



## **FortiGate Multi-Threat Security Systems II Secured Network Deployment and IPSec VPN**

### **Course 301 v4.1 (for FortiOS 4.0 MR2)**

#### **Course Overview**

The **Secured Network Deployment and IPSec VPN** course provides 3 days of instructor-led training (in a public or private on-site class setting) where participants will gain a comprehensive understanding of the advanced networking and security features of FortiGate Unified Threat Management security appliances.

Hands-on labs allow students to perform the tasks associated with the configuration and troubleshooting of virtual domains, routing, WAN optimization, high availability, IPS, authentication and IPSec VPNs.

This course demonstrates features that can be easily adapted when planning a secure network deployment using FortiGate Unified Threat Management appliances.

This advanced-level course is a continuation of the topics discussed in FortiGate Multi-Threat Security System I – Administration, Content Inspection and SSL VPN (Course 201).

#### **Course Objectives**

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

- Construct virtual domains and configure inter-VDOM routing.
- Use the built-in FortiOS diagnostic tools for troubleshooting and performance monitoring.
- Enable logging to a FortiAnalyzer device.
- Configure static and policy routing.
- Implement FortiGate traffic optimization techniques.
- Configure IPS protection to protect network resources from attack.
- Control access to network resources by enabling LDAP or Directory Services authentication.
- Debug IKE exchanges to troubleshoot connection negotiations.
- Create IPSec VPNs to permit client access to a FortiGate VPN gateway.
- Set up a high availability cluster configuration.



## Products Used in This Course

- FortiGate, FortiAnalyzer and FortiClient

## Prerequisites

- Previous experience working with the FortiGate Unified Threat Management device.
- Solid knowledge of the Web Config administrative interface and the FortiGate Command Line Interface.
- Knowledge of dynamic routing protocols, IPSec VPNs, and intrusion detection concepts.
- Completion of FortiGate Multi-Threat Security System I – Administration, Content Inspection and SSL VPN (Course 201) is highly recommended.

## Who Should Attend

This course is intended for networking professionals involved in the design and implementation of a security infrastructure using FortiGate Unified Threat Management appliances. This advanced-level course is a continuation of the topics discussed in FortiGate Multi-Threat Security System I – Administration, Content Inspection and SSL VPN (Course 201). Content in the 301 course is geared to professionals with a sound knowledge of the concepts involved in the operation of a FortiGate device. It is assumed that students are familiar with the topics presented in the 201 course.

## Certification

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

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

## Course Topics

AGENDA - Day 1

### Lesson 1 – Virtual Networking

- VLANs on a FortiGate Unit
- Global and Virtual Domain Configuration Settings
- Configuring Virtual Domains
- Inter-VDOM Links



## **Lesson 2 – Diagnostics**

- Diagnostic commands
- Self Help Options

## **Lesson 3 – Routing**

- NAT/Route Mode
- Static Routes
- Policy Routes
- Dynamic Routing
  - Routing Information Protocol
  - Open Shortest Path First
  - Border Gateway Protocol
- Multicast Routing

## **AGENDA - Day 2**

## **Lesson 4 – Traffic Optimization**

- FortiGate WAN Optimization Techniques
- Configuring WAN Optimization
- Configuring Web Cache
- WCCP v2 Support
- Monitoring WAN Optimization

## **Lesson 5 – Intrusion Prevention System**

- IPS Signatures
- IPS Sensors
- Attack Types
- Monitoring IPS Attacks

## **Lesson 6 – LDAP Authentication**

- Directory Configuration
- LDAP Authentication



## **Lesson 9 – Directory Services Authentication**

- Fortinet Server Authentication Extensions
- Configuring FSAE on Windows Active Directory
- Configuring FSAE on FortiGate Units

### AGENDA - Day 3

## **Lesson 9 – IPSec VPN**

- IPSec Architecture
- IPSec Protocols
- Internet Key Exchange
- IPSec VPN Modes
- Configuring IPSec VPN
- Internet Browsing
- IPSec VPN Monitor
- Overlapping Subnets
- IPSec Debugging
- VPN Troubleshooting Tips

## **Lesson 10 – High Availability**

- High Availability Clusters
- High Availability Modes of Operation
  - Active-Passive
  - Active-Active
- FortiGate Clustering Protocol
  - Virtual Addresses
  - FGCP Heartbeat
  - Heartbeat Interfaces
  - HA Configuration Synchronization
- Load Balancing
- Failover
- Virtual Clustering
- Session Synchronization



## **Lesson 11 – Transparent Mode**

- Operating Modes
- Ethernet Frame and VLAN Tags
- VLANs on a FortiGate Unit Operating in Transparent Mode
- Transparent Bridge
- Broadcast Domains
- Forwarding Domains
- Spanning Tree Protocol
- Link Aggregation