Introduction to Juniper Security (IJSEC)

ID IJSEC **Price** CHF 2,700.—(excl. VAT) **Duration** 3 days

Who should attend

- Individuals who are responsible for network security.
- Individuals who want to learn how to secure their networks using SRX Series Firewalls.

This course is part of the following Certifications

Juniper Networks Certified Internet Associate Junos Security (JNCIA-SEC)

Prerequisites

- Basic networking skills.
- General understanding of networking architecture

Course Objectives

- Describe Junos OS architecture.
- Describe SRX Series security architecture.
- Create security and functional zones.
- Configure screen options.
- Configure address and application objects.
- Implement traditional security policies.
- Implement unified security policies.
- Configure security policy logging, counting, and scheduling.
- Troubleshoot security policies.
- Enable application tracking.
- Implement antivirus and antispam capabilities.
- Enable content filtering and Web filtering.
- Configure source NAT.
- Configure destination NAT.
- Configure static NAT.

Course Content

Module 01: Introduction to Juniper Security

- Explain the challenges faced by network security administrators
- Describe the physical and virtual device options of the SRX Series Firewall
- Explain the SRX Series management options

Module 02: Juniper SRX Series Security Architecture

- Explain the Junos OS architecture
- Explain the SRX Series security architecture
- Explain SRX Series traffic processing

Module 03: Managing Zones

- Explain security zones and functional zones
- Configure security zones
- Use screen options

Lab 01: Managing Zones

Module 04: Managing Addresses, Applications, and ALGs

- Create address objects
- Create applications
- Use ALGs

Lab 02: Managing Addresses and Applications

Module 05: Managing Traditional Security Policies

- Explain traditional security policy processing
- Create traditional security policies
- Modify, reorder, deactivate, and delete security policies

Lab 03: Managing Traditional Security Policies

Module 06: Managing Unified Security Policies

- Describe AppID
- Implement unified security policies

Lab 04: Managing Unified Security Policies

Module 07: Configuring Security Policy Options

- Implement security policy logging and counting
- Create schedulers
- Examine session options

Lab 05: Configuring Security Policy Options

Module 08: Troubleshooting Security Policies

- Troubleshoot the flow process
- Enable trace options

Lab 06: Troubleshooting Security Policies

Module 09: Implementing AppTrack

- Explain AppSecure capabilities
- Configure AppTrack

Lab 07: Implementing AppTrack

Module 10: Implementing Antivirus and Antispam

- Describe content security
- Configure antivirus
- Configure antispam

Lab 08: Implementing Antivirus and Antispam

Module 11: Implementing Content Filtering and NextGen Web Filtering

- Explain content filtering and NextGen Web Filtering
- Configure content filtering
- Configure NextGen Web Filtering

Lab 09: Implementing Content Filtering and NextGen Web Filtering

Module 12: Implementing Source NAT

- Explain source NAT
- Configure interface-based source NAT
- Configure pool-based source NAT
- Implement proxy ARP

Lab 10: Implementing Source NAT

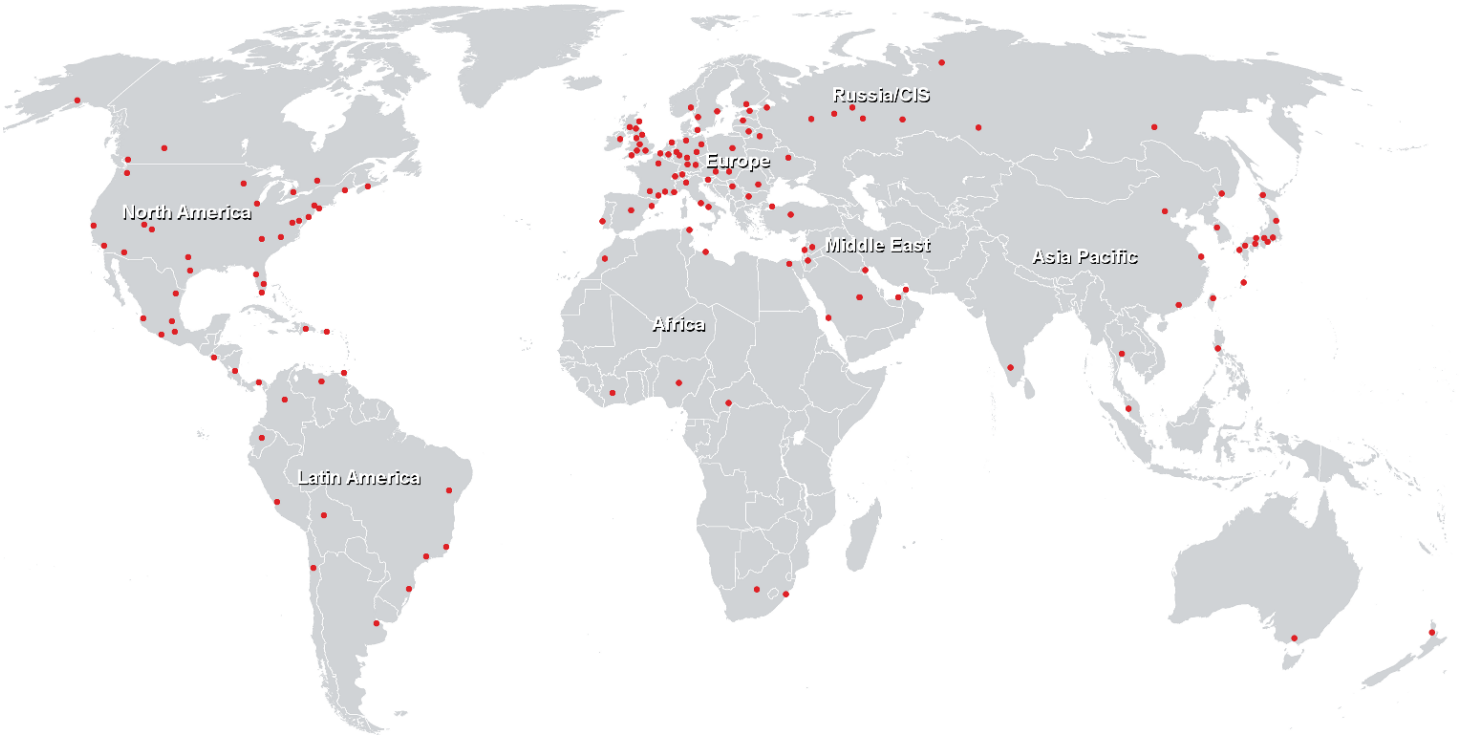
Module 13: Implementing Destination NAT and Static NAT

- Explain destination NAT
- Configure destination NAT
- Configure static NAT

Lab 11: Implementing Destination NAT and Static NAT

Introduction to Juniper Security (IJSEC)

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