

WatchGuard Fireware XTM Full Course In-Depth Training Class



Overview:

The WatchGuard Fireware XTM Full Course In-Depth training class offered by J. Stengel Consulting is designed for network administrators who are installing or have installed a WatchGuard XTM appliance. The class is applicable to all WatchGuard firewalls (Core, Edge, Peak, XTM 2, 5, 8, or 1050 series). The course is very hands on and students will configure and test each item in the labs. The last two days of this course go more in depth into specific deployment scenarios and advanced configuration. This gives students a full understanding of the firewall and its capabilities.

Registration:

Students can go to www.jstengel.net/trainingform.php to register and view available classes. They can also [call or email us](#) directly. Custom onsite classes are also available, [contact us](#) for more information.

Duration:

5 Days from 9:00am to 5:00pm with a 1 Hour Lunch Break. Friday, the last day, will wrap up early.

Materials:

Students will be furnished with a computer, XTM Firewall device, writing materials, and a training book (theirs to keep). Students don't need to bring anything to class.

Course Outline:

- Firewall Setup and Configuration
 - Quick Setup Wizard
 - Feature Keys
- Administration
 - Managing Your Firewall
 - Configuration Firewall's
 - Backing Up
 - Restoring
 - Changing Passphrases
- Configuring Network Settings
 - External Network Configuration
 - Trusted Interfaces
 - Optional Interfaces

- Secondary Networks
 - DHCP
 - DNS/Wins
 - Network Modes
 - Dynamic DNS
 - Network Bridges
- Network Address Translation – NAT
 - 1-to-1 NAT
 - Policy Based NAT
 - Static NAT
 - Dynamic NAT
 - Nat Loopback
- Traffic Management
 - Multi WAN Failover
 - Quality of Service
 - Traffic Prioritization
 - Limiting Bandwidth
- Policies
 - Policies and Rules
 - Packet Filter and Proxy Policies
 - Custom Templates
 - Policy Logging
 - Scheduling
 - Advanced Properties
- Authentication
 - Using Authentication to Secure your Network
 - Authentication Types
 - Firebox Database
 - Adding Users and Groups
 - Single Sign On
 - Authentication Values
- Proxy Policies
 - FTP Proxy
 - DNS Proxy
 - TCP/UDP Proxy
 - SIP Application Layer Gateway
 - H.323 Application Layer Gateway
- Email Proxies
 - SMTP
 - POP3
 - Protecting Your Email Server
- Blocking SPAM
 - Configuring SPAMBlocker
 - Quarantine Server

- Monitoring SPAM Activity
- Web Traffic
 - HTTP Proxy Policy
 - HTTPS Proxy Policy
 - HTTP Deep Packet Inspection
 - WebBlocker Configuration
 - Restricting Access to Web Sites by User and Group
 - Protecting Your Web Server
- Threat Protection
 - Intrusion Detection Measures
 - Packet Handling
 - Port Blocking
 - Hostile Sites and Automatically Blocking Bad IP's
- Signature Services
 - Gateway Anti-Virus Protection
 - Intrusion Prevention Protection
 - Protecting Against Spyware
- Logging
 - Log Server Configuration
 - Log Database Configuration and Encryption
 - Logging Traffic
 - Viewing and Interpreting Logs
- Monitoring Firewall Activity
 - Firebox System Manager
 - Using Traffic Monitor
 - Using HostWatch
 - Monitoring Firewall and Bandwidth Performance
- Reports
 - Report Server Configuration
 - Viewing and Running Reports
 - Archiving Reports
- Mobile VPN
 - PPTP Configuration
 - SSL Client VPN Configuration
 - IPSEC VPN Configuration
 - Restricting Access by VPN Clients
- Branch Office VPN
 - Manual BOVPN Configuration
 - Encrypting Traffic
 - Branch Office Gateways
 - Branch Office Tunnels
 - Restricting Access from BOVPN's
- Management Server
 - Configuring a management Server

- Role Based Administration
 - Configuring a managed Device
- Centralized Management
 - Device Configuration Templates
 - Scheduling OS Updates
 - Drag and Drop VPN's
 - VPN Resources
- Web UI
 - Accessing the Web UI
 - Managing the Firewall through the Web UI
 - Restricting Access
- Active Directory
 - Configuring Integrating Active Directory Authentication
 - Deploying Active Directory Authentication into Policies
 - Mobile VPN and Active Directory Authentication
 - Authentication and Policies
 - Single Sign On
 - Outbound Security and Active Directory
- Multi WAN
 - WAN Failover
 - Load Balancing
 - Policy Based Routing
 - User Load Balancing
 - Round Robin – Weighted Configuration
 - WAN Failover
 - Monitoring External Connections
- FireCluster – Students get 2 Firewall's for this Section
 - Configuring FireCluster
 - Active/Active Configuration
 - Active/Passive Configuration
 - Testing Cluster
 - Upgrading Cluster Firmware
 - Licensing
- Branch Office VPN's
 - Advanced BOVPN Configuration
 - BOVPN Policies
 - Vendor VPN Configurations
 - VPN's and Multi WAN Configuration
- VLAN's
 - Configuring VLAN's
 - Tagged and Untagged VLAN's
 - Securing Networks Through VLAN's