Checkpoint

Exam 156-515.65

Check Point Certified Security Expert Plus NGX R65

Version: 3.0

[Total Questions: 70]

Question No : 1

Which of the following explanations best describes the command fw lslogs?

A. Display a remote machine's log-file list.
B. Create a new log file. The old log has moved.
C. Control kernel.
D. Send signal to a daemon.
E. Display protected hosts.

Answer: A

Question No : 2

Which of the following processes is responsible for Policy related functions and communicationbetween a SmartConsole and SmartCenter Server?

A. cpd
B. fw monitor
C. fwd
D. fw sam
E. fwm

Answer: E

Question No : 3

What can you do in the advanced mode of GuiDbEdit Query that you cannot do in the simplemode?

A. Run a CPMI Query.
B. Log when modifications are made.
C. Query by object name.
D. Query by table name.

Answer: A

Question No : 4

Exhibit:

You create a FTP resource and select the Get check box. Which of the following actions are

denied to users, on net-detroit, when using FTP to an external host when the rule action is

"accept" and no other permissive ftp rule exists lower in the rule base?

A. mget
B. change
C. put
D. directory
E. list

Answer: C

Question No : 5

After a sudden spike in traffic, you receive this system log file message:

"kernel: FW-1: Log buffer is full".

Which is NOT a solution?

A. Increase the log buffer size.
B. Disable logging.
C. Reconfigure the minimum disk space "stop logging" threshold.
D. Decrease the amount of logging.

Answer: C

Question No : 6

When collecting information relating to the perceived problem, what is the most importantquestion to ask?

A. Is this problem repeatable?
B. Is this problem software or hardware related?
C. Under what circumstances does this problem occur?
D. What action or state am I trying to achieve?

E. Does the problem appear random or can you establish a pattern?

Answer: C

Question No : 7

fw monitor packets are collected from the kernel in a buffer. What happens if the buffer becomesfull?

A. The information in the buffer is saved and packet capture continues, with new data stored inthe buffer.
B. Older packet information is dropped as new packet information is added.
C. Packet capture stops.
D. All packets in it are deleted, and the buffer begins filling from the beginning.

Answer: D

Question No : 8

To cross-reference srfw monitor output what should you do?

A. run fw monitor on the client.
B. run srfw monitor a second time.
C. run fw monitor from the Gateway.
D. restart the client and run srfw monitor a second time.
E. run fw monitor and compare against a known good baseline.

Answer: C

Question No : 9

You use fwm to input the following command: fwm lock_adminA.What does this command do?

A. Uninstalls all Administrators, except the default Administrator
B. Locks all Administrator accounts
C. Unlocks all Administrator accounts
D. Sets the access level of Administrators to "all-access"

Answer: C

Question No : 10

Which of the following commands would you run to debug a VPN connection?

A. debug vpn ike
B. debug vpn ikeon
C. vpn debug ike
D. debug vpn ike on
E. vpn debug ikeon

Answer: E

Question No : 11

After configuring ClusterXL, where do you install the Security Policy?

A. On the Gateway Cluster
B. On the backup Security Gateway
C. On the Management Server
D. Policy installation is not required after configuring ClusterXL. This is automatic in NGX
E. On each Security Gateway in the Gateway Cluster

Answer: A

Question No : 12

Which of the following fw monitor commands only captures traffic between IP addresses

192.168.11.1 and 10.10.10.1?

A. fw monitor -e "accept src=192.168.11.1 or dst=192.168.11.1 or src=10.10.10.1 or dst=10.10.10.1;"
B. fw monitor -e "accept src=192.168.11.1 or dst=192.168.11.1; src=10.10.10.1 or dst=10.10.10.1;"
C. fw monitor -e "accept src=192.168.111 and dst=192.168.11.1; src=10.10.10.1 and dst=10.10.10.1;"
D. fw monitor -e "accept src=192.168.11.1 or dst=192.168.11.1; and src=10.10.10.1 or