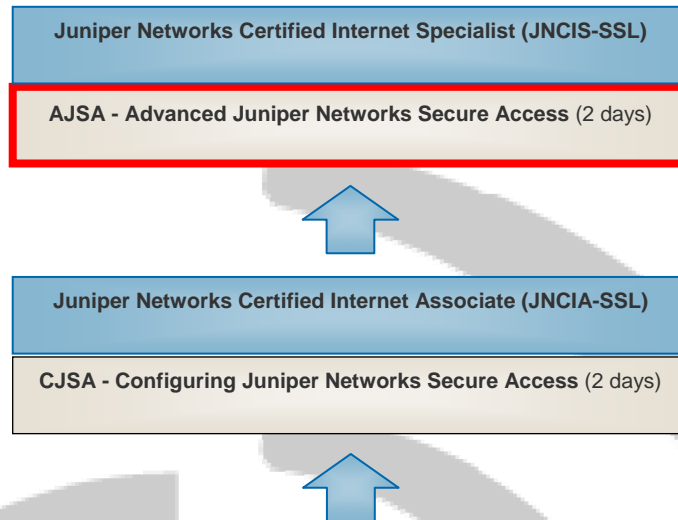




JUNIPER SECURE ACCESS (SSL VPN)



Advanced Juniper Secure Access (AJSA)

Course Overview

This two-day course discusses the advanced configuration of Juniper Networks SA Series SSL VPN Appliances. Key topics include public key infrastructure (PKI) support, additional authentication and authorization servers, complex policies, customization, virtual systems, troubleshooting, high availability, and Secure Meeting. This course is based on software Release 7.1.

Objectives

After successfully completing this course, you should be able to deploy the SA products to support common environments. Specific topics include the following:

- Advanced access management:
- PKI support.
- Certificate revocation lists (CRLs).
- Virtual hosting.
- Single sign-on (SSO).
- Advanced authentication:
- Certificate.
- Anonymous.
- SiteMinder.
- Security Assertion Markup Language (SAML).
- Advanced policies:
- Rewriting policies.
- Authentication policies.
- Role mapping.
- Resource policies.
- Password management.
- Administrative delegation.
- Custom user interface (UI).
- Advanced Client and Server Configuration:
- Secure Application Manager (SAM).

- Network Connect.
- Junos Pulse.
- Enhanced Endpoint Security (EES).
- Clustering.
- Troubleshooting.
- Virtualization:
- Instant Virtual System (IVS).
- Virtual Appliances.
- Secure Meeting.

Target Audience

The target audience includes network engineers, support personnel, reseller support, and anyone responsible for implementing SA Series products.

Course Level

Advanced

Prerequisites

This course assumes that students have successfully attended the Configuring Juniper Networks Secure Access (CJSA) course or have equivalent experience with the Juniper Networks Secure Access products. Specifically, students must be familiar with the configuration of the following:

- Roles;
- Realms;
- Resource policies; and
- Authentication servers



Day One

Chapter 1: Course Introduction

Chapter 2: Authentication Options

- Creating Sign-In URLs
- Organizing Sign-In URLs
- Multiple Sign-In Credentials
- Configuring SSO
- Lab 1: Configuration Review and Authentication Options

Chapter 3: Certificates

- Certificates
- Configuring the Certificate Authentication Server
- Configuring Multiple Server Certificates
- Lab 2: Using Certificates

Chapter 4: Complex Policies

- Resource Policies
- Role Mapping Rules
- Resource Profile Templates
- Specialized Web Resource Policies
- Lab 3: Complex Policies

Chapter 5: Client and Server

- Describe Network Connect
- IKEv2
- Junos Pulse
- Federation of Users with IF-MAP
- Describe Installers
- Describe Launchers
- Lab 4: Client and Server

Chapter 6: Administration

- Administration
- Delegated Administration
- System Logs
- Lab 5: Administration

Day Two

Chapter 7: Endpoint Security

- Describing Endpoint Security
- Configuring Host Checker
- Describing Enhanced Endpoint Security
- Configuring Endpoint Solutions
- Lab 6: Host Checker (Demo)

Chapter 8: Virtualization

- Describing Virtualization
- Configuring the Instant Virtual System
- Configuring Virtual Appliance Licensing
- Lab 7: Virtual Systems

Chapter 9: Troubleshooting

- Troubleshooting Concepts
- Content Intermediation Engine
- Troubleshooting Network Connect
- General Troubleshooting
- Lab 8: Troubleshooting

Chapter 10: Clustering

- Describing Clustering
- Configuring Clustering
- Lab 9: Active/Passive Clustering

Chapter 11: Secure Meeting

- Describing Secure Meeting
- Configuring Secure Meeting
- Meetings
- Secure Meeting Client
- Lab 10: Secure Meeting

Cost AUD \$1,499 inc. GST

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