Introduction to Juniper Security

Course overview

This three-day, introductory-level course provides students with the knowledge to secure their network using SRX Series Firewalls. Key topics include security zones, security policies, content security, and Network Address Translation (NAT).
Through demonstrations and hands-on labs, students will gain experience with each of these concepts. This course is based on OS Release 24.2R1.17.

Course level

Introduction to Juniper Security is an introductory-level course.

Audience

The primary audiences for this course include:

- Individuals who are responsible for network security.
- Individuals who want to learn how to secure their networks using SRX Series Firewalls.

Prerequisites

- Basic networking skills.
- General understanding of networking architecture.

Related products

SRX Series

Related certification

JNCIA-Sec

Recommended Next Course

Juniper Security

Objectives

- Describe Junos OS architecture.
- Describe SRX Series security architecture.
- Create security and functional zones.
- Configure screen options.
- Configure address and application objects.
- Implement traditional security policies.
- Implement unified security policies.
- Configure security policy logging, counting, and scheduling.
- Troubleshoot security policies.
- Enable application tracking.
- Implement antivirus and antispam capabilities.
- Enable content filtering and Web filtering.
- Configure source NAT.
- Configure destination NAT.
- Configure static NAT.

Course contents

Day 1

Module 01: Introduction to Juniper Security

- Explain the challenges faced by network security administrators
- Describe the physical and virtual device options of the SRX Series Firewall
- Explain the SRX Series management options

Module 02: Juniper SRX Series Security Architecture

- Explain the Junos OS architecture
- Explain the SRX Series security architecture
- Explain SRX Series traffic processing

Module 03: Managing Zones

- Explain security zones and functional zones
- Configure security zones
- Use screen options

Lab 01: Managing Zones

Module 04: Managing Addresses, Applications, and ALGs

- Create address objects
- Create applications
- Use ALGs

Lab 02: Managing Addresses and Applications

Day 2

Module 05: Managing Traditional Security Policies

- Explain traditional security policy processing
- Create traditional security policies
- Modify, reorder, deactivate, and delete security policies

Lab 03: Managing Traditional Security Policies

Module 06: Managing Unified Security Policies

- Describe AppID
- Implement unified security policies

Lab 04: Managing Unified Security Policies

Module 07: Configuring Security Policy Options

- Implement security policy logging and counting
- Create schedulers
- Examine session options

Lab 05: Configuring Security Policy Options

Module 08: Troubleshooting Security Policies

- Troubleshoot the flow process
- Enable trace options

Lab 06: Troubleshooting Security Policies

Module 09: Implementing AppTrack

- Explain AppSecure capabilities
- Configure AppTrack

Lab 07: Implementing AppTrack

Day 3

Module 10: Implementing Antivirus and Antispam

- Describe content security
- Configure antivirus
- Configure antispam

Lab 08: Implementing Antivirus and Antispam

Module 11: Implementing Content Filtering and NextGen Web Filtering

- Explain content filtering and NextGen Web Filtering
- Configure content filtering
- Configure NextGen Web Filtering

Lab 09: Implementing Content Filtering and NextGen Web Filtering

Module 12: Implementing Source NAT

- Explain source NAT
- Configure interface-based source NAT
- Configure pool-based source NAT
- Implement proxy ARP

Lab 10: Implementing Source NAT

Module 13: Implementing Destination NAT and Static NAT

- Explain destination NAT
- Configure destination NAT
- Configure static NAT

Lab 11: Implementing Destination NAT and Static NAT

Resources

All-Access Training Pass

On-Demand

Courses

Schedule

Learning Paths

Certification

Key contacts

Americas: networking.training.ams@hpe.com

Europe, Middle East, Africa: networking.training.emea@hpe.com

Asia Pacific & Japan:-networking.training.apj@hpe.com

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.
Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Trademark acknowledgments, if needed. All third-party marks are property of their respective owners.

EDU-JUN-IJSEC, Revision 25A.1

HPE.com