# FortiGate Multi-Threat Security Systems II

Secured Network Deployment and IPSec VPN
Course #301

## Course Overview

Through this 3-day instructor-led classroom or online virtual training, participants will gain a comprehensive understanding of the advanced networking and security functions of FortiGate Unified Threat Management (UTM) appliances. With a focus on core feature skills, specific topics include routing, virtual domains, transparent mode, high availability, advanced IPSec VPN, intrusion prevention system, single sign on, certificate operations, data leak prevention, advanced application control and resource utilization. At the end of this course, students complete an interactive in-lab assessment of skills learned.

Designed to demonstrate advanced use of FortiGate UTM appliance features, this training is a continuation of the FortiGate Multi-Threat Security System I Course.

At the conclusion of this course, participants may take a proctored exam and earn a Fortinet Certified Network Security Professional (FCNSP) status. This industry-recognized certification has many benefits that include: Direct access to Level II Fortinet Technical Support; Beta program participation; and FCNSP Logo usage.

## Course Objectives

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

- Describe various routing operations, configure policy routing and execute diagnostic commands to monitor routes and troubleshoot problems
- Set up virtual domains and configure inter-VDOM routing between two FortiGate units
- Configure a FortiGate unit in Transparent Mode
- Implement a high availability cluster configuration using two FortiGate devices and use diagnostics and debug commands to troubleshoot and monitor HA operations
- Configure a Hub-Spoke and partial meshed VPN as well as execute diagnostics to troubleshoot and monitor IKE exchanges
- Work with intrusion prevention system (IPS) profiles as well as denial of service (DoS) policies to protect network resources from attack
- Use diagnostics and logging to monitor proper use of IPS
- Describe Fortinet Single Sign On (FSSO) communications and configure FSSO to allow the FortiGate unit to collect authentication information from Windows Active Directory
- Prepare the FortiGate unit for SSL-based inspection as well as understand details of how inspection is performed, general layout of a certificate and how encryption functions are used

**Fortinet, Inc.** 1090 Kifer Road | Sunnyvale, CA 94086 | USA
Training Services: 1-866-868-3678 Fax: (613) 225-2951
training@fortinet.com

- Use data leak prevention rules and sensors to block and archive the transmission of sensitive data outside the network
- Work with advanced functions of application control including traffic shaping and instant messaging inspection as well as use diagnostics commands for troubleshooting and performance monitoring

## Products Used in This Course

- FortiGate appliance
- FortiClient

## Prerequisites

- Previous experience working with FortiGate UTM appliances
- Solid knowledge of the web management interface and the FortiGate unit Command Line Interface (CLI)
- Knowledge of dynamic routing protocols, IPSec, VPNS and intrusion detection concepts
- Successful completion of the FortiGate Multi-Threat Security System I course is highly recommended

## System Requirements

If this training is performed online, students will require the following:

- A high-speed Internet connection
- A Web browser that supports the Adobe Flash Player to launch the Virtual Classroom
- Speakers or a headset to follow along with the audio portion of the presentation
- Adobe Reader to view class materials

## 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)

# AGENDA - Day 1

## Module 11: Routing

This module introduces students to the logic used behind FortiGate device routing decisions. Students will learn how to read routing table entries, perform routing diagnostics and create routes on a FortiGate device.

**Objectives**

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

- Interpret routing information in the routing table
- Execute and interpret routing diagnostics

**Topics**

- Routing Table Elements
- Viewing Routing Information
- Route Selection Process
- Routing Table Refresh
- Policy Routing
- Black hole Routes
- Reverse Path Forwarding
- Equal Cost Multipath
- Dead Gateway Detection
- Reverse Path Forwarding Modes
- Strict Reverse Path Forwarding
- Dynamic Routes
- Multicast Routing
- Routing Diagnostic Commands
- Packet Sniff Command

## Module 12: Virtual Networking

This module introduces the concept of working with virtual network resources including VLANs, virtual domains and link aggregation.

