FortiGate Multi-Threat Security Systems I

Administration, Content Inspection and SSL VPN
Course #201
Course Overview

Through this 3-day instructor-led classroom participants learn the basic configuration and administration aspects of the most commonly used features on the FortiGate Unified Threat Management (UTM) Appliance. Through interactive modules, participants explore firewall policies, user authentication, VPNs, virus detection, email filtering, web filtering, application control and more. FortiGate unit administrative fundamentals provide a solid understanding of how to integrate and ensure operational maintenance for optimal performance in the corporate environment.

Course Objectives

At the conclusion of this course, participants will be able to:
» Describe the capabilities of the FortiGate Unified Threat Management appliance
» Use the web management interface and CLI to complete administration and maintenance tasks
» Understand the basic differences between the NAT/Route and Transparent operational modes
» Enable logging, read and interpret different event log entries
» Create firewall policies for any situation to control traffic passing through the FortiGate unit
» Work through a list of configuration situations and identify the firewall policies and settings needed
» Enable authentication for local users
» Implement SSL VPNs to offer secure access to private networks
» Configure a working IPSec VPN tunnel between two FortiGate devices in policy and tunnel-based mode
» Implement threat management filtering including antivirus, email filtering, web filtering, and application control

Products Used in This Course

- FortiGate VM

Prerequisites

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

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.

AGENDA - Day 1

Module 1: Introduction to Fortinet Unified Threat Management

This module introduces students to the FortiGate unit, comparing and describing the essential FortiGate features, as compared to other firewall devices. Feature usage and their order of operations are explained and students examine how these can affect system performance and resources. Finally this module will cover configuration backup and restore, factory default settings and establishing connectivity to the FortiGate device GUI.

Objectives

At the conclusion of this module, participants will be able to:
» Identify major features of the FortiGate Unified Threat Management appliance
» Access and use the FortiGate unit's administration interfaces
» Create Administrators
» Work with examine configuration files (backup, restore, identify config file problems)

Topics

- Introduction to Unified Threat Management
- The Fortinet Solution
- FortiGate Appliance Capabilities and Components
- Device Administration (Firmware Upgrade, Downgrade)
- Administrator Users
- Initial Device Configuration (IPs, Gateway, DHCP, DNS)

Module 2: Logging and Monitoring

This module familiarizes students with how to search various logs from the FortiGate device GUI and understand how these logs are used. Different methods of logging will be discussed (both on and off the device), as well as getting information from the logs that may not be initially visible.

Objectives

At the conclusion of this module, participants will be able to:
» Define the storage location for log information
» Enable logging for different FortiGate unit events
» View and search logs
» Monitor log activity
» Understand RAW log output
» Customize widgets on the dashboard

Topics

- Logging Severity Levels
- Log Storage Locations
- Log Types and Subtypes
- Structure and Behavior of Logs
- Traffic Log Generation
- Viewing Logs (Log Viewer Filtering, Raw Logs)
- Alert Email

- SNMP
- Event Logging
- Monitoring
- Customizing Status Widgets (GUI)

Module 3: Firewall Policies

This module demonstrates setting up the Firewall policies on a FortiGate device and explains the logic for how a match on a firewall policy is determined.

Objectives

At the conclusion of this module, participants will be able to:

» Identify the components used in a firewall policy
» Create firewall objects
» Create Address and Device Identity policies and manage the order of their processing
» Monitor traffic through policies

Topics

- Firewall Policies (Types, Subtypes, Actions)
- Device Identification (Bring Your Own Device - BYOD)
- Firewall Address Objects, Interfaces, Service Objects
- Traffic Logging
- Network Address Translation (Source NAT)
- NAT Dynamic IP Pool (Source NAT)
- Central NAT
- Traffic Shaping
- Source NAT IP Address and Port
- Fixed Port (Source NAT)
- Virtual IPs (Destination NAT)
- Threat Management
- Denial of Service Policies
- Endpoint Control
- Firewall Policy Object Management (Object Tagging)
- Monitoring Policies

AGENDA - Day 2

Module 4: Local User Authentication

This module familiarizes students with utilizing Identity based policies.
The focus will be on setting up and manipulating traffic based on authentication using local users.

Objectives

At the conclusion of this module, participants will be able to:

» Describe available FortiGate device authentication mechanisms
» Create local users and user groups

» Create identity-based policies to enable local user authentication
» Monitor active users
» Check authentication Log entries

Topics

- Local User Authentication
- User Authentication via Remote Server
- User Authentication Groups
- Identity-Based Policies
- Disclaimers
- Password Policies
- Two-Factor Authentication
- Policy Configuration
- User Monitor

Module 5: SSL VPN

In this module students learn how to configure and connect to an SSL VPN.

