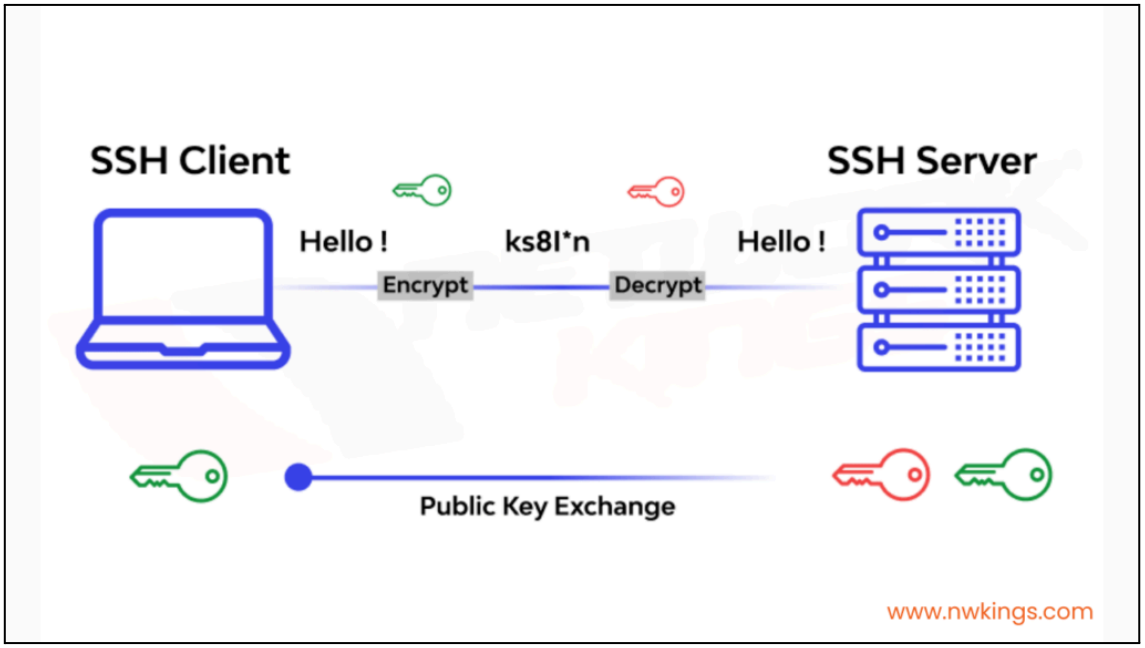
Guía Completa para Configurar SSH en un Router Cisco

1. ¿Qué es SSH?

SSH (Secure Shell) es un protocolo que permite la administración remota de dispositivos de red de manera segura. Utiliza técnicas de cifrado y autenticación para garantizar que la comunicación entre el cliente y el servidor sea segura. SSH reemplaza protocolos inseguros como Telnet, proporcionando una conexión encriptada que protege contra ataques de interceptación de datos.

2. ¿Cómo funciona SSH?

1. **Autenticación:** SSH puede autenticarse mediante contraseñas o claves RSA.
2. **Contraseñas:** El usuario ingresa un nombre de usuario y una contraseña, que se cifran antes de enviarse al servidor.
3. **Claves RSA:** SSH también puede utilizar un par de claves (pública y privada) para la autenticación. La clave pública se almacena en el servidor, mientras que la clave privada permanece en el cliente. Durante la conexión, el servidor envía un desafío que solo el cliente con la clave privada correcta puede descifrar.
4. **Cifrado:** SSH cifra todos los datos transmitidos usando algoritmos como AES, asegurando que la información no pueda ser leída por atacantes.
5. **Integridad:** SSH asegura que los datos no han sido alterados durante la transmisión utilizando códigos de autenticación de mensajes (MAC).



3. Configuración Paso a Paso

Paso 1: Configurar la Contraseña Secreta

Antes de acceder al modo de configuración global, es necesario configurar una contraseña secreta.

enable secret strongpassword

enable secret strongpassword: Este comando establece una contraseña cifrada para acceder al modo privilegiado.

Paso 2: Acceder al Modo de Configuración Global

Paso 3: Configurar el Nombre de Dominio

ip domain-name example.com
ip domain-name example.com: Establece el nombre de dominio que será utilizado en la generación de claves RSA.

Paso 4: Crear un Usuario Local

username admin privilege 15 secret yourpassword

username admin privilege 15 secret yourpassword: Crea un usuario "admin" con privilegios completos y una contraseña cifrada.

Paso 5: Generar Claves RSA

#crypto key generate rsa general-keys modulus 2048

crypto key generate rsa general-keys modulus 2048: Genera un par de claves RSA de 2048 bits, utilizadas para cifrar la comunicación y autenticación mediante SSH.

Paso 6: Configurar las Líneas VTY para Usar SSH

line vty 0 4
transport input ssh
login local
exit

line vty 0 4: Selecciona las líneas VTY (líneas virtuales) que permiten acceso remoto al router.
transport input ssh: Configura las líneas VTY para aceptar solo conexiones SSH.
login local: Utiliza la base de datos local de usuarios para la autenticación.

Paso 7: Habilitar SSH Versión 2

#ip ssh version 2

ip ssh version 2: Habilita la versión 2 de SSH, que es más segura y moderna que la versión 1.

Paso 8: Cifrado de las Claves RSA (Opcional)

crypto key encrypt rsa

crypto key encrypt rsa: Cifra las claves RSA generadas para añadir una capa adicional de seguridad.

Paso 9: Verificar la Configuración de SSH

#show ip ssh

show ip ssh: Muestra la configuración actual de SSH en el router.