

2018

# Práctica VPN pfSense

Ana M<sup>a</sup> Cuenca Hoyo  
María Moreno Muñoz



## Contenido

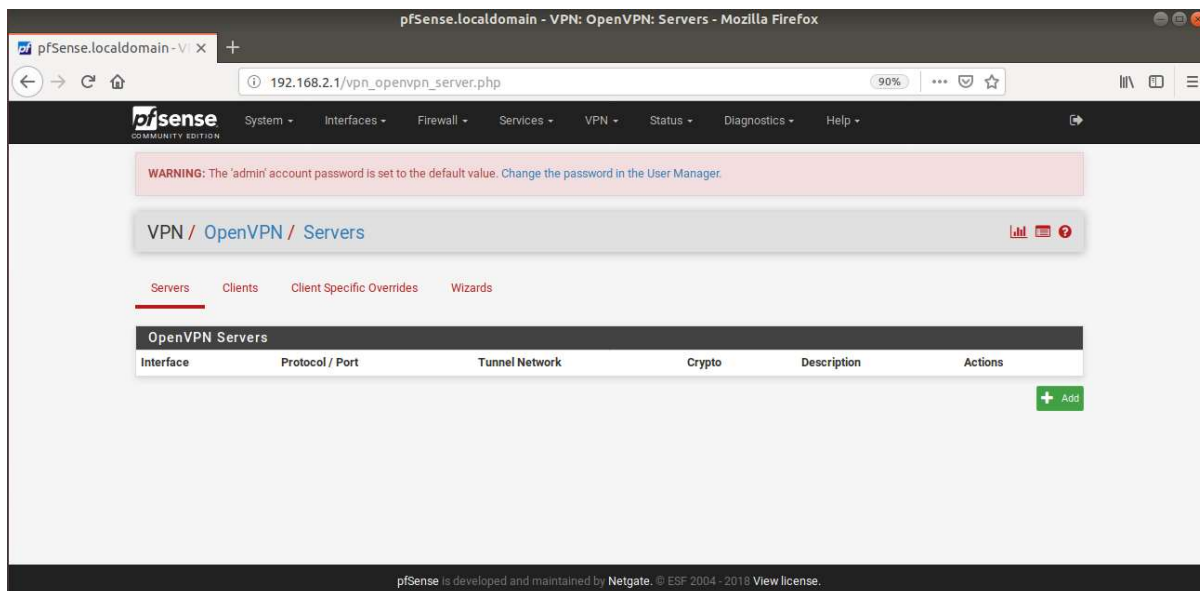
Práctica VPN pfSense .....	2
Servidor .....	2
Configuración del servidor .....	2
Comprobaciones servidor .....	8
Cliente .....	9
Configuración del cliente .....	9
Comprobaciones cliente .....	12

## Práctica VPN pfSense

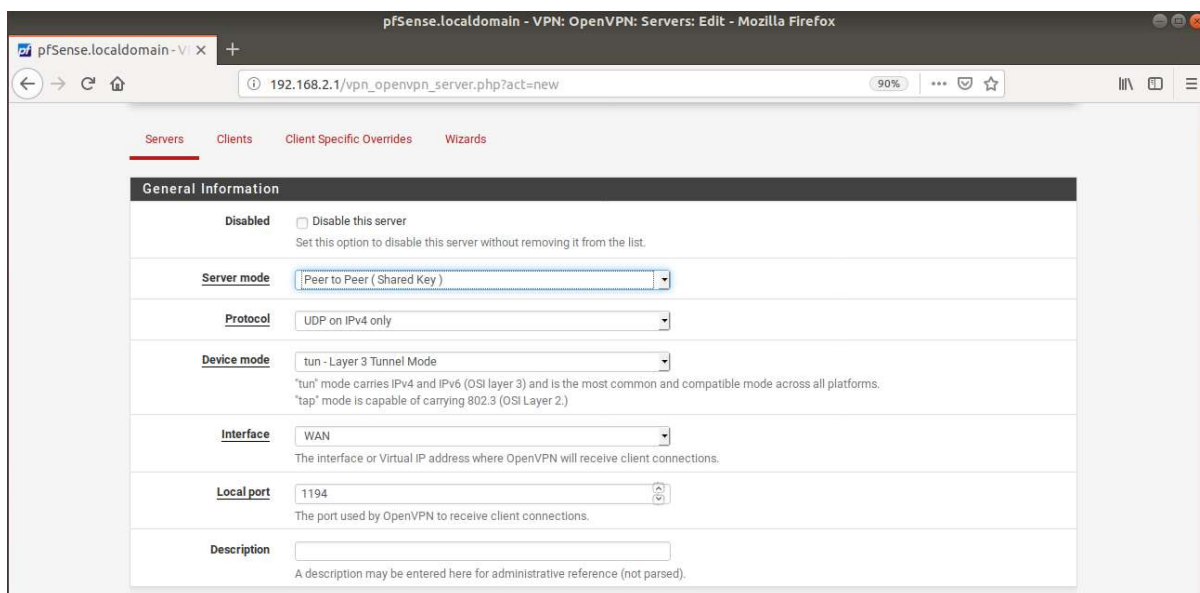
### Servidor

#### Configuración del servidor

Lo primero que tenemos que hacer es irnos al apartado *VPN* → *OpenVPN* → *Servers*. Y una vez estemos en dicho apartado hacemos click sobre el botón *Add* para añadir una nueva conexión.



