Course Outline

Junos Security - 5 days

5 Day Course

DESCRIPTION

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, Network Address Translation (NAT), IP Security (IPsec), and high availability clusters, as well as details pertaining to basic implementation, configuration, management, and troubleshooting.

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 and Security Director for the hands-on component. This course is based on Junos OS Release 15.1X49-D70.3 and Junos Space Security Director 16.1.

Junos Security (JSEC) is an intermediate-level course.

PARTICIPANTS

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

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 attend the Introduction to the Junos Operating System (IJOS) course, or have equivalent experience prior to attending this class.

OBJECTIVES

After successfully completing this course, you should be able to perform the following:

- 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 user firewall 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 IP Security (IPsec) virtual private networks (VPNs).
- Implement and monitor policy-based and route-based IPsec VPNs.
- Describe, configure, and monitor high availability chassis clusters.
- Describe how to deploy and manage vSRX.
- Describe and configure Group VPNs.
- Describe and configure ADVPNs.
- Troubleshoot chassis clusters, IPsec VPNs, zones, and Security Policies

PROGRAMME

Day 1

Chapter 1: Course Introduction
Chapter 2: Introduction to Junos Security
- Traditional Routing
- Traditional Security
- The Junos OS Architecture

Chapter 3: Zones
- The Definition of Zones
- Zone Configuration
- Monitoring Security Zones
- Screen Options

Lab 1: Configuring and Monitoring Zones
Chapter 4: Security Policies
- Security Policy Overview
- Policy Components
- Verifying Policy Operation
- Policy Case Study

Lab 2: Security Policies

Day 2

Chapter 5: Advanced Policy Options
- Session Management
- Junos ALGs
- Policy Scheduling
- Logging

Chapter 6: Troubleshooting Security Zones and Policies
- Troubleshoot Security Zones
- Troubleshoot Security Policies
- Case Studies

Lab 3: Troubleshooting Security Zones and Policies
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 4: Network Address Translation

Day 3

Chapter 8: Advanced NAT Concepts
- NAT Interaction with Policy and ALGs
- DNS Doctoring
- Cone NAT
- Multi-Tenant NAT
- IPv4-to-IPv6 NAT
- Advanced NAT Scenarios

Lab 5: Advanced NAT Implementations

Chapter 9: IPsec VPN Concepts
- VPN Types
- Secure VPN Requirements
- IPsec Overview
- IPsec Details

Chapter 10: IPsec VPN Implementation
- Configuration of IPsec VPNs
- IPsec VPN Case Studies
- Monitoring IPsec VPN
- Traffic Selectors

Lab 6: Implementing IPsec VPNs

Day 4

Chapter 11: Group VPNs
- Group VPN Overview
- GDOI Protocol
- Group VPN Configuration and Monitoring

Lab 7: Implementing Group VPNs

Chapter 12: ADVPNs
- ADVPN Overview
- ADVPN Member Roles
- Shortcut Termination
- Routing with ADVPNs
- IKEv2
- ADVPN Implementation

Lab 8: Implementing ADVPNs

Chapter 13: IPsec VPN Case Studies and Solutions
- Routing over VPNs
- NAT with IPsec
- Enterprise VPN Deployment Best Practices

Lab 9: Implementing Routing over VPN Tunnels and IPsec Best Practices

Chapter 14: Troubleshooting IPsec
- IKE Phase 1 Troubleshooting
- IKE Phase 2 Troubleshooting
- Case Studies

Lab 10: Troubleshooting IPsec

Day 5

Chapter 15: Virtualized SRX
- vSRX Overview
- Installation of vSRX
- Chassis Clustering
- Deployment Scenarios and Use Cases
- Automated Deployments Options
- AWS Deployment Scenarios

Chapter 16: High Availability Clustering Theory
- High Availability Overview
- Chassis Cluster Components
- Advanced Chassis Cluster Topics

Chapter 17: High Availability Clustering Implementation
- Chassis Cluster Configuration

- Chassis Cluster Monitoring
- Advanced Chassis Cluster Topics

Lab 12: Implementing High Availability Techniques

Chapter 18: Troubleshooting Chassis Clusters

- Chassis Cluster Troubleshooting
- Case Studies
- IDP Policy Components and Configuration

Lab 13: Troubleshooting Chassis Clusters

Appendix A: SRX Series Hardware and Interfaces

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