

## 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**

You are in VPN troubleshooting with a Partner and you suspect a mismatch configuration in Diffie- Hellman (DH) group to Phase1. After starting a vpn debug, in which packet would you look to analyze this option in your debug file?

- A. Packet3
- B. Packet4
- C. Packet5
- D. Packet1

Correct Answer: D

---

**QUESTION 2**

You are experiencing an issue where Endpoint Connect client connects successfully however, it disconnects every 20 seconds. What is the most likely cause of this issue?

- A. The Accept Remote Access control connections is not enabled in Global Properties > FireWall Implied Rules.
- B. You have selected IKEv2 only in Global Properties > Remote Access > VPN Authentication and Encryption.
- C. You are not licensed for Endpoint Connect client.
- D. Your remote access community is not configured.

Correct Answer: A

---

**QUESTION 3**

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

- A. fw ctl get int fw\_peak\_connections
- B. netstat -ni
- C. fw tab -t connections -s
- D. top

Correct Answer: C

---

**QUESTION 4**

A firewall administrator knows the details of the packet header for an already established connection going through a firewall. What command will show if SecureXL will accelerate that packet?

- A. fw ctl zdebug + sxl error warning asm
- B. fwaccel conns
- C. fwaccel templates
- D. fw tab t connections f | grep `dest. port #` | grep `source port #` | grep `dest. IP address`

Correct Answer: C

---

#### QUESTION 5

What command would you use to check if CoreXL is enabled?

- A. fw ctl multik stat
- B. cpconfig
- C. fw ctl affinity -1
- D. fw ctl pstat

Correct Answer: A

---

#### QUESTION 6

You run the commands:

```
fw ctl debug 0
```

```
fw ctl debug -buf 32000
```

Which of the following commands would be best to troubleshoot a clustering issue?

- A. fw ctl zdebug -m cluster + all
- B. fw ctl debug -m CLUSTER + conf stat
- C. fw ctl debug -m cluster + pnote stat if
- D. fw ctl kdebug -m CLUSTER all

Correct Answer: C

---

#### QUESTION 7

The 'Maximum Entries' value in the GAIa Portal corresponds to the 'gc\_thresh3' parameter in the Linux kernel and has value of 1024. Knowing this, you know that gc\_thresh2 and gc\_thresh1 if are automatically set to the values:

- A. gc\_thresh2=256 and gc\_thresh1=128

- B. gc\_thresh2=512 and gc\_thresh1=256
- C. gc\_thresh2=1024 and gc\_thresh1=1024
- D. gc\_thresh1=256 and gc\_thresh2=128

Correct Answer: B

---

## QUESTION 8

How do you enable IPv6 support on a R77 gateway running the GAIA OS?

- A. IPv6 is enabled by default.
- B. Under WebUI go to System Management > System Configuration, turn on IPv6 Support, click apply and reboot.
- C. Enable the IPv6 Software Blade for the gateway in Smart Dashboard.
- D. Run the IPv6 script \$FWDIR/scripts/fwip6\_enable and reboot.

Correct Answer: B

---

## QUESTION 9

Tom is troubleshooting NAT issues using fw monitor and Wireshark. He tries to initiate a connection from the external network to a DMZ server using the public IP which the firewall translates to the actual IP of the server. He analyzes the captured packets using Wireshark and observes that the destination IP is being changed as required by the firewall but does not see the packet leave the external interface. What could be the reason?

- A. The translation might be happening on the client side and the packet is being routed by the OS back to the external interface.
- B. The translation might be happening on the server side and the packet is being routed by OS back to the external interface.
- C. Packet is dropped by the firewall.
- D. After the translation, the packet is dropped by the Anti-Spoofing Protection.

Correct Answer: B

---

## QUESTION 10

What does the command fwaccel templates do?

- A. Starts firewall acceleration after fwaccel off was run or SecureXL was enabled by using the command cpconfig.
- B. That SecureXL has been enabled in the cpconfig command menu.
- C. Shows templates existing in the SecureXL device. This is so that an administrator can look for the template that matches the specific traffic.

D. The Rule Base mapping between actual rules and the template built up in Layer 2.

Correct Answer: C

### QUESTION 11

You are troubleshooting an issue for your HR team. One of the users is using IP 10.10.10.24. They having been trying to access the vacation servers but all connections are failing. You have checked the logs and do not see any dropped traffic. You have a suspicion that the drop is not being logged. What command could you use to confirm this?

- A. fw -t connections -s
- B. fw ctl zdebug + log dynlog
- C. You cannot run a command for this; you must enable logging on all rules
- D. fw ctl pstat host 10.10.10.24

Correct Answer: B

### QUESTION 12

Compare these two images to establish which blade/feature was disabled on the firewall.



