Checkpoint

Exam 156-515

Check Point Certified Security Expert Plus NGX

Version: 5.0

[Total Questions: 70]

Topic break down

Topic	No. of Questions
Topic 0: A	70

Topic 0, A

A

Question No : 1 - (Topic 0)

Which native UNIX utility displays fw monitor output on Solaris?

A. tcpdump
B. Ethereal
C. snoop -i (lowercase)
D. CapView
E. snoop (lowercase)

Answer: C

Question No : 2 - (Topic 0)

How do you run fw ctl debug, to see all information about a cluster?

A. fw ctl debug cluster all
fw ctl debug > output
fw ctl debug uf 1024
B. fw ctl pstat
fw ctl debug all
fw ctl debug > out
C. fw ctl debug uf 1024
fw ctl debug cluster all
fw ctl kdebug > output
D. fw ctl debug on
fw ctl debug cluster all
fw ctl kdebug > output
E. fw ctl debug on
fw ctl debug uf 1024
fw ctl debug cluster all
fw ctl kdebug > output

Answer: C

Question No : 3 - (Topic 0)

Which one of these is a temporary pointer log file?

A. $FWDIR/log/xx.logptr
B. $FWDIR/log/xx.log
C. $FWDIR/log/xx.logaccount_ptr
D. $FWDIR/log/xx.logLuuidDB

Answer: D

Question No : 4 - (Topic 0)

Which of the following types of information should an Administrator use tcpdump to view?

A. DECnet traffic analysis
B. VLAN trunking analysis
C. NAT traffic analysis
D. Packet-header analysis
E. AppleTalk traffic analysis

Answer: D

Question No : 5 - (Topic 0)

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 dst=10.10.10.1;"
E. fw monitor -e "accept (src=192.168.11.1 and dst=10.10.10.1) or (src=10.10.10.1 and dst=192.168.11.1);"

Answer: E

Question No : 6 - (Topic 0)

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?

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		Net_Detroit	Tech-Support	Any Traffic	ftp->External	accept	Log

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

Answer: C

Question No : 7 - (Topic 0)

Which of the following commands can you run to view packet flow of a VPN-1 SecuRemote/SecureClient connection?

A. cpd monitor
B. vpn monitor
C. fw monitor
D. srfw monitor
E. sc monitor

Answer: D

Question No : 8 - (Topic 0)

Gill Bates is in charge of a large enterprise, which requires VPN connections between offices around the world. To achieve this Gill decides to use a dynamic routing protocol to make sure all offices are connected through the VPN community using tunnel interfaces among all peers. Nothing is configured in vpn_route.conf. However, Gill is experiencing connectivity problems and when examining the logs he discovers multiple "out of state" drops. What is the most likely cause of and solution to this problem?

A. Asymmetric routing will happen if nothing has been configured in vpn_route.conf. The vpn_route.conf should be configured to prevent asymmetric routing
B. The firewall security policy drops the traffic. Gill should introduce a Directional VPN rule to allow the VPN traffic