# DUMPSBOSS.COM

# Check Point Certified Security Master

## Checkpoint 156-115.77

## Version Demo

## Total Demo Questions: 15

## Total Premium Questions: 295

## Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

dumpsboss.com

# 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

What are the kernel parameters that control "Magic MACs"?

**A.** fwha_magic_mac and fw_forward_magic_mac

**B.** fwha_mac_magic and fw_mac_forward_magic

**C.** cpha_mac_magic and cp_mac_forward_magic

**D.** cpha_magic_mac and cpha_mac_forward_magic

**ANSWER: B**

## QUESTION NO: 2

In a VPN configuration, the following mode can be used to increase throughput by bypassing firewall enforcement.

**A.** Virtual Tunnel Interface (VTI) Mode can bypass firewall for all encrypted traffic

**B.** Hub Mode can be used to bypass stateful inspection

**C.** There is no such mode that can bypass firewall enforcement

**D.** Wire mode can be used to bypass stateful inspection

**ANSWER: D**

## QUESTION NO: 3

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**

## QUESTION NO: 4

In IPS what does a high confidence rating mean?

**A.** This is a rating for how confident Check Point is with catching this attack

**B.** This is a rating for how likely this attack is to penetrate most systems

**C.** There is a high likelihood of false positives

**D.** There is a low likelihood of false positives

**ANSWER: D**

## QUESTION NO: 5

How do you set up Port Address Translation?

**A.** Since Hide NAT changes to random high ports it is by definition PAT (Port Address Translation).

**B.** Create a manual NAT rule and specify the source and destination ports.

**C.** Edit the service in SmartDashboard, click on the NAT tab and specify the translated port.

**D.** Port Address Translation is not support in Check Point environment

**ANSWER: B**

## QUESTION NO: 6

Since R76 GAiA, what is the method for configuring proxy ARP entries for manual NAT rules?

**A.** WebUI or add proxy ARP ... commands via CLISH

**B.** SmartView Tracker

**C.** local.arp file

**D.** SmartDashboard

**ANSWER: A**

## QUESTION NO: 7

For URL Filtering in the Cloud in R75 and above, what table is used to contain the URL

Filtering cache values?

**A.** urlf_blade_on_gw

**B.** urlf_cache_tbl

**C.** urlf_cache_table

**D.** url_scheme_tab

**ANSWER: C**

## QUESTION NO: 8

Your gateway object is currently defined with a max connection count of 25k connections in Smart Dashboard. Which of the following commands would show you the current and peak connection counts?

**A.** show connections all

**B.** fw ctl conn

**C.** fw ctl chain

**D.** fw ctl pstat

**ANSWER: D**

## QUESTION NO: 9

The command that lists the firewall kernel modules on a Security Gateway is:

**A.** fw list kernel modules

**B.** fw ctl kernel chain

**C.** fw ctl debug -m

**D.** fw list modules

**ANSWER: C**

## QUESTION NO: 10

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: 11

You are having issues with dynamic routing after a failover. The traffic is now coming from the backup and is being dropped as out of state. What is the BEST configuration to avoid stateful inspection dropping your dynamic routing traffic?

**A.** Implement Wire mode.

**B.** In Global Properties select Accept other IP protocols stateful replies for unknown services.

**C.** Enable Visitor mode.

**D.** Create additional explicit rules.

**ANSWER: A**

## QUESTION NO: 12

What does the command vpn shell interface add numbered 192.168.0.1 192.168.0.2

Gateway_A to_B accomplish?

**A.** Between Security Gateways A and B, 192.168.0.1 is assigned as the endpoint IP address to Gateway A 192.168.0.2 is assigned to Gateway B

**B.** Between Security Gateways A and B 192.168.0.2 is assigned as the endpoint IP address to Gateway A 192.168.0.1 is assigned to Gateway B

**C.** shell is not a valid option for the command vpn.

**D.** This command can be used to create a VPN tunnel from the command line without having any VPN configuration in Smart Dashboard (although "IPSec VPN" must still be enabled on the gateway).

**ANSWER: A**

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.

**ANSWER: D**

**QUESTION NO: 14**

Where would an administrator set an email alert for a specific permanent VPN tunnel?

**A.** Edit the file vpnconf.

**B.** Run sysconfig.

**C.** In the Tunnel Properties select Mail Alert.

**D.** You can only enable logging or SNMP traps.

ANSWER: C

**Explanation:**

:

C11O2 - Advanced VPN

## QUESTION NO: 15

Which feature is not supported with unnumbered VTI?

**A.** Proxy interfaces

**B.** High availability

**C.** Policy based routing

**D.** Anti-spoofing

ANSWER: D