156-215.81^{Q&As}

Check Point Certified Security Administrator R81

Pass CheckPoint 156-215.81 Exam with 100% Guarantee

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

https://www.pass4itsure.com/156-215-81.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

A. SmartManager

B. SmartConsole

C. Security Gateway

D. Security Management Server

Correct Answer: D

The Security Management Server is the component that changes most often and should be backed up most frequently, because it stores all the security policies and configurations for the Check Point components in your network. The other components are either clients or gateways that do not change as frequently. References: Check Point Security Management Administration Guide R81, p. 9

QUESTION 2

True or False: The destination server for Security Gateway logs depends on a Security Management Server configuration.

A. False, log servers are configured on the Log Server General Properties

B. True, all Security Gateways will only forward logs with a SmartCenter Server configuration

C. True, all Security Gateways forward logs automatically to the Security Management Server

D. False, log servers are enabled on the Security Gateway General Properties

Correct Answer: B

The destination server for Security Gateway logs depends on a Security Management Server configuration. This is true because the Security Management Server defines the log servers that receive logs from the Security Gateways. The log servers can be either the Security Management Server itself or a dedicated Log Server.

References: Check Point R81 Logging and Monitoring Administration Guide, Check Point R81 Quantum Security Gateway Guide

QUESTION 3

Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	⌘ NBT	⬤ Drop	- None	* Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh	⬤ Accept	🗎 Log	* Policy Targets
3	Stealth	* Any	GW-R7730	* Any	* Any	⬤ Drop	🗎 Log	* Policy Targets
4 🔒	DNS	Net_10.28.0.0	* Any	* Any	* Any	⬤ Accept	🗎 Log	* Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http https	⬤ Accept	🗎 Log	* Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	⬤ Accept	🗎 Log	* Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	⬤ Drop	🗎 Log	* Policy Targets

What is the possible explanation for this?

A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.

B. Another administrator is logged into the Management and currently editing the DNS Rule.

C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.

D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Correct Answer: B

The padlock sign next to the DNS rule in the Rule Base indicates that another administrator is logged into the Management and currently editing the DNS Rule. This is a feature of R80 that allows multiple administrators to work on the same policy simultaneously. The padlock sign prevents other administrators from modifying the same rule until the editing administrator publishes or discards the changes. The other options are not valid explanations for the padlock sign. References: 156-215.80:Check Point Certified Security Administrator (CCSA R80) : Part 19, Multi-User Policy Editing

QUESTION 4

An administrator wishes to use Application objects in a rule in their policy but there are no Application objects listed as options to add when clicking the"+" to add new items to the "Services and Applications" column of a rule. What should be done to fix this?

A. The administrator should drag-and-drop the needed Application objects from the Object Explorer into the new rule

B. The "Application Control" blade should be enabled on a gateway

C. "Applications and URL Filtering" should first be enabled on the policy layer where the rule is being created.

D. The administrator should first create some applications to add to the rule.

Correct Answer: C

To use Application objects in a rule, the "Applications and URL Filtering" blade should be enabled on the policy layer where the rule is being created. Enabling the "Application Control" blade on a gateway is not enough. References: Check Point R81 Security Management Administration Guide, page 102.

QUESTION 5

Gaia has two default user accounts that cannot be deleted. What are those user accounts?

A. Admin and Default

B. Expert and Clish

C. Control and Monitor

D. Admin and Monitor

Correct Answer: D

Gaia has two default user accounts that cannot be deleted. They are Admin and Monitor. Admin is the user account that has full administrative privileges and can access both WebUI and CLI. Monitor is the user account that has read-only privileges and can access only WebUI2. The other options are not default user accounts in Gaia.