+33 (0)1 48 10 09 46
formation@ambient-it.net 140 Avenue Jean Lolive 93500 Pantin - France

Updated on 06/12/2026

Sign up

WatchGuard Network Security Essentials Training

2 days (14 hours)

Overview

WatchGuard Firebox is a network security solution that protects enterprise infrastructures with firewall, filtering, VPN, traffic inspection, UTM services, monitoring, and reporting capabilities.

Our WatchGuard Network Security Essentials training will help you master the fundamentals of installing, configuring, and administering a WatchGuard Firebox environment.

You will learn how to configure network interfaces, security policies, NAT, segmentation, UTM services, authentication, remote access, and site-to-site VPNs.

Upon completion of this training, you will be able to administer a Firebox on a daily basis, secure access, analyze logs, monitor network activity, and diagnose common incidents.

This training also covers hardening best practices: updates, backups, administrator accounts, least privilege policies, VPN security, certificates, logs, and secure configuration.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the WatchGuard Firebox architecture and Fireware fundamentals
- Configure interfaces, routes, DNS, DHCP, and network settings
- Create security policies, NAT rules, and filtering services

- Set up UTM services: IPS, WebBlocker, Application Control, and proxies
- Configure remote access VPNs and site-to-site tunnels
- Utilize logs, reports, monitoring tools, and troubleshooting methods

Target Audience

- Network administrators
- System and network administrators
- Network engineers
- Network security engineers
- Advanced network technicians
- Infrastructure Managers and Security Integration Consultants

Prerequisites

- Basic knowledge of TCP/IP networks
- Understanding of routing, DNS, DHCP, NAT, and IP addressing
- General understanding of network security principles

Technical prerequisites

- A computer with a modern web browser
- A stable internet connection

WatchGuard Network Security Essentials Training Agenda

[Day 1 - Morning]

Introduction to WatchGuard Firebox and Fireware fundamentals

- Understand the role of WatchGuard Firebox in a network security architecture
- Identify key components: Fireware, Web UI, WatchGuard System Manager, WatchGuard Cloud, and security services
- Understand deployment modes: router, bridge, drop-in, local network, DMZ, and segmentation
- Configure interfaces, IP addresses, DNS, DHCP, static routes, and gateways
- Discover best practices for initial configuration, backup, restoration, and Fireware updates
- Hands-on workshop: initialize a Firebox, configure network interfaces, and verify connectivity

[Day 1 - Afternoon]

Security policies, NAT, and traffic control

- Understand how firewall policies work in Fireware
- Create and organize filtering rules based on sources, destinations, ports, protocols, and services
- Configure NAT, SNAT, DNAT, port forwarding, and publishing rules
- Apply best practices for segmentation between LAN, WAN, DMZ, guest, and business networks
- Test, diagnose, and adjust rules to prevent excessive exposure
- Hands-on workshop: create security policies, configure a NAT rule, and validate allowed or blocked traffic

UTM Security and Protection Services

- Understand WatchGuard security services: Gateway AntiVirus, IPS, WebBlocker, Application Control, and spamBlocker
- Configure HTTP, HTTPS, SMTP, DNS, or FTP proxies according to filtering needs
- Implement web filtering, application control, and intrusion prevention
- Enable security profiles tailored to users, networks, and business risks
- Identify the impact of security services on performance and user experience
- Hands-on workshop: Apply UTM services to a traffic policy and analyze the generated events

[Day 2 - Morning]

VPN, remote access, and site-to-site connectivity

- Understand VPN use cases in WatchGuard: remote access, site-to-site, and secure interconnection
- Configure a Mobile VPN for remote users
- Set up a Branch Office VPN to connect multiple sites
- Understanding IKE settings, tunnels, authorized networks, routing, and associated rules
- Applying VPN security best practices: authentication, encryption, permissions, and monitoring
- Hands-on workshop: Configure a remote access VPN or site-to-site tunnel and validate communications

[Day 2 - Afternoon]

Authentication, administration, and hardening

- Configure user and group authentication to control network access
- Manage administrator accounts, roles, permissions, passwords, and remote access
- Securing local and remote administration of the Firebox
- Implement best practices: updates, backups, certificates, accounts, interfaces, and minimum policies
- Prepare a configuration that meets operational and maintenance requirements
- Hands-on workshop: hardening a Firebox configuration and applying a security checklist

Monitoring, logs, reporting, and troubleshooting

- Use Firebox logs to understand authorized, blocked, or inspected traffic
- Use WatchGuard monitoring tools, dashboards, alerts, and reports
- Diagnose common issues: connectivity, policies, NAT, VPN, DNS, and security services
- Analyze events related to proxies, IPS, web filtering, authentication, and VPN
- Implement a structured troubleshooting method for daily operations
- Hands-on workshop: Resolve a network or security incident using available logs, diagnostic tools, and reports

Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams in new advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.