Network Security Essentials Exam Guide

The Network Security Essentials exam tests your knowledge of basic networking and 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 v12.4.

Exam Overview

Key Concepts

To successfully complete the Network Security 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 Network and Security Knowledge

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

Copyright © 2019 WatchGuard Technologies, Inc. All rights reserved.

Exam Description

Content

70 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 Network Security video course or instructor-led course is recommended, but not required.

Prepare for the Exam

WatchGuard provides training and online courseware to help you prepare for the Network Security Exam. In addition to the training and courseware described in this document, we strongly recommend that you install, deploy, and manage one or more Firebox devices that run Fireware v12.4 or higher before you begin the exam.

Instructor-Led Training

To get hands-on experience, we recommend that you attend an instructor-led training class. 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 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 video-based courseware that you can use for self-study, or to reinforce instructor-led training. To prepare for this exam, review the *Network Security Essentials* course.

The *Network Security Essentials* course is available on the WatchGuard Portal (login required).

- Partners — This course is available in the Learning Center in the Partner Portal.
- End-users — This course is available in the *Training & Certification* section of WatchGuard Support Center.

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 Security 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 Network Security 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	Knowledge Areas	Weight
Network and Network Security Basics	Understand basic networking concepts that are not unique to the Firebox. ■ IPv4 addresses, subnetting, and routing ■ Network Address Translation ■ Packet headers (TCP, IP, HTTP) ■ MAC addresses ■ Network services, ports, and protocols	10%
Administration and Setup	Understand how to set up a Firebox with a basic configuration, and complete basic Firebox administration tasks. ■ Firebox default policies and network settings ■ Fireware Web Setup Wizard ■ Feature keys ■ Firebox backup and restore ■ Configuration file migration ■ Default Threat Protection	10%
Monitoring, Logging, and Reporting	Understand how to use management tools to monitor or troubleshoot a Firebox. ■ Tools to monitor Firebox status and activity ■ Diagnostic tools in Firebox System Manager ■ Firebox logging to Dimension or WatchGuard Cloud ■ Firebox log messages ■ Logging settings	15%
Networking and NAT	Understand how to configure Firebox network settings and NAT. ■ Network interface types, security zones, and settings ■ WINS/DNS ■ Routing and static routes ■ NAT types and configuration ■ DHCP ■ VLANs ■ Multi-WAN and SD-WAN actions	25%

Category	Knowledge Areas	Weight
Policies, Proxies, and Security Services	Understand how to configure Firebox policies, proxies, and security services. ■ Packet filter policies and proxy policies ■ Policy precedence ■ HTTP proxy ■ HTTPS proxy content inspection ■ Content actions and domain name rules ■ Fireware subscription security services	25%
Authentication and VPNs	Understand user authentication and VPN settings on the Firebox. ■ Authentication servers ■ Users and groups in policies ■ Firebox authentication portal ■ Mobile VPN routing options and protocols ■ Branch Office VPN gateways and tunnel routes ■ Branch Office VPN and NAT ■ BOVPN virtual interfaces	15%

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. Which of these is a Class B subnet mask? (Select one.)
    a. /8
    b. /12
    c. /16
    d. /24
    e. /28

2. What is the purpose of the *WG-Auth* policy? (Select one.)
    a. Allows management users to authenticate to Fireware Web UI
    b. Allows branch office VPN connections between two Fireboxes
    c. Allows user connections to the Firebox Authentication Portal
    d. Allows Mobile VPN users to authenticate to the Firebox

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

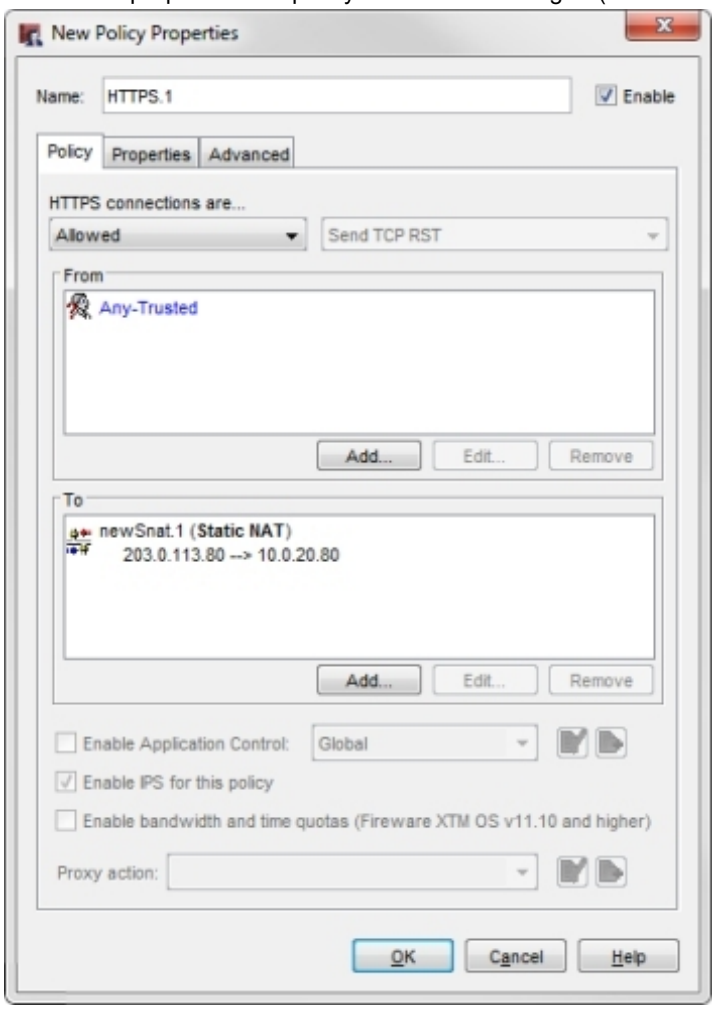
Order	Action	Policy Name	Policy Type	From	To
1	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External
2	✓	HTTP	HTTP	Sales (Firebox-DB)	Any-External
3	✓	HTTPS-proxy	HTTPS-proxy	Accounting (Firebox-DB)	Any-External
4	✓	WatchGuard Authen...	WG-Auth	Any-Trusted, Any-Optional	Firebox
5	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI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

4. You can configure Dynamic NAT to route incoming connections from the Internet to two different FTP servers on the trusted network.
    a. True
    b. False

5. What port and protocol is used by DNS? (Select one.)
    a. UDP/67
    b. UDP/53
    c. TCP/20
    d. TCP/25

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



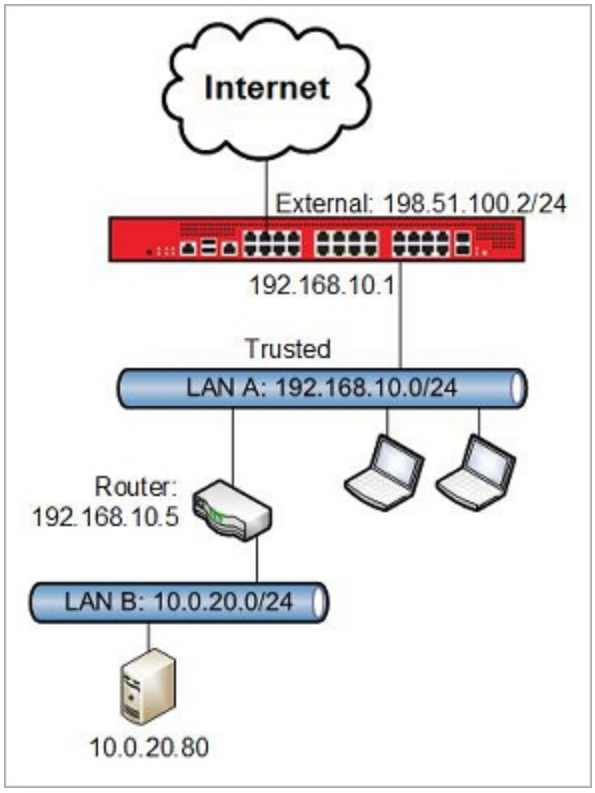
   a. To allow clients on an external network to connect to a secure web server on a trusted or optional network using its public IP address
   b. To allow clients on your trusted network to connect to a secure web server on a trusted or optional network using its private IP address
   c. To allow clients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

7. 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.)

```
iked (203.0.113.50<->203.0.113.20)IKE phase-2 negotiation from 203.0.113.50:500 to
203.0.113.20:500 failed. Tunnel='tunnel.1' Reason=Received proposal without PFS, Expecting
PFS enabled id="0205-0002" Debug
```

   a. BOVPN Gateway settings
   b. BOVPN Tunnel settings
   c. BOVPN over TLS settings
   d. IKEv2 Shared settings

8. 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.)



   a. Route to 10.0.20.0, Gateway 10.0.2.1
   b. Route to 10.0.20.80, Gateway 192.168.10.5
   c. Route to 192.168.10.5, Gateway 192.168.10.1
   d. Route to 10.0.20.0/24, Gateway 192.168.10.5

9. You can use the TCP-UDP proxy to control Web, FTP, and SIP traffic on ports other than 80, 21, and 5060.
   a. True
   b. False

10. Which authentication servers can be used with any type of Mobile VPN (Select two.)
   a. Firebox-DB
   b. Active Directory
   c. RADIUS
   d. LDAP

Answers

Note: Many exam questions test knowledge in more than one area.

1. c. A class B subnet mask is 255.255.0.0, which is 16 bits, and is represented in slash notation as /16.
2. c. The WG-Auth policy allows users to connect to the Authentication Portal from the trusted or optional networks.
3. d. Yes, the Outgoing policy allows this traffic.
4. b. False. Dynamic NAT applies only to outgoing connections.
5. b. DNS uses UDP port 53.
6. c. This is an example of NAT loopback.
7. b. Phase 2 authentication is configured in the BOVPN Tunnel settings.
8. b and d. You can configure a static 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.
9. a. True. The TCP-UDP proxy applies to TCP and UDP traffic on any TCP or UDP port. The default Outgoing policy is an example of this.
10. a and c. Only Firebox-DB and RADIUS are supported by all Mobile VPN types.

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 © 1998–2019 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/.