



Fireware Essentials Exam Guide

The Fireware Essentials exam tests your knowledge of how to configure, manage, and monitor a WatchGuard Firebox. This exam is appropriate for network administrators who have experience configuring and managing Firebox devices that run Fireware v12.2.1.

Exam Overview

Key Concepts

To successfully complete the Fireware Essentials Exam, you must understand these key concepts:

Fireware Knowledge

- Firebox activation and initial setup
- Network configuration
- Policy and proxy configuration
- Subscription services configuration
- User authentication
- Device monitoring, logging, and reporting
- Branch office and mobile VPN configuration

General IT Knowledge

- IPv4 networking concepts (DNS, TCP/IP, DHCP, NAT, static routing)
- General understanding of firewalls

Exam Description

Content

60 multiple choice (select one option), multiple selection (select more than one option), true/false, and matching questions

Passing score

75% correct

Time limit

Two hours

Reference material

You cannot look at printed or online materials during the exam.

Test environment

This is a proctored exam, with two location testing options:

- Kryterion testing center
- Online, with virtual proctoring through an approved webcam

Prerequisites

The Fireware Essentials instructor-led course is recommended, but not required.

Prepare for the Exam

WatchGuard provides training, courseware, and reference materials to help you prepare for the Fireware Essentials Exam. In addition to the training, courseware, and reference materials described in the next sections, we strongly recommend that you install, deploy, and manage one or more Firebox devices that run Fireware v12.2.1 or higher before you begin the exam.

Instructor-Led Training

We recommend that you attend an instructor-led training class with hands-on lab exercises. Classes are often held in-region, sponsored by sales or a local WatchGuard distributor. We also offer complimentary VILT technology-based training classes for partners. WatchGuard end-users can also register for a class in our network of WatchGuard Certified Training Partners (WCTPs).

- Partners — Register for training [here](#) (login required)
- End-users — View the current [WCTP training schedule](#) on the WatchGuard website

Self-Study Materials

WatchGuard offers courseware that you can use for self-study, or to reinforce instructor-led training. We recommend that you review all available courseware before you take the exam. Courseware is available on the Technical Training tab in the WatchGuard Portal (login required).

Fireware Essentials Student Guide

The *Fireware Essentials Student Guide* courseware (PDF) is used in the instructor-led Fireware Essentials course, and is also available online for self-study and review.

If your schedule allows you the time to set up one or more Firebox devices to complete all of the exercises in the *Student Guide*, we recommend that you use the *Student Guide* as your primary self-study material to prepare for the exam.

Other Resources

Online Help

The Online Help systems provided for the various WatchGuard Fireware management tools include detailed information to expand on the principles presented in the Fireware Essentials training courseware.

For the knowledge categories included in the [Assessment Objectives](#) section, we recommend that you review the corresponding content in the appropriate Help system.

You can find *Fireware Help* in the [WatchGuard Help Center](#).

Video Tutorials

The Fireware Video Tutorials include information about specific subjects to help you learn more about some areas of Fireware OS. You can use these videos to help you expand your understanding of Fireware, as it relates to the knowledge categories specified in the [Assessment Objectives](#) section.

You can find the Video Tutorials on the WatchGuard website documentation pages: [Video Tutorials](#)

Configuration Examples

Fireware configuration examples give you the information you need to configure your Firebox to meet specific business needs. For each example we provide reference configuration files so you can see the final configuration of the features involved in each use case. We also include a guide to cover the details of each configuration. You can use these configuration examples to help you expand your understanding of Fireware, as it relates to the knowledge categories specified in the [Assessment Objectives](#) section.

You can find the Configuration Examples on the WatchGuard website documentation pages: [Configuration Examples](#)

Assessment Objectives

The Fireware Essentials Exam evaluates your knowledge of the categories in the subsequent list. For each knowledge category assessed in this exam, the *Weight* column includes the approximate percentage of exam questions from that knowledge category. Because some exam questions require skills or knowledge from more than one category, the weights do not exactly correspond to the percentage of exam questions.

