

# 156-115.77<sup>Q&As</sup>

Check Point Certified Security Master

## Pass CheckPoint 156-115.77 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/156-115-77.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



## QUESTION 1

Which flag in the fw monitor command is used to print the position of the kernel chain?

- A. -all
- B. -k
- C. -c
- D. -p

Correct Answer: D

---

## QUESTION 2

From the output of the following cphaprob -i list, what is the most likely cause of the clustering issue? Cluster B> cphaprob -i list Built-in Devices: Device Name: Interface Active Check Current state: OK Device Name: HA Initialization Current state: OK Device Name: Recovery Delay Current state: OK Registered Devices: Device Name: Synchronization Registration number: 0 Timeout: none Current state: OK Time since last

report: 3651.5 sec

Device Name: Filter Registration number: 1 Timeout: none Current state: problem Time since last report:

139 sec

Device Name: routed Registration number: 2 Timeout: none Current state: OK Time since last report:

3651.9 sec

Device Name: cphad Registration number: 3 Timeout: none Current state: OK Time since last report:

3696.5 sec

Device Name: fwd Registration number: 4 Timeout: none Current state: OK Time since last report:

3696.5 sec

- A. There is an interface down on Cluster A
- B. There is a sync network issue between Cluster A and Cluster B
- C. The routing table on Cluster B is different from Cluster A
- D. Cluster B and Cluster A have different versions of policy installed.

Correct Answer: D

---

## QUESTION 3

What command should a firewall administrator use to begin debugging SecureXL?

- A. fwaccel dbg api + verbose add
- B. fwaccel debug m
- C. fwaccel dbg -m
- D. SecureXL cannot be debugged and the kernel debug will give enough output to help the firewall administrator to understand the firewall's behaviour. The right command to use is fw ctl debug m fw.

Correct Answer: C

---

## QUESTION 4

While troubleshooting a connectivity issue with an internal web server, you know that packets are getting to the upstream router, but when you run a tcpdump on the external interface of the gateway, the only traffic you observe is ARP requests coming from the upstream router. Does the problem lie on the Check Point Gateway?

- A. Yes This could be due to a misconfigured route on the firewall.
- B. No This is a layer 2 connectivity issue and has nothing to do with the firewall.
- C. No The firewall is not dropping the traffic, therefore the problem does not lie with the firewall.
- D. Yes This could be due to a misconfigured Static NAT in the firewall policy.

Correct Answer: D

---

## QUESTION 5

When using Geo Protections, you find there are logs for a country that you believe is incorrect. What file do you review to verify what country Geo Protections should identify the traffic as?

- A. asm.C
- B. objects.C
- C. objects\_5\_0.C
- D. IpToCountry.csv

Correct Answer: D

---

## QUESTION 6

You are analyzing your firewall logs, /var/log/messages, and repeatedly see the following kernel message:

\\'kernel: neighbor table overflow\\'

What is the cause?

- A. Arp cache overflow
- B. OSPF neighbor down
- C. Nothing, you can disconsider it.
- D. Cluster member table overflow

Correct Answer: A

## QUESTION 7

According to this Rule Base, templates will be created until which rule?



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	0	Terminal server	Corporate-internal-	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
2	0	Mail and Web servers	InternalNet	Corporate-dmz-net	Any Traffic	http https smtp	accept	Log	Policy Targets	Any
3	0	SMTP	Corporate-mail-sen	Internal-net-group	Any Traffic	smtp	accept	Log	Policy Targets	Work-Ho
4	0	DMZ and Internet	Internal-net-group	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
5	0	Clean up rule	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any

©2014 Check Point Software Technologies Ltd.

8

- A. Rule 4
- B. Rule 2
- C. Rule 3
- D. Rule 5

Correct Answer: B

## QUESTION 8

Which of the following is NEVER affected by incorrect OS time and date configuration?

- A. VPN PSK authentication
- B. VPN certificate authentication
- C. SIC
- D. Identity Awareness Kerberos authentication

Correct Answer: A

**QUESTION 9**

A system administrator wants to convert an IPv6 gateway from a standard gateway into a gateway running VSX mode. What does he need to consider?

- A. It is not possible to convert a gateway with IPv6 enabled to VSX mode.
- B. There needs to be proper IPv6 routing setup.
- C. At least two interfaces need to be configured with IPv6.
- D. Policy needs to be properly applied to the gateway before converting the system to VSX mode.

Correct Answer: A

---

**QUESTION 10**

The command fwaccel stat displays what information?

- A. Accelerator status, accept templates, drop templates
- B. Accelerated packets, accept templates, dropped packets
- C. Accelerator status, accelerated rules, drop templates
- D. Accelerator status, CoreXL state, drop templates

Correct Answer: A

---

**QUESTION 11**

You are adding a new gateway into your network. You must make sure that it is running the latest Corporate approved IPS profile. How can you get this information to your new gateway?

- A. From the command line, run: `ips_import -f [-p ]`.
- B. IPS profiles must be manually configured on each gateway.
- C. From the command line, run: `ips_export_import import -f [-p ]`.
- D. From the Smart Dashboard IPS tab select import IPS profiles and select the gateway to get the profile from.

Correct Answer: C

---

**QUESTION 12**

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.

Correct Answer: D

---

## QUESTION 13

In the process of troubleshooting traffic issues across a VPN tunnel, you notice on the output of fw monitor -e host(172.21.1.10), accept; that packets are going through the inbound chain (i > I) and then disappearing after the outbound chain (o > \_\_), while you were expecting to see the packet leave on O. What could be causing this issue?

- A. When packets are destined to leave through a VPN tunnel, it is encrypted and encapsulated in an ESP packet, and thus will not show up on a fw monitor.
- B. It\\'s not showing up on the fw monitor because it is exiting the wrong interface
- C. The packet is getting silently dropped because there is no route for the packet.
- D. The gateway never completed the IKE and IPSec key exchange, and the tunnel does not exist yet.

Correct Answer: A

---

## QUESTION 14

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

- A. vpnView
- B. Check PointView
- C. IKEView
- D. vpndebugView

Correct Answer: C

---

## QUESTION 15

You have just configured HA and find that connections are not being synced. When you have a failover, users complain that they are losing their connections. What command could you run to see the state synchronization statistics?

- A. fw ctl pstat
- B. fw sync stats
- C. cphaprob stat
- D. fw ctl get int fw\_state\_sync\_stats

Correct Answer: A

[Latest 156-115.77 Dumps](#)

[156-115.77 PDF Dumps](#)

[156-115.77 Study Guide](#)