Network Security Support Engineer

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, high availability (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 7.6.2

Course Duration

- Lecture time (estimated): 9 hours
- Lab time (estimated): 8 hours
- Total course duration (estimated): 17 hours
  - 3 full days and 5 half 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 FCSS - *Network Security 7.6 Support Engineer* 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 Administrator* course, or have equivalent experience.

It is also recommended that you have an understanding of the topics covered in the FCSS - *Enterprise Firewall* course.

Agenda

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 should 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, RADIUS, and SAML 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 troubleshoot common OSPF problems with debug commands

- Monitor and verify the BGP status with commands and troubleshoot common BGP issues

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Contact your Fortinet Resellers or Authorized Training Partners to purchase this course.

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the Fortinet Training Institute
- Purchase order (PO), through Fortinet Resellers or Authorized Training Partners

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

For training and lab SKUs, or additional purchasing information, refer to Purchasing Process.

ISC2

- CPE training hours: 9
- CPE lab hours: 8
- CISSP domains: Security Operations

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.