SASE—Deploying Juniper Security Service Edge

Juniper Networks | Education Services

COURSE OVERVIEW

This three-day course is designed to provide students with the knowledge of securing on-premises as well as remote users by implementing security policies in Juniper Secure Edge managed by Juniper Security Director cloud. Students will gain foundational knowledge of cloud security policies configured and deployed by Juniper Secure Edge, including Firewall as a Service (FWaaS), secure Web gateway, user identity management, SSL explicit proxy, Web and content filtering, intrusion prevention system (IPS), advanced anti-malware, securing DNS and advanced threat prevention (ATP). Through demonstrations and hands-on labs, students will gain experience with the Secure Edge features of Juniper Secure Access Service Edge (SASE). This course is based on Junos OS Release 22.1R1.10, Security Director 22.1R1.1.

COURSE LEVEL

Intermediate-level course

AUDIENCE

Individuals responsible for managing enterprise on-premises and remote user security configurations on Juniper Secure Edge using the Security Director Cloud application.

PREREQUISITES

- Basic networking knowledge
- Understanding of the OSI reference model and the TCP/IP protocol suite
- Understanding of the session-based L4-L7 firewall concepts
- Basic Junos operating system (OS) knowledge including device management, routing, and security policy
- Completion of the *Juniper Security* course, or equivalent experience

RELATED CERTIFICATION

JNCIA-SEC

RECOMMENDED NEXT COURSE

Juniper SD-WAN with Mist AI

CONTACT YOUR REGIONAL EDUCATION SERVICES TEAM:

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

OBJECTIVES

- Describe the elements of Juniper Secure Access Service Edge.
- Explain Service Locations and sites.
- Configure SSL Proxy in Secure Edge.
- Describe and configure how to secure remote user traffic.
- Explain user identity management in Secure Edge.
- Implement user identity management for remote users.
- Explain how to configure Web filtering and content filtering.
- Describe Juniper ATP Cloud features in Secure Edge.
- Explain how Juniper ATP Cloud features are implemented in Juniper Secure Edge.
- Explain IPS in Secure Edge.
- Use the monitoring tools in Secure Edge.
- Implement Secure Edge for a new site.

SASE—Deploying Juniper Security Service Edge

Juniper Networks | Education Services

COURSE CONTENTS

DAY 1

1 Course Introduction

2 Introducing SASE

- Describe the security challenges of the modern enterprise
- Describe the network challenges of the modern enterprise
- Describe the cloud-delivered approach to securing the enterprise
- Describe the SD-WAN approach to connecting the enterprise
- Explain Juniper Networks Secure Access Service Edge

3 Provisioning Service Locations and Sites

- Describe Secure Edge Service Locations and sites
- Explain the structure and function of Secure Edge policy
- Deploy a Service Location
- Deploy a Secure Edge site

Lab 1: Deploying Service Locations and Sites

4 SSL Proxy

- Describe how SSL proxy works
- Configure and apply SSL proxy profiles in Secure Edge

Lab 2: Configuring SSL Proxy

5 Connecting Remote Users with PAC Files

- Describe how PAC files work
- Create and deploy a PAC file using the PAC file builder
- Modify a PAC file manually using JavaScript

Lab 3: Enrolling Remote Users

6 User Identity and JIMS

- Explain the importance of user identity in securing the enterprise edge
- Describe the available options for authentication in Secure Edge
- Deploy JIMS on-premises user authentication
- Configure Secure Edge policies based on user identity

Lab 4: Implement User Identity Management for On-Premises Users

DAY 2

7 Managing Identity for Remote Users

- Review available options for user identity management
- Configure hosted database to authenticate remote users
- Deploy a third-party SAML identity provider for remote users
- Configure Secure Edge policies based on user identity for remote users

Lab 5: Identity Management for Remote Users

8 Web Filtering and Content Filtering

- Describe Web filtering and content filtering features
- Configure and deploy Secure Edge policy rules with Web filtering and content filtering profiles

Lab 6: Configure Content Filtering and Web Filtering Policies

9 ATP Cloud

- Explain Security Intelligence
- Describe Encrypted Traffic Insights
- Describe DNS filtering

10 ATP Cloud Features in Secure Edge

- Describe how ATP Cloud provides functionality to Secure Edge
- Configure ETI and DNS security
- Configure allowlists and blocklists
- Configure and apply SecIntel profiles
- Configure and apply anti-malware profiles

Lab 7: Implement ATP Cloud Security Features

11 IPS Policies

- Describe IPS
- Configure and apply IPS policies

12 Monitoring Secure Edge

- Navigate the logging workspace
- Configure alerts
- Monitor ATP functions
- Define and generate reports
- Monitor Service Location status

Lab 8: Monitoring Secure Edge

DAY 3

Capstone Case Study

- Explain the case study requirements
- Implement the case study requirements

SSE03202023