Juniper Networks - Advanced Junos Security - JNCIP-SEC Certification Course (AJSEC) (AJSEC)

Code: 6205
Length: 4 days
URL: View Online

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.

Skills Gained

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 Can Benefit

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.
