
Advanced Junos Security

Duración: 4 Días Código del Curso: AJSEC Version: 20.1R

Temario:

This four-day course, which is 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 advanced coverage of advanced logging and reporting, next generation Layer 2 security, 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 is based on Junos OS Release 20.1R1.11, Junos Space Security Director 19.4, Juniper ATP On-Prem version 5.0.7.

Dirigido a:

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

Objetivos:

- 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.
-

Prerequisites:

- Strong level of TCP/IP networking and security knowledge
 - Complete the Juniper Security (JSEC) course prior to attending this class
 - JSEC - Junos Security
 - JUTM - Junos Unified Threat Management
-

Siguientes cursos recomendados:

- JIPS - Junos Intrusion prevention System Functionality
-

Contenido:

Day 1

1 COURSE INTRODUCTION

2 Junos Layer 2 Packet Handling and Security Features

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

LAB 1: Implementing Layer 2 Security

3 Firewall Filters

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

LAB 2: Implementing Firewall Filters

4 Troubleshooting Zones and Policies

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

LAB 3: Troubleshooting Zones and Policies

Day 2

5 Hub-and-Spoke VPN

- Overview
- Configuration and Monitoring

LAB 4: Implementing Hub-and-Spoke VPNs

6 Advanced NAT

- Configuring Persistent NAT
- Demonstrate DNS Doctoring
- Configure IPv6 NAT Operations
- Troubleshooting NAT

LAB: 5: Implementing Advanced NAT Features

7 Logical and Tenant Systems

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

LAB 6: Implementing TSYS

Day 3

8 PKI and ADVPNs

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

LAB 7: Implementing ADVPNs

9 Advanced IPsec

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

LAB 8: Implementing Advanced IPsec Solutions

10 Troubleshooting IPsec

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

LAB 9: Troubleshooting IPsec

Day 4

11 Juniper Connected Security

- Security Models
- Enforcement on Every Network Device

12 SecIntel

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

LAB 10: Implementing SecIntel

13 Advanced Juniper ATP On-Prem

- Collectors
- Private Mode
- Incident Response
- Deployment Models

LAB 11: Implementing Advanced ATP On-Prem

14 Automated Threat Mitigation

- Identify and Mitigate Malware Threats
- Automate Security Mitigation

LAB 12: Identifying and Mitigating Threats

A Group VPNs

- Overview
- Implementing Group VPNs

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid