| **VPN CON WIREGUARD** |
| --- |



Ángel González Martínez

Nicolás Jaraiz Bravo

Rubén Bautista Maya

SMX 2 A

**ÍNDICE**

[**¿QUÉ ES WIREGUARD? 2**](#_yz3q5t9z2mkm)

[Su competencia 2](#_1yoxs8s2rcky)

[**CARACTERÍSTICAS 2**](#_gwgwf3aien10)

[**INSTALACIÓN 2**](#_g7oyxwlzbiwp)

[**CONFIGURACIÓN 3**](#_m1f0h057zowg)

[**FUNCIONAMIENTO 4**](#_nidl8salp3za)

### **¿QUÉ ES WIREGUARD?**

Wireguard es una herramienta de creación de VPNs simples y rápidas que utiliza criptografía de clave pública para realizar el proceso.

Gracias a su simplicidad, Wireguard es muy fácil de configurar y nos permite a nosotros, los usuarios, poder conectarnos de una máquina a otra con SSH, permitiendo así poder conectarse a las máquinas desde otro ordenador y poder editar sus configuraciones.

En Net RNA, queríamos crear una VPN para poder conectarnos al servidor de la planta inferior del centro desde nuestra clase, por lo tanto, creamos una máquina virtual de Isard (Servidor Wireguard), que es con la cual vamos a hacer la conexión al MikroTik (cliente Wireguard).

#### **Su competencia**

Habitualmente, la herramienta clásica de GNU/Linux siempre ha sido OpenVPN, una herramienta modular que, a decir verdad, es bastante completa, y funciona perfectamente, el inconveniente es que resulta ser una herramienta compleja. Wireguard nunca ha aspirado a sustituir a OpenVPN, ni mucho menos, sinó a facilitar la creación de VPNs a aquellos usuarios que dispongan de menos conocimientos técnicos.

### **CARACTERÍSTICAS**

Al utilizar Wireguard, debemos tener presentes las siguientes características:

* Se utiliza UDP como protocolo de transporte de paquetería y mensajes.
* Los equipos con Wireguard deben tener abiertos los puertos UDP y tener una IP visible.
* Se usan claves públicas.
* Wireguard solamente se encarga de mantener el túnel.

### **INSTALACIÓN**

Para poder instalar Wireguard, solamente debemos escribir en el terminal la siguiente orden:

| sudo apt install wireguard-tools |
| --- |

### **CONFIGURACIÓN**

En nuestro caso, hemos editado el archivo de configuración de Wireguard (*/etc/wireguard/wg0.conf*) de tanto el servidor como el cliente en cuestión:

**Servidor** (Máquina de Isard)

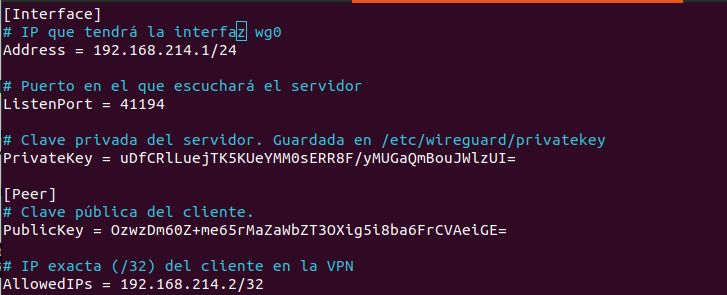
* Clave Pública



* Clave Privada



* Configuración Wireguard



**Cliente** (Smoothoperator55)

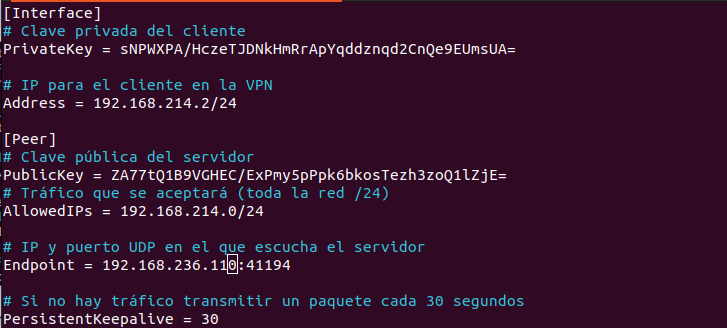
* Clave Pública



* Clave Privada



* Configuración Wireguard



### **FUNCIONAMIENTO**

Wireguard encapsula de manera segura los paquetes IP y los envía a través de UDP. Cuando añadimos una interfaz de Wireguard, y la configuramos de la forma correspondiente con las claves públicas y privadas en sus lugares, la herramienta nos asociará las IP de los clientes y el servidor con sus claves públicas, Wireguard realizará los siguientes pasos para realizar la comunicación entre ambos lados de la VPN:

* Cuando la interfaz envía los paquetes:
  + Observa a qué dirección IP se envía el paquete. Si conoce la dirección, pasa al siguiente paso, si no la conoce, lo *droppea*.
  + Encripta el paquete.
  + Observa cuál es el puerto que tiene asignado para enviar el paquete encriptado.
  + Envía el paquete por el puerto asociado.
* Cuando la interfaz recibe los paquetes:
  + Recibe un paquete por un puerto en concreto y lo desencripta.
  + Observa la IP proveniente del paquete una vez lo desencripta.
  + Si conoce la IP y tiene permitida su comunicación con esta interfaz, acepta el paquete, si no, no *droppea*.

### **RESULTADO**

Tras muchos intentos con variaciones en las direcciones IP y otros parámetros de la configuración de ambos componentes del servidor, no hemos podido conectarlos, y creémos que se debe a que los routers no dejan pasar la conexión del servidor en Isard con el cliente, pero no teníamos tiempo para arreglarlo.

Probamos de montar una VPN en varias ocasiones, en las cuales el servidor se encontraba dentro de la red de la clase, y no dentro de la red de los routers, y la conexión funcionaba correctamente y sin problemas, pero como ya se ha comentado anteriormente, no tuvimos tiempo para permitir el paso del túnel entre los routers.