

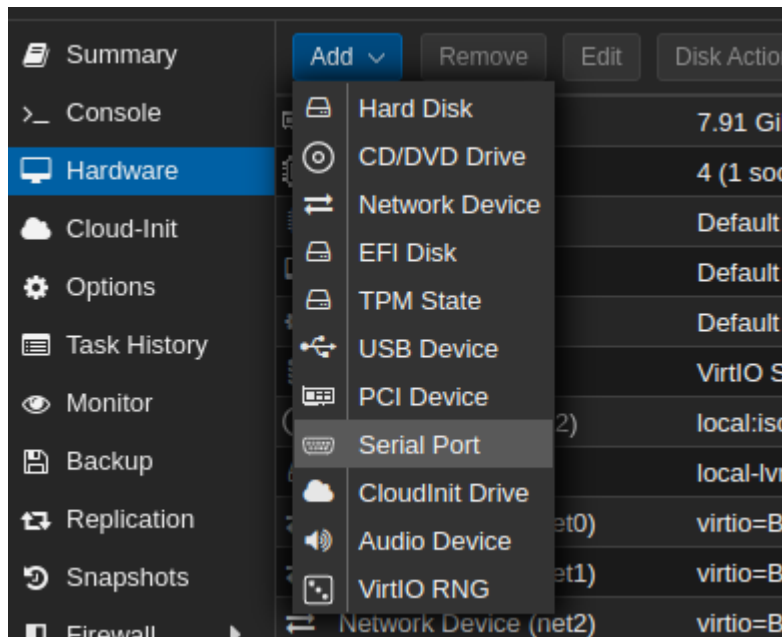
Implementación de alta disponibilidad WAN en calisto

Índice

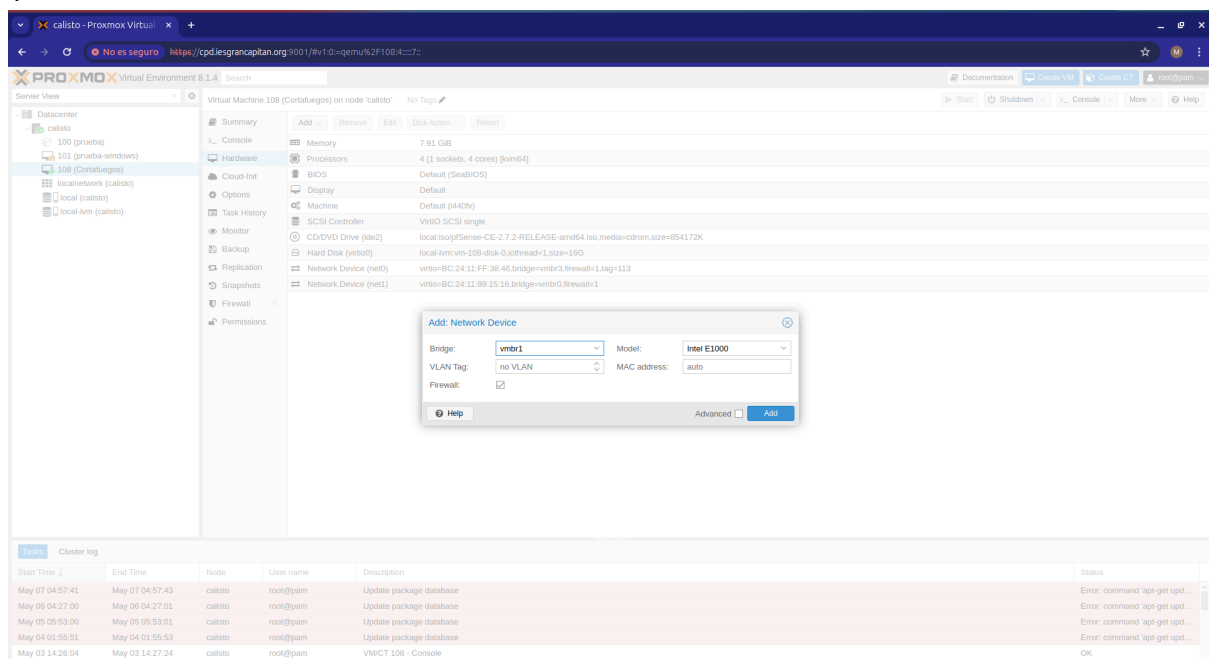
1. Añadimos la NIC.....	3
2. Configuración de interfaz.....	4
3. Creación de los Gateway.....	5
4. Creación de reglas firewall.....	7

