DUMPSARENA

Check Point Certified Security Master

Checkpoint 156-115.77

Version Demo

Total Demo Questions: 15

Total Premium Questions: 295

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

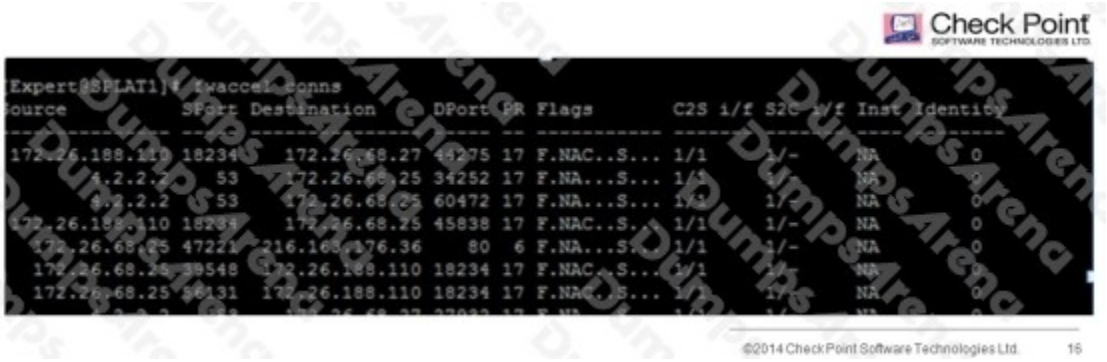
Topic Break Down

Topic	No. of Questions
Topic 1, Chain Modules	27
Topic 2, NAT	25
Topic 3, ClusterXL	35
Topic 4, VPN Troubleshooting	27
Topic 5, SecureXL Acceleration debugging	24
Topic 6, Hardware Optimization	33
Topic 7, Software Tuning	16
Topic 8, Enable CoreXL	16
Topic 9, IPS	30
Topic 10, IPV6	15
Topic 11, Advanced VPN	47
Total	295

QUESTION NO: 1

You run the command fwaccel conns and notice in the output that all the connections have

“F” in the “flags” column, see below:



What does this mean?

A. Connections are being “forward to firewall” (“f2f”).

B. Connections are being “forwarded” to the accelerating engine.

C. Connections are accelerated (“fastpath”).

D. Connections have the fragment flag set.

ANSWER: A

QUESTION NO: 2

What command would you use for a packet capture on an absolute position for TCP streaming (out) 1ffffe0

A. fw ctl chain -po 1ffffe0 -o monitor.out

B. fw monitor -po -0x1ffffe0 -o monitor.out

C. fw monitor -e 0x1ffffe0 -o monitor.out

D. fw monitor -pr 1ffffe0 -o monitor.out

ANSWER: B

QUESTION NO: 3

In R77, Under what circumstances would IPS bypass be enforced?

A. Single CoreXL fw instance usage over ‘High’ threshold, Average Memory over ‘High’ threshold

B. Single CoreXL fw instance usage over ‘Low’ threshold, Average Memory over ‘High’ threshold

C. Average CPU over ‘High’ threshold, Average Memory over ‘Low’ threshold

D. Average CPU over ‘High’ threshold, Average Memory over ‘High’ threshold

ANSWER: A

QUESTION NO: 4

PXL is considered to be what type of acceleration?

A. Fast Path

B. Slow Path

C. Medium Path

D. PXL is not related to acceleration

ANSWER: C

QUESTION NO: 5

Your cluster member is showing a state of "Ready". Which of the following is NOT a reason one would expect for this behaviour?

A. One cluster member is configured for 32 bit and the other is configured for 64 bit

B. CoreXL is configured differently on the two machines

C. The firewall that is showing "Ready" has been upgraded but the other firewall has not yet been upgraded

D. Firewall policy has not yet been installed to the firewall

ANSWER: D

QUESTION NO: 6

When troubleshooting a performance problem on multicore firewall that is using CoreXL, what command checks the number of connections each core is processing?

A. sim affinity -l

B. cat fwkern.conf

C. fw CTL pstat

D. fw ctl multik stat

ANSWER: D

QUESTION NO: 7

Which technology is not supported with route-based VPNs?

A. Unnumbered VTI

B. Numbered VTI

C. IKEv2

D. OSPF

ANSWER: C

QUESTION NO: 8

Which of the following BEST describes the command fw ctl chain function?

A. View how CoreXL is distributing traffic among the firewall kernel instances.

B. View established connections in the connections table.

C. View the inbound and outbound kernel modules and the order in which they are applied.

D. Determine if VPN Security Associations are being established.

ANSWER: C

QUESTION NO: 9

Which of the following IPS Layers is a set of signatures and/or handlers, where:

?Signature is a malicious pattern that is searched for.

?Handler is the INSPECT code that performs more complex inspection.

A. Passive Streaming Library (PSL)

B. Protections

C. Context Management Interface layer (CMI)

D. Protocol Parsers

ANSWER: B

QUESTION NO: 10

How do you add the route entry for the “Enforcement Point Gateway” on the Management

Server?

A. Designate this gateway in the VPN community properties.

B. Update file $FWDIR/conf/user.def on each peer with a route entry to the enforcement point gateway.

C. Edit file $FWDIR/conf/vpn_route.conf with a new route entry.

D. Edit peers’ WebUI to add a static route to the “designated enforcement point”.

ANSWER: C

QUESTION NO: 11

You run the command fw tab -t connections -s on both members in the cluster. Both members report differing values for "vals" and "peaks". Which may NOT be a reason for this difference?

A. Synchronization is not working between the two members

B. SGMs in a 61k environment only sync selective parts of the connections table.

C. Heavily used short-lived services have had synchronization disabled for performance improvement.

D. Standby member does not synchronize until a failover is needed.

ANSWER: D

QUESTION NO: 12

You are running a debugging session and you have set the debug environment to

TDERROR_ALL_ALL=5 using the command export TDERROR_ALL_ALL=5. How do you return the debug value to defaults?

A. fw ctl debug 0x1ffffe0

B. fw debug 0x1ffffe0

C. export TDERROR_ALL_ALL

D. unset TDERROR_ALL_ALL

ANSWER: D

QUESTION NO: 13

In IKEView while troubleshooting a VPN issue between your gateway and a partner site you see an entry that states “Invalid ID”. Which of the following is the most likely cause?

A. IKEv1 is not supported by the peer.

B. Time is not matching between two members.

C. The encryption parameters (hash, encryption type, etc.) do not match.

D. Wrong subnets are being negotiated.

ANSWER: D

QUESTION NO: 14

Which file should be edited to modify ClusterXL VIP Hide NAT rules, and where?

A. $FWDIR/lib/base.def on the cluster members

B. $FWDIR/lib/table.def on the SMC

C. $FWDIR/lib/table.def on the cluster members

D. $FWDIR/lib/base.def on the SMC

ANSWER: B

QUESTION NO: 15

Which program could you use to analyze Phase I and Phase II packet exchanges?

A. vpnView

B. Check PointView

C. IKEView

D. vpndebugView

ANSWER: C