Course Name: Junos Intrusion Prevention Systems

Course Code: EDU-JUN-JIPS

Duration: Two days

Introduction

This two-day course is designed to provide an introduction to the Intrusion Prevention System (IPS) feature set (provided by Junos IPS Secure) 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.

Objective

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

- Explain the terms and concepts related to intrusion prevention.
- Describe general types of intrusions and network penetration steps.
- Explain how scanning can be used to gather information about target networks.
- Define and describe the terminology that comprises Juniper Networks IPS functionality.
- Describe the basic functions and features available on the SRX Series platform that provide IPS functionality.
- Describe how to access the SRX Series Services Gateways with IPS functionality for configuration and management.
- Describe the steps that the IPS engine takes when inspecting packets.
- Configure the SRX Series Services Gateways for IPS functionality.
- Describe the components of IPS rules and rulebases.
- Configure an IPS exempt rule.
- Explain the types of signature-based attacks.
- Configure a custom signature attack object.
- Describe the uses of custom signatures and how to configure them.
- Describe commonly used evasion techniques and how to block them.
- Explain the mechanisms available on the SRX Series Services Gateway to detect and block DoS and DDoS attacks.
- Configure screens to block IP spoofing and SYN flooding.
- Describe additional security flow protection mechanisms.

- Demonstrate how the SRX Series device performs TCP SYN checking.
- Explain the STRM capabilities for capturing, logging, and reporting network traffic.
- Describe the logging and reporting capabilities available for SRX IP functionality within STRM.

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.

Course Outline

Day 1	
Chapter 1	**Course Introduction**
Chapter 2	**Introduction to Intrusion Prevention Systems**
Chapter 3	**IPS Policy and Initial Configuration**
Chapter 4	**IPS Rulebase Operations**
Day 2	
Chapter 5	**Custom Attack Objects**
Chapter 6	**Additional Attack Protection Mechanisms**
Chapter 7	**IPS Logging and Reporting**

Training Location

Mideast Communication Systems
Juniper Authorized Training Center