

Check Point CCSA NGX (Exam 156-215.1)

1

What is the advantage of using VPN-1/FireWall-1 Password for the authentication scheme, rather than using OS Password?

- A. The OS Password authentication scheme can only be used with services available to a user's local machine.
- B. There is no advantage, because VPN-1/FireWall-1 Password can only be used, if a user has an operating-system account on the network.
- C. The OS Password authentication scheme can only be used with users who are present on the local network protected by the Enforcement Module. No external users can be configured for OS Password authentication.
- D. VPN-1/FireWall-1 Passwords can be cached on the Enforcement Module. If a user in the user database attempts a connection, that user will not be prompted to re-enter the password.
- E. VPN-1/FireWall-1 Passwords can be used, even if a user does not have an operating-system account on the network.

2

Which statement below BEST describes how VPN-1/FireWall-1 handles hidden rules?

Hidden rules are:

- A. Not included when the Security Policy is installed.
- B. Removed from the existing Security Policy.
- C. Enforced when the Security Policy is installed.
- D. Automatically installed, when the `unhide ALL` option is selected from the Hide Rules menu.
- E. Enforced as implied rules, before the explicitly defined Rule Base.

3

Which of the following denial-of-service attacks does SmartDefense defeat? Choose three.

- A. Ping of Death
- B. Rogue Applets
- C. Teardrop
- D. Host System Hogging
- E. LAND

4

Choose two. The SmartDefense Storm Center Module agent receives the Dshield.org Block List, and:

- A. Populates CPDShield with blocked address ranges, every three hours.
- B. Generates logs from rules tracking internal traffic.
- C. Submits the number of authentication failures, and drops, rejects, and accepts.
- D. Generates regular and compact log digests.
- E. Populates the firewall daemon with log trails.

5

At ABC Company, auditors are Check Point Security Administrators with a customized permissions profile. Auditors must have the ability to review information from SmartView Tracker, SmartView Status, and SmartView Monitoring, but they may not make changes to the information. Auditors are not permitted to view Security Policies or the objects database.

Which of the following settings grants auditors the MOST appropriate set of permissions, based on the corporate environment, described above for ABC Company?

- A. Read-Only SmartView Reporter
- B. Read-Only Monitoring
- C. Read-Only Security Policy
- D. Read-Only SmartUpdate
- E. Read-Only Log Consolidator

6

Hidden (or masked) rules are used to:

- A. Hide rules from administrators with lower privileges.
- B. View only a few rules, without the distraction of others.
- C. Temporarily disable rules, without having to reinstall the Security Policy.
- D. Temporarily convert specifically defined rules to implied rules.
- E. Delete rules, without having to reinstall the Security Policy.

7

Which of the following objects are allowed in the Source components of the Rule Base? Choose two.

- A. Host-Node Objects
- B. Time Objects
- C. LDAP Account Units
- D. Services
- E. User Groups

8

What type of TCP attack is a bandwidth attack, where a client fools a server into sending large amounts of data, using small packets?

- A. SMURF
- B. SYN-Flood
- C. Host System Hogging
- D. Small PMTU
- E. LAND