Junos Intrusion prevention System Functionality

JIPS

Delivery Type: Classroom
Duration: 2 days

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 10.4R1.

Pre-Requisites

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.

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

93 Tsar Boris III Blvd., 1612 Sofia, Bulgaria
+359 2 903 59 33 @ sales@dada.bg

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.

Target Audience

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

Certification

Recommended preparation for exam(s):

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

93 Tsar Boris III Blvd., 1612 Sofia, Bulgaria
+359 2 903 59 33 @ sales@dada.bg