156-315.81$^{\text{Q\&As}}$

Check Point Certified Security Expert R81

Pass CheckPoint 156-315.81 Exam with 100% Guarantee

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

https://www.geekcert.com/156-315-81.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

After finishing installation admin John likes to use top command in expert mode. John has to set the expert-password and was able to use top command. A week later John has to use the top command again, He detected that the expert password is no longer valid. What is the most probable reason for this behavior?

A. "write memory" was not issued on clish

B. changes are only possible via SmartConsole

C. "save config" was not issued in expert mode

D. "save config" was not issued on clish

Correct Answer: D

The most probable reason for the expert password to be no longer valid after a week is that save config was not issued on clish. The clish command set expert- password sets the expert password for the current session only. To make the password persistent, the clish command save config must be issued after setting the expert password2. The other options are not relevant for setting the expert password. References: 2: Check Point Software, Getting Started, Setting Expert Password.

QUESTION 2

From SecureXL perspective, what are the three paths of traffic flow:

A. Initial Path; Medium Path; Accelerated Path

B. Layer Path; Blade Path; Rule Path

C. Firewall Path; Accelerated Path; Medium Path

D. Firewall Path; Accept Path; Drop Path

Correct Answer: C

From SecureXL perspective, the three paths of traffic flow are Firewall Path, Accelerated Path, and Medium Path. Firewall Path is the path that handles packets that are not processed by SecureXL and are sent to the Firewall kernel for inspection. Accelerated Path is the path that handles packets that are processed by SecureXL and bypass the Firewall kernel. Medium Path is the path that handles packets that are partially processed by SecureXL and partially by the Firewall kernel1. References: Check Point R81 Performance Tuning Administration Guide

QUESTION 3

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the tight protections in place. Check Point has been selected for the security vendor. Which Check Point product protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

A. IPS AND Application Control

B. IPS, anti-virus and anti-bot

C. IPS, anti-virus and e-mail security

D. SandBlast

Correct Answer: D

SandBlast is the best Check Point product to protect against malware and zero-day attacks while ensuring quick delivery of safe content to your users. SandBlast is an advanced network threat prevention solution that uses a combination of technologies to detect and block known and unknown threats before they reach your network. SandBlast uses Threat Emulation, which is a sandboxing technology that inspects files for malicious behavior in a virtual environment; Threat Extraction, which removes potentially malicious elements from files and delivers clean and safe content to your users; Anti-Bot, which identifies and blocks botnet communications and prevents data exfiltration; Anti-Virus, which scans files for known malware signatures; and IPS, which monitors network traffic for malicious or anomalous patterns. SandBlast also provides comprehensive reports and forensic analysis on the detected threats and their origin and behavior.

QUESTION 4

How many images are included with Check Point TE appliance in Recommended Mode?

A. 2(OS) images

B. images are chosen by administrator during installation

C. as many as licensed for

D. the newest image

Correct Answer: A

The Check Point TE appliance in Recommended Mode includes 2(OS) images. One image is used for running the appliance, and the other image is used for backup and recovery purposes. The images are not chosen by the administrator during installation, nor based on the license or the latest version. References: [Check Point R81 Threat Emulation Administration Guide]

QUESTION 5

Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs

B. Capsule Cloud

C. Capsule Enterprise

D. Capsule Workspace

Correct Answer: C

Check Point Capsule is a suite of solutions designed to provide comprehensive mobile security and secure access. The components of Check Point Capsule include:

Capsule Docs (Option A): A component that secures document sharing and protects sensitive data.

Capsule Cloud (Option B): A component that provides cloud-based security services.

Capsule Workspace (Option D): A component that provides secure workspace on mobile devices.

Option C, "Capsule Enterprise," is not a recognized component of Check Point Capsule based on the available information. Therefore, it is the correct answer as the component that is NOT part of Check Point Capsule.

References: Check Point Certified Security Expert (CCSE) R81 training materials and documentation.