
CONFIGURING JUNIPER NETWORKS FIREWALL/IPSEC VPN PRODUCTS

Course No: EDU-JUN-CJFV

Length: Three days

Course Overview

This course is the first in the ScreenOS curriculum. It is a three-day, instructor-led course that focuses on configuration of the Juniper Networks firewall/VPN products in a variety of situations, including basic administrative access, routing, firewall policies and policy options, attack prevention features, address translation, and VPN implementations.

The course combines both lecture and labs, with significant time allocated for hands-on experience. Students completing this course should be confident in their ability to configure Juniper Networks firewall/VPN products in a wide range of installations.

Objectives

After successfully completing this course, you should be able to:

- Explain the Juniper Networks security architecture.
- Configure administrative access and options.
- Back up and restore configuration and ScreenOS files.
- Configure a Juniper Networks device in transparent, route, and NAT modes.
- Discuss the applications of multiple virtual routers.
- Configure the Juniper Networks firewall to permit and deny traffic based on user defined policies.
- Configure advanced policy options.
- Identify and configure network designs for various types of network address translation.
- Configure policy-based and route-based VPN tunnels.

Intended Audience

This course is intended for network engineers, support personnel, reseller support, and others responsible for implementing Juniper Networks firewall products.

Course Level

This is an introductory-level course.

Prerequisites

This course assumes that students have basic networking knowledge and experience in the following areas:

- The Internet;
- Networking concepts; and
- Terms including TCP/IP, bridging, switching, and routing.

Course Contents

Day 1

Chapter 1: Course Introduction

Chapter 2: ScreenOS Concepts, Terminology, and Platforms

- Security Device Requirements
- ScreenOS Security Architecture
- Juniper Networks Platforms

Chapter 3: Initial Connectivity

- System Components
- Establishing Connectivity
- Verifying Connectivity
- Lab 1: Initial Configuration

Chapter 4: Device Management

- Management
- Recovery
- Lab 2: Device Administration

Day 2

Chapter 5: Layer 3 Operations

- Need for Routing
- Configuring Layer 3
- Verifying Layer 3
- Loopback Interface
- Interface-Based NAT
- Lab 3: Layer 3 Operations

Chapter 6: Basic Policy Configuration

- Functionality
- Policy Configuration
- Common Problems
- Global Policy
- Verifying Policies
- Lab 4: Basic Policy Configuration

Chapter 7: Policy Options

- Overview
- Logging
- Counting
- Scheduling

- User Authentication
- Lab 5: Policy Options

Chapter 8: Address Translation

- Scenarios
- NAT-src
- NAT-dst
- VIP Addresses
- MIP Addresses
- Lab 6: Address Translation

Day 3

Chapter 9: Transparent Mode (Optional)

- Description
- Configuration
- Verifying Operations
- Lab 7: Transparent Mode

Chapter 10: VPN Concepts

- Concepts and Terminology
- IP Security

Chapter 11: Policy-Based VPNs

- Configuration
- Verifying Operations
- Lab 8: Policy-Based VPNs

Chapter 12: Route-Based VPNs

- Concepts and Terminology
- Configuring VPNs
- Verifying Operations
- Lab 9: Route-Based VPNs

Appendix A: Additional Features

- Hardware