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

A network administrator has informed you that they have identified a malicious host on the network, and instructed you to block it. Corporate policy dictates that firewall policy changes cannot be made at this time. What tool can you use to block this traffic?

A. Anti-Bot protection

B. Anti-Malware protection

C. Policy-based routing

D. Suspicious Activity Monitoring (SAM) rules

Correct Answer: D

If a network administrator has identified a malicious host on the network and instructed you to block it, but you cannot make any firewall policy changes at this time, you can use Suspicious Activity Monitoring (SAM) rules to block this traffic. SAM rules are temporary rules that allow you to block or limit traffic from specific sources or destinations without modifying the security policy. SAM rules are created and managed by SmartView Monitor and are enforced by the security gateway for a specified duration. Anti-Bot protection, Anti-Malware protection, and Policy-based routing are not tools that can be used to block traffic without changing the firewall policy. References: [Check Point R81 SmartView Monitor Administration Guide]

QUESTION 2

Which message indicates IKE Phase 2 has completed successfully?

A. Quick Mode Complete

B. Aggressive Mode Complete

C. Main Mode Complete

D. IKE Mode Complete

Correct Answer: A

Quick Mode Complete is the message that indicates IKE Phase 2 has completed successfully2. IKE Phase 2 is also known as Quick Mode or Child SA in IKEv1 and IKEv2 respectively. Aggressive Mode and Main Mode are part of IKE Phase 1, which establishes the IKE SA. IKE Mode is not a valid term for IKE negotiation. References: How to Analyze IKE Phase 2 VPN Status Messages, IKEv2 Phase 1 (IKE SA) and Phase 2 (Child SA) Message Exchanges, Understand IPsec IKEv1 Protocol

QUESTION 3

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.

Correct Answer: B

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. References: [Check Point R81 Security Management Administration Guide], [Check Point Learning and Training Frequently Asked Questions (FAQs)]

QUESTION 4

Which statement is TRUE of anti-spoofing?

A. Anti-spoofing is not needed when IPS software blade is enabled

B. It is more secure to create anti-spoofing groups manually

C. It is BEST Practice to have anti-spoofing groups in sync with the routing table

D. With dynamic routing enabled, anti-spoofing groups are updated automatically whenever there is a routing change

Correct Answer: C

The statement that is TRUE of anti-spoofing is that it is BEST Practice to have anti- spoofing groups in sync with the routing table. Anti-spoofing prevents attackers from sending packets with a false source IP address. Anti-spoofing groups define which IP addresses are expected on each interface of the Security Gateway. If the routing table changes, the anti-spoofing groups should be updated accordingly. References: Check Point R81 ClusterXL Administration Guide, Network Defined by Routes: Anti-Spoofing

QUESTION 5

What is the most complete definition of the difference between the Install Policy button on the SmartConsole\\'s tab, and the Install Policy within a specific policy?

A. The Global one also saves and published the session before installation.

B. The Global one can install multiple selected policies at the same time.

C. The local one does not install the Anti-Malware policy along with the Network policy.

D. The second one pre-select the installation for only the current policy and for the applicable gateways.

Correct Answer: D

The difference between the Install Policy button on the SmartConsole\\'s tab and the Install Policy within a specific policy is that the former installs all the policies that are selected in the Install Policy window, while the latter pre-selects the installation for only the current policy and for the applicable gateways . The other options are not accurate differences. References: Installing Policies, []

Latest 156-215.81 Dumps 156-215.81 Practice Test 156-215.81 Braindumps