Firewall Policies Exam Guide

The Firewall Policies exam tests your knowledge of how to configure firewall policies for a Firebox that runs Fireware v12.2.1.

Exam Overview

Key Concepts

To successfully complete the Firewall Policies Exam, you must understand these key concepts:

Fireware Knowledge

- General policy settings
- Default firewall policies
- Security zones and aliases
- Packet filter policy configuration
- How NAT is used in firewall policies
- Proxy policy and proxy action configuration
- HTTP content actions and routing actions
- Policy precedence
- Security service basics

General IT Knowledge

- IPv4 networking concepts (DNS, NAT, FQDN, static routing)
- Standard ports and protocols (HTTP, HTTPS, FTP, SMTP, DNS)
- General understanding of firewalls

Exam Description

Content

40 multiple choice (select one option), multiple selection (select more than one option), and true or false questions

Passing score

75% correct

Time limit

Two hours

Reference material

You cannot reference 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

None

Prepare for the Exam

WatchGuard provides reference materials to help you prepare for the Firewall Policies exam. In addition to the reference materials described in the subsequent sections, we strongly recommend that you use WatchGuard System Manager v12.2.1 to set up firewall policies on a Firebox that uses Fireware v12.2.1 before you take this exam.

Self-Study Materials

WatchGuard offers courseware that you can use for self-study. We recommend that you review all available courseware before you take the exam. Courseware is available in the Technical Training section of the WatchGuard Portal (login required).

Firewall Policies Courseware

The *Firewall Policies* courseware (PPT) is available online for self-study and review.

Other Resources

Online Help

The Fireware Help system, available online includes detailed information to expand on the principles presented in the Firewall Policies 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:

Recommended Video Tutorial: Getting Started with Policies

All Video Tutorials: Video Tutorials

Configuration Examples

Fireware configuration examples give you the information you need to configure your Firebox to meet certain 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 Firewall Policies 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 / Knowledge	Weight
Policy Settings and General Knowledge		33%
	Add a packet filter or proxy policy	
	Configure a policy source and destination	
	Configure a policy schedule	
	Aliases and interface types	
	Use an FQDN in a policy	
	Configure policies for web and email traffic	
	Understand when and why to use policy-based routing	
	Add a custom policy templates	
	Configure traffic management actions in a policy	
	Enable logging in a policy	
Network Address Translation (NAT)		10%
	Use Static NAT in a policy	
	Understand how dynamic NAT and 1-to-1 NAT apply to traffic handled by a policy	
Proxy Actions		10%
	Select the appropriate proxy action for a proxy policy	
	Configure HTTP, HTTPS, SMTP, and TCP/UDP proxy actions	
	Enable content inspection in the HTTPS proxy	
HTTP Content Actions & Routing Actions		8%
	Understand when to use an HTTP content action	
	Understand when to use a routing action	
Subscription Services		12%
	Enable security services in policies	
	Understand which security services apply only to proxy policies	
Policy Precedence		10%
	Understand how Policy Manager automatically orders policies	

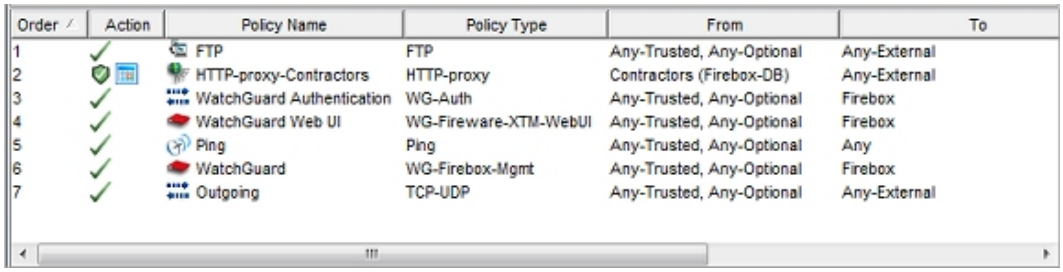
Category	Skills / Knowledge	Weight
	Use policy precedence to create multiple policies of the same type that apply to different users	
Default Firewall Policies		10%
	Understand function of the default firewall policies created by the Web Setup Wizard and Quick Setup Wizard	
	Understand how RapidDeploy QuickStart configures a Firebox with a default policies	
Traffic Log Messages		7%
	Read a traffic log message to identify which policy allowed or denied a packet	
	Read a traffic log message to determine which port and protocol is used by a packet	
	Understand the meaning of (Unhandled Internal Packet) and (Unhandled External Packet) in a log message.	

Example Exam Questions

The exam includes multiple choice, multiple selection, and true or false 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. Which proxy action do you use for an FTP policy that applies to traffic from Any-Trusted to Any-External? (Select one.)
    a. FTP-Client
    b. FTP-Server
    c. FTP-Outgoing
    d. FTP-Incoming
2. Which of these connections are allowed by the default firewall policies? (Select three.)
    a. TCP and UDP connections from any trusted or optional source to any external network.
    b. Connections between hosts on different trusted networks.
    c. Outgoing FTP connections from any trusted or optional network.
    d. Ping connections from the trusted network to the optional network.
3. Which type of NAT is configured by default on a Firebox? (Select one.)
    a. 1-to-1 NAT
    b. Static NAT
    c. Dynamic NAT
    d. NAT loopback
4. The **HTTP-proxy-Contractors** policy has bandwidth and time quotas enabled, and is configured with a schedule that makes the policy operational only during business hours. With policies configured as shown in this image, can authenticated users in the Contractors group browse the web during non-business hours?



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

    a. Yes
    b. No
5. How can you configure a Firebox to route inbound HTTP requests received for one public IP address to different internal web servers based on the content of the HTTP header? (Select one.)
    a. Configure an inbound HTTP proxy policy to use an HTTP proxy action that contains domain name rules. In each domain name rule, specify the pattern to match in the HTTP header, and a routing action with the IP address of the internal web server.
    b. Configure an inbound HTTP proxy policy to use an HTTP content action. In the HTTP content action, add content rules for each pattern to match in the HTTP header and a routing action with the IP address of the internal web server.
    c. Configure separate HTTP proxy policies for traffic to each internal web server. In each proxy policy add a static NAT action that specifies the pattern to match in the HTTP header and the IP address of the internal web server.

Answers

1. a. The FTP-Client proxy action protects outgoing connections from FTP clients on your network.
2. a, c, d. The default policies do not allow traffic between hosts on different trusted networks.
3. c. Only Dynamic NAT is enabled by default.
4. a. Yes - the Outgoing policy allows the traffic when the HTTP-proxy-Contractors policy is not active.
5. b. An HTTP content action contains content rules that specify the pattern to match in the HTTP header and an associated routing action.

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.