Category	Skills	Weight
Firebox Administration and Initial Setup	Use the setup wizards to configure a Firebox with default security settings	10%
	Connect to Fireware Web UI	
	Edit a device configuration in Policy Manager	
	Understand the function of the feature key	
	Upgrade Fireware OS	
	Create a Firebox backup image	
	Enable remote administration	
	Migrate a Firebox configuration to another Firebox	
	Understand the default threat protection features of Fireware	
Firebox Monitoring, Logging, and Reporting	Use WatchGuard System Manager and Firebox System Manager to monitor a device	15%
	Use Dimension to monitor a Firebox and generate reports	
	Use FireWatch or Network Discovery to monitor traffic through a Firebox	
	Use Firebox System Manager to run diagnostic tasks	
	Enable logging to Dimension	
	Review log messages generated by a Firebox	
	Understand how to enable logging for reports	
Networking and Network Address Translation (NAT)	Configure an external, trusted, optional, or custom interface	15%
	Configure a secondary network on an interface	
	Add a static route for traffic between two networks	
	Read the Route table	
	Configure WINS and DNS, and understand why this is important	
	Understand when to use dynamic NAT, 1-to-1 NAT, static NAT, and NAT loopback	
	Configure dynamic NAT, 1-to-1 NAT, and static NAT	

Category	Skills	Weight
Policies, Proxies, and Default Threat Protection	Understand policy precedence	20%
	Understand the function of the default firewall policies	
	Understand the function of incoming and outgoing proxy actions	
	Use aliases in policies	
	Configure policies for different users and groups	
	Configure Firebox authentication for users and groups	
	Understand the difference between a packet filter and a proxy policy	
	Understand the ports and protocols each proxy policy handles	
	Configure SMTP-proxy, HTTP-proxy, and HTTPS-proxy action settings	
Subscription Services	Configure Application Control, WebBlocker, spamBlocker, Gateway AntiVirus, IntellifentAV, Intrusion Prevention Service, Data Loss Prevention, Reputation Enabled Defense, Botnet Detection, APT Blocker, and Geolocation	20%
	Understand the functions of all subscription services	
	Understand dependencies between subscription services	
	Understand how the feature key enables security services	
Authentication and Virtual Private Networking	Configure Firebox authentication for users and groups	20%
	Understand the differences between a manual BOVPN and a BOVPN virtual interface	
	Configure a manual BOVPN between two Firebox devices	
	Use log messages to troubleshoot a branch office VPN tunnel	
	Understand the differences between the supported mobile VPN types	
	Configure Mobile VPN with IPSec and Mobile VPN with SSL	
	Configure authentication for mobile VPN users	

Example Exam Questions

The exam includes multiple choice, multiple selection, true/false, and matching questions. The subsequent examples show the types of questions to expect on the exam. Answers to each question appear on the last page.

Questions

1. What is the purpose of the *WatchGuard* policy? (Select one.)
 - a. Allows management connections to the Fireware Web UI
 - b. Allows branch office VPN connections between two Fireboxes
 - c. Allows management connections to the Firebox from WatchGuard System Manager
 - d. Allows connections to the Firebox from a WatchGuard Log Server

2. From the policies shown in this image, can users in the Sales group connect to websites with HTTPS? (Select one.)

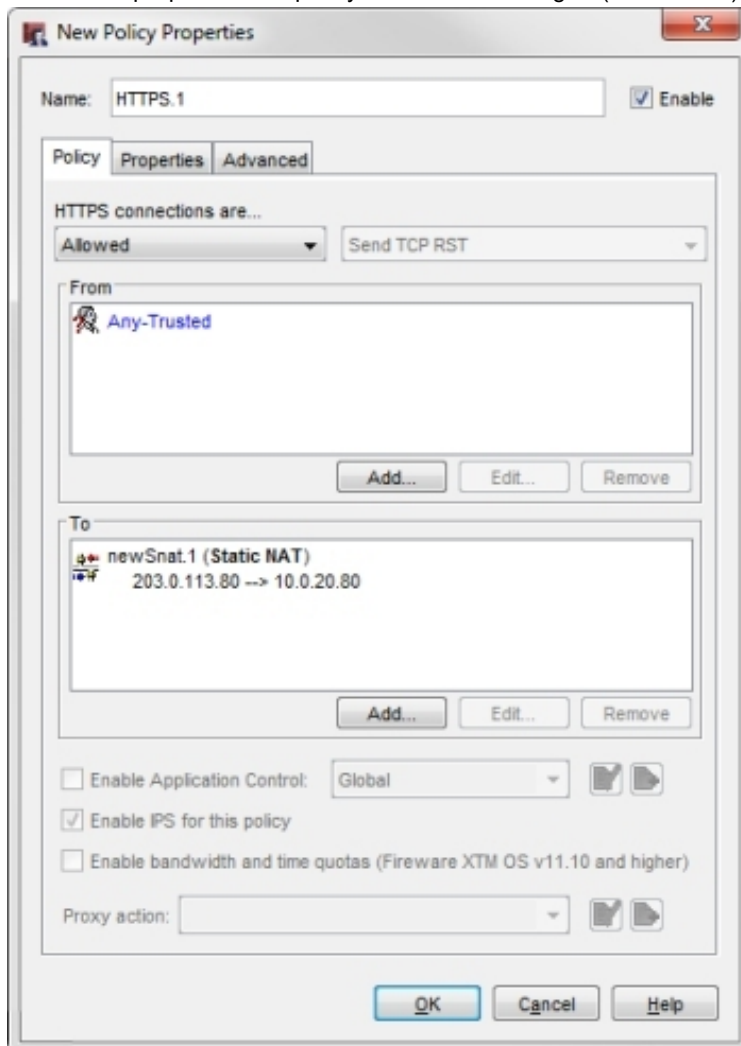
Order /	Action	Policy Name	Policy Type	From	To
1	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External
2	✓	HTTP	HTTP	Sales (Firebox-DB)	Any-External
3	✓	HTTPS-proxy	HTTPS-proxy	Accounting (Firebox-DB)	Any-External
4	✓	WatchGuard Authen...	WG-Auth	Any-Trusted, Any-Optional	Firebox
5	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox
6	✓	Ping	Ping	Any-Trusted, Any-Optional	Any
7	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox
8	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External

- a. No. The HTTPS-Proxy policy only allows HTTPS traffic for the Accounting group.
 - b. No. The Outgoing policy does not allow any traffic from the Sales group.
 - c. Yes. The HTTP policy allows HTTP and HTTPS traffic for the Sales group.
 - d. Yes. The Outgoing policy allows HTTPS traffic from the Sales group.

3. You can use LDAP authentication for L2TP Mobile VPNs.
 - a. True
 - b. False

4. You can use the Geolocation dashboard in Fireware Web UI to see the location of which types of connections? (Select one.)
 - a. Allowed connections
 - b. Denied connections
 - c. Both allowed and denied connections

5. What is the purpose of the policy shown in this image? (Select one.)



- To allow clients on an external network to connect to a secure web server on a trusted or optional network using its public IP address
- To allow clients on your trusted network to connect to a secure web server on a trusted or optional network using its private IP address
- To allow clients on your trusted network to connect to a secure web server on a trusted or optional network using its public IP address
- To allow clients on an external network to connect to a secure web server on a trusted or optional network using its private IP address

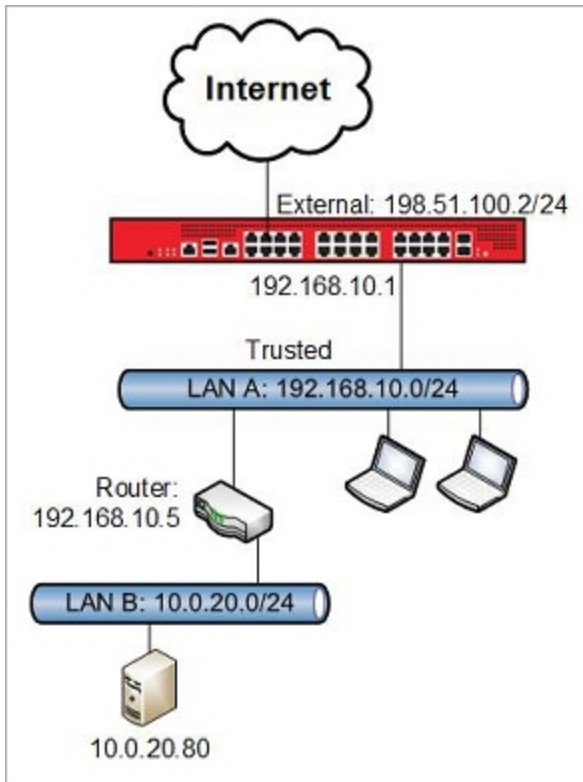
6. The Firebox Device Administrator, Bob, is a member of the SSLVPN-Users group. With the policies configured as shown in the image, which methods can he use to remotely manage this Firebox? (Select two.)

Order	Action	Policy Name	Policy Type	From	To
1	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External
2	✓	WatchGuard SSLVPN	SSL-VPN	Any-External, Any-Trusted, Any-Optional	Firebox
3	✓	WatchGuard Authentic...	WG-Auth	Any-Trusted, Any-Optional, Any-External	Firebox
4	✓	WatchGuard Web UI	WG-Fireware-XTM-We	Any-Trusted, Any-Optional	Firebox
5	✓	Ping	Ping	Any-Trusted, Any-Optional	Any
6	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Bob (Firebox-DB)	Firebox
7	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External
8	✓	Allow SSLVPN-Users	Any	SSLVPN-Users (Any)	Any

