JUNOS INTRUSION PREVENTION SYSTEM FUNCTIONALITY

DURATION: 2 DAYS

COURSE OVERVIEW

The Junos Intrusion prevention System Functionality (JIPS) course is designed to provide an introduction to the Intrusion Prevention System (IPS) feature set available on the Juniper Networks SRX Series Services Gateway. The course covers concepts, ideas, and terminology relating to providing intrusion prevention using the SRX Series platform. Hands-on labs offer students the opportunity to configure various IPS features and to test and analyze those functions.

TARGET AUDIENCE

This course is designed for:

Individuals responsible for configuring and monitoring the IPS aspects of SRX Series devices.

COURSE OBJECTIVES

Upon completing this course, the learner will be able to meet these overall objectives:

1. Describe general types of intrusions and network penetration steps.
2. Describe how to access the SRX Series Services Gateways with IPS functionality for configuration and management.
3. Configure the SRX Series Services Gateways for IPS functionality.
4. Define and describe terminology which comprises Juniper Networks IPS functionality.
5. Describe the steps that the IPS engine takes when inspecting packets.
6. Describe the components of IPS rules and rulebases.
7. Explain the types of signature-based attacks.
8. Describe the uses of custom signatures and how to configure them.
9. Explain how scanning can be used to gather information about target networks.
10. Configure screens to block various scan types.
11. Describe commonly used evasion techniques and how to block them.
12. Describe denial of service (DoS) and distributed denial of service (DDoS) attacks.

13. Explain the mechanisms available on the SRX Series device to detect and block DoS and DDoS attacks.
14. Configure screens to block DoS and DDoS attacks.
15. Describe the reporting capabilities available for IPS functionality.
16. Explain the terms and concepts related to intrusion prevention.
17. Describe the basic functions and features available on the SRX Series platform that provide IPS functionality.
18. Configure fundamental IPS features and functions on an SRX240 device.

COURSE CONTENT

Overview of IPS Functionality

- Reasons for Network Attacks
- Categories of Attacks
- Anatomy of an Attack
- IPS Mechanisms on SRX Series Devices
  - Initial Device Configuration
- Deployment Options for IPS Functionality
- Management Options
- Network Settings
- Preparing the SRX Series Device for IPS Features
  - IPS Terminology and Concepts
- Terminology Overview
- Attack Objects
- IPS Rulebase Details
- Rule Match Conditions
- Rule Actions
- Terminal Rules
- IP Actions
- Notification
- Terminology Review
- IPS Traffic Flow
  - IPS Attack Objects
- IPS Rules and Rulebases

Attack Objects

Custom Signatures

Scanning and Reconnaissance

Overview of Scanning

Types of Scans

Fingerprinting

IPS Scan Prevention

Blocking Evasion Techniques and Denial of Service

FIN Scans

IP Spoofing

IP Source Routing Options

DoS and DDoS Attacks

Mechanisms for Blocking DoS and DDoS

COURSE PREREQUISITES

The knowledge and skills that a learner must have before attending this course are as follows:

Students should have basic networking knowledge, an understanding of the Open Systems Interconnection (OSI) reference model for layered communications and computer network protocol design, and an understanding of the TCP/IP protocol suite.

To gain the prerequisite skills and knowledge, Juniper strongly recommends the knowledge of the following courses:

Introduction to the Junos Operating System (IJOS)

Junos Routing Essentials (JRE)

Junos Security (JSEC)

TEST CERTIFICATION

Recommended preparation for:

JN0-633 - Juniper Networks Certified Internet Professional (JNCIP-SEC)

JIPS is one of the courses required for the **Juniper Networks Certified Internet Professional (JNCIP-SEC)** Certification

FOLLOW ON COURSES

Advanced Junos Security (AJSEC)

JIPS and AJSEC are the courses required for the **Juniper Networks Certified Internet Professional (JNCIP-SEC)** Certification