Advanced Junos Security (AJSEC)

Engineering Simplicity

COURSE LEVEL

Advanced Junos Security (AJSEC) is an advanced-level course.

AUDIENCE

This course benefits individuals responsible for implementing, monitoring, and troubleshooting Junos security components.

PREREQUISITES

Students should have a strong level of TCP/IP networking and security knowledge. Students should also attend the Introduction to the Junos Operating System (IJOS) and Junos Security (JSEC) courses prior to attending this class.

ASSOCIATED CERTIFICATION

JNCIP-SEC

RELEVANT JUNIPER PRODUCT

- Security
- Junos OS
- SRX Series
- vSRX Series
- Sky ATP
- SDSN

RECOMMENDED NEXT COURSE

JNCIE-SEC Bootcamp

CONTACT INFORMATION

training@juniper.net

COURSE OVERVIEW

This five-day course, which is designed to build off the current Junos Security (JSEC) offering, delves deeper into Junos security and next-generation security features. Through demonstrations and hands-on labs, you will gain experience in configuring and monitoring the advanced Junos OS security features with advanced coverage of virtualization, AppSecure, advanced logging and reporting, next generation Layer 2 security, user firewall, next generation advanced anti-malware with Sky ATP, next generation security intelligence with software-defined secure networks. This course uses Juniper Networks SRX Series Services Gateways for the hands-on component.

This course is based on Junos OS Release 15.1X49-D90.7 and Junos Space Security Director 16.2.

OBJECTIVES

- Demonstrate understanding of concepts covered in the prerequisite Junos Security course.
- Describe the various forms of security supported by the Junos OS.
- Implement features of the AppSecure suite, including AppID, AppFW, AppTrack, AppQoS, and SSL Proxy.
- Configure custom application signatures.
- Describe Junos security handling at Layer 2 versus Layer 3.
- Implement next generation Layer 2 security features.
- Demonstrate understanding of Logical Systems (LSYS).
- Describe Junos routing instance types used for virtualization.
- Implement virtual routing instances in a security setting.
- Describe and configure route sharing between routing instances using logical tunnel interfaces.
- Describe and discuss Sky ATP and its function in the network.
- Describe and configure UTM functions.
- Discuss IPS and its function in the network.
- Implement IPS policies.
- Describe and implement SDSN and Policy Enforcer in a network.
- Describe the purpose of SSL proxy.
- Implement client-protection SSL proxy.
- Implement server-protection SSL proxy.
- Describe and implement user role firewall in a network.
- Demonstrate the understanding of user firewall.

COURSE CONTENT

Day 1

1 COURSE INTRODUCTION

2 Junos Layer 2 Packet Handling and Security Features

- Transparent Mode Security
- Secure Wire
- Layer 2 Next Generation Ethernet Switching
- MACsec

LAB 1: Implementing Layer 2 Security

3 Virtualization

- Virtualization Overview
- Routing Instances
- Logical Systems

LAB 2: Implementing Junos Virtual Routing

4 AppSecure Theory

- AppSecure Overview
- AppID Overview
- Installing the Application Signature Package
- Customer Application Signatures
- Application System Cache

Day 2

5 AppSecure Implementation

- AppTrack
- AppFW
- AppQoS
- APBR

LAB 3: Implementing AppSecure

6 Sky ATP Concepts and Setup

- Sky ATP Overview
- Sky ATP Features
- Sky ATP Setup
- Sky ATP Enrollment Troubleshooting

7 Sky ATP Implementation

- Configuring Sky ATP using the Web UI
- Configuring Sky ATP with Security Director
- Monitoring Infected Hosts
- Infected Host Case Study

LAB 4: Implementing Sky ATP Demo

Day 3

8 SDSN with Policy Enforcer

- Policy Enforcer Overview
- Configuring Policy Enforcer and SDSN
- Infected Host Case Study

LAB 5: Implementing SDSN with Policy Enforcer

9 Implementing UTM

- UTM Overview
- AntiSpam
- AntiVirus
- Content and Web Filtering

LAB 6: Implementing UTM

Day 4

10 Introduction to IPS

- IPS Overview
- Network Asset Protection
- Intrusion Attack Methods
- Intrusion Prevention Systems
- IPS Inspection Walkthrough

11 IPS Policy and Configuration

- SRX IPS Requirements
- IPS Operation Modes
- Basic IPS Policy Review
- IPS Rulebase Operations

LAB 7: Implementing Basic IPS Policy

12 SSL Proxy

- SSL Proxy Overview
- Client-Protection SSL Proxy
- Server-Protection SSL Proxy
- SSL Proxy Case Study

Day 5

13 User Authentication

- User Role Firewall and Integrated User Firewall Overview
- User Role Firewall Implementation
- Monitoring User Role Firewall
- Integrated User Firewall Implementation
- Monitoring Integrated User Firewall

LAB 8: Implementing User Integrated Firewall

14 Monitoring and Reporting

- Log Director Overview
- Log Director Installation
- Working with Log Events
- Alerts and Reports

LAB 9: Deploying Log Director

Appendix A: SRX Series Hardware and Interfaces

- Branch SRX Platform Overview
- High End SRX Platform Overview
- SRX Traffic Flow and Distribution
- SRX Interfaces

Appendix B: Virtual SRX

- Virtualization Overview
- Network Virtualization and Software-Defined Networking
- Overview of the vSRX Platform
- Deployment Scenarios for the vSRX
- Integrating vSRX with AWS