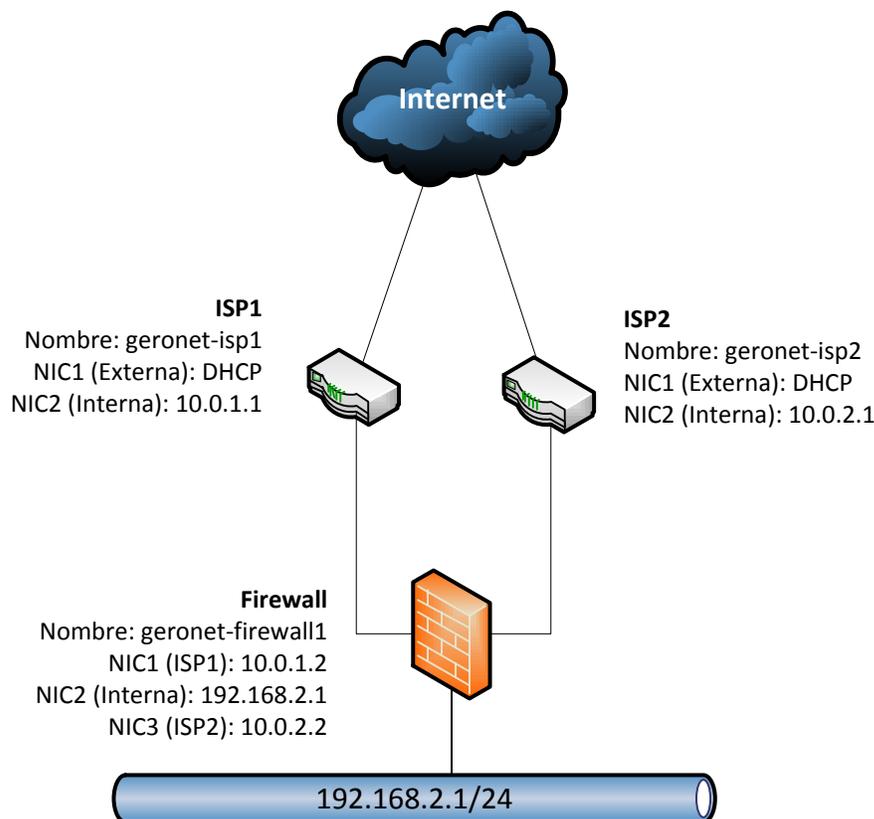


Balanceo de carga y redundancia entre dos ISP con PFSense y MultiWAN

En muchas organizaciones es vital no perder la conexión a internet en ningún momento. Por lo cual en los departamentos IT se suele contratar dos proveedores diferentes de internet o más. A continuación mostraré el procedimiento para implementar un sistema multi WAN con balanceo de carga y redundancia que tiene la ventaja de que si se cae un proveedor todo el tráfico sea redirigido por el ISP activo y a su vez si ambos funcionan correctamente, dividir todas las conexiones salientes por ambos servicios. Para ello utilizaremos un firewall basado en la distribución PFSense 2.0.

Para comenzar con el ejemplo, muestro un esquema con el escenario propuesto:



En resumen contamos con:

- 2 Proveedores de internet (ISP) diferentes.
- 1 Firewall implementado mediante PFSense 2.0 y con **tres placas de red**.
- 1 LAN Interna conectada a nuestra organización.

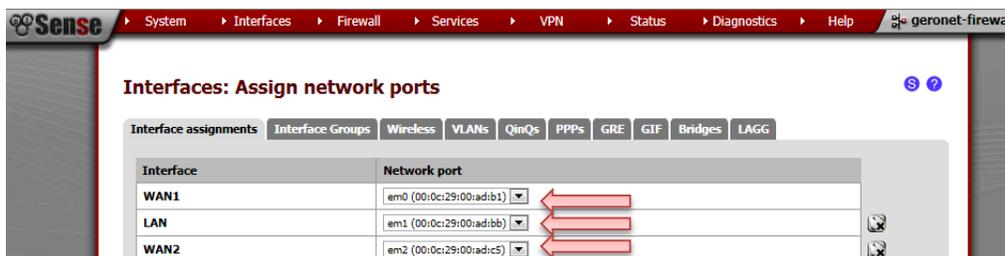
Para comenzar con la configuración, una vez instalado el SO PFSense, debemos asignar a cada una

de las interfaces una conexión.

