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 groups (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 FortiEdge Cloud.

Product Version:

- FortiGate 7.6
- FortiSwitch 7.6
- FortiAnalyzer 7.6
- FortiAuthenticator 6.6

Course Duration:

3 days

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:
    - FortiGate 7.6 Administrator

Outlines:

1. Switch Fundamentals
2. Managed Switch
3. Basic Administration
4. STP
5. Layer 2 Design
6. Layer 2 Security
7. Advanced Features
8. QoS and Multi-Tenancy
9. Monitoring
10. Standalone Switch and FortiEdge Cloud
11. Standalone Switch—Layer 2 and Layer 3
12. 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 groups (LAG), multichassis link aggregation groups (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
- Simplify endpoint deployment by using Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
- Share FortiSwitch ports across different VDOMs using multi-tenancy
- Monitor FortiSwitch using SNMP, sFlow, and flow sampling
- Describe the most useful troubleshooting tools available on FortiSwitch

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.