Firewall from A-Z

Course 1768 – 40 Hours

Overview

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 and Cisco products in a wide range of installations.

Who Should Attend

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

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

Course Introduction

ScreenOS Concepts, Terminology, and Platforms

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

Initial Connectivity

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

Device Management

- Management
- Recovery
- Lab 2: Device Administration

Layer 3 Operations

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

- Interface-Based NAT
- Lab 3: Layer 3 Operations

Basic Policy Configuration

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

Address Translation

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

Cisco Firewall

- INTRODUCING ASA
- GETTING START
- Firewall basic configuration
- FIREWALL EXTENDED CONFIGURATION
- SITE TO SITE VPN
- REMOTE ACCESS VPN
- WEB VPN