Network and Traffic Management with Fireware Exam Guide

The Network and Traffic Management with Fireware Exam tests your knowledge of how to configure and manage the network and traffic management features of a WatchGuard Firebox that runs Fireware OS. This exam is appropriate for network administrators who have experience configuring and managing Fireboxes that run the most current version of Fireware OS.

Exam Overview

Key Concepts

To successfully complete the Network and Traffic Management with Fireware Exam, you must understand these key concepts:

Fireware Knowledge

- Network configuration
- VLAN configuration
- Traffic Management configuration
- Link Aggregation configuration
- Multi-WAN methods
- Routing
- FireCluster configuration

General IT Knowledge

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

Exam Description

Content

40 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 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

The Network and Traffic Management 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 Network and Traffic Management with Fireware Exam. In addition to the training, courseware, and reference materials described in the subsequent sections, we strongly recommend that you install, deploy, and manage one or more Fireboxes 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 that includes hands-on lab exercises. Classes are often held in-region, sponsored by WatchGuard Sales or a local WatchGuard distributor. We also offer complimentary VILT technology-based training classes for partners. WatchGuard end-users can 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).

Network and Traffic Management with Fireware Student Guide

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

If your schedule allows you the time to set up one or more Fireboxes 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 Network and Traffic Management with Fireware 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 complete list of Video Tutorials on the WatchGuard website:

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:

Configuration Examples

Assessment Objectives

The Network and Traffic Management with Fireware 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
Routing	Configure a static route between two Fireboxes	25%
	Configure a BOVPN virtual interface route	
	Configure dynamic routing between two Fireboxes	
	Understand when to use each supported dynamic routing protocol	
	Configure Fireware to automatically fail over to a branch office VPN if a primary route becomes unavailable	
	Understand how dynamic routing populates routes in the Route table on the Firebox	
	Read the Routes table in the Status Report in Firebox System Manager	
	Use Traffic Monitor to troubleshoot dynamic routing issues	
Traffic Management	Understand what happens when you configure the Outgoing Interface Bandwidth setting for an interface	18%
	Configure Quality of Service (QoS) to prioritize network traffic	
	Use Traffic Management actions in policies	
	Use Traffic Management actions with Application Control	
VLAN Configuration	Configure VLANs to separate traffic for users on the same physical network	18%
	Configure a VLAN that includes users on different network segments	
	Configure VLANs to handle tagged or untagged traffic	
	Configure VLAN settings on the switch that connects to a VLAN interface	
Multi-WAN	Configure each of the four multi-WAN methods	15%
	Understand how each multi-WAN method distributes traffic among the external interfaces	
	Configure reliable link monitor targets for multi-WAN	
	Configure the sticky connection settings in the multi-WAN settings and in policies	
	Configure the round-robin multi-WAN method with optional weights for each interface	

Category	Skills	Weight
	Understand how Fireware makes multi-WAN routing decisions	
Link Aggregation	Understand the difference between dynamic, static, and active-backup link aggregation modes	12%
	Configure a link aggregation interface	
	Understand the switch requirements for different link aggregation modes	
FireCluster	Configure two Fireboxes as a FireCluster	12%
	Configure network switches that connect to a FireCluster	
	Enable security services on a FireCluster	
	Understand the impact of a FireCluster failover on network connections	

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. If you create a *Per Policy* Traffic Management action that sets a minimum guaranteed bandwidth and apply it to two policies, what is the effect? (Select one.)
    a. The minimum bandwidth is reserved to be shared by the two policies and is not available for other policies.
    b. The two policies that use this action share the minimum bandwidth when it is needed, otherwise the bandwidth is available for other policies.
    c. The two policies that use this action are each guaranteed the minimum bandwidth only when it is needed, otherwise the bandwidth is available for other policies.
2. If you add a static route and the Firebox does not have a route to the gateway specified in the route, what do you see in the Routes table on the Firebox? (Select one.)
    a. The static route is listed with a metric of 0.
    b. The static route is listed with a metric of 255.
    c. The static route is not listed.
    d. The static route is listed with 0.0.0.0 as the gateway.
3. When multi-WAN is enabled, which of these settings has the highest precedence to determine through which interface the Firebox routes an outbound packet? (Select one.)
    a. The multi-WAN method configured in the network settings
    b. The multi-WAN sticky connection setting
    c. A static route that matches the destination of the packet
    d. Policy-based routing in a policy that matches the source and destination of the packet
4. Which of these interface settings are not supported for a link aggregation interface? (Select two.)
    a. VLAN
    b. Traffic management
    c. Multi-WAN
    d. MAC access control
    e. IPv6
5. If you enable the **Apply firewall policies to intra-VLAN traffic** option in a VLAN configuration, how does this change the way the Firebox applies policies to VLAN traffic? (Select one.)
    a. Enables the Firebox to apply firewall policies to traffic between two VLANs on the same Firebox interface.
    b. Enables the Firebox to apply firewall policies to traffic between two VLANs on different Firebox interfaces.
    c. Enables the Firebox to apply policies to traffic within the same VLAN, on different Firebox interfaces.

Answers

1. c. A per-policy traffic management action guarantees the specified bandwidth for each policy, when it is needed.
2. c. A route does not appear in the Routes table if there is no route to the gateway specified in the route.
3. d. The policy-based routing has higher precedence than a static route or the multi-WAN method or sticky connection settings.
4. b and d. Link aggregation interfaces do not support MAC access control or traffic management.
5. c. Intra-VLAN traffic is traffic from a VLAN that is destined for the same VLAN. With this option enabled, the Firebox applies policies to traffic that passes through the firewall between hosts that are on the same VLAN.

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.