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

What is NOT an advantage of Packet Filtering?

A. Low Security and No Screening above Network Layer

B. Application Independence

C. High Performance

D. Scalability

Correct Answer: A

Packet Filter Advantages and Disadvantages

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

Reference: https://www.checkpoint.com/smb/help/utm1/8.2/7078.htm

QUESTION 2

You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

A. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0.fws configuration file.

B. Select Block intruder from the Tools menu in SmartView Tracker.

C. Create a Suspicious Activity Rule in Smart Monitor.

D. Add a temporary rule using SmartDashboard and select hide rule.

Correct Answer: C

QUESTION 3

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

A. UserCheck

B. Active Directory Query

C. Account Unit Query

D. User Directory Query

Correct Answer: B

:

AD Query extracts user and computer identity information from the Active Directory Security Event Logs.

The system generates a Security Event log entry when a user or computer accesses a network resource.

For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.

Reference : https://sc1.checkpoint.com/documents/R76/

CP_R76_IdentityAwareness_AdminGuide/62402.htm

QUESTION 4

The SIC Status "Unknown" means

A. There is connection between the gateway and Security Management Server but it is not trusted.

B. The secure communication is established.

C. There is no connection between the gateway and Security Management Server.

D. The Security Management Server can contact the gateway, but cannot establish SIC.

Correct Answer: C

SIC Status

After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security

Management Server can communicate securely with this gateway:

Communicating - The secure communication is established.

Unknown - There is no connection between the gateway and Security Management Server.

Not Communicating - The Security Management Server can contact the gateway, but cannot establish

SIC. A message shows more information. Reference: https://sc1.checkpoint.com/documents/R80/

CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/125443

QUESTION 5

Which of the following statements is TRUE about R80 management plug-ins?

A. The plug-in is a package installed on the Security Gateway.

B. Installing a management plug-in requires a Snapshot, just like any upgrade process.

C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.

D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Correct Answer: C