

 ${\bf 1}$ – Conéctate mediante consola al router y ponte en modo de configuración de terminal:

en conf t

2 - Dale una IP a la interfaz del router por la que vayas a acceder mediante SSH:

int gi0/0 ip address 192.168.1.1 255.255.255.0 no shutdown exit

3 - Dale hostname y dominio al router

hostname routerprueba
ip domain-name routerprueba.com

4 - Generar las claves rsa

crypto key generate rsa

Elige la longitud de la clave. 2048 es bastante fuerte pero va a tardar un buen rato

5 - Configura el servidor SSH

ip ssh version 2

Opcional: Configura la cantidad de reintentos y el time-out:

ip ssh authentication-retries 3
ip ssh time-out 30

6 - Configura la línea virtual teletipo (usada sólo para conexiones de entrada):

line vty 0 15
login local
exit

7 - Configura el/los usuario/s:

username nico password nico username pepito password pepito

8 - Crea una contraseña cifrada para acceder al modo privilegiado:

enable secret clave123

NOTA: Si no quieres tener dos contraseñas diferentes y, al mismo tiempo, quieres que no se vea la contraseña sin cifrar (aunque en este caso da igual porque no tiene privilegios), puedes crear un usuario directamente con la contraseña cifrada y los privilegios suficientes para entrar al modo enabled. Podrías incluso agregarlo como segundo usuario o, si quieres, borrar el primero (quitando también el secret) y poner este nuevo con todo incluido. El comando es:



username NombreDeUsuario privilege 15 secret Contraseña

Así, en vez de tener dos líneas en el running-config, sólo tendrás una que no dará información de nada. Eso si, si pierdes la contraseña de ese usuario tendrás que recurrir al cable de consola. Por eso, a lo mejor, te convendría crear dos usuarios diferentes usando el mismo método. Al menos, si no tienes alzheimer, te acordarás de una de ambas contraseñas.