



ESSENTIALS^{Q&As}

Fireware Essentials Exam

Pass WatchGuard ESSENTIALS Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/essentials.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by
WatchGuard Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Authentication Methods Available with Fireware

Fireware supports these authentication servers:

- Firebox-DB
- Active Directory
- LDAP (Lightweight Directory Access Protocol)
- RADIUS
- SecureID
- VASCO

When your users connect to the Authentication Portal page to authenticate, they see a security warning message in their browsers, which they must accept before they can authenticate. How can you make sure they do not see this security warning message in their browsers? (Select one.)

- A. Import a custom self-signed certificate or a third-party certificate to your Firebox and import the same certificate to all client computers or web browsers.
- B. Replace the Firebox certificate with the trusted certificate from your web server.
- C. Add the user accounts for your users who use the Authentication Portal to a list of trusted users on your Firebox.
- D. Instruct them to disable security warning message in their preferred browsers.

Correct Answer: A

QUESTION 2

Which WatchGuard tools can you use to review the log messages generated by your Firebox? (Select three).

- A. Firebox System Manager > Traffic Monitor
- B. Fireware XTM Web UI > Traffic Monitor
- C. Firebox System Manager > Status Report
- D. Dimension > Log manager
- E. WatchGuard System Manager > Policy Manager

Correct Answer: ABD

A: You can use Firebox System Manager (FSM) to see log messages from your XTM device as they occur.

1.



Start Firebox System Manager.

2.

Select the Traffic Monitor tab.

Reference: http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#cshid=en-US/fsm/

[log_msgs_traffic_mon_wsm.html](#)

D: You can use Firebox System Manager to see log messages in real-time on the Traffic Monitor tab. You can also examine log messages with Log Manager or WatchGuard Dimension.

B: After you connect to WatchGuard WebCenter, you can review the log messages sent from your XTM devices to your WatchGuard Log Server. Log Manager enables you to see log messages from your device for any period of time you specify, if log messages were generated in the selected time frame. To see log messages for an XTM device as they are generated, in real-time, you can use Firebox System Manager Traffic Monitor.

Reference: http://www.watchguard.com/help/docs/wsm/XTM_11/en-US/index.html#en-US/logging/

[log_mgr_view_device_wsm.html](#)

Incorrect:

Not C: The Status Report tab shows statistics about Firebox or XTM device traffic and performance. It does not display log messages.

To see the Status Report:

1.

Start Firebox System Manager.

2.

Select the Status Report tab.




Firebox System Manager - 203.0.113.10 [Connected]

File View Tools Help

Authentication List | Blocked Sites | Subscription Services | Gateway Wireless Controller | Traffic Management
Front Panel | Traffic Monitor | Bandwidth Meter | Service Watch | Status Report

Status report for 'WatchGuard-XTM' from Thu Apr 3 13:22:52 2014

Version : 11.9.B445145
sysb :
Serial #: 
Model : XTM1050
CPU cores: 8

Current local time: Thu Apr 3 13:22:52 2014
Current UTC time : Thu Apr 3 13:22:52 2014
Uptime : 6d 22h 39m 45s

Firebox Modular Components

Module	Version	Build Number
xtables6	11.9	445145
xtables-addons	11.9	445145
wgversion	11.9	445145
wgsync	11.9	445145
wgplatform	11.9	445145
wgcore	11.9	445145
wgbase	11.9	445145
webui	11.9	445145

Refresh Interval: 30 seconds | Pause | Support...

QUESTION 3

Which of these options are private IPv4 addresses you can assign to a trusted interface, as described in RFC 1918, Address Allocation for Private Internets? (Select three.)

- A. 192.168.50.1/24
- B. 10.50.1.1/16
- C. 198.51.100.1/24
- D. 172.16.0.1/16
- E. 192.0.2.1/24

Correct Answer: ABD



QUESTION 4

For which of these third party authentication methods must you specify a search base? (Select two.)

- A. RADIUS
- B. Active Directory
- C. SecurID
- D. LDAP

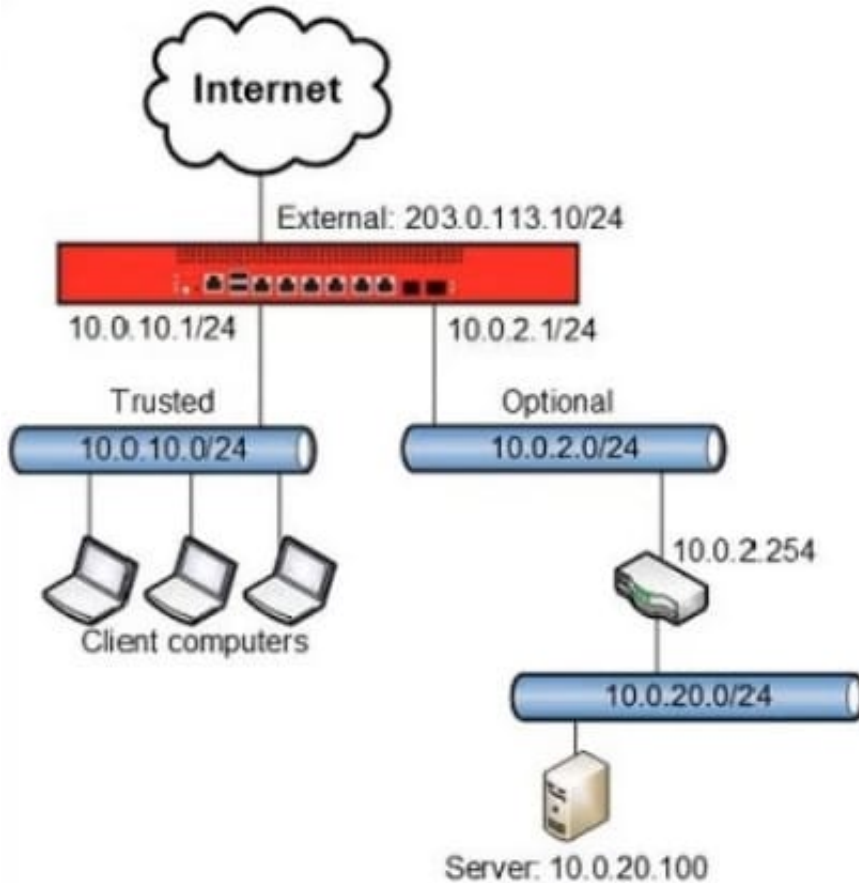
Correct Answer: BD

B: Configuring the Firebox to use Active Directory authentication is similar to the process for LDAP authentication. You must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match.

D: When you configure the Firebox to use LDAP authentication, you must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 83-84

QUESTION 5

Clients on the trusted network need to connect to a server behind a router on the optional network. Based on this image, what static route must be added to the Firebox for traffic from clients on the trusted network to reach a server at 10.0.20.100? (Select one.)



- A. Route to 10.0.20.0/24, Gateway 10.0.2.1
- B. Route to 10.0.20.0/24, Gateway 10.0.2.254
- C. Route to 10.0.20.0, Gateway 10.0.2.254
- D. Route to 10.0.10.0/24, Gateway 10.0.10.1

Correct Answer: B

We must add a trusted static route to the 10.0.20.0/24 network through the 10.0.2.254 gateway.

[Latest ESSENTIALS Dumps](#) [ESSENTIALS PDF Dumps](#) [ESSENTIALS Braindumps](#)