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

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

SecureXL templates are a mechanism to accelerate the rate of connection establishment by grouping connections that match a particular service and whose sole differentiating element is the source port. SecureXL templates enable even the very first packets of a TCP handshake to be accelerated, without waiting for the Firewall kernel to create a connection entry. 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. The template will contain all the relevant information for the connection, such as source and destination IP addresses, destination port, NAT information, policy decision, etc. The template will be used by SecureXL to handle subsequent connections on the same service, without involving the Firewall kernel. This reduces the CPU load and increases the throughput. There are three types of SecureXL templates: Accept, Drop, and NAT. Accept templates are used for connections that are allowed by the Firewall policy. Drop templates are used for connections that are blocked by the Firewall policy. NAT templates are used for connections that require NAT translation. Deny templates are not a valid type of SecureXL template. References: SecureXL NAT Templates in R80.20 and lower, Part 3 - SecureXL, Security Gateway Performance Optimization - Part 5 - SecureXL

QUESTION 2

What is the default shell of Gaia CLI?

A. Monitor

B. CLI.sh

C. Read-only

D. Bash

Correct Answer: A

The default shell of Gaia CLI is clish. Clish stands for Command Line Interface Shell and it is a restrictive shell that controls the number of commands available in the CLI. Clish provides a user-friendly interface that supports command completion, history, and help functions. Clish also supports role-based administration, which means that different users can have different levels of access to Gaia features and commands based on their roles.

QUESTION 3

What two ordered layers make up the Access Control Policy Layer?

A. URL Filtering and Network

B. Network and Threat Prevention

C. Application Control and URL Filtering

D. Network and Application Control

Correct Answer: D

What two ordered layers make up the Access Control Policy Layer? Network and Application Control are the two ordered layers that make up the Access Control Policy Layer. The Network layer controls network access based on source, destination, service, time, etc. The Application Control layer controls application access based on users, groups, applications, content categories, etc. The Network layer is always processed before the Application Control layer. References: R81 Security Management Administration Guide, page 29.

QUESTION 4

Which of the following is NOT an alert option?

A. SNMP

B. High alert

C. Mail

D. User defined alert

Correct Answer: B

High alert is not an alert option in Check Point. Alert options are ways to notify the administrator or other parties when a security event occurs. The available alert options are SNMP, Mail, User defined alert, Log, Popup alert, and User alert. References: Training and Certification | Check Point Software, Check Point Resource Library

QUESTION 5

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

A. Threat Emulation

B. Mobile Access

C. Mail Transfer Agent

D. Threat Cloud

Correct Answer: B

Mobile Access is not part of the SandBlast component. Mobile Access is a software blade that provides secure remote access to corporate resources from various devices, such as smartphones, tablets, and laptops. Mobile Access

supports different connectivity methods, such as SSL VPN, IPsec VPN, and Mobile Enterprise Application Store (MEAS). Mobile Access also integrates with Mobile Threat Prevention (MTP) to protect mobile devices from malware and network attacks. References: Check Point Security Expert R81 Course, Mobile Access Administration Guide, SandBlast Mobile Datasheet