156-315.81 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.pass4itsure.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

What is the limitation of employing Sticky Decision Function?

A. With SDF enabled, the involved VPN Gateways only supports IKEv1

B. Acceleration technologies, such as SecureXL and CoreXL are disabled when activating SDF

C. With SDF enabled, only ClusterXL in legacy mode is supported

D. With SDF enabled, you can only have three Sync interfaces at most

Correct Answer: B

Sticky Decision Function (SDF) is a feature that ensures that VPN traffic is handled by the same core on a Security Gateway with multiple CPU cores. This improves the performance and stability of VPN tunnels by avoiding out-of-order packets and reducing encryption overhead. However, the limitation of employing SDF is that acceleration technologies, such as SecureXL and CoreXL are disabled when activating SDF. This means that SDF may reduce the overall throughput and scalability of the Security Gateway. Therefore, SDF should be used only when necessary and only on gateways that are dedicated to VPN traffic. References: R81 Performance Tuning Administration Guide

QUESTION 2

In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

A. Publish changes

B. Save changes

C. Install policy

D. Install database

Correct Answer: C

In order for changes made to policy to be enforced by a Security Gateway, an administrator must perform the action of installing policy. Installing policy is the process of transferring the policy package from the Security Management Server to the Security Gateway. Publishing changes is the process of saving changes to the database and making them available to other administrators. Saving changes is the process of saving changes to a session without publishing them2. References: Check Point R81 Security Management Guide

QUESTION 3

Return oriented programming (ROP) exploits are detected by which security blade?

A. Data Loss Prevention

B. Check Point Anti-Virus / Threat Emulation

C. Application control

D. Intrusion Prevention Software

Correct Answer: B

Return-oriented programming (ROP) exploits are detected by Check Point Anti-Virus / Threat Emulation blade. ROP exploits are a type of code reuse attack that bypasses common exploit mitigation techniques such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). Check Point Anti-Virus / Threat Emulation blade can detect and prevent ROP exploits using its behavioral analysis engine that monitors the execution flow of processes and identifies malicious patterns. References: [Check Point Security Expert R81 Threat Prevention Administration Guide], page 17.

QUESTION 4

What is false regarding prerequisites for the Central Deployment usage?

A. The administrator must have write permission on SmartUpdate

B. Security Gateway must have the latest CPUSE Deployment Agent

C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.

D. The Security Gateway must have a policy installed

Correct Answer: C

Establishing SIC between gateways and the management server is a prerequisite for Central Deployment usage, as the CDT tool will not take care of this automatically1. The administrator must have write permission on SmartUpdate, the Security Gateway must have the latest CPUSE Deployment Agent, and the Security Gateway must have a policy installed2. These are the basic requirements for using the Central Deployment Tool (CDT), which is a utility that lets you manage a deployment of software packages from your Management Server to the multiple managed Security gateways and cluster members at the same time2. The CDT can perform various actions, such as installation of software packages, taking snapshots, running shell scripts, pushing/pulling files, and automating the RMA backup and restore process2. The CDT is supported on Check Point Appliances with R80.40 and higher versions2. References: How to keep your Security Gateways up to date - Check Point Software, Central Deployment Tool (CDT) - Check Point CheckMates.

QUESTION 5

During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

A. Dropped without sending a negative acknowledgment

B. Dropped without logs and without sending a negative acknowledgment

C. Dropped with negative acknowledgment

D. Dropped with logs and without sending a negative acknowledgment

Correct Answer: D

For packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are dropped with

logs and without sending a negative acknowledgment. Firewall Kernel Inspection is the process of applying security policies and rules to network traffic by the Firewall kernel module. If a packet does not match any rule or matches a rule with an action of Drop or Reject, the packet is dropped by the Firewall kernel module. The difference between Drop and Reject is that Drop silently discards the packet without informing the sender, while Reject discards the packet and sends a negative acknowledgment (such as an ICMP message) to the sender. However, both Drop and Reject actions generate logs that record the details of the dropped packets, such as source, destination, protocol, port, rule number, etc. The other options are either incorrect or describe different scenarios.