**Objectives**

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

- Understand the use of virtual LANs (VLANs)
- Create VLAN sub interfaces on the FortiGate unit
- Understand the use of virtual domains (VDOMs)
- Create virtual domains
- Add administrators specific to virtual domains
- Configure inter-VDOM links

**Topics**

- Virtual Local Area Networks
- VLAN Tags
- VLANs on a FortiGate Appliance
- Virtual Domains and Settings
- Enabling Virtual Domains
- Accessing a Virtual Domain Configuration
- VDOM Resource Limits
- Per-VDOM Configurations
- Virtual Domain Administrators
- Inter-VDOM Links
- Independent VDOM Configuration
- Management VDOM Configuration
- Meshed VDOM Configuration

## Module 13: Transparent Mode

This module familiarizes students with operating a FortiGate appliance in transparent mode and discusses aspects to consider in this type of deployment.

**Objectives**

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

- Describe FortiGate unit operating modes
- Describe how VLANs are used on a FortiGate unit operating in Transparent Mode
- Configure a VDOM in Transparent Mode

**Topics**

- Operating Modes
- NAT/Route Mode
- Transparent Mode
- Forwarding Domain
- VLANs on a FortiGate Unit in Transparent Mode
- Port Pairing
- Transparent Bridge
- Broadcasting Domain
- Forwarding Domain
- Spanning Tree Protocol
- Link Aggregation

## Module 14: High Availability

This module discusses the functionality of a FortiGate unit operating in HA mode.

**Objectives**

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

- Identify the components in a FortiGate high availability (HA) cluster
- Describe the FortiGate HA modes of operation
- Define the failover methods used in FortiGate HA mode
- Configure session synchronization
- Configure a FortiGate HA cluster

**Topics**

- High Availability Overview
- Cluster Membership
- Cluster Units
- Primary Unit Selection
- Viewing Cluster Members
- Modes of Operation (Active-Passive, Active-Active)
- Primary Unit (Master)
- Subordinate Unit (Slave)
- Workload
- Subordinate Unit Failure
- FortiGate Clustering Protocol
- Virtual MAC Addresses and Failover
- FGCP Heartbeat
- Heartbeat Interfaces and IP Addresses
- HA Configuration Synchronization
- Load Balancing AV Scan Sessions SYN
- Device Failover
- Link Failover
- Session Failover
- Virtual Clustering
- Firmware Upgrades
- Full Mesh HA

# AGENDA - Day 2

## Module 15: Advanced IPSec VPN

This module covers the advanced methods of VPN deployment (hub and spoke, star, full and partial meshed configurations), PPTP and in depth troubleshooting diagnostics.

**Objectives**

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

- Configure dialup VPN access
- Implement advanced topologies
- Debug IPSec communications

**Topics**

- Dialup VPN
- IPSec Topologies
- Hub-and-Spoke VPN
- Full/Martial Mesh VPN
- FortiGate Device and Third-Party VPN
- VPN Tunnel Name Behavior
- Hub-and-Spoke Working Example
- IPSec Debugging
- VPN Troubleshooting

## Module 16: Intrusion Prevention System

This module provides a detailed look at the configuration and operating behavior of the FortiGate appliance's intrusion prevention system.

**Objectives**

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

- Use the FortiGate intrusion prevention system (IPS) to detect network intrusions
- Create IPS filters and sensors
- Design firewall policies that incorporate IPS sensors
- Create denial of service (DoS) sensors and interface policies

**Topics**

- Intrusion Prevention System Overview
- Protocol Decoders
- Predefined Signatures
- FortiGuard Intrusion Prevention System Service
- Custom Signatures
- Custom Signature Syntax and Examples
- IPS Sensors and Filters
- IPS Overrides
- Denial of Service Attacks
- Denial of Service Policies
- SYN Flood Attacks
- ICMP Sweep
- DDoS Attacks
- Logging
- One-Arm (Sniffer)

## Module 17: Fortinet Single Sign On (FSSO)

In this module, Fortinet Single Sign On communications are explained and students will learn how to configure FSSO to link domain log in credentials to firewall policies in order to restrict access.

