

## Introduction to Juniper Security (IJSEC)

**ID IJSEC** **Prix CHF 2 700,— (Hors Taxe)** **Durée 3 jours**

### A qui s'adresse cette formation

The primary audiences for this course are the following:

- Operators of Juniper Networks security solutions, including network engineers, administrators, support personnel, and resellers.

### Cette formation prépare à la/aux certifications

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

### Pré-requis

- Students should have basic networking knowledge and an understanding of the Open Systems Interconnection (OSI) reference model and the TCP/ IP protocol suite.

### Objectifs

After successfully completing this course, you should be able to:

- Identify high-level security challenges in today's networks.
- Identify products that are incorporated into the Juniper Connected Security solution.
- Explain the value of implementing security solutions.
- Explain how Juniper Connected Security solves the cyber security challenges of the future.
- Explain the SRX Series devices and the added capabilities that next-generation firewalls provide.
- Explain traffic flows through the SRX Series devices.
- List the different security objects and how to create them.
- Describe interface types and perform basic interface configuration tasks.
- Describe the initial configuration for an SRX Series device.
- Explain security zones.
- Describe screens and their use.
- Explain address objects.
- Describe services and their use.
- Describe the purpose for security policies on an SRX Series device.
- Describe zone-based policies.
- Describe global policies and their use.

- Explain unified security policies.
- Configure unified security policies with the J-Web user interface.
- Describe IDP signatures.
- Configure an IDP policy using predefined templates with the J-Web user interface.
- Describe the use and configuration of the integrated user firewall feature.
- Describe the UTM security services
- List the available UTM services on the SRX Series device.
- Configure UTM filtering on a security policy with the J-Web user interface.
- Explain Sky ATP's use in security.
- Describe how Sky ATP and SRX Series devices operate together in blocking threats.
- Describe NAT and why it is used.
- Explain source NAT and when to use it.
- Explain destination NAT and when to use it.
- Explain static NAT and its uses.
- Describe the operation and configuration the different types of NAT.
- Identify various types of VPNs.
- Describe IPsec VPNs and their functionality.
- Describe how IPsec VPNs are established.
- Describe IPsec traffic processing.
- Configure IPsec VPNs with the J-Web user interface.
- Describe and configure proxy IDs and traffic selectors with the J-Web user interface.
- Monitor IPsec VPNs with the J-Web user interface.
- Describe the J-Web monitoring features.
- Explain the J-Web reporting features.
- Describe the Sky Enterprise service and how it can save resources.
- Explain the functionality of Junos Space Security Director.

### Contenu

#### Day 1

#### Module 1: COURSE INTRODUCTION

#### Module 2: Juniper Security Concept

- Security Challenges
- Security Design Overview

# Introduction to Juniper Security (IJSEC)

---

- Juniper Connected Security

## Module 3: Juniper Connected Security – SRX Series Devices

- Connected Security
- Interfaces
- Initial Configuration

LAB 1: Initial Configuration

## Module 4: Security Objects

- Security Zone Objects
- Security Screen Objects
- Security Address Objects
- Security Services Objects

LAB 2: Creating Security Objects with J-Web

## Module 5: Security Policies

- Security Policy Overview
- Zone-Based Policies
- Global Security Policies
- Application Firewall with Unified Security Policies

LAB 3: Creating Security Policies with J-Web

## Module 6: Security Services – IDP and User Firewall

- IDP Security Services
- Integrated User Firewall

LAB 4: Adding IDP and User Firewall Security Services to Security Policies

## Day 2

## Module 7: Security Services – UTM

- Content Filtering
- Web Filtering
- Antivirus
- Antispam

LAB 5: Adding UTM Security Services to Security Policies

## Module 8: Juniper Connected Security – Sky AT

- Sky ATP Overview

- Blocking Threats

Lab 6: Demonstrating Sky ATP

## Module 9: Network Address Translation

- NAT Overview
- Source NAT
- Destination NAT
- Static NAT

Lab 7: Implementing Network Address Translation

## Day 3

## Module 10: IPsec VPN Concepts

- VPN Types
- Secure VPN Requirements
- IPsec Tunnel Establishment
- IPsec Traffic Processing

