Configuring Juniper Networks Firewall/IPsec VPN Products (CJFV)

COURSE LEVEL

Configuring Juniper Networks Firewall/IPsec VPN Products is an introductory-level course

AUDIENCE

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

PREREQUISITES

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

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 ScreenOS firewall/virtual private network (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. This course is based on ScreenOS version 6.3r14.

OBJECTIVES

- Explain the ScreenOS security architecture.
- Configure administrative access and options
- Back up and restore configuration and ScreenOS files.
- Configure a ScreenOS device in transparent, route, Network Address Translation (NAT), and IP version 6 (IPv6) modes.
- Discuss the applications of multiple virtual routers.
- Configure the ScreenOS 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.

ASSOCIATED CERTIFICATION

JNCIA-FWV, JNCIS-FWV

RELEVANT JUNIPER PRODUCT

- NetScreen Series
- SSG Series

RECOMMENDED NEXT COURSE

- Attack Prevention with Juniper Networks Firewalls (APJF)
- Advanced Juniper Networks IPsec VPN Implementations (AJVI)
- Integrating Juniper Networks Firewalls and VPNs into High-Performance Networks (IFVH)

CONTACT INFORMATION

training@juniper.net

Configuring Juniper Networks Firewall/IPsec VPN Products (CJFV)

COURSE CONTENT

Day 1

1 COURSE INTRODUCTION

2 ScreenOS Concepts, Terminology, and Platforms

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

3 Initial Connectivity

- System Components
- Establishing Connectivity
- Verifying Connectivity

LAB: Initial Configuration

4 Device Management

- Management
- Recovery

LAB: Device Administration

Day 2

5 Layer 3 Operations

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

LAB: Layer 3 Operations

6 Basic Policy Configuration

- Functionality
- Policy Configuration
- Common Problems
- Global Policy
- Verifying Policies

LAB: Basic Policy Configuration

7 Policy Options

- Overview
- Logging
- Counting
- Scheduling
- User Authentication

LAB: Policy Options

8 Address Translation

- Scenarios
- NAT-src
- NAT-dst
- VIP Addresses
- MIP Addresses

LAB: Address Translation

Day 3

9 VPN Concepts

- Concepts and Terminology
- IP Security

10 Policy-Based VPNs

- Configuration
- Verifying Operations
- **LAB: Policy-Based VPNs**

11 Route-Based VPNs

- Concepts and Terminology
- Configuring VPNs
- Verifying Operations
- **LAB: Route-Based VPNs**

12 IPv6

- IPv6 Concepts
- Configuring IPv6
- Verifying IPv6
- **Lab: IPv6**

Appendix A: Additional Features

- Hardware

Appendix B: Transparent Mode

- Description
- Configuration
- Verifying Operations
- Lab: Transparent Mode (Optional)