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.passapply.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

QUESTION 1

Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

A. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop

B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop

C. 192.168.1.1 AND 172.26.1.1 AND drop

D. 192.168.1.1 OR 172.26.1.1 AND action:Drop

Correct Answer: B

src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop is the correct log query to show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1. The AND operator means that all conditions must be true for the query to match. The OR operator means that any condition can be true for the query to match. The other queries will either show packets that are not dropped or packets that have different source or destination addresses.

QUESTION 2

Which of the following statements about Site-to-Site VPN Domain-based is NOT true?

A. Route-based- The Security Gateways will have a Virtual Tunnel Interface (VTI) for each VPN Tunnel with a peer VPN Gateway. The Routing Table can have routes to forward traffic to these VTIs. Any traffic routed through a VTI is automatically identified as VPN Traffic and is passed through the VPN Tunnel associated with the VTI.

B. Domain-based-- VPN domains are pre-defined for all VPN Gateways. A VPN domain is a service or user that can send or receive VPN traffic through a VPN Gateway.

C. Domain-based-- VPN domains are pre-defined for all VPN Gateways. A VPN domain is a host or network that can send or receive VPN traffic through a VPN Gateway.

D. Domain-based-- VPN domains are pre-defined for all VPN Gateways. When the Security Gateway encounters traffic originating from one VPN Domain with the destination to a VPN Domain of another VPN Gateway, that traffic is identified as VPN traffic and is sent through the VPN Tunnel between the two Gateways.

Correct Answer: B

Domain-based-- VPN domains are pre-defined for all VPN Gateways. A VPN domain is a service or user that can send or receive VPN traffic through a VPN Gateway. This statement is not true because a VPN domain is not a service or user, but a host or network that can send or receive VPN traffic through a VPN Gateway. This is the definition given in the Site to Site VPN R81 Administration Guide. The other statements are true according to the same guide. Remote Access VPN R81.20 Administration Guide Site to Site VPN R81 Administration Guide DeepDive Webinar - R81.20 Seamless VPN Connection to Public Cloud

QUESTION 3

How many users can have read/write access in Gaia Operating System at one time?

A. One

B. Three

C. Two

D. Infinite

Correct Answer: A

Only one user can have read/write access in Gaia Operating System at one time. This is to prevent conflicts and errors when multiple users try to modify the same configuration settings. References: Check Point Gaia Administration Guide

QUESTION 4

How do you manage Gaia?

A. Through CLI and WebUI

B. Through CLI only

C. Through SmartDashboard only

D. Through CLI, WebUI, and SmartDashboard

Correct Answer: D

Gaia can be managed through CLI, WebUI, and SmartDashboard, p. 17-18. CLI is a command-line interface that allows administrators to configure and monitor Gaia using commands and scripts. WebUI is a web-based interface that allows administrators to configure and monitor Gaia using a browser. SmartDashboard is a graphical user interface that allows administrators to manage security policies and objects for Gaia devices. , [Check Point Gaia Administration Guide R81], [Check Point Security Management Administration Guide R81]

QUESTION 5

What technologies are used to deny or permit network traffic?

A. Stateful Inspection. Firewall Blade, and URL\\'Application Blade

B. Packet Filtenng. Stateful Inspection, and Application Layer Firewall

C. Firewall Blade. URL/Application Blade and IPS

D. Stateful Inspection. URL/Application Blade, and Threat Prevention

Correct Answer: A

The technologies that are used to deny or permit network traffic are Stateful Inspection, Firewall Blade, and URL/Application Blade. Stateful Inspection is a technology that inspects network traffic at the packet level and maintains the state and

context of each connection. Firewall Blade is a software blade that enforces security policy and prevents unauthorized access to protected resources. URL/Application Blade is a software blade that enables administrators to control access

to

millions of websites and applications based on users, groups, and machines.

References: Check Point R81 Security Gateway Administration Guide, page 9. : Check Point R81 Security Gateway Administration Guide, page 10. : Check Point R81 Security Gateway Administration Guide, page 12.