FORTINET
TRAINING SERVICES

FortiGate Multi-Threat Security Systems II

Secured Network Deployment and IPSec VPN

Course 301 (for FortiOS 4.0 MR3 Patch 1)

Course Overview

The **Secured Network Deployment and IPSec VPN** course provides 3 days of instructor-led training (in a public or private on-site class setting) 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 Multi-Threat Security System I – Administration, Content Inspection and SSL VPN (Course 201).

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.
- 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.

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.
- Completion of FortiGate Multi-Threat Security System I – Administration, Content Inspection and SSL VPN (Course 201) is highly recommended.

System Requirements

Since this training is performed online, students will view the lecture component of the class and perform the hands-on exercises over the web.

To participate in the course 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)**

Course Topics

AGENDA - Day 1

Virtual Networking

- VLANs on a FortiGate Unit
- Global and Virtual Domain Configuration Settings
- Virtual Domains
- VDOM Resource Limits
- Inter-VDOM Links

Diagnostics

- Diagnostic Commands
- Packet Sniffing
- Self Help Options

Routing

- Routing Tables
- Route Elements
- Static and Policy Routes
- Route Selection
- Reverse Path Forwarding
- Dynamic Routing
  - Routing Information Protocol
  - Open Shortest Path First
  - Border Gateway Protocol
  - Intermediate System to Intermediate System
- Multicast Routing
- Routing Diagnostics

AGENDA - Day 2

Intrusion Prevention System

- IPS Signatures
- IPS Sensors
- Filters
- IPS Overrides
- Attack Types
- Monitoring IPS Attacks

Remote User Authentication

- RADIUS Authentication
- Dynamic Profiles
- LDAP Authentication
- TACACS+ Authentication
- Digital Certificate Authentication
- Directory Services Authentication

Fortinet Single Sign On

- Directory Services Authentication
- Fortinet Single Sign On Components
- Fortinet Single Sign On Modes
- NTLM Authentication

Certificate-Based Operations

- Introduction to Cryptography
- Secure Socket Layer Security
- Certificate authentication
- SSL Content Inspection

IPSec VPN

- IPSec Architecture and Protocols
- Internet Key Exchange
- IPSec Phase 1 and Phase 2
- IPSec VPN Modes
- IPSec Topologies
- Configuring Route-Based and Policy-Based VPNs
- IPSec VPN Monitor
- Overlapping Subnets
- IPSec Debugging
- VPN Troubleshooting Tips

AGENDA - Day 3

Transparent Mode

- Operating Modes
- Ethernet Frame and VLAN Tags
- VLANs on a FortiGate Unit Operating in Transparent Mode
- Port Pairing
- Transparent Bridge
- Broadcast Domains
- Forwarding Domains
- Spanning Tree Protocol
- Link Aggregation

WAN Optimization

- FortiGate WAN Optimization Techniques
- WAN Optimization Rules
- WAN Optimization Modes
- Web Caching
- Transparent Proxy
- WCCP v2 Support
- Monitoring WAN Optimization

Wireless

- Wireless Concepts
- Thick and Thin Access Points
- FortiGate Wireless Controllers
- Managed AP Topologies
- Controller Discovery
- Virtual Access Points
- Guest Networks
- Wireless Security Modes
- Access Point Profiles
- Rogue Access Point Detection
- Wireless Roaming

High Availability

- High Availability Clusters
- High Availability Modes of Operation
  - Active-Passive
  - Active-Active
- FortiGate Clustering Protocol
  - Virtual Addresses
  - FGCP Heartbeat
  - Heartbeat Interfaces
  - HA Configuration Synchronization
- Virtual MAC Addresses
- Load Balancing
- Failover
- Virtual Clustering
- Session Synchronization
- Firmware Upgrades