



FortiGate Multi-Threat Security Systems I Administration, Content Inspection and SSL VPN

Course 201 v4.1 (for FortiOS 4.0 MR2)

Course Overview

The **Administration, Content Inspection and SSL VPN** course 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 the FortiGate Unified Threat Management appliance.

Through a variety of hands-on labs, students will learn about the most commonly used 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:

- Describe the capabilities of the FortiGate Unified Threat Management appliance.
- Use Web Config and CLI to complete administration and maintenance tasks.
- Understand the basic differences between the NAT/Route and Transparent operational modes.
- Implement logging to a FortiAnalyzer appliance.
- Construct firewall policies to control traffic passing through the FortiGate unit.
- Define identity-based policies for authentication.
- Implement SSL VPNs to offer secure access to private networks.
- Configure updates to the FortiGuard Subscriptions Services.
- Implement threat management filtering including antivirus, email filtering, web filtering, data leak prevention, application control and endpoint control.



Prerequisites

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

Self-Paced Training Requirements:

- FortiGate SOHO-level device (FortiGate110C and lower)
- FortiOS 4.0 MR2 firmware
- Valid FortiGuard Subscription Services license
- Available serial port on PC/laptop or USB to serial adaptor
- Internet connectivity

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. Students must be familiar with the topics presented in this course before attending the FortiGate Multi-Threat Security Systems II - Secured Network Deployment and IPSec VPN course.

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
- Firewall Basics
- FortiGate Capabilities and Components
- Device Administration

Lesson 2 – Logging and Alerts



- Logging Levels
- Log Storage Locations
- Log Types
- Viewing Log Files
- Content Archiving
- Alert Email
- SNMP
- Reporting using a FortiAnalyzer device

Lesson 3 – Firewall Policies

- Policy Matching
- Firewall Policy Elements
- Identity-Based Policies
- Threat Management
- Traffic Shaping
- Load Balancing

Lesson 4 – Authentication

- Authentication Methods
- Authenticated Operations
- Users and User Groups
- Identity-Based Policies and Authentication Rules
- Monitoring Firewall Authentication

AGENDA - Day 2

Lesson 5 – SSL VPN

- FortiGate VPN
- SSL VPN Operating Modes
- User Groups
- Portals
- SSL VPN Firewall Policies

Lesson 6 – FortiGuard Subscription Services

- FortiGuard Distribution Network
- FortiGuard Antivirus Service
- FortiGuard Intrusion Prevention System Service



- FortiGuard Web Filtering Service
- FortiGuard Antispam Service
- FortiGuard Vulnerability Management Service
- FortiGuard Subscription Services Licensing
- Updating Antivirus and IPS Services
- Web Filtering and Antispam Options
- FortiGuard Center

Lesson 7 – Threat Management

- Content Scanning Techniques
- Threat Management Architectural Components

Lesson 8 – Antivirus

- Virus Types
- Antivirus Elements
- File Filters
- Virus Databases
- Grayware
- Quarantine
- Antivirus Profiles

Lesson 9 – Email Filtering

- Email Filtering Actions
- Email Filtering Methods
- FortiGuard Email Filters
- Banned Word
- IP Address Filtering
- Email Address Filtering
- Multipurpose Internet Mail Extensions (MIME) Headers Check
- DNS Blackhole List and Open Relay Database List
- Email Filter Profiles
- FortiMail Email Filtering

Lesson 10 – Web Filtering

- Web Filtering Elements
- URL Filter
- FortiGuard Web Filter
- Web Filtering Overrides
- Local Ratings



- Local Categories
- Web Content Filter
- Web Filter Profiles

Lesson 11 – Data Leak Prevention

- Monitored Data Types
- Data Leak Preventions Rules
- Data Leak Prevention Sensors

Lesson 12 – Application Control

- Application Types
- Application Control Lists

Lesson 13 – Endpoint Control

- Endpoint Network Access Control
- Application Sensors
- Endpoint NAC Profiles
- Vulnerability Scanning
- Monitoring Endpoints