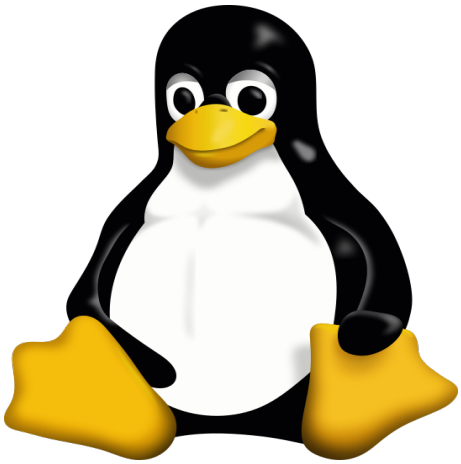

Bootcamp Especialidad GNU/Linux (2023)

Lab 11 - Creación de túneles PPTP con Wireguard

Pedro Antonio Mayorgas Parejo

10 de septiembre de 2023

Índice

1. Topología

Tenemos la siguiente topología, donde tenemos conectados a través de un switch de L2, dos pfsense que hacen de doble funcionalidad, de router y de firewall. Así como a los host finales que consisten en un

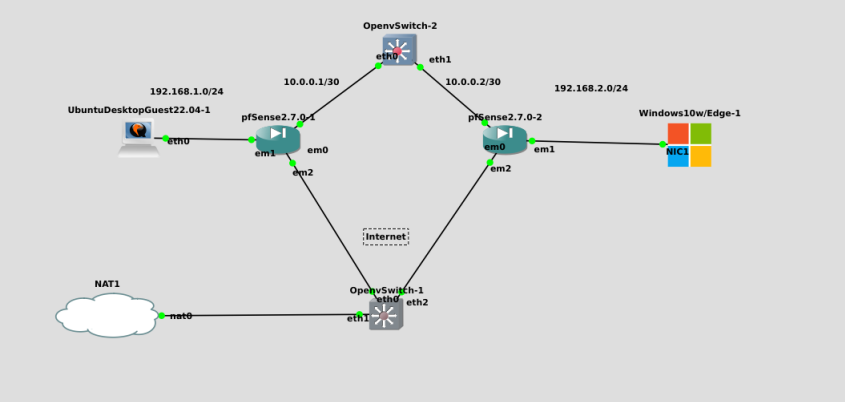

Figura 1: Topología de red

De la topología además podemos ver las direcciones de red, las cuales son sencillas de seguir. Como punto importante, la conexión se realiza a través de la red 10.0.0.0/30, aunque se puede hacer por la otra que será marcada por el router como OPT1, que es la que permite que nuestro pfsense pueda instalar las utilidades necesarias para poder usar Wireguard.

OPT1, se ha configurado con DHCP y DNS, para poder instalar Wireguard, como la instalación y configuración de interfaces conectadas a Internet está fuera de este manual no se dará más importancia más allá de que es una red de management la conectada por OPT1.

2. Configuración de WAN y toma de contacto con Pfsense

Bueno el sistema es un router/firewall, el cual nos permite varias ventajas y además podemos evolucionarlo a través de paquetes como UTM. Bueno la pantalla principal se nos presenta como la siguiente:

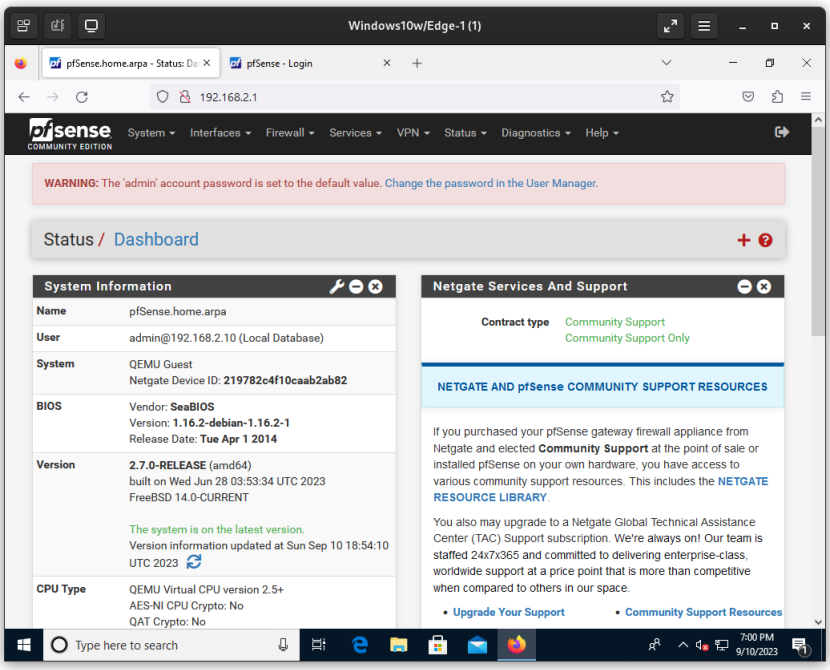

Figura 2: Interfaz de Pfsense

Lo primero que debemos configurar son las interfaces de red básicas, porque si recordamos que tiene 3 dos de ellas las asigna automáticamente como WAN y LAN, en concreto las 2 primeras respectivamente, el router/firewall durante su instalación proveerá por defecto de una LAN 192.168.1.0/24 a todos los routers sin excepción, en mi caso como necesitamos enrutar redes privadas por PPTP de Wireguard, necesitamos que las redes sean distintas, en ese caso el segundo router/firewall DEBE tener otra subred privada diferente, esto es para poder generar unas rutas estáticas que nos permite enrutar paquetes que tengan como destino la red privada conectada.

Ahora la WAN debe configurarse como dirección IP estática, normalmente está todo preparado para que puedas usar DHCP para que tu proveedor de servicios o un router neutro que haga de bridge te de una dirección IP. Para ello tenemos que ir a **Interfaces ->WAN**, nos mostrará una ventana como va a aparecer en al siguiente captura, donde nos tenemos que concentrar es en:

1. IPv4 Configuration Type ->Static IPv4; Esto es para que la configuración la realicemos nosostros.

2. IPv4 Configuaration - Aparecerá una caja nueva que nos indicará los siguientes campos:
   a) IPv4 Address - Redes de máscara CIDR (Classless Inter Domain Routing) 30 - 255.255.255.252
      - 10.0.0.1 - Para el router firewall conectado a Ubuntu.
      - 10.0.0.2 - Para el router firewall conectado a Windows.
   b) IPv4 Upstream GW ->Podemos usarlo si queremos utilizar la ruta directa sin seguridad, pero como vamos a establecer un Tunel punto a punto cifrado, lo dejamos en blanco.

Una vez terminada la configuración de arriba, almacenamos las respectivas configuraciones pulsando Save.

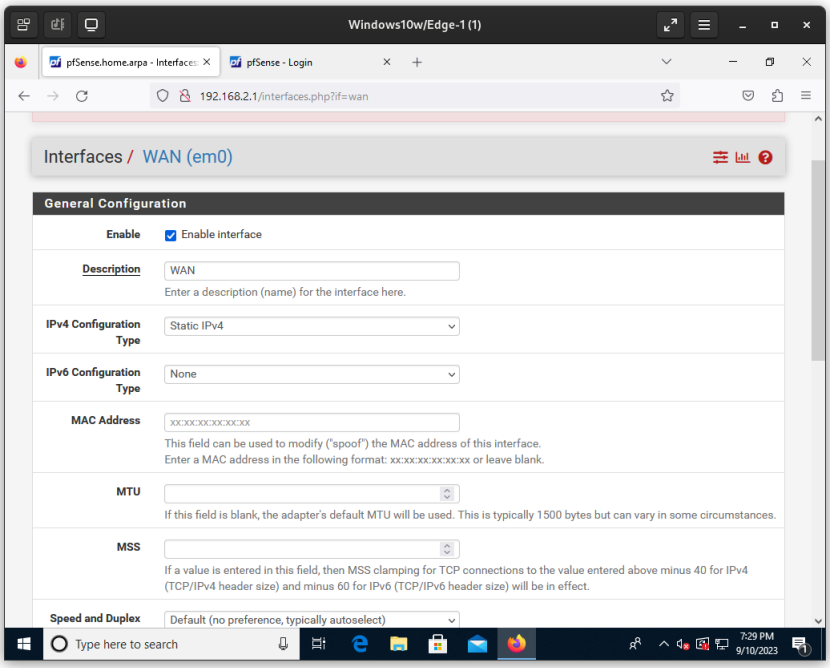

Figura 3: Configuración de WAN

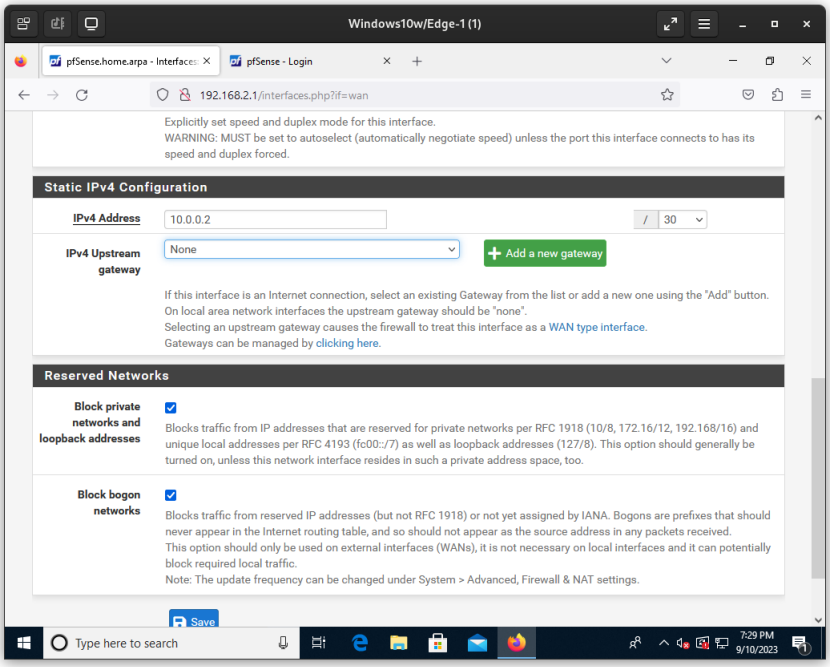

Figura 4: Configuración de WAN - parte 2

En el otro router firewall, seguimos básicamente los mismos pasos, pero cambiando la IP.

3. Configuración de Wireguard

Ahora debemos configurar Wireguard, para ello nos vamos a **VPN ->Wireguard**, luego una vez dentro tenemos que añadir un tunel en cada router/firewall. Tenemos que introducir los siguientes campos del formulario:

1. Marcar el checkbox de *Enable Tunnel*.
2. Introducir una descripción: en mi caso ponemos OFFICE1_PPTP o OFFICE2_PPTP.
3. Listen Port - Podemos cambiarlo a otro que no sea el por defecto por seguridad y ofuscación. Pero para el objetivo de este manual, lo dejamos en el por defecto de Wireguard el **UDP - 51820**.
4. Interface Keys: Aquí tenemos que generar nuevas claves pulsando el botón de la derecha y DEBEMOS guardar bien la clave pública, la privada la dejamos sin tocar y solo debe saberla el router/firewall.

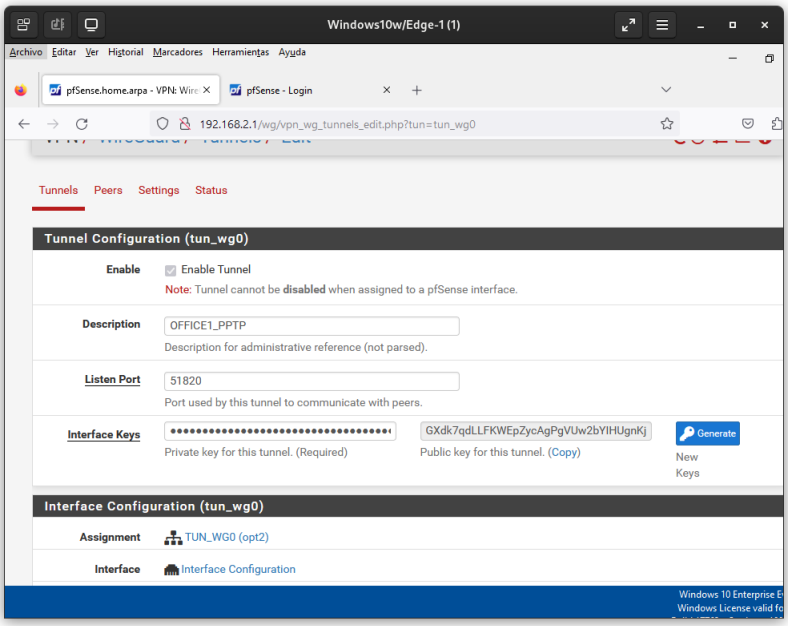

Figura 5: Configuración del tunel de Wireguard

Una vez realizada la configuración debemos pulsar guardar y tras lo cual debemos activar el servicio de Wireguard en Settings, luego tenemos que volver al mismo tunel para permitir la asignación de la interfaz propia, es decir la dirección IP del tunel junto a su máscara. en tal caso debemos activar esa interfaz a tráves del menú de interfaces y asignarla.

