
Network Security Support Engineer (NST)

ID NST Price on request 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.

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

Prerequisites

This course assumes advanced knowledge of networking, and extensive hands-on experience working with FortiGate.

You must have an understanding of the topics covered in the [FortiGate Security \(FORT-SECI\)](#) and [FortiGate Infrastructure \(FORT-INFRA\)](#) courses, or have equivalent experience.

It is also recommended that you have an understanding of the topics covered in the [Enterprise Firewall \(FORT-ENTFIREWALL\)](#) course.

Course 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 and sniffer commands
- Troubleshoot rerouting problems with debug commands
- Monitor OSPF status and troubleshoot common OSPF

Network Security Support Engineer (NST)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>