FORTINET NSE Training Institute

Course Description

Secure Access

In this three-day course, you will learn how FortiGate, FortiAP, FortiSwitch, and FortiAuthenticator enable secure connectivity over wired and wireless networks. You will also learn how to provision, administer, and monitor FortiAP and FortiSwitch devices using FortiManager. This course covers the deployment, integration, and troubleshooting of advanced authentication scenarios, as well as best practices for securely connecting wireless and wired users. You will learn how to keep the network secure by leveraging Fortinet Security Fabric integration between FortiGate, FortiSwitch, FortiAP, and FortiAnalyzer to automatically quarantine risky and compromised devices using IOC triggers.

Product Versions

- FortiGate 6.4.1
- FortiAP 6.4.2
- FortiSwitch 6.4.2
- FortiAnalyzer 6.4.2
- FortiAuthenticator 6.1.1

Formats

- Instructor-led classroom
- Instructor-led online
- Self-paced online

Agenda

1. RADIUS and LDAP
2. Certificate-Based Authentication
3. Radius and Syslog Single Sign-On
4. Centralized Management
5. FortiSwitch
6. Port Security
7. Integrated Wireless
8. Guest Access
9. Enhanced Wireless

Objectives

After completing this course, you should be able to:

- Configure advanced user authentication and authorization scenarios using RADIUS and LDAP
- Troubleshoot user authentication and authorization problems
- Implement two-factor authentication using digital certificates
- Implement and troubleshoot RADIUS and syslog single sign-on solutions
- Provision, configure, and manage FortiSwitch using FortiManager over FortiLink

- Configure Layer 2 authentication for wired and wireless users using 802.1.x
- Provision, deploy, and manage FortiAP using FortiManager over FortiLink
- Deploy complex wireless networks with dynamic VLAN assignments
- Implement and deploy wireless network with IoT segmentation
- Secure the wired and wireless network
- Provide secure access to guest users
- Monitor and analyze wireless clients and traffic using Wireless Manager
- Automatically quarantine wired and wireless clients using IOC triggers

Who Should Attend

This course is intended for networking and security professionals involved in the management, configuration, administration, and monitoring of FortiGate, FortiManager, FortiAP, FortiSwitch, and Wireless Manager devices used to secure access to their organizations' resources.

Prerequisites

- Knowledge of network authentication protocols
- Knowledge of Layer 2 switching
- Understanding of wireless networks
- Understanding of the topics covered in the following courses:
  - NSE 4 FortiGate Security
  - NSE 4 FortiGate Infrastructure
- Understanding of the topics covered in the following courses is also recommended:
  - NSE 5 FortiManager
  - NSE 6 FortiAuthenticator
  - NSE 6 Integrated and Cloud Wireless

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:
  - HTML5 support
  - An up-to-date Java Runtime Environment (JRE) with 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.

Certification

This course is intended to help you prepare for the NSE 7 Secure Access certification exam.