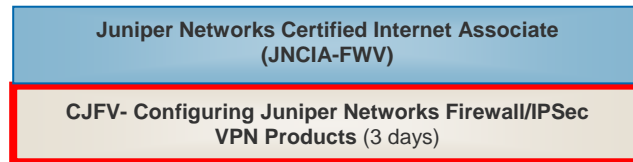




JUNIPER (ScreenOS, NetScreen, SSG, ISG) FIREWALL/VPN



Configuring Juniper Networks Firewall/IPSec VPN Products (CJFV)

Course Overview

This three day course is a survey of the most-commonly used features of ScreenOS, and is designed to provide a broad overview of the wide range of functions these devices can serve in a network. Upon completing this course, a student should be able to return to work and successfully install, configure, and verify that a ScreenOS-based device is providing basic firewall and VPN functionality

Target audience

Network engineers, support personnel, reseller support, and others responsible for implementing Juniper firewall products.

Course Level

Introductory

Prerequisites

This course assumes that students have basic networking knowledge and experience in the areas of; Routing Ethernet, Transparent bridging, TCP/IP operations and IP addressing

Day One

Introduction

- ScreenOS Concepts, Terminology, and Platforms
- Describe the requirements of a security device
- Describe the ScreenOS Security Architecture
- Describe the flow of a packet through a ScreenOS device
- Select ScreenOS-based devices based on deployment requirement

Initial Connectivity

- Describe the functions performed by different system components
- Select a user interface based on business and task requirements
- Establish connectivity to the ScreenOS device using best-practice recommendations

Device Management

- Connect to external management devices
- Manage license keys
- Manage configuration and software image files
- Perform disaster recovery procedures

Day Two

Layer 3 Operations

- Layer 3 Operations
- Explain the virtual router architecture
- Configure static routes
- Explain the use of a loopback interface
- Configure a loopback interface
- Configure interfaces for NAT or route mode
- Verify and troubleshoot Layer 3 operations

Basic Policy Configuration

- Review security policy functionality
- Configure a basic security policy using the following elements
 - Address book entries and groups
 - Custom services and service groups
 - Multi-cell policies
- List potential problems associated with policy creation and modification
- Configure global policy rules
- Verifying policies



Policy Options

- Configure policy options, including:
 - Traffic logging
 - Traffic counters
 - Scheduling
 - User Authentication
- Verify operations of policy options

Address Translation

- Discuss scenarios for policy-based translation
 - Unidirectional outbound
 - Unidirectional inbound
 - Bidirectional
- Configure policy-based translation
 - NAT-src
 - NAT-dst
 - VIP
 - MIP

Day Three

VPN Concepts

- Define virtual private network
- List three security concerns and describe how to address them
- List the components of the IPSec protocol suite
- Explain the IKE protocol process for tunnel establishment

Policy Based VPNs

- Define the term policy-based VPN
- Identify the minimum components needed to configure a Policy-based VPN
- Configure a IKE based VPN binding to Policies with:
 - Phase 1 Gateways
 - Phase 2 AutoKey IKE
 - Address and Service Books
- Verify operations

Route Based VPNs

- Explain the concepts of a route-based VPN
- Configure route-based VPNs with the following options:
 - Fixed IP v Unnumbered IP
 - Proxy ID Settings
 - VPN Monitoring
- Verify operations

Transparent Mode (optional time permitting)

- Describe the advantages of Transparent Mode operation
- Distinguish between transparent mode zones and interfaces and Layer 3 mode zones and interfaces
- Use the VLAN1 interface to manage the ScreenOS device in Transparent Mode

Cost AUD \$2,099 inc. GST

For Available Dates & Terms and Conditions see:
www.crystalecho.com