Las opciones de la nueva conexión tendrán que ser: *Server mode: Peer to peer (shared key)* con esta opción haremos que para poder establecer una nueva conexión el cliente tenga que introducir la clave generada por el servidor. Y lo demás lo dejaremos por defecto porque en este caso esta conexión se realizará mediante la tarjeta WAN.



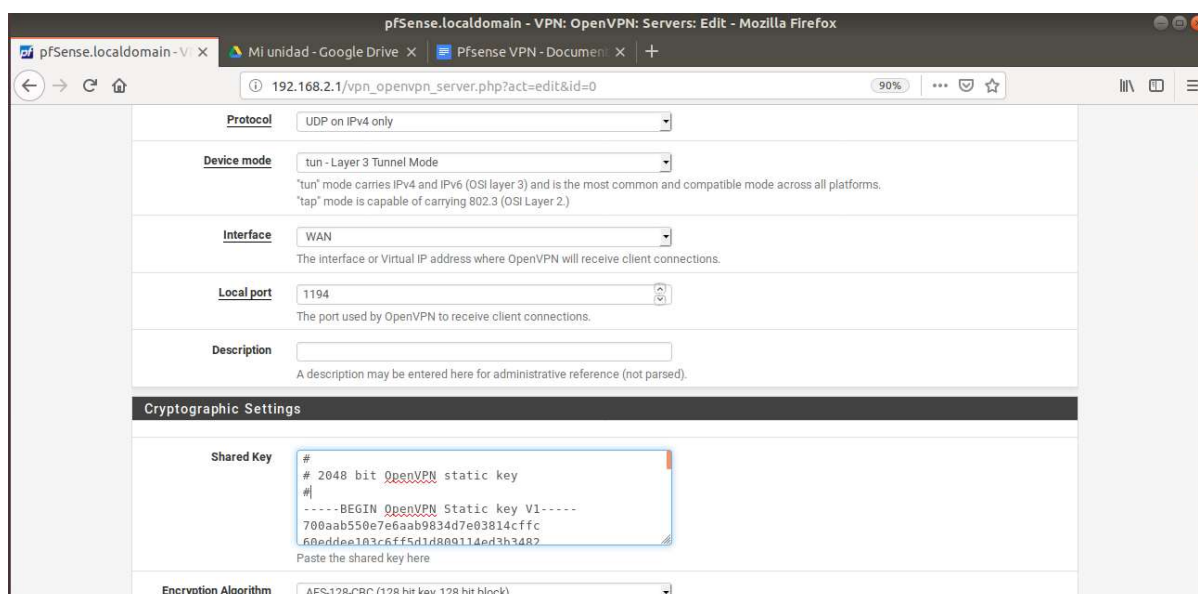
También marcaremos la opción *Shared key* para que se genere la clave automáticamente. Ésta es necesaria para que el cliente pueda establecer la conexión.

The screenshot shows the 'Cryptographic Settings' tab in the pfSense OpenVPN Server configuration. The 'Shared key' section has the checkbox 'Automatically generate a shared key' checked. The 'Encryption Algorithm' dropdown is set to 'AES-128-CBC (128 bit key, 128 bit block)'. The 'Enable NCP' section has the checkbox 'Enable Negotiable Cryptographic Parameters' checked. The 'NCP Algorithms' section shows a list of available algorithms on the left and a list of allowed algorithms on the right, which currently contains 'AES-128-GCM'. The 'Auth digest algorithm' dropdown is set to 'SHA256 (256-bit)'.

