fw debug truncon

C. cp debug truncon

D. vpn truncon debug

Correct Answer: A

QUESTION 15

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

Correct Answer: C