

## ACTUALIZAR EL SISTEMA

Antes que nada actualizar todos los paquetes de OPNSense yendo a System >> Firmware >> Updates.

## INSTALAR EL PAQUETE

Luego, para instalar WireGuard, vamos a System >> Firmware >> Plugins, buscamos «wireguard» e instalamos el paquete.

Una vez instalado, y para que nos aparezca en el menú, actualizaremos la página en el navegador (F5). Después de refrescarla, deberíamos poder ver el submenú de WireGuard dentro del menú VPN.

## CREAR EL TÚNEL LOCAL

Iremos a VPN >> Wireguard y seleccionaremos la pestaña «Local». Dentro, pincharemos en el símbolo + para crear el nuevo túnel. En la siguiente ventana configuraremos lo siguiente:

- Enabled: Marcado.
- Nombre: WireGuard.
- Listen Port: 51820.
- Tunnel Address: 192.168.255.0/24.

...y guardamos los cambios.

## ACTIVAR WIREGUARD

Iremos a VPN >> Wireguard >> Pestaña «General», marcaremos «Enable Wireguard» y aplicaremos los cambios.

## CREAR LA INTERFAZ

Iremos a Interfaces >> Assignments y pincharemos en el símbolo + que aparece a la derecha de la interfaz wg1. Tendremos que seleccionar el nombre OPT\* que nos salga disponible para esa interfaz.

En la siguiente ventana marcaremos «Enable Interface», «Prevent interface removal», asignaremos la descripción «WG» y salvaremos los cambios.

## CREAR LA REGLA WAN

Iremos a Firewall >> Rules >> WAN y agregaremos una regla con la siguiente configuración:

- Protocolo: UDP.
- Destination: WAN address.
- Destination port range: From other 51820 To other 51820.
- Description: Allow wg in.

## CREAR LA REGLA WG

Iremos a Firewall >> Rules >> WG y agregaremos una regla con la siguiente configuración:

- Action: Pass.

- Direction: in.
- Protocol: any.
- Source: any.
- Destination: any.
- Destination port range: From any To any.
- Description: Allow all in

Y salvaremos los cambios.

## CONFIGURAR USUARIOS

Los usuarios o pares (peers) son los dispositivos a los que vamos a permitir el acceso al túnel que creamos arriba. Si queremos una red bien securizada y fácil de loguear, deberemos crear un peer por cada dispositivo que se conecte, restringiendo su máscara a /32, para que ese dispositivo sólo pueda usar la única IP reservada para él, y ninguna otra más. Sin embargo, por motivos de comodidad, es posible que abramos su máscara de forma que pueda ser usado por varios dispositivos, asignándoles a cada uno, una IP dentro de las IPs posibles que la máscara abierta le permita.

Es decir, que, por ejemplo, si asignamos como IPs posibles a un peer la subred 192.168.255.128/25, la cuenta de ese peer podrá ser usada desde 126 dispositivos, asignándole a cada uno de ellos una IP en el rango de 192.168.255.129 a 192.168.255.254. Pero, como digo más arriba, no es la mejor de las prácticas.

Entonces, entendiendo esto, crearemos en cada dispositivo que queramos conectar al túnel de OPNSense, «la otra boca del túnel». Y para lograrlo instalaremos y utilizaremos la aplicación WireGuard en cada uno de ellos. Una vez instalada crearemos un nuevo túnel, de forma manual, en cada uno de ellos, y lo rellenaremos con el siguiente contenido:

- Nombre: wg
- Clave privada: Le damos a auto-generar.
- Clave pública: Se auto-genera al crear la clave privada. (Tomamos nota para meterla como endpoint en el OPNSense).
- Direcciones: La IP que queremos dar a este nuevo dispositivo, en la subred definida en la interfaz wg1 pero con máscara /24.
- Servidores DNS: El que más te apetezca (Desde Europa, y públicos, mejor 9.9.9.9 y 149.112.112.112).

Por ejemplo:

- Nombre: wg.
- Clave privada: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.
- Clave pública: sjHT3e5OxtnNNjnTSV2ePwEacUDWAav6LL8ZvZpG6aH.
- Direcciones: 192.168.255.10/24.
- Servidores DNS: 9.9.9.9, 149.112.112.112.

Esto nos habrá creado el nuevo túnel en ese nuevo dispositivo. Pero ahora deberemos decirle a ese túnel recién creado cual será la otra boca por donde salir. Y para ello, lógicamente, deberemos crear, también en ese nuevo dispositivo, un peer que no será otro que nuestro OPNSense. Entonces, añadiremos un par (peer) con los siguientes datos:

- Clave pública: La clave pública del OPNSense (VPN >> WireGuard >> «Pestaña local» >> Editar...).
- Punto final: La IP y puerto (O dominio y puerto) por donde se accederá al OPNsense).
- IPs Permitidas: 0.0.0.0/0 (Para routear todo el tráfico) o la subred que te apetezca que sea routeada mediante el túnel).

Por ejemplo:

- Clave pública: 4n3aW5QextnNNJnTSV2ePwEacUDWAav6LL8ZvZpG6aH
- Punto final: 88.87.23.233:51820 o negrocubanito.com:12345.
- IPs Permitidas: 0.0.0.0/0 o 10.0.0.0/8 o 172.16.0.0/16 o 192.168.0.0/24

Entonces, esto nos dejará el dispositivo su boca propia del túnel configurada y con la otra boca (que es nuestro OPNSense, también configurada). Sólo nos falta crear un endpoint para ese dispositivo en el propio OPNSense. Para ello vamos a VPN >> WireGuard, pestaña «Endpoints» y creamos uno con los siguientes datos:

- Name: Nombre del dispositivo.
- Public Key: La clave pública de la boca del túnel del propio dispositivo.
- Allowed IPs: La IP individual que el dispositivo utilizará en la subred del tunel del OPNSense. Normalmente un /32.

Por ejemplo:

- Name: CelularDePedro.
- Public Key: sjHT3e5OxtnNNJnTSV2ePwEacUDWAav6LL8ZvZpG6aH.
- Allowed IPs: 192.168.255.10/32.

## AGREGAR EL ENDPOINT AL TÚNEL LOCAL

Vamos a VPN >> Wireguard >> «Pestaña Local» >> Editar wg1 y Agregamos el Endpoint que acabamos de crear (CelularDePedro).

## REINICIAR WIREGUARD

Para poder efectivamente conectarnos al túnel, primero deberemos reiniciar WireGuard en OPNSense. Para ello vamos a VPN >> Wireguard >> «Pestaña General», desactivamos WireGuard y salvamos los cambios. Inmediatamente hacemos lo opuesto. Es decir, activamos y salvamos los cambios.

A partir de ese momento, ya nos podremos conectar a OPNSense desde el «CelularDePedro» y podremos acceder a toda la subred 192.168.255.0/24.

