



Course No: (TWI-JUN-CJSA)
Length: 2 days

About this Course

This two-day course discusses the configuration of Juniper Networks SA Series SSL VPN Appliances in a typical network environment. Key topics include Secure Sockets Layer (SSL) access technologies, basic implementation, and configuration and management options. This course is based on software Release 7.1.

Through demonstrations and hands-on labs, students will gain experience in configuring, testing, and troubleshooting basic facets of the SA Series products.

Objectives

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

- Introduction to the SA Series device.
- Introduction to the SSL protocol and public key infrastructure (PKI).
- Typical deployment scenarios.
- SA Series terminology.
- Roles.
- Role restrictions.
- Realms.
- Resource policies.
- Sign-in policies.
- Authentication servers:
 - Local.
 - The Lightweight Directory Access Protocol (LDAP).
 - RADIUS (including two-factor).
 - Active Directory/NT.
 - Network Information Service (NIS).
- Authentication policies.
- Host Checker.
- Cache Cleaner.
- Secure Virtual Workspace (SVW).
- Enhanced Endpoint Security (EES).
- Client and server support:
 - Java Secure Application Manager (JSAM).
 - Windows Secure Application Manager (WSAM).
- Network Connect.
- Junos Pulse.
- Troubleshooting.

twine networks



Intended Audience

This course is intended for network engineers, support personnel, reseller support, and anyone responsible for implementing SA Series products.

Course Level

CJSA is an introductory-level course.

Prerequisites

This course assumes that students have basic networking knowledge and experience in the following. This course assumes that students have moderate background in internetworking basics, basic security concepts, network administration, and application support.

Course Contents

Day1

Chapter 1: Course Introduction

Chapter 2: Products and Features

- Secure Remote Access Overview
- SSL VPN Deployment Options
- SA Series Platforms and Feature Sets

Chapter 3: Technology and Terminology

- SSL and TLS Overview
- SSL VPN Access Methods
- SSL VPN Platform Architecture
- SSL VPN Terminology

Chapter 4: Initial Configuration

- Console Configuration
- Administrative UI
- Lab 1: Initial Configuration

Chapter 5: User Roles

- Configuring User Roles
- Role Mapping
- Customizing the User Experience
- Lab 2: User Roles

Chapter 6: Logging and Troubleshooting

- Logs
- Troubleshooting Tools
- Lab 3: Logging and Troubleshooting

twine networks



Day 2

Chapter 7: Resource Policies

- What Is a Resource?
- Resource Policy Configuration
- Resource Policy Options
- Resource Profile Configuration
- Lab 4: Resource Policies and Profiles

Chapter 8: Authentication Options

- The Authentication Process
- Configuring Authentication
- Lab 5: Authentication Servers and Realms

Chapter 9: Client and Server Applications

- The Need for Client/Server Support
- Secure Application Manager
- Network Connect
- Junos Pulse
- Telnet and SSH
- Terminal Services
- Lab 6: Client and Server Support

Chapter 10: Endpoint Security

- The TNC Architecture
- Configuring Host Checker
- Configuring Enhanced Endpoint Security
- Configuring Secure Virtual Workspace
- Configuring Cache Cleaner
- Configuring Authentication Policies
- Configuring Role Restrictions
- Lab 7: Endpoint Security

twine networks