WatchGuard™ Certified Online Training Course

The WatchGuard Certified Online Training Course certifies that individuals have the expertise necessary to manage the day-to-day operations of WatchGuard firewalls in support of specific corporate policies. Participants will learn the basic and advanced configuration and administration aspects of the most commonly used features on the WatchGuard T Series and M Series Appliances. Through interactive modules, participants explore firewall policies, user authentication, VPNs, virus scanning, email filtering, web filtering, application control and more.

This WatchGuard training course will provide a solid understanding of how to integrate and ensure a high level of security and operational maintenance for optimal performance in the corporate environment. This course is recommended for anyone who is responsible for the day-to-day administration and management of a WatchGuard firewall.

Course Trainer

Our certified WatchGuard trainer has over 28 years, starting with the Firebox II. He manages firewalls world-wide and has been providing managed security services to many industries, including Healthcare, Manufacturing, Retail, Financial, and Government, among others.

Course Structure

This online course will be administered over 5 half day sessions from 9am PST to 1pm PST with breaks. Each student will be given remote access to a Windows workstation and a WatchGuard Firewall during the training session. Each student will be provided with WatchGuard course materials before the start of the course.

Recommended Experience

- Basic knowledge of networking
- Basic understanding of firewall concepts

Required Equipment

- Workstation with Windows and access to the Internet (recommended the student has 2 screens but is not required)
- Student will be required to install the WatchGuard Mobile SSL VPN Client. Please white list the IP 12.24.54.107 prior to the training

Course Dates

- March 2nd – 6th, 2020

Course Topics:

1. **Course Introduction**
   Materials and lab network configuration as well as expectations
2. **Firebox Administration**
   Connecting to the firewall, feature keys, device management, backup and restoration
3. **Network Settings**
   Interface configuration, Secondary Networks, WINS/DNS, routes
4. **Setup Logging and Servers**
   Connecting to Dimension and WatchGuard Server Center
5. **Monitoring Your Firewall**
   Traffic Monitor, FireWatch, Network Discovery
6. **NAT**
   DNAT, SNAT, NAT Loopback, and 1 to 1
7. **Threat Prevention**
   IPS, Default packet handling, Geolocation, Auto-Block rules
8. **Policies – Filter/Proxy**
   Filter and Proxies, custom filters, advanced policy properties, precedence
9. **In Depth Proxy Policies**
   DNS and FTP proxies and ALG's
10. **Email Proxies and Blocking Spam**
    SMTP, POP3, and SpamBlocker
11. **Web Traffic**
    HTTP, Reputation Enabled Defense, WebBlocker
12. **Signature Service and APT Blocker**
    Sandboxing, Gateway AV, Intelligent AV, DLP, Application Control, Botnet
13. **Authentication**
    AD Integration, Single Sign On, Group policies
14. **Logging and Reporting**
    WSC and Dimension overview
15. **Branch Office VPN**
    VPN Negotiations, different types of BoVPN, manual and automatic BoVPN creation
16. **Mobile VPN**
    IPSEC, L2TP, SSL, and PPTP* (Not recommended)
17. **Fireware Web UI**
    Web GUI and Firewall CLI
18. **Threat Detection and Response**
    Total Security Package, Ransomware destroyer
19. **DNS Watch**
    Protection from malicious phishing sites

To register contact your eSecurity Solutions sales rep or email sales@esecuritysolutions.com