IJSEC
Introduction to Juniper Security

Overview

This three-day course is designed to provide students with the foundational knowledge required to work with SRX Series devices. This course will use the J-Web user interface to introduce students to the Junos operating system. The course provides a brief overview of security problems and how Juniper Networks approaches a complete security solution with Juniper Connected Security. Key topics include configuration tasks for initial system configuration, interface configuration, security object configuration, security policy configuration, IPsec VPN configuration, and NAT configuration. The course then delves into Layer 7 security using UTM, IDP, and AppSecure to provide students with the understanding of application level security to block advanced threats. An overview of Sky ATP is included for students to understand zero-day network protection technologies. Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring the Junos OS and monitoring basic device operations. This course is based on Junos OS Release 19.1R1.6

Intended Audience

Operators of Juniper Networks security solutions, including network engineers, administrators, support personnel, and resellers.

Course Level

Introductory.

Prerequisites

- Basic networking knowledge
- Basic understanding of the Open Systems Interconnection (OSI) reference model
- Basic understanding of the TCP/ IP protocol suite

Objectives

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

- Identify high-level security challenges in today's networks.

- Identify products that are incorporated into the Juniper Connected Security solution.
- Explain the value of implementing security solutions.
- Explain how Juniper Connected Security solves the cyber security challenges of the future.
- Explain the SRX Series devices and the added capabilities that next-generation firewalls provide.
- Explain traffic flows through the SRX Series devices.
- List the different security objects and how to create them.
- Describe interface types and perform basic interface configuration tasks.
- Describe the initial configuration for a SRX Series device.
- Explain security zones.
- Describe screens and their use.
- Explain address objects.
- Describe services and their use.
- Describe the purpose for security policies on an SRX Series device.
- Describe zone-based policies.
- Describe global policies and their use.
- Explain unified security policies.
- Configure unified security policies with the J-Web user interface.
- Describe IDP signatures.
- Configure an IDP policy using predefined templates with the J-Web user interface.
- Describe the use and configuration of the integrated user firewall feature.
- Describe the UTM security services.
- List the available UTM services on the SRX Series device.
- Configure UTM filtering on a security policy with the J-Web user interface.
- Explain Sky ATP's use in security.
- Describe how Sky ATP and SRX Series devices operate together in blocking threats.
- Describe NAT and why it is used.
- Explain source NAT and when to use it.
- Explain destination NAT and when to use it.
- Explain static NAT and its uses.
- Describe the operation and configuration the different types of NAT.
- Describe IPsec VPNs and their functionality.

- Describe how IPsec VPNs are established.
- Configure IPsec VPNs with the J-Web user interface.
- Describe and configure proxy IDs and traffic selectors with the J-Web user interface.
- Monitor IPsec VPNs with the J-Web user interface.
- Describe the J-Web monitoring features.
- Explain the J-Web reporting features.
- Describe the Sky Enterprise service and how it can save resources.
- Explain the functionality of Junos Space Security Director.

Course Length

3 Days

Course Contents

Day 1

- Course Introduction
- Juniper Connected Security
  - Security Challenges
  - Security Design Overview
  - Juniper Connected Security
- Juniper Connected Security – SRX Series Devices
  - SRX Architectural Overview
  - Traffic Processing
  - J-Web Overview
  - Initial Configuration
  - Interface Configuration
  - Lab 1: Initial Configuration
- Security Objects
  - Security Zone Objects
  - Security Screen Objects
  - Security Address Objects
  - Security Services Objects
  - Lab 2: Creating Security Objects

- Security Policies
  - Security Policy Overview
  - Security Policy Components
  - Application Firewall with Unified Security Policies
  - Security Policy Case Study
  - Lab 3: Implementing Security Policies

Day 2

- Security Services – IDP and Integrated User Firewall
  - Introduction to IPS
  - IPS Policy Components
  - Configuring IPS Policies
  - User Firewall Overview
  - Configuring Integrated User Firewall
  - Lab 4: Implementing Security Services
- Security Services – UTM
  - Content Filtering
  - Web Filtering
  - Antivirus
  - Antispam
  - Lab 5: Implementing UTM
- Juniper Connected Security – SKY ATP
  - Sky ATP Overview
  - Sky ATP Features
  - Sky ATP Setup
  - Monitor Sky ATP
  - Demo: Sky ATP Overview

Day 3

- Network Address Translation
  - NAT Overview
  - Source NAT
  - Destination NAT

- Static NAT
- Lab 7: Implementing Network Address Translation

- Site-to-Site VPNs
  - IPsec Site-to-Site VPN Configuration
  - IPsec Site-to-Site VPN Case Study
  - Proxy IDs and Traffic Selectors
  - Monitoring Site-to-Site IPsec VPNs
  - Lab 8: Implementing IPsec
- Monitoring and Reporting
  - Monitor Platform and Interface Operations
  - Network Utilities
  - Maintaining the Junos OS
  - J-Web Reports
  - Lab 9: Using Monitoring and Reporting Tools

- SRX Series Hardware and Interfaces
- Virtual SRX
- Juniper Sky Enterprise
- IPsec VPN Concepts

Certification Information

- JNCIA-SEC