Juniper Security (JSEC)

Duration: 5 Days Course Code: JUN_JSEC

Overview:

This five-day course is designed to provide students with the knowledge required to work with Juniper Connected Security devices.
This course uses Junos CLI, Security Directory, J-Web, and other Web user interfaces to introduce students to Juniper Connected Security devices.
The course provides further instruction on how Juniper Networks approaches a complete security solution for current and future security problems, called Juniper Connected Security.
Key topics include tasks for advanced security policies, application-layer security using the AppSecure suite, intrusion prevention system (IPS) rules and custom attack objects, Security Director management, Juniper Advanced Threat Prevention (ATP) Cloud management, Juniper ATP Appliance management, Juniper Secure Analytics (JSA) management, Policy Enforcer management, Juniper Identity Management Service (JIMS), vSRX and cSRX usage, SSL Proxy configuration, and SRX high availability configuration and troubleshooting.
Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring the Junos OS and monitoring basic device operations.
This course is based on Junos OS Release 22.1R2, Junos Space 22.2R1, Security Director 22.2R1, JATP 5.0.6.0, JSA v7.3.2, Policy Enforcer 22.2R1, and JIMS 1.1.5R1.
Course Level
Juniper Security (JSEC) is an intermediate-level course.
Relevant Juniper Product
• JIMS • JSA • Juniper ATP Appliance • Juniper ATP Cloud • Junos OS • Security Director • SRX Series

Target Audience:

Benefits individuals responsible for security operations using Juniper Networks security solutions, including network engineers, security engineers, administrators, support personnel, and resellers.

Objectives:

- After successfully completing this course, you should be able to:
- • Explain the function of SSL Proxy.
- • Explain how application security theory works.
- • Discuss in depth the AppSecure modules.
- • Describe unified security policies.
- • Review the different security policy options.
- • Explain the basics of intrusion detection.
- • Describe the Juniper ATP Cloud solutions.
- • Describe the ATP Cloud features.
- • Introduce Security Director.
- • Explain the purpose of Policy Enforcer.
- • Examine the different virtualized SRX instances.
- • Describe the Juniper Identity Management Service.
- • Explain chassis cluster concepts.
- • Explain how to set up a chassis cluster.
- • Review troubleshooting steps for chassis clusters.
- • Explain Juniper ATP Appliance components.
- • Explain how to set up a Juniper ATP Appliance.
- • Explain how the Juniper Secure Analytics device works.

Prerequisites:

• Basic networking knowledge

• Understanding of the OSI reference model and the TCP/IP protocol suite

Testing and Certification

JNCIS-SEC exam topics are based on the content of the recommended instructor-led training courses, as well as the additional resources.
• Exam code: JN0-335
• Written exam

- Completion of the Introduction to Juniper Security course

- Administered by Pearson VUE
- Exam length: 90 minutes
- Exam type: 65 multiple-choice questions
- Pass/fail status is available immediately
- Junos OS 22.3

The JNCIS-SEC certification is valid for three years.
Exams can be purchased at an additional cost – please ask for details - and scheduled at https://home.pearsonvue.com/junipernetworks/

Follow-on-Courses:

Advanced Juniper Security (AJSEC)

Content:

Day 1

Course Introduction

SSL Proxy

- Explain why SSL proxy is necessary
- Describe and configure client-protection SSL proxy
- Describe and configure server-protection SSL proxy
- Discuss how to monitor SSL proxy
- Explain SSL mirror decrypt feature

Lab 1: SSL Proxy Client Protection

Application Security Theory

- Describe the functionality of the AppSecure suite
- Explain how application identification works
- Describe how to create custom application signatures
- Explain the purpose of the application system cache

Application Security Implementation

- Discuss in depth the AppSecure modules

Lab 2: Implementing AppSecure

Unified Security Policies

- Explain unified security policy evaluation
- Explain URL Category options
- Utilize and configure IPS policy using a template
- Monitor IPS operations Lab 5: IPS

Juniper ATP Cloud

- Describe the Juniper ATP Cloud Web UI options
- Configure the SRX Series Firewall to use Juniper ATP Cloud anti-malware
- Discuss an Infected Host case study

Lab 6: Juniper ATP Cloud Anti-Malware

Juniper ATP Cloud Features

- Explain Security Intelligence
- Describe Encrypted Traffic Insights
- Describe Adaptive Threat Profiling
- Explain IoT Security

Lab 7: ATP Cloud Features

Day 3

Introduction to Security Director

- Explain how to use Security Director
- Describe how to configure firewall policies
- Deploy configuration changes using Security Director

Lab 8: Working with Security Director

Security Director with Policy Enforcer

- Explain how to install Juniper Identity Management Service
- Configure Juniper Identity Management Service
- Describe troubleshooting Juniper Identity Management Service

Lab 11: Juniper Identity Management Service

Day 4

Chassis Cluster Concepts

- Describe chassis clusters
- Identify chassis cluster components
- Describe chassis cluster operation

Chassis Cluster Implementation

- Configure chassis clusters
- Describe advanced chassis cluster options

Lab 12: Implementing Chassis Clusters

Chassis Cluster Troubleshooting

- Troubleshoot chassis clusters
- Review chassis cluster case studies

Lab 13: Troubleshooting Chassis Clusters

Day 5

Juniper ATP Appliance—Overview

- Explain the Cyber Kill Chain model

Lab 3: Unified Security Policies

Day 2

Security Policy Options

- Explain session management options
- Explain Junos ALG functionality
- Implement policy scheduling
- Explain logging

Lab 4: Security Policy Options

Intrusion Detection and Prevention

- Describe the purpose of IPS
- Utilize and update the IPS signature database
- Configure IPS policy

- Explain how to configure a secure fabric
- Describe how infected host remediation occurs

Lab 9: Configuring Juniper Connected Security

Virtual SRX and cSRX

- Explain virtualization
- Discuss network virtualization and software-defined networking
- Review the virtual SRX platform
- Review the cSRX platform
- Deploy the virtual SRX
- Integrate the virtual SRX with public cloud services

Lab 10: vSRX Implementation

Juniper Identity Management Service

- Define deployment models for Juniper ATP Appliance

Implementing Juniper ATP Appliance

- Describe how to configure an SRX Series device with ATP Appliance
- Describe how to mitigate a threat with the ATP Appliance Web UI
- Demo Video: Implementing Juniper ATP Appliance

Juniper Secure Analytics

- Describe the JSA Series device and its basic functionality
- Define how JSA processes log activity
- Explain how JSA processes network activity
- Explain how to customize the processing of information

Lab 14: Monitoring with JSA

Additional Information:

Delegates will receive an official set of e-kit courseware approximately 1 week prior to the start of the course.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK