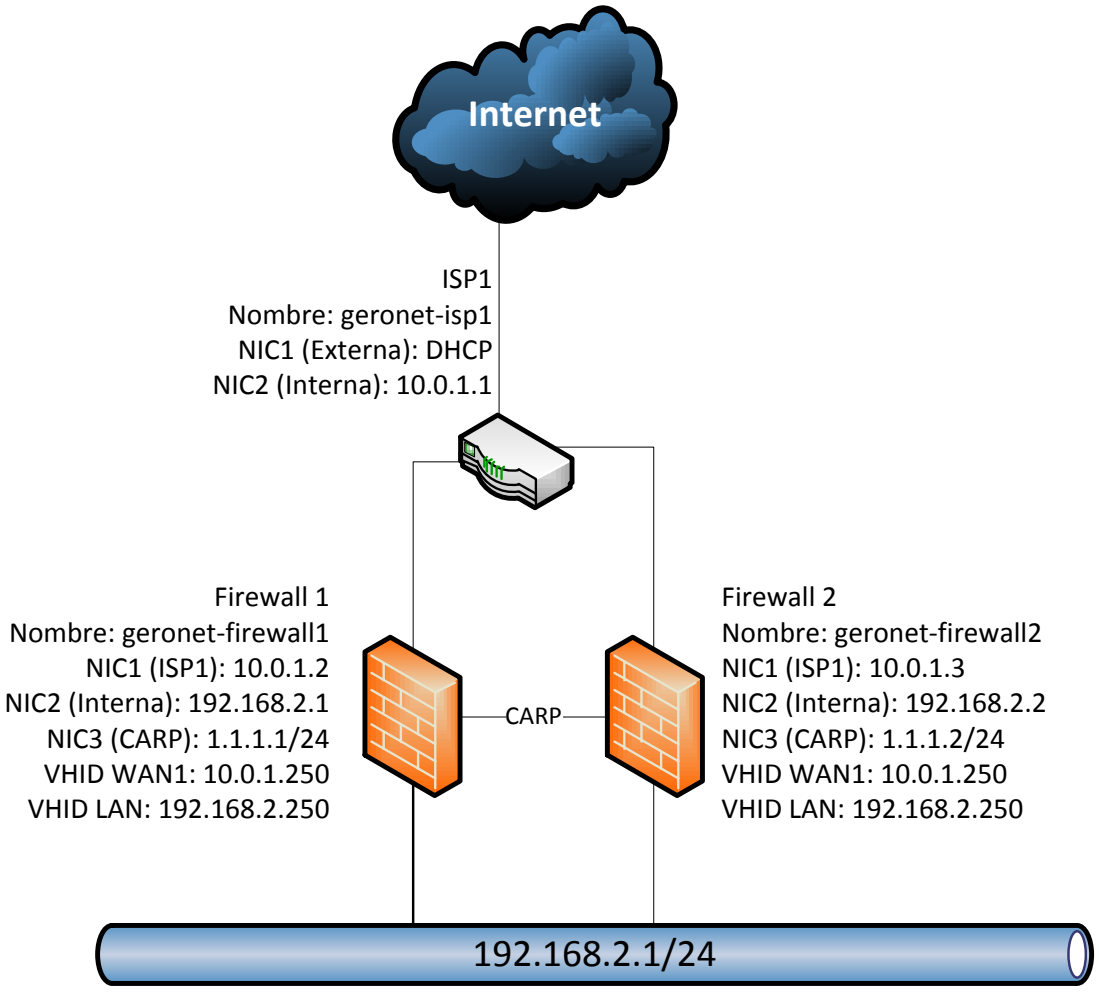
Configurar un firewall con failover en PFSense 2.0.1

Básicamente la idea consiste en configurar en nuestra organización un firewall con redundacia en la cual se replican los estados de las conexiones en un equipo de backup y en caso de producirse una falla en el principal, el secundario entre en funcionamiento automáticamente sin producir cortes en las comunicaciones.

Por ello en el ejemplo configuraremos dos firewall capaces de funcionar sincronizadamente, uno como equipo principal y otro como secundario de backup.

Nuestro esquema propuesto es el siguiente:



Elementos necesarios.

- 1 Proveedor de internet que nos proporcione tres IP para conectarnos a la red.
- 2 Equipos que funcionen como firewall y PFSense 2.0 instalado.

- 3 Placas de red en cada firewall.
- 1 dirección IP VHID definida para la red WAN.
- 1 dirección IP VHID definida para la red LAN (esta será el gateway para los clientes de la LAN).

Las direcciones VHID son las direcciones IP virtuales que serán compartidas por los firewalls para establecer las conexiones tanto en la LAN interna como en la WAN. Es decir, ambos equipos responderan a la misma IP, sin embargo tambien cada equipo debe tener su dirección particular.

En resumen en cada equipo configuraremos las siguientes direcciones en cada placa:

Firewall 1 (Principal):

WAN: 10.0.1.2

LAN: 192.168.2.1

SYNC: 1.1.1.1 (Será la IP utilizada para sincronizar los firewalls)

Firewall 2 (Backup):

WAN: 10.0.1.3

LAN: 192.168.2.2

SYNC: 1.1.1.2

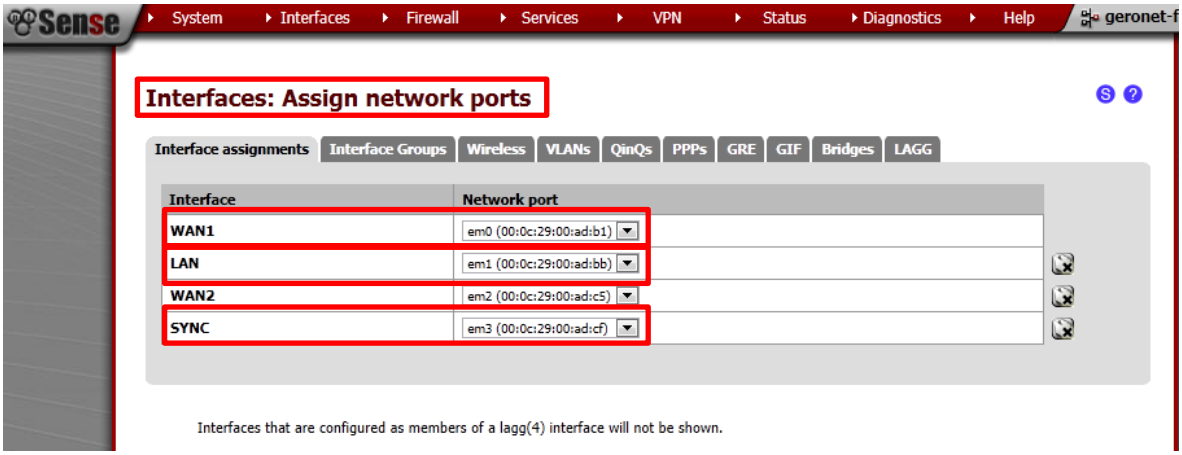
Y a su vez, en ambos equipos las siguientes IP Virtuales:

VHID WAN: 10.0.1.250 (Debe ser provista por el ISP)

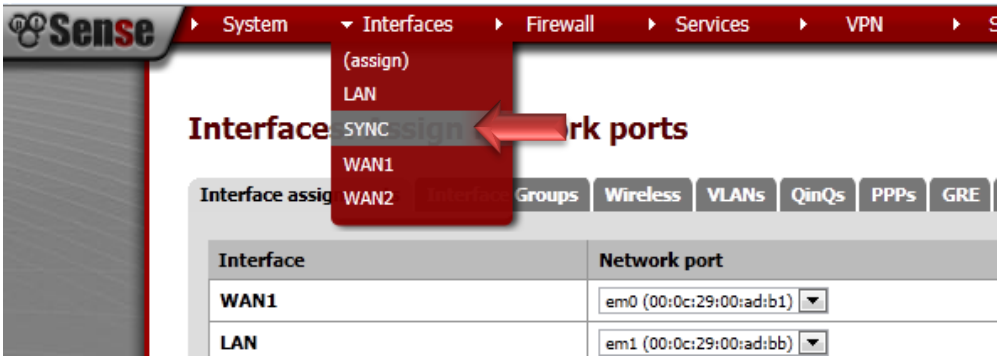
VHID LAN: 192.168.2.250 (Será el gateway al que deben aputar los clientes)

Comencemos entonces con la configuración:

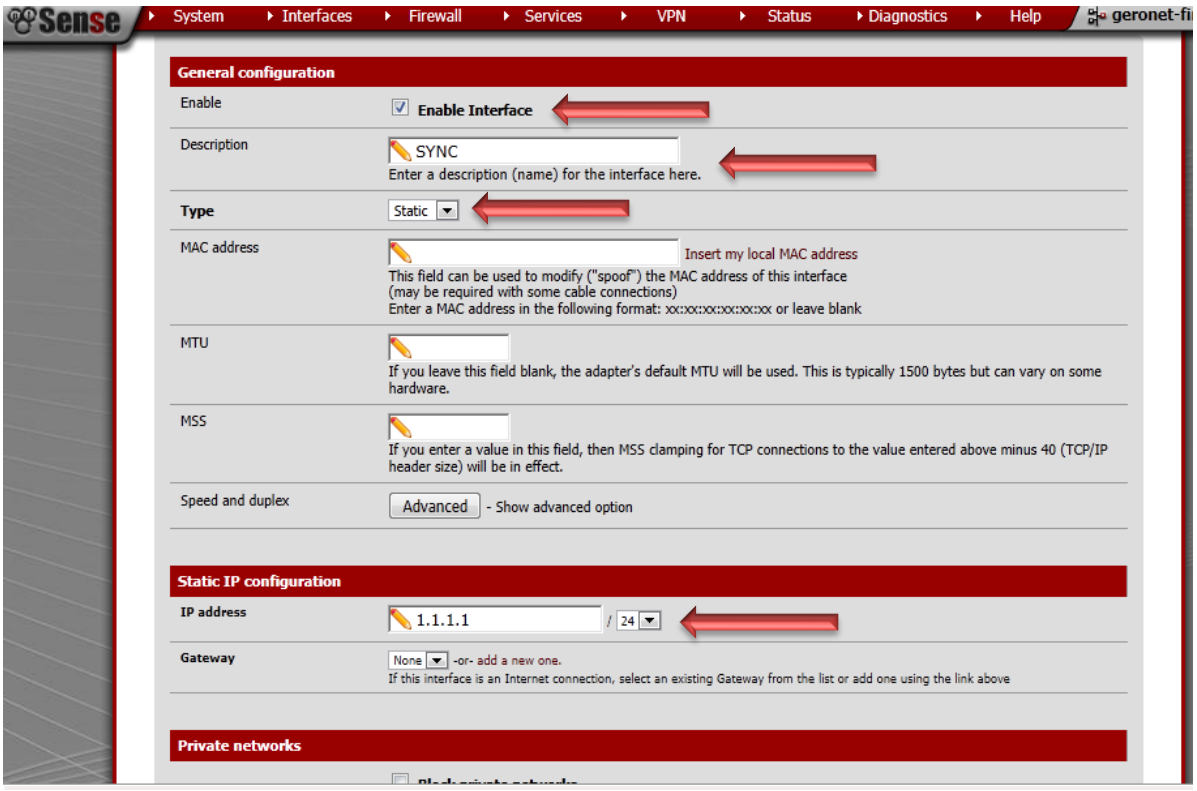
Primero asignamos las placas de red a las diferentes interfaces desde el menú **Interfaces → Assing**



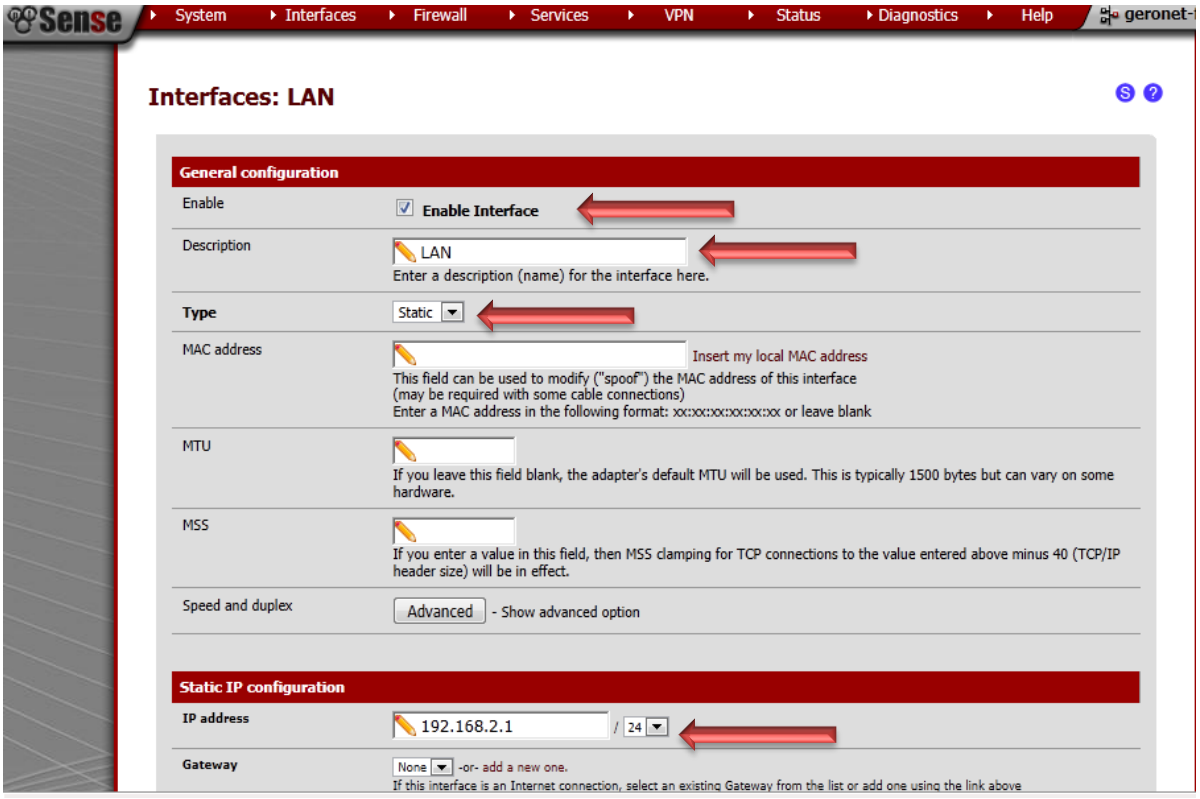
Luego asignamos la IP correspondiente a cada interfaz desde Interfaces → [Placa Correspondiente]



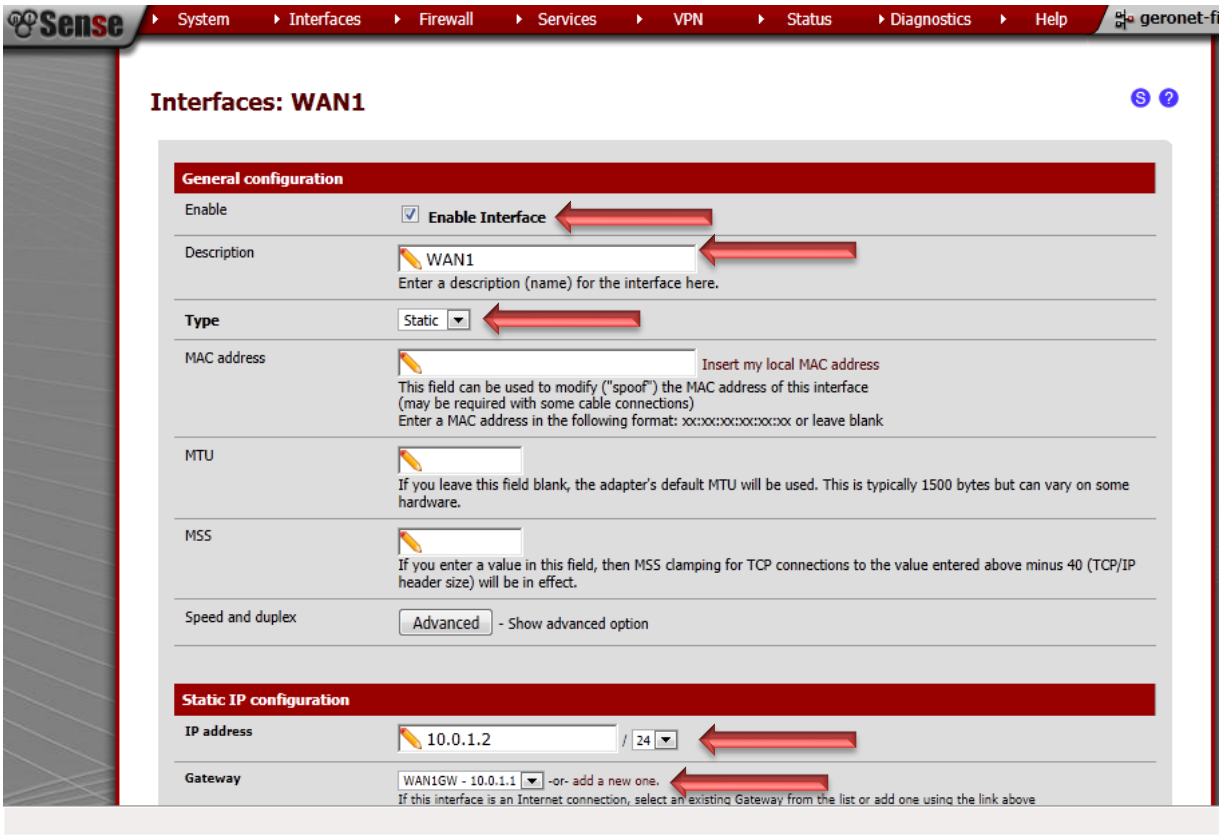
Asignamos la IP a la interfaz de sincronización:



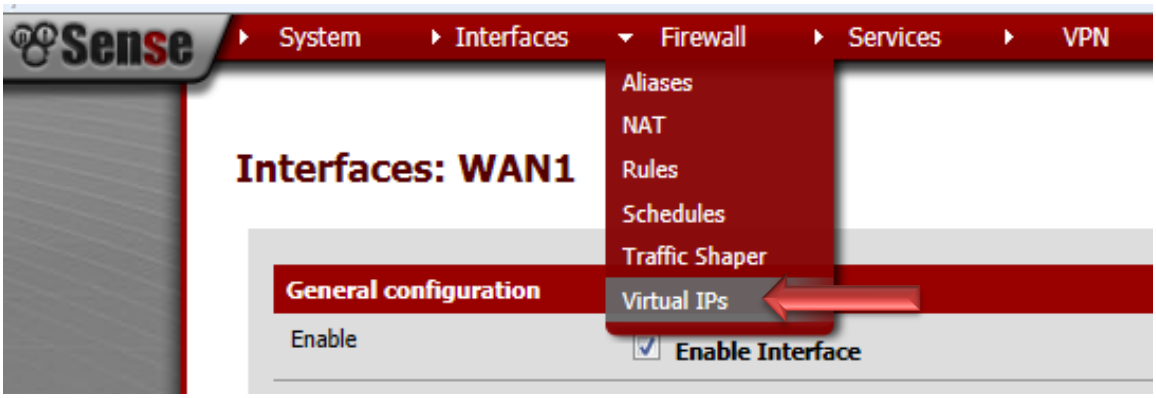
Luego a la placa de LAN:



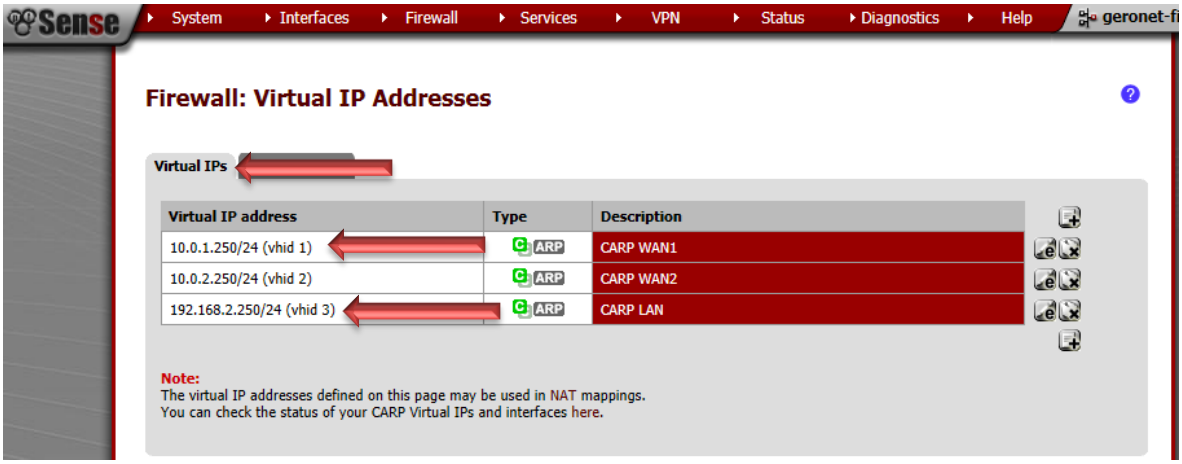
Y por último a la placa WAN, a la cual ademas le asignamos el gateway correspondiente proporcionado por el ISP:



Ahora se deben asignar las IPs Virtuales que hemos definido. Vamos a Firewall → Visrtual IPs



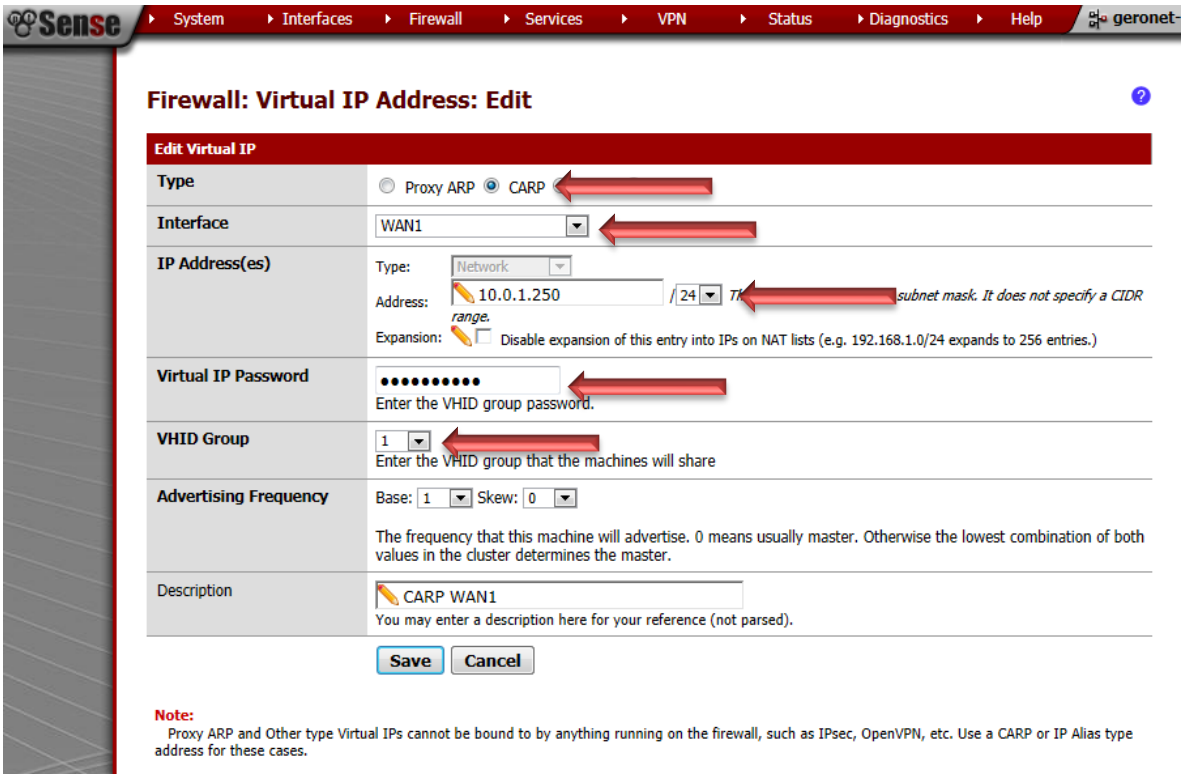
En la pestaña Virtual IPs debemos pulsar en el botón (+) para agregar una nueva VHID.



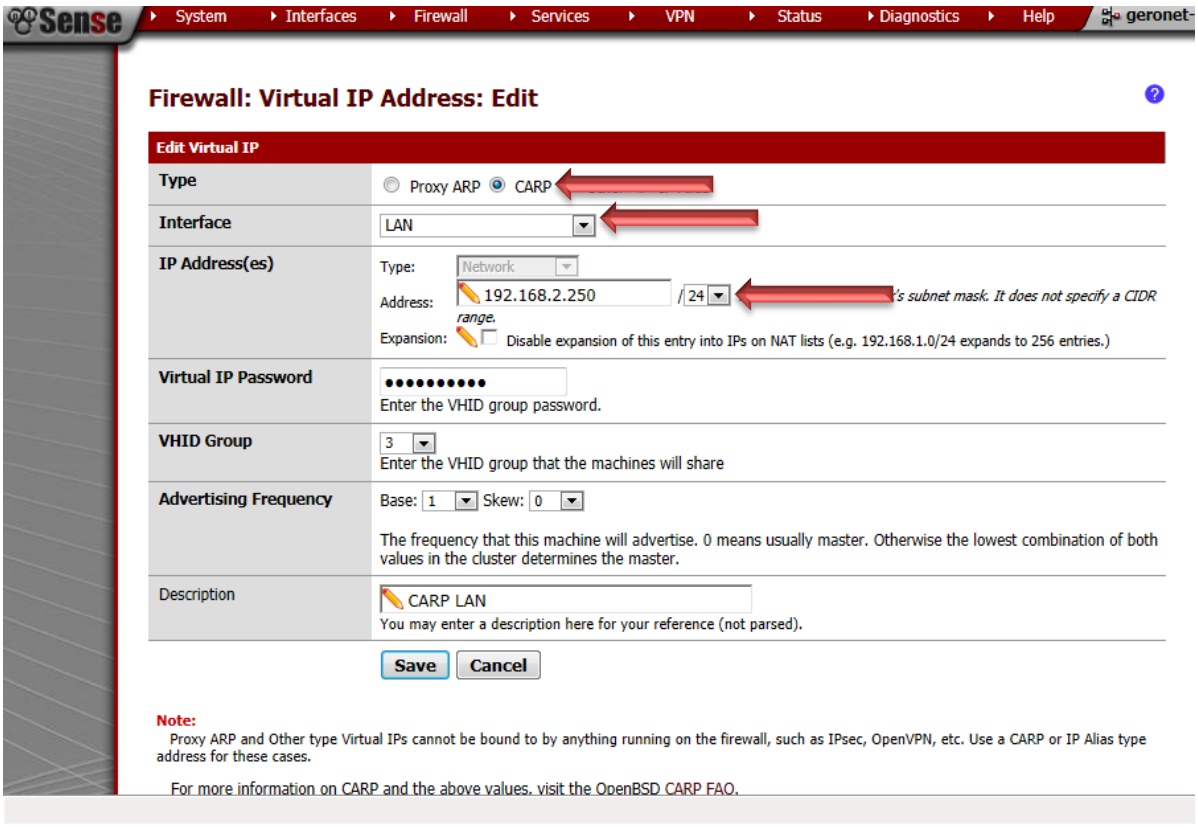
Primero agregamos la IP virtual de la WAN. Es importante que se seleccione el **Type CARP**.

En el campo Virtual IP Password debemos settear una clave que se insertará igual en ambos firewall.

Y ademas el VHID Group debe configurarse de la misma forma en ambos firewalls.

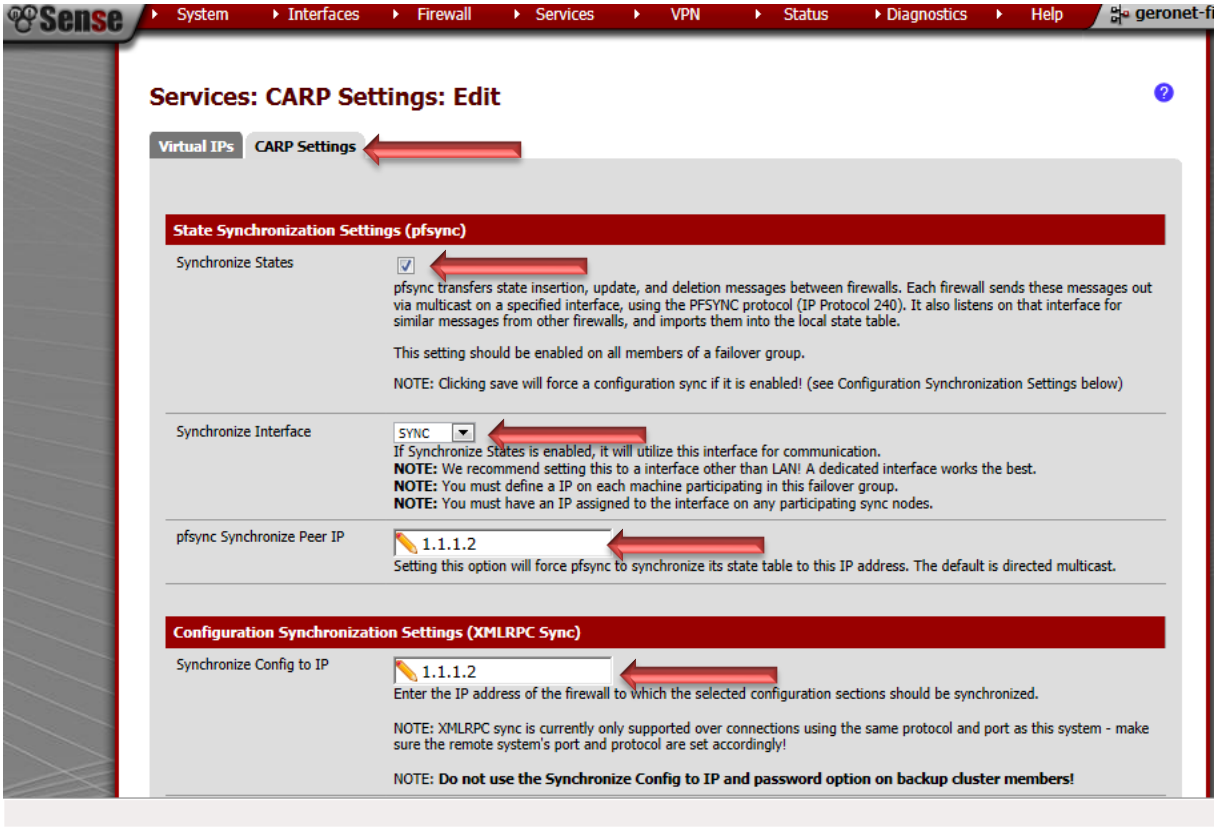


Luego configuramos el VHID de la red LAN de la misma forma en ambos dispositivos.

