Junos Intrusion prevention System Functionality

Duration: 2 Days Course Code: JIPS

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 analyze those functions. This course is based on the Junos operating system Release 12.1X44-D10.4.

Target Audience:

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

Objectives:

- **After you complete this course you will 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.

Prerequisites:

Attendees should meet the following prerequisites:

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. Students should also attend the Introduction to the Junos Operating System (IJOS) course, the Junos Routing Essentials (JRE) course, and the Junos Security (JSEC) course, or they should have equivalent experience prior to attending this class.

Testing and Certification

Recommended preparation for exam(s):

- Exam code: JN0-632 -Juniper Networks Certified Internet Professional (JNCIP-SEC)

Follow-on-Courses:

The following courses are recommended for further study:

- There are no recommended courses for further study.

Content:

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

Initial Device Configuration

- Deployment Options for IPS Functionality
- Management Options
- Network Settings
- Preparing the SRX Series Device for IPS Features
- Lab 2: Initial IDP Setup

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

IPS Attack Objects

- IPS Rules and Rulebases
- Attack Objects
- Custom Signatures
- Lab 6: 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
- Lab 7: Detecting Evasion Attempts
- Lab 8: Denial of Service

Reporting

- NSM Reports
- Junos Syslog and Operational Commands

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK