FortiGate Multi-threat Security Systems 2 (301)

Duration 3 Days

COURSE DESCRIPTION

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.

Students should have completed a network certification training program and/or had at least one year of experience configuring and supporting switches and networks.

WHAT YOU'LL LEARN

- Virtual Local Area Networks and Virtual Domains
- Diagnostics
- Transparent Mode
- Firewall Policies
- Routing
- Traffic Optimization
- Threat Management
- Advanced Authentication
- Virtual Private Networks
- High Availability

PRE-REQUISITES

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.

Students should be familiar with networking essentials, such as LAN, Internet, security, and IP protocols.

OUTLINE

- **Module 1**: Routing
- **Module 2:** Virtual Networking
- **Module 3:** Transparent Mode
- **Module 4:** High Availability
- **Module 5:** Advanced IPSec VPN
- **Module 6:** Intrusion Prevention System
- **Module 7:** Fortinet Single Sign On (FSSO)
- **Module 8:** Certificate-Based Operations
- **Module 9:** Data Leak Prevention
- **Module 10:** Diagnostics
- **Module 11:** Putting It All Together