JUNIPER NETWORKS

EDUCATION SERVICES

Implementing Juniper Networks Secure Analytics (IJSA)

Engineering Simplicity

COURSE LEVEL

Implementing Juniper Networks Secure Analytics is an introductory-level course

AUDIENCE

This course is intended for network engineers, support personnel, reseller support, and anyone responsible for implementing the JSA system.

PREREQUISITES

- Understanding of TCP/IP operation;
- Understanding of network security concepts; and
- Experience in network security administration.

ASSOCIATED CERTIFICATION

N/A

RELEVANT JUNIPER PRODUCT

- Network Management
- JSA Series
- STRM Series
- Instructor-Led Training

RECOMMENDED NEXT COURSE

N/A

CONTACT INFORMATION

Contact Juniper Education Services

COURSE OVERVIEW

This three-day course discusses the configuration of Juniper Networks JSA Series Secure Analytics (formerly known as Security Threat Response Manager [STRM]) in a typical network environment. Key topics include deploying a JSA Series device in the network, configuring flows, running reports, and troubleshooting.

Through demonstrations and hands-on labs, students will gain experience in configuring, testing, and troubleshooting the JSA Series device. This course uses the Juniper Networks Secure Analytics (JSA) VM virtual appliance for the hands-on component. This course is based on JSA software 2014.2R4.

OBJECTIVES

- Describe the JSA system and its basic functionality
- Describe the hardware used with the JSA system
- Identify the technology behind the JSA system.
- Identify the JSA system’s primary design divisions—display versus detection, and events versus traffic.
- Plan and prepare for a new installation.
- Access the administration console.
- Configure the network hierarchy.
- Configure the automatic update process.
- Access the Deployment Editor.
- Describe the JSA system’s internal processes.
- Describe event and flow source configuration.
- List key features of the JSA architecture.
- Describe the JSA system’s processing logic.
- Interpret the correlation of flow and event data.
- List the architectural component that provides each key function.
- Describe Events and explain where they come from.
- Access the Log Activity interface.
- Describe flows and their origin.
- Configure the Network Activity interface.
- Execute Flow searches.
- Specify the JSA system’s Asset Management and Vulnerability Assessment functionality.
- Access the Assets interface.
- View Asset Profile data.
- View Server Discovery.
- Access the Vulnerability Assessment Scan Manager to produce vulnerability assessments (VAs).
- Access vulnerability scanner configuration.
- View vulnerability profiles.
- Describe rules.
- Configure rules.
- Configure Building Blocks (BBs).
- Explain how rules and flows work together.
- Access the Offense Manager interface.
- Understand Offense types.
- Configure Offense actions.
- Navigate the Offense interface.
- Explain the Offense summary screen.
- Search Offenses.

OBJECTIVES(contd)

- Use the JSA system's Reporting functionality to produce graphs and reports.
- Navigate the Reporting interface.
- Configure Report Groups.
- Demonstrate Report Branding.
- View Report formats.
- Identify the basic information on maintaining and troubleshooting the JSA system.
- Navigate the JSA dashboard.
- List flow and event troubleshooting steps.
- Access the Event Mapping Tool.
- Configure Event Collection for Junos devices.
- Configure Flow Collection for Junos devices.
- Explain high availability (HA) functionality on a JSA device.

COURSE CONTENT

Day 1

1 **COURSE INTRODUCTION**

2 **Product Overview**

- Overview of the JSA Series Device
- Hardware
- Collection
- Operational Flow

3 **Initial Configuration**

- A New Installation
- Administration Console
- Platform Configuration
- Deployment Editor

LAB 1: Initial Configuration

4 **Architecture**

- Processing Log Activity
- Processing Network Activity
- JSA Deployment Options

5 **Log Activity**

- Log Activity Overview
- Configuring Log Activity

LAB 2: Log Activity

Day 2

6 **Network Activity**

- Network Activity Overview
- Configuring Network Activity

LAB 3: Network Activity

7 **Assets and Vulnerability Assessment**

- Asset Interface
- Vulnerability Assessment
- Vulnerability Scanners

LAB 4: Assets and Vulnerability Assessment

8 **Rules**

- Rules
- Configure Rules and Building Blocks

LAB 5: Rules

9 **Offense Manager**

- •Offense Manager
- •Offense Manager Configuration
- •Offense Investigation

LAB 6: Configure the Offense Manager

Day 3

10 JSA Reporting

- Reporting Functionality
- Reporting Interface

LAB 7: Reporting

11 Basic Tuning and Troubleshooting

- Basic Tuning
- Troubleshooting

12 Configuring Junos Devices for Use with JSA

- Collecting Junos Events
- Collecting Junos Flows

LAB 8: Configuring Junos Devices for JSA

Appendix A: High Availability

•High Availability
•Configuring High Availability