AJSEC
Advanced Junos Security

Overview

This three-day course, which is designed to build off of the current Junos Security (JSEC) offering, delves deeper into Junos security.

Through demonstrations and hands-on labs, students gain experience in configuring and monitoring the advanced Junos operating system security features with advanced coverage of IPsec deployments, virtualization, AppSecure, advanced Network Address Translation (NAT) deployments, and Layer 2 security. 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 12.1R1.9.

Objectives

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

- Demonstrate understanding of concepts covered in the prerequisite Junos Security course.
- Describe the various forms of security supported by the Junos OS.
- Implement features of the AppSecure suite, including AppID, AppFW, and AppTrack.
- Configure custom application signatures.
- Describe Junos security handling at Layer 2 versus Layer 3.
- Implement Layer 2 transparent mode security features.
- Demonstrate understanding of Logical Systems (LSYS).
- Implement address books with dynamic addressing.
- Compose security policies utilizing ALGs, custom applications, and dynamic addressing for various scenarios.
- Use Junos debugging tools to analyze traffic flows and identify traffic processing patterns and problems.
- Describe Junos routing instance types used for virtualization.
- Implement virtual routing instances.
- Describe and configure route sharing between routing instances using logical tunnel interfaces.
- Describe and implement static, source, destination, and dual NAT in complex LAN environments.
- Describe and implement variations of persistent NAT.
- Describe and implement Carrier Grade NAT (CGN) solutions for IPv6 NAT, such as NAT64, NAT46, and DS-Lite.
- Describe the interaction between NAT and security policy.
- Demonstrate understanding of DNS doctoring.
- Differentiate and configure standard point-to-point IP Security (IPsec) virtual private network (VPN) tunnels, hub-and-spoke VPNs, dynamic VPNs, and group VPNs.
- Implement IPsec tunnels using virtual routers.
- Implement OSPF over IPsec tunnels and utilize generic routing encapsulation (GRE) to interconnect to legacy firewalls.
- Monitor the operations of the various IPsec VPN implementations.

- Describe public key cryptography for certificates.
- Utilize Junos tools for troubleshooting Junos security implementations.
- Perform successful troubleshooting of some common Junos security issues.

Intended Audience
This course benefits individuals responsible for implementing, monitoring, and troubleshooting Junos security components.

Course Level
AJSEC is an advanced-level course.

Prerequisites
Students should have a strong level of TCP/IP networking and security knowledge. Students should also attend the Introduction to the Junos Operating System (IJOS), Junos Routing Essentials (JRE), and Junos Security (JSEC) courses prior to attending this class.

Course Contents
Day 1
- Course Introduction
- AppSecure
  - AppSecure Overview
  - AppID
  - AppTrack
  - AppFW
  - AppDoS
  - AppQoS
- Junos Layer 2 Packet Handling and Security Features
  - Transparent Mode Security
  - Layer 2 Ethernet Switching
  - Lab 2: Implementing Layer 2 Security
- Virtualization
  - Virtualization Overview
  - Routing Instances
  - Logical Systems
  - Lab 3: Implementing Junos Virtual Routing

Day 2
- Advanced NAT Concepts
  - Operational Review
  - NAT: Beyond Layer 3 and Layer 4 Headers
  - DNS Doctoring
  - IPv6 NAT
  - Advanced NAT Scenarios
  - Lab 4: Advanced NAT Implementations
- IPsec Implementations
  - Standard VPN Implementations Review
  - Public Key Infrastructure
  - Hub-and-Spoke VPNs
  - Lab 5: Hub-and-Spoke IPsec VPNs

Day 3
- Enterprise IPsec Technologies: Group and Dynamic VPNs

- Group VPN Overview
- GDOI Protocol
- Group VPN Configuration and Monitoring
- Dynamic VPN Overview
- Dynamic VPN Implementation
- Lab 6: Configuring Group VPNs

- IPsec VPN Case Studies and Solutions
  - Routing over VPNs
  - IPsec with Overlapping Addresses
  - Dynamic Gateway IP Addresses
  - Enterprise VPN Deployment Tips and Tricks
  - Lab 7: Implementing Advanced IPsec VPN Solutions
- Troubleshooting Junos Security
  - Troubleshooting Methodology
  - Troubleshooting Tools
  - Identifying IPsec Issues
  - Lab 8: Performing Security Troubleshooting Techniques
- Appendix A: SRX Series Hardware and Interfaces
  - Branch SRX Platform Overview
  - High End SRX Platform Overview
  - SRX Traffic Flow and Distribution
  - SRX Interfaces