Introduction to Juniper Security (IJSEC)

Duration: 3 Days **Course Code: JUN_IJSEC**

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

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

• Basic understanding of the Open Systems Interconnection (OSI) reference model

• Basic understanding of the TCP/ IP protocol suite

Testing and Certification

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

Course Introduction

Juniper Connected Security

• Identify the high-level security challenges in today's network

• Describe basic network security design

• Identify the key factors in Juniper Networks security focus

Juniper SRX Overview

• Describe the Junos architecture and SRX features

• Explain the traffic processing and logical packet flow on an SRX Series device

• Describe the Junos J-Web UI and its features

Juniper SRX Initial Configuration

• List and perform initial configuration tasks

• Perform basic interface configuration tasks

Lab 1: Initial System Configuration

UI Options – The Junos CLI

• Perform Junos CLI basics

• Describe Junos operational mode

• Describe Junos configuration mode

Security Zones and Screen Objects

• Describe and configure security zones objects

• Implement security policy for a given use case

Lab 3: Creating Security Policies

Security Services—IPS

• Explain the purpose of IPS

• Define the IPS policy components

• Configure IPS policies

Security Services—Integrated User-Based Firewall

• Explain the purpose of user-based firewall

• Configure integrated user-based firewall

Lab 4: Security Services—IPS Integrated User Firewall

UTM—Antivirus and Antispam

• Describe the purpose of UTM services

• Explain antispam and its functionality

UTM—Content Filtering and Web Filtering

• Explain the functionality of Content filtering

• Explain the functionality of Web filtering

Lab 5: Implementing UTM Virtual SRX

Juniper Connected Security—JATP Cloud

• Explain the purpose of JATP

• Describe the features of JATP

• Configure and monitor static NAT

Lab 7: Implementing NAT

Site-to-Site IPsec VP

• Describe the high-level overview and configuration options for IPsec VPN

• Implement IPsec VPN for a given use case

• Describe the functionality of proxy-id and traffic selectors

• Monitor site-to-site IPsec VPN

Lab 8: Implementing IPsec VPN

Juniper Secure Connect

• Describe Juniper Secure Connect features

• Explain Juniper Secure Connect UI options

• Deploy Juniper Secure Connect

• Monitor Juniper Secure Connect

Lab 9: Implementing Juniper Secure Connect

SRX Troubleshooting

• Discuss SRX and vSRX licensing

• Describe how to use packet capture

• Describe the traceoptions on the SRX Series device

• Discuss how to verify Content Security policy usage

Monitoring and Reporting

• Describe and configure screen objects

Address Objects and Service Objects

• Describe and configure address objects

• Describe and configure service objects

Lab 2: Creating Security Objects

DAY 2

Security Policies

• Describe the purpose and types of security policies

• Define the security policy components

• Configure an application firewall with unified security policies

• Describe the process to enroll devices with JATP cloud

• Monitor JATP

Lab 6: JATP Overview

DAY 3

Source Network Address Translation

• Describe the purpose and functionality of NAT and PAT

• Configure and monitor source NAT

• Explain the purpose of proxy ARP

Destination Network Address Translation and Static Network Address Translation

• Configure and monitor destination NAT

• Explain the basic monitoring features

• Explain the use of network utility tools on the SRX Series device

• Describe the procedure of maintaining Junos OS

• Identify the various reports available on SRX J-Web interface

Lab 10: Monitoring and Reporting

The following appendices can be covered - time permitting - if requested by the delegate/s at the time of booking the course:

SRX Series Hardware and Interfaces

Virtual SRX

Juniper Sky Enterprise

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