Advanced Junos Security (AJSEC)

Course Summary

Description

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
At the end of this course, students will 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.
- Describe Junos security handling at Layer 2 versus Layer 3.
- Describe the placement and traffic distribution of the various components of SRX devices.
- Configure, utilize, and monitor the various interface types available to the SRX Series product line.
- Describe Junos OS processing of Application Layer Gateways (ALGs).
- Alter the Junos default behavior of ALG and application processing.
- 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.
- Implement selective packet-based forwarding.
- Implement filter-based forwarding.
- Describe and implement static, source, destination, and dual NAT in complex LAN environments.
- Describe and implement variations of cone, or persistent NAT.
- Describe the interaction between NAT and security policy.
- Implement optimized chassis clustering.
- Describe IP version 6 (IPv6) support for chassis clusters.
- 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 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.

Advanced Junos Security (AJSEC)

Course Summary (cont'd)

Topics

- Course Introduction
- Junos Security Review
- Security Policy Components
- Virtualization
- Advanced NAT Concepts
- High Availability Clustering
- IPsec Implementations
- Enterprise IPsec Technologies: Group and Dynamic VPNs
- IPsec VPN Case Studies and Solutions
- Troubleshooting Junos Security

Audience

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

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.

Duration

Three days

ProTech

protechtraining.com

"Charting the Course ...

... to Your Success!"

Advanced Junos Security (AJSEC)

Course Outline

I. Course Introduction

II. AppSecure
- A. AppSecure Overview
- B. AppID
- C. AppTrack
- D. AppFW
- E. AppDoS
- F. AppQoS
- G. Lab 1: Implementing AppSecure

III. Junos Layer 2 Packet Handling and Security Features
- A. Transparent Mode Security
- B. Layer 2 Ethernet Switching
- C. Lab 2: Implementing Layer 2 Security

IV. Virtualization
- A. Virtualization Overview
- B. Routing Instances
- C. Logical Systems
- D. Lab 3: Implementing Junos Virtual Routing

V. Advanced NAT Concepts
- A. Operational Review
- B. NAT: Beyond Layer 3 and Layer 4 Headers
- C. DNS Doctoring
- D. IPv6 NAT
- E. Advanced NAT Scenarios
- F. Lab 4: Advanced NAT Implementations

VI. IPsec Implementations
- A. Standard VPN Implementations Review
- B. Public Key Infrastructure
- C. Hub-and-Spoke VPNs
- D. Lab 5: Hub-and-Spoke IPsec VPNs

VII. Enterprise IPsec Technologies: Group and Dynamic VPNs
- A. Group VPN Overview
- B. GDOI Protocol
- C. Group VPN Configuration and Monitoring
- D. Dynamic VPN Overview
- E. Dynamic VPN Implementation
- F. Lab 6: Configuring Group VPNs

VIII. IPsec VPN Case Studies and Solutions
- A. Routing over VPNs
- B. IPsec with Overlapping Addresses
- C. Dynamic Gateway IP Addresses
- D. Enterprise VPN Deployment Tips and Tricks
- E. Lab 7: Implementing Advanced IPsec VPN Solutions

IX. Troubleshooting Junos Security
- A. Troubleshooting Methodology
- B. Troubleshooting Tools
- C. Identifying IPsec Issues
- D. Lab 8: Performing Security Troubleshooting Techniques

X. Appendix A: SRX Series Hardware and Interfaces
- A. Branch SRX Platform Overview
- B. High End SRX Platform Overview
- C. SRX Traffic Flow and Distribution
- D. SRX Interfaces