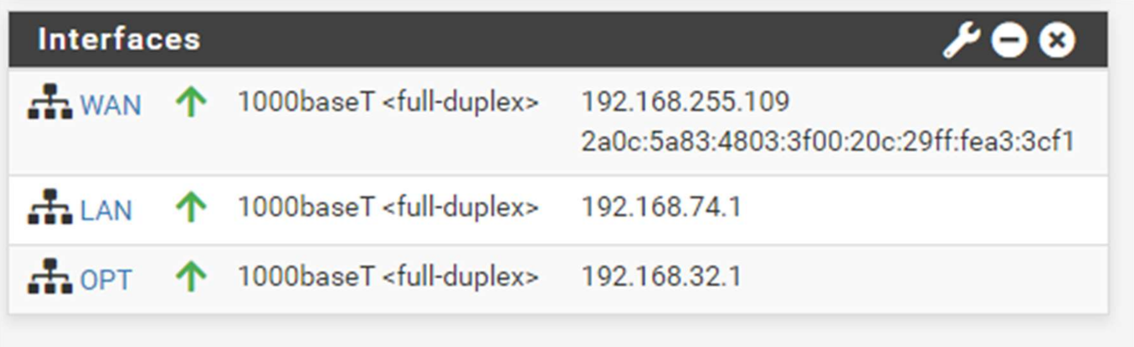
Diseño general de pfSense sobre Proxmox

Índice

1. Instalación pfSense

La instalación que seguiremos es la común, solo que añadiremos la interfaz OPT para poder acceder al servidor de máquinas virtuales.

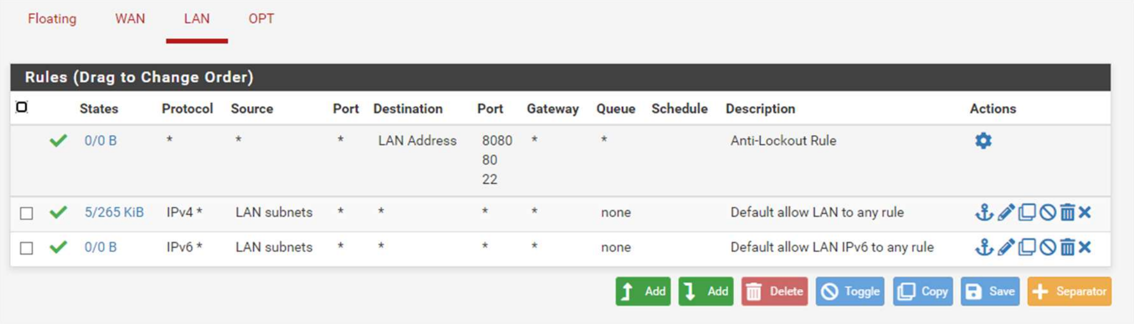


Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.255.109 2a0c:5a83:4803:3f00:20c:29ff:fea3:3cf1
LAN	↑	1000baseT <full-duplex>	192.168.74.1
OPT	↑	1000baseT <full-duplex>	192.168.32.1

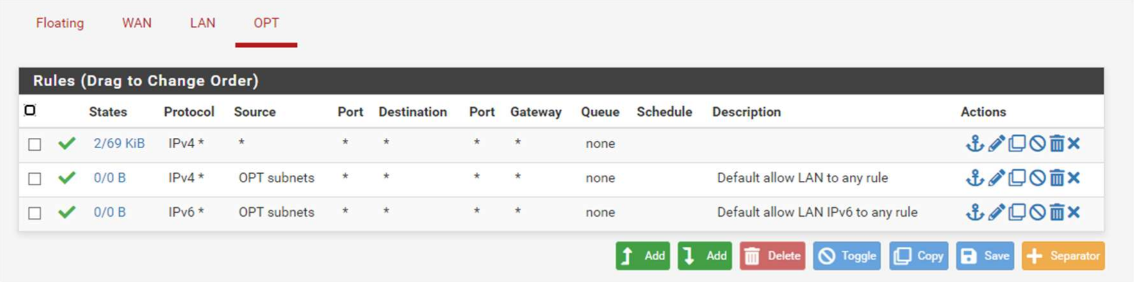
2. Configuración Firewall

Para que las máquinas puedan acceder a internet para actualización de paquetes permitimos el tráfico en las interfaces LAN y OPT, cuando queramos securizar se cambiarán las reglas.



Rules (Drag to Change Order)

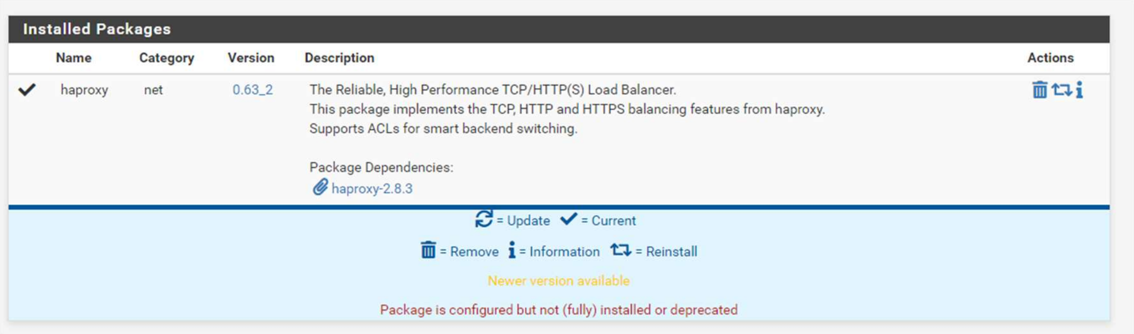
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/0 B	*	*	*	LAN Address	8080 80 22	*	*		Anti-Lockout Rule	
□	✓	5/265 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	2/69 KiB	IPv4 *	*	*	*	*	*	none			
□	✓	0/0 B	IPv4 *	OPT subnets	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0/0 B	IPv6 *	OPT subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

