FortiNAC-F Administrator

Course Description

In this course, you will learn how to leverage the powerful and diverse capabilities of FortiNAC-F, using best practices for achieving visibility, control, and response. These fundamentals will provide you with a solid understanding of how to implement network visibility and security automation.

Who Should Attend

Network and security administrators, managers, and other IT staff who will use FortiNAC-F should attend this course.

Prerequisites

It is recommended that you have an understanding of the following topics:

- Networking concepts and terms
- Networking protocols
- Infrastructure configurations

Agenda

1. Introduction and Initial Configuration
2. Achieving Network Visibility
3. Identification and Classification of Rogues
4. Visibility, Troubleshooting, and Logging
5. Logical Networks and Fortinet Security Fabric Integration
6. State-Based Control
7. Security Policies
8. Guest and Contractor Management
9. Security Device Integration and Automated Response
10. Advanced Features
11. FortiNAC-F Manager Integrations

Objectives

After completing this course, you should be able to:

- Configure a FortiNAC-F system to achieve network visibility
- Leverage the control capabilities for network access and automated policy enforcement
- Integrate FortiNAC-F into the Fortinet Security Fabric
- Combine the visibility and control features with security device integrations to automate threat responses to security risks

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones
- One of the following:
  - HTML 5 support
  - An up-to-date Java Runtime Environment (JRE) with the Java Plugin enabled in your web browser

You should use a wired Ethernet connection, *not* a Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Product Versions

- FortiNAC-F 7.6.3
- FortiGate 7.6.3

Course Duration

- Lecture time (estimated): 11 hours
- Lab time (estimated): 6 hours
- Total course duration (estimated): 17 hours
  - 3 full days or 5 half days

Formats

- Instructor-led (classroom and online)
- Self-paced online

ISC2

- CPE training hours: 11
- CPE lab hours: 6
- CISSP domains: Communication and Network Security

Part Number (SKU)

See Purchasing Process for more information

Certification

Datacipher Education Services | FORTINET