Objectives

At the conclusion of this module, participants will be able to:
» Identify the VPN technologies available on the FortiGate device
» Configure the FortiGate device's SSL VPN operating modes
» Define user restrictions
» Setup SSL VPN portals
» Configure firewall policies and authentication rules for SSL VPNs

Topics

- Virtual Private Networks
- FortiGate Device VPNs
- SSL VPN Operating Modes (Web-Only, Tunnel)
- User Groups
- Authentication
- SSL VPN Server Certificate
- Encryption Key Algorithm
- Web Portal Interface
- Full-Access Web Portal Interface
- Tunnel Mode Split-Tunnelling
- Client Checking (Integrity Checks, Host Checks)
- Tunnel Mode Connection
- Client Port Forward
- Policy De-Authentication
- Access Modes (Web Mode, Tunnel Mode, Port Forward Mode)
- SSL VPN Configuration

Module 6: IPSec VPN

The students will be shown how to configure an IPSec VPN on the FortiGate device using Interface-based and policy-based modes.

Objectives

At the conclusion of this module, participants will be able to:

» Define the architectural components of IPSec VPN
» Define the protocols used as part of an IPSec VPN
» Identify the phases of Internet Key Exchange (IKE)
» Identify the FortiGate unit IPSec VPN modes
» Configure IPSec VPN on the FortiGate unit

Topics

- IPSec VPN
- Internet Key Exchange
- Defining Phase 1 and Phase 2 Parameters
- IPSec VPN Modes (Interface Mode, Tunnel Mode)
- Overlapping Subnets
- IPSec Topologies
- IPSec VPN Monitor
- IPSec VPN Configuration

AGENDA - Day 3

Module 7: Antivirus

This section will teach students how to configure and enable traffic scanning for the detection of viruses.

Objectives

At the conclusion of this module, participants will be able to:

» Describe conserve mode conditions and AV system behavior
» Define the virus scanning techniques used on the FortiGate unit
» Identify the differences between file-based and flow-based virus scanning
» Configure quarantine options
» Define firewall policies using antivirus profiles
» Update FortiGuard Services

Topics

- Conserve Mode
- Antivirus Fail-Open
- Antivirus Overview
- Scanning Order
- Proxy-based Scanning
- Flow-based Scanning
- Virus Databases
- Unknown and Known Viruses

- Heuristic Scanning
- Antivirus Profiles
- UTM Proxy Options
- Quarantine
- Logging

Module 8: Email Filtering

This module will introduce students to email inspection and spam detection.

Objectives

At the conclusion of this module, participants will be able to:

» Identify the email filtering methods used on the FortiGate device

» Configure banned word, IP address and email address filters

» Define firewall policies using email filter profiles

» Identify the differences between the email filtering capabilities of the FortiGate and FortiMail units

Topics

- Email Filtering
- Spam Actions
- Email Filtering Methods
- Email Filtering Order of Operations (SMTP)
- Email Filtering Order of Operations (POP)
- FortiGuard IP (Address, URL, Email Address and Email Checksum Check)
- IP Address Black/White List (BWL)
- Email Address Black/White List
- HELO DNS Lookup
- Return Email DNS Check
- Banned Word Check
- MIME Headers Check
- DNSBL and ORDBL Check
- Dealing with False Positives
- FortiGuard Email Filtering Options
- Email Filter Profile

Module 9: Web Filtering

This module introduces students to the web filtering functions available on the FortiGate unit.

Objectives

At the conclusion of this module, participants will be able to:

» Identify the web filtering mechanisms used on the FortiGate device

» Create web content and URL filters

» Configure FortiGuard Web Filtering

» Configure FortiGuard Web Filtering exemptions and rating overrides

» Define firewall policies using web filter profiles

Topics

- Web Filtering Overview
- Types of Web Filtering (Proxy-based, Flow-based, DNS-based)
- Web Filtering Activation
- HTTP Inspection Order
- Web Content Filtering
- Web URL Filtering
- Forcing Safe Search
- FortiGuard Category Filter
- FortiGuard Caching, Usage Quotas, Rating Submissions and Rating Overrides
- Local Categories
- Filtering Actions (Warning, Authenticate)
- Web Filter Profiles

Module 10: Application Control

This module teaches Students the inner workings of Application Control, how to configure it, and how signature triggers are accomplished.

Objectives

At the conclusion of this module, participants will be able to:

» Configure application control

» Create firewall policies using application control lists

» Define application control operation and best practices

Topics

- Application Control Overview
- Application Control Lists
- Application Control Profiles
- Order of Operations
- Implicit Rules
- Creating Filter Rules
- Application Categories
- Proper Identification
- Functional Overview (Under the Hood)
- Peer-to-Peer Detection