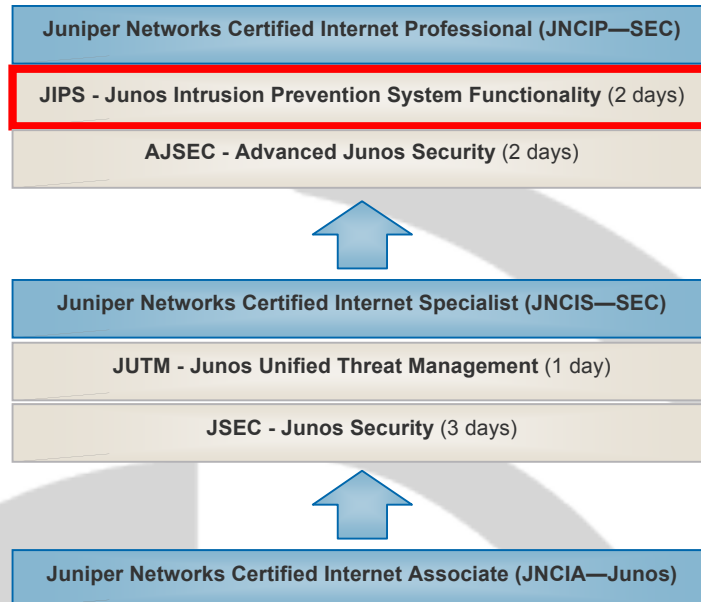




JUNIPER JUNOS SECURITY (SRX)



Junos Intrusion Prevention System Functionality (JIPS)

Course Overview

This two-day 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 analyse those functions.

Objectives

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

- Describe general types of intrusions and network penetration steps.
- Describe how to access the SRX Series Services Gateways with IPS functionality for configuration and management.
- Configure the SRX Series Services Gateways for IPS functionality.
- Define and describe terminology which comprises Juniper Networks IPS functionality.
- Describe the steps that the IPS engine takes when inspecting packets.
- Describe the components of IPS rules and rulebases.
- Explain the types of signature-based attacks.
- Describe the uses of custom signatures and how to configure them.
- Explain how scanning can be used to gather information about target networks.
- Configure screens to block various scan types.
- Describe commonly used evasion techniques and how to block them.
- Describe denial of service (DoS) and distributed denial of service (DDoS) attacks.
- Explain the mechanisms available on the SRX Series device to detect and block DoS and DDoS attacks.
- Configure screens to block DoS and DDoS attacks.
- Describe the reporting capabilities available for IPS functionality.
- Explain the terms and concepts related to intrusion prevention.
- Describe the basic functions and features available on the SRX Series platform that provide IPS functionality.
- Configure fundamental IPS features and functions on an SRX240 device.



Target Audience

This course benefits individuals responsible for configuring and monitoring the IPS aspects of SRX Series devices.

Course Level

Intermediate

Prerequisites

Students should:

- have an understanding of the OSI model.
- know the TCP/IP protocol suite

Students should attend the following courses:

- IJOS
- JRE
- JSEC

Day One

Chapter 1: Course Introduction

Chapter 2: Overview of IPS Functionality

- Reasons for Network Attacks
- Categories of Attacks
- Anatomy of an Attack
- IPS Mechanisms on SRX Series Devices
- Lab 1: Initial Configuration

Chapter 3: Initial Device Configuration

- Deployment Options for IPS Functionality
- Management Options
- Network Settings
- Preparing the SRX Series Device for IPS Features
- Lab 2: Creating a Basic Policy

Chapter 4: 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
- Lab 3: Examining and Modifying the Recommended Policy
- Lab 4: Exempt Rulebase
- Lab 5: Rule Actions

Day Two

Chapter 5: IPS Attack Objects

- IPS Rules and Rulebases
- Attack Objects
- Custom Signatures
- Lab 6: Custom Signatures

Chapter 6: Scanning and Reconnaissance

- Overview of Scanning
- Types of Scans
- Fingerprinting
- IPS Scan Prevention

Chapter 7: 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
- Lab 7: Detecting Evasion Attempts
- Lab 8: Denial of Service

Chapter 8: Reporting

- NSM Reports
- Junos Syslog and Operational Commands

Cost AUD \$1,599 inc. GST

For Available Dates and Terms and Conditions see:
www.crystalecho.com

