

Exam : Essentials

Title : Fireware Essentials Exam

Version: DEMO

1. You configured four Device Administrator user accounts for your Firebox.

To see a report of witch Device Management users have made changes to the device configuration, what must you do? (Select two.)

A. Start Firebox System Manager for the device and review the activity for the Management Users on the Authentication List tab.

- B. Connect to Report Manager or Dimension and view the Audit Trail report for your device.
- C. Open WatchGuard Server Center and review the configuration history for managed devices.
- D. Configure your device to send audit trail log messages to your WatchGuard Log Server or Dimension Log Server.

Answer: B,C

- 2. Which takes precedence: WebBlocker category match or a WebBlocker exception?
- A. WebBlocker exception
- B. WebBlocker category match

Answer: B

- 3.From the Firebox System Manager >Authentication List tab, you can view all of the authenticated users connected to your Firebox and disconnect any of them.
- A. True
- B. False

Answer: B

4. Users on the trusted network cannot browse Internet websites.



Based on the configuration shown in this image, what could be the problem with this policy configuration? (Select one.)

- A. The default Outgoing policy has been removed and there is no policy to allow DNS traffic.
- B. The HTTP-proxy policy has higher precedence than the HTTPS-proxy policy.
- C. The HTTP-proxy policy is configured for the wrong port.
- D. The HTTP-proxy allows Any-Trusted and Any-Optional to Any-External.

Answer: C

5.HOTSPOT

Match each WatchGuard Subscription Service with its function:

Uses full-system emulation analysis to identify characteristics and behavior of zero-day malware



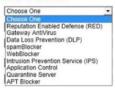
Manages use of applications on your network



A repository where email messages can be sent based on analysis by spamBlocker, Gateway AntiVirus, or Data Loss Prevention



Cloud based service that controls access to website based on a site's previous behavior



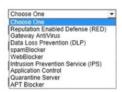
Scans files to detect malicious software infections



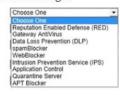
Prevents accidental or unauthorized transmission of confidential information outside your network



Uses signatures to provide real-time protection against network attacks



Uses rules, pattern matching, and sender reputation to block unwanted email messages



Controls access to website based on content categories



The safer	easier way	to help	vou pass	anv II	exams.

Uses full-system emulation analysis to identify characteristics and behavior of zero-day malware



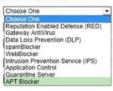
Manages use of applications on your network



A repository where email messages can be sent based on analysis by spamBlocker, Gateway AntiVirus, or Data Loss Prevention



Cloud based service that controls access to website based on a site's previous behavior



Scans files to detect malicious software infections



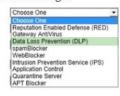
Prevents accidental or unauthorized transmission of confidential information outside your network



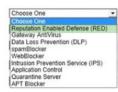
Uses signatures to provide real-time protection against network attacks



Uses rules, pattern matching, and sender reputation to block unwanted email messages



Controls access to website based on content categories



Explanation:

WebBlocker

Spam Blocker

Gateway / Antivirus

APT Blocker

Application Control

Quarantee Server

Intrusion Prevention Server IPS

Data Loss Prvention DLP

Reputation Enable Defense RED