#### Before

```
[Expert@fw1:0]# fw ctl chain
in chain (16):
0: -7f300000 (c26a9c70) (ffffffff) IP Options Strip (in) (ipopt_strip)
1: - 20000000 (c183b020) (00000003) vpn decrypt (vpn)
2: - 1ffffff6 (c1846080) (00000001) l2tp inbound (l2tp)
3: - 1ffffff6 (c26ab420) (00000001) Stateless verifications (in) (asm)
4: - 1ffffff2 (c1862a60) (00000003) vpn tagging inbound (tagging)
5: - 1ffffff0 (c1838700) (00000003) vpn decrypt verify (vpn_ver)
6: - 10000000 (c2728940) (00000003) SecureXL conn sync (secxl_sync)
7: 0 (c2654220) (00000001) fw VM inbound (fw)
8: 1 (c26cb2b0) (00000002) wire VM inbound (wire_vm)
9: 20000000 (c1839b90) (00000003) vpn policy inbound (vpn_pol)
10: 10000000 (e2726e40) (00000003) SecureXL inbound (secxl)
11: 7f600000 (c269f2b0) (00000001) fw SCV inbound (scv)
12: 7f730000 (c2835210) (00000001) passive streaming (in) (pass_str)
13: 7f750000 (c2a2b3f0) (00000001) TCP streaming (in) (cpas)
14: 7f800000 (c26aa010) (ffffffff) IP Options Restore (in) (ipopt_res)
15: 7fb00000 (c2db29f0) (00000001) HA Forwarding (ha_for)
out chain (14):
0: -7f300000 (c26a9c70) (ffffffff) IP Options Strip (out) (ipopt_strip)
1: - 1ffffff6 (c1837fc0) (00000003) vpn nat outbound (vpn_nat)
2: - 1ffffff0 (c2a2b270) (00000001) TCP streaming (out) (cpas)
3: - 1fffff50 (c2835210) (00000001) passive streaming (out) (pass_str)
4: - 1ff00000 (c1862a60) (00000003) vpn tagging outbound (tagging)
5: - 1ff00000 (c26ab420) (00000001) Stateless verifications (out) (asm)
6: 0 (c2654220) (00000001) fw VM outbound (fw)
7: 1 (c26cb2b0) (00000002) wire VM outbound (wire_vm)
8: 20000000 (c18381c0) (00000003) vpn policy outbound (vpn_pol)
9: 10000000 (c2726e40) (00000003) SecureXL outbound (secxl)
10: 1ffffff0 (c1845a30) (00000001) l2tp outbound (l2tp)
11: 20000000 (c183ba60) (00000003) vpn encrypt (vpn)
12: 7f700000 (c2a2d840) (00000001) TCP streaming post VM (cpas)
13: 7f800000 (c26aa010) (ffffffff) IP Options Restore (out) (ipopt_res)
```

#### After

```
[Expert@fw1:0]# fw ctl chain
in chain (11):
0: -7f300000 (c26a9c70) (ffffffff) IP Options Strip (in) (ipopt_strip)
1: - 1ffffff6 (c26ab420) (00000001) Stateless verifications (in) (asm)
2: - 10000000 (c1728940) (00000003) SecureXL conn sync (secxl_sync)
3: 0 (c2654220) (00000001) fw VM inbound (fw)
4: 1 (c26cb2b0) (00000002) wire VM inbound (wire_vm)
5: 10000000 (c1726e40) (00000003) SecureXL inbound (secxl)
6: 7f300000 (c169f2b0) (00000001) fw SCV inbound (scv)
7: 7f730000 (c2835210) (00000001) passive streaming (in) (pass_str)
8: 7f750000 (c1a2b3f0) (00000001) TCP streaming (in) (cpas)
9: 7f300000 (c26aa010) (ffffffff) IP Options Restore (in) (ipopt_res)
10: 7fb00000 (c2db29f0) (00000001) HA Forwarding (ha_for)
out chain (9):
0: -7f300000 (c26a9c70) (ffffffff) IP Options Strip (out) (ipopt_strip)
1: - 1ffffff0 (c1a2b270) (00000001) TCP streaming (out) (cpas)
2: - 1fffff50 (c1835210) (00000001) passive streaming (out) (pass_str)
3: - 1ff00000 (c26ab420) (00000001) Stateless verifications (out) (asm)
4: 0 (c2654220) (00000001) fw VM outbound (fw)
5: 1 (c26cb2b0) (00000002) wire VM outbound (wire_vm)
6: 10000000 (c1726e40) (00000003) SecureXL outbound (secxl)
7: 7f700000 (c1a2d840) (00000001) TCP streaming post VM (cpas)
8: 7f300000 (c26aa010) (ffffffff) IP Options Restore (out) (ipopt_res)
```

- A. IPS
- B. VPN

C. NAT

D. L2TP

Correct Answer: B

---

## QUESTION 13

From which version can you add Proxy ARP entries through the GAIa portal?

A. R77.10

B. R77

C. R75.40

D. R76

Correct Answer: C

---

## QUESTION 14

What command would you use to determine if a particular connection is being accelerated by SecureXL?

A. fw tab t connections u

B. fw ctl kdebug

C. fwaccel stat

D. fwaccel conns

Correct Answer: D

---

## QUESTION 15

What type(s) of VTI interfaces do Edge gateways support?

A. Both numbered and unnumbered

B. Unnumbered interfaces

C. Numbered interfaces

D. Neither numbered and unnumbered

Correct Answer: C

---