FORTINET
Premier Authorized Training Center

fast lane

FORTINET CERTIFIED SOLUTION SPECIALIST
Network Security

Network Security Engineer

Course Description

In this course, you will learn how to diagnose and troubleshoot the most common networking and security problems in a Fortinet protected network security solution. In interactive break-and-fix labs, you will use tools, diagnostics, and debug commands to detect, isolate, and resolve problems related to the most commonly used FortiGate features, such as IPsec, routing, web filtering, HA, IPS, and more. These skills and this knowledge will give you an advanced understanding of how to support a network security solution based on FortiGate devices.

Product Version:

- FortiGate 7.2.4

Course Duration:

3 days

Who should attend?.

Networking and security professionals involved in diagnosing, troubleshooting, and supporting an enterprise security infrastructure using FortiGate devices should attend this course. This course assumes advanced knowledge of networking, and extensive hands-on experience working with FortiGate.

Certification:

This course is intended to help you prepare for the Fortinet NSE 7 - Network Security 7.2 Support Engineer certification exam. This exam is part of the Fortinet Certified Solution Specialist - Network Security certification track.

Prerequisites:

You must have an understanding of the topics covered in the FCP - FortiGate Security and FCP – FortiGate Infrastructure courses or have equivalent experience. It is also recommended that you have an understanding of the topics covered in the FCSS - Enterprise Firewall course.

Outlines:

1. Troubleshooting Concepts
2. System Resources
3. Sessions, Traffic Flow, and Networking
4. Security Fabric
5. Firewall Authentication
6. FSSO
7. Security Profiles
8. High Availability
9. IPsec
10. IPsec—IKEv2
11. Routing
12. BGP
13. OSPF

Objectives:

After completing this course, you will be able to:

- Set up a baseline for FortiGate and analyze the first steps to diagnose a FortiGate
- Monitor process activity, diagnose conserve mode, and troubleshoot unexpected reboots and frozen devices
- Analyze information in the session table and debug flow output
- Troubleshoot session helpers
- Troubleshoot common problems related to local, LDAP, and RADIUS authentication
- Troubleshoot common FSSO problems
- Troubleshoot FortiGuard and web filtering problems
- Monitor an HA cluster and troubleshoot common HA problems
- Troubleshoot and diagnose IPsec VPNs with debug and sniffer commands
- Troubleshoot routing problems with debug commands
- Monitor OSPF status and o troubleshoot common OSPF problems with debug commands