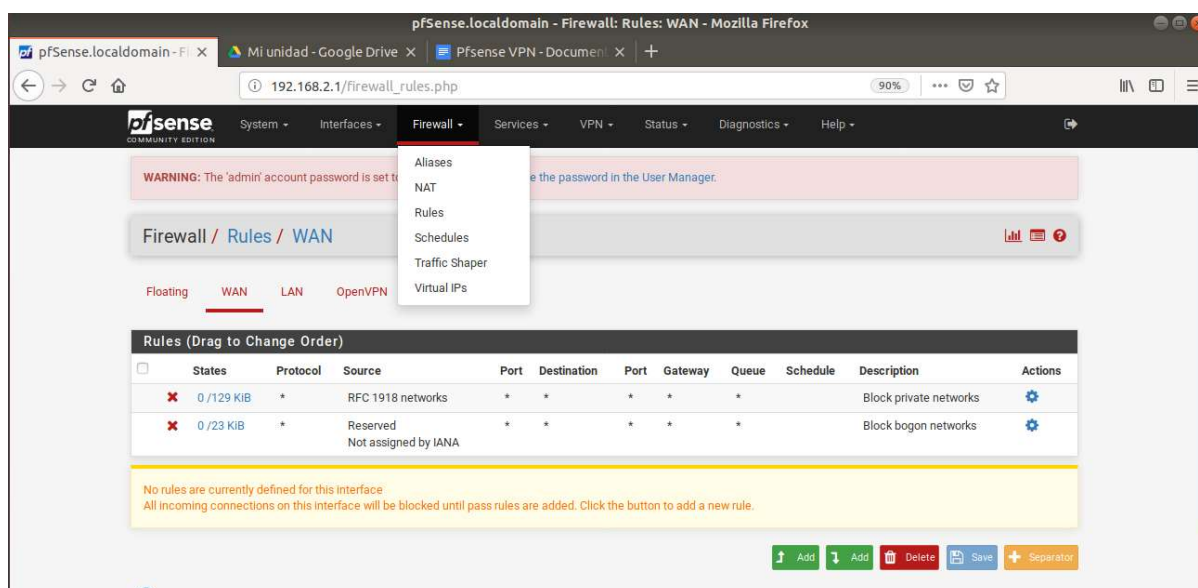
Definiremos la red del túnel, y la red a la que queremos acceder. Hecho todo esto guardaremos los cambios.

The screenshot shows the 'Tunnel Settings' tab in the pfSense OpenVPN Server configuration. The 'IPv4 Tunnel Network' field is set to '192.168.112.0/24'. The 'IPv6 Tunnel Network' field is empty. The 'IPv4 Remote network(s)' field is set to '192.168.1.0/24'. The 'IPv6 Remote network(s)' field is empty. The 'Concurrent connections' field is set to '1'. The 'Compression' dropdown is set to 'Disable Compression, retain compression packet framing [compress]'.

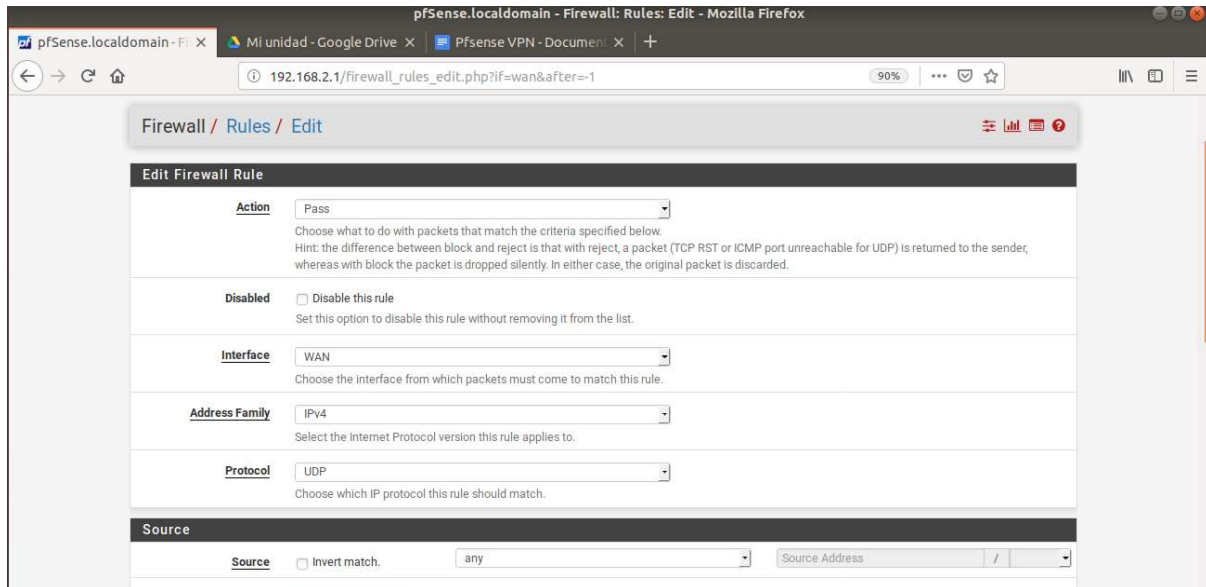
Ahora copiaremos la clave que se ha generado, y se la pasaremos a nuestro compañero.



Hecho todo esto nos iremos a *Firewall* → *Rules*. Y añadiremos una nueva regla.



Definiremos la acción de la regla como *Pass*, la interfaz a la que se le aplicará, y el tipo de protocolo.



Firewall / Rules / Edit

**Edit Firewall Rule**

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** WAN  
Choose the interface from which packets must come to match this rule.

