

Introduction to Juniper Security

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

COURSE LEVEL

Introductory

AUDIENCE

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

PREREQUISITES

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

RELEVANT JUNIPER PRODUCT

- SRX Series
- Juniper Connected Security
- Juniper AppSecure
- Juniper ATP

ASSOCIATED CERTIFICATION

[JNCIA-SEC](#)

CONTACT YOUR REGIONAL EDUCATION SERVICES TEAM:

- Americas: training-amer@juniper.net
- EMEA: training-emea@juniper.net
- APAC: training-apac@juniper.net

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

COURSE CONTENTS

DAY 1

| | |
|----------|---|
| 1 | Course Introduction |
| 2 | Juniper Connected Security <ul style="list-style-type: none"> Identify the high-level security challenges in today's network Describe basic network security design Identify the key factors in Juniper Networks security focus |
| 3 | Juniper SRX Series Overview <ul style="list-style-type: none"> 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 |
| 4 | Juniper SRX Initial Configuration <ul style="list-style-type: none"> List and perform initial configuration tasks Perform basic interface configuration tasks Lab 1: Initial System Configuration |
| 5 | UI Options - The Junos CLI <ul style="list-style-type: none"> Perform Junos CLI basics Describe Junos operational mode Describe Junos configuration mode |
| 6 | Security Zones and Screen Objects <ul style="list-style-type: none"> Describe and configure security zones objects Describe and configure screen objects |
| 7 | Address Objects and Service Objects <ul style="list-style-type: none"> Describe and configure address objects Describe and configure service objects Lab 2: Creating Security Objects |

DAY 2

| | |
|-----------|--|
| 8 | Security Policies <ul style="list-style-type: none"> Describe the purpose and types of security policies Define the security policy components Configure an application firewall with unified security policies Implement security policy for a given use case Lab 3: Creating Security Policies |
| 9 | Security Services—IPS <ul style="list-style-type: none"> Explain the purpose of IPS Define the IPS policy components Configure IPS policies |
| 10 | Security Services—Integrated User-Based Firewall <ul style="list-style-type: none"> Explain the purpose of user-based firewall Configure integrated user-based firewall Lab 4: Security Services—IPS Integrated User Firewall |
| 11 | UTM—Antivirus and Antispam <ul style="list-style-type: none"> Describe the purpose of UTM services Explain antispam and its functionality |
| 12 | UTM—Content Filtering and Web Filtering <ul style="list-style-type: none"> Explain the functionality of Content filtering Explain the functionality of Web filtering Lab 5: Implementing UTM Virtual SRX |
| 13 | Juniper Connected Security—JATP Cloud <ul style="list-style-type: none"> Explain the purpose of JATP Describe the features of JATP Describe the process to enroll devices with JATP Cloud Monitor JATP Lab 6: JATP Overview |

Continued on the next page

COURSE CONTENTS

DAY 3

- 14 Source Network Address Translation**
- Describe the purpose and functionality of NAT and PAT
 - Configure and monitor source NAT
 - Explain the purpose of proxy ARP

- 15 Destination Network Address Translation and Static Network Address Translation**
- Configure and monitor destination NAT
 - Configure and monitor static NAT

Lab 7: Implementing NAT

- 16 Site-to-Site IPsec VPN**
- 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

- 17 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

- 18 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

- 19 Monitoring and Reporting**
- 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

APPENDICES

- A SRX Series Hardware and Interfaces**

- B Virtual SRX**

- C Juniper Sky Enterprise**

- D IPsec VPN Concepts**

IJSEC05262022