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

Check Point Certified Security Expert R81

QUESTION 1

In the Firewall chain mode FFF refers to:

A. Stateful Packets

B. No Match

C. All Packets

D. Stateless Packets

Correct Answer: C

In the Firewall chain mode FFF refers to all packets. Firewall chain mode is a feature that allows administrators to define how packets are processed by different firewall kernel modules in inbound and outbound directions. FFF is one of the predefined chain modes that applies all firewall kernel modules (Firewall, VPN, IPS, etc.) to all packets, regardless of their state or connection. This mode provides maximum security, but also consumes more CPU resources.

QUESTION 2

What are the Threat Prevention software components available on the Check Point Security Gateway?

A. IPS, Threat Emulation and Threat Extraction

B. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction

C. IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction

D. IDS, Forensics, Anti-Virus, Sandboxing

Correct Answer: C

The Threat Prevention software components available on the Check Point Security Gateway are IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction. These components provide comprehensive protection against various types of cyber threats, such as network attacks, malware, ransomware, phishing, zero-day exploits, data leakage, and more. IPS is a network security component that detects and prevents malicious traffic based on signatures, behavioral patterns, and anomaly detection. Anti-Bot is a network security component that detects and blocks botnet communications and command-and- control servers. Anti-Virus is a network security component that scans files for known viruses, worms, and trojans. Threat Emulation is a network security component that emulates files in a sandbox environment to detect unknown malware and prevent zero-day attacks. Threat Extraction is a network security component that removes malicious content from files and delivers clean files to users. References: [Check Point R81 Threat Prevention Administration Guide], page 9-10

QUESTION 3

Hit Count is a feature to track the number of connections that each rule matches, which one is not benefit of Hit Count.

A. Better understand the behavior of the Access Control Policy

B. Improve Firewall performance - You can move a rule that has hot count to a higher position in the Rule Base

C. Automatically rearrange Access Control Policy based on Hit Count Analysis

D. Analyze a Rule Base - You can delete rules that have no matching connections

Correct Answer: C

Hit Count is a feature to track the number of connections that each rule matches, which can help to optimize the Rule Base efficiency and analyze the network traffic behavior. The benefit that is not provided by Hit Count is automatically rearrange Access Control Policy based on Hit Count Analysis. Hit Count does not change the order of the rules automatically, but it allows the administrator to manually move the rules up or down based on the hit count statistics. The administrator can also use the SmartOptimize feature to get suggestions for improving the Rule Base order and performance. References: R81 Security Management Administration Guide, page 97.

QUESTION 4

Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

A. logd

B. fwd

C. fwm

D. cpd

Correct Answer: B

The fwd process within the Security Management Server is responsible for the receiving of log records from Security Gateway. The fwd process handles the communication with the Security Gateways and log servers via TCP port 2571. The other processes have different roles, such as logd for writing logs to the database, fwm for handling GUI clients, and cpd for infrastructure tasks2. References: Check Point Ports Used for Communication by Various Check Point Modules, Check Point Processes Cheat Sheet ?LazyAdmins

QUESTION 5

SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:

A. 19090,22

B. 19190,22

C. 18190,80

D. 19009,443

Correct Answer: D

To use SmartConsole R81 for managing SmartEvent R81, you need to have the following ports open:

Port 19009 for communication over HTTPS (443)

Port 19009 for communication over HTTP (80)

These ports are necessary for the SmartConsole to communicate with SmartEvent for management and monitoring purposes.

References: Check Point Certified Security Expert R81 documentation and learning resources.