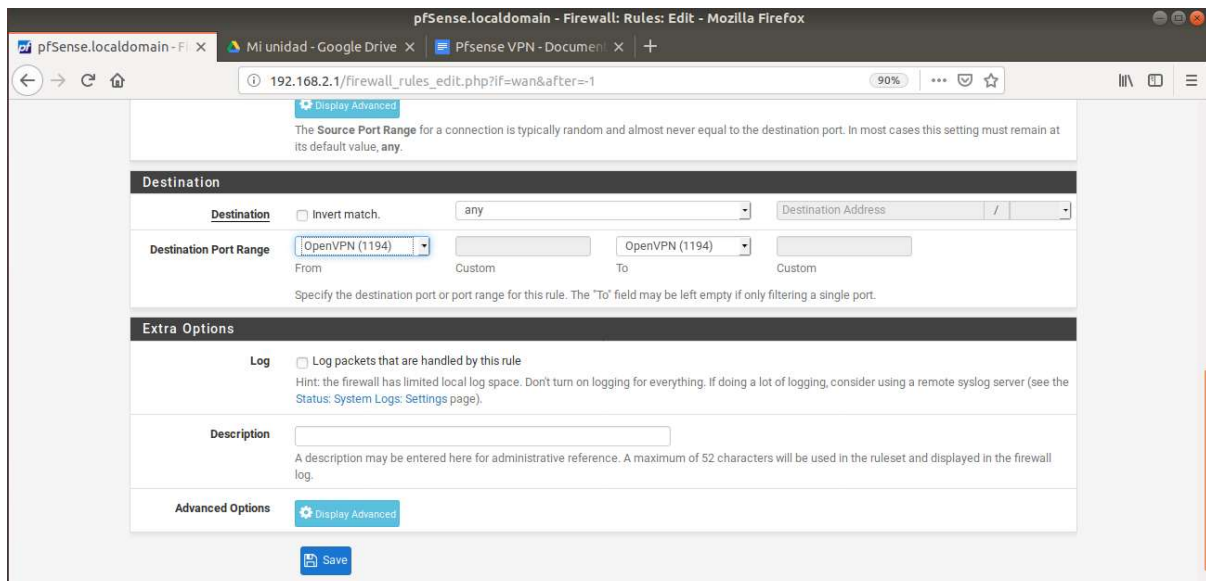
**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** UDP  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match. any Source Address /

Después elegiremos *OpenVPN* como puerto de destino. Y guardaremos los cambios.



Display Advanced  
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

**Destination**

**Destination** ☐ Invert match. any Destination Address /

**Destination Port Range** OpenVPN (1194) Custom To OpenVPN (1194) Custom  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

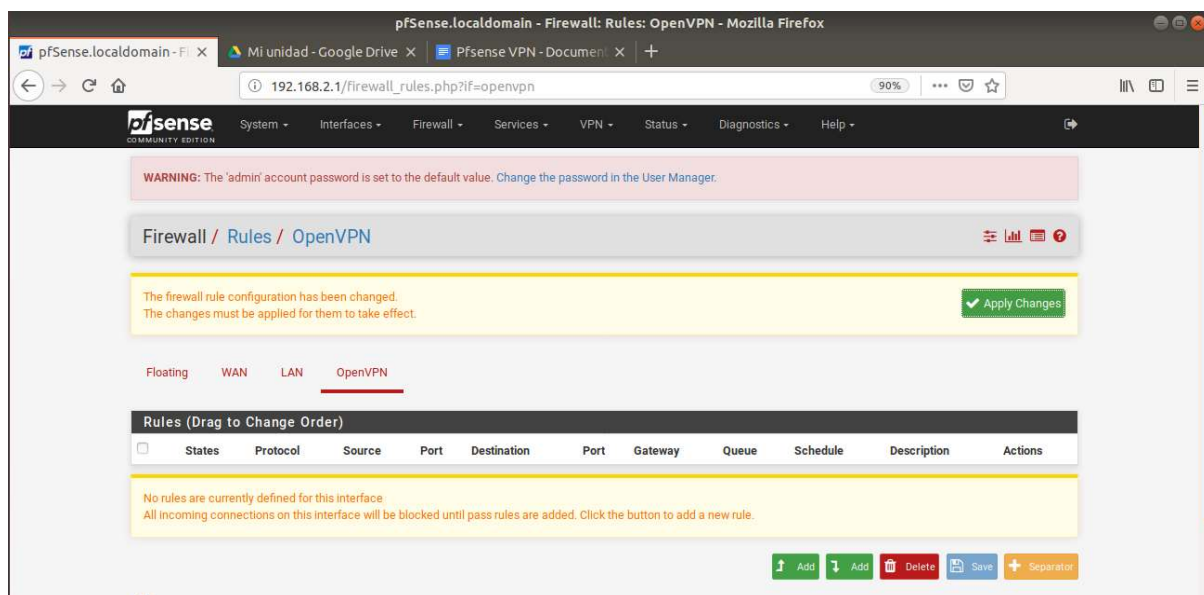
**Log** ☒ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description**  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

