

Security, Associate (JNCIA-SEC)

Earn an associate-level certification that demonstrates understanding of security technology and Junos OS software for SRX Series devices

One of four security certifications in the Security track, the Security, Associate (JNCIA-SEC), is designed for networking professionals with beginner to intermediate knowledge of the Junos® operating system for Juniper Networks® SRX Series Services Gateways. The written exam for this associate-level certification verifies your understanding of security technologies and related platform configuration and troubleshooting skills.

Exam Preparation

We recommend the following resources to help you prepare for your exam. However, these resources aren't required, and using them doesn't guarantee you'll pass the exam.

Recommended Training

- [Introduction to Juniper Security](#)

Exam Resources

- Industry/product knowledge
- [Juniper TechLibrary](#)

Additional Preparation

- [Juniper Learning Portal](#)

Exam Objectives

Here is a high-level view of the skillset required to successfully complete the JNCIA-SEC certification exam.

SRX Series Service Gateways

Identify concepts or general features of SRX Series devices:

- General Junos architecture
- Interfaces
- Hardware
- Initial configuration
- Traffic flow/security processing
- J-Web
- Juniper vSRX Virtual Firewall

Junos OS Security Objects

Identify the concepts or general functionalities of security zone, screen, address, or application objects.

- Zones
- Screens
- Addresses
- Applications and Application Layer Gateways (ALGs)

Security Policies

Describe the concepts, benefits, or operation of security policies:

- Zone-based policies
- Global policies
- Unified security policies

Network Address Translation

Describe the concepts, benefits, or operation of Network Address Translation (NAT):

- Source NAT
- Destination NAT
- Static NAT

Content Security

Identify the concepts, benefits, or operation of content security (formerly Unified Threat Management).

- Content filtering
- Web filtering
- Antivirus
- Antispam

Monitoring and Troubleshooting

Describe methods for monitoring, logging, or troubleshooting for Juniper security solutions:

- Troubleshooting security policies
- Validating behaviors
- Monitoring the packet flow process

Exam Details

Exam questions are derived from the recommended training and the exam resources listed in this flyer. Pass/fail status is available immediately after taking the exam. The exam is only provided in English.

Exam Code

JN0-232

Prerequisite Certification

None

Delivered by

Pearson VUE

Exam Length

90 minutes

Exam Type

65 multiple-choice questions

Recertification

Juniper certifications are valid for three years. For more information, see [Recertification](#).

About Juniper Networks

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Mist™, Juniper's AI-native networking platform, is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud.

Additional information can be found at juniper.net or connect with Juniper on [X](#) (formerly Twitter), [LinkedIn](#), and [Facebook](#).

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701



Copyright 2024 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.