Tenemos que poner los siguientes cambios:

1. IPv4 Configuration Type ->Static IPv4; Esto es para que la configuración la realicemos nosostros.

2. IPv4 Configuaration - Aparecerá una caja nueva que nos indicará los siguientes campos:

   a) IPv4 Address - Redes de máscara CIDR (Classless Inter Domain Routing) 30 - 255.255.255.252

      - 172.16.0.1- Para el router firewall conectado a Ubuntu.
      - 172.16.0.2 - Para el router firewall conectado a Windows.

   b) IPv4 Upstream GW - Aquí inicializamos como puerta la dirección del otro router, esto es importante porque a pesar de su nombre, te permite crear una ruta estática hacia la otra subred privada donde estén conectados los host y servicios de otra oficina. Para crearlo debemos pulsar new Gateway que nos hará un nuevo formulario.

      - 172.16.0.2- Para el router firewall conectado a Ubuntu.
      - 172.16.0.1 - Para el router firewall conectado a Windows.

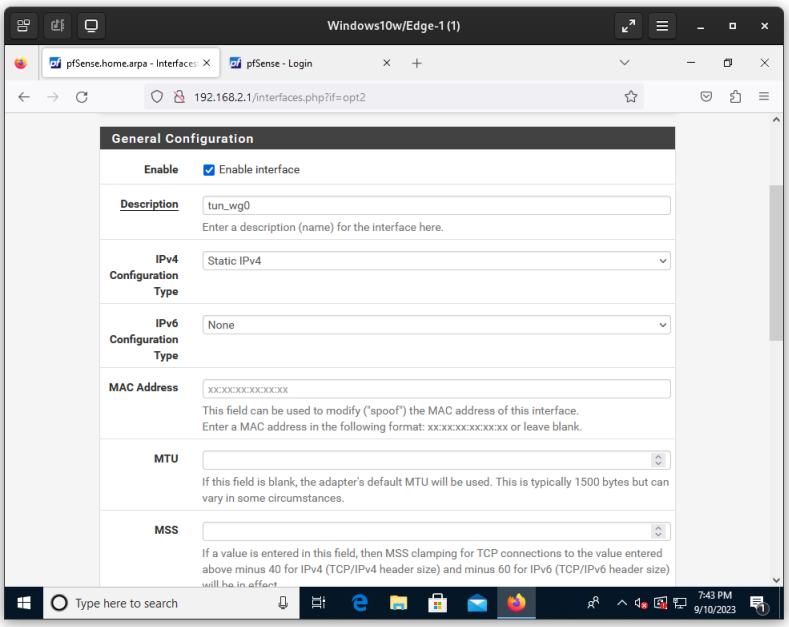

Figura 6: Configuración de la interfaz del tunel parte 1

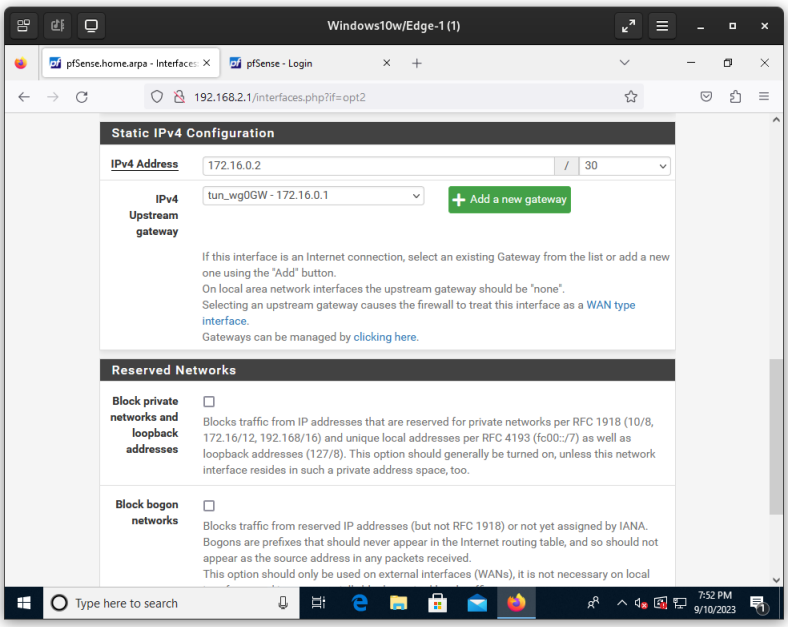

Figura 7: Configuración de la interfaz del tunel parte 2

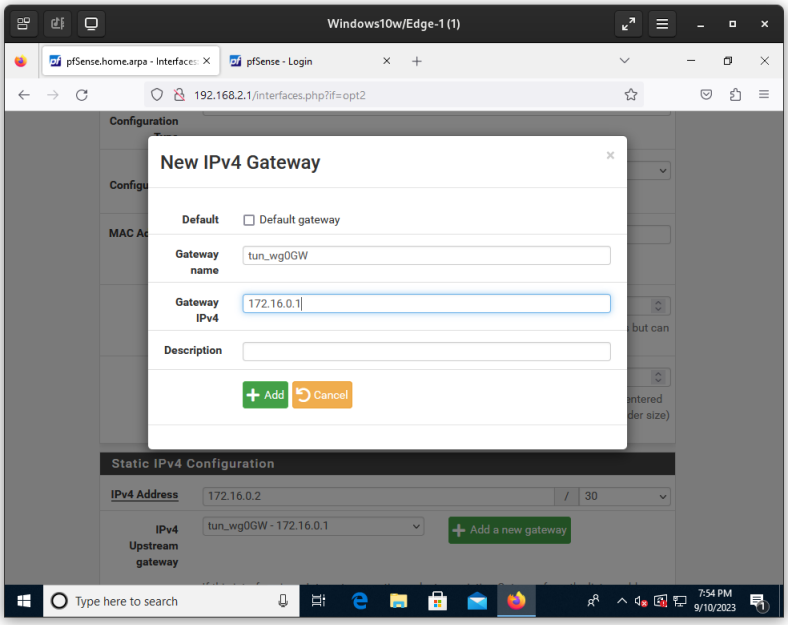

Figura 8: Configuración de la interfaz del tunel parte 3 - Creación del Gateway

4. Creación de los Peer