1. Añadimos la NIC

Para añadir nuestra tarjeta de red debemos situarnos en la pestaña de hardware y seleccionamos añadir:



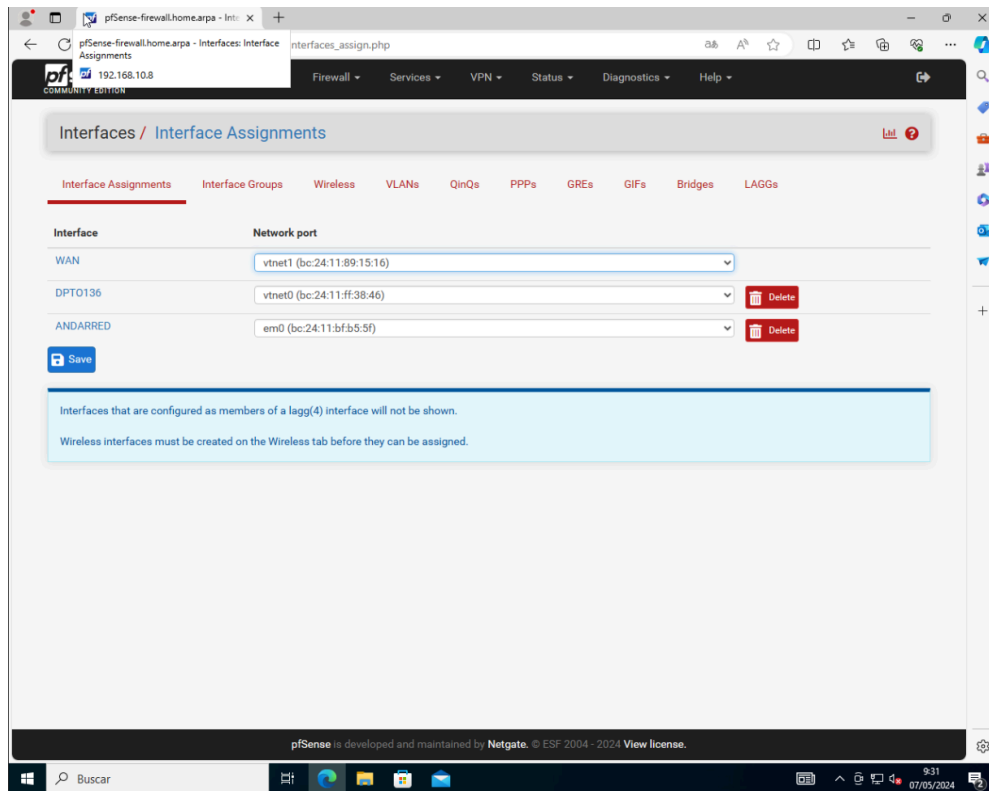
Seleccionamos Network Device y una vez allí seleccionamos en el desplegable la NIC que queremos añadir, en mi caso la de Andared:



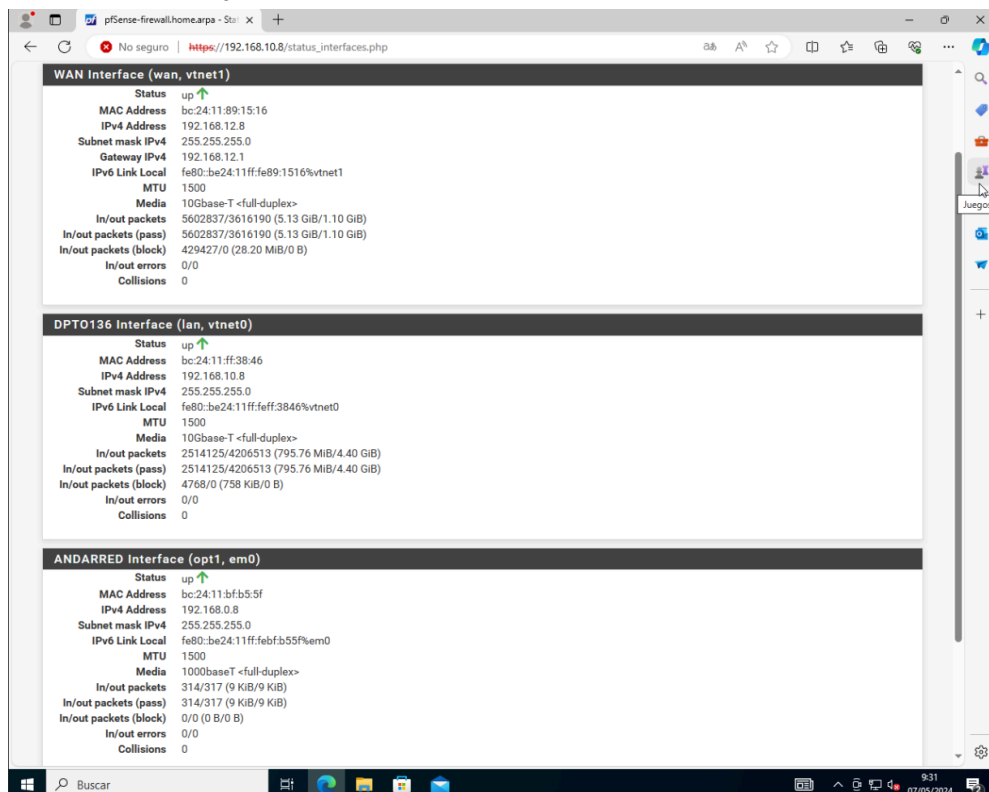
Una vez añadida la NIC ya podemos disponernos a entrar en nuestro firewall y configurar dicha interfaz.

2. Configuración de interfaz.

Al igual que ocurre con el laboratorio que monté, debemos de asignar las interfaces a las NIC, así que nos disponemos en interfaces > assignment y quedarán de la siguiente manera:

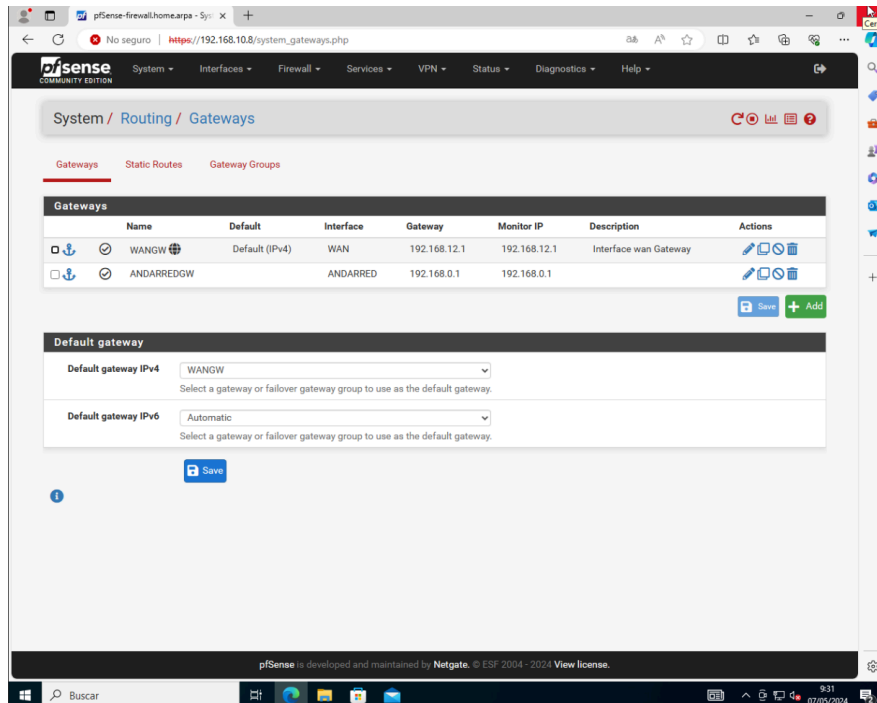


La interfaz queda configurada con la IP, DNS y gateway necesarios según se me pide en mi paquete de trabajo:



3. Creación de los Gateway.

Ahora debemos de crear una Gateway nueva para nuestra interfaz ANDARED, para ello nos situamos en System > Routing > Gateway, y ahí creamos las Gateway según se pide en el paquete de trabajo:



Una vez creadas las interfaces debemos de configurar el grupo de gateway, dicho grupo nos servirá más tarde para configurar el balanceo de carga entre ambas interfaces la de informática y la de andared, para ello vamos a gateway groups y establecemos la siguiente configuración:

System / Routing / Gateway Groups / Edit

Edit Gateway Group Entry

Group Name

Gateway

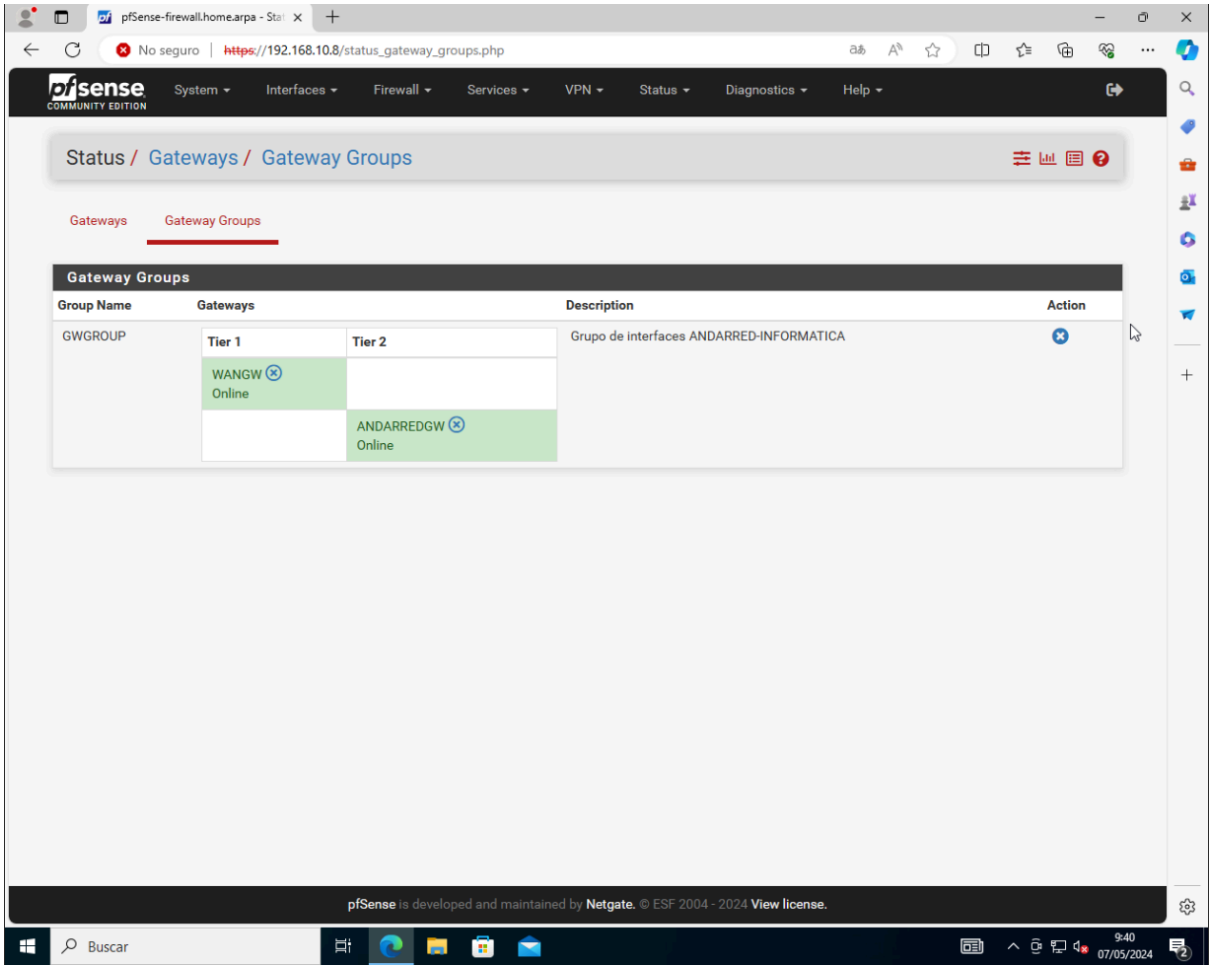
Gateway	Tier	Interface	Virtual IP	Description
WANGW	Tier 1	Interface	Interface wan Gateway	
ANDARREDGW	Tier 2	Interface	Group Name	

Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.

Virtual IP The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.

Trigger Level When to trigger exclusion of a member

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



4. Creación de reglas firewall.

Ahora debemos de crear las reglas que obligarán a al tráfico de la LAN a circular por el grupo de gateway, para ello nos disponemos a firewall > rules y creamos la siguiente regla:

The screenshot shows the 'Edit Firewall Rule' page in the pfSense web interface. The browser address bar shows the URL: https://192.168.10.8/firewall_rules_edit.php?fif=lan&after=-1. The page has a dark header with the pfSense logo and navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Firewall / Rules / Edit' and contains the 'Edit Firewall Rule' form.

The form fields are as follows:

- Action:** Pass (dropdown menu). Hint: 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:** DPT0136 (dropdown menu). Choose the interface from which packets must come to match this rule.
- Address Family:** IPv4 (dropdown menu). Select the Internet Protocol version this rule applies to.
- Protocol:** Any (dropdown menu). Choose which IP protocol this rule should match.
- Source:**
 - Source:** ☐ Invert match. DPT0136 subnets (dropdown menu). Source Address: / (dropdown menu).
- Destination:**
 - Destination:** ☐ Invert match. Any (dropdown menu). Destination Address: / (dropdown menu).
- 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:** (text input field). 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.
- Any flags:** ☐ Any flags. Use this to choose TCP flags that must be set or cleared for this rule to match.
- No pfSync:** ☐ Prevent states created by this rule to be synced over pfync.
- State type:** Keep (dropdown menu). Keep: works with all IP protocols.
- No XMLRPC Sync:** ☐ Prevent the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
- VLAN Prio:** none (dropdown menu). Choose 802.1p priority to match on.
- VLAN Prio Set:** none (dropdown menu). Choose 802.1p priority to apply.
- Schedule:** none (dropdown menu). Leave as 'none' to leave the rule enabled all the time.
- Gateway:** GWGROUP - Grupo de interfaces ANDARRED-INFORMATICA (dropdown menu). Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing. Gateway selection is not valid for 'IPv4+IPv6' address family.
- In / Out pipe:** none (dropdown menu). Choose the Out queue/Virtual interface only if In is also selected. The Out selection is applied to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface. If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out the selections are reversed, Out is for incoming and In is for outgoing.
- Ackqueue / Queue:** none (dropdown menu). Choose the Acknowledge Queue only if there is a selected Queue.

A 'Save' button is located at the bottom of the form.

Como se puede ver hace que todo el tráfico saliente de la LAN sea obligado a circular por el grupo de gateway.
Quedando de la siguiente manera, es importante ponerla la primera de todas ya que las reglas están ordenadas por orden de prioridad:

