

JNCIE Security Bootcamp (JNCIE-SEC)

Course Overview

This five-day course is designed to serve as the ultimate preparation for the Juniper Networks Certified Internet Expert—Security (JNCIE-SEC) exam. The course focuses on caveats and tips useful for potential test candidates and emphasizes hands-on practice through a series of timed lab simulations. On the final day of the course, students are given a six-hour lab simulation emulating the testing topics and environment from the real exam. This course is based on Junos OS Release 12.1X46-D10.2 for SRX Series devices.

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.



Course Length

5 days

Intended Audience

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

Course Level

JNCIE Security Bootcamp is an advanced-level course.

Prerequisites

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


Malaysia (HQ)


C-43-3 Block C Jaya One
No. 72A Jalan Universiti
46200 Petaling Jaya, Selangor, Malaysia
Tel: +603-7954 7433 / +603-7954 8433
Fax: +603-7954 9433

Singapore

420 North Bridge Road
#03-20 North Bridge Centre
Singapore 188727
Tel: +65-6635 5590
Fax: +65-6234 2462

Hong Kong
Thailand
Brunei
Vietnam
Philippines
Indonesia

 enquiry@greensysconsulting.net

 www.greensysconsulting.net

Course Contents

Day 1	Chapter 1: Course Introduction Chapter 2: Exam Strategies <ul style="list-style-type: none"> Prior to the Exam Exam Day After the Exam Chapter 3: Infrastructure Concepts <ul style="list-style-type: none"> Section Topics System Tasks Zones Issues and Tips Infrastructure and Zones Lab Chapter 4: Building Clusters <ul style="list-style-type: none"> Setting Up Clustering Redundancy Groups and Reth Groups Failovers Issues and Tips Creating Clusters Lab 	Day 2	Chapter 5: Security Policies <ul style="list-style-type: none"> Security Policies ALGs Schedulers Bypass Flow Forwarding Logging Issues and Tips Building Security Policies Lab Chapter 6: IPsec VPNs <ul style="list-style-type: none"> Overview of VPN Configuration IKE Proposals, Policies, and Gateways IPsec Proposals, Policies, and Gateways Route-Based, Dynamic, and Certificate-Based VPNs Identifying IPsec Issues Issues and Tips Building IPsec VPNs Lab
Day 3	Chapter 7: Network Address Translation <ul style="list-style-type: none"> Implementation of NAT Source NAT Destination NAT Static NAT Overlapping IP Addresses Verification Commands and Common Issues Network Address Translation Lab Chapter 8: Attack Prevention <ul style="list-style-type: none"> Overview of Attack Prevention IDP AppSecure Additional Prevention Capabilities Issues and Tips Attack Prevention Lab 	Day 4	Chapter 9: Unified Threat Management and Screen Options <ul style="list-style-type: none"> Overview of UTM Web Filtering Anti-Virus Screen Options UTM and Screen Options Lab Chapter 10: Extended Implementation Concepts <ul style="list-style-type: none"> Transparent Mode Filter-Based Forwarding Extended Implementations Lab
Day 5	<ul style="list-style-type: none"> JNCIE-SEC Full Lab Simulation 		