CONFIGURING JUNIPER NETWORKS FIREWALL/IPSEC VPN PRODUCTS

DURATION: 3 DAYS

COURSE OVERVIEW

This course is the first in the Screen OS curriculum. It is a three-day, instructor-led course that focuses on configuration of the Screen OS 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 Screen OS version 6.3r14. Configuring Juniper Networks Firewall/IPsec VPN Products is an introductory-level course.

TARGET AUDIENCE

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

COURSE OBJECTIVES

1. **After you complete this course you will be able to:**
2. After successfully completing this course, you should be able to:
3. Explain the Screen OS security architecture.
4. Configure administrative access and options.
5. Backup and restore configuration and Screen OS files.
6. Configure a Screen OS device in transparent, route, Network Address Translation (NAT), and IP version 6 (IPv6) modes.
7. Discuss the applications of multiple virtual routers.

8. Configure the Screen OS firewall to permit and deny traffic based on user defined policies.
9. Configure advanced policy options.
10. Identify and configure network designs for various types of network address translation.
11. Configure policy-based and route-based VPN tunnels.

COURSE CONTENT

Chapter 1: Course Introduction

Chapter 2: Screen OS Concepts, Terminology, and Platforms

Security Device Requirements

Screen OS 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

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

Chapter 9: VPN Concepts

Concepts and Terminology

IP Security

Chapter 10: Policy-Based VPNs

Configuration

Verifying Operations

Lab 7: Policy-Based VPNs

Chapter 11: Route-Based VPNs

Concepts and Terminology

Configuring VPNs

Verifying Operations

Lab 8: Route-Based VPNs

Chapter 12:IPv6

IPv6 Concepts

Configuration

Verifying IPv6 Operations

Lab 9: IPv6

Appendix A: Additional Feature

Hardware

Appendix B: Transparent Mode

Description

Configuration

Verifying Operations

Lab: Transparent Mode (Optional)

COURSE PREREQUISITES

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

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