**Objectives**

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

- Describe how domain login credentials can be used to authenticate users to the FortiGate device
- Configure Fortinet Single Sign On (FSSO)

**Topics**

- Directory Services Authentication
- FSSO Overview
- FSSO Components
- FSSO Domain Controller Agent Mode
- FSSO Polling Mode
- FSSO Using NTLM Authentication

**Fortinet, Inc.** 1090 Kifer Road | Sunnyvale, CA 94086 | USA
Training Services: 1-866-868-3678 Fax: (613) 225-2951
training@fortinet.com

## Module 18: Certificate-Based Operations

This module lays the groundwork for all SSL based inspection that a FortiGate appliance is capable of performing.

**Objectives**

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

- Define how cryptography is used to secure information from unintended audiences
- Identify the information stored in a digital certificate
- Describe how digital certificates are used for authentication on the FortiGate unit
- Create a certificate request and submit the request to an authorized CA
- Import digital certificates onto the FortiGate unit
- Describe how SSL content inspection is performed

**Topics**

- Cryptography Overview
- Symmetric and Asymmetric Cryptography
- Diffie-Hellman
- Digital Certificates
- Secure Socket Layer Security
- Generating a Certificate Request
- Importing Certificates
- Importing the CA Certificate
- Backing Up and Restoring Certificates
- Certificate Revocation List
- SSL Content Inspection
- Purpose of a Certificate
- Enabling SSL Inspection

# AGENDA - Day 3

## Module 19: Advanced Application Control

This module describes some of the more advanced deployment options that are available with the application control function. Students will look at how application control can be combined with traffic shaping and also set up a configuration to restrict instant messenger access.

**Objectives**

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

- Allow and fine tune instant messenger access
- Use application control to apply traffic shaping

**Topics**

- Instant Messenger
- Fine Tuning Instant Messenger
- Instant Messenger Users
- Monitoring
- Traffic Shaping Working Example
- Investigating Lack of Resources
- Memory Diagnostics
- AV/IPS Troubleshooting
- Process State
- CPU Troubleshooting
- Testing Hardware and Memory
- Loading a Test Image

**Fortinet, Inc.** 1090 Kifer Road | Sunnyvale, CA 94086 | USA
Training Services: 1-866-868-3678 Fax: (613) 225-2951
training@fortinet.com

## Module 20: Data Leak Prevention

This module will introduce students to working with the data leak prevention (DLP) feature including configuration, methodology, diagnostics, and debugging.

**Objectives**

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

- Identify the data types that can be monitored through FortiGate DLP
- Define regular and compound rules
- Define DLP sensors
- Define firewall policies using DLP sensors

**Topics**

- Data Leak Prevention Overview
- File Type Filtering
- File Name Pattern
- Message Filter
- File Filter List
- Document Fingerprinting
- DLP Archiving
- Data Leak Prevention Profile

**Fortinet, Inc.** 1090 Kifer Road | Sunnyvale, CA 94086 | USA
Training Services: 1-866-868-3678 Fax: (613) 225-2951
training@fortinet.com

## Module 21: Putting It All Together

In this module, students will be given an opportunity to put their skills to the test. This multi-part interactive lab assesses the student's ability to work with multiple FortiGate features at once to fulfill a set of customer needs and requirements.

**Objectives**

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

- Configure a combination of FortiGate features to satisfy a given scenario including Web Filtering, Authentication, IPS, Antivirus, Email Filtering, Application Control and more…

**Fortinet, Inc.** 1090 Kifer Road | Sunnyvale, CA 94086 | USA
Training Services: 1-866-868-3678 Fax: (613) 225-2951
training@fortinet.com