Latest Version: 6.0

Question: 1

Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

A. The firewall topologies
B. NAT Rules
C. The Rule Base
D. The VPN Domains

Answer: D

Explanation:
The VPN Domains configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear. The VPN Domain is the set of hosts and networks that are allowed to communicate securely with the gateway12. The firewall topologies, NAT rules, and the rule base do not directly affect the VPN encryption decision. Check Point R82 Security Gateway Technical Administration Guide, CCSA/CCSE Exam Tips & Content - R80.X vs. R82.X - Check Point CheckMates

Question: 2

You have discovered suspicious activity in your network. What is the BEST immediate action to take?

A. Create a policy rule to block the traffic.
B. Create a suspicious action rule to block that traffic.
C. Wait until traffic has been identified before making any changes.
D. Contact ISP to block the traffic.

Answer: B

Explanation:
The BEST immediate action to take when you have discovered suspicious activity in your network is to create a suspicious action rule to block that traffic. A suspicious action rule is a special type of rule that is triggered when a predefined condition is met, such as a malicious file download, a ransomware attack, or a data exfiltration attempt13. A suspicious action rule can block the traffic, quarantine the source, or send an alert to the administrator. Creating a policy rule to block the traffic may not be effective if the traffic does not match the rule criteria or if the policy installation is delayed. Waiting until traffic has been identified before making any

changes may allow the threat to spread or cause more damage. Contacting ISP to block the traffic may not be feasible or timely, and may also affect legitimate traffic. Check Point R82 Security Gateway Technical Administration Guide, Check Point CCSA - R82: Practice Test & Explanation | Udemy

Question: 3

Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made?

A. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.
B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
C. Tom's changes will be lost since he lost connectivity and he will have to start again.
D. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

Answer: D

Explanation:
Tom’s changes will have been stored on the Management when he reconnects and he will not lose any of his work. This is because SmartConsole uses a session mechanism that allows users to work offline and save their changes locally until they are ready to publish them to the Management13. If Tom loses connectivity, he can resume his session when he reconnects and continue working on his Rule Base changes. He does not need to reboot his SmartConsole computer, clear the cache, or restore changes. His changes will not be lost since he lost connectivity. Check Point R82 Security Management Administration Guide, Check Point CCSA - R82: Practice Test & Explanation | Udemy

Question: 4

Which GUI tool can be used to view and apply Check Point licenses?

A. cpconfig
B. Management Command Line
C. SmartConsole
D. SmartUpdate

Answer: D

Explanation:

The GUI tool that can be used to view and apply Check Point licenses is SmartUpdate. SmartUpdate is a centralized tool that allows you to manage licenses, software packages, and hotfixes for multiple gateways and clusters12. cpconfig, Management Command Line, and SmartConsole are not tools for license management. Check Point R82 SmartUpdate Administration Guide, Check Point CCSA - R82: Practice Test & Explanation | Udemy

Question: 5

How would you determine the software version from the CLI?

A. fw ver
B. fw stat
C. fw monitor
D. cpinfo

Answer: A

Explanation:
The command that can be used to determine the software version from the CLI is fw ver. This command displays the version of the firewall module and the build number3 . fw stat, fw monitor, and cpinfo are not commands for software version identification. Check Point R82 Command Line Interface Reference Guide, [156-315.81 Checkpoint Exam Info and Free Practice Test - ExamTopics]

Question: 6

In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

A. 3rd Party integration of CLI and API for Gateways prior to R80.
B. A complete CLI and API interface using SSH and custom CPCode integration.
C. 3rd Party integration of CLI and API for Management prior to R80.
D. A complete CLI and API interface for Management with 3rd Party integration.

Answer: B

Explanation:
In R80 Management, apart from using SmartConsole, objects or rules can also be modified using a complete CLI and API interface using SSH and custom CPCode integration. This allows you to automate tasks, integrate with third-party tools, and create custom scripts . 3rd Party integration of CLI and API for Gateways or Management prior to R80 is not relevant for R80 Management. A complete CLI and API interface for Management with 3rd Party integration is

not a specific option. [Check Point R82 Security Management Administration Guide], [Check Point Learning and Training Frequently Asked Questions (FAQs)]

Question: 7

When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

A. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
B. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
C. The entire Management Database and all sessions and other administrators can connect only as Read-only.
D. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.

Answer: D

Explanation:
The answer is D because in R80 and above, the first administrator to connect to the Management Server using SmartConsole gets a lock on only the objects being modified in his session of the Management Database. Other administrators can connect to make changes using different sessions, but they cannot modify the same objects as the first administrator until he publishes his changes. This is called concurrent administration and it allows multiple administrators to work on the same policy package simultaneously12 Check Point R80.10 Concurrent Administration, Check Point R80.40 Security Management Administration Guide

Question: 8

Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

A. AES-GCM-256
B. AES-CBC-256
C. AES-GCM-128

Answer: B

Explanation:

The answer is B because AES-CBC-256 is not a supported encryption algorithm for IPsec Security Associations (Phase 2) in R82. The supported encryption algorithms are AES-GCM-128, AES-GCM-256, AES-CBC-128, 3DES, and NULL3 Check Point R82 VPN Administration Guide

Question: 9

Fill in the blank: To create policy for traffic to or from a particular location, use the _____.

A. DLP shared policy
B. Geo policy shared policy
C. Mobile Access software blade
D. HTTPS inspection

Answer: B

Explanation:
The answer is B because Geo policy shared policy is used to create policy for traffic to or from a particular location based on the source or destination country. DLP shared policy is used to prevent data loss by inspecting files and data for sensitive information. Mobile Access software blade is used to provide secure remote access to corporate resources from various devices. HTTPS inspection is used to inspect encrypted web traffic for threats and compliance4

Check Point R82 Geo Policy Administration Guide, [Check Point R82 Data Loss Prevention Administration Guide], [Check Point R82 Mobile Access Administration Guide], [Check Point R82 HTTPS Inspection Administration Guide]

Question: 10

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust
B. The Security Gateway name cannot be changed in command line without re-establishing trust
C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Answer: A

Explanation:

The answer is A because changing the Security Gateway IP-address requires re-establishing the trust with the Security Management Server by initializing the Secure Internal Communication (SIC). Changing the Security Gateway name in command line or changing the Security Management Server name or IP-address in SmartConsole does not require re-establishing the trust, but it may require updating the topology and pushing the policy.

[Check Point R82 Security Management Administration Guide], [Check Point R82 Security Gateway Administration Guide]