Configuring Juniper Networks Secure Access

Duración: 2 Días   Código del Curso: CJSA

Temario:

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.

Dirigido a:

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

Objetivos:

- **After you complete this course you will be able to:**

- 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.

Prerequisitos:

Attendees should meet the following prerequisites:

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

Exámenes y certificación

Recommended preparationfor exam(s):

- Exam code: JN0-562 Juniper Networks Certified Internet Associate (JNCIA-SSL)

Siguientes cursos recomendados:

The following courses are recommended for further study:

- Advanced Juniper Networks Secure Access (AJSA)

Contenido:

Products and Features

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

Technology and Terminology

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

Initial Configuration

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

User Roles

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

Logging and Troubleshooting

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

Resource Policies

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

Authentication Options

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

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

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

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.es

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid

---