Juniper Security

Category: Networking & Security | **Vendor:** Juniper

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This four-day, intermediate-level course provides students with the knowledge required to work with Juniper Connected Security devices. This course uses Junos CLI, Junos Space® Security Director. 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 intrusion detection and prevention (IDP) rules and custom attack objects, IPSec VPNs, Security Director management, Juniper® Advanced Threat Prevention management (ATP) Cloud management, Policy Enforcer management, Identity aware security policies, Secure Sockets Layer (SSL) Proxy configuration, and Juniper Networks® SRX Series Firewalls high availability configuration and troubleshooting. Through demonstrations and hands-on labs, students will gain experience with the features of each of these devices.

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 24.2R1, Junos Space 23.1R1, Security Director 23.1R1, and JIMS 1.7.0R2.

About This Course

- Implementing Intrusion Detection and Prevention
- Implementing SSL Proxy
- IPsec VPN Concepts
- Implementing Site-to-Site IPsec VPNs
- Implementing Juniper Secure Connect
- Implementing Identity Aware Security Policies
- Introducing Security Director
- Introducing Policy Enforcer
- Implementing Juniper ATP Cloud Anti-Malware
- Implementing Juniper ATP Cloud Features
- Understanding Chassis Cluster Concepts
- Implementing a Chassis Cluster
- Troubleshooting a Chassis Cluster

Self-Study Module

- Explain Junos OS Routing Fundamentals

Who Should Attend

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

Prerequisites & Entry Requirements

General Prerequisites:

- Basic networking knowledge and an understanding of the OSI reference model and the TCP/ IP protocol suite
- Completing the Introduction to the Junos Operating System (IJOS) course

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Explain the basics of intrusion detection.
- Explain the function of SSL Proxy.
- Explain IPsec VPN concepts.
- Implement site-to-site IPsec VPNs.
- Implement Juniper® Secure Connect.
- Implement identity-aware security policies.
- Explain Security Director.
- Introduce Policy Enforcer.
- Describe the Juniper ATP Cloud Anti-Malware.
- Describe the Juniper ATP Cloud features.
- Explain the concepts of a chassis cluster.
- Explain how to set up a chassis cluster.
- Review troubleshooting steps for chassis clusters.
- Explain how to set up a chassis cluster.

Detailed Course Outline

DAY 1

Module 1: Implementing Intrusion Detection and Prevention

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

Lab 1: Implementing IDP

Module 2: Implementing 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 the SSL mirror decrypt feature

Lab 2: Implementing SSL Proxy

Module 3: IPsec VPN Concepts

- Identify various types of VPNs
- Describe IPsec VPNs and their functionalities
- Describe how IPsec VPNs are established
- Describe IPsec traffic processing

Module 4: Implementing Site-to-Site IPsec VPNs

- Describe the high-level configuration options for an IPsec VPN
- Describe the functionality of proxy IDs and traffic selectors
- Configure an IPsec site-to-site VPN
- Monitor a site-to-site IPsec VPN

Lab 3: Implementing Site-to-Site IPsec VPNs

DAY 2

Module 5: Implementing Juniper Secure Connect

- Describe Juniper Secure Connect features

- Explain Juniper Secure Connect UI options
- Configure Juniper Secure Connect on SRX Series devices
- Connect Juniper Secure Connect Client

Lab 4: Implementing Juniper Secure Connect

Module 6: Implementing Identity Aware Security Policies

- Describe identity-aware firewall and list supported identity sources
- Describe Active Directory as identity source
- Configure Active Directory as identity source
- Describe Juniper Identity Management Service
- Explain how to install Juniper Identity Management Service
- Configure Juniper Identity Management Service
- Describe how to troubleshoot Juniper Identity Management Service

Lab 5: Implementing Identity Aware Security Policies

Module 7: Introducing Security Director

- Explain the benefits of Security Director
- Explain Security Director deployment options
- Demonstrate how to access and use the Security Director UI
- Demonstrate how to onboard a device
- Demonstrate how to manage security policies
- Demonstrate how to deploy and validate configuration changes

Lab 6: Using Security Director

DAY 3

Module 8: Introducing Policy Enforcer

- Explain the benefits of Policy Enforcer

- Explain how to configure a secure fabric

- Describe how infected host remediation occurs

Module 9: Implementing Juniper ATP Cloud Anti-Malware

- Describe Juniper ATP Cloud anti-malware capabilities

- Describe the Juniper ATP Cloud Web UI options

- Configure the SRX Series Firewall to use Juniper ATP Cloud anti-malware

- Discuss a Juniper ATP Cloud anti-malware case study

Lab 7: Enrolling Devices in Juniper ATP Cloud

Module 10: Implementing Juniper ATP Cloud Features

- Explain Security Intelligence

- Describe Encrypted Traffic Insights

- Describe Adaptive Threat Profiling

- Explain IoT Security

Lab 8: Implementing ATP Cloud Features

DAY 4

Module 11: Understanding Chassis Cluster Concepts

- Describe why customers implement a chassis cluster

- Identify chassis cluster components

- Describe the causes of failover

Module 12: Implementing a Chassis Cluster

- Configure a chassis cluster

- Explain additional chassis cluster configuration options

Lab 9: Implementing a Chassis Cluster

Module 13: Troubleshooting a Chassis Cluster

- Troubleshoot a chassis cluster

- Explain the chassis cluster case studies

SELF-STUDY MODULE

Module 14: Explain Junos OS Routing Fundamentals

- Explain the difference between directly connected, static, and dynamic routes

- Explain how route preference determines the active route to a destination

- Demonstrate how to display and examine the inet.0 and inet6.0 routing tables

- Configure and validate static routing

- Explain the flow process

Skills You Will Learn:

- Explain the basics of intrusion detection.
- Explain the function of SSL Proxy.
- Explain IPsec VPN concepts.
- Implement site-to-site IPsec VPNs.
- Implement Juniper® Secure Connect.
- Implement identity-aware security policies.
- Explain Security Director.
- Introduce Policy Enforcer.
- Describe the Juniper ATP Cloud Anti-Malware.
- Describe the Juniper ATP Cloud features.
- Explain the concepts of a chassis cluster.
- Explain how to set up a chassis cluster.
- Review troubleshooting steps for chassis clusters.
- Explain how to set up a chassis cluster.

Frequently Asked Questions

Q: What delivery options are available for Juniper Security?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 4-day Juniper Security course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Juniper Security training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Juniper Security?

Yes, we provide corporate training, dedicated training, and closed classes for Juniper Security. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Juniper Security, Junos Security, JSEC

Q: Why choose Nexus Human for Juniper Security?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Juniper Security training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)