skillsoft global knowledge™

ADVANCED JUNOS SECURITY - JNCIP-SEC CERTIFICATION COURSE (AJSEC)

Course Code: 6205

Designed to build off the current Juniper Security (JSEC) offering, delves deeper into Junos security, next-generation security features, and ATP supporting software.

This four-day course, designed to build off the current Juniper Security (JSEC) offering, delves deeper into Junos security, next-generation security features, and ATP supporting software. Through demonstrations and hands-on labs, you will gain experience in configuring and monitoring the advanced Junos OS security features with coverage of advanced logging and reporting, next-generation Layer 2 security, and next-generation advanced anti-malware with Juniper ATP On-Prem and SecIntel. This course uses Juniper Networks SRX Series Services Gateways for the hands-on component. This course uses on Junos OS Release 20.1R1.11, Junos Space Security Director 19.4, and Juniper ATP On-Prem version 5.0.7.

Advanced Juniper Security (AJSEC) is an advanced-level course.

What You'll Learn

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

- Demonstrate understanding of concepts covered in the prerequisite Juniper Security courses.
- Describe the various forms of security supported by the Junos OS.
- Describe the Juniper Connected Security model.
- Describe Junos security handling at Layer 2 versus Layer 3.
- Implement next generation Layer 2 security features.
- Demonstrate understanding of Logical Systems (LSYS).
- Demonstrate understanding of Tenant Systems (TSYS).
- Implement virtual routing instances in a security setting.
- Describe and configure route sharing between routing instances using logical tunnel interfaces.
- Describe and discuss Juniper ATP and its function in the network.
- Describe and implement Juniper Connected Security with Policy Enforcer in a network.

- Describe firewall filters use on a security device.
- Implement firewall filters to route traffic.
- Explain how to troubleshoot zone problems.
- Describe the tools available to troubleshoot SRX Series devices.
- Describe and implement IPsec VPN in a hub-and-spoke model.
- Describe the PKI infrastructure.
- Implement certificates to build an ADVPN network.
- Describe using NAT, CoS and routing protocols over IPsec VPNs.
- Implement NAT and routing protocols over an IPsec VPN.
- Describe the logs and troubleshooting methodologies to fix IPsec VPNs.
- Implement working IPsec VPNs when given configuration that are broken.
- Describe Incident Reporting with Juniper ATP On-Prem device.
- Configure mitigation response to prevent spread of malware.
- Explain SecIntel uses and when to use them.
- Describe the systems that work with SecIntel.
- Describe and implement advanced NAT options on the SRX Series devices.
- Explain DNS doctoring and when to use it.
- Describe NAT troubleshooting logs and techniques.

Who Needs to Attend

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

Prerequisites

Students should have a strong level of TCP/IP networking and security knowledge. Students should also attend the Juniper Security (JSEC) course prior to attending this class.

ADVANCED JUNOS SECURITY - JNCIP-SEC CERTIFICATION COURSE (AJSEC)

Course Code: 6205

CLASSROOM LIVE	$3,800 USD	4 Day

Classroom Live Outline

Day 1

Chapter 1: Course Introduction

Chapter 2: Junos Layer 2 Packet Handling and Security Features

- Transparent Mode Security
- Secure Wire
- Layer 2 Next Generation Ethernet Switching
- MACsec

Chapter 3: Firewall Filters

- Using Firewall Filters to Troubleshoot
- Routing Instances
- Filter-Based Forwarding

Chapter 4: Troubleshooting Zones and Policies

- General Troubleshooting for Junos Devices
- Troubleshooting Tools
- Troubleshooting Zones and Policies
- Zone and Policy Case Studies

Day 2

Chapter 5: Hub-and-Spoke VPN

- Overview
- Configuration and Monitoring

Chapter 6: Advanced NAT

- Configuring Persistent NAT
- Demonstrate DNS doctoring
- Configure IPv6 NAT operations
- Troubleshooting NAT

Chapter 7: Logical and Tenant Systems

- Overview
- Administrative Roles
- Differences Between LSYS and TSYS
- Configuring LSYS
- Configuring TSYS

Day 3

Chapter 8: PKI and ADVPNs

- PKI Overview
- PKI Configuration
- ADVPN Overview
- ADVPN Configuration and Monitoring

Chapter 9: Advanced IPsec

- NAT with IPsec
- Class of Service with IPsec
- Best Practices
- Routing OSPF over VPNs

Chapter 10: Troubleshooting IPsec

- IPsec Troubleshooting Overview
- Troubleshooting IKE Phase 1 and 2
- IPsec Logging
- IPsec Case Studies

Day 4

Chapter 11: Juniper Connected Security

- Security Models
- Enforcement on Every Network Device

Chapter 12: SecIntel

- Security Feed
- Encrypted Traffic Analysis
- Use Cases for SecIntel

Chapter 13:Advanced Juniper ATP On-Prem

- Collectors
- Private Mode

- Incident Response
- Deployment Models

Chapter 14: Automated Threat Mitigation

- Identify and Mitigate Malware Threats
- Automate Security Mitigation

Appendix A: Group VPNs

- Overview
- Implementing Group VPNs

Classroom Live Labs

- Lab 1: Implementing Layer 2 Security
- Lab 2: Implementing Firewall Filters
- Lab 3: Troubleshooting Zones and Policies
- Lab 4: Implementing Hub-and-Spoke VPNs
- Lab 5: Implementing Advanced NAT Features
- Lab 6: Implementing TSYS
- Lab 7: Implementing ADVPNs
- Lab 8: Implementing Advanced IPsec Solutions
- Lab 9: Troubleshooting IPsec
- Lab 10: Implementing SecIntel
- Lab 11: Implementing Advanced ATP On-Prem
- Lab 12: Identifying and Mitigation of Threats

ADVANCED JUNOS SECURITY - JNCIP-SEC CERTIFICATION COURSE (AJSEC)

Course Code: 6205

VIRTUAL CLASSROOM LIVE	$3,800 USD	4 Day

Virtual Classroom Live Outline

Day 1

Chapter 1: Course Introduction

Chapter 2: Junos Layer 2 Packet Handling and Security Features

- Transparent Mode Security
- Secure Wire
- Layer 2 Next Generation Ethernet Switching
- MACsec

Chapter 3: Firewall Filters

- Using Firewall Filters to Troubleshoot
- Routing Instances
- Filter-Based Forwarding

Chapter 4: Troubleshooting Zones and Policies

- General Troubleshooting for Junos Devices
- Troubleshooting Tools
- Troubleshooting Zones and Policies
- Zone and Policy Case Studies

Day 2

Chapter 5: Hub-and-Spoke VPN

- Overview
- Configuration and Monitoring

Chapter 6: Advanced NAT

- Configuring Persistent NAT
- Demonstrate DNS doctoring
- Configure IPv6 NAT operations
- Troubleshooting NAT

Chapter 7: Logical and Tenant Systems

- Overview
- Administrative Roles
- Differences Between LSYS and TSYS
- Configuring LSYS
- Configuring TSYS

Day 3

Chapter 8: PKI and ADVPNs

- PKI Overview
- PKI Configuration
- ADVPN Overview
- ADVPN Configuration and Monitoring

Chapter 9: Advanced IPsec

- NAT with IPsec
- Class of Service with IPsec
- Best Practices
- Routing OSPF over VPNs

Chapter 10: Troubleshooting IPsec

- IPsec Troubleshooting Overview
- Troubleshooting IKE Phase 1 and 2
- IPsec Logging
- IPsec Case Studies

Day 4

Chapter 11: Juniper Connected Security

- Security Models
- Enforcement on Every Network Device

Chapter 12: SecIntel

- Security Feed
- Encrypted Traffic Analysis
- Use Cases for SecIntel

Chapter 13:Advanced Juniper ATP On-Prem

- Collectors
- Private Mode

- Incident Response
- Deployment Models

Chapter 14: Automated Threat Mitigation

- Identify and Mitigate Malware Threats
- Automate Security Mitigation

Appendix A: Group VPNs

- Overview
- Implementing Group VPNs

Virtual Classroom Live Labs

- Lab 1: Implementing Layer 2 Security
- Lab 2: Implementing Firewall Filters
- Lab 3: Troubleshooting Zones and Policies
- Lab 4: Implementing Hub-and-Spoke VPNs
- Lab 5: Implementing Advanced NAT Features
- Lab 6: Implementing TSYS
- Lab 7: Implementing ADVPNs
- Lab 8: Implementing Advanced IPsec Solutions
- Lab 9: Troubleshooting IPsec
- Lab 10: Implementing SecIntel
- Lab 11: Implementing Advanced ATP On-Prem
- Lab 12: Identifying and Mitigation of Threats

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 12/7/2025 6:06:16 PM