Advanced Junos Security - 4 days

Learn via: **Classroom**
Duration: **4 Days**

Overview

This five-day course, which is designed to build off of the current Junos Security (JSEC) offering, delves deeper into Junos security.

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 Network Address Translation (NAT) deployments, Layer 2 security, and Sky ATP.

This course uses Juniper Networks SRX Series Services Gateways for the hands-on component. This course is based on Junos OS Release 15.1X49-D70.3 and Junos Space Security Director 16.1.

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.

What You Will Learn

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).
• Use Junos debugging tools to analyze traffic flows and identify traffic processing patterns and problems.
• 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.
• Utilize Junos tools for troubleshooting Junos security implementations.
• Perform successful troubleshooting of some common Junos security issues.
• 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 policy.
• Describe and implement SDSN in a network.
• Describe and implement user role firewall in a network.
• Demonstrate the understanding of integrated user firewall.
Contents

Outline

Day 1

Chapter 1: Course Introduction

Chapter 2: Junos Layer 2 Packet Handling and Security Features
• Transparent Mode Security
• Secure Wire
• Layer 2 Next Generation Ethernet Switching
• MACsec
• Lab 2: Implementing Layer 2 Security

Chapter 3: Virtualization
• Virtualization Overview
• Routing Instances
• Logical Systems
• Lab 3: Implementing Junos Virtual Routing

Chapter 4: AppSecure Theory
• AppSecure Overview
• AppID Overview
• AppID Techniques
• Application System Cache
• Custom Application Signatures

Day 2

Chapter 5: AppSecure Implementation
• AppTrack
• AppFW
• AppQoS
• APBR
• SSL Proxy
• Lab 4: Implementing AppSecure

Chapter 6: Working with Log Director
• Log Director Overview
• Log Director Components
• Installing and setting up Log Director
• Clustering with the Log Concentrator VM
• Administrating Log Director
• Lab 5: Deploying Log Director

Day 3

Chapter 7: Sky ATP Theory
• Sky ATP Overview
• Monitoring Sky ATP
• Analysis and Detection of Malware
Chapter 8: Sky ATP Implementation
• Configuring Sky ATP
• Installing Sky ATP
• Analysis and detection of Malware
• Infected Host Case Study
• Lab 6: Instructor Led Sky ATP Demo

Chapter 9: Implementing UTM
• UTM Overview
• AntiSpam
• AntiVirus
• Content and Web Filtering
• Lab 7: Implementing UTM

Day 4

Chapter 10: Introduction to IPS
• IPS Overview
• Network Asset Protection
• Intrusion Attack Methods
• Intrusion Prevention Systems
• IPS Inspection Walkthrough
Chapter 11: IPS Policy and Configuration

• SRX IPS Requirements
• IPS Operation Modes
• Basic IPS Policy Review
• IPS Rulebase Operations
• Lab 8: Implementing Basic IPS Policy

Day 5

Chapter 12: SDSN
• SDSN Overview
• SDSN Components
• SDSN Configuration
• Policy Enforcer Troubleshooting
• SDSN Use Cases
• Lab 9: Implementing SDSN

Chapter 13: Enforcement, Monitoring, and Reporting
• 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 10: Configure User Role Firewall and Integrated User Firewall

Chapter 14: Troubleshooting Junos Security
• Troubleshooting Methodology
• Troubleshooting Tools
• Identifying IPsec Issues
• Lab 11: Performing Security Troubleshooting Techniques

Appendix A: SRX Series Hardware and Interfaces
• Branch SRX Platform Overview
• High End SRX Platform Overview
• SRX Traffic Flow and Distribution
• SRX Interfaces