

## Fortinet 301 – Secured Network Deployment and IPSec VPN

---

### Course Summary

#### Description

This course provides two days of instructor-led training where participants will gain a comprehensive understanding of the advanced networking and security features of FortiGate Unified Threat Management security appliances. The lecture and demonstration components of the classroom are presented by a Fortinet-certified trainer. Hands-on labs allow students to perform the tasks associated with the configuration and troubleshooting of virtual domains, routing, WAN optimization, high availability, IPS, remote user authentication, Fortinet Single Sign On 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 201 – Administration, Content Inspection and SSL VPN.

#### 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.
- Configure static and dynamic routing.
- Define identity-based policies for authentication.
- Control access to network resources by enabling LDAP and Directory Services authentication.
- Configure IPS protection to protect network resources from attack.
- Create IPSec VPNs to permit client access to a FortiGate VPN gateway.
- Debug IKE exchanges to troubleshoot connection negotiations.
- Set up a high availability cluster configuration.
- Configure a FortiGate unit in Transparent Mode.
- Implement FortiGate traffic optimization techniques.

#### Topics

- |                               |                                |
|-------------------------------|--------------------------------|
| • Virtual Networking          | • Certificate-Based Operations |
| • Diagnostics                 | • IPSec VPN                    |
| • Routing                     | • Transparent Mode             |
| • Intrusion Prevention System | • WAN Optimization             |
| • Remote User Authentication  | • Wireless                     |
| • Fortinet Single Sign On     | • High Availability            |

#### Audience

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.

#### Prerequisites

Students should have previous experience working with the FortiGate Unified Threat Management device and 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 Fortinet 201 – Administration, Content Inspection and SSL VPNs is high recommended.

#### Duration

Three days

## Fortinet 301 – Secured Network Deployment and IPsec VPN

### Course Outline

- I. *Virtual Networking*
  - A. VLANs on a FortiGate Unit
  - B. Global and Virtual Domain Configuration Settings
  - C. Virtual Domains
  - D. VDOM Resource Limits
  - E. Inter-VDOM Links
- II. *Diagnostics*
  - A. Diagnostic Commands
  - B. Packet Sniffing
  - C. Self Help Options
- III. *Routing*
  - A. Routing Tables
  - B. Route Elements
  - C. Static and Policy Routes
  - D. Route Selection
  - E. Reverse Path Forwarding
  - F. Dynamic Routing (Routing Information Protocol, Open Shortest Path First, Border Gateway Protocol, Intermediate System to Intermediate System)
  - G. Multicast Routing
  - H. Routing Diagnostics
- IV. *Intrusion Prevention System*
  - A. IPS Signatures
  - B. IPS Sensors
  - C. Filters
  - D. IPS Overrides
  - E. Attack Types
  - F. Monitoring IPS Attacks
- V. *Remote User Authentication*
  - A. RADIUS Authentication
  - B. Dynamic Profiles
  - C. LDAP Authentication
  - D. TACACS+ Authentication
  - E. Digital Certificate Authentication
  - F. Directory Services Authentication
- VI. *Fortinet Single Sign On*
  - A. Directory Services Authentication
  - B. Fortinet Single Sign On Components
  - C. Fortinet Single Sign On Modes
  - D. NTLM Authentication
- VII. *Certificate-Based Operations*
  - A. Introduction to Cryptography
  - B. Secure Socket Layer Security
  - C. Certificate authentication
  - D. SSL Content Inspection
- VIII. *IPsec VPN*
  - A. IPsec Architecture and Protocols
  - B. Internet Key Exchange
  - C. IPsec Phase 1 and Phase 2
  - D. IPsec VPN Modes
  - E. IPsec Topologies
  - F. Configuring Route-Based and Policy-Based VPNs
  - G. IPsec VPN Monitor
  - H. Overlapping Subnets
  - I. IPsec Debugging
  - J. VPN Troubleshooting Tips
- IX. *Transparent Mode*
  - A. Operating Modes
  - B. Ethernet Frame and VLAN Tags
  - C. VLANs on a FortiGate Unit Operating in Transparent Mode
  - D. Port Pairing
  - E. Transparent Bridge
  - F. Broadcast Domains
  - G. Forwarding Domains
  - H. Spanning Tree Protocol
  - I. Link Aggregation
- X. *WAN Optimization*
  - A. FortiGate WAN Optimization Techniques
  - B. WAN Optimization Rules
  - C. WAN Optimization Modes
  - D. Web Caching
  - E. Transparent Proxy
  - F. WCCP v2 Support
  - G. Monitoring WAN Optimization
- XI. *Wireless*
  - A. Wireless Concepts
  - B. Thick and Thin Access Points
  - C. FortiGate Wireless Controllers
  - D. Managed AP Topologies
  - E. Controller Discovery
  - F. Virtual Access Points
  - G. Guest Networks
  - H. Wireless Security Modes
  - I. Access Point Profiles
  - J. Rogue Access Point Detection
  - K. Wireless Roaming

## Fortinet 301 – Secured Network Deployment and IPSec VPN

---

### Course Outline (cont)

#### *XII. High Availability*

- A. High Availability Clusters
- B. High Availability Modes of Operation (Active-Passive, Active-Active)
- C. FortiGate Clustering Protocol (Virtual Addresses, FGCP Heartbeat, Heartbeat Interface, HA Configuration Synchronization)
- D. Virtual MAC Addresses
- E. Load Balancing
- F. Failover
- G. Virtual Clustering
- H. Session Synchronization
- I. Firmware Upgrades