

100% Money Back
Guarantee

Vendor:CheckPoint

Exam Code:156-215.75

Exam Name:Check Point Certified Security
Administrator

Version:Demo

QUESTION 1

Can you upgrade a clustered deployment with zero downtime?

- A. No, this is not possible.
- B. Yes, if you select the option zero downtime, it will keep one member active
- C. No, you must bring all gateways down.
- D. Yes, this is the default setting.

Correct Answer: B

QUESTION 2

Which of these security policy changes optimize Security Gateway performance?

- A. Use Automatic NAT rules instead of Manual NAT rules whenever possible
- B. Putting the least-used rule at the top of the Rule Base
- C. Using groups within groups in the manual NAT Rule Base
- D. Using domain objects in rules when possible

Correct Answer: A

QUESTION 3

How is wear on the flash storage device mitigated on appliance diskless platforms?

- A. A RAM drive reduces the swap file thrashing which causes fast wear on the device.
- B. The external PCMCIA-based flash extension has the swap file mapped to it, allowing easy replacement.
- C. Issue FW-1 bases its package structure on the Security Management Server, dynamically loading when the firewall is booted.
- D. PRAM flash devices are used, eliminating the longevity.

Correct Answer: A

QUESTION 4

NAT can NOT be configured on which of the following objects?

- A. Address Range

B. HTTP Logical Server

C. Host

D. Gateway

Correct Answer: B

QUESTION 5

If you check the box Use Aggressive Mode in the IKE Properties dialog box, the standard:

A. three-packet IKE Phase 2 exchange is replaced by a six-packet exchange

B. three-packet IKE Phase 2 exchange is replaced by a two-packet exchange

C. six-packet IKE Phase 1 exchange is replaced by a three-packet exchange

D. three-packet IKE Phase 1 exchange is replaced by a six-packet exchange

Correct Answer: C

QUESTION 6

Your Security Gateways are running near performance capacity and will get upgraded hardware next week. Which of the following would be MOST effective for quickly dropping all connections from a specific attacker's IP at a peak time of day?

A. SAM - Block Intruder feature of SmartView Tracker

B. Intrusion Detection System (IDS) Policy install

C. SAM - Suspicious Activity Rules feature of SmartView Monitor

D. Change the Rule Base and install the Policy to all Security Gateways

Correct Answer: C

QUESTION 7

Which of the following statements accurately describes the snapshot command?

A. snapshot creates a full OS-level backup, including network-interface data, Check Point product information, and configuration settings during an upgrade of a SecurePlatform Security Gateway.

B. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server.

C. snapshot creates a full system-level backup of the Security Management Server on any OS

D. snapshot stores only the system-configuration settings on the Gateway.

Correct Answer: A

QUESTION 8

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. SecureClient
- B. Security Gateway
- C. SmartConsole
- D. None, Security Management Server would be installed by itself

Correct Answer: B

QUESTION 9

For which service is it NOT possible to configure user authentication?

- A. HTTPS
- B. FTP
- C. SSH
- D. Telnet

Correct Answer: C

QUESTION 10

Your company has two headquarters, one in London, one in New York. Each of the headquarters includes several branch offices. The branch offices only need to communicate with the headquarters in their country, not with each other, and the headquarters need to communicate directly. What is the BEST configuration for establishing VPN Communities among the branch offices and their headquarters, and between the two headquarters? VPN Communities comprised of:

- A. Three mesh Communities: one for London headquarters and its branches; one for New York headquarters and its branches; and one for London and New York headquarters.
- B. Three star Communities: The first one is between New York headquarters and its branches. The second star Community is between London headquarters and its branches. The third star Community is between New York and London headquarters but it is irrelevant which site is "center" and which "satellite".
- C. Two mesh and one star Community: Each mesh Community is set up for each site between headquarters their branches. The star Community has New York as the center and London as its satellite.
- D. One star Community with the option to mesh the center of the star: New York and London Gateways added to the center of the star with the "mesh center Gateways" option checked; all London branch offices defined in one satellite window; but, all New York branch offices defined in another satellite window.

Correct Answer: B

QUESTION 11

Which type of R75 Security Server does not provide User Authentication?

- A. FTP Security Server
- B. SMTP Security Server
- C. HTTP Security Server
- D. HTTPS Security Server

Correct Answer: B

QUESTION 12

When using AD Query to authenticate users for Identity Awareness, identity data is received seamlessly from the Microsoft Active Directory (AD). What is NOT a recommended usage of this method?

- A. Leveraging identity in Internet application control
- B. Identity-based enforcement for non-AD users (non-Windows and guest users)
- C. Identity-based auditing and logging
- D. Basic identity enforcement in the internal network

Correct Answer: B