

Pfsense Alta disponibilidad

– *TFG* –

Dos Hermanas, 14 de junio 2021

Autor: José Miguel Calderón Frutos

Tabla de contenido

Indice

1 Pfsense-alta-disponibilidad.....	1
1.1 Escenario.....	1
1.1.1 Redes.....	1
1.1.2 Maquinas.....	2
1.1.3 instalación de pfsense.....	2
1.2 Configuración de pfsense.....	11
1.2.1 Configuración de las interfaces.....	11
1.2.2 Configuración de High Availability Sync.....	12
1.2.3 Configuración de Ip Virtuales.....	13
1.2.4 Configuración del dhcp.....	14
1.2.5 Configuración del Snat.....	14
1.2.6 Configuración del Alisas.....	15
1.2.7 Configurar firewall para salir a internet.....	15

1 Pfsense-alta-disponibilidad

Proyecto de fin de grado

1.1 Escenario

Voy a realizar un escenario desplegado en libvirt el cual estará compuesto por 4 maquinas las cuales dos serán pfsense y las otras dos serán Debían las cuales usaremos para realizar pruebas.

1.1.1 Redes

Lo primero que configuraremos en Libvirt serán las redes.

En principio crearemos un total de 4 redes.

1. default

La red por defecto es la red que tiene un nat hacia mi tarjeta de red real de mi maquina.

Es la red que usaremos para simular la salida a internet.

Tendrá un direccionamiento de 192.168.122.0/24 y sera la única red que tenga activado el dhcp.

2. exter

Es la red extermina de nuestra lan como su propio nombre indica, sera la red que albergue uno de los servidores de debían simulando un fronten.

Tendrá un direccionamiento de 10.10.10.0/24 y no tendrá habilitado el dhcp puesto que de eso se encargan los servidores de pfsense.

3. intra

Es la red interna de nuestra lan, sera la red que albergue uno de los servidores de debían simulando un backend.

Tendrá un direccionamiento de 10.10.20.0/24 y no tendrá habilitado el dhcp puesto que de eso se encargan los servidores de pfsense.

4. net-pfsense

Esta red es una red necesaria para configurar pfsense en alta disponibilidad.

Tendrá un direccionamiento de 10.10.0.0/24 y no tendrá habilitado el dhcp.

Todas estas redes estan definidas por medio de xml el cual se encuentra en el repositorio de github.

1.1.2 Maquinas

Primero crearemos las dos maquinas debían, para ello utilizaremos la herramienta **virt-builder** para crear la imagen y luego los xml para definir las maquinas.

```
virt-builder debian-10 --hostname db --format qcow2 --  
root-password password:root --size 10G -o db.qcow2
```

```
virt-builder debian-10 --hostname web --format qcow2 --  
root-password password:root --size 10G -o web.qcow2
```

Y las definiremos con los xml que se encuentran en el repositorio de github.

```
define web.xml
```

```
define db.xml
```

1.1.3 instalación de pfsense

Para la instalación de pfsense, he utilizado la herramienta de libvier **virt-install**.

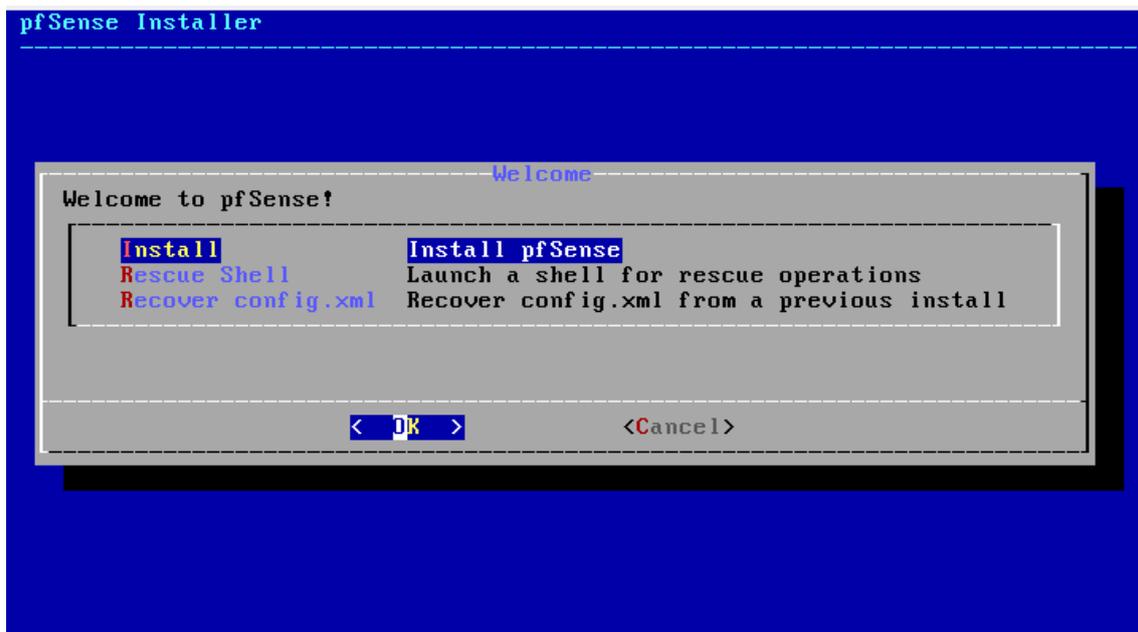
Pfsense master

```
virt-install --connect qemu:///system --cdrom
~/Iso/pfSense-CE-2.5.0-RELEASE-amd64.iso --disk
size=10,pool="MVs" --network network=default --network
network=exter --network network=intra --network
network=net-pfsense --name pfsense-master --memory 1024 --
vcpus 1
```