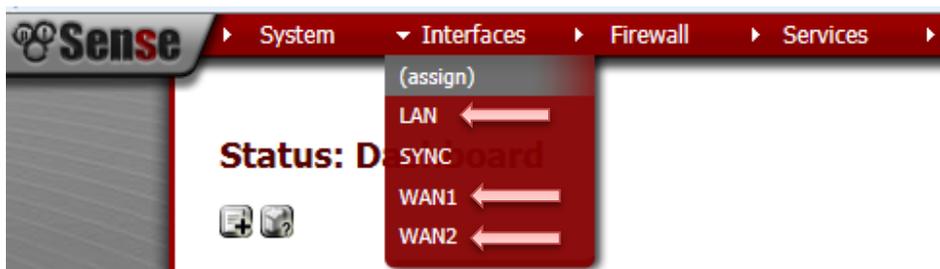
Para ello vamos a **Interfaces** → **assign** y configuramos la conexión WAN1, WAN2 y LAN. Es decir definimos que placa se va a conectar a que servicio.



Se nos muestra la siguiente pantalla donde se realiza la asignación:



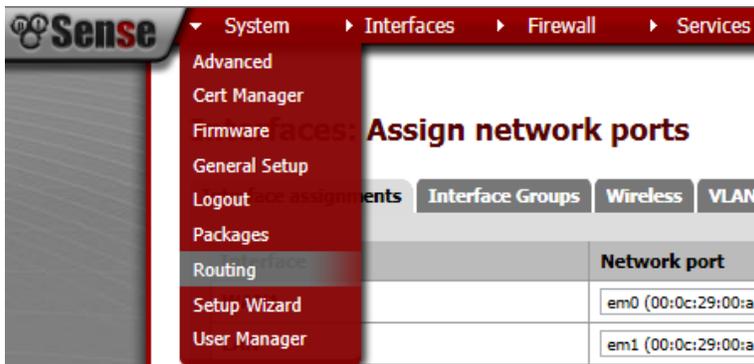
Una vez definidas las interfaces se debe indicar la IP de cada placa desde el menú Interfaces e ingresando en cada dispositivo:



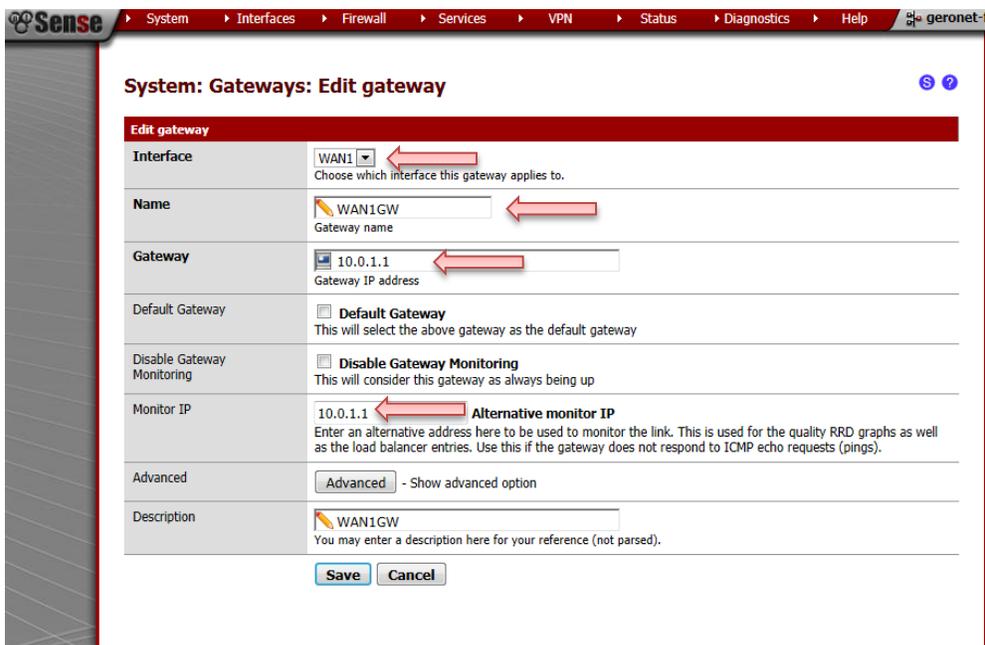
En nuestro caso: IP Placa WAN1: 10.0.1.2, WAN2: 10.0.2.2 y LAN: 192.168.2.1

Luego debemos definir nuestros Gateway. En nuestro caso asignaremos las direcciones provistas por nuestros ISP (En el ejemplo: WAN1: 10.0.1.1 y WAN2: 10.0.2.1).

