JNCIS Security Certification Boot Camp (JSEC, JUTM)

Learn to configure and monitor SRX Series devices while preparing for the JNCIS-SEC exam in this accelerated Boot Camp.

In this accelerated Boot Camp, you will gain the knowledge needed to succeed on the Juniper Networks Certified Internet Specialist - Security (JNCIS-SEC) exam, and you will gain hands-on experience configuring and monitoring the Junos OS for SRX Series devices.

During the first half of class, you will review SRX Series Services Gateway configuration, operation, and implementation in a typical network environment. Key topics include security zones, security policies, intrusion detection and prevention (IDP), Network Address Translation (NAT), High Availability (HA) clusters, and basic implementation, configuration, and management.

In the second half, you will cover web filtering, antivirus (AV), anti-spam, and content filtering. Also, through demonstrations and hands-on labs, you will gain experience configuring and monitoring the Unified Threat Management (UTM) features of the Junos OS.

What You'll Learn

- SRX Series devices and software architecture
- Logical packet flow and session creation performed by SRX Series devices
- Configure and monitor zones, security policies, and firewall user authentication
- Various types of network attacks
- Configure and monitor SCREEN options to prevent network attacks
- Implement and monitor NAT on Junos security platforms
- Purpose and mechanics of IP Security (IPsec) virtual private networks (VPNs)
- Implement and monitor policy-based and route-based IPsec VPNs
- Use and update the IDP signature database
- Configure and monitor IDP policy with policy templates
- Configure and monitor HA chassis clusters
- Major features that UTM offers and how they address the challenge of branch offices
- SRX Series Services Gateways hardware devices on which UTM is available
- UTM features that require specific licenses
- Terms used in the creation of effective anti-spam UTM policies
- How UTM examines traffic for spam
- Configuring an anti-spam UTM policy
- Information available from the device when it has detected spam
- How the AV process examines traffic
- Differences between full file-based AV and express AV
- Settings required for configuring AV protection and how they affect scanning performance and effectiveness
- Options for scanning supported protocols

- Steps required to configure AV
- Statistical information available to verify AV functionality
- Parameters and steps used to configure and monitor web and content filtering

Prerequisites

- JNCIA-JUNOS

Course Outline

1. Junos Security Platforms

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

2. Zones

- Definition of Zones
- Zone Configuration
- Monitoring Security Zones

3. Security Policies

- Policy Components
- Verifying Policy Operation
- Policy Scheduling and Rematching
- Policy Case Study

4. Firewall User Authentication

- Firewall User Authentication Overview
- Pass-Through Authentication
- Web Authentication
- Client Groups
- Using External Authentication Servers
- Verifying Firewall User Authentication

5. SCREEN Options

- Multilayer Network Protection
- Stages and Types of Attacks
- Using Junos SCREEN Options
    - Reconnaissance Attack Handling
    - Denial of Service Attack Handling
    - Suspicious Packets Attack Handling

- Applying and Monitoring SCREEN Options

6. NAT

- Source NAT Operation and Configuration
- Destination NAT Operation and Configuration
- Static NAT Operation and Configuration
- Proxy ARP
- Monitoring and Verifying NAT Operation

7. IPsec VPNs

- VPN Types
- Secure VPN Requirements
- IPsec Details
- Configuration of IPsec VPNs
- IPsec VPN Monitoring

8. IDP

- Junos IDP
- Policy Components
- Configuration
- Signature Database
- Case Study: Applying the Recommended IDP Policy
- Monitoring IDP Operation

9. HA Clustering

- Chassis Cluster Components
- Chassis Cluster Operation
- Chassis Cluster Configuration
- Chassis Cluster Monitoring

10. Unified Threat Management

- Branch Office Challenges
- UTM Feature Overview
- Design Basics
- Hardware Support
- Licensing of Features

11. Anti-Spam

- Terminology and Process
- UTM Policy
- Configuration Steps
- Monitoring Anti-Spam

12. Full File-Based and Express AV

- AV Terminology and Process
- AV Operation
- Full File-based AV Configuration
- Express AV Configuration
- Monitoring AV

13. Content and Web Filtering

- Overview and Terminology
- Configuration
- Verification and Monitoring