AJSEC
Advanced Junos Security

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.

Intended Audience

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

Course Level

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

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

Objectives

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

- 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 Length

5 Days

Course Contents

Day 1

- Course Introduction
- 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
- Virtualization
  - Virtualization Overview
  - Routing Instances
  - Logical Systems
  - Lab 2: Implementing Junos Virtual Routing

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

Day 2

- AppSecure Implementation
  - AppTrack
  - AppFW
  - AppQoS
  - APBR
  - Lab 3: Implementing AppSecure
- Sky ATP Concepts and Setup
  - Sky ATP Overview
  - Sky ATP Features
  - Sky ATP Setup
  - Sky ATP Enrollment Troubleshooting
- 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

- SDSN with Policy Enforcer
  - Policy Enforcer Overview
  - Configuring Policy Enforcer and SDSN
  - Infected Host Case Study
  - Lab 5: Implementing SDSN with Policy Enforcer
- Implementing UTM
  - UTM Overview

- AntiSpam
- AntiVirus
- Content and Web Filtering
- Lab 6: Implementing UTM

Day 4

- Introduction to IPS
  - IPS Overview
  - Network Asset Protection
  - Intrusion Attack Methods
  - Intrusion Prevention Systems
  - IPS Inspection Walkthrough
- IPS Policy and Configuration
  - SRX IPS Requirements
  - IPS Operation Modes
  - Basic IPS Policy Review
  - IPS Rulebase Operations
  - Lab 7: Implementing Basic IPS Policy
- SSL Proxy
  - SSL Proxy Overview
  - Client-Protection SSL Proxy
  - Server-Protection SSL Proxy
  - SSL Proxy Case Study

Day 5

- 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: Configure User Role Firewall and Integrated User Firewall
- 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

Certification Information

- JNCIP-SEC