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

Course Number 9214 – 16 Hours

Overview

The Administration, Content Inspection and SSL VPN course provides 2 days of instructor-led training where participants will gain an introduction to the configuration and administration of the FortiGate Unified Threat Management appliance.
The lecture and demonstration components of the classroom are presented by a Fortinet certified trainer. Through a variety of hands-on labs, students will learn about some of 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.

On Completion, Delegates will be able to

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.
- Enable authentication for local users
- Implement SSL VPNs to offer secure access to private networks.
- Implement threat management filtering including antivirus, email filtering, web filtering, data leak prevention, application control and endpoint control.

Who Should Attend

This introductory-level course is intended for anyone who is responsible for the day-today 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.

Prerequisites

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

Course Contents

Introduction to Fortinet Unified Threat Management

- Unified Threat Management
- The Fortinet Solution
- FortiGate Capabilities and Components
- Device Administration
- Initial Device Configuration

Logging and Monitoring

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

Firewall Policies

- Policy Matching
- Firewall Policy Elements
- Identity-Based Policies
- Threat Management
- Traffic Shaping
- Load Balancing
- Virtual IPs
- Denial of Service Policies
- Object Tagging

Local User Authentication

- Authentication Methods
- Authentication Groups
- Local and Remote Users
- User Groups
- Identity-Based Policies
- Authentication Rules
- Disclaimers
- Password Policies
- Two-Factor Authentication
- FortiToken Administration

SSL VPN

- FortiGate VPN
- SSL VPN Operating Modes
- User Groups
- Portals
- SSL VPN Firewall Policies
- Client Integrity Checking

Antivirus

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

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

Web Filtering

- Web Filtering Elements
- Web Content Filter
- Flow-based Web Filtering
- URL Filters
- FortiGuard Web Filter
- Web Filtering Quotas
- Overrides
- Local Ratings
- Local Categories
- Web Filter Profiles

Data Leak Prevention

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

- File Type/Pattern Filtering

Application Control

- Application Types
- Application Control Lists
- Application Control Profiles

Endpoint Control

- Endpoint Detection Lists
- FortiClient Compliance
- Application Detection
- Endpoint Control Profiles
- Vulnerability Scanning
- Monitoring Endpoints