Datacipher Education Services

Juniper Security

JUNIPER NETWORKS EDUCATION SERVICES

COURSE 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

Intermediate

AUDIENCE

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

PREREQUISITES

- Basic networking knowledge
- Understanding of the OSI reference model and the TCP/IP protocol suite
- Completion of the *Introduction to Juniper Security* course

RELEVANT JUNIPER PRODUCT

- JIMS
- JSA
- Juniper ATP Appliance
- Juniper ATP Cloud
- Junos OS
- Security Director
- SRX Series

RELATED CERTIFICATION

JNCIS-SEC

CONTACT YOUR REGIONAL EDUCATION SERVICES TEAM:

- Americas: training-amer@juniper.net
- EMEA: training-emea@juniper.net
- APAC: training-apac@juniper.net

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.

COURSE CONTENTS

DAY 1

1 Course Introduction

2 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

3 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

4 Application Security Implementation

- Discuss in depth the AppSecure modules

Lab 2: Implementing AppSecure

5 Unified Security Policies

- Explain unified security policy evaluation
- Explain URL Category options

Lab 3: Unified Security Policies

DAY 2

6 Security Policy Options

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

Lab 4: Security Policy Options

7 Intrusion Detection and Prevention

- Describe the purpose of IPS
- Utilize and update the IPS signature database
- Configure IPS policy
- Utilize and configure IPS policy using a template
- Monitor IPS operations

Lab 5: IPS

8 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

9 Juniper ATP Cloud Features

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

Lab 7: ATP Cloud Features

COURSE CONTENTS (contd.)

DAY 3

10 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

11 Security Director with Policy Enforcer

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

Lab 9: Configuring Juniper Connected Security

12 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

13 Juniper Identity Management Service

- 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

14 Chassis Cluster Concepts

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

15 Chassis Cluster Implementation

- Configure chassis clusters
- Describe advanced chassis cluster options

Lab 12: Implementing Chassis Clusters

16 Chassis Cluster Troubleshooting

- Troubleshoot chassis clusters
- Review chassis cluster case studies

Lab 13: Troubleshooting Chassis Clusters

DAY 5

17 Juniper ATP Appliance—Overview

- Explain the Cyber Kill Chain model
- Define deployment models for Juniper ATP Appliance

18 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

19 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

JSEC11152022