

Introduction to Juniper Security (IJSEC)

Duration: 3 Days **Course Code: JUN_IJSEC** **Delivery Method: Virtual Learning**

Overview:

This three-day course provides students with the foundational knowledge required to work with the Junos operating system and to configure Junos security devices.

The course provides a brief overview of the Juniper security products and discusses the key architectural components of the Junos software. Key topics include UI options with a heavy focus on CLI, configuration tasks typically associated with the initial setup of devices, interface configuration basics with configuration examples, secondary system configuration, and the basics of operational monitoring and maintenance of Junos Security devices.

The course then delves into foundational knowledge of security objects, security policies, and configuration examples including types of security objects, security policies, security services NAT, site-to-site IPsec VPN, and Juniper Secure Connect VPN.

Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring Junos OS and monitoring basic device operations on the SRX device.

This course is based on Junos OS Release 21.2R1.10.

Course Level

Introduction to Juniper Security (IJSEC) is an introductory level course.

Relevant Juniper Product

• SRX Series • Juniper Connected Security • Juniper AppSecure • Juniper Sky ATP

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

This course benefits individuals responsible for configuring and monitoring Juniper Security devices.

Objectives:

- • Describe Juniper Networks connected security device framework
- • Describe SRX Series device features
- • Describe initial and basic configuration
- • Describe and demonstrate the Junos CLI options
- • Configure security zone and screen objects
- • Configure address and service objects
- • Implement security policies
- • Describe IPS and implement IPS policies
- • Describe user-based firewall and implement integrated user-based firewall
- • Describe UTM—Antivirus and Antispam
- • Describe UTM—Content Filtering and Web Filtering
- • Describe JATP Cloud Features
- • Implement Source NAT
- • Implement Destination and Static NAT
- • Implement Site-to-Site IPsec VPN
- • Describe SSL VPN by using Juniper Secure Connect
- • Administer and Troubleshoot Security Services on an SRX Series Device
- • Describe Monitoring and Reporting Features on the SRX Series Device

Prerequisites:

- Basic networking knowledge

Testing and Certification

JNCIA-SEC exam topics are based on the content of the recommended instructor-led training courses, as well as the additional

- Basic understanding of the Open Systems Interconnection (OSI) reference model
- Basic understanding of the TCP/ IP protocol suite

resources.

- Exam code: JN0-230
- Administered by Pearson VUE
- Exam length: 90 minutes
- Exam type: 65 multiple-choice questions
- Scoring and pass/fail status is available immediately
- Junos Software Release: 19.1

The JNCIA-SEC certification is valid for three years.

Exams can be purchased and scheduled at
<https://home.pearsonvue.com/junipernetworks/>

Follow-on-Courses:

Juniper Security (JSEC)

Content:

DAY 1	<ul style="list-style-type: none">• Implement security policy for a given use case	<ul style="list-style-type: none">• Configure and monitor static NAT
Course Introduction	Lab 3: Creating Security Policies	Lab 7: Implementing NAT
Juniper Connected Security	Security Services—IPS	Site-to-Site IPsec VP
<ul style="list-style-type: none">• Identify the high-level security challenges in today's network	<ul style="list-style-type: none">• Explain the purpose of IPS	<ul style="list-style-type: none">• Describe the high-level overview and configuration options for IPsec VPN
<ul style="list-style-type: none">• Describe basic network security design	<ul style="list-style-type: none">• Define the IPS policy components	<ul style="list-style-type: none">• Implement IPsec VPN for a given use case
<ul style="list-style-type: none">• Identify the key factors in Juniper Networks security focus	<ul style="list-style-type: none">• Configure IPS policies	<ul style="list-style-type: none">• Describe the functionality of proxy-id and traffic selectors
Juniper SRX Overview	Security Services—Integrated User-Based Firewall	<ul style="list-style-type: none">• Monitor site-to-site IPsec VPN
<ul style="list-style-type: none">• Describe the Junos architecture and SRX features	<ul style="list-style-type: none">• Explain the purpose of user-based firewall	Lab 8: Implementing IPsec VPN
<ul style="list-style-type: none">• Explain the traffic processing and logical packet flow on an SRX Series device	<ul style="list-style-type: none">• Configure integrated user-based firewall	Juniper Secure Connect
<ul style="list-style-type: none">• Describe the Junos J-Web UI and its features	Lab 4: Security Services—IPS Integrated User Firewall	<ul style="list-style-type: none">• Describe Juniper Secure Connect features
Juniper SRX Initial Configuration	UTM—Antivirus and Antispam	<ul style="list-style-type: none">• Explain Juniper Secure Connect UI options
<ul style="list-style-type: none">• List and perform initial configuration tasks	<ul style="list-style-type: none">• Describe the purpose of UTM services	<ul style="list-style-type: none">• Deploy Juniper Secure Connect
<ul style="list-style-type: none">• Perform basic interface configuration tasks	<ul style="list-style-type: none">• Explain antispam and its functionality	<ul style="list-style-type: none">• Monitor Juniper Secure Connect
Lab 1: Initial System Configuration	UTM—Content Filtering and Web Filtering	Lab 9: Implementing Juniper Secure Connect
UI Options – The Junos CLI	<ul style="list-style-type: none">• Explain the functionality of Content filtering	SRX Troubleshooting
<ul style="list-style-type: none">• Perform Junos CLI basics	<ul style="list-style-type: none">• Explain the functionality of Web filtering	<ul style="list-style-type: none">• Discuss SRX and vSRX licensing
<ul style="list-style-type: none">• Describe Junos operational mode	Lab 5: Implementing UTM Virtual SRX	<ul style="list-style-type: none">• Describe how to use packet capture
<ul style="list-style-type: none">• Describe Junos configuration mode	Juniper Connected Security—JATP Cloud	<ul style="list-style-type: none">• Describe the traceoptions on the SRX Series device
Security Zones and Screen Objects	<ul style="list-style-type: none">• Explain the purpose of JATP	<ul style="list-style-type: none">• Discuss how to verify Content Security policy usage
<ul style="list-style-type: none">• Describe and configure security zones objects	<ul style="list-style-type: none">• Describe the features of JATP	Monitoring and Reporting

• Describe and configure screen objects	• Describe the process to enroll devices with JATP cloud	• Explain the basic monitoring features
Address Objects and Service Objects	• Monitor JATP	• Explain the use of network utility tools on the SRX Series device
• Describe and configure address objects	Lab 6: JATP Overview	• Describe the procedure of maintaining Junos OS
• Describe and configure service objects	DAY 3	• Identify the various reports available on SRX J-Web interface
Lab 2: Creating Security Objects	Source Network Address Translation	Lab 10: Monitoring and Reporting
DAY 2	• Describe the purpose and functionality of NAT and PAT	The following appendices can be covered - time permitting - if requested by the delegate/s at the time of booking the course:
Security Policies	• Configure and monitor source NAT	SRX Series Hardware and Interfaces
• Describe the purpose and types of security policies	• Explain the purpose of proxy ARP	Virtual SRX
• Define the security policy components	Destination Network Address Translation and Static Network Address Translation	Juniper Sky Enterprise
• Configure an application firewall with unified security policies	• Configure and monitor destination NAT	IPsec VPN Concepts

Additional Information:

Delegates will receive an official set of e-kit courseware approximately 1 week prior to the start of the course.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK