



FortiGate Multi-Threat Security Systems I

- Administration, Content Inspection and Basic VPN Access

Course 201-v3.0

Course Overview

FortiGate Multi-Threat Security Systems I is available as a 2-day instructor-led course, (public class or private on-site session) or a self-paced training course. The course provides an introduction to the configuration and administration of FortiGate Unified Threat Management appliances.

Through a variety of hands-on labs, students will learn about the most common features of the FortiGate unit.

Participants will gain a solid understanding of how to integrate the FortiGate unit into their existing environment, and the operational maintenance involved to ensure optimal performance and full protection of their corporate assets.

Course Objectives

Upon completion of this course, students will be able to:

- Use Web Config and CLI to complete administration and maintenance tasks for FortiGate devices including: system settings and network configuration; creation of administrative accounts; system back-ups; monitoring of system alerts, device performance and operational status; FortiGuard Distribution Network Services and updates; and firmware management to ensure availability and reliability.
- Implement logging and monitoring features of the FortiGate device using a FortiAnalyzer appliance for content archiving.
- Construct firewall policies with content inspection, schedules, source and service type restrictions, and log unauthorized traffic.
- Apply firewall policy options for authentication, virtual IP access, IP pool and traffic shaping.
- Create firewall protection profiles to implement FortiGate antivirus features such as file pattern blocking, grayware scanning, file quarantine, and antivirus scanning.
- Configure antisipam filtering using the subscription-based FortiGuard Antispam Service and banned word methods.



- Use FortiGate Web filtering features including URL filtering, content blocking and the FortiGuard Web Filtering Service.
- Understand the differences between NAT/Route and Transparent operational modes of the FortiGate unit.

Prerequisites

- Introductory-level network security experience
- Basic understanding of core network security and firewall concepts

Self-Paced Training Requirements:

- SOHO models only (FortiGate100A and lower)
- FortiOS 3.0 MR6 (b0660) firmware
- Valid FortiGuard Subscription Services license
- Available serial port on PC/laptop or USB to serial adaptor
- Internet connection

Who Should Attend

This introductory-level course is intended for anyone who is responsible for the day-to-day administration and management of a FortiGate unit.

Certification

This course helps to prepare students for the following certification exams:

- **Fortinet Certified Network Security Associate (FCNSA)**
- **Fortinet Certified Network Security Professional (FCNSP)**

Course Topics

AGENDA - Day 1

Lesson 1 – Overview and System Setup

- Unified Threat Management
- The Fortinet Solution

Fortinet, Inc. 1090 Kifer Road | Sunnyvale, CA 94086 | USA
Training Services: (613) 225-9381 Fax: (613) 225-2951
training@fortinet.com



- Firewall Basics
- FortiGate Appliances
- Device Administrations

Lesson 2 – FortiGuard Subscription Services

- FortiGuard Distribution Network
- FortiGuard Antivirus Service
- FortiGuard Intrusion Prevention System Service
- FortiGuard Web Filtering Service
- FortiGuard Antispam Service
- Enabling FortiGuard Subscription Services
- Configuring FortiGuard Subscription Services
- FortiGuard Center

Lesson 3 – Logging and Alerts

- Log Storage Locations
- Logging Levels
- Log Types
- Configuring Logging
- Viewing Log Files
- Content Archiving
- Alert Email
- SNMP

Lesson 4 – Firewall Policies

- Overview
- Policy Matching
- User Authentication to Firewall Policies
- Creating or Editing Policies

Lesson 5 – Basic VPN

- FortiGate VPN
- SSL VPN
- PPTIP VPN
- IPSec VPNs

Lesson 6 – Authentication

- Overview



- Authentication Methods
- Users and User Groups
- Authentication Settings
- PKI Authentication
- RADIUS Authentication
- LDAP Authentication
- TACACS+
- Windows Active Directory Authentication

AGENDA - Day 2

Lesson 7 – Antivirus

- Antivirus Elements
- File Filter
- Enabling File Filtering
- Virus Scan
- Grayware
- Quarantine
- Proxies
- Scanning Options

Lesson 8 – Spam Filtering

- Spam Filtering Methods
- FortiGuard Antispam
- Enabling Antispam
- Banned Word
- Black/White List
- Multipurpose Internet Mail Extensions (MIME) Headers Check
- DNS Blackhole List and Open Relay Database List
- FortiMail Antispam

Lesson 9 – Web Filtering

- Order of Filtering
- Web Content Block
- Web Content Block Exemption
- URL Filter
- FortiGuard Web Filter

