

Junos for Security Platforms

Course No: EDU-JUN-JSEC

Length: Three days

About this Course

This three-day course covers configuration, operation, and implementation of SRX Series Services Gateways in a typical network environment. Key topics within this course include security technologies such as security zones, security policies, intrusion detection and prevention (IDP), Network Address Translation (NAT), and high availability clusters, as well as details pertaining to basic implementation, configuration, and management. This course is based on Junos operating system Release 10.1R1.8.

Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring the Junos OS for SRX Series devices.

Objectives

After successfully completing this course, you should be able to:

- Describe traditional routing and security and the current trends in internetworking.
- Provide an overview of SRX Series devices and software architecture.
- Describe the logical packet flow and session creation performed by SRX Series devices.
- Describe, configure, and monitor zones.
- Describe, configure, and monitor security policies.
- Describe, configure, and monitor firewall user authentication.
- Describe various types of network attacks.
- Configure and monitor SCREEN options to prevent network attacks.
- Explain, implement, and monitor NAT on Junos security platforms.
- Explain the purpose and mechanics of IP Security (IPsec) virtual private networks (VPNs).
- Implement and monitor policy-based and route-based IPsec VPNs.
- Utilize and update the IDP signature database.
- Configure and monitor IDP policy with policy templates.
- Describe, configure, and monitor high availability chassis clusters.

Intended Audience

This course benefits operators of SRX Series devices. These operators include network engineers, administrators, support personnel, and reseller support personnel.

Course Level

JSEC is an intermediate-level course.

Prerequisites

Students should have basic networking knowledge and an understanding of the Open Systems Interconnection (OSI) reference model and the TCP/IP protocol suite. Students should also either attend the *Introduction to Junos Software* (IJS) and *Junos Routing Essentials* (JRE) courses prior to attending this class, or have equivalent experience with the Junos OS.

Course Contents

Day 1

Chapter 1: Course Introduction

Chapter 2: Introduction to Junos security platforms

- Traditional Routing
- Traditional Security
- Breaking the Tradition
- The Junos OS Architecture

Chapter 3: Zones

- The Definition of Zones
- Zone Configuration
- Monitoring Security Zones
- Lab 1: Configuring and Monitoring Zones

Chapter 4: Security Policies

- Overview of Security Policy
- Policy Components
- Verifying Policy Operation
- Policy Scheduling and Rematching
- Policy Case Study
- Lab 2: Security Policies

Day 2

Chapter 5: Firewall User Authentication

- Firewall User Authentication Overview
- Pass-Through Authentication
- Web Authentication
- Client Groups
- Using External Authentication Servers
- Verifying Firewall User Authentication
- Lab 3: Configuring Firewall Authentication

Chapter 6: SCREEN Options

- Multilayer Network Protection
- Stages and Types of Attacks
- Using Junos SCREEN Options—Reconnaissance Attack Handling
- Using Junos SCREEN Options—Denial of Service Attack Handling

- Using Junos SCREEN Options—Suspicious Packets Attack Handling
- Applying and Monitoring SCREEN Options
- Lab 4: Implementing SCREEN Options

Chapter 7: Network Address Translation

- NAT Overview
- Source NAT Operation and Configuration
- Destination NAT Operation and Configuration
- Static NAT Operation and Configuration
- Proxy ARP
- Monitoring and Verifying NAT Operation
- Lab 5: Network Address Translation

Day 3

Chapter 8: IPsec VPNs

- VPN Types
- Secure VPN Requirements
- IPsec Details
- Configuration of IPsec VPNs
- IPsec VPN Monitoring
- Lab 6: Implementing IPsec VPNs

Chapter 9: Introduction to Intrusion Detection and Prevention

- Introduction to Junos IDP
- IDP Policy Components and Configuration
- Signature Database
- Case Study: Applying the Recommended IDP Policy
- Monitoring IDP Operation
- Lab 7: Implementing IDP

Chapter 10: High Availability Clustering

- High Availability Overview
- Chassis Cluster Components
- Chassis Cluster Operation
- Chassis Cluster Configuration
- Chassis Cluster Monitoring
- Lab 8: Implementing Chassis Clusters