Check Point Certified Security Master

1. 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(s): B

---

2. When VPN user-based authentication fails, which of the following debug logs is essential to understanding the issue?

A. Vpnd.elg

B. IKE.elg

C. VPN-1 kernel debug logs

D. fw monitor trace

Answer(s): B

---

3. What command allows you to monitor IPV6 packets in the kernel module?

A. ip -6 neigh show

B. tcpdump -nni eth<n> ip6

C. fw6 monitor

D. ip -6 addr show

Answer(s): C

---

4. What would be a reason for changing the "Magic MAC"?

A. To allow two or more cluster members to exist on the same network.

B. To allow for automatic upgrades.

C. To allow the two cluster members to use the same virtual IP address.

D. To allow two or more clusters to exist on the same network.

Answer(s): D

---

5. What is the log file that shows the keep alive packets during the debug process?

A. $FWDIR/log/ikev2.xmll

B. $FWDIR/log/ike.elg

C. $FWDIR/log/ike.xmll

D. $FWDIR/log/vpnd.elg

Answer(s): B

---

6. You want to verify that the majority of your connections are being optimized by SecureXL. What command would you run to establish this information?

A. fwaccel conns -s

B. fw ctl pstat

C. sim_dbg -s

D. fw tab -t connections -s

Answer(s): A

---

7. Which of the following items is NOT part of the columns of the chain modules?

A. Chain position

B. Inbound/Outbound chain

C. Module location

D. Function Pointer

Answer(s): B

---

8. With the default ClusterXL settings what will be the state of an active gateway upon using the command ClusterXL_admin up?

A. Standby

B. Ready

C. Active

D. Down

Answer(s): A

---

9. Which routing protocols are not supported with GAIA OS running VTIs?

A. RIPv1; RIPv2

B. OSPF

C. BGP

D. Static routes

Answer(s): A

---

10. CoreXL on IPSO R77.20 does NOT support which of the following features?

A. Route-based VPN

B. Overlapping NAT

C. Check Point QoS

D. IPv6

Answer(s): C

---

11. ACME Corp has a cluster consisting of two 13500 appliances. As the Firewall Administrator, you notice that on an output of top, you are seeing high CPU usage of the cores assigned as SNDs, but low CPU usage on cores assigned to individual fw_worker_X processes. What command should you run next to performance tune your cluster?

A. fw ctl debug -m cluster + all - this will show you all the connections being processed by ClusterXL and explain the high CPU usage on your appliance.

B. fwaccel off - this will turn off SecureXL, which is causing your SNDs to be running high in the first place.

C. fwaccel stats -s - this will show you the acceleration profile of your connections and potentially why your SNDs are running high while other cores are running low.

D. fw tab -t connections -s - this will show you a summary of your connections table, and allow you to determine whether there is too much traffic traversing your firewall.

Answer(s): C

---

12. What command displays the Connections Table for a specified CoreXL firewall instance?

A. fw tab -t connection | grep fw<FW_INSTANCE_ID>

B. fw tab -t connections -s

C. fw tab -t connections

D. fw -i FW_INSTANCE_ID tab -t connections [flags]

Answer(s): D

---

13. What is the length of an IPv6 address?

A. 128 bits

B. 128 Bytes

C. 6 Bytes

D. 54 bits

Answer(s): A

---

14. what command other than fw ctl pstat, will display your peak concurrent connections?

A. fw ctl get int fw_peak_connections

B. top

C. netstat -ni

D. fw tab -t connections -s

Answer(s): D

---

15. Using the default values in R77 how many kernel instances will there be on a 16-core gateway?

A. 12

B. 8

C. 16

D. 14

Answer(s): D

---

16. Why would you choose to combine dynamic routing protocols and VPNs?

A. Dynamic-routing information can propagate over the VPN, utilizing the VPN as just another point-to-point link in the network.

B. All options listed.

C. The VPN device can be automatically updated with network changes on any VPN peer Gateway without the need to update the VPN Domain's configuration.

D. In the case of one tunnel failure, other tunnels may be used to route the traffic.

Answer(s): B

---

17. The "Hide internal networks behind the Gateway's external IP" option is selected. What defines what traffic will be NATted?

A. The Firewall policy of the gateway

B. The network objects configured for the network

C. The VPN encryption domain of the gateway object

D. The topology configuration of the gateway object

Answer(s): D

---

18. What happens to manual changes in the file $FWDIR/conf/local.arp when adding Proxy ARP entries through the GAiA portal or Clish?

A. They are merged with the new entries added from the GAiA Portal / Clish.

B. Nothing.

C. They are overwritten.

D. If the file $FWDIR/conf/local.arp has been edited manually, you are not able to add Proxy ARP entries through the GAiA portal or Clish.

Answer(s): C

---

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

A. Set the following parameter to true using GuiDBedit: enable_inspect_debug_compilation.

B. Run command fw ctl set int enable_inspect_debug 1 from the command line.

C. WebUI

D. Toggle the checkbox in Global Properties > Firewalls > Inspection section.

Answer(s): A

---

20. When viewing connections using the command fw tab -t connections, all entries are displayed with a 6-tuple key, the elements of the 6-tuple include the following EXCEPT:

A. direction (inbound / outbound)

B. destination port number

C. interface id

D. source port number

Answer(s): C
