Juniper Networks Design – Security (JND-SEC)

COURSE LEVEL

JND-SEC is an intermediate-level course.

AUDIENCE

This course is targeted specifically for those who have a solid understanding of operation and configuration and are looking to enhance their skill sets by learning the principles of security design.

PREREQUISITES

- Knowledge of network security concepts, including:
- Traditional and next-generation firewalls;
- IPsec VPNs;
- Network Address Translation (NAT); and
- Security intelligence.
- Knowledge of Juniper Networks products and solutions.
- Network automation and virtualization concepts.
- Basic knowledge of hypervisors and high availability concepts.
- Completion of the Juniper Networks Design Fundamentals (JNDF) course.

ASSOCIATED CERTIFICATION

JNCDS-SEC

RELEVANT JUNIPER PRODUCT

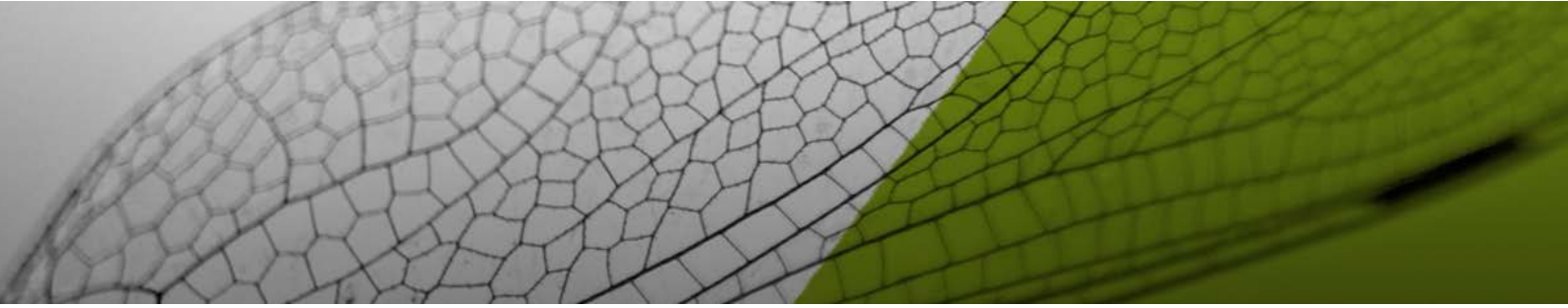
- Design
- Network Design
- ACX Series
- Appsecure
- AX Series
- BTI Series
- BX Series
- C Series
- Contrail
- CSE Series
- CTP Series
- CX Series
- E Series
- EX Series
- IDP Series
- ISG Series
- JCS1200
- JSA Series
- Junos OS
- Junos Space
- Junos Space Network Director
- Junos Space Security Director
- Junos Space Services Activation Director
- Junos SDK
- Junosphere / VJX

COURSE OVERVIEW

This five-day course is designed to cover best practices, theory, and design principles for security design, including traditional and modern security principles such as security design specifics for campus and branch, enterprise wide area network (WAN), service provider WAN, and data center deployments. This course also includes design principles for security management, automation, and virtualization.

OBJECTIVES

- Identify high level security challenges with different design architectures.
- Explain the value of implementing security solutions in any network design.
- Identify key factors in Juniper Networks security focus.
- List and describe the security platforms and solutions offered by Juniper Networks.
- Perform the steps necessary to identify customer security requirements.
- Explain what is required to define the scope of the security design.
- Identify the data required to perform a data analysis of the customer's existing network and use that information in the design.
- Describe traditional security practices used to secure a network.
- Explain the added capabilities that next generation firewalls provide.
- Explain the evolution of modern security models.
- Describe intelligent networks.
- Explain how Software-Defined Secure Networking improves security in network design.
- Explain the need for centralized Security Management.
- Describe what Junos Space Security Director can do to manage network security.
- Describe the function of Juniper Secure Analytics in managing network security.
- List the main components of the Juniper Automation Stack.
- Explain Juniper Networks automation solutions.
- Describe the benefits of automating security.
- Describe how security works in a virtualized environment.
- Explain the benefits of service chaining.
- Describe Juniper Virtual SRX and Container SRX products.
- Describe network virtualization with VMware NSX.
- Describe the benefits of HA with security devices.
- Discuss how to handle asymmetric traffic with security devices.
- Describe different options for SRX chassis cluster deployments.
- Describe the main security concerns for the campus and the branch networks.
- Explain end-to-end security concepts.
- Describe security functions at different network layers.
- Explain network authentication and access control concepts.
- Describe common campus and branch network security design examples.
- Describe security considerations for the enterprise WAN.
- Explain when to use IPsec and NAT in the enterprise WAN.
- Explain virtual router applications for the enterprise WAN.
- Discuss security best practices in the enterprise WAN.
- Describe security in the service provider WAN.
- Discuss security best practices for the service provider WAN.
- Discuss the security requirements and design principles of the data center.
- Describe the security elements of the data center.
- Describe network security implementation options in the data center.
- Discuss network security functionality in the data center.



RELEVANT JUNIPER PRODUCT(Contd)

- LN Series
- M Series
- MX Series
- NetScreen Series
- NFX Series
- NSM Central Manager
- NSMXpress
- Odyssey Access Client
- QFabric
- QFX Series
- SBR Series - Software
- SDX300
- SRC Series
- SRX Series
- SSG Series
- STRM Series
- T Series
- vGW Series
- WLA Series
- WLC Series
- WLM Series
- WXC Series
- Design Track
- Instructor-Led Training.

