ADVANCED JUNOS SECURITY

DURATION: 5 DAYS

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, App Secure, 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.

TARGET AUDIENCE

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

COURSE OBJECTIVES

1. Demonstrate understanding of concepts covered in the prerequisite Junos Security course.
2. Describe the various forms of security supported by the Junos OS.
3. Implement features of the App Secure suite, including App ID, App FW, App Track, App QoS, and SSL Proxy.
4. Configure custom application signatures.
5. Describe Junos security handling at Layer 2 versus Layer 3.
6. Implement next generation Layer 2 security features.
7. Demonstrate understanding of Logical Systems (LSYS).
8. Describe Junos routing instance types used for virtualization.
9. Implement virtual routing instances in a security setting.

10. Describe and configure route sharing between routing instances using logical tunnel interfaces.
11. Describe and discuss Sky ATP and its function in the network.
12. Describe and configure UTM functions.
13. Discuss IPS and its function in the network.
14. Implement IPS policies.
15. Describe and implement SDSN and Policy Enforcer in a network.
16. Describe the purpose of SSL proxy.
17. Implement client-protection SSL proxy.
18. Implement server-protection SSL proxy.
19. Describe and implement user role firewall in a network.
20. 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

MAC sec

LAB 1: Implementing Layer 2 Security

3. Virtualization:

Virtualization Overview

Routing Instances

Logical Systems

LAB 2: Implementing Junos Virtual Routing

4 .App Secure Theory:

App Secure Overview

App ID Overview

Installing the Application Signature Package

Customer Application Signatures

Application System Cache

DAY 2:

5 .App Secure Implementation

- App Track
- App FW
- App QoS
- APBR
- LAB 3: Implementing App Secure

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
- Anti-Spam
- Anti-Virus
- 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 Rule base 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 v SRX Platform

Deployment Scenarios for the v SRX

Integrating v SRX with AWS