## Module 11: Site-to-Site VPNs

- IPsec Configuration
- IPsec Site-to-Site Tunnel

Lab 8: Implementing Site-to-Site IPsec VPNs **Module 12: Monitoring and Reporting**

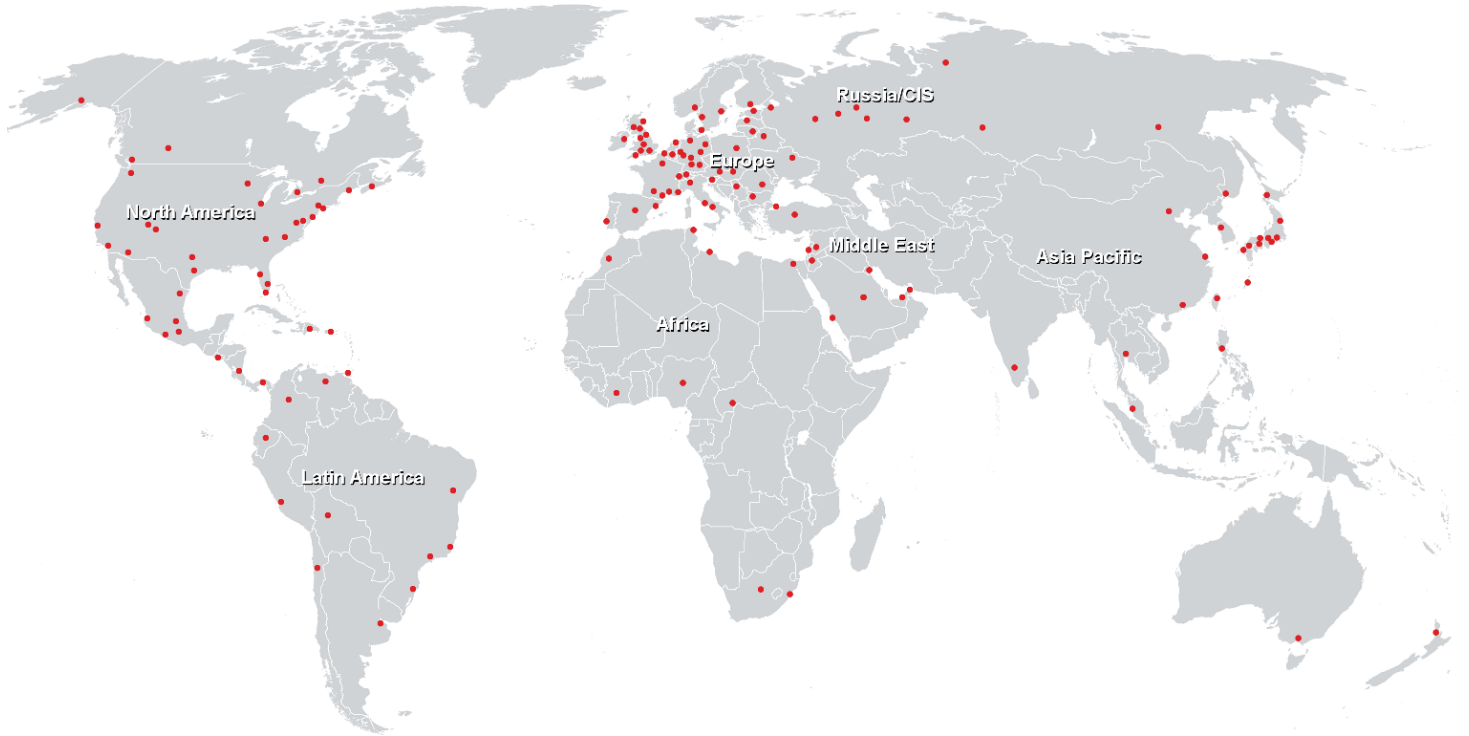
- J-Web monitoring options
- J-Web Reporting options

Lab 9: Using Monitoring and Reporting Appendix A: SRX Series Hardware Appendix D: Sky Enterprise Services Appendix B: Virtual SRX Appendix E Junos Space Security Director Appendix CCLI Prime

# Introduction to Juniper Security (IJSEC)

---

## Centres de formation dans le monde entier



## Fast Lane Institute for Knowledge Transfer (Switzerland) AG

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

[info@flane.ch](mailto:info@flane.ch), <https://www.flane.ch>