RECOMMENDED NEXT COURSE

N/A

CONTACT INFORMATION

Contact Juniper Education Services

COURSE CONTENT

Day 1

1 **COURSE INTRODUCTION**

2 **Security in Network Design**

- The Value of Security in Network Design
- Juniper's Security Focus

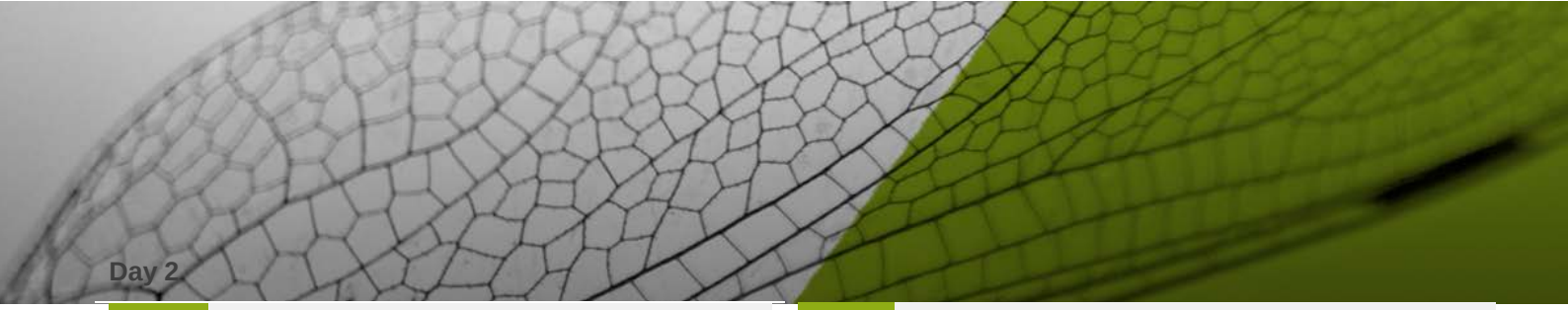
3 **Assessing Security in Network Design**

- Overview
- Customer Security Requirements
- Customer Scope
- Data Analysis

4 **Traditional Security Architectures**

- Traditional Security Practices
- NAT
- IPsec VPNs
- Next Generation Firewalls
- Unified Threat Management

Lab: Designing a Traditional Security Architecture



Day 2

5 Modern Security Principles

- Modern Security Models
- Designing an Intelligent Network
- Use Cases
- Modularity in Security Design

Lab: Designing for Security Intelligence

6 Managing Security

- Security Management Challenges
- Junos Space Security Director
- Juniper Secure Analytics

Lab: Security Management

Day 3

7 Automating Security

- Automating Security Introduction
- Juniper Automation Stack
- Juniper Automation Tools
- Automating Security

Lab: Automating Security

8 Virtualizing Security

- Security in a Virtualized Environment
- Virtual SRX
- Security with SDN and NFV
- Container SRX
- Network Virtualization with VMware NSX

Lab: Virtualizing Security

9 Providing High Availability in Security Design

- Benefits of High Availability with Security Devices
- Implementing Physical High Availability
- Assymmetrical Traffic Handling
- SRX Chassis Clustering

Lab: High Availability

Day 4

10 Securing the Campus and Branch

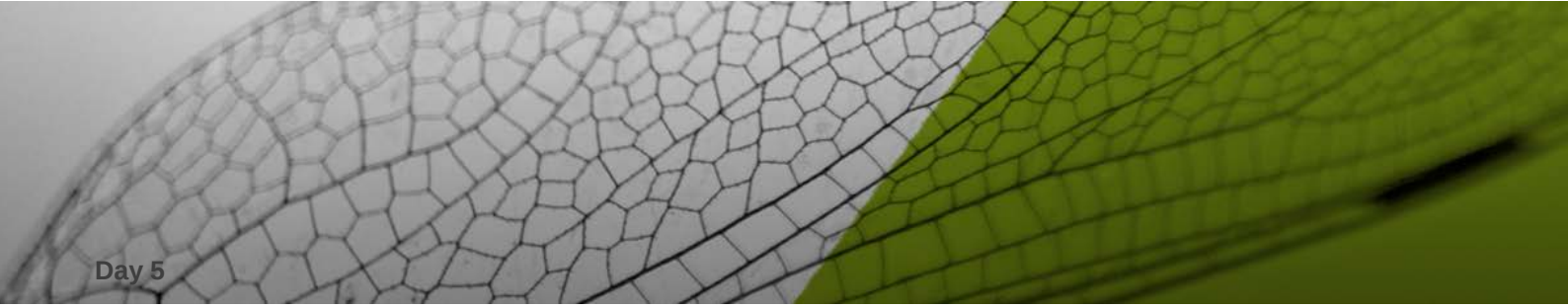
- Campus and Branch Security: An Overview
- Network Segmentation and Perimeter Security
- Application-Level Security
- Access Control and Authentication
- Layer 2 Security Functions
- Case Studies and Example Architectures

Lab: Designing for Campus and Branch Security

11 Securing the Enterprise WAN

- Security in the Enterprise WAN: An Overview
- Best Practices and Considerations
- Case Studies and Example Architectures

Lab: Designing for Enterprise WAN Security



12

Securing the Service Provider WAN

- Security in the Service Provider WAN: An Overview
- Best Practices and Considerations
- Case Studies and Example Architectures

Lab: Designing for Service Provider WAN Security

A

Appendix A: Juniper Security Solutions

- Security Products and Solutions

13

Securing the Data Center

- Overview of Data Center Security
- Security Elements
- Network Security in the Data Center
- Network Security Functions in the Data Center

Lab: Securing the Data Center

JND-SEC080317