

# ESSENTIALS<sup>Q&As</sup>

Fireware Essentials Exam

## Pass WatchGuard ESSENTIALS Exam with 100% Guarantee

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

<https://www.pass2lead.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**

You can configure the SMTP-proxy policy to restrict email messages and email content based on which of these message characteristics? (Select four.)

- A. Sender Mail From address
- B. Check URLs in message with WebBlocker
- C. Email message size
- D. Attachment file name and content type
- E. Maximum email recipients

Correct Answer: ACDE

A: Another way to protect your SMTP server is to restrict incoming traffic to only messages that use your company domain. In this example, we use the mywatchguard.com domain. You can use your own company domain.

1.

From the SMTP-Incoming Categories list, select Address > Rcpt To.

2.

In the Pattern text box, type \*.mywatchguard.com. Click Add. This denies any email messages with a Rcpt To address that does not match the company domain.

3.

Click OK to close the SMTP Proxy Action Configuration dialog box.

C: In this exercise we will reduce the maximum email size to 5 MB (5, 000 kilobytes).

1.

From the SMTP Proxy Action dialog box under the Categories list, select General > General Settings.

2.

Find the Limits section. In the Set the maximum email size value box, type 5000.

D: Example: He must configure the Firebox to allow Microsoft Access database files to go through the SMTP proxy. He must also configure the Firebox to deny Apple iTunes MP4 files because of a recent vulnerability announced by Apple.

1.

From the SMTP-Incoming Categories list, select Attachments > Content Types.

2.

In the Actions to take section, use the None Matched drop-down list to select Allow.

This allows all content types through Firebox to the SMTP server. After Successful Company is able to add in the specific content types they want to allow, they set this parameter to strip content type that does not match their list of allowed content types.

From the SMTP-Incoming Categories list, select Attachments > Filenames.

4. The filename extension for Microsoft Access databases is “.mdb”. In the list of filenames, find and select .mdb. Click Remove. Click Yes to confirm.

3. If no rules match, the Action to take option is set to allow the attachment. In this example, MS Access files are now allowed through the Firebox.

5. In the Pattern text box, type \*.mp4. Click Add.

This rule configures the Firebox to deny all files with the Apple iTunes “.mp4” file extension bound for the SMTP server.

E: The Set the maximum email recipient checkbox is used to set the maximum number of email recipients to which a message can be sent in the adjacent text box that appears, type or select the number of recipients.

The XTM device counts and allows the specified number of addresses through, and then drops the other addresses. For example, if you set the value to 50 and there is a message for 52 addresses, the first 50 addresses get the email message. The last two addresses do not get a copy of the message.

Incorrect:

Not B: Webblocker is configured through a HTTP-policy, not through an SMTP policy.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 125, 126

Reference: [http://watchguard.com/help/docs/wsm/xtm\\_11/en-us/content/en-us/proxies/smtp/proxy\\_smtp\\_gen\\_settings\\_c.html](http://watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/proxies/smtp/proxy_smtp_gen_settings_c.html)

---

## QUESTION 2

Match each WatchGuard Subscription Service with its function.

Uses rules, pattern matching, and sender reputation to block unwanted email messages. (Choose one).

- A. Reputation Enable Defense RED
- B. Gateway / Antivirus
- C. Spam Blocker
- D. Intrusion Prevention Server IPS
- E. APT Blocker

Correct Answer: C

SpamBlocker provides a spam scanning engine that works in concert with WatchGuard's cloud-based technology to prevent spam from gaining access to the email servers (and clients).

Reference: <http://www.tomsitpro.com/articles/network-security-solutions-guide,2-866-6.html>

---

### QUESTION 3

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](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](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 4**

Which WatchGuard Subscription Service must be enabled in a proxy policy before you can use APT Blocker? (Select one.)

- A. RED
- B. Application Control
- C. Gateway Antivirus
- D. WebBlocker
- E. IPS

Correct Answer: C

#### QUESTION 5

Which of these services would you use to allow the use of P2P programs for a specific department in your organization?  
(Select one.)

- A. Reputation Enabled Defense
- B. Application Control
- C. Data Loss Prevention
- D. IPS

Correct Answer: B

[Latest ESSENTIALS Dumps](#) [ESSENTIALS PDF Dumps](#) [ESSENTIALS Practice Test](#)