



FortiGate Multi-Threat Security Systems II

- Secured Network Deployment and Virtual Private Networks

Course 301

Course Overview

The **FortiGate Multi-Threat Security Systems II** course provides 2 days of instructor-led training (in a public or private on-site class setting) where participants will gain a comprehensive understanding of many of the advanced networking and security features of FortiGate UTM security appliances.

Extensive hands-on labs allow students to perform the tasks associated with the configuration and troubleshooting of virtual domains, high availability, IPS, Routing and IPsec VPNs.

This implementations-based course demonstrates features that can be easily adapted for planning your own network security deployment using FortiGate Unified Threat Management appliances.

Course Objectives

Upon completion of this course, students will be able to:

- Install a FortiGate security appliance in "Transparent Mode" in order to minimize disruption to an existing networking infrastructure.
- Use the built-in FortiOS diagnostic tools for troubleshooting, performance monitoring and install validation.
- Construct Virtual Domains and configure Inter-VDOM routing.
- Configure Static and Policy routing for bandwidth and policy traffic shaping.
- Configure link failover and ECMP.
- Configure IPS protection and IPS Anomaly thresholds on a FortiGate device to protect network resources from attack.
- Explore differences between IPsec interface and Policy based VPNs, and create redundant site-to-site tunnels with OSPF Dynamic Routing.
- Create a policy-based 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

- FortiGate, FortiAnalyzer and FortiClient

Products Trained On

- FortiGate (FortiOS) – All models

Prerequisites

- Intermediate level network security experience
- Basic understanding of the Dynamic routing protocol, IPSec VPN, Intrusion Detection and Prevention concepts

Who Should Attend

This course is intended for anyone who is involved in the design and implementation of a security infrastructure using FortiGate UTM appliances.

Certification

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

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

Course Topics

AGENDA - Day 1

Module 1 – System Setup and CLI Review

- Initial System Configuration
- CLI Review



Module 2 – Diagnostics and Troubleshooting

- Problem Definition
- FortiNet Self-Help Resources
- System Performance Monitoring
- Sanity Checking
- Conserve Mode
- Packet Sniffer
- ARP Table
- Session Table
- Debug

Module 3 – Virtual Domains

- Overview of Virtual Domains
- Network Positioning
- Managing Virtual Domains
- The Management VDOM
- Global Configuration
- VDOM Administrative Users
- Per-VDOM Objects
- Interface Management
- Inter-VDOM Routing
- Independent, Management, Meshed
- Forwarding Domains
- Gateway Firewall VDOM

Module 4 – Transparent Mode

- Operational Modes
- Ethernet Frame and VLAN Tag
- How to Read Ethernet Headers from the Packet Sniffer
- Transparent Bridging
- Broadcast Domain
- VLAN Trunks
- Forwarding Domains: Tagged and Non-Tagged Interfaces
- TP Proxies and MAC Address Changes
- What is the Spanning Tree Protocol?
- FortiOS TP opmode and the Spanning Tree Protocol
- Installing a FortiGate in TP opmode
- TP and 802.3ad Aggregate Interfaces



- Duplicate MAC Addresses
- TP Opmode Session Table



Module 5 – Routing

- Routing Overview
- Static
 - Static Routes
 - Directly Connected Networks
 - Default Routes
- Dynamic Routing
 - RIP, OSPF and BGP
 - Interior Gateway Protocol (IGP)
 - Exterior Gateway Protocol (EGP)
 - Access Control Lists (ACL)
- Policy Route
 - Overview
 - Characteristics
 - Load Sharing
- Dead Gateway Detection
- Loopback Interfaces

Module 6 – Intrusion Prevention System

- Overview of IPS
- IPS Components
 - IPS Engine Module
 - DoS Module
 - IPS Signature Database
- Protocol Decoders
- Zero Day Attacks
- IM and P2P
- Evasion Attempts
- IPS Configuration
- IPS Signature List Updates
- Custom Signatures
- IPS Anomalies
- IPS Detection Actions
- IPS Logging
- Implementation Considerations
- Advanced IPS Settings



AGENDA - Day 2

Module 7 – IPSec VPN

- IPSec VPN Overview
- VPN Topologies
 - Site-to-Site
 - Site-to-Multi-site
 - Site-to-Client
- Configuration Types
 - Firewall Policy (Flow, Configuration, Hub and Spoke)
 - Interface (Flow, Configuration, Hub and Spoke)
- What about Dynamic Routing?
- Site-to-Client Tunnels
- Site-to-Client Configuration
- DHCP over IPSec

Module 8 – High Availability

- High Availability Overview
- System Requirements
- Modes of Operation
 - Active-Active
 - Active-Passive
 - Virtual Cluster
- Master Device Selection
- Synchronization
- FortiGate Cluster Protocol Heartbeat
- High Availability Configuration
- Uninterruptible Upgrade
- Load Balancing
 - Active-Active Mode
 - Load Balancing AV Scan Sessions SYN
 - Load Balancing AV Scan Sessions SYN, ACK ACK
- Virtual Clusters
- High Availability Failover
- Virtual MAC Address
- Full Mesh High Availability
- High Availability Statistics