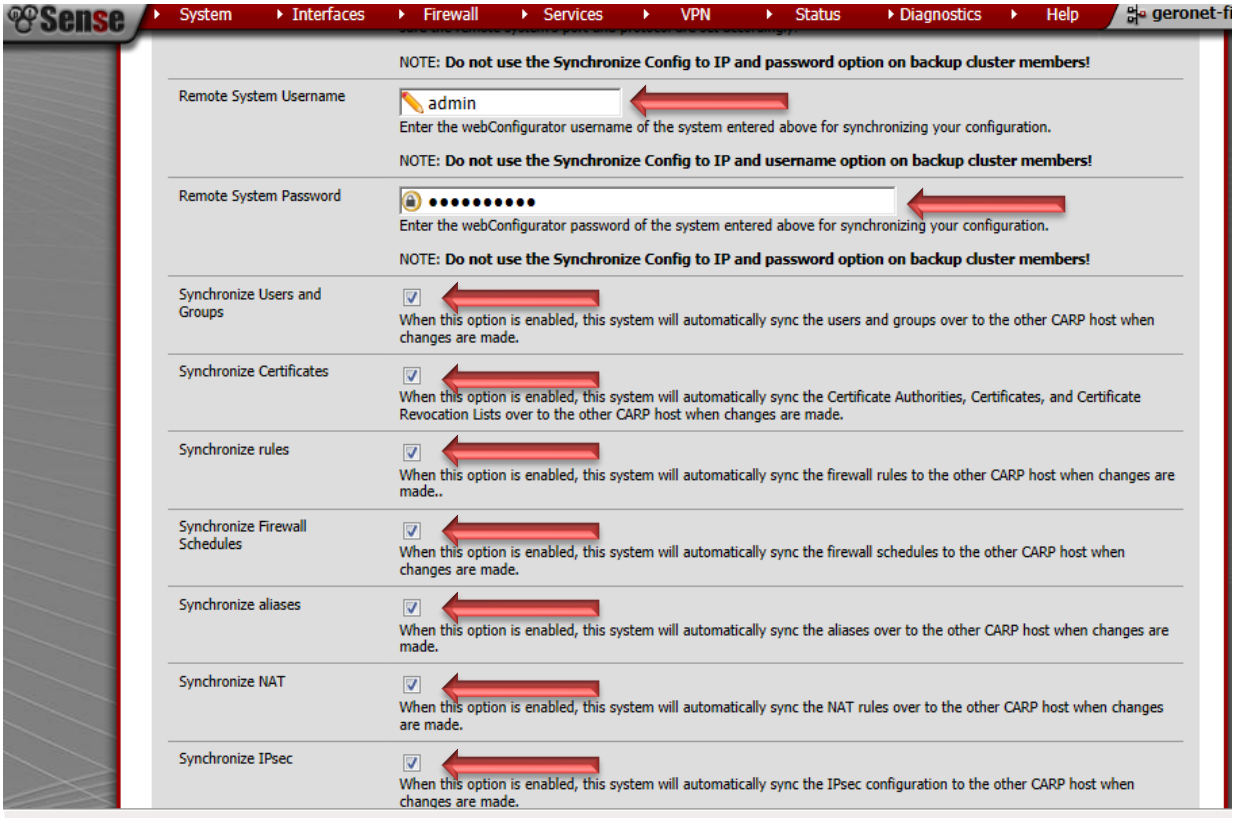

pfSense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
geronet-
Firewall: Virtual IP Address: Edit
Edit Virtual IP
Type
Proxy ARP
CARP
Interface
LAN
IP Address(es)
Type:
Network
Address:
192.168.2.250
/ 24
's subnet mask. It does not specify a CIDR range.
Expansion:
Disable expansion of this entry into IPs on NAT lists (e.g. 192.168.1.0/24 expands to 256 entries.)
Virtual IP Password
Enter the VHID group password.
VHID Group
3
Enter the VHID group that the machines will share
Advertising Frequency
Base: 1
Skew: 0
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description
CARP LAN
You may enter a description here for your reference (not parsed).
Save
Cancel
Note:
Proxy ARP and Other type Virtual IPs cannot be bound to by anything running on the firewall, such as IPsec, OpenVPN, etc. Use a CARP or IP Alias type address for these cases.
For more information on CARP and the above values, visit the OpenBSD CARP FAQ.

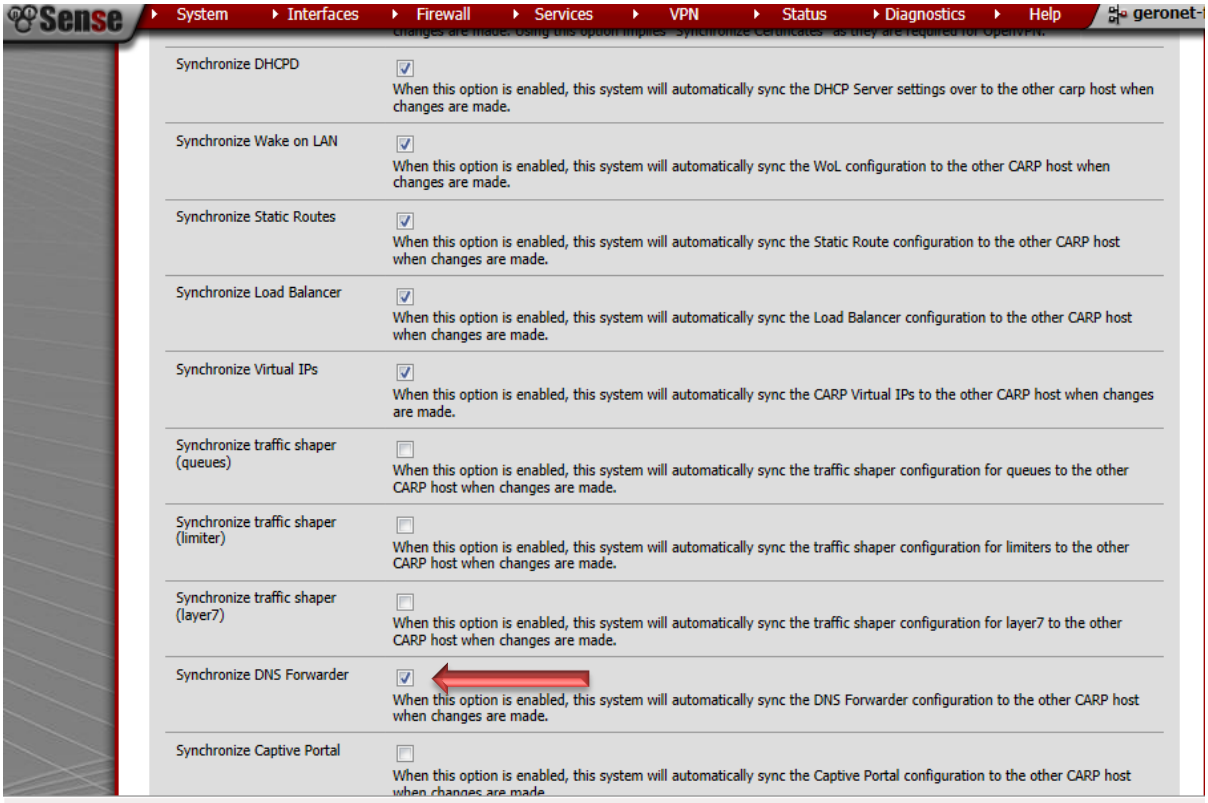
El siguiente paso solo debemos hacerlo en el firewall principal:

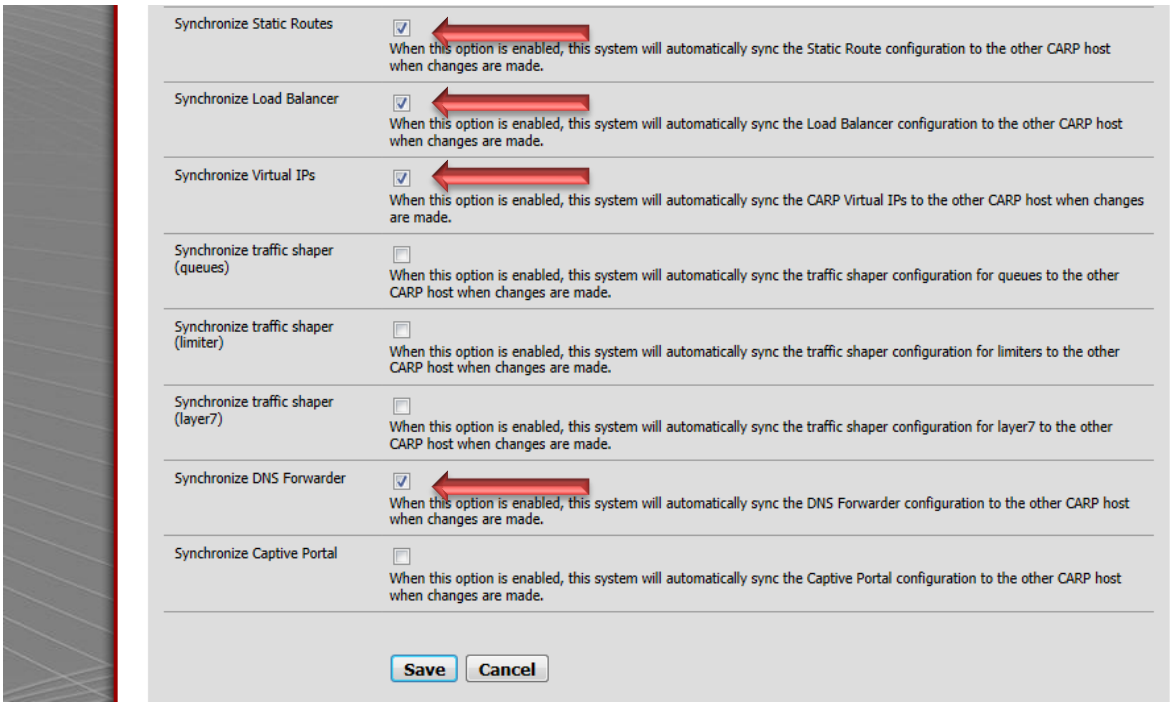
En la pestaña **CARP Settings** debemos tildar la opción Synchronize States, seleccionamos la interfaz definida para tal caso (SYNC) y seteamos la IP del otro firewall (en el ejemplo la IP de sincronización del firewall 2 de backup) con la cual se replicará el estado.



Mas abajo debemos establecer el usuario y clave de administración del dispositivo de backup y sellecionar las características que se desean sincronizar:


pfSense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
geronet-fi
NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!
Remote System Username
admin
Enter the webConfigurator username of the system entered above for synchronizing your configuration.
NOTE: Do not use the Synchronize Config to IP and username option on backup cluster members!
Remote System Password
Enter the webConfigurator password of the system entered above for synchronizing your configuration.
NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!
Synchronize Users and Groups
When this option is enabled, this system will automatically sync the users and groups over to the other CARP host when changes are made.
Synchronize Certificates
When this option is enabled, this system will automatically sync the Certificate Authorities, Certificates, and Certificate Revocation Lists over to the other CARP host when changes are made.
Synchronize rules
When this option is enabled, this system will automatically sync the firewall rules to the other CARP host when changes are made..
Synchronize Firewall Schedules
When this option is enabled, this system will automatically sync the firewall schedules to the other CARP host when changes are made.
Synchronize aliases
When this option is enabled, this system will automatically sync the aliases over to the other CARP host when changes are made.
Synchronize NAT
When this option is enabled, this system will automatically sync the NAT rules over to the other CARP host when changes are made.
Synchronize IPsec
When this option is enabled, this system will automatically sync the IPsec configuration to the other CARP host when changes are made.





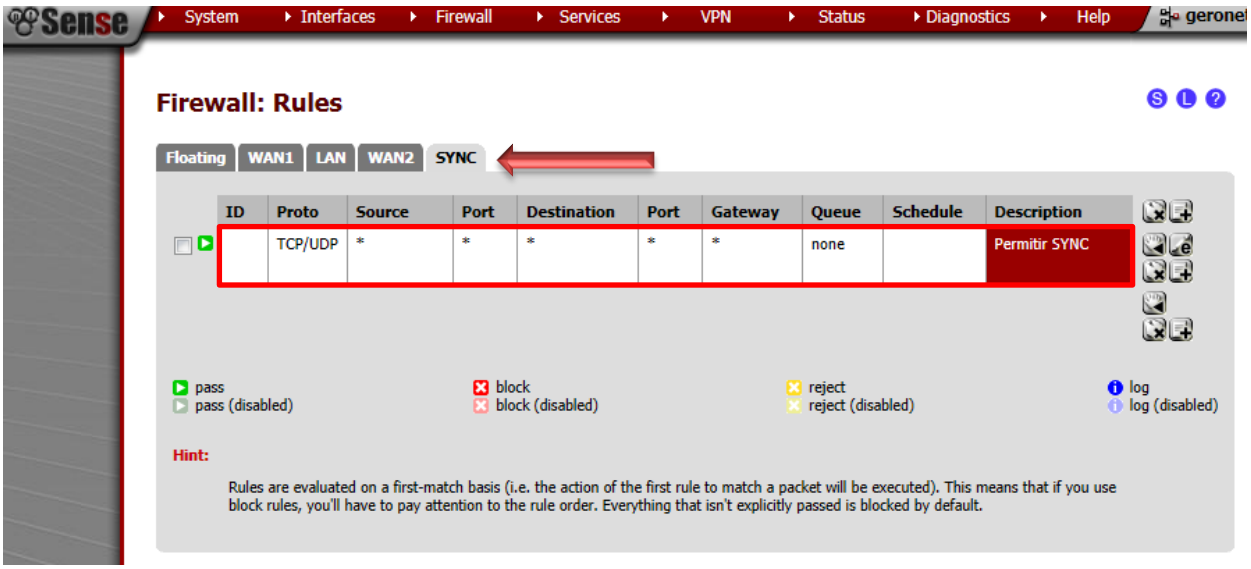
Pulsando en **Save** guardaremos los cambios.

El siguiente paso consiste en habilitar en ambos firewalls una regla que permita la comunicación

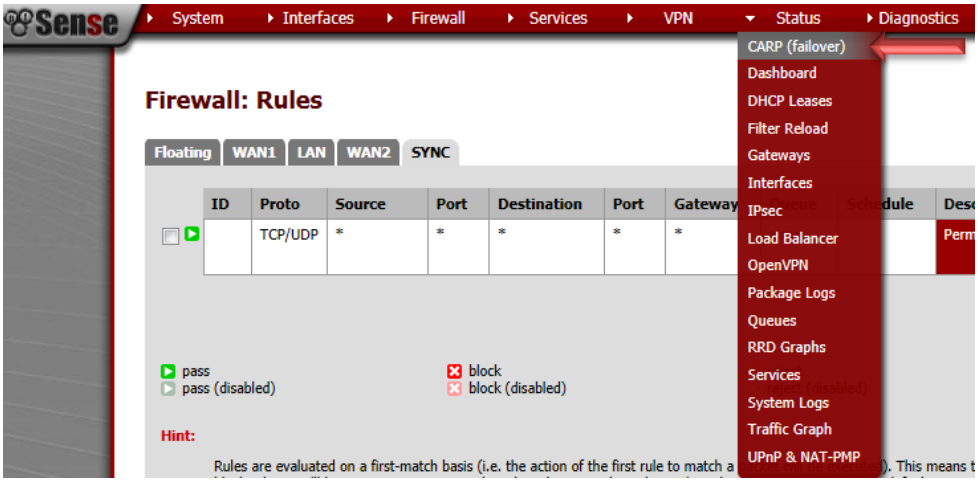
entre las placas de sincronización de ambos dispositivos.

Para ello vamos a **Firewall →Rules → Placa SYNC**

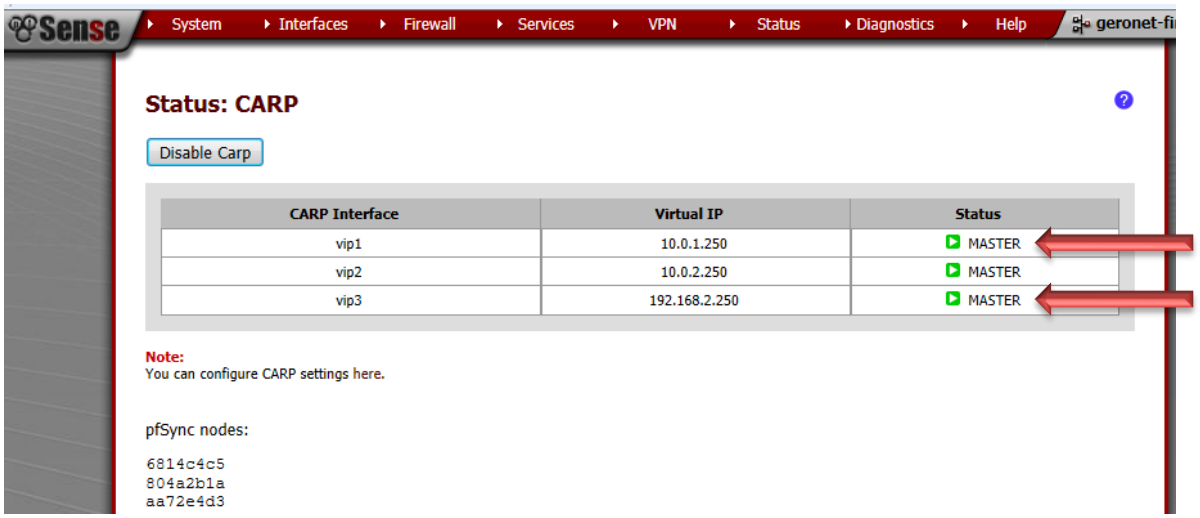
En nuestro caso habilitamos el tráfico completo en dicha interfaz:



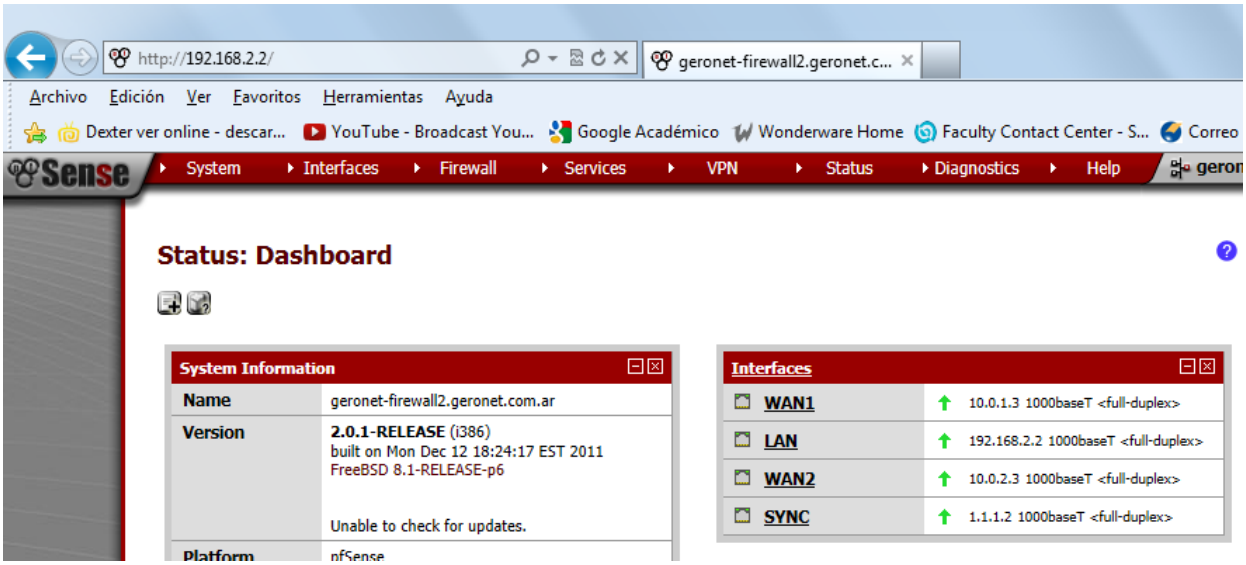
Una vez aplicada la regla en ambos equipos, podremos comprobar el status del Cluster de firewall llendo a **Status → CARP (failover)**

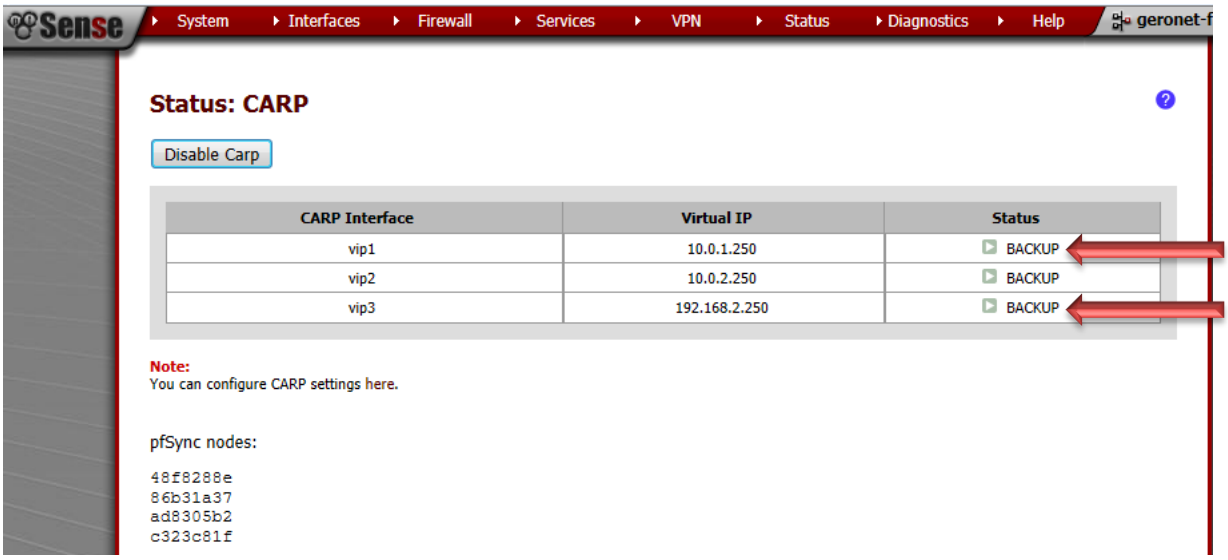


Si estamos situados en el firewall principal veremos que el status de las Virtuals IPs es MASTER y con la flecha verde nos indica que está online:



Si nos logueamos en el firewall de backup veremos que el status de las Virtuals IPs dice **Backup**





Por último, si queremos verificar que la sincronización está funcionando correctamente podemos probarlo aplicando una regla de firewall en uno de los dispositivos y luego verificando que en el otro se a replicado automáticamente.