# WatchGuard e-Series Accreditation Training – v10

## You Will Learn How To:

- Install, configure and manage the WatchGuard Firebox X e-Series
- Understand the environment for Firewall installation
- Set up proxies including E-mail, FTP and Web proxies
- Configure services and authentication
- Review and configure network settings
- Specify and implement relevant security policies and settings
- Develop and implement an extended corporate network with Virtual Private Networks (VPNs)
- Understand centralised management of devices & VPNs using Management Server
- Understand and be able to manage logging and reporting.

## Course Benefits:

Multi-functional security is a major requirement for small and medium-sized enterprises. Additionally, IPSec VPNs provide major benefits for organisations providing secure authenticated communications inexpensively over the internet. Due to increased firewall requirements there is increasing need for packet and proxy filtering and for remote management.

Firebox X training enables detailed configuration and implementation of firewall policies, VPNs, add-on modules and associated management and reporting.

This course covers specification, installation, configuration and management of the FireBox X range of multi-function security appliances using latest WSM version 10. It includes a mixture of hands-on and theoretical sessions leading to the WCSP exam (successful completion of which leads to WatchGuard accreditation status)

## Course Content:

- Organising your network
- Firebox X configuration options
- Firebox X placement and setup
- Running the Quick Setup Wizard for Edge, Core and Peak
- Using WatchGuard System Manager
- Using Policy Manager to define services and security policies:
  - Schedules
  - QOS
- Working with configuration files
- Configuring application proxies for added security:
  - HTTP proxy
  - FTP Proxy
  - SMTP Proxy
- Creating new policy templates
- Configuring and modifying Firebox X network settings
- Network Address Translation
- Using WebBlocker to filter outgoing web traffic
- Firebox Defences
  - Intrusion Prevention
  - Gateway Anti virus
  - Blocking dangerous sites and ports
  - SpamBlocker
- Understanding user authentication
- Defining policies by group and user
- Using new Log server, management server, Web-blocker server
- Understanding Firebox X log files
- Monitoring network
- Using HostWatch to monitor user activity
- Generating reports of network activity
- Working with MUVPN
- BOVPN configuration
- Managing the Edge remotely
- Developing policy and security templates
- Monitoring and maintaining your VPNs
- Configuring the Firebox for VLANs
- Exploring multi-WAN
- Working with Quality of Service

## Who Should Attend:

This course is valuable for all IT professionals who are responsible for the specification, installation, management, and support or reporting for firebox X multi-function security appliances.

Some knowledge of basic networking concepts including network topologies, IP addressing and subnets is assumed. Some knowledge of security is helpful but not essential.

**Duration:** 3 Days

## Materials:

Delegates receive a student guide including all training materials presented during the course as well as hands on lab exercises used in the course.

**Price:** £999.00

## Venue:

WatchGuard Accredited Training Centre
Wick Hill Ltd,
River Court, Albert Drive
Woking, Surrey,
GU21 5RP