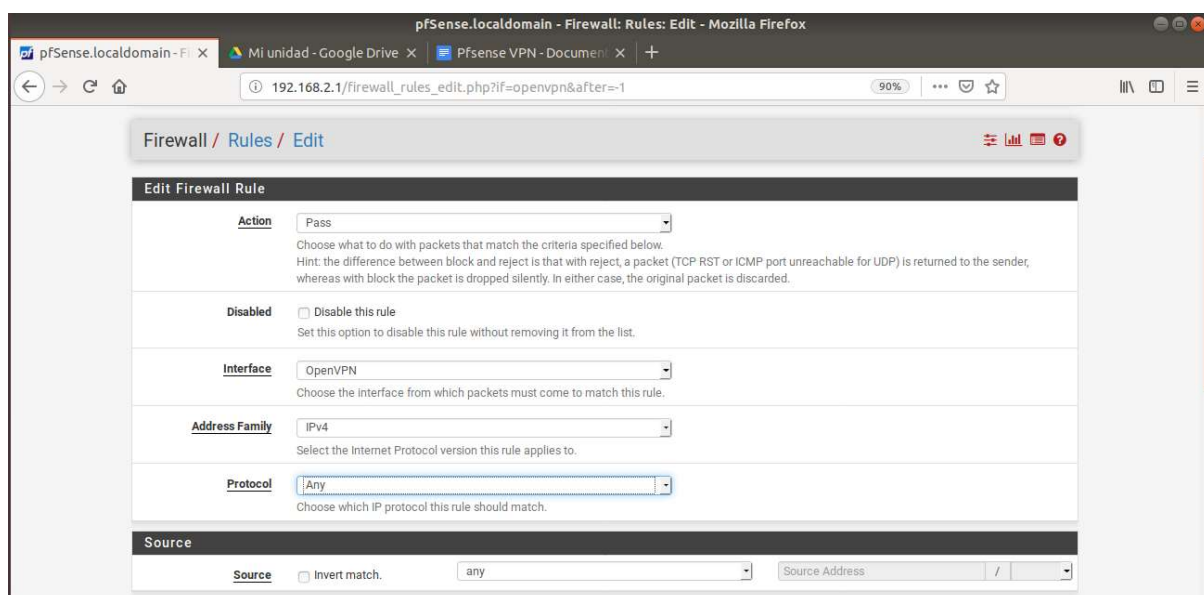
**Advanced Options** Display Advanced

Save

Hecho esto nos iremos a la opción *OpenVPN*, y añadiremos una nueva regla.

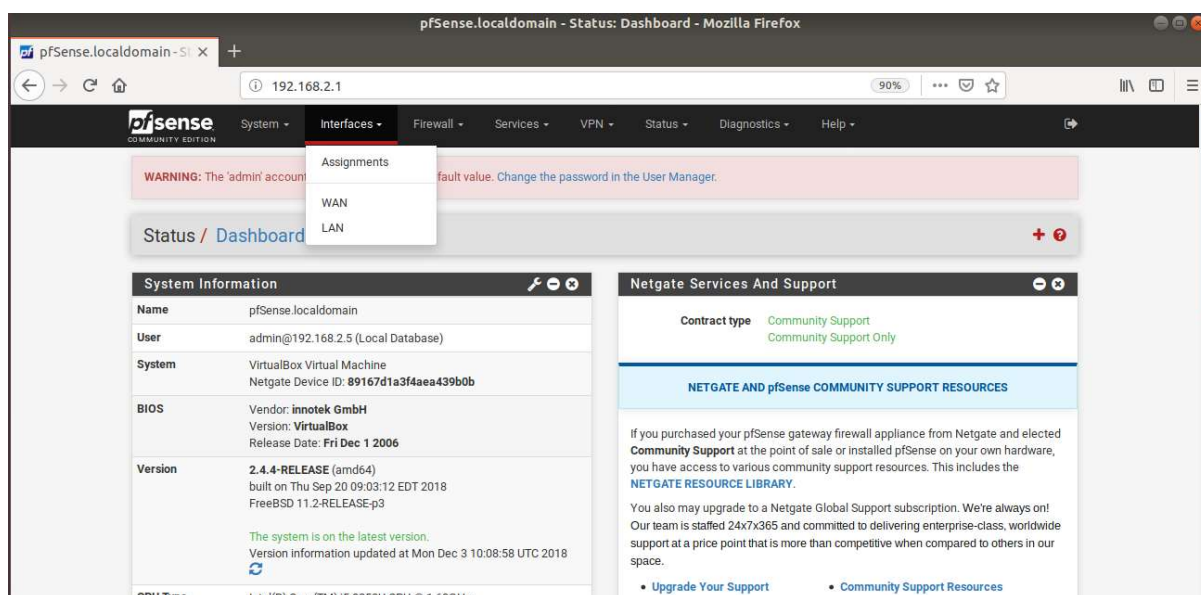


La acción al igual que antes también la dejaremos como Pass, la interfaz será *OpenVPN*, y el tipo de protocolo será cualquiera.

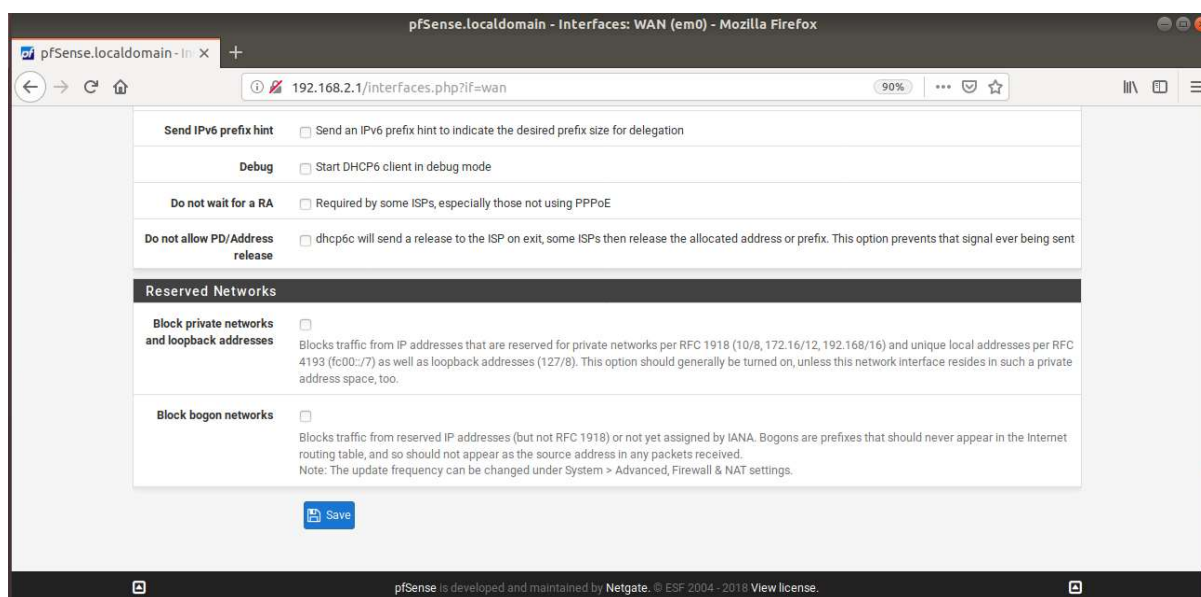




Antes de seguir tendremos que quitar las reglas que vienen definidas por defecto en la tarjeta WAN. Para ellos nos iremos a *Interfaces* → *WAN*.



Para desactivar las reglas tan solo tendremos que desmarcar las casillas de las mismas.

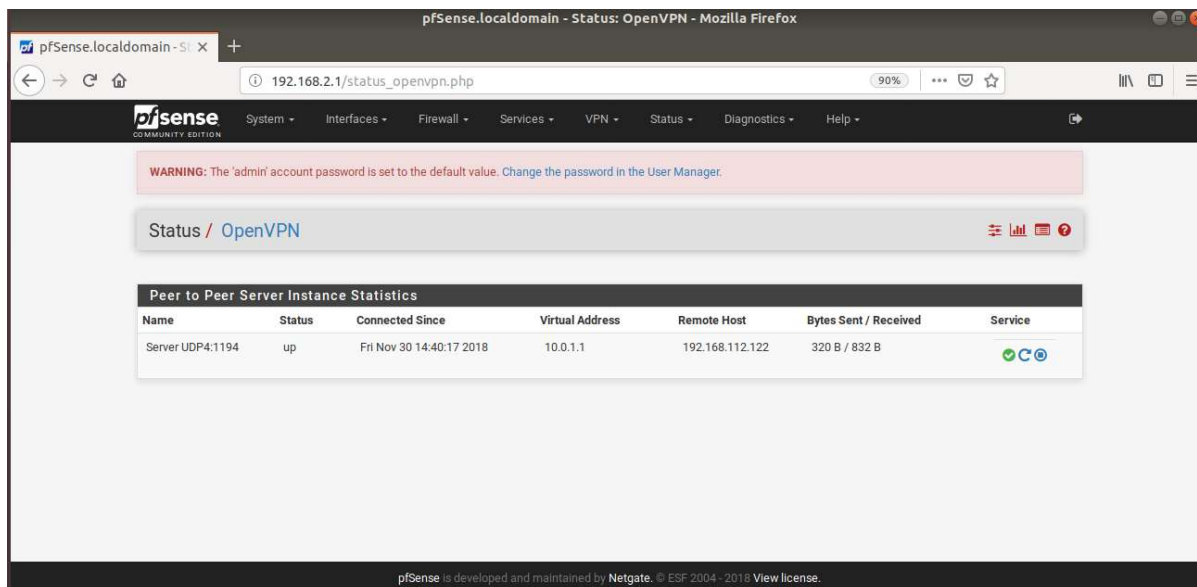




## Comprobaciones servidor

Ya tan solo nos quedaría irnos a *Status* → *OpenVPN*.

Y como podemos observar si hemos realizado bien la configuración nos aparecerá que el estado de la conexión es up, es decir, que está activa.