3. Instalación HAProxy

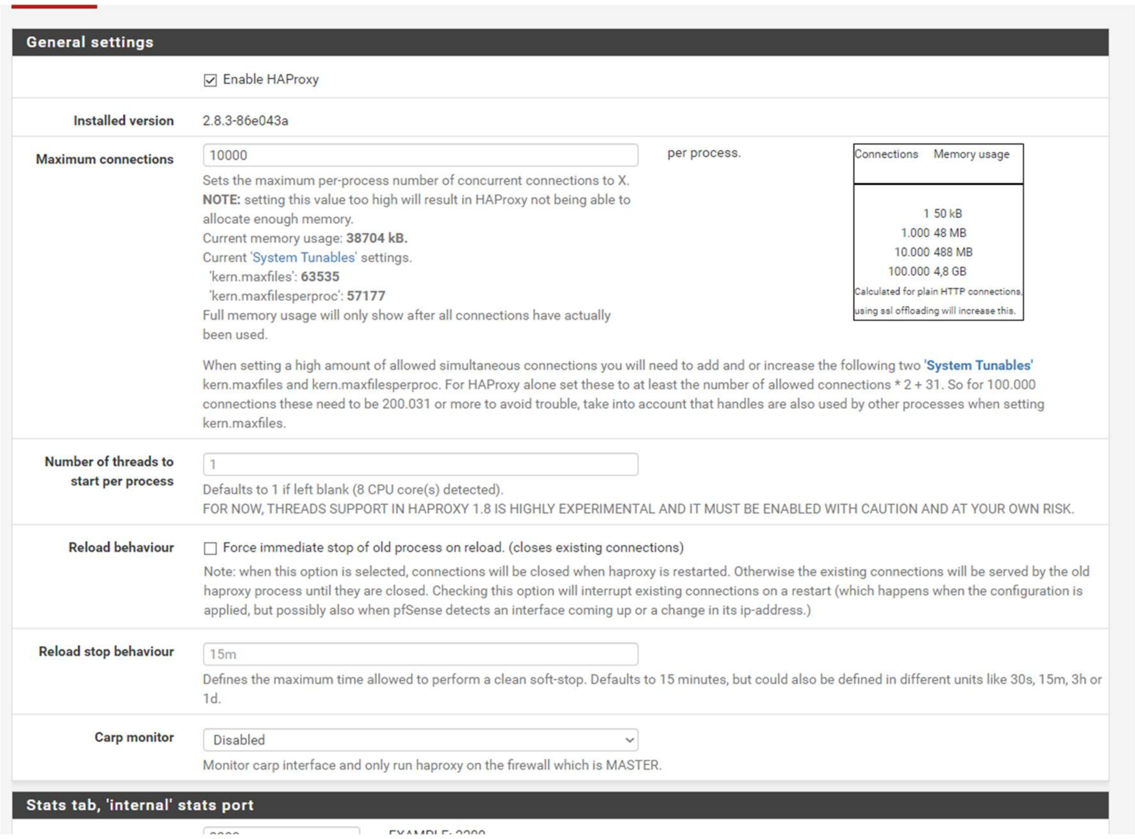


Installed Packages

	Name	Category	Version	Description	Actions
✓	haproxy	net	0.63_2	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching. Package Dependencies: haproxy-2.8.3	

= Update ✓ = Current
= Remove = Information = Reinstall
Newer version available
Package is configured but not (fully) installed or deprecated

Activamos el paquete y establecemos un número máximo de conexiones.



General settings

☑ Enable HAProxy

Installed version 2.8.3-86e043a

Maximum connections 10000 per process.

Sets the maximum per-process number of concurrent connections to X.
NOTE: setting this value too high will result in HAProxy not being able to allocate enough memory.
Current memory usage: **38704 kB.**
Current 'System Tunables' settings.
'kern.maxfiles': **63535**
'kern.maxfilesperproc': **57177**
Full memory usage will only show after all connections have actually been used.

Connections	Memory usage
1	50 kB
1.000	48 MB
10.000	488 MB
100.000	4,8 GB

Calculated for plain HTTP connections, using ssl offloading will increase this.

When setting a high amount of allowed simultaneous connections you will need to add and or increase the following two **'System Tunables'** kern.maxfiles and kern.maxfilesperproc. For HAProxy alone set these to at least the number of allowed connections * 2 + 31. So for 100.000 connections these need to be 200.031 or more to avoid trouble, take into account that handles are also used by other processes when setting kern.maxfiles.

Number of threads to start per process 1

Defaults to 1 if left blank (8 CPU core(s) detected).
FOR NOW, THREADS SUPPORT IN HAPROXY 1.8 IS HIGHLY EXPERIMENTAL AND IT MUST BE ENABLED WITH CAUTION AND AT YOUR OWN RISK.

Reload behaviour ☐ Force immediate stop of old process on reload. (closes existing connections)

Note: when this option is selected, connections will be closed when haproxy is restarted. Otherwise the existing connections will be served by the old haproxy process until they are closed. Checking this option will interrupt existing connections on a restart (which happens when the configuration is applied, but possibly also when pfSense detects an interface coming up or a change in its ip-address.)

Reload stop behaviour 15m

Defines the maximum time allowed to perform a clean soft-stop. Defaults to 15 minutes, but could also be defined in different units like 30s, 15m, 3h or 1d.

