FORTINET
Premier Authorized Training Center

fast lane

FORTINET CERTIFIED PROFESSIONAL
Network Security

FortiSwitch

Course Description

In this course, you will learn how to deploy, provision, and manage a FortiSwitch with FortiGate using FortiLink. This course also covers the deployment and troubleshooting of Layer 2 and Layer 3 features, as well as the most common FortiSwitch stack topologies, including those that leverage multichassis link aggregation group (MCLAG) for redundancy and higher performance. You will also learn about FortiSwitch in standalone mode, its unique features, and how to manage a standalone switch directly, or from FortiLAN Cloud.

Product Version:

- FortiGate 7.2.1
- FortiSwitch 7.2.0
- FortiAnalyzer 7.2.1

Course Duration:

3 days

Who should attend?

Networking and security professionals involved in the management, configuration, administration, and monitoring of FortiSwitch devices used to provide secure network access to endpoints should attend this course.

Certification:

This course is intended to help you prepare for the Fortinet NSE 6 - FortiSwitch 7.2 certification exam. This exam is part of the Fortinet Certified Professional - Network Security certification track.

Prerequisites:

- Basic knowledge of networking
- An understanding of layer 2 switching
- An understanding of the topics covered in the following
- courses:
  - FCP - FortiGate Security
  - FCP - FortiGate Infrastructure

Outlines:

1. Managed Switch
2. Switch Fundamentals
3. Layer 2 Design
4. Layer 2 Security
5. Advanced Features
6. Monitoring
7. Standalone Switch
8. Troubleshooting

Objectives:

After completing this course, you will be able to:

- Explore the FortiSwitch portfolio and identify the supported management modes
- Describe and deploy FortiSwitch in managed switch mode (FortiLink mode)
- Understand Ethernet switching, VLANs, link aggregation (LAG), MCLAG, and layer 2 discovery
- Identify the most common FortiSwitch topologies when deploying FortiSwitch in managed switch mode
- Understand Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree protocol (MSTP) operation and configuration, as well as other loop protection features
- Describe and configure Layer 2 security to filter unwanted traffic and perform antispoofing
- Configure layer 2 authentication using 802.1.X, and leverage 802.1X to assign dynamic VLANs to endpoints
- Implement advanced features to increase port density, control network access, forward multicast traffic more effectively, and quarantine compromised devices
- Prioritize traffic on FortiSwitch by using QoS marking, queuing, and rate limiting features
- Simplify endpoint deployment by using Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)