+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 12/18/2025

Register

JNCIS-SEC Certification Training

3 days (21 hours)

Overview

JNCIS-SEC is a Specialist-level certification entirely dedicated to mastering network security on Juniper SRX firewalls. Based on a high-performance flow-based security engine, the Juniper Security platform protects enterprise infrastructures with advanced policies, NAT, IPsec VPNs, and application control services.

Our JNCIS-SEC training will give you an in-depth understanding of the SRX architecture, enable you to build effective security policies, deploy complex NAT scenarios, implement IPsec VPNs, and leverage AppSecure features.

You will also learn how to diagnose incidents, analyze logs, and set up a high-availability environment suitable for production.

Part of the training is specifically dedicated to exam preparation.
JNCIS-SEC (JN0-335): detailed review of the blueprint, revision tips, best practices, and targeted exercises.

Upon completion of this training, you will be able to administer Juniper SRX firewalls on a daily basis and approach the JNCIS-SEC certification with confidence.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the security architecture of Juniper SRX firewalls.
- Configure and optimize advanced security policies.
- Implement and troubleshoot NAT and IPsec VPNs.

- Use AppSecure for application visibility and control.
- Deploy a high-availability SRX environment.
- Effectively prepare for the JNCIS-SEC (JN0-335) exam.

Target audience

- Security engineers
- Network administrators
- Security technicians
- IT professionals preparing for JNCIS-SEC certification

Prerequisites

- Good basic knowledge of TCP/IP, routing, and firewalling
- Level equivalent to JNCIA
- Previous experience working on a corporate network

JNCIS-SEC training program

[Day 1 - Morning]

Juniper security fundamentals and SRX architecture

- Introduction to the SRX range and positioning in the security architecture
- Understanding the flow-based engine and packet processing
- Security zones, interfaces, and segmentation model
- Configuration objects: Address Book, applications, services
- Basics of Juniper security strategy
- Hands-on workshop: Getting started with an SRX and exploring flow mode.

[Day 1 - Afternoon]

Security policies: creation, logic, and best practices

- Security policy structure and evaluation order
- Address-, application-, and user-based policies
- Logging management and security decision tracking
- Organization, readability, and optimization of rules
- First steps in policy troubleshooting
- Hands-on workshop: Creating and testing a complete set of policies.

NAT: source, destination, static, and advanced scenarios

- Concepts of source NAT, destination NAT, and static NAT
- Port translation, port overloading, and specific behaviors
- Interaction between NAT and security policies
- Typical use cases: Internet access, DMZ, published access
- Diagnostic tools: traces, tables, and sessions
- Hands-on workshop: Setting up a complete NAT scenario and analyzing traffic flows.

[Day 2 - Morning]

Site-to-site IPsec VPN and remote access

- Review of IPsec concepts: IKE, Phase 1, and Phase 2
- Creating and configuring a site-to-site VPN on SRX
- Managing proposals, profiles, and encryption policies
- Common topologies: site-to-site, hub-and-spoke, multi-site
- IPsec VPN troubleshooting methods
- Hands-on workshop: Deploying and testing an IPsec VPN between two SRX devices.

[Day 2 - Afternoon]

Routing, advanced zones, and security services

- Integrating static and dynamic routing with SRX devices
- Advanced use of zones and host-inbound-traffic
- Screen protection and L3/L4 hardening options
- Critical service management
- Positioning SRX in the overall network architecture
- Hands-on workshop: Configuring secure multi-zone routing.

AppSecure: application visibility and control

- AppSecure components: AppID, AppFW, AppTrack
- Creating application-based policies
- Using AppTrack for application traffic visibility
- Analysis and control of critical or unauthorized applications
- Integrating AppSecure with existing security policies
- Hands-on workshop: Implementing AppTrack and AppFW on a real-world case study.

[Day 3 - Morning]

SRX high availability and redundancy

- Principles of chassis clustering on SRX
- Active/passive modes and failover scenarios
- State and session synchronization

- Monitoring critical links, interfaces, and paths
- Best practices for HA deployment in production
- Hands-on workshop: Configuring an SRX cluster and failover testing.

[Day 3 - Afternoon]

Detection, prevention, and monitoring

- Using logs, events, and traffic logs
- Troubleshooting tools: flow sessions, captures, traceoptions
- Detection of anomalies and common attacks
- Integration with monitoring or SIEM tools
- Best practices for daily operation of an SRX
- Hands-on workshop: Incident analysis and advanced diagnostics.

Preparation for JNCIS-SEC certification (JN0-335)

- Structure, format, and requirements of the JNCIS-SEC exam
- Detailed review of the official blueprint domains
- Common pitfalls and methods for analyzing questions
- Revision plan: documentation, labs, Juniper resources
- Time management and answer validation strategies
- Hands-on workshop: Taking the practice exam + correction.

Companies involved

This training is aimed at both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Placement at the start of training

The placement test at the start of the training course complies with Qualiopi quality criteria. Once they have finalized their registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training course, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and

reflection sessions and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.