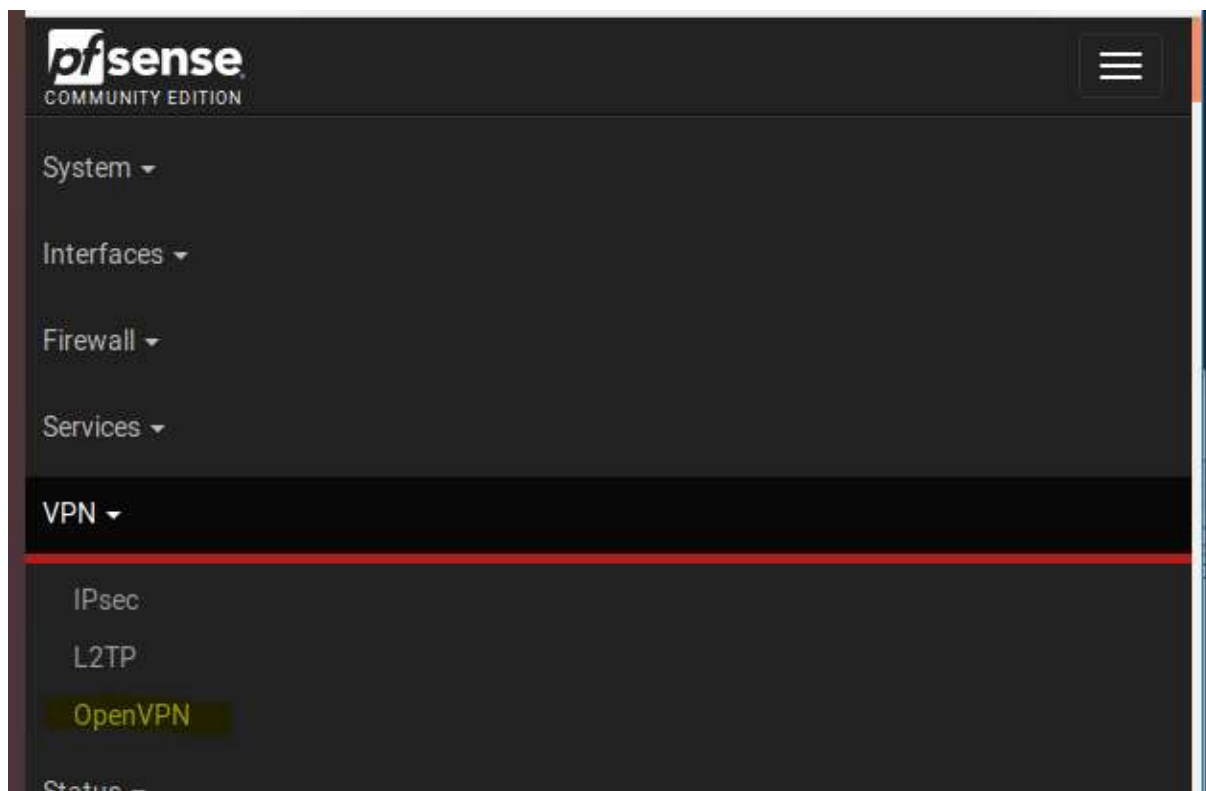
Ahora para comprobar si realmente está funcionando bien vamos a realizar un ping al servidor pfsense del compañero, y también le haremos un ping a una máquina que está en la red interna.

```
ana@ana-ubuntu:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=1.94 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=2.71 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=3.04 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.947/2.570/3.045/0.462 ms
ana@ana-ubuntu:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=62 time=3.00 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=62 time=4.68 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=62 time=2.95 ms
^C
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.954/3.545/4.682/0.805 ms
ana@ana-ubuntu:~$
```

## Ciente

### Configuración del cliente

Vamos a VPN → OpenVPN, ficha "Client" y creamos una nueva conexión.



Nos vamos a cliente para añadir una nueva regla y indicamos como server mode: **Peer to peer(shared key)**, como host or address la ip del servidor que está en la misma red en este caso 192.168.112.116. El resto de acciones las dejamos como estaban.

<b>Interface</b>	WAN	The interface used by the firewall to originate this OpenVPN client connection
<b>Local port</b>		Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
<b>host or address</b>	192.168.112.116	The IP address or hostname of the OpenVPN server.
<b>Server port</b>	1194	The port used by the server to receive client connections.
<b>host or address</b>		The address for an HTTP Proxy this client can use to connect to a remote server. TCP must be used for the client and server protocol.
<b>Proxy port</b>		
<b>Authentication</b>	none	The type of authentication used by the proxy server.
<b>Description</b>		A description may be entered here for administrative reference (not parsed).

Cuando llegamos a las opciones de **Cryptographic settings** indicamos que no genere la contraseña automáticamente y le indicamos la que nos da el servidor. El resto de opciones no las tocamos.

