



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



156-585 Dumps
156-585 Braindumps
156-585 Real Questions
156-585 Practice Test
156-585 Actual Questions



killexams.com

CheckPoint

156-585

CheckPoint Certified Troubleshooting Expert

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/156-585>



Question: 108

Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0, choose the correct answer.

- A. fw monitor Cpo -0x1ffffe0
- B. fw monitor Cp0 0x1ffffe0
- C. fw monitor Cpo 1ffffe0
- D. fw monitor Cp0 Cox1ffffe0

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/Content/Topics-PTG/CLI/fw-monitor.htm

Question: 109

What are the four ways to insert an FW Monitor into the firewallkernel chain?

- A. Relative position using location, relativepositionusing 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

Question: 110

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

Question: 111

What are some measures you can take to prevent IPS false positives?

- A. Exclude problematic services from being protected by IPS (sip, H 323, etc)
- B. Use IPS only in Detect mode
- C. Use Recommended IPS profile
- D. Capture packets. Update the IPS database, and Back up custom IPS files

Answer: A

Question: 112

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

Question: 113

What command sets a specific interface as not accelerated?

- A. noaccel-s<interface1>
- B. fwaccel exempt state <interface1>
- C. nonaccel -s <interface1>
- D. fwaccel -n <intetface1 >

Answer: C

Question: 114

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?

- A. Configuration data of Log Servers and saved queries for applications
- B. Active Logs received from Security Gateways and Management Servers
- C. Active and past logs received from Gateways and Servers
- D. Log Domain is not stored in Postgres database, it is part of Solr indexer only

Answer: D

Question: 115

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

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

Answer: A

Question: 116

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 an access rule is missing
- B. the license became invalid 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

Question: 117

What table does the command "fwaccel conns" pull information from?

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

Answer: A

Question: 118

Which process is responsible for the generation of certificates?

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

Answer: B

Question: 119

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 cant be debugged

Answer: D

Question: 120

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=sk97638

SAMPLE QUESTIONS



*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:



Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>
Kill your exam at First Attempt....Guaranteed!