JUNOS for Security Platforms (JSEC)

Course 1804 – 24 Hours

Overview

This course provides students with the skills for configuration, operation, and implementation of JUNOS security platforms in a typical network environment. This course is based on JUNOS Software version 9.5R1.8.Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring JUNOS Software for JUNOS security platforms.

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

On Completion, Delegates will be able to

- Describe traditional routing and security and the current trends in internetworking;
- Provide an overview of JUNOS security platforms and software architecture;
- Describe the logical packet flow and session creation performed by JUNOS security platforms;
- 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 IPsec VPNs;
- Implement and monitor policy-based and route-based IPsec VPNs;
- Utilize and update the IDP signature database on JUNOS security platforms;
- Configure and monitor IDP policy with policy templates; and
- Describe, configure, and monitor high availability chassis clusters.

Who Should Attend

Students should have basic networking knowledge and an understanding of the OSI 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 JUNOS Software.

Course Contents

Chapter 1: Course Introduction

Chapter 2: Introduction to JUNOS security platforms

- Traditional Routing
- Traditional Security
- Breaking the Tradition
- JUNOS Software Architecture

Chapter 3: Zones

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

Chapter 4: Security Policies

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

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 Software SCREEN Options
- Applying and Monitoring SCREEN Options
- Lab 4: Implementing SCREEN Options

Chapter 7: Network Address Translation

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

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 Software IDP
- IDP Policy Components and Configuration
- Attack and 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 Clustering