Advanced Juniper Security

COURSE OVERVIEW

This four-day, advanced-level course provides students with the knowledge to configure and monitor advanced Junos OS security features for enterprise, campus, and service provider applications. Key topics include advanced Junos OS security features with coverage of advanced reporting, next-generation Layer 2 security, next-generation advanced features, Ethernet VPN (EVPN) Virtual Extensible LAN (VXLAN) security, advanced policy-based routing, virtualization features, advanced IPsec VPNs, advanced Network Address Translation (NAT) features, and multinode high availability.

Through demonstrations and hands-on labs, students will gain experience with the features of SRX Series devices and vSRX Series devices.

This course is based on Junos OS Release 23.2.

COURSE LEVEL

Advanced Juniper Security is an advanced course

AUDIENCE

Individuals responsible for implementing, monitoring, and troubleshooting Juniper security components. It is also beneficial to prepare for the JNCIP-SEC certification.

PREREQUISITES

- Strong skill level in TCP/IP, Layer 2 Ethernet, security policies, and security concepts
- General understanding of stateful firewalls, NAT, and IPsec
- Recommended, but not required:
  - Completing the *Introduction to Juniper Security* and *Juniper Security* courses
  - Experience with packet captures

RELATED CERTIFICATION

JNCIP-SEC

RELATED JUNIPER PRODUCTS

Junos OS, Juniper ATP Cloud, Juniper Security Director

OBJECTIVES

- Describe Layer 2 security features.
- Discuss ways to use packet-based security.
- Describe how to troubleshoot zones and policies.
- Describe how to implement a hub-and-spoke VPN.
- Discuss advanced NAT capabilities.
- List the ways that the SRX firewall may be virtualized.
- Describe how to implement an Auto Discovery VPN (ADVPN) setup.
- List options using IPsec to accomplish advanced configurations.
- Discuss how to troubleshoot IPsec VPNs.
- Describe how to route traffic based on the application.
- Describe how to secure VXLAN traffic within the network.
- Implement multinode high availability.
- Discuss how to mitigate network threats automatically.

Course Outline

COURSE CONTENTS

DAY 1

Module 1: Junos Layer 2 Packet Handling and Security Features

- Explain transparent mode security operations
- Define secure wire implementation
- Describe MACsec uses

Lab 1: Implementing Layer 2 Security

Module 2: Packet-Based Security

- Explain routing instances
- Describe filter-based forwarding

Lab 2: Implementing Packet-Based Security

Module 3: Troubleshooting Zones and Policies

- Describe troubleshooting tools available in Junos OS
- Discuss troubleshooting of security zones and security policies
- Examine troubleshooting case studies

Lab 3: Troubleshooting Zones and Policies

DAY 2

Module 4: Hub-and-Spoke VPN

- Explain transparent mode security operations
- Define secure wire implementation

Lab 4: Implementing Hub-and-Spoke VPNs

Module 5: Advanced NAT

- Explain the difference between address persistence and persistent NAT
- Describe DNS doctoring
- Describe advanced NAT scenarios
- Discuss NAT troubleshooting

Lab 5: Implementing Advanced NAT

Module 6: Logical and Tenant Systems

- Describe logical systems
- Describe tenant systems

Lab 6: Implementing Tenant Systems

DAY 3

Module 7: PKI and ADVPNs

- Describe PKI
- Configure PKI for Junos security devices
- Describe how ADVPNs function
- Configure and monitor ADVPNs

Lab 7: Implementing ADVPNs

Module 8: Advanced IPsec

- Explain NAT interoperability with IPsec
- Describe the CoS feature with IPsec VPNs
- Explain IPsec best practices
- Configure OSPF over IPsec
- Configure IPsec with overlapping addresses
- Configure IPsec when using dynamic gateway IP addresses

Lab 8: Implementing Advanced IPsec Solutions

Module 9: Troubleshooting IPsec

- Describe general troubleshooting for IPsec VPNs
- Discuss how to troubleshoot IKE Phase 1 and Phase 2
- Configure and analyze logging for IPsec VPNs
- Examine IPsec troubleshooting case studies

Lab 9: Troubleshooting IPsec VPNs

DAY 4

Module 10: Advanced Policy-Based Routing

- Define advanced policy-based routing
- Configure advanced policy-based routing
- Explain application quality of experience

Lab 10: Implementing APBR

Module 11: EVPN VXLAN Security

- Describe the EVPN VXLAN protocols
- Explain VXLAN tunnel security
- Configure security on VXLAN tunnels

Lab 11: Securing Traffic Between Data Centers

Module 12: Multinode High Availability

- Identify the benefits of high availability and security
- Explain the use of multinode high availability
- Identify multinode high availability modes
- Discuss services redundancy groups

Lab 12: Implementing Multinode HA

Module 13: Automated Threat Mitigation

- Explain Automated Threat Mitigation
- Discuss Juniper Connected Security third-party integrations
- Discuss Juniper Connected Security multicloud integrations
- Discuss the Secure Enterprise use case