FortiADC Administrator

Duration: 3 Days

Course Description:

In this course, you will learn how to configure and administer the most commonly used features of FortiADC. You will learn about layer 4 and layer 7 server load balancing, link load balancing, global load balancing, high availability (HA), firewall policies, advanced routing, and more. You will also learn about FortiADC web application protection features, including web application firewall (WAF) with adaptive learning, and other enhanced security features such as DDoS, IPS, and so on.

Target Audience:

Security professionals involved in the deployment, administration, maintenance, and troubleshooting of FortiADC devices should attend this course.

Course Objectives:

- System Settings
- Virtual Servers and Load Balancing
- Advanced Server Load Balancing
- Link Load Balancing and Advanced Networking
- Global Load Balancing
- Application Security
- Network Security
- Advanced Configurations
- Monitoring, Troubleshooting, and System Maintenance

Course Outlines:

- Describe the characteristics and components of an application delivery network
- Identify the security challenges faced in an application delivery network
- Evaluate deployment options
- Configure initial network and system settings
- Manage administrator accounts
- Configure virtual servers, real servers, and server pools
- Configure application profiles
- Configure page speed optimization
- Configure layer 7 compression offloading
- Configure content routing and content rewrite
- Configure link load balancing
- Create virtual tunnels and link groups
- Configure policy routing, QoS, and NAT features
- Configure BGP and OSPF routing
- Configure DNS services and policies
- Configure global load balancing
- Configure the web application firewall (WAF)
- Configure and manage adaptive learning
- Configure bot mitigation and API gateway policies
- Configure VDOMs and high availability (HA)
- Create automated action scripts using the REST API
- Configure OWASP Top 10 profile
- Configure DLP
- Configure advanced bot protection
- Configure firewall policies and connection limits
- Protect against DoS attacks
- Configure ZTNA integration
- Configure local logging, remote logging, and alert emails
- Configure SNMP monitoring
- Use diagnostic commands available through the CLI
- Identify the most common issues
- Back up and restore the system configuration
- Upgrade the firmware