

100% Money Back
Guarantee

Vendor:CheckPoint

Exam Code:156-315.81

Exam Name:Check Point Certified Security Expert
R81

Version:Demo

QUESTION 1

Using fw monitor you see the following inspection point notion E and i what does that mean?

- A. E shows the packet before the VPN encryption, i after the inbound firewall VM
- B. E shows the packet reaching the external interface, i leaving the internal interface
- C. E shows the packet after the VPN encryption, i before the inbound firewall VM
- D. E shows the packet leaving the external interface, i reaching the internal interface

Correct Answer: C

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_CLI_Reference_Guide/Topics-CLIG/FWG/fw-monitor.htm i (for example, eth4:i) Pre-Inbound - Before the inbound FireWall VM E (for example, eth4:E) Post-Outbound - VPN Outbound after encrypt

QUESTION 2

The Check Point history feature in R81 provides the following:

- A. View install changes and install specific version
- B. View install changes
- C. Policy Installation Date, view install changes and install specific version
- D. Policy Installation Date only

Correct Answer: D

QUESTION 3

Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

- A. show interface eth0 mq
- B. ethtool A eth0
- C. ifconfig -i eth0 verbose
- D. ip show Int eth0

Correct Answer: A

QUESTION 4

The log server sends what to the Correlation Unit?

A. Authentication requests

B. CPMI dbsync

C. Logs

D. Event Policy

Correct Answer: C

QUESTION 5

When an encrypted packet is decrypted, where does this happen?

A. Security policy

B. Inbound chain

C. Outbound chain

D. Decryption is not supported

Correct Answer: A

QUESTION 6

What is the SandBlast Agent designed to do?

A. Performs OS-level sandboxing for SandBlast Cloud architecture

B. Ensure the Check Point SandBlast services is running on the end user's system

C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with the network

D. Clean up email sent with malicious attachments

Correct Answer: C

QUESTION 7

Alice and Bob are going to deploy Management Data Plane Separation (MDPS) for all their Check Point Security Gateway(s)/Cluster(s). Which of the following statement is true?

A. Each network environment is dependent and includes interfaces, routes, sockets, and processes

B. Management Plane -To access, provision and monitor the Security Gateway

C. Data Plane -To access, provision and monitor the Security Gateway

D. Management Plane -for all other network traffic and processing

Correct Answer: B

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolution_details=andsolutionid=sk138672

QUESTION 8

What needs to be configured if the NAT property `Translate destination or client side` is not enabled in Global Properties?

- A. A host route to route to the destination IP.
- B. Use the file local.arp to add the ARP entries for NAT to work.
- C. Nothing, the Gateway takes care of all details necessary.
- D. Enabling `Allow bi-directional NAT` for NAT to work correctly.

Correct Answer: C

QUESTION 9

CoreXL is NOT supported when one of the following features is enabled: (Choose three)

- A. Route-based VPN
- B. IPS
- C. IPv6
- D. Overlapping NAT

Correct Answer: ACD

CoreXL does not support Check Point Suite with these features: Check Point QoS (Quality of Service)

Route-based VPN IPv6 on IPSO Overlapping NAT Reference:

[https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731 .htm](https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm)

QUESTION 10

In order to get info about assignment (FW, SND) of all CPUs in your SGW, what is the most accurate CLI command?

- A. fw ctl sdstat
- B. fw ctl affinity -l -a -r -v
- C. fw ctl multik stat
- D. cpinfo

Correct Answer: B

QUESTION 11

Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

- A. Check Point Remote User
- B. Check Point Capsule Workspace
- C. Check Point Mobile Web Portal
- D. Check Point Capsule Remote

Correct Answer: C

QUESTION 12

To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

- A. Accept Template
- B. Deny Template
- C. Drop Template
- D. NAT Template

Correct Answer: B