Introduction to Juniper Security (IJSEC)

Engineering Simplicity

COURSE LEVEL

Introductory-level course

INTENDED AUDIENCE

The primary audience for this course includes the following:

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

PREREQUISITES

The following are the prerequisites for this course:

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

ASSOCIATED CERTIFICATION

N/A

CONTACT INFORMATION

training@juniper.net

COURSE OVERVIEW

This 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.

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 an 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.

OBJECTIVES (contd.)

- 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.
- Identify various types of VPNs.
- Describe IPsec VPNs and their functionality.
- Describe how IPsec VPNs are established.
- Describe IPsec traffic processing.
- 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 CONTENT

Day 1

1 **Course Introduction**

2 **Juniper Security Concepts**

- Security Challenges
- Security Design Overview
- Juniper Connected Security

3 **Juniper Connected Security – SRX Series Devices**

- Connected Security
- Interfaces
- Initial Configuration

LAB 1: Initial Configuration

5 **Security Objects**

- Security Zone Objects
- Security Screen Objects
- Security Address Objects
- Security Services Objects

LAB 2: Creating Security Objects with J-Web

5 **Security Policies**

- Security Policy Overview
- Zone-Based Policies
- Global Security Policies
- Application Firewall with Unified Security Policies

LAB 3: Creating Security Policies with J-Web

Day 2

6 **Security Services – IDP and User Firewall**

- IDP Security Services
- Integrated User Firewall

LAB 4: Adding IDP and User Firewall Security Services to Security Policies

8 **Juniper Connected Security – Sky ATP**

- Sky ATP Overview
- Blocking Threats

Lab 6: Demonstrating Sky ATP

7 **Security Services – UTM**

- Content Filtering
- Web Filtering
- Antivirus
- Antispam

LAB 5: Adding UTM Security Services to Security Policies

9 **Network Address Translation**

- NAT Overview
- Source NAT
- Destination NAT
- Static NAT

Lab 7: Implementing Network Address Translation

Day 3

10 **IPsec VPN Concepts**

- VPN Types
- Secure VPN Requirements
- IPsec Tunnel Establishment
- IPsec Traffic Processing

12 **Monitoring and Reporting**

- J-Web Monitoring Options
- J-Web Reporting options

Lab 9: Using Monitoring and Reporting

11 **Site-to-Site VPNs**

- IPsec Configuration
- IPsec Site-to-Site Tunnel

Lab 8: Implementing Site-to-Site IPsec VPNs

A **Appendix: SRX Series Hardware**

D **Appendix: Sky Enterprise Services**

B **Appendix: Virtual SRX**

E **Appendix: Junos Space Security Director**

C **Appendix: CLI Primer**