



FortiGate Multi-Threat Security Systems Secured Network Deployment and Virtual Private Networks

Course 301 v4.0

Course Overview

The **Secured Network Deployment and Virtual Private Networks** course provides 3 days of instructor-led training (in a public or private on-site class setting) where participants will gain a comprehensive understanding 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, firewall policies, 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.

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 and configure reports.
- 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 authentication.
- Debug IKE exchanges to troubleshoot connection negotiations.
- Create a route-based and a redundant IPSec VPN to permit client access to a FortiGate VPN gateway.
- Set up a high availability cluster configuration and implement the virtual clustering feature of the FortiGate appliance.



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.

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 geared to professionals with a good knowledge of the concepts involved in the operation of a FortiGate device.

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 Local Area Networks and Virtual Domains

- 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 – Transparent Mode

- Operating Modes on the FortiGate Unit
- 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

Lesson 4 – Firewall Policies

- Creating Firewall Policies
- Virtual IPs
- Load Balancing
- Logging
- Reporting

AGENDA - Day 2

Lesson 5 – Routing

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



Lesson 6 – Traffic Optimization

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

Lesson 7 – Threat Management

- Content Scanning Techniques
- Threat Management Architectural Components
- Antivirus
- Intrusion Prevention System
- Web Filtering
- Spam Filtering
- Data Leak Prevention
- Application Control
- Content Archive
- NAC Quarantine
- SSL Content Inspection

AGENDA - Day 3

Lesson 8 – Advanced Authentication

- Authenticated Operations
- Identity-Based Policies
- User Groups
- Authentication Settings
- Monitoring User Authentication
- LDAP Authentication
- Certificate Authentication
- Directory Services Authentication



Lesson 9 – Virtual Private Networks

- SSL VPN
- IPSec VPN
- IPSec Architecture
- Internet Key Exchange
- IPSec Topologies
- IPSec VPN Modes
- Internet Browsing
- IPSec VPN Monitor
- Overlapping Subnets
- IPSec Debugging
- VPN Troubleshooting Tips

Lesson 10 – High Availability

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