

## **Implementing FortiGate Security and Content Inspection**

**Course 925-201b**  
**3 Day – Hands on**  
**(Replaces 925-201)**

### **Certification:**

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

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

### **Prerequisites:**

Before attending this course, students should have knowledge of the following topics:

- TCP/IP Networking
- Network security
- Firewall concepts
- Virtual Private Networks (IPSec and PPTP)
- Email (SMTP, POP3, IMAP) and web (HTTP) basics
- Intrusion detection and prevention basics

### **Objective:**

Upon completion of this course students will have the comprehensive knowledge and lab experience required to implement a variety of security services in medium to large enterprise networks using FortiGate devices. Through a series of practical hands on labs, students will have the opportunity to configure various FortiGate devices focusing on initial setup and firewall policy configuration, through to web and email filtering (content inspection) and more advanced topics such as dual Internet connections, site-to-site and dial-up IPSec VPN tunnel configuration, and High Availability.

During this three-day class students will work with Fortigate-60's, and larger SMB models (Fortigate-300 to FortiGate-800) as well as with the FortiLog-100 logging system, gaining valuable experience that can then be applied to the specific FortiGate models in their production and lab environments.

## Detailed Outline:

### Day One: Setup, Policies and IPS

- Initial Setup and Configuration of a FortiGate
  - Interface configuration
  - Setting up DHCP Services
  - Configuring additional parameters such as timeouts, time zones, NTP, default routes, etc.
  - Upgrading system Firmware
  - Configuring Logging
  - NAT/Route Mode Operation
- Transparent Mode Operation
- Virtual LANs
- Virtual Domains
- Creating and Configuring Policies
  - Firewall Policies
  - Policy Routing
  - Policy Ordering
  - User Groups and Authentication
  - Troubleshooting Policies
- Intrusion Prevention System (IPS)
  - Traffic Signatures
  - Custom Signatures
  - Signature Updates and the FortiProtect Distribution Network (FDN)
  - FortiLog IPS Reports

## Day 2: Content Inspection

- SPAM Filters
  - Configuring SPAM Filters
  - FortiGuard AntiSPAM Service
  - Protection Profiles for AntiSPAM
  - FortiLog Mail Reports
  
- Web Filters
  - Configuring Web Filters
  - FortiGuard URL Categorization Service
  - Protection Profiles for Web Filtering
  - FortiLog Web Filter and Traffic Logs
  
- Anti-Virus Protection
  - Configuring Anti-Virus Protection
  - Virus Detection
  - Greyware Detection
  - Configuring Oversize Thresholds
  - Updates and FortiProtect Distribution Network
  - Protection Profiles for Anti-Virus Protection
  - FortiLog Anti-Virus Reports
  
- Configuring Alert e-mails and Replacement Messages

### **Day 3: Virtual Private Networks & High Availability**

- Virtual Private Networks
  - FortiGate VPN Overview
  - IPSec Dial-up VPNs
  - IPSec Site to Site VPNs
  - PPTP VPNs
  - AV Scanning of VPN Tunnels
  - FortiLog VPN Activity Reports
  
- High Availability
  - FortiGate HA Overview
  - HA Configuration (Active-Active / Active-Passive)
  - HA – VPN Fail Over
  - Cluster Creation Best Practices