FortiADC Administrator

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.

Product Version

FortiADC 7.6

Course Duration

- Lecture time (estimated): 8 hours
- Lab time (estimated): 9 hours
- Total course duration (estimated): 17 hours
  - 3 full days or 5 half days

Who Should Attend

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

Certification

This course is not included in the certification program.

Prerequisites

You must be familiar with the topics covered in FCA - *FortiGate Operator* or have equivalent knowledge of basic firewall technologies.

You should be familiar with web applications.

Agenda

1. System Settings
2. Virtual Servers and Load Balancing
3. Advanced Server Load Balancing
4. Link Load Balancing and Advanced Networking
5. Global Load Balancing
6. Application Security
7. Network Security
8. Advanced Configurations
9. Monitoring, Troubleshooting, and System Maintenance

Objectives

After completing this course, you should be able to:

- 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

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Contact your Fortinet Resellers or Authorized Training Partners to purchase this course.

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using a purchase order (PO) through Fortinet Resellers or Authorized Training Partners.

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

For training and lab SKUs, or additional purchasing information, refer to Purchasing Process.

ISC2

- CPE training hours: 8
- CPE lab hours: 9
- CISSP domains: Communication and Network Security

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.