



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.geekcert.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

Which software blade does NOT accompany the Threat Prevention policy?

- A. IPS
- B. Application Control and URL Filtering
- C. Threat Emulation
- D. Anti-virus

Correct Answer: B

The Threat Prevention policy is a unified policy that manages three software blades: IPS, Anti-Virus, and Threat Emulation. The Threat Prevention policy enables you to configure settings and actions for detecting and preventing various types of threats, such as malware, exploits, botnets, etc. Application Control and URL Filtering are not part of the Threat Prevention policy, but they are part of a separate policy that controls access to applications and websites based on categories, users, groups, and machines

QUESTION 2

When a Security Gateway sends its logs to an IP address other than its own, which deployment option is installed?

- A. Distributed
- B. Standalone
- C. Bridge Mode
- D. Targeted

Correct Answer: A

When a Security Gateway sends its logs to an IP address other than its own, it means that the deployment option is distributed. In a distributed deployment, the Security Management Server and the Security Gateway are installed on separate machines. The Security Management Server collects logs from one or more Security Gateways and manages them centrally. In a standalone deployment, the Security Management Server and the Security Gateway are installed on the same machine. The Security Gateway sends logs to its own IP address. In a bridge mode deployment, the Security Gateway acts as a transparent bridge between two network segments and does not have an IP address of its own. In a targeted deployment, the Security Gateway sends logs to a specific log server that is configured in the gateway object properties³⁴ References: Part 4 - Installing Security Gateway, Deployment Options

QUESTION 3

An administrator can use section titles to more easily navigate between large rule bases.

Which of these statements is FALSE?

- A. Section titles are not sent to the gateway side.



- B. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement.
- C. A Sectional Title can be used to disable multiple rules by disabling only the sectional title.
- D. Sectional Titles do not need to be created in the SmartConsole.

Correct Answer: C

The statement that a Sectional Title can be used to disable multiple rules by disabling only the sectional title is false. A Sectional Title is a visual divider that helps organize and navigate large rule bases. It does not affect the rule enforcement order or the rule functionality. Disabling a Sectional Title does not disable the rules under it. To disable multiple rules, you need to select them individually or use Shift+Click or Ctrl+Click to select them in bulk, and then right-click and choose Disable Rule(s). The other statements are true. Section titles are not sent to the gateway side, they are only displayed in SmartConsole. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement. Sectional Titles do not need to be created in SmartConsole, they can also be created using SmartConsole CLI or API commands. References: [Sectional Titles], [SmartConsole CLI Guide], [SmartConsole API Reference Guide]

QUESTION 4

What protocol is specifically used for clustered environments?

- A. Clustered Protocol
- B. Synchronized Cluster Protocol
- C. Control Cluster Protocol
- D. Cluster Control Protocol

Correct Answer: D

The protocol that is specifically used for clustered environments is Cluster Control Protocol (CCP). CCP is a proprietary Check Point protocol that is used for communication between cluster members and for cluster administration. CCP enables cluster members to exchange state information, synchronize connections, monitor interfaces, and perform failover operations. The other options are incorrect. Clustered Protocol, Synchronized Cluster Protocol, and Control Cluster Protocol are not valid terms in Check Point terminology. References: [Cluster Control Protocol (CCP) - Check Point Software]

QUESTION 5

Fill in the blank RADIUS Accounting gets _____ data from requests generated by the accounting client

- A. Location
- B. Payload
- C. Destination
- D. Identity

Correct Answer: D



RADIUS Accounting gets identity data from requests generated by the accounting client. RADIUS Accounting is a feature that allows tracking and measuring resource usage of network services by users. The accounting client, which is usually a network access server (NAS), sends accounting requests to a RADIUS server with information about user sessions, such as start and stop times, bytes transmitted and received, IP addresses, etc. The RADIUS server records this information in a database for billing, auditing, or reporting purposes. One of the mandatory attributes that the accounting client must include in every accounting request is the User-Name attribute, which identifies the user who is accessing the network service.

[Latest 156-215.81 Dumps](#)[156-215.81 VCE Dumps](#)[156-215.81 Study Guide](#)