- Use the Mobile VPN with SSL client to authenticate to the Firebox, then connect to the trusted interface in WatchGuard System Manager.
 - Use the Authentication Portal to authenticate to the Firebox, then connect to Fireware Web UI on the external interface.
 - Use the Authentication Portal to authenticate to the Firebox, then connect to the external interface in WatchGuard System Manager.
 - Use the Authentication Portal to authenticate to the Firebox, then connect to the trusted interface in WatchGuard System Manager.
7. What rule in the SMTP-Outgoing proxy action can you use to prevent spam relay through your email server? (Select one.)
- Rcpt To
 - Mail From
 - Headers
 - Authentication
 - Greeting Rules
8. While troubleshooting a branch office VPN tunnel, you see the log message below. What settings could you modify in the local device configuration to resolve the configuration issue? (Select one.)
- ```
2014-07-23 13:11:04iked (203.0.113.10<->203.0.113.20)Peer proposes phase 2 ESP authentication MD5-HMAC, expecting SHA1-HMAC
```
- BOVPN Gateway settings
  - BOVPN Tunnel settings
  - BOVPN Tunnel Route settings
  - BOVPN-Allow policy



9. Based on this network diagram, which of these static routes could you add to the Firebox to enable the Firebox to route traffic from clients on the 192.168.10.0/24 subnet to a server at 10.0.20.80? (Select two.)



- Route to 10.0.20.0, Gateway 10.0.2.1
  - Route to 10.0.20.80, Gateway 192.168.10.5
  - Route to 192.168.10.5, Gateway 192.168.10.1
  - Route to 10.0.20.0/24, Gateway 192.168.10.5
10. You can use the TCP-UDP proxy to control Web, FTP, and SIP traffic on ports other than 80, 21, and 5060.
- True
  - False

## Answers

For each example question, the answer includes the knowledge categories the question tests. Many exam questions test knowledge in more than one area.

1. c. The WatchGuard policy allows connections to the Firebox from WatchGuard System Manager.

Tested knowledge categories:

- Understand the function of the default firewall policies
- Enable remote administration

2. d. Yes, the Outgoing policy allows this traffic.

Tested knowledge categories:

- Understand policy precedence
- Configure policies for different users and groups
- Understand the function of the default firewall policies

3. b. False. You cannot use LDAP authentication for connections from L2TP VPN clients.

Tested knowledge categories:

- Understand the differences between the three mobile VPN types

4. a. The Geolocation dashboard shows the geographic location of allowed connections.

Tested knowledge categories:

- Geolocation

5. c. This is an example of NAT loopback.

Tested knowledge categories:

- Understand when and how to use dynamic NAT, 1-to-1 NAT, static NAT, NAT loopback

6. a and c. Bob can either authenticate to the Firebox and then connect to the Firebox on the external interface, or he can use the SSL VPN client to authenticate and then connect to the Firebox on the trusted interface. He cannot connect to the Web UI on the external interface because the WatchGuard Web UI policy does not allow connections from the external network or connections from the user Bob or the group SSLVPN-Users.

Tested knowledge categories:

- Configure Firebox authentication for users and groups
- Enable remote administration
- Configure policies for different users and groups

7. b. To prevent relay of messages from another domain through your SMTP server, you can configure the **Mail From** setting in the SMTP-Outgoing proxy action to deny mail from domains other than the ones you specify.

Tested knowledge categories:

- SMTP proxy actions

8. b. Phase 2 authentication is configured in the BOVPN Tunnel settings.

Tested knowledge categories:

- Use log messages to troubleshoot a branch office VPN
- Configure a branch office VPN

9. b and d. You can configure a route to the specific server, or to the entire subnet it is on. In either case, the gateway is the IP address of the router that connects to that network, and the gateway must be reachable by the firewall.

Tested knowledge categories:

- General IT knowledge / IPv4 networking
- Add a static route

10. a. True

Tested knowledge categories:

- Understand the ports and protocols each proxy policy handles

# Register for the Exam

To schedule an exam, you must create a Kryterion user account.

1. Log in to the WatchGuard website with your WatchGuard account credentials.
2. Select the **Technical Training** tab.
3. At the right side of the page, click **Register for an exam**.  
*This opens a WatchGuard-branded Kryterion web page.*
4. At the top-right corner of the page, click the link to create a new Kryterion user account, or log in with an existing Kryterion user account for WatchGuard exams.
5. Click **Schedule an Exam**.

For more information about the certification process, see this [FAQ](#).

---

## Copyright, Trademark, and Patent Information

Copyright © 1998–2018 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the *Copyright and Licensing Guide*, available online at <http://www.watchguard.com/help/documentation/>.