Ahora una vez creadas las interfaces tenemos que irnos al mismo lugar donde creamos los túneles y crear un nuevo peer, para ello debemos pulsar en Add Peer que es el icono que aparece a la derecha del tunel.

1. Enable Peer - Lo marcamos.
2. Tunnel - seleccionamos el tunel con el que queramos asociar el peer, en nuestro caso es wg0.
   a) Dynamic Endpoint, lo desmarcamos porque conocemos los detalles del peer, es decir esto se suele utilizar como VPN estándar donde los clientes se conectan desde distintos puntos de Internet. En este caso nos aparecerán dos cuadros de texto.
      - Endpoint - IPv4 - Introducimos la IP WAN de los routers, es decir si estamos en el router de Ubuntu, tenemos que poner la de Windows, porque es nuestro par que se conecta a ese tunel.
      - Endpoint port - Introducimos el puerto que corresponda. si lo hemos cambiando.

   b) KeepAlive - 1s. Es el intérvalo de los paquetes que se envían apra indicar que se mantenga la conexión abierta.

   c) Public Key - Pegamos aquí la clave pública del tunel del peer.

   d) Address Configuration - Aquí indicamos qué redes son alcanzables desde este túnel.
      - 192.168.1.0/24 - Para conectar desde el router windows a Ubuntu.
      - 192.168.2.0/24 - Para conectar desde el router Ubuntu a Windows.
      - 172.16.0.1/32 - Para permitir la conectividad de IP del tunel desde windows a Ubuntu.
      - 172.16.0.2/32 - Para permitir la conectividad de IP del tunel desde Ubuntu a Windows.

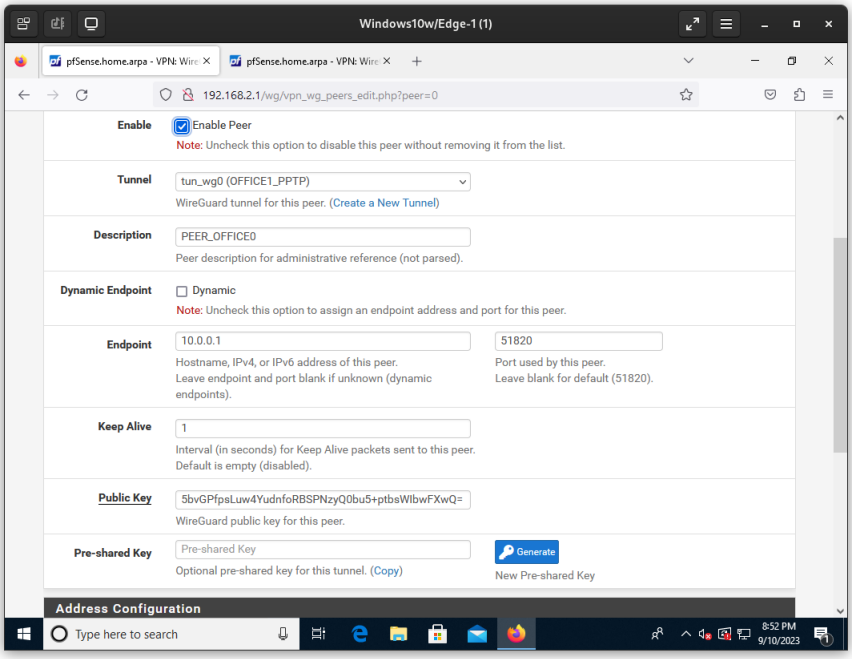

Figura 9: Configuración del peer - De router Windows a Ubuntu

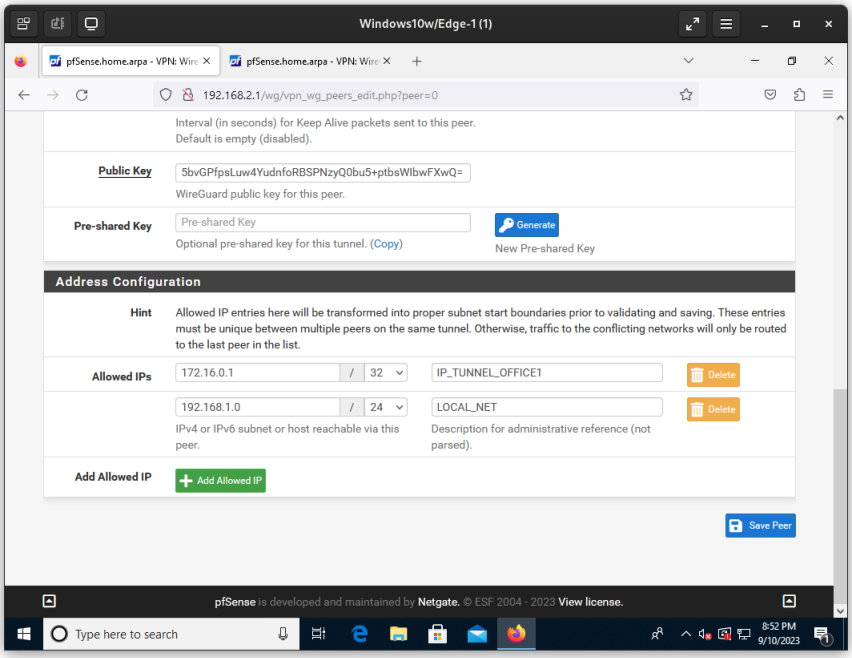

Figura 10: Configuración del peer - De router Windows a Ubuntu - Direcciones enrutables

Ahora una vez creados los peer para los túneles, podemos ver en el estado que no se conectan, esto es porque necesitamos en la interfaz WAN una regla de firewall que permita las conexiones entrantes hacia el puerto UDP de Wireguard. las reglas son como siguen:

