Advanced Junos Security

Duration: 3 Days Course Code: AJSEC

Overview:

In the Advanced Junos Security (AJSEC) course, students will 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.

Target Audience:

This course is designed for:Individuals responsible for implementing, monitoring, and troubleshooting Junos security components.

Objectives:

- Upon completing this course, the learner will be able to meet these overall objectives:
- 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.

Prerequisites:

The knowledge and skills that a learner must have before attending this course are as follows:

- Students should have a strong level of TCP/IP networking and security knowledge.

Testing and Certification

Recommended preparation for:

- JN0-633 - Juniper Networks Certified Internet Professional (JNCIP-SEC)

AJSEC is one of the courses required for the **Juniper Networks**

To gain the prerequisite skills and knowledge, Juniper strongly recommends the knowledge of the following courses:

- Introduction to the Junos Operating System (IJOS)
- Junos Routing Essentials (JRE)
- Junos Security (JSEC)

Certified Internet Professional (JNCIP-SEC) Certification

Follow-on-Courses:

- Junos Intrusion Prevention System Functionality (JIPS)

AJSEC and JIPS are the courses required for the **Juniper Networks Certified Internet Professional (JNCIP-SEC)** Certification

Content:

AppSecure

- AppSecure Overview
- AppID
- AppTrack
- AppFW
- AppDoS
- AppQoS

Junos Layer 2 Packet Handling and Security Features

- Transparent Mode Security
- Layer 2 Ethernet Switching

Virtualization

- Virtualization Overview
- Routing Instances
- Logical Systems

Advanced NAT Concepts

- Operational Review
- NAT: Beyond Layer 3 and Layer 4 Headers
- DNS Doctoring
- IPv6 NAT
- Advanced NAT Scenarios

IPsec Implementations

- Standard VPN Implementations Review
- Public Key Infrastructure
- Hub-and-Spoke VPNs

Enterprise IPsec Technologies: Group and Dynamic VPNs

- Group VPN Overview
- GDOI Protocol
- Group VPN Configuration and Monitoring
- Dynamic VPN Overview
- Dynamic VPN Implementation

IPsec VPN Case Studies and Solutions

- Routing over VPNs
- IPsec with Overlapping Addresses
- Dynamic Gateway IP Addresses
- Enterprise VPN Deployment Tips and Tricks

Troubleshooting Junos Security

- Troubleshooting Methodology
- Troubleshooting Tools
- Identifying IPsec Issues

Further Information:

For More information, or to book your course, please call us on +254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya