# Juniper Networks Certified Internet Specialist (Security)


The Juniper Networks Certification Program (JNCP) Junos Security certification track is a program that allows participants to demonstrate competence with Juniper Networks technology. Successful candidates demonstrate thorough understanding of security technology in general and Junos software for SRX Series devices.This course covers the configuration, operation, and implementation of SRX Series Services Gateways in a typical network environment. Key topics within this course include security technologies such as security zones, security policies, intrusion detection and prevention (IDP), Network Address Translation (NAT), and high availability clusters, as well as details pertaining to basic implementation, configuration, and management. Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring the Junos OS and monitoring device operations. This course uses Juniper Networks SRX Series Services Gateways for the hands-on component, but the lab environment does not preclude the course from being applicable to other Juniper hardware platforms running the Junos OS.

**Prerequisites**

Students should have basic networking knowledge and an understanding of the Open Systems Interconnection (OSI)

reference model and the TCP/IP protocol suite. Students should also attend the *Introduction to the Junos Operating*

*System* (IJOS) course and the *Junos Routing Essentials* (JRE) course, or have equivalent experience prior to attending this

class.

**JNCIS Security Syllabus:**

**Junos for security Platform**

**Introduction to Junos Security**

- Traditional Routing
- Traditional Security
- The Junos OS Architecture

**Zones**

- The Definition of Zones
- Zone Configuration
- Monitoring Security Zones
- Lab 1: Configuring and Monitoring Zones

**Security Policies**

- Security Policy Overview
- Junos ALGs
- Policy Components
- Verifying Policy Operation
- Policy Scheduling and Rematching
- Policy Case Study
- Lab 2: Security Policies

**Firewall User Authentication**

- Firewall User Authentication Overview
- Pass-Through Authentication
- Web Authentication
- Client Groups
- Using External Authentication Servers
- Verifying Firewall User Authentication
- Lab 3: Configuring Firewall Authentication

**Screen Options**

- Multilayer Network Protection
- Stages and Types of Attacks
- Using Junos Screen Options—Reconnaissance Attack Handling
- Using Junos Screen Options—Denial of Service Attack Handling
- Using Junos Screen Options—Suspicious Packets Attack Handling
- Applying and Monitoring Screen Options
- Lab 4: Implementing Screen Options

**Network Address Translation**

- NAT Overview

- Source NAT Operation and Configuration
- Destination NAT Operation and Configuration
- Static NAT Operation and Configuration
- Proxy ARP
- Monitoring and Verifying NAT Operation
- Lab 5: Network Address Translation

**IPsec VPNs**

- VPN Types
- Secure VPN Requirements
- IPsec Details
- Configuration of IPsec VPNs
- IPsec VPN Monitoring
- Lab 6: Implementing IPsec VPNs

**Introduction to Intrusion Detection and Prevention**

- Introduction to Junos IDP
- IDP Policy Components and Configuration
- Signature Database
- Case Study: Applying the Recommended IDP Policy
- Monitoring IDP Operation
- Lab 7: Implementing IDP

**High Availability Clustering Theory**

- High Availability Overview
- Chassis Cluster Components
- Advanced Chassis Cluster Topics

**High Availability Clustering Implementation**

- Chassis Cluster Operation
- Chassis Cluster Configuration
- Chassis Cluster Monitoring
- Lab 8: Implementing High Availability Techniques

**SRX Series Hardware and Interfaces**

- Branch SRX Platform Overview
- High End SRX Platform Overview
- SRX Traffic Flow and Distribution
- SRX Interfaces

**Junos unified Threat Management**

**UTM Overview**

- Branch Office Challenges
- UTM Feature Overview
- Design Basics
- Hardware Support
- Licensing of Features
- Lab 1: Connecting to the Lab Equipment and Testing Connectivity

**Antispam**

- Antispam Terminology
- Overview of Antispam Process
- UTM Policy Overview
- Configuration Steps
- Monitoring Antispam
- Lab 2: Configuring an Antispam Policy

**Full File-Based and Express Antivirus**

- Antivirus Terminology
- Overview of Antivirus Process
- AV Operation
- Full File-based AV Configuration
- Express AV Configuration
- Monitoring AV
- Lab 3: Antivirus Configuration and Testing

**Content and Web Filtering**

- Overview and Terminology
- Configuration

- Verification and Monitoring
- Lab 4: Configuring Content and Web Filtering



**Hyderabad:**
#304,305 Ashoka Capital building, Road Number 2 , BanjaraHills, Hyderabad, Telangana, India – 500034.
Ph: 8686348800, 040-66446695 | leads@firewalllearning.com