



FortiGate Multi-Threat Security Systems II

-Secured Network Deployment & Virtual Private Networks

Course Number: 301

Duration: 2 days

Products Covered:

This course provides training on the following Fortinet products:

- **FortiGate**
- **FortiAnalyzer**
- **FortiClient**

Certification:

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

Fortinet Certified Network Security Professional (FCNSP)

Prerequisites:

- Course 201: FortiGate Multi-Threat Security Systems I

Detailed Course Outline:

- **Module 1: FortiGate Routing**
 - Policy Routing
 - Dynamic Routing
 - Static Route Priorities
 - Dual Internet Connections
 - Blackholes
- **Module 2: Virtual Domains (V-Doms)**
 - TP Mode Forwarding Domains
 - V-Dom Configuration and Management
 - Radius Authentication
 - Inter V-Dom Routing
- **Module 3: High Availability**
 - HA Clusters
 - Active-Passive Operation
 - Active-Active Operation
 - Virtual Clusters

- Module 4: IPS
 - IPS Signatures
 - IPS Network Anomalies
 - Severity Levels
 - Custom Signatures
 - Packet Logging
 - Vulnerability Tests
 - IPS and FortiAnalyzer
 - PEN Test Tools
 - IPS and VPNs
- Module 5: IPSec VPNs
 - Interface Based VPNs
 - Dynamic Routing
 - Redundant IPSec VPNs
 - Policy Based IPSec VPNs
 - Xauth
 - DHCP Over IPSec
 - Internet Browsing
 - FortiClient Dial-Up VPN
 - Hub & Spoke VPN Using Certificates
- Module 6: SSL VPNs
 - Tunnel Mode SSL VPNs
 - Authentication Groups
 - Web Mode SSL VPNs
- Module 7: Troubleshooting
 - Troubleshooting Methodology
 - System Diagnostic Commands
 - Session Table Analysis
 - Using the Built-in Packet Sniffer
 - FortiGate Flowchart for Troubleshooting
 - Log Analysis