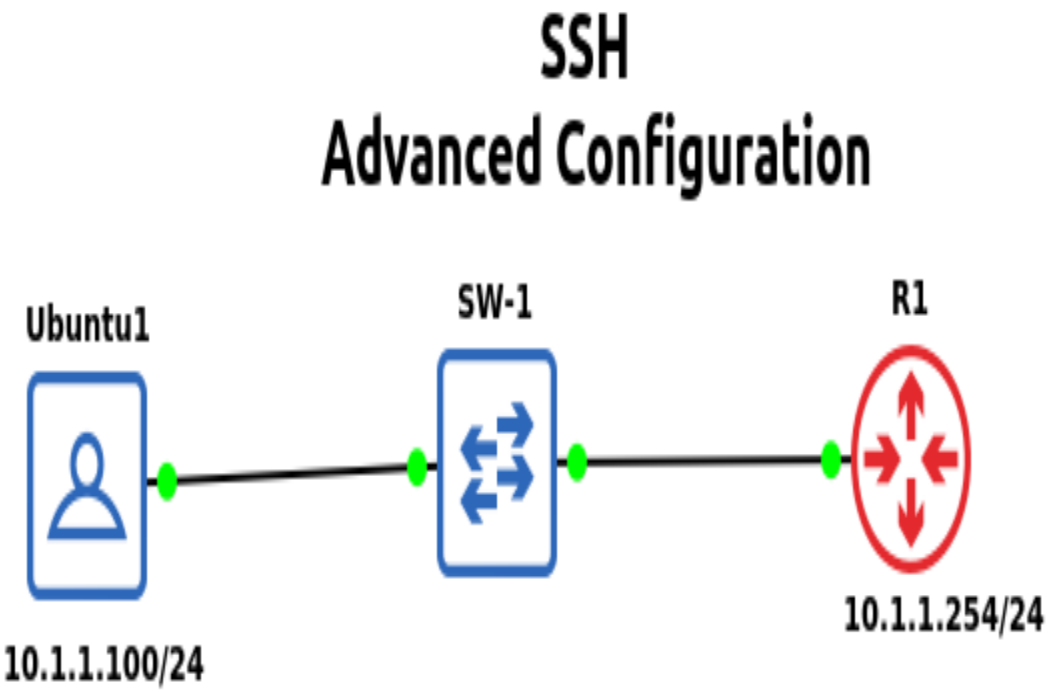
SSH
Advance Configuration on a Router R1



Objetivos de la Práctica

Configurar el dispositivo **Router R1** para que pueda ser alcanzado a través de **SSH** con llave Pública.

Actividades

En el Cliente SSH "**Ubuntu1**" es necesario utilizar el comando "**ssh-keygen**" para generar la l**lave Privada** y **llave Pública**, esta última será configurada dentro de "**R1**" para evitar que al iniciar una conexión a tráves de **SSH** por este cliente se evite pedir la contraseña.

1.- Realizar un cambio de directorio hacia ***/root/.ssh/***

cd /root/.ssh/

2.- Dentro de esta carpeta ejecutaremos el comando "***ssh-keygen***" con los siguientes argumentos.

ssh-keygen -t rsa -b 2048

Donde:

-t rsa	Es el tipo de sistema de encriptación (***Rivest-Shamir-Adleman***).
-b 2048	Es el tamaño en bits de la ***llave Pública*** y ***Privada***.

Después se nos pedirá que ingresemos el nombre a las llaves.

```
root@Ubuntu1:~/.ssh# ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:SbL4wy5+KZFHv2eMhVmxe/DMcDjJGLxhuP3vqxm1h6k root@Ubuntu1
The key's randomart image is:
+---[RSA 2048]----+
|       o         |
|      . = .      |
|      .+.* =     |
|     .o++.X .    |
|    .o..S= X.    |
|    oo. + +.=+   |
|     o+. =.o+ .  |
|    o.o.o ++..   |
|   ..+.  oEoo.   |
+----[SHA256]-----+
```

2.- Una vez creada las llaves es necesario pasar el contenido de la ***llave Pública*** hacia ***R1***, para ello utilizaremos el comando siguiente:

more id_rsa.pub

Copiaremos el contenido al portapapeles o a un archivo de texto.

```
root@Ubuntu1:~/.ssh# more id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC84aQodDO2rQRqWo05E/iVOPqSexowdkfpf/05ENF7A5RzPWwVzdJwLjKUiXltVZjv3Q7t6XL/ADR
Vz5gZncGQ+Ks3FQowrp2lfX7wDJj1aX7FmCfaffekGmfHD3sGVMYPv3ak0BmBylB4EAElJmtIoCRDdH5D5qJcjbi17i8Kn5B47VP+CNy1yAqcrdSvdc
AyJTO8E/dzndFq3l7wl9wwg5NnUFxjEdBi/oQQDu8zc+/1wn9rwJlEzAqBhgce/OCSkgit8k4m1ZLhjfWIpJtYx3x2MzB7RsPxMsxlaYSIo7C0siFli
xZpZ2QND3a00j1JDDiQrFHz7l+HlT7SFb0L root@Ubuntu1
```

3.- Dentro de R1, ejecutaremos los siguientes comando.

R1(config)#ip ssh pubkey-chain
R1(conf-ssh-pubkey)#username root
R1(conf-ssh-pubkey-user)#key-string

4.- A continuación ingresaremos el contenido de la llave Pública de "***Ubuntu1***".

R1(conf-ssh-pubkey-data)#$Ck6aMDFu2m5EtkwzgfiB9uwF6+J/5T/ZLgJheWE3IGns
R1(conf-ssh-pubkey-data)#$tkLrbvZIKpkPnD9fpqBKMu7Zrz6Xo9VqRh1p2oTafYqJ
R1(conf-ssh-pubkey-data)#$F3MJ18zoaJm9nhzCSsbgQYFLouXeyVTPzK4QqzrqP9zH
R1(conf-ssh-pubkey-data)#pZgrtCTmDdnTjopddqlcSb39SFfWX3FcxJZ root@Ubuntu1
R1(conf-ssh-pubkey-data)#exit
R1(conf-ssh-pubkey-user)#exit

5.- Crearemos el usuario con el nombre de sistema operativo en este caso "***root***" con "***privilegios 15***" para que permita el acceso a modo privilegiado este no deberá tener alguna contraseña.

R1(config)#username root privilege 15

6.- Crearemos las llaves publicas y privadas en el router

R1(config)#crypto key generate rsa modulus 2048

7.- Realizaremos una ***conexión SSH*** a tráves del cliente.

 # ssh 10.1.1.254

Comandos utililes para esta práctica.

show running-config
copy running-config startup-config
crypto key zeroize rsa
crypto key zeroize pub-key