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.passapply.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

Which statement is true regarding redundancy?

A. System Administrators know when their cluster has failed over and can also see why it failed over by using the cphaprob if command.

B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.

C. Machines in a ClusterXL High Availability configuration must be synchronized.

D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

Correct Answer: D

The statement that is true regarding redundancy is Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments. ClusterXL and VRRP are two technologies that provide high availability and load sharing for Security Gateways. They are both supported by Gaia OS and can be deployed on various platforms5. The other statements are either false or incomplete regarding redundancy. References: Check Point R81 ClusterXL Administration Guide, Check Point R81 Gaia Administration Guide

QUESTION 2

How is communication between different Check Point components secured in R81? As with all questions, select the BEST answer.

A. By using IPSEC

B. By using SIC

C. By using ICA

D. By using 3DES

Correct Answer: B

Communication between different Check Point components is secured by using SIC, which stands for secure internal communication. SIC is a certificate-based channel that uses standards-based TLS 1.2 for creating secure connections and AES128 for encryption. SIC ensures that only authorized components can communicate with each other and that the communication is protected from eavesdropping and tampering. SIC is established by using a one-time password (OTP) that is generated when a Check Point component is created or installed. The OTP is used to initialize the trust relationship between the component and the Security Management Server, which acts as an internal certificate authority (ICA) that issues and revokes certificates for the components.

QUESTION 3

Using Web Services to access the API, which Header Name-Value had to be in the HTTP Post request after the login?

A. X-chkp-sid Session Unique Identifier

B. API-Key

C. user-uid

D. uuid Universally Unique Identifier

Correct Answer: A

The header name-value that has to be in the HTTP Post request after the login when using Web Services to access the API is X-chkp-sid Session Unique Identifier. This header contains the session ID that is returned by the login command and identifies the session for subsequent API commands. The session ID is valid for a limited time and can be extended by using keepalive or logout commands. References: [Check Point R81 Management API Reference Guide]

QUESTION 4

In CoreXL, the Firewall kernel is replicated multiple times. Each replicated copy or instance can perform the following:

A. The Firewall kernel only touches the packet if the connection is accelerated

B. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out

C. The Firewall can run the same policy on all cores

D. The Firewall can run different policies per core

Correct Answer: C

CoreXL is a performance-enhancing technology that enables the Security Gateway to utilize multiple CPU cores for processing traffic. CoreXL creates multiple instances of the Firewall kernel, each running on a separate CPU core. Each Firewall instance can handle traffic concurrently and independently, applying the same security policy to the packets that are assigned to it. CoreXL does not allow different policies per core, as this would create inconsistency and complexity in the security enforcement. The references are: Best Practices - Security Gateway Performance Check Point Certified Security Expert R81.20 (CCSE) Core Training, slide 16 Check Point R81 Quantum Security Gateway Guide, page 42

QUESTION 5

What is the correct order of the default "fw monitor" inspection points?

A. i, o, I, O

B. i, I, o, O

C. 1, 2, 3, 4

D. I, i, O, o

Correct Answer: B

https://community.checkpoint.com/t5/General-Topics/Check-Point-Inspection-points- iIoO/td-p/34938

The default order of the "fw monitor" inspection points is:

i (input): this is the first inspection point, where packets enter the firewall. I (local): this is the second inspection point, where packets are processed locally by the firewall, before being forwarded to the next hop. o (output): this is the third

inspection point, where packets are sent out to their final destination.

O (offload): this is the fourth inspection point, where packets are offloaded to hardware acceleration for faster processing.