JNCIE Security Self-Study Bundle (JNCIE-SEC)

COURSE OVERVIEW

Juniper Networks' JNCIE-SEC Certification Self-Study Bundle is a hands-on guide to validate your skills needed to pass the official JNCIE-SEC lab exam. The guide is based on the official JNCIE-SEC exam blueprint. Each chapter covers several technologies with expert-level configuration tasks and detailed answers. In this workbook you will find several technology introductions and theoretical knowledge about the JNCIE-SEC lab exam blueprint topics. However, do not expect a full explanation about route-based VPNs, UTM, NAT, and other advanced services since there are other resources available for prerequisite knowledge. The guide contains two full practice exams to simulate a real JNCIE-SEC lab exam. This guide is targeted at JNCIP-SEC certified engineers who are studying for the expert-level certification and need extra help preparing for the exam.

With the purchase of this self-study bundle, you will be provided with access to the course materials via Online Secure PDF, a secure PDF workbook of technology-specific lessons and exercises and two JNCIE-SEC practice exams (Super Labs), and one year of lab access with up to 10 hours of lab access per reservation (Maximum of 50 reservations, default reservation is 4 hours)

COURSE LEVEL

JNCIE-SEC Certification Self-Study Bundle is an advanced level course.

AUDIENCE

This bundle benefits individuals who have already honed their skills on security technologies and could use some practice and tips in preparation for the JNCIE-SEC exam.

PREREQUISITES

Students should have passed the Juniper Networks Certified Internet Professional—Service Provider (JNCIP-SEC) written exam or achieved an equal level of expertise through Education Services courseware and hands-on experience.

CONTACT YOUR REGIONAL EDUCATION SERVICES TEAM

- Americas: training-amer@juniper.net
- Europe, Middle East, Africa: training-emea@juniper.net
- Asia-Pacific: training-apac@juniper.net

OBJECTIVES

After successfully completing this course, you should:

- Be better prepared for success in taking the actual JNCIE-SEC exam.
- Be well-versed in exam topics, environment, and conditions.

SELF-STUDY BUNDLE CONTENTS

1

Chapter 1: General System Features

- Initial Configuration
- Authentication and Authorization
- Syslog
- NTP
- SNMP

2

Chapter 2: High Availability

- Creating Clusters – Initial Setup
- Configuring Redundancy Groups and Redundant Ethernet Interfaces

3

Chapter 3: Firewall - Security Policies

- Configuring Interfaces and Security Zones
- Local Traffic and Static Routing
- Security Policies

4

Chapter 4: Unified Threat Management

- Web-filtering
- Antivirus
- Content filtering
- Antispam

COURSE CONTENTS (contd.)

5 Chapter 5: IPsec VPNs

- Configuring Policy-based VPN
- Configuring Route-based VPN
- Configuring GRE-tunnel over Route-based VPN
- Configuring ADVPN

6 Chapter 6: NAT

- IPv4 Source NAT
- IPv4 Destination NAT
- IPv4 Static NAT
- NAT Protocol Translation (IPv6/IPv4)

7 Chapter 7: Attack Prevention and Mitigation

- Firewall Filters
- SCREEN
- Intrusion Prevention System

8 Chapter 8: Extended Implementation Concepts

- Transparent Mode
- Filter Based Forwarding

9 Chapter 9: Advanced Services

- Application Identification
- AppTrack
- AppQoS
- SSL Proxy
- Juniper Identity Management Service (JIMS)
- Security Logging
- Software Defined Secure Network (SDSN)

Superlab 1:

- Initial Configuration - Part 1
- Initial Configuration - Part 2
- Interfaces, Zones, Local Traffic, Routing, and Routing Instances
- UTM
- NAT
- IPsec VPN
- Attack Prevention and Mitigation
- Advanced Services – Central Cluster
- Software Defined Secure Network (SDSN)

Superlab 2:

- Initial Configuration - Part 1
- Initial configuration - Part 2
- Control Plane Protection
- Interfaces, Zones, Local Traffic, and Routing
- UTM
- NAT
- IPsec VPN
- Attack Prevention and Mitigation
- Advanced Services – Central cluster
- Software Defined Secure Network (SDSN)

Appendix – Chapter 1: General System Features

- Initial Configuration
- Authentication and Authorization
- Syslog
- NTP
- SNMP

Appendix – Chapter 2: High Availability

- Creating Clusters – Initial Setup
- Configuring Redundancy Groups and Redundant Ethernet Interfaces

Appendix – Chapter 3: Firewall - Security Policies

- Configuring Interfaces and Security Zones
- Local Traffic and Static Routing
- Security Policies

Appendix – Chapter 4: Unified Threat Management

- Web-filtering
- Antivirus
- Content filtering
- Antispam

Appendix – Chapter 5: IPsec VPNs

- Configuring Policy-based VPN
- Configuring Route-based VPN
- Configuring GRE-tunnel over Route-based VPN
- Configuring ADVPN

COURSE CONTENTS (contd.)

Appendix – Chapter 6: NAT

- IPv4 Source NAT
- IPv4 Destination NAT
- IPv4 Static NAT
- NAT Protocol Translation (IPv6/IPv4)

Appendix – Chapter 7: Attack Prevention and Mitigation

- Firewall Filters
- SCREEN
- Intrusion Prevention System

Appendix – Chapter 8: Extended Implementation Concepts

- Transparent Mode
- Filter Based Forwarding

Appendix – Chapter 9: Advanced Services

- Application Identification
- AppTrack
- AppQoS
- SSL Proxy
- Juniper Identity Management Service (JIMS)
- Security Logging
- Software Defined Secure Network (SDSN)

Appendix – Superlab 1:

- Initial Configuration - Part 1
- Initial Configuration - Part 2
- Interfaces, Zones, Local Traffic, Routing, and Routing Instances
- UTM
- NAT
- IPsec VPN
- Attack Prevention and Mitigation
- Advanced Services – Central Cluster
- Software Defined Secure Network (SDSN)

Appendix – Superlab 2:

- Initial Configuration - Part 1
- Initial configuration - Part 2
- Control Plane Protection
- Interfaces, Zones, Local Traffic, and Routing
- UTM
- NAT
- IPsec VPN
- Attack Prevention and Mitigation
- Advanced Services – Central cluster
- Software Defined Secure Network (SDSN)