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 1: Introduction to Juniper Security

- Explain network security challenges.
- Explain SRX Series Firewall physical and virtual device options.
- Explain SRX Series Firewall device management options.

Module 2: Juniper SRX Series Security Architecture

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

Module 3: Managing Zones

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

Lab 1: Managing Zones

Module 4: Managing Addresses, Zones, and ALGs

- Create address objects
- Create applications
- Use ALGs

Lab 2: Managing Addresses, Zones, and ALGs

Module 5: Manage Traditional Security Policies

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

Lab 3: Managing Traditional Security Policies

Module 6: Managing Unified Security Policies

- Describe AppID
- Implement unified security policies

Lab 4: Managing Unified Security Policies

Module 7: Configuring Security Policy Options

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

Lab 5: Managing Security Policy Options

Module 8: Troubleshooting Security Policies

- Troubleshoot the flow process
- Enable trace options

Lab 6: Troubleshooting Security Policies

Module 9: Implementing AppTrack

- Explain AppSecure capabilities
- Configure AppTrack

Lab 7: Implementing AppTrack

Module 10: Implementing Antivirus and Antispam

- Describe content security
- Configure antivirus
- Configure antispam

Lab 8: Deploying Antivirus and Antispam

Module 11: Implementing Content Filtering and NextGen Web Filtering

- Configure content filtering
- Configure NextGen web filtering

Lab 9: Deploying Content Filtering and Enhanced Web Filtering

Module 12: Implementing Source NAT

- Explain source NAT
- Configure interface-based source NAT
- Configure pool-based source NAT
- Validate source NAT functionality

Lab 10: Implementing Source NAT

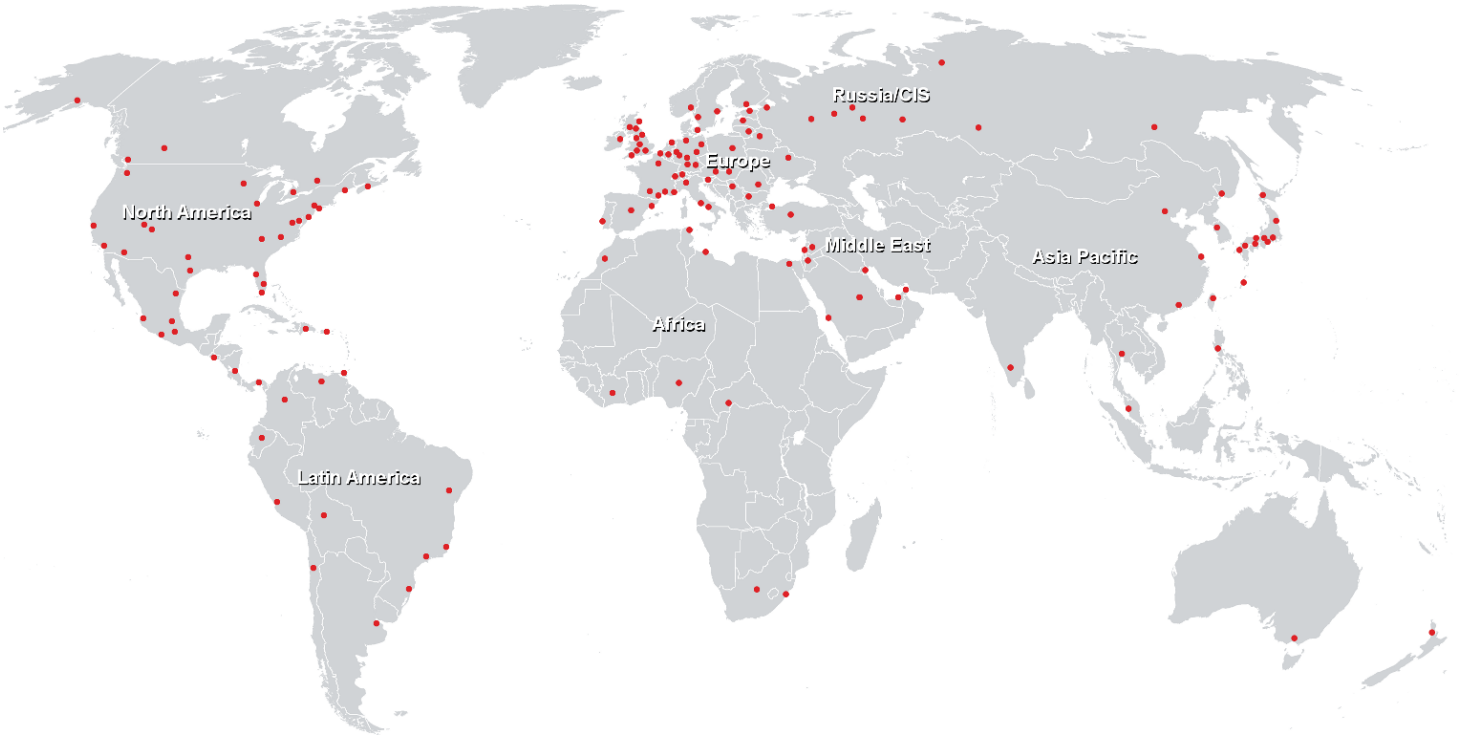
Module 13: Implementing Destination NAT and Static NAT

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

Lab 11: Implementing Destination 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