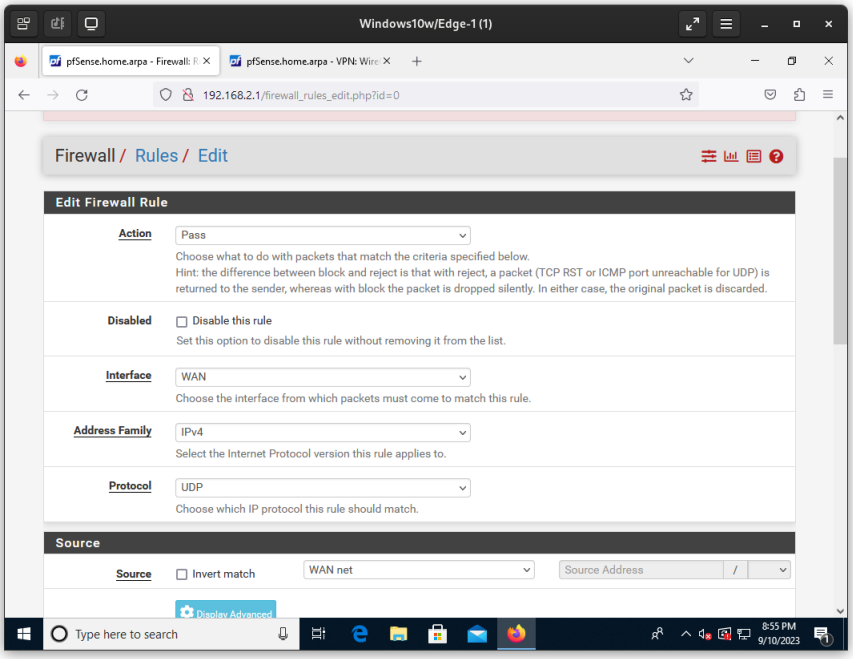

Figura 11: Configuración de las reglas de Firewall

De estas reglas debemos tener en cuenta, que como Source debemos poner la red de la WAN, es decir toda la máscara de subred de la WAN se acepta, luego como destino tenemos que poner a este firewall. Finalmente ponemos el rango de puertos de destino con el servicio de Wireguard, el de origen es efímero.

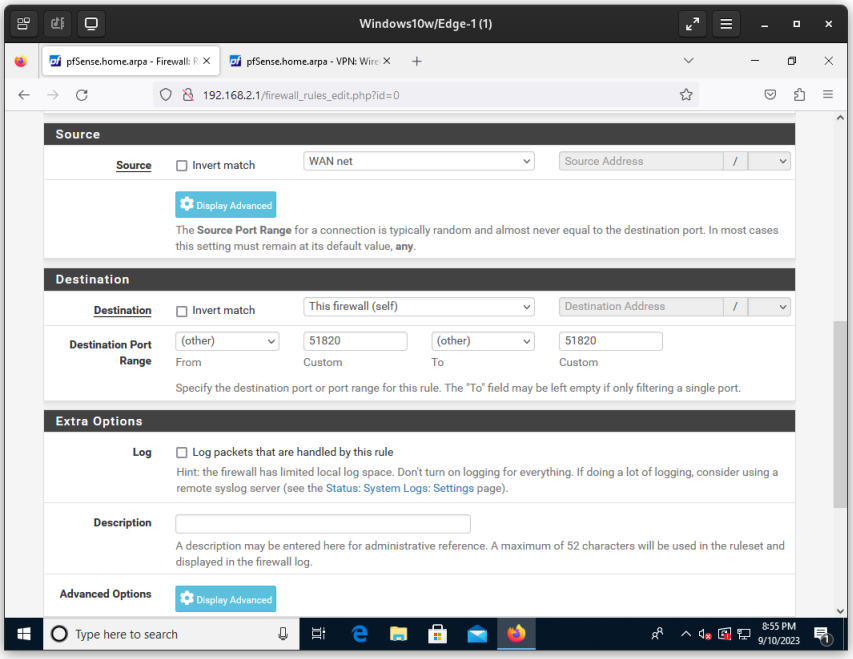

Figura 12: Configuración de las reglas de Firewall - Parte 2

Ahora una vez que se han configurado y guardado las reglas de Firewall, podemos comprobar que la conectividad se ha realizado, porque ha cambiado la fecha del último handshake o si está conectad actualmente aparecerá en verde el handshake.

