QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

156-585 Dumps
156-585 Braindumps
156-585 Real Questions
156-585 Practice Test
156-585 dumps free

CheckPoint

156-585

Check Point Certified Troubleshooting Expert Exam

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 ox1ffffe0
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 thesecuritypolicy 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 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 adresses 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 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

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