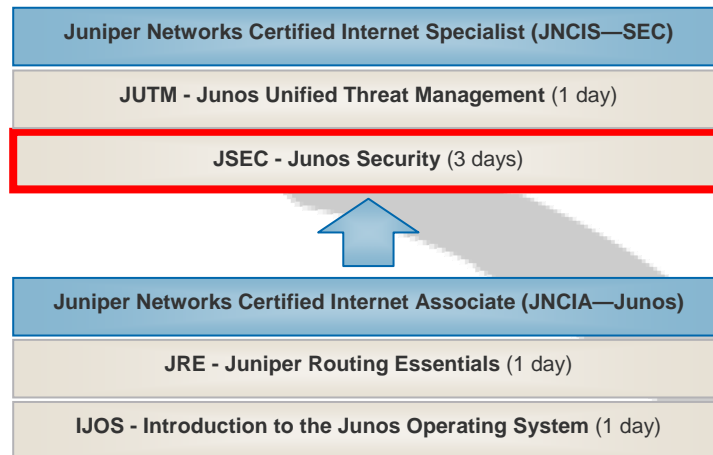




JUNIPER JUNOS SECURITY (SRX)



Junos Security (JSEC)

Course Overview

This three-day course provides students with the skills for configuration, operation, and implementation of JUNOS security platforms in a typical network environment.

Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring JUNOS Software for JUNOS security platforms.

Objectives

- After successfully completing this course, you should be able to:
- Describe traditional routing and security and the current trends in internetworking;
- Provide an overview of the JUNOS security platforms and software architecture;
- Describe the logical packet flow and session creation performed by JUNOS security platforms;
- Describe, configure, and monitor zones;
- Describe, configure, and monitor security policies;
- Describe, configure, and monitor firewall user authentication;
- Describe various types of network attacks;
- Configure and monitor SCREEN options to prevent network attacks;
- Explain, implement, and monitor NAT as implemented on JUNOS security platforms;

- Explain the purpose and mechanics of IPsec VPNs;
- Implement and monitor policy-based and route-based IPsec VPNs;
- Utilize and update the IDP signature database on JUNOS security platforms;
- Configure and monitor IDP policy with policy templates; and
- Describe, configure, and monitor high availability chassis clusters.

Target Audience

This course benefits operators of JUNOS security platforms. These operators include network engineers, administrators, support personnel, and reseller support personnel

Course Level

Intermediate

Prerequisites

Students should:

- have an understanding of the OSI model.
- know the TCP/IP protocol suite

Students should attend the following courses:

- IJOS
- JRE



crystalecho.com

Chapter 1: Course Introduction

Chapter 2: Introduction to JUNOS security platforms

- Traditional Routing
- Traditional Security
- Breaking the Tradition
- JUNOS Software Architecture

Chapter 3: Zones

- The Definition of Zones
- Zone Configuration
- Monitoring Security Zones
- Lab 1: Configuring and Monitoring Zones

Chapter 4: Security Policies

- Security Policy Overview
- Policy Components
- Verifying Policy Operation
- Policy Scheduling and Rematching
- Policy Case Study
- Lab 2: Security Policies

Chapter 5: Firewall User Authentication

- Firewall User Authentication Overview
- Pass-Through Authentication
- Web Authentication
- Client Groups
- Using External Authentication Servers
- Verifying Firewall User Authentication
- Lab 3: Configuring Firewall Authentication

Chapter 6: SCREEN Options

- Multilayer Network Protection
- Stages and Types of Attacks
- Using Junos SCREEN Options—Reconnaissance Attack Handling
- Using Junos SCREEN Options—Denial of Service Attack Handling
- Using Junos SCREEN Options—Suspicious Packets Attack Handling
- Applying and Monitoring SCREEN Options
- Lab 4: Implementing SCREEN Options

Chapter 7: Network Address Translation

- NAT Overview
- Source NAT Operation and Configuration
- Destination NAT Operation and Configuration
- Static NAT Operation and Configuration
- Proxy ARP
- Monitoring and Verifying NAT Operation
- Lab 5: Network Address Translation

Chapter 8: IPsec VPNs

- VPN Types
- Secure VPN Requirements
- IPsec Details
- Configuration of IPsec VPNs
- IPsec VPN Monitoring
- Lab 6: Implementing IPsec VPNs

Chapter 9: Introduction to Intrusion Detection and Prevention

- Introduction to JUNOS Software IDP
- IDP Policy Components and Configuration
- Attack and Signature Database
- Case Study: Applying the Recommended IDP Policy
- Monitoring IDP Operation
- Lab 7: Implementing IDP

Chapter 10: High Availability Clustering

- High Availability Overview
- Chassis Cluster Components
- Chassis Cluster Operation
- Chassis Cluster Configuration
- Chassis Cluster Monitoring
- Lab 8: Implementing Chassis Clustering

Cost AUD \$2,099 inc. GST

For Available Dates & Terms and Conditions see:
www.crystalecho.com

JUNIPER
NETWORKS
EDUCATION SERVICES
AUTHORIZED PARTNER