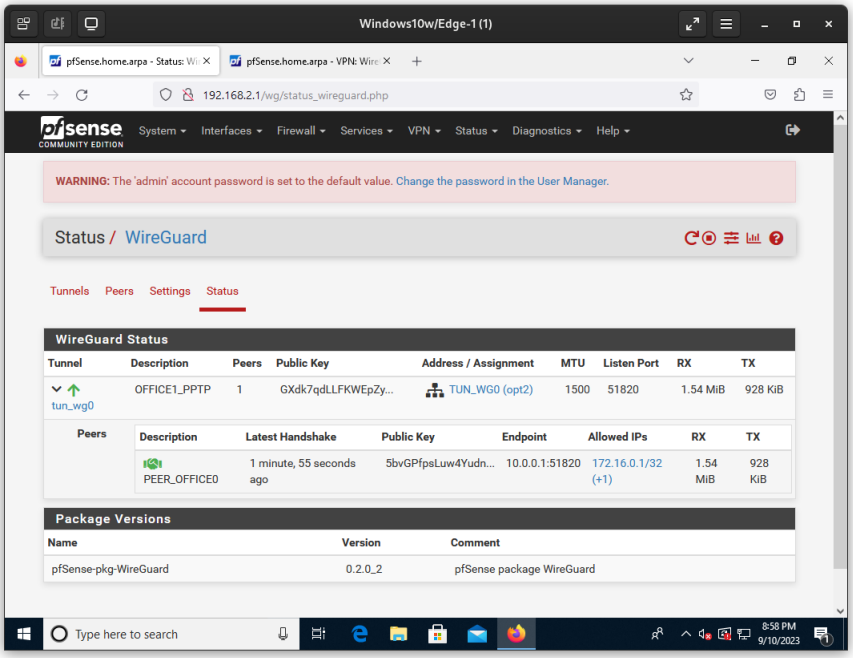

Figura 13: handshake realizado

5. Configuración de ruta estática y prueba

Por último tenemos que poner una ruta estática para poder llegar a la red privada al otro lado del tunel. Para ello tenemos que crear una ruta por el Gateway creado por el tunel anteriormente, para ello vamos a System ->Routing ->Static Routes. Creamos una nueva con la siguiente configuración.

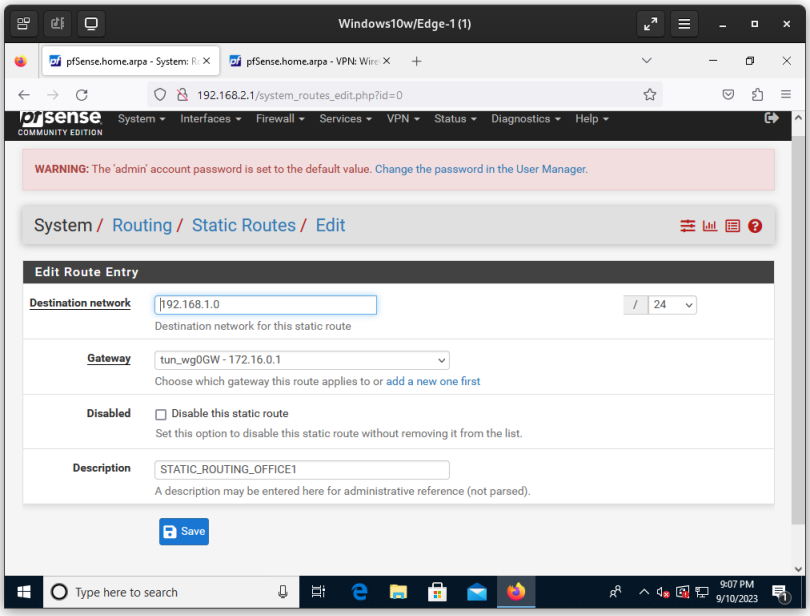

Figura 14: Configuración de ruta estática

En el caso de que sea la red de ubuntu, tenemos que poner 192.168.2.0.

Como prueba se accede al otro router firewall con la IP privada de su red local. Se puede ver que accede a través del tunel porque pone la IP de acceso a la izquierda en User admin@172.16.0.2 que es la IP del tunel del equipo de Windows.

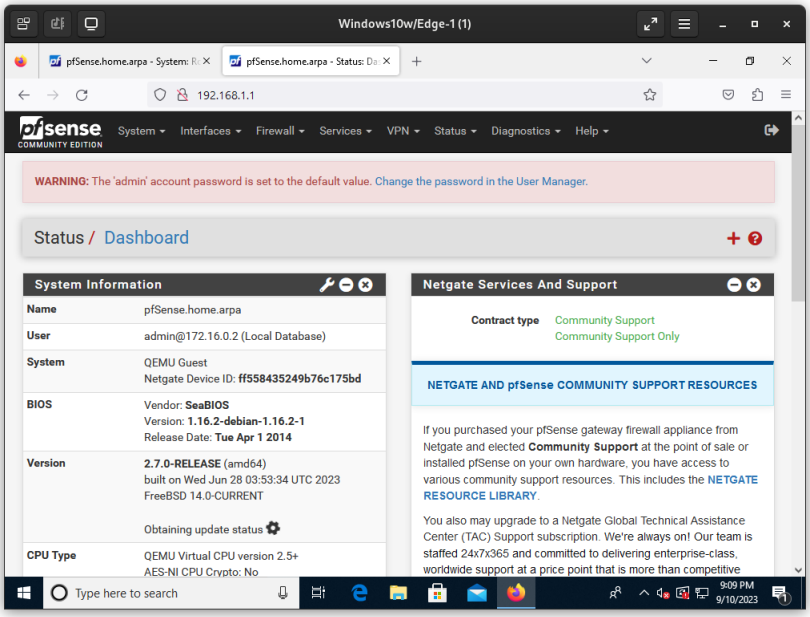

Figura 15: Prueba