FORTINET FORTIGATE TRAINING

UPGRADE YOUR KNOWLEDGE

Fortinet Fortigate Training

Course Overview

The Fortinet Firewall course aims to provide practical skills on security mechanisms, their configuration and troubleshooting in enterprise environments. This course is intended for networking professionals with little or no experience in Fortigate FortiOS products.

Duration & Module Coverage

Duration: 7 Days (14hrs)

Session Options	Module Coverage
Session Weekdays[4] : 2 hours per day 4 days per week **Session Weekends:** 2 hours per day	**Day 1 - Module 1** **Day 2 - Module 2** **Day 3 - Module 3** **Day 4 - Module 4** **Day 5 - Module 5** **Day 6 – Module 6** **Day 7 – Module 7**

Learning Goals

By the end of this course participants will be able to:

1. Demonstrate knowledge of the Fortigate FortiOS devices.
2. Understand security technologies used in Fortigate Series Devices.
3. Configuration and troubleshooting skills of related platforms.

Pre-Requisites

This course is for security professionals looking to work in a Fortigate environment. Understanding of basic networking and security is a pre-requisite to attend this training.

Teaching Methodology

This is a very hands-on course where participants carry out practical exercises according to the lab guide provided. The concepts are taught through implementation of real-world use-cases. Our exercises have been carefully designed to replicate scenarios participants will face in real life work conditions.

Who Should Take This Course?

This course is designed for security professionals with knowledge of basic networking looking forward to gain understanding of security technologies offered by Fortinet Next-Generation Firewalls and configuration and troubleshooting of related platforms.

Course Content

1. **Introduction to Fortigate Firewalls**
   - Packet processing in fortigate
   - Modes of operation
   - Initial installation and setup
   - Security policies and NAT
   - Static routes, policy routes, and dynamic routing
   - Equal cost multi-path (ECMP)
   - Loose and strict reverse path forwarding (RPF)
   - Link aggregation
   - Loopback interfaces and black hole routes
   - WAN link load balancing
   - How to diagnose broken routes

2. **Virtual Domains, VLAN and VLAN Tagging**
   - Virtual Domains (VDOMs)
   - Global and per-VDOM resources
   - Per-VDOM administrative accounts
   - Inter-VDOM Links
   - Monitoring per-VDOM resources
   - VDOM topologies

3. **Modes of operations**
   - Transparent mode vs. NAT mode
   - Transparent bridging
   - Forwarding domains
   - Port pairing
   - STP configuration
   - Monitoring the MAC address table

4. **High Availability**
   - Active-passive vs. active-active mode
   - How and HA cluster elects the primary
   - Active-active traffic balancing
   - HA failover
   - Configuration synchronization
   - Session synchronization
   - Virtual clustering
   - Checking the status of a HA cluster

5. **IPSec VPNs**
   - VPN Main vs. aggressive mode negotiations
   - Static vs. dynamic peers

- Benefits and cost of VPN technologies
- Dialup VPN configuration
- Redundant VPNs
- Troubleshooting

6. Data Loss Prevention

- Why use DLP?
- Files vs. messages
- Sensors and filters
- Document fingerprinting
- Summary vs. full content archiving

7. Diagnostics

- Why do you need to know precisely what is normal?
- Network diagrams
- Monitoring network usage & system resource usage
- Physical layer troubleshooting
- Network layer troubleshooting
- Transport layer troubleshooting

Practical Learning Exercises

A lab guide will be provided to each student with requirement scenarios. Along with lab guide required VMs will be provided to set up individual labs for self practice.

A sample scenario would consist of one interface of Fortigate appliance connected to internal network, one interface connected to Server farm and one interface connected to the internet.

Similarly there would be scenarios for implementing, verifying and troubleshooting all modules covered in the course.