Para ello vamos a **System** → **Routing**

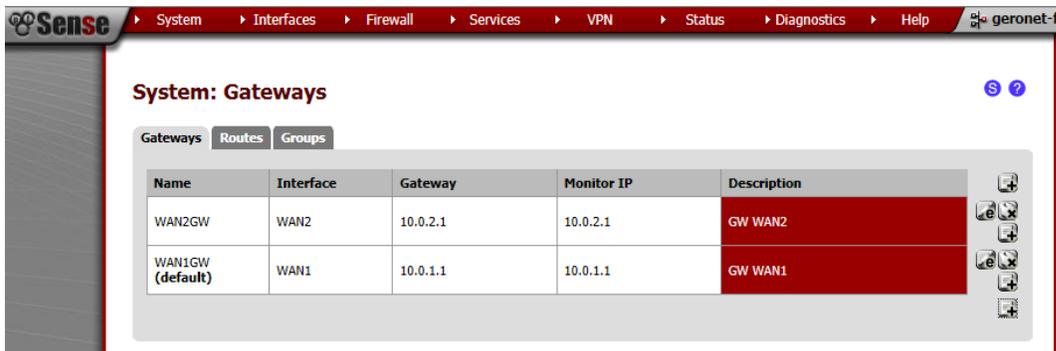


Pulsando en el signo (+), agregaremos los Gateway:



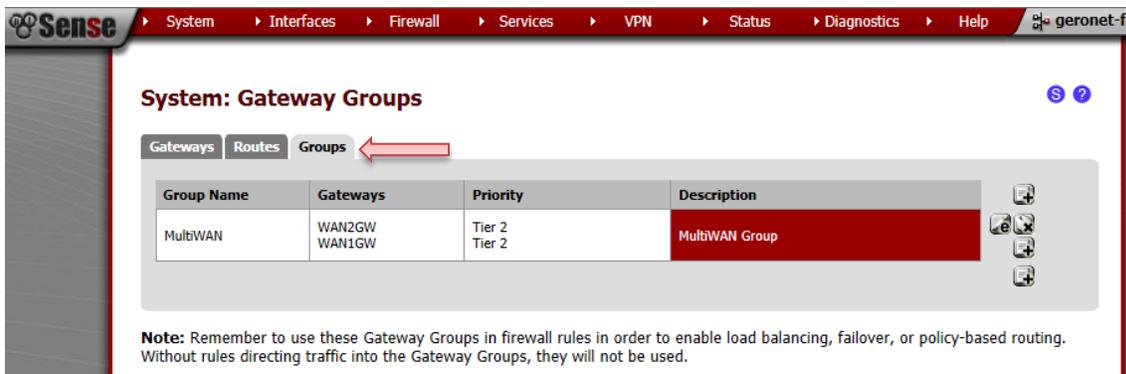
En el campo Monitor IP debemos ingresar la dirección de un equipo que responda al comando PING. Este puede ser el router del ISP o algún DNS público. Esto se utiliza para determinar si el link se encuentra activo o no.

Debemos agregar de la misma forma los dos gateway:

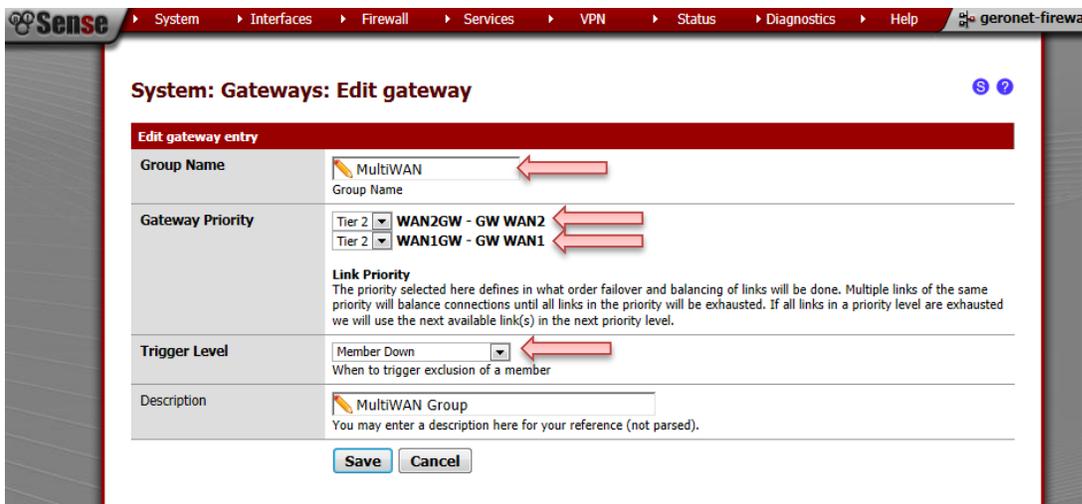


El siguiente paso es definir un Grupo de Gateway que en una misma conexión contará con nuestros dos Gateway provistos por nuestros ISP y se encargará de proveernos la salida a internet.