**Cryptographic Settings**

**Peer Certificate Authority**  
No Certificate Authorities defined. One may be created here: [System > Cert. Manager](#)

**Auto generate**  
☐ Automatically generate a shared key

**Shared Key**  
247f86d78b4f245ed5641d1d913b1ece  
2e2ab83a62a3fd1237df06fd51a37170  
7719c5ac145cedca07b568153c8b4abf  
6356a9b50c780e1b2412e9a0deee1470  
ec0f20e7ba5b7ca2068218fb783da1d7  
112273376b859bdf211fdb353710e607  
Paste the shared key here

**Encryption Algorithm**  
AES-128-CBC (128 bit key, 128 bit block)  
The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

**Enable NCP**  
☒ Enable Negotiable Cryptographic Parameters

Después nos vamos a la configuración de **Tunnel setting** e indicamos la ipv4 que utilizaremos para crear el túnel en este caso 10.0.1.0/24 y luego la IPv4 de la red interna del servidor

**Tunnel Settings**

**IPv4 Tunnel Network**

10.0.1.0/24

This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). The second usable address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

**IPv6 Tunnel Network**

This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

**IPv4 Remote network(s)**

192.168.2.0/24

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

**IPv6 Remote network(s)**

Nos vamos a firewall, rules y creamos una nueva regla con los parámetros que vemos en esta ya creada.

Firewall / Rules / WAN

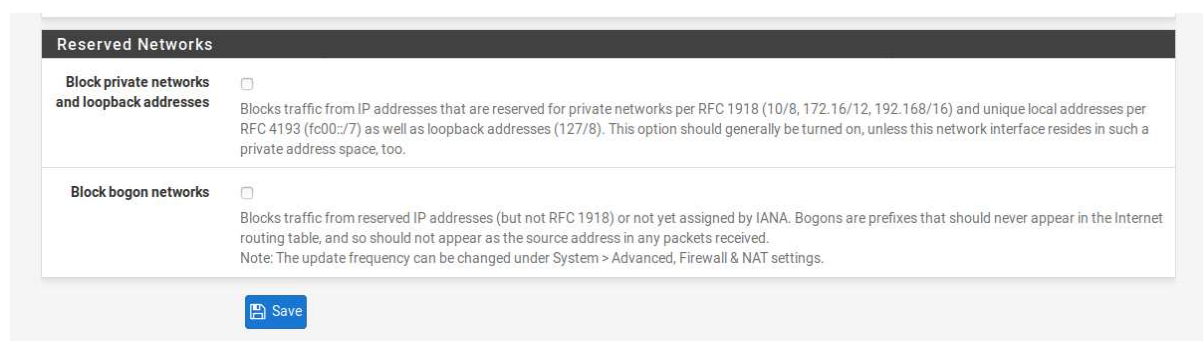
Floating **WAN** LAN OpenVPN

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	1194 (OpenVPN)	*	none		<a href="#">Add</a> <a href="#">Add</a> <a href="#">Delete</a> <a href="#">Save</a> <a href="#">Separator</a>

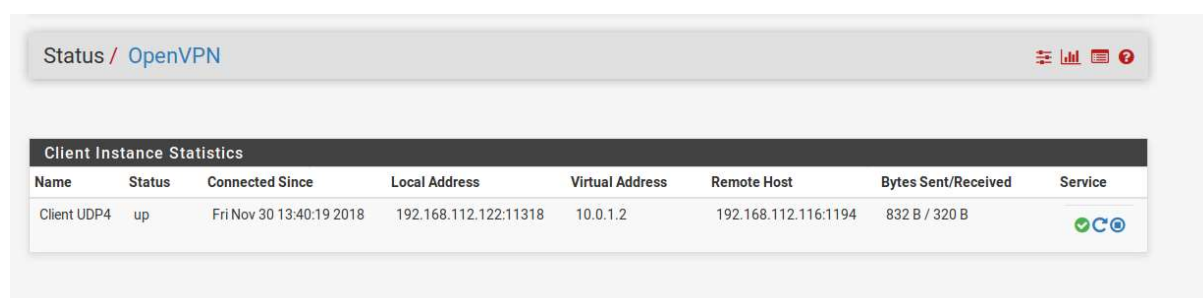


Por otro lado, para terminar la configuración nos vamos a interfaces, a WAN y desactivamos los estos dos campos y guardamos.



## Comprobaciones cliente

Nos vamos al estado de openVPN y vemos que está conectado.



Realizamos ping con la red interna del pfSense del servidor y con una de las maquinas de la red interna del servidor.

```
[1] Detectado ping 192.168.1.1
maria@maria-VirtualBox:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=3.54 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=21.2 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=3.13 ms
^X^C
--- 192.168.2.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.136/9.298/21.216/8.429 ms
maria@maria-VirtualBox:~$ ping 192.168.2.5
PING 192.168.2.5 (192.168.2.5) 56(84) bytes of data.
64 bytes from 192.168.2.5: icmp_seq=1 ttl=62 time=3.37 ms
64 bytes from 192.168.2.5: icmp_seq=2 ttl=62 time=4.18 ms
64 bytes from 192.168.2.5: icmp_seq=3 ttl=62 time=4.57 ms
64 bytes from 192.168.2.5: icmp_seq=4 ttl=62 time=4.32 ms
^X^C
--- 192.168.2.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 3.376/4.114/4.573/0.448 ms
maria@maria-VirtualBox:~$
```