Checkpoint

Exam 156-115.77

Check Point Certified Security Master

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Chain Modules	2
Topic 2: NAT	1
Topic 3: ClusterXL	2
Topic 4: VPN Troubleshooting	1
Topic 5: SecureXL Acceleration debugging	1
Topic 6: Hardware Optimization	1
Topic 8: Enable CoreXL	1
Topic 9: IPS	1

Topic 1, Chain Modules

Question No : 1 - (Topic 1)

The command _____ shows which firewall chain modules are active on a gateway.

A. fw stat
B. fw ctl debug
C. fw ctl chain
D. fw ctl multik stat

Answer: C

Question No : 2 - (Topic 1)

What flag option(s) must be used to dump the complete table in friendly format, assuming there are more than one hundred connections in the table?

A. fw tab -t connections -f
B. fw tab -t connect -f -u
C. fw tab -t connections -s
D. fw tab -t connections -f –u

Answer: B

Topic 2, NAT

Question No : 3 - (Topic 2)

When viewing a NAT Table, What represents the second hexadecimal number of the 6-tuple:

A. Source port
B. Protocol
C. Source IP
D. Destination port

Answer: C

Topic 3, ClusterXL

Question No : 4 - (Topic 3)

Adam wants to find idle connections on his gateway. Which command would be best suited for viewing the connections table?

A. fw tab -t connections
B. fw tab -t connections -u –f
C. fw tab -t connections –x
D. fw tab -t connections –s

Answer: B

Question No : 5 - (Topic 3)

Which command should you run to debug the VPN-1 kernel module?

A. fw debug vpn on
B. vpn debug on TDERROR_ALL_ALL=5
C. fw ctl zdebug crypt kbuf
D. fw ctl debug -m VPN all

Answer: D

Topic 4, VPN Troubleshooting

Question No : 6 - (Topic 4)

Check Point Best Practices suggest that when you finish a kernel debug, you should run the command _____ .

A. fw debug 0
B. fw debug off
C. fw ctl debug default
D. fw ctl debug 0

Answer: D

Topic 5, SecureXL Acceleration debugging

Question No : 7 - (Topic 5)

When are rules that include Identity Awareness Access (IDA) roles accelerated through SecureXL?

A. Only when 'Unauthenticated Guests' is included in the access role.
B. Never, the inclusion of an IDA role disables SecureXL.
C. The inclusion of an IDA role has no bearing on whether the connection for the rule is accelerated.
D. Always, the inclusion of an IDA role guarantees the connection for the rule is accelerated.

Answer: C

Topic 6, Hardware Optimization

Question No : 8 - (Topic 6)

What is the difference between "connection establishment acceleration" (templating) and "traffic acceleration"?

A. These are the same technologies with different names.
B. "Connection establishment acceleration" only accelerates a single connection, while "traffic acceleration" accelerates similar traffic.
C. "Traffic acceleration" is accelerated through hardware, and "connection establishment acceleration" is accelerated in software.
D. "Traffic acceleration" only accelerates a single connection, while "connection establishment acceleration" accelerates similar traffic.

Answer: D

Topic 8, Enable CoreXL

Question No : 9 - (Topic 8)

What is required when changing the configuration of the number of workers in CoreXL?

A. A reboot

B. cpstop/cpstart
C. evstop/evstart
D. A policy installation

Answer: A

Topic 9, IPS

Question No : 10 - (Topic 9)

How would one enable 'INSPECT debugging' if one suspects IPS false positives?

A. Run command fw ctl set int enable_inspect_debug 1 from the command line.
B. Toggle the checkbox in Global Properties > Firewalls > Inspection section.
C. WebUI
D. Set the following parameter to true using GuiDBedit:
enable_inspect_debug_compilation.

Answer: D