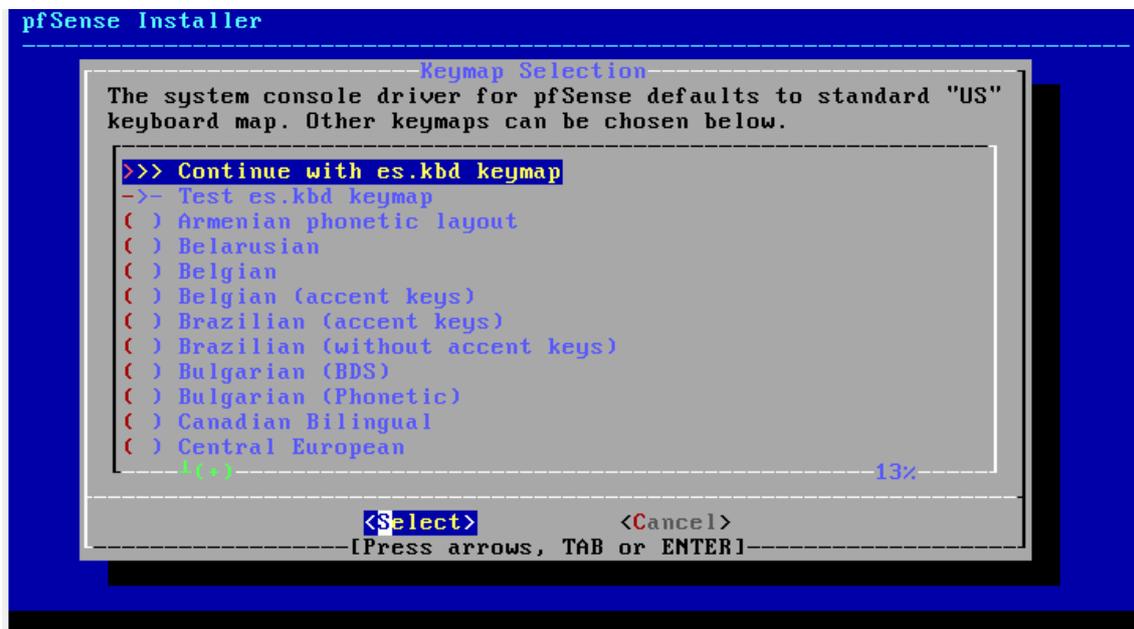
Pfsense slave

```
virt-install --connect qemu:///system --cdrom
~/Iso/pfSense-CE-2.5.0-RELEASE-amd64.iso --disk
size=10,pool="MVs" --network network=default --network
network=exter --network network=intra --network
network=net-pfsense --name pfsense-slave --memory 1024 --
vcpus 1
```

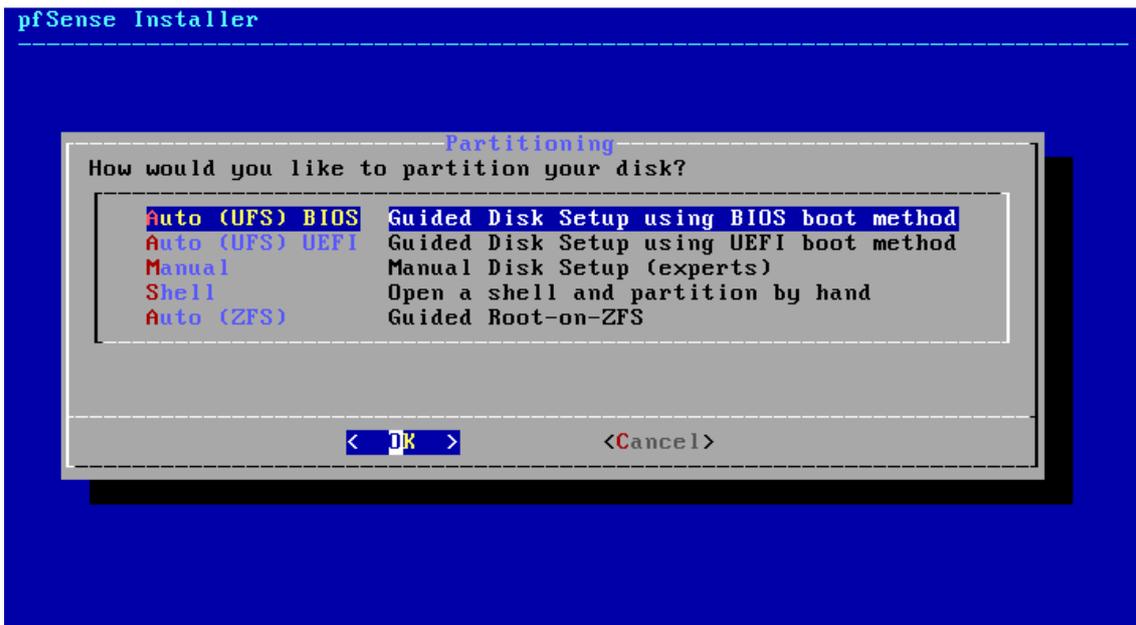
Tras ejecutar esto nos abrira una ventana con el instalador de pfsense en el primer paso pulsaremos en install



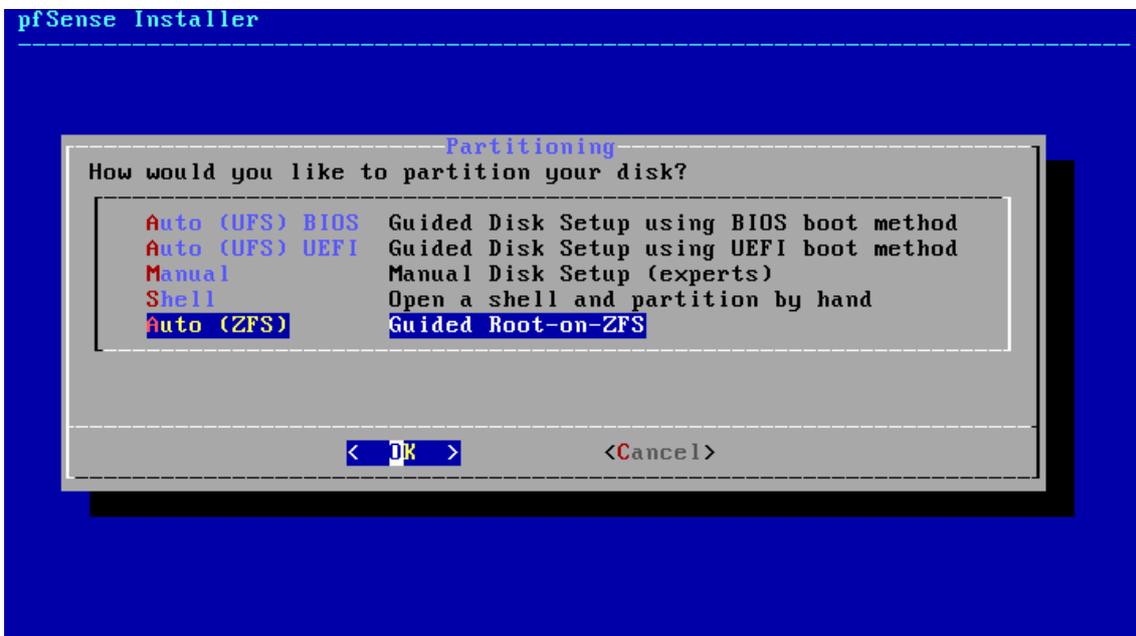
Luego nos pedira el idioma del teclado, buscaremos spanish y probaremos las teclas en test keymap si todo esta correcto pulsaremos continuar.