Para ello vamos a **Systems → Gateway → Groups**:



Pulsando (+), accederemos a la pantalla para configurar el grupo:



Debemos asignar un nombre de grupo, en el ejemplo lo llamamos: **MultiWAN**.

Luego en el campo Gateway Priority nos aparecerán las pasarelas definidas en el paso anterior.

Por lo que en ambos casos debemos asignarle a cada una un **Tier**.

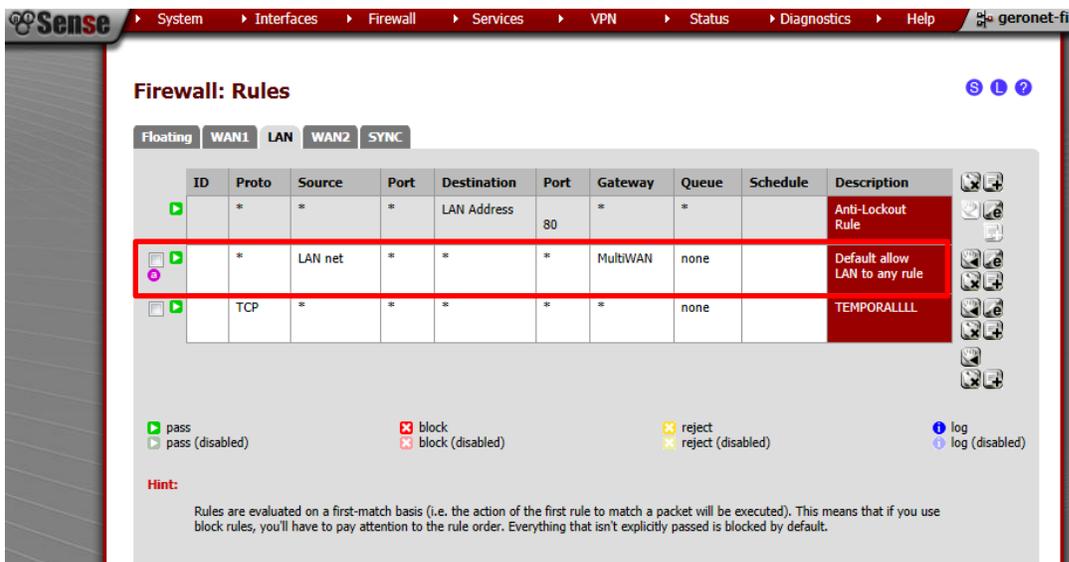
Importante: si asignamos el mismo **Tier**, el sistema realizará un balanceo de carga de las solicitudes y no dará prioridad a ningún ISP en particular. En cambio si a uno le asignamos un Tier 1 y a otro un **Tier2**, el sistema priorizará al que tenga **Tier1** y sino está disponible, entonces luego redirigirá el tráfico por el ISP con **Tier 2**.

Una vez definido esto, debemos especificar una regla de ruteo de las solicitudes.

Para esto vamos a **Firewall → Rules**



Debemos agregar la regla que nos permita redirigir el tráfico saliente a nuestro grupo MultiWAN definido anteriormente:



Pulsando el botón (+) agregaremos nuestra regla de ruteo:

Sense System Interfaces Firewall Services VPN Status Diagnostics Help geronet

Firewall: Rules: Edit

Edit Firewall rule

Action	<input type="text" value="Pass"/> <p>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.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="text" value="LAN"/> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<input type="text" value="any"/> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="LAN subnet"/> Address: <input type="text"/> / <input type="text"/>
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text"/> / <input type="text"/>
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

En este caso indicamos que permitiremos todo el tráfico saliente desde nuestra LAN a internet por medio del Gateway **MultiWAN**:

Description
You may enter a description here for your reference.

Advanced features

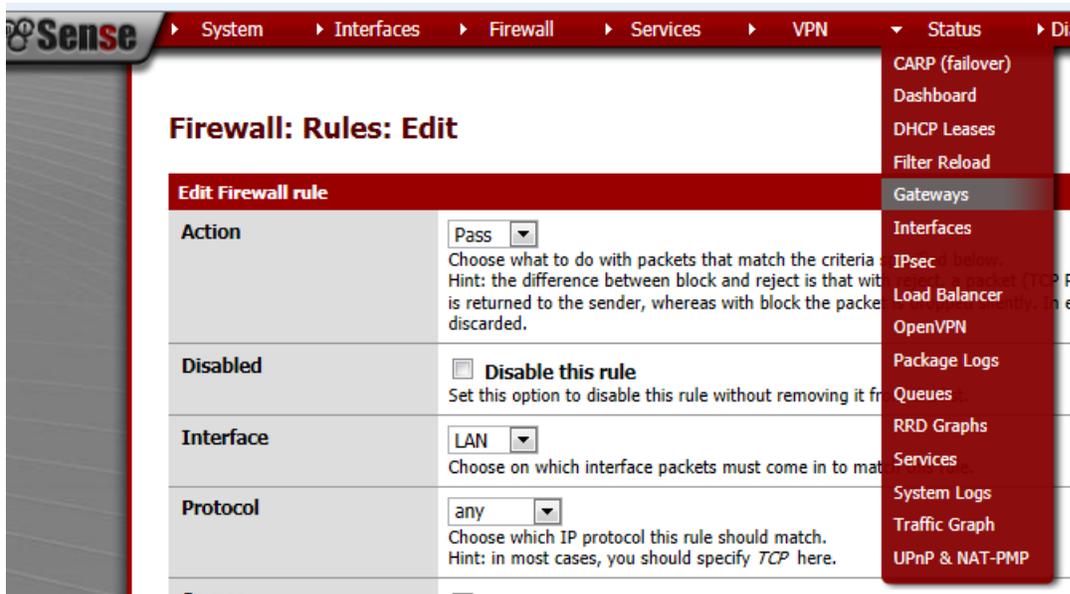
Source OS	<input type="text" value="Advanced"/> - Show advanced option
Diffserv Code Point	<input type="text" value="Advanced"/> - Show advanced option
Advanced Options	<input type="text" value="Advanced"/> - Show advanced option
State Type	<input type="text" value="Advanced"/> - Show advanced option
No XMLRPC Sync	<input type="text" value="Advanced"/> - Show advanced option
Schedule	<input type="text" value="Advanced"/> - Show advanced option
Gateway	<input type="text" value="MultiWAN"/> <ul style="list-style-type: none"> default WAN2GW - 10.0.2.1 WAN1GW - 10.0.1.1 MultiWAN <p>Use the system routing table. Or choose a gateway to utilize policy based routing.</p>
In/Out	<input type="text" value="Advanced"/> - Show advanced option
Ackqueue/Queue	<input type="text" value="Advanced"/> - Show advanced option
Layer7	<input type="text" value="Advanced"/> - Show advanced option

De esta forma todas las peticiones a internet se redirirán por nuestro grupo de Gateway y el

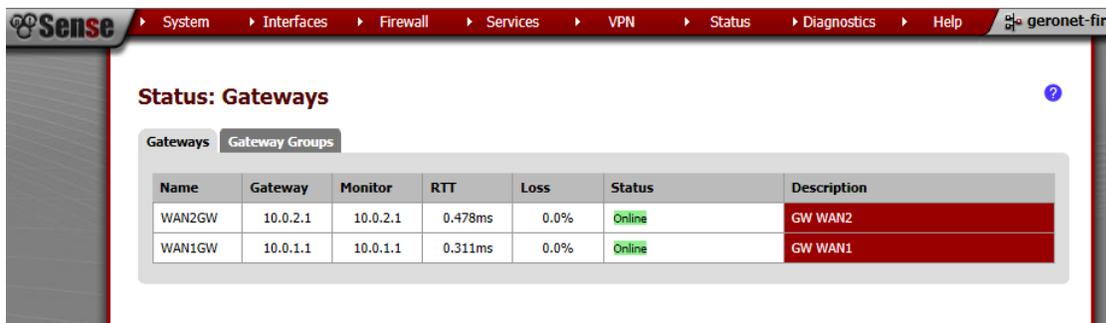
sistema se encargará de realizar el balanceo de cargas y redirigir el tráfico cuando uno de los dos ISP no se encuentre activo.

Finalmente nos será útil realizar el monitoreo del estado de los enlaces.

Para ello vamos a: **Status** → **Gateways**



En la siguiente pantalla podremos apreciar el status de cada link:



Espero, les sea útil.

Saludos.