COURSE LEVEL
Intermediate-level course

INTENDED AUDIENCE
The primary audiences for this course are the following:

- Operators of Juniper Networks security solutions, including network engineers, administrators, support, personnel, and resellers.

PREREQUISITES
The following are the prerequisites for this course:

- Basic networking knowledge and an understanding of the Open Systems Interconnection (OSI) reference model and the TCP/IP protocol suite
- Successful completion of the Introduction to Juniper Security (JSEC) course

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

- Identify security challenges in today’s networks.
- Identify products that are incorporated into the Juniper Connected Security solution.
- Explain the value of implementing security solutions.
- Explain how Juniper Connected Security solves the cyber security challenges of the future.
- Explain SRX Series session management.
- Explain Junos ALG functions and when to use them.
- Describe policy logging on the SRX series device.
- Explain security policy scheduling.
- Describe application security theory.
- Explain application signature usage in AppID.
- Describe the AppTrack service.
- Describe the AppFW service.
- Describe the AppQoS service.
- Configure security policies using the AppSecure suite of services.
- Explain unified security policies.
- Describe IPS signatures.
- Configure an IPS policy using pre-defined templates.
- Describe how to update the IPS attack object database.
- Describe IPS rules and rule bases.
- Configure custom attack objects.
- Describe Junos Space and Security Director.
- Configure policy management using Security Director.
- Describe Security Director objects.
- Explain the different licensing options for Sky ATP
- List Sky ATP’s features and benefits.
- Configure Sky ATP profiles and enroll an SRX Series device.
- Configure file scanning on Sky ATP.
- Configure Sky ATP to scan email
- Configure GeoIP on Sky ATP.
- Describe the JATP features and benefits

ASSOCIATED CERTIFICATION
JNCIS-SEC

RELEVANT JUNIPER PRODUCT
- Security
- Junos OS
- SRX Series
- vSRX Series

RECOMMENDED NEXT COURSE
Advanced Juniper Security (AJSEC)

CONTACT INFORMATION
training@juniper.net
OBJECTIVES (CONT’D)

- List the JATP device options.
- Explain the JATP architecture.
- List 3rd party support options for JATP.
- Explain JATP SmartCore analytics processes.
- Describe Policy Enforcer configuration options.
- Describe Policy Enforcer integration with Sky ATP.
- Configure Policy Enforcer to block lateral malware movement.
- Explain Juniper Secure Analytics features and benefits.
- Describe JSA log collection.
- Describe JSA network flow collection.
- Describe the JSA Offense Management workspace.
- Explain the JSA Risk Manager features.
- Configure JSA to collect network and log collection.
- Explain the features of JIMS.
- Describe JIMS integration into the current AD network.
- Describe the Sky Enterprise service and how it can save resources.
- Explain the Sky Enterprise monitoring service.
- Explain the vSRX Series device benefits.
- Describe use cases for the vSRX.
- Explain the cSRX Series device benefits.
- Describe use cases for the cSRX.
- Describe SSL Proxy Concepts.
- Explain Forward and Reverse Proxy and the limitations of each.
- Configure both Forward and Reverse Proxy.
- Troubleshoot SSL Proxy configurations.
- Explain how to cluster the SRX Series.
- Describe chassis cluster interfaces.
- Explain advanced chassis clustering options.
- Configure chassis clustering on the vSRX.
- Troubleshoot chassis clustering on the vSRX.
COURSE CONTENT

Day 1

1 Course Introduction

2 CLI Overview
   • User Interface Options
   • Command-Line Interface
   • Initial Configuration
   • Interface Configuration

LAB 1: CLI Overview

3 Advanced Security Policy
   • Session Management
   • Junos ALGs
   • Policy Scheduling
   • Policy Logging

LAB 2: Advanced Security Policy

4 Application Security Theory
   • Application ID
   • Application Signatures
   • App Track
   • App Firewall
   • App QoS
   • App QoE

5 Application Security Implementation
   • AppTrack Implementation
   • AppFW Implementation
   • AppQos Implementation
   • APBR Implementation

LAB 3: Application Security

6 Intrusion Detection and Prevention
   • IPS Overview
   • IPS Policy
   • Attack Objects
   • IPS Configuration
   • IPS Monitoring

LAB 4: Implementing IPS

Day 2

7 Security Director
   • Overview
   • Security Director Objects
   • Security Director Policy Management

LAB 5: Security Director

8 Sky ATP Implementation
   • Architecture and Key Components
   • Features and Benefits
   • Configuration
   • Compromised Hosts
   • Command and Control
   • File Scanning
   • E-mail Scanning
   • Geo IP
   • Security Policy Integration
   • Troubleshooting

LAB 6: Sky ATP Implementation

9 Policy Enforcer
   • Policy Enforcer Concepts
   • Configuration Options
   • Policy Enforcer Installation

LAB 7: Policy Enforcer
Day 3

10 JATP Overview
- Traffic Inspection
- Threat Detection
- Threat Analysis
- JATP Architecture

11 JATP Implementation
- Data Collectors
- Configure SmartCore Analytics Engine
- Log Ingestion
- Incident Management
- SRX Threat Prevention
- 3rd Party support for Threat Prevention
- Reporting

LAB 8: JATP

12 Juniper Secure Analytics (JSA)
- JSA Overview
- Data Collection
- Log Analytics
- Threat Analytics
- Vulnerability Management
- Risk Management

LAB 9: JSA

Day 4

13 JIMS
- JIMS Overview
- JIMS Integration

LAB 10: JIMS

14 vSRX and cSRX
- vSRX Overview
- vSRX Supported Features
- vSRX Use Cases
- cSRX Overview

LAB 11: vSRX Installation

Day 5

16 Cluster Concepts
- Chassis Cluster Concepts
- Chassis Cluster Operation

17 Chassis Cluster Implementation
- Chassis Cluster Configuration
- Chassis Cluster Advanced Options

LAB 13: Chassis Cluster Implementation

18 Chassis Cluster Troubleshooting
- Chassis Cluster Case Studies
- Troubleshooting Examples

LAB 13: Chassis Cluster Troubleshooting

A Juniper Sky Enterprise

B SRX Series Hardware and Interfaces