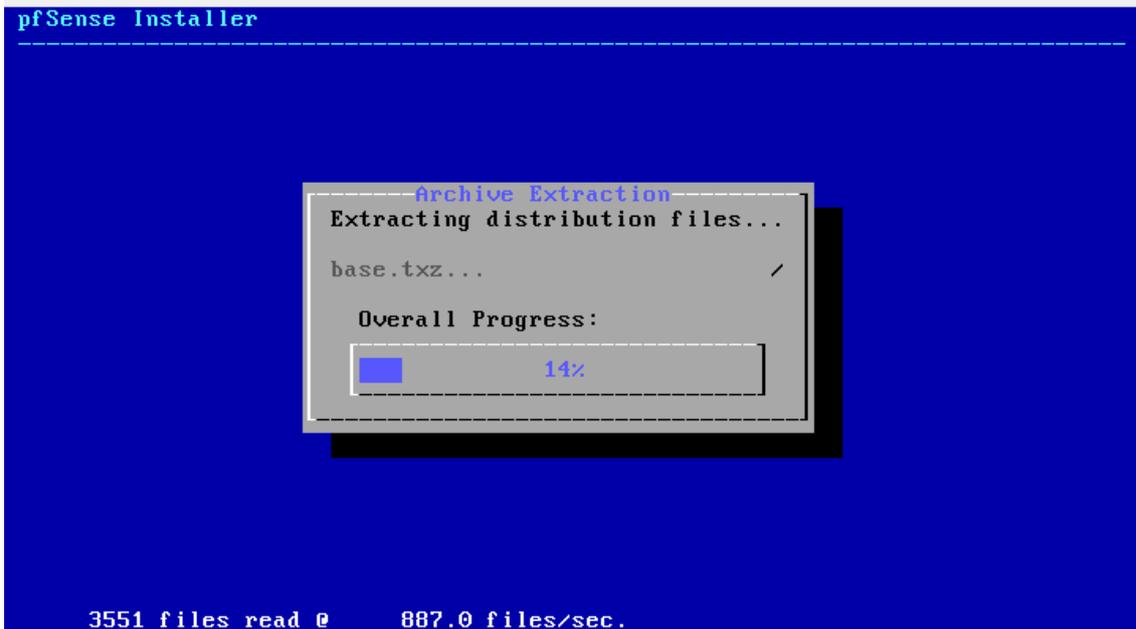
Despues nos pedira que configuremos las particiones, aqui tenemos varias opciones, tenemos las opciones de auto particionado tanto para bios como para uefi la creara unicamente un particion / en el systema de archivos ufs y una linux swap.



Pero tambien tenemos la opción de auto zsh la cual creara el mismo esquema de particiones pero con el sistema de archivos zfs el cual es mucho mas potente y nos ofrece nuevas configuraciones como la de crear raid.

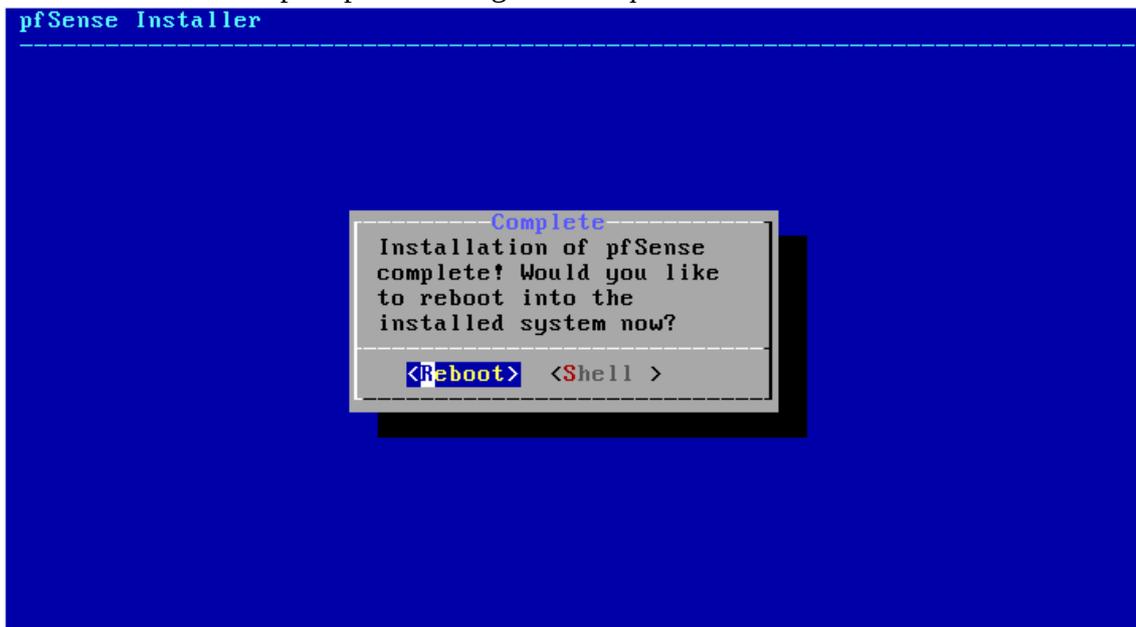


Por ultimo y no menos importante siempre podremos entrar en una configuración manual de las particiones.



Una vez configurado todo esto pararemos a la instalación, una de las cosas que mas me ha sorprendido de pfsense es que se instala en menos de 5 minutos puesto que es un software que pesar de tener muchas funcionalidades es muy liviano.

Tras la instalación nos encontraremos con una pestaña la cual nos pedirá reiniciar o nos ofrecerá un shell para poder configurar cualquier detalle a mano.



Tras reiniciar nos encontraremos que automáticamente a configurado la primera red como WAN y la segunda como Lan.

Esto es un problema puesto que desde la Wan no tenemos reglas creadas para poder acceder a la web de pfsense donde terminaremos la configuración.

Por lo que tendremos que crear dos nuevas reglas en el firewall en la red de wan.

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

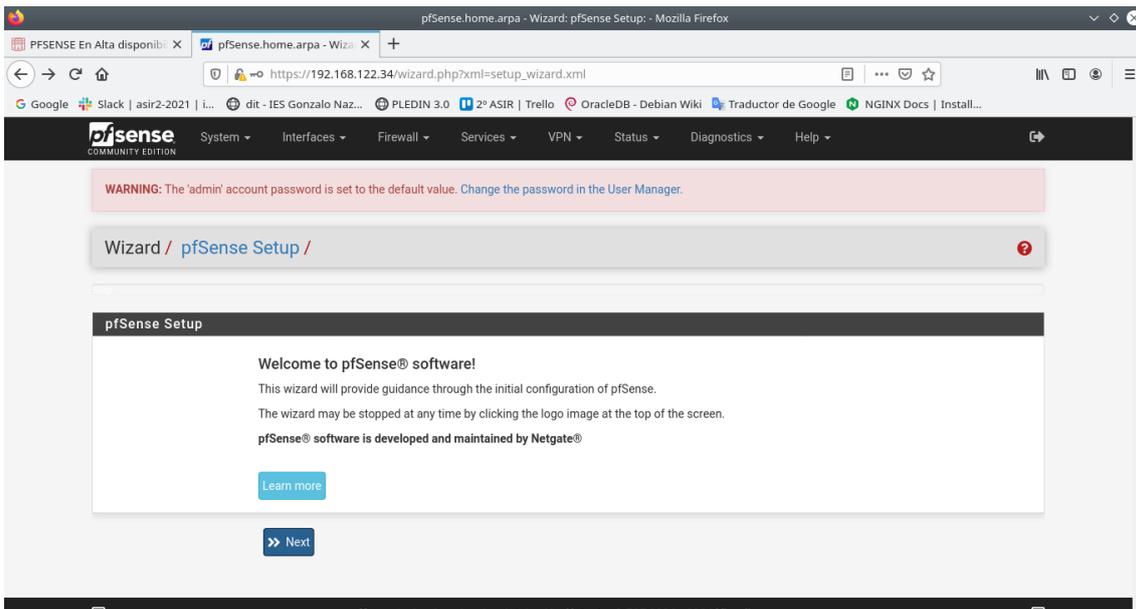
Para ello seleccionaremos la opción 8 y entraremos en la shell de pfsense.

```
easyrule pass wan tcp any any 80
easyrule pass wan tcp any any 443
```

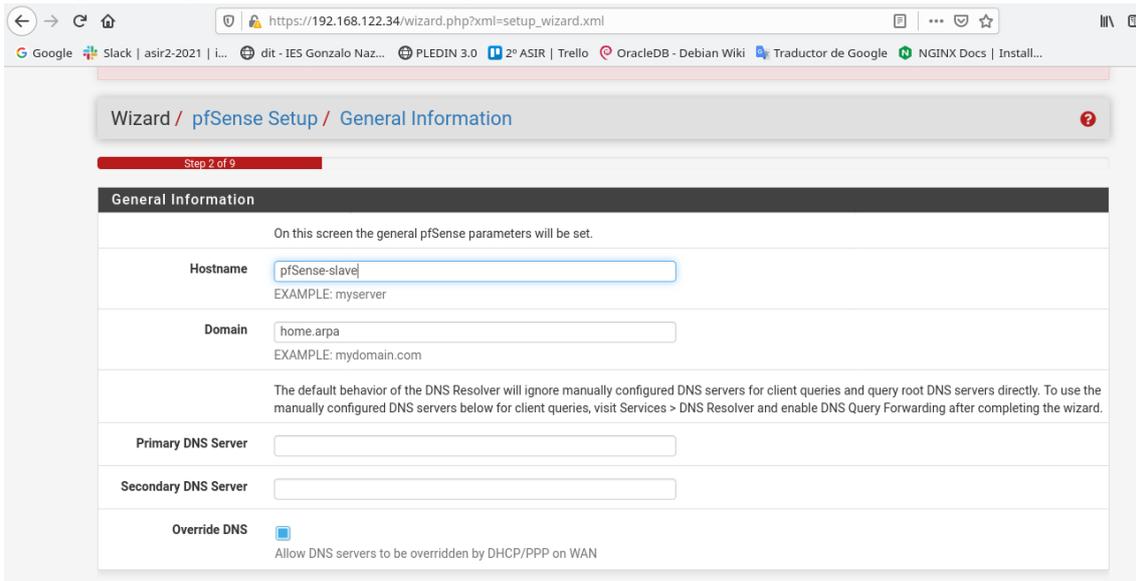
Una vez creadas estas reglas podremos acceder a la pagina de configuración de pfsense.

Lo primero que encontramos es una bienvenida y algunas políticas.
pulsaremos siguiente y seguiremos.

Pfsense alta disponibilidad



Aquí configuraremos el nombre y el dominio.



Luego configuraremos el servidor de hora.

Pfsense alta disponibilidad

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

[Next](#)

Después podremos configurar la interfaz wan, nosotros la dejaremos por defecto.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

General configuration

MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

Por ultimo nos pedirá que cambiemos la contraseña del administrador puesto que por defecto es "pfsense".

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

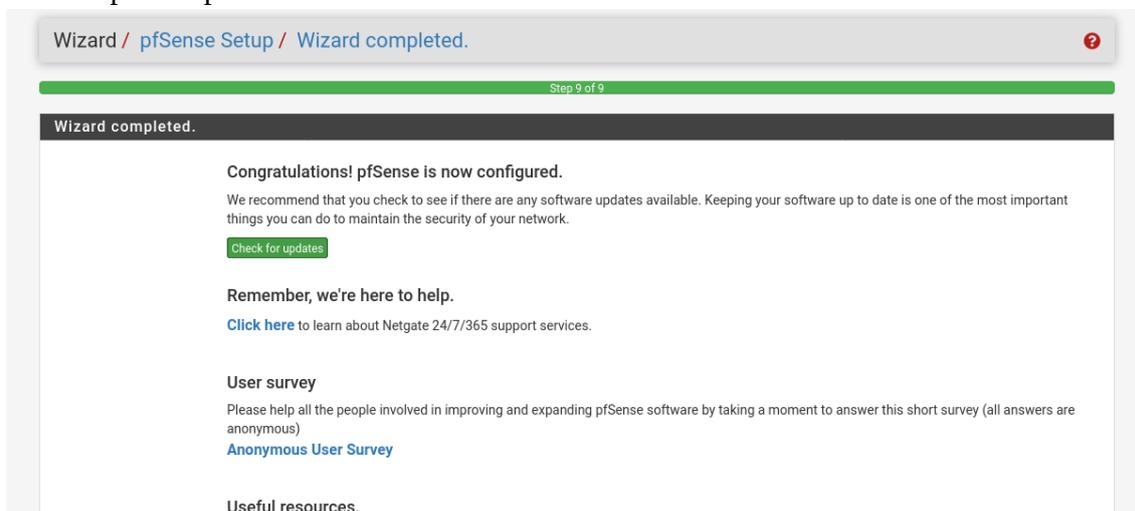
Admin Password

Admin Password AGAIN

[Next](#)

Pfsense alta disponibilidad

Aquí tendremos un resumen de la instalación y si queremos buscar alguna actualización, tras esto el pfsense se reiniciara de nuevo y ya tendremos instalado nuestro primer pfsense.



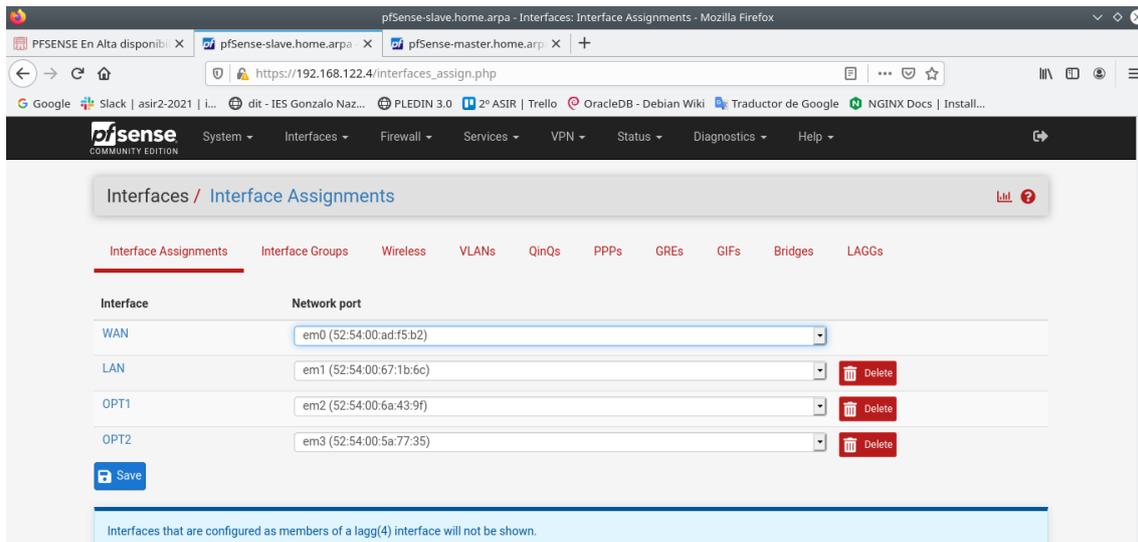
Recordemos que para configurar lo en alta disponibilidad necesitaremos como mínimo otro mas.

1.2 Configuración de pfsense

1.2.1 Configuración de las interfaces

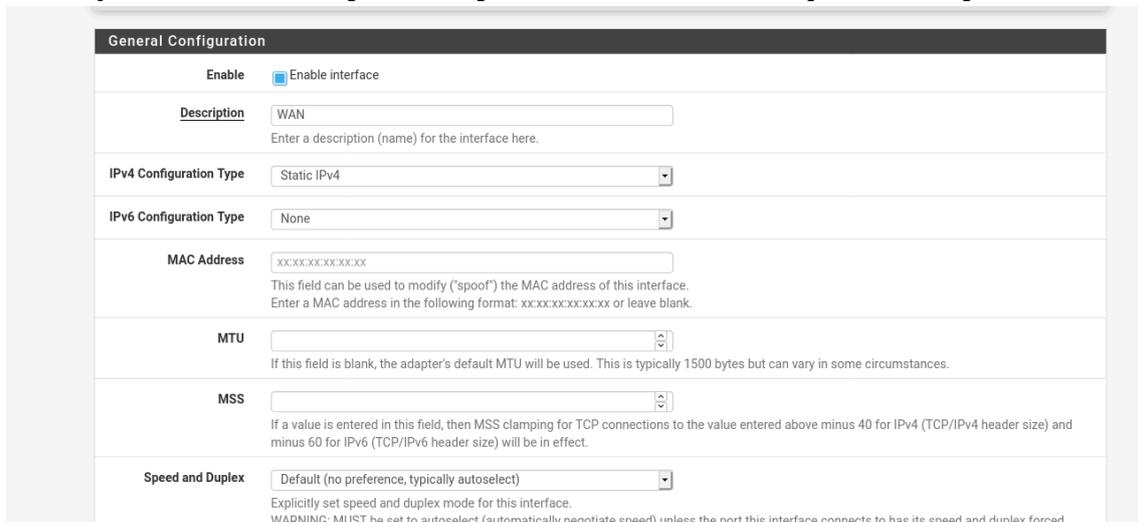
Por defecto en principio solo se abra configurado la red wan y una de las primeras redes, por lo que tendremos que añadir mas.

Para ello iremos a la pestaña Interfaces / Interface / Assignments y añadiremos todas las interfaces.

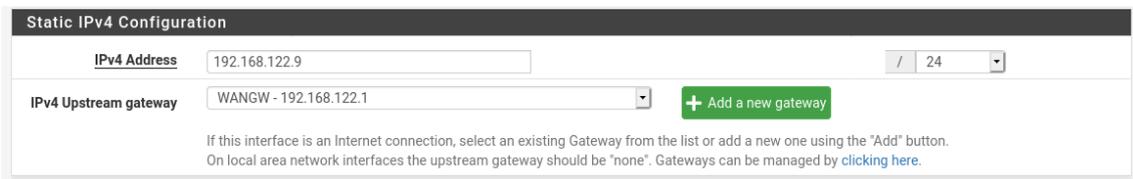


Tras guardarlas iremos a configurarlas 1 a 1 en la pestaña interfaces.

La primera sera la wan la cual la cambiaremos la dirección del dhcp por una ip statica y añadiremos en la pestaña `_ipv4 address_` la dirección que le corresponda.



Pfsense alta disponibilidad



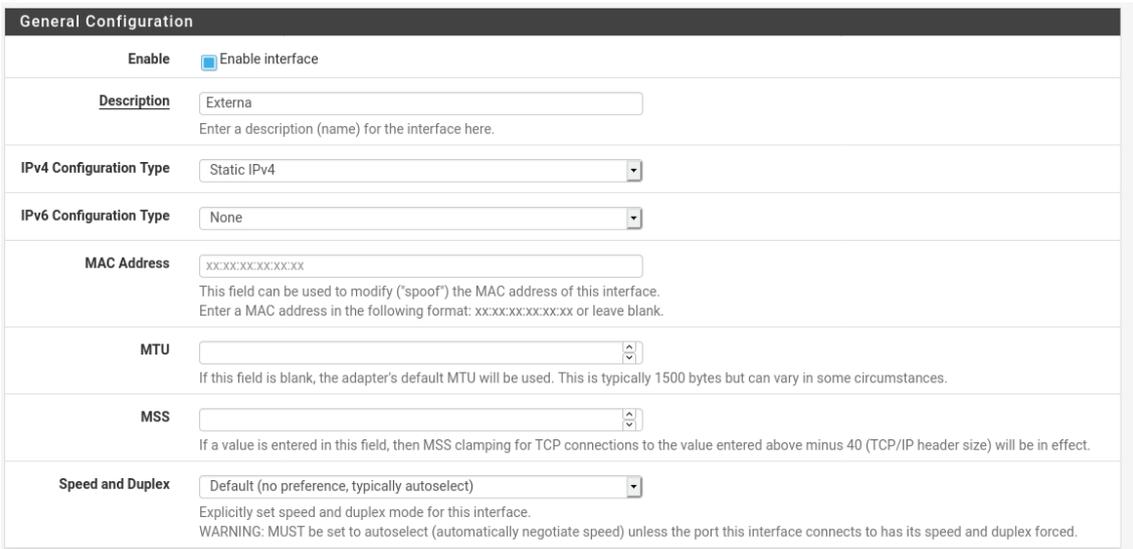
Static IPv4 Configuration

IPv4 Address: 192.168.122.9 / 24

IPv4 Upstream gateway: WANGW - 192.168.122.1 [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Luego en las demás interfaces realizaremos los mismos cambios con sus respectivas ips.



General Configuration

Enable: Enable interface

Description: Externa
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.



Static IPv4 Configuration

IPv4 Address: 10.10.10.102 / 32

IPv4 Upstream gateway: None [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Las interfaces deben quedar asi configuradas.

- Maestro

```
WAN (wan)      -> em0      -> v4: 192.168.122.9/24
EXTERNA (lan)  -> em1      -> v4: 10.10.10.101/24
INTERNA (opt1) -> em2      -> v4: 10.10.20.101/24
PFSYNC (opt2) -> em3      -> v4: 10.10.0.101/24
```

- Esclavo

```
WAN (wan)      -> em0      -> v4: 192.168.122.15/24
EXTERNA (lan)  -> em1      -> v4: 10.10.10.102/24
INTERNA (opt1) -> em2      -> v4: 10.10.20.102/24
PFSYNC (opt2) -> em3      -> v4: 10.10.0.102/24
```

1.2.2 Configuración de High Availability Sync

Lo primero que haremos es ir al cortafuegos y habilitar el trafico en la red que usaran exclusivamente los pfsense.

En mi caso esa sera la tercera red (Pfsync)

The screenshot shows the Pfsense Firewall Rules configuration page for the PFSYNC interface. The breadcrumb trail is "Firewall / Rules / PFSYNC". The interface tabs include Floating, WAN, EXTERNA, INTERNA, and PFSYNC. A table titled "Rules (Drag to Change Order)" contains one rule with the following details:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1 / 486 B	IPv4 *	*	*	*	*	none		Todo el trafico	↓ ↻ 📄 🗑️

Below the table are buttons for "Add" (up and down arrows), "Delete", "Save", and "Separator".

The screenshot shows the "Edit Firewall Rule" page. The breadcrumb trail is "Firewall / Rules / Edit". The configuration fields are as follows:

- Action:** Pass. Description: 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:** PFSYNC. 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:** Any. Choose which IP protocol this rule should match.
- Source:** Invert match. Source Address: any / []

Pfsense alta disponibilidad

Destination

Destination Invert match /

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](#)

Rule Information

Tracking ID	1623520823
Created	6/12/21 18:00:23 by admin@192.168.122.1 (Local Database)
Updated	6/12/21 18:57:08 by admin@192.168.122.1 (Local Database)

[Save](#)

Tras permitir todo el trafico en la red lo siguiente que haremos sera ver que tenemos ping entre la maquina para ello utilizaremos una utilizada de la pagina para realizar los ping, la encontraremos en Diagnostics / ping.

Ping

Hostname

IP Protocol

Source address
Select source address for the ping.

Maximum number of pings
Select the maximum number of pings.

Seconds between pings
Select the number of seconds to wait between pings.

[Ping](#)

Results

```
PING 10.10.0.102 (10.10.0.102): 56 data bytes
64 bytes from 10.10.0.102: icmp_seq=0 ttl=64 time=1.047 ms
64 bytes from 10.10.0.102: icmp_seq=1 ttl=64 time=2.023 ms
64 bytes from 10.10.0.102: icmp_seq=2 ttl=64 time=1.867 ms

--- 10.10.0.102 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.047/1.645/2.023/0.428 ms
```

Pfsense alta disponibilidad

Ping

Hostname	<input type="text" value="10.10.0.101"/>
IP Protocol	<input type="text" value="IPv4"/>
Source address	<input type="text" value="Automatically selected (default)"/> <small>Select source address for the ping.</small>
Maximum number of pings	<input type="text" value="3"/> <small>Select the maximum number of pings.</small>
Seconds between pings	<input type="text" value="1"/> <small>Select the number of seconds to wait between pings.</small>

 Ping

Results

```
PING 10.10.0.101 (10.10.0.101): 56 data bytes
64 bytes from 10.10.0.101: icmp_seq=0 ttl=64 time=0.738 ms
64 bytes from 10.10.0.101: icmp_seq=1 ttl=64 time=1.989 ms
64 bytes from 10.10.0.101: icmp_seq=2 ttl=64 time=1.563 ms

--- 10.10.0.101 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.738/1.410/1.989/0.515 ms
```

Después de comprobar la conexión primero iremos al servidor maestro y realizaremos los siguientes cambios.

Iremos a systema / High Availability Sync

System / High Availability Sync

State Synchronization Settings (pfsync)

Synchronize states pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username
Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System

Pfsense alta disponibilidad

Marcaremos la casilla de `_Synchronize states_`, en `_Synchronize Interface_` añadiremos la interfaz que van a realizar la sincronización y en `_pfsync Synchronize Peer IP_` la ip de la maquina esclava.

Seguidamente en `_Synchronize Config to IP_` añadiremos de nuevo la ip de la maquina esclava, y en `_Remote System_` las credenciales de una cuenta administradora de la maquina esclava.

Synchronize admin synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- WoL Server settings
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal
- Toggle All

Por ultimo seleccionaremos los servicios que se sincronizaran, en mi caso he seleccionado todos.

Tras guardar esta configuración iremos a el servidor esclavo a hacer una configuración similar.

Iremos a la misma pestaña `systema / High Availability Sync`

Pfsense alta disponibilidad

The screenshot shows the pfSense web interface for the 'High Availability Sync' settings. The page title is 'System / High Availability Sync'. The main section is 'State Synchronization Settings (pfsync)'. It includes a checkbox for 'Synchronize states' which is checked, with a description of the pfsync protocol. Below this is a dropdown menu for 'Synchronize Interface' set to 'PFSYNC'. At the bottom, there is a text input field for 'pfsync Synchronize Peer IP' containing '10.10.0.101'.

y configuraremos los dos primeros campos igual que el maestro y en `_pfsync Synchronize Peer IP_` pondremos la ip del maestro.

Tras eso guardaremos y ya deberíamos tener sincronizado los pfsense.

Importante: Puede que tengas errores en la sincronización si algún pfsense no tiene la misma versión que el resto o no utilice el mismo puerto para la interfaz web.

The screenshot shows the 'System Update' page in pfSense. It features a 'Confirmation Required to update pfSense system.' section. A dropdown menu for 'Branch' is set to 'Latest stable version (2.5.x)'. Below this, there are two rows of system information: 'Current Base System' and 'Latest Base System', both showing version '2.5.1'. At the bottom, the 'Status' is indicated as 'Up to date.' in green text.

Recomiendo actualizar los dos pfsense antes de la sincronización

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

Protocol HTTP HTTPS (SSL/TLS)

SSL/TLS Certificate webConfigurator default (60c2587514d65)
Certificates known to be incompatible with use for HTTPS are not included in this list.

TCP port [443]
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes [2]
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect Disable webConfigurator redirect rule
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

Recomiendo que todos estén configurado por https antes de la sincronización

1.2.3 Configuración de Ip Virtuales.

Lo siguiente que haremos sera crear ips virtuales para cuando el servidor maestro o el esclavo se caigan no tener que esperar que los clientes cambien de ip.

Para ello nos iremos en el pfsense maestro a Firewall/Virtual IPs y crearemos la ip virtual de la red wan.

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface WAN

Address type Single address

Address(es) 192.168.122.100 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password. Confirm

VHID Group 1
Enter the VHID group that the machines will share.

Advertising frequency 1 Base 0 Skew
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 IP virtual de wan
A description may be entered here for administrative reference (not parsed).

El tipo de ip seleccionaremos para que utilicé el protocolo CARP, en address añadiremos la ip que vamos a crear, y en virtual ip password pondremos una contraseña.

Pfsense alta disponibilidad

Realizaremos esto tanto con la externa como con la interna.

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface EXTERNA

Address type Single address

Address(es) 10.10.10.100 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password. Confirm

VHID Group 2
Enter the VHID group that the machines will share.

Advertising frequency 1 0
Base Skew
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 IP virtual de externa
A description may be entered here for administrative reference (not parsed).

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface INTERNA

Address type Single address

Address(es) 10.10.20.100 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password. Confirm

VHID Group 3
Enter the VHID group that the machines will share.

Advertising frequency 1 0
Base Skew
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 IP virtual de interna
A description may be entered here for administrative reference (not parsed).

Tras realizar esta configuración en el pfsense maestro podemos probar la configuración de la alta disponibilidad puesto que deberían haberse creado las mismas ips virtuales en el pfsense esclavo.

Virtual IP address	Interface	Type	Description	Actions
192.168.122.100/24 (vhid: 1)	WAN	CARP	IP virtual de wan	
10.10.10.100/24 (vhid: 2)	EXTERNA	CARP	IP virtual de externa	
10.10.20.100/24 (vhid: 3)	INTERNA	CARP	IP virtual de interna	

Tras comprobar esto ya tendremos configurado las virtual ip

1.2.4 Configuración del dhcp

Para configura el dhcp iremos a Services/DHCP Server y ahi realizaremos la siguiente configuración con las redes interna y externa.

WAN **EXTERNA** INTERNA PFSYNC

General Options

Enable Enable DHCP server on EXTERNA interface

BOOTP Ignore BOOTP queries

Deny unknown clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 10.10.10.0

Subnet mask 255.255.255.0

Available range 10.10.10.1 - 10.10.10.254

Range
From To

Marcaremos la señal de enable para activar el servidor dhcp, y configuraremos el rango de ips que queremos que reparta.

Pfsense alta disponibilidad

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	8.8.8.8
	DNS Server 2
	DNS Server 3
	DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

Después configuraremos el Dns

Other Options	
Gateway	10.10.10.100

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Y la puerta de enlace que sera la ip virtual que hemos creado para la red externa.

Por ultimo también configuraremos la red interna igual que la externa.

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on INTERNA interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	Allow all clients <small>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.</small>
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
Ignore client identifiers	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</small>
Subnet	10.10.20.0
Subnet mask	255.255.255.0
Available range	10.10.20.1 - 10.10.20.254
Range	From 10.10.20.2 To 10.10.20.40

Servers

WINS servers WINS Server 1

WINS Server 2

DNS servers 8.8.8.8

DNS Server 2

DNS Server 3

DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

Other Options

Gateway 10.10.20.100

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

1.2.5 Configuración del Snat

Tras configurar el DHCP tendremos que configura el Snat para que los clientes de las redes externas y internas puedan salir a internet.

Para ello iremos a Firewall/NAT/Outbound y crearemos una nueva regla.

Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

Disabled Disable this rule

Do not NAT Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface WAN
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

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

Protocol any
Choose which protocol this rule should match. In most cases "any" is specified.

Source Network 10.10.10.0 / 24
Type Source network for the outbound NAT mapping. Port or Range

Destination Any
Type Destination network for the outbound NAT mapping. Port or Range

Not
Invert the sense of the destination match.

Pfsense alta disponibilidad

La interfaz sera la wan, la red de la que viene la redirección en este caso 10.10.10.0/24

Translation	
Address	192.168.122.100 (IP virtual de wan) <small>Connections matching this rule will be mapped to the specified Address. The Address can be an Interface, a Host-type Alias, or a Virtual IP address.</small>
Port or Range	<input type="text"/> <input type="checkbox"/> Static Port <small>Enter the external source Port or Range used for remapping the original source port on connections matching the rule. Port ranges are a low port and high port number separated by ":". Leave blank when Static Port is checked.</small>
Misc	
No XMLRPC Sync	<input type="checkbox"/> <small>Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.</small>
Description	Nat EXTERNA para WAN <small>A description may be entered here for administrative reference (not parsed).</small>
Rule Information	
Created	6/13/21 17:39:03 by Manual Outbound NAT Switch
Updated	6/14/21 15:50:11 by admin@192.168.122.1 (Local Database)

y tendremos que poner la interfaz de salida la cual es importante que sea la ip virtual que creamos antes.

Luego haremos lo mismo con la red interna.

Firewall / NAT / Outbound / Edit			
Edit Advanced Outbound NAT Entry			
Disabled	<input type="checkbox"/> Disable this rule		
Do not NAT	<input type="checkbox"/> Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules <small>In most cases this option is not required.</small>		
Interface	WAN <small>The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.</small>		
Address Family	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>		
Protocol	any <small>Choose which protocol this rule should match. In most cases "any" is specified.</small>		
Source	Network	10.10.20.0 / 24	<input type="text"/>
	Type	Source network for the outbound NAT mapping.	Port or Range
Destination	Any	<input type="text"/> / 24	<input type="text"/>
	Type	Destination network for the outbound NAT mapping.	Port or Range
	<input type="checkbox"/> Not <small>Invert the sense of the destination match.</small>		

Pfsense alta disponibilidad

Translation

Address

Connections matching this rule will be mapped to the specified Address. The Address can be an Interface, a Host-type Alias, or a Virtual IP address.

Port or Range Static Port

Enter the external source Port or Range used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by ":". Leave blank when Static Port is checked.

Misc

No XMLRPC Sync

Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

Description

A description may be entered here for administrative reference (not parsed).

Rule Information

Created 6/13/21 17:39:03 by Manual Outbound NAT Switch

Updated 6/14/21 15:46:10 by admin@192.168.122.1 (Local Database)

Asi es como tendría que quedar el conjunto de reglas.

Port Forward 1:1 **Outbound** NAT

Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	✓ WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	<input type="button" value="edit"/> <input type="button" value="copy"/>
<input type="checkbox"/>	✓ WAN	127.0.0.0/8	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	<input type="button" value="edit"/> <input type="button" value="copy"/>
<input type="checkbox"/>	✓ WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	<input type="button" value="edit"/> <input type="button" value="copy"/>
<input type="checkbox"/>	✓ WAN	::1/128	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	<input type="button" value="edit"/> <input type="button" value="copy"/>
<input type="checkbox"/>	✓ WAN	10.10.10.0/24	*	*	*	192.168.122.100	*	✗	Nat EXTERNA para WAN	<input type="button" value="edit"/> <input type="button" value="copy"/>
<input type="checkbox"/>	✓ WAN	10.10.20.0/24	*	*	*	192.168.122.100	*	✗	Nat Interna para WAN	<input type="button" value="edit"/> <input type="button" value="copy"/>

1.2.6 Configuración del Alisas

Pfsense ofrece la posibilidad de crear grupos de ips puertos y url para usar en las reglas del firewall.

Crearemos un grupo de puertos que usaremos mas tarde de la siguiente firma.

Iremos a Firewall/Aliases.

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type

Port(s)

Hint Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	Entry added	Action
<input type="text" value="80"/>	Entry added Mon, 14 Jun 2021 08:29:37 +0000	Delete
<input type="text" value="443"/>	Entry added Mon, 14 Jun 2021 08:29:50 +0000	Delete
<input type="text" value="53"/>	Entry added Mon, 14 Jun 2021 08:29:50 +0000	Delete

Añadiremos los puertos necesarios para salir a internet y pulsaremos guardad.

Firewall / Aliases / Ports

IP Ports URLs All

Firewall Aliases Ports

Name	Values	Description	Actions
Internet	80, 443, 53	dar acceso a internet	

1.2.7 Configurar firewall para salir a internet.

Crearemos una nueva regla en la red externa de la siguiente forma.

Entraremos en Firewall / rules y pulsaremos añadir.

Pfsense alta disponibilidad

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 EXTERNA
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 TCP/UDP
Choose which IP protocol this rule should match.

Source

Source Invert match EXTERNA net Source Address /

[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.

Aquí la interface que seleccionaremos sera externa, la familia sera ipv 4 y el protocolo sera tanto udp como tcp, en source dejaremos externa net.

Destination

Destination Invert match any Destination Address /

Destination Port Range (other) Internet (other) Internet
From Custom To 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 habilitar internet en red externa
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](#)

Rule Information

Tracking ID	1623659453
Created	6/14/21 08:30:53 by admin@192.168.122.1 (Local Database)
Updated	6/14/21 15:37:59 by admin@192.168.122.1 (Local Database)

[Save](#)

Por ultimo en destinación port escribiremos `_Internet_` que es el alias que creamos en el apartado anterior.

Para finalizar haremos lo mismo para la red interna.

Pfsense alta disponibilidad

Firewall / Rules / Edit

Edit Firewall Rule

Action
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
Choose the interface from which packets must come to match this rule.

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

Protocol
Choose which IP protocol this rule should match.

Source

Source Invert match /

[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 /

Destination Port Range
From Custom To 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](#)

Rule Information

Tracking ID	1623672068
Created	6/14/21 12:01:08 by admin@192.168.122.1 (Local Database)
Updated	6/14/21 12:01:08 by admin@192.168.122.1 (Local Database)

[Save](#)

Asi es como tendría que quedar

Pfsense alta disponibilidad

Firewall / Rules / EXTERNA

Floating WAN **EXTERNA** INTERNA PFSYNC

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 50.09 MiB	IPv4 TCP/UDP	EXTERNA net	*	*	Internet	*	none	habilitar internet en red externa	   

 Add  Add  Delete  Save  Separator



Firewall / Rules / INTERNA

Floating WAN EXTERNA **INTERNA** PFSYNC

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 934.90 MiB	IPv4 TCP/UDP	INTERNA net	*	*	Internet	*	none	dar acceso a internet	   

 Add  Add  Delete  Save  Separator

