Junos Security

Duration: 5 Days **Course Code: JSEC** **Version: 12.c** **Delivery Method: Company Event**

Overview:

This five day course covers the configuration, operation and implementation of SRX Series Services Gateways in a typical network environment. Key topics within this course include security technologies such as security zones, security policies, intrusion detection and prevention (IDP), Network Address Translation (NAT), and high availability clusters, as well as details pertaining to basic implementation, configuration, and management. Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring the Junos OS and monitoring device operations. This course uses Juniper Networks SRX Series Services Gateways for the hands-on component, but the lab environment does not preclude the course from being applicable to other Juniper hardware platforms running the Junos OS. This course is based on Junos OS Release 12.1X47-D30.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

This course benefits operators of SRX Series devices. These operators include network engineers, administrators, support personnel, and reseller support personnel.

Objectives:

- After you complete this course you will be able to:
- Describe traditional routing and security and the current trends in internetworking.
- Provide an overview of SRX Series devices and software architecture.
- Describe the logical packet flow and session creation performed by SRX Series devices.
- 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 implementedon Junos security platforms.
- Explain the purpose and mechanics of IP Security (IPsec) virtual private networks (VPNs).
- Implement and monitor policy-based and route-based IPsec VPNs.
- Utilize and update the IDP signature database.
- Configure and monitor IDP policy with policy templates.
- Describe, configure, and monitor high availability chassis clusters.

Prerequisites:

Attendees should meet the following prerequisites:

Students should have basic networking knowledge and an understanding of the Open Systems Interconnection (OSI) reference model and the TCP/IP protocol suite. Students should also either attend the Introduction to the Junos Operating System (IJOS) and Junos Routing Essentials (JRE) courses prior to attending this class, or have equivalent experience with the Junos OS.

Testing and Certification

Recommended preparation for exam(s):

- Exam code: JN0-332 Juniper Networks Certified Internet Specialist (JNCIS-SEC)

Follow-on-Courses:

The following courses are recommended for further study:

- AJSEC - Advanced Junos Security
- JIPS - Junos Intrusion Prevention System Functionality
- JUTM - Junos Unified Threat Management

Content:

Introduction to Junos security platforms

- Traditional Routing
- Traditional Security
- Breaking the Tradition
- The Junos OS Architecture

Zones

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

Security Policies

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

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

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

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

IPsec VPNs

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

Introduction to Intrusion Detection and Prevention

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

High Availability Clustering Theory

- High Availability Overview
- Chassis Cluster Components
- Advanced Chassis Cluster Topics

High Availability Clustering Implementation

- Chassis Cluster Operation
- Chassis Cluster Configuration
- Chassis Cluster Monitoring
- Lab 8: Implementing High Availability Techniques

SRX Series Hardware and Interfaces

- Branch SRX Platform Overview
- High End SRX Platform Overview
- SRX Traffic Flow and Distribution
- SRX Interfaces

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK