

TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!



Exam : Essentials

Title : Firewall 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.

Order /	Action	Policy Name	Policy Type	From	To	Port
1	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21
2	✓	HTTP-proxy	HTTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:80
3	✓	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-Optional	Any-External	tcp:443
4	✓	WatchGuard Authent...	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
5	✓	WatchGuard Web UI	WG-Fireware-X...	Any-Trusted, Any-Optional	Firebox	tcp:8080
6	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	ICMP (type: 8, code: 255)
7	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:41...

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Manages use of applications on your network

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Scans files to detect malicious software infections

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Prevents accidental or unauthorized transmission of confidential information outside your network

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Uses signatures to provide real-time protection against network attacks

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Controls access to website based on content categories

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Answer:

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Manages use of applications on your network

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Scans files to detect malicious software infections

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Prevents accidental or unauthorized transmission of confidential information outside your network

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Uses signatures to provide real-time protection against network attacks

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

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

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Controls access to website based on content categories

Choose One

- Choose One
- Reputation Enabled Defense (RED)
- Gateway AntiVirus
- Data Loss Prevention (DLP)
- spamBlocker
- WebBlocker
- Intrusion Prevention Service (IPS)
- Application Control
- Quarantine Server
- APT Blocker

Explanation:

WebBlocker

Spam Blocker

Gateway / Antivirus

APT Blocker

Application Control

Quarantee Server

Intrusion Prevention Server IPS

Data Loss Prvention DLP

Reputation Enable Defense RED