

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

<https://www.2passeasy.com/dumps/156-585/>



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 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 4

Which daemon governs the Mobile Access VPN blade and works with VPND to create Mobile Access VPN connections? It also handles interactions between HTTPS and the Multi-Portal Daemon.

- A. Connectra VPN Daemon - cvpnd
- B. Mobile Access Daemon - MAD
- C. mvpnd
- D. SSL VPN Daemon - sslvpnd

Answer: A

NEW QUESTION 5

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 6

Jenna has to create a VPN tunnel to a CISCO ASA but has to set special property to renegotiate the Phase 2 tunnel after 10 MB of transferee1 data. This can not be configured in the smartconsole, so how can she modify this property?

- A. using GUIDBEDIT located in same directory as Smartconsole on the Windows client
- B. she need to install GUIDBEDIT which can be downloaded from the Usercenter
- C. she need to run GUIDBEDIT from CLISH which opens a graphical window on the smartcenter
- D. this cant be done anymore as GUIDBEDIT is not supported in R80 anymore

Answer: C

NEW QUESTION 7

Your fwm constantly crashes and is restarted by the watchdog. You can't find any coredumps related to this process, so you need to check If coredumps are enabled at all How can you achieve that?

- A. in dish run show core-dump status
- B. in expert mode run show core-dump status
- C. in dish run set core-dump status
- D. in dish run show coredumb status

Answer: D

NEW QUESTION 8

Which process is responsible for the generation of certificates?

- A. cpm
- B. cpcap
- C. dbsync
- D. fwm

Answer: B

NEW QUESTION 9

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

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

Answer: A

NEW QUESTION 10

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?

- A. The kernel parameter ids_assume_stress is set to 0
- B. The kernel parameter ids_assume_stress is set to 1
- C. The kernel parameter ids_tolerance_no_stress is set to 10
- D. The kernel parameter ids_tolerance_stress is set to 10

Answer: D

NEW QUESTION 12

The Check Point Firewall Kernel is the core component of the Gaia 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 15

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 19

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 SFWDIR/config/db/initial
- D. cat /etc/sysconfig/coredump/cdm conf

Answer: C

NEW QUESTION 24

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

Answer: A

NEW QUESTION 25

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?

- A. set core-dump enable
- B. set core-dump per_process
- C. set user-dump enable
- D. set core-dump total

Answer: A

NEW QUESTION 30

You are upgrading your NOC Firewall (on a Check Point Appliance) from R77 to R80 30 but you did not touch the security policy 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?

- A. new console port is 19009 and a access rule ts missing
- B. the license became invalig and the firewall does not start anymore
- C. the upgrade process changed the interfaces and IP addresses and you have to switch cables
- D. the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall

Answer: D

NEW QUESTION 33

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 38

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 43

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 46

Which Threat Prevention Daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?

- A. ctasd
- B. in.msds
- C. ted
- D. scrub

Answer: C

NEW QUESTION 47

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 must 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 50

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 54

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 56

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

Answer: A

NEW QUESTION 60

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

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

Answer: B

NEW QUESTION 65

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-585 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-585 Product From:

<https://www.2passeasy.com/dumps/156-585/>

Money Back Guarantee

156-585 Practice Exam Features:

- * 156-585 Questions and Answers Updated Frequently
- * 156-585 Practice Questions Verified by Expert Senior Certified Staff
- * 156-585 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-585 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year