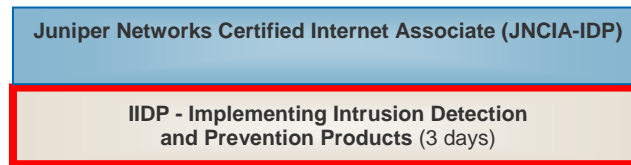




## JUNIPER IDP (SENSOR & ISG BLADE)



### Implementing Intrusion Detection and Prevention (IIDPv4)

#### Course Overview

This three-day course discusses the configuration of Juniper Intrusion Detection and Prevention (IDP) sensors in a typical network environment.

Key topics include: sensor configuration, creating and fine-tuning security policies, managing attack objects, creating custom signatures, and troubleshooting. This course is based upon IDP software version 4.0, and Security Manager 2006.1.

Through demonstrations and hands on labs, students will gain experience in configuring, testing, and troubleshooting the IDP sensor.

#### Target audience

Network engineers, support personnel, reseller support, and others responsible for implementing Juniper IDP products.

#### Course Level

Introductory

#### Prerequisites

This course assumes that students have basic networking knowledge and experience in the following areas:

- Internetworking basics
- TCP/IP Operations
- Network security concepts
- Network administration
- Application support

#### Chapter 1: Introduction

#### Chapter 2: Intrusion Detection Concepts

- Network attack phases and detection
- Juniper IDP product offerings
- IDP three-tier architecture
- IDP sensor transparent mode

#### Chapter 3: Initial Configuration of IDP Sensor

- Overview of IDP sensor deployment process
- Attach IDP sensor to network
- Establishing communication between SM and IDP sensor
- Creating initial IDP policy
- Installing policy on IDP sensor

#### Chapter 4: Policy Basics

- IDP attack terminology
- IDP rule components
- Packet flow through IDP sensor

#### Chapter 5: Fine-tuning Security Policies

- Step 1: Identify Machines to Monitor
- Step 2: Eliminate False Positives
- Step 3: Configure Response to Real Attacks
- Step 4: Configure Other Rulebases to Detect Attacks

#### Chapter 6: Configuring Other Rulebases

- Exempt Rulebase
- Traffic Anomalies Rulebase
- Backdoor Detection Rulebase
- SYN Protector Rulebase
- Network Honeypot Rulebase



### Chapter 7: Profiler

- Profiler Overview
- How to Operate the Profiler
- Using Profiler for Network Discovery
- Using Profiler to Detect New Devices and Ports
- Using Profiler to Detect Policy Violations
- Chapter 8: Sensor Operation and Command-line Utilities
- Sensor main components
- Description of sensor processes
- Managing policies and decoder engine with scio
- Managing sensor configuration with scio
- Monitoring with sctop
- Using tech-support tool

### Chapter 9: Managing Attack Objects

- Examining predefined attack objects
- Examining predefined attack object groups
- Creating new custom attack groups: static groups vs dynamic groups
- Updating attack objects
- Searching attack DB

### Chapter 10: Creating Custom Signatures

- IDP packet inspection
- Obtaining attack information using scio ccap & scio pcap
- Using regular expressions
- Configuring a simple signature
- Configuring a compound signature

### Chapter 11: Maintenance & Troubleshooting

- Appliance Configuration Manager (ACM)
- Backup of sensor
- Re-imaging sensor with reinstall CD
- Removing old logs, exporting logs
- Troubleshooting connectivity problems between Security Manager and IDP sensor

### Chapter 12: High-Availability

- NIC bypass
- Standalone HA
- External HA

**Cost AUD \$2,099 inc. GST**

For Available Dates & Terms and Conditions see:  
[www.crystalecho.com](http://www.crystalecho.com)

**JUNIPER**  
NETWORKS  
EDUCATION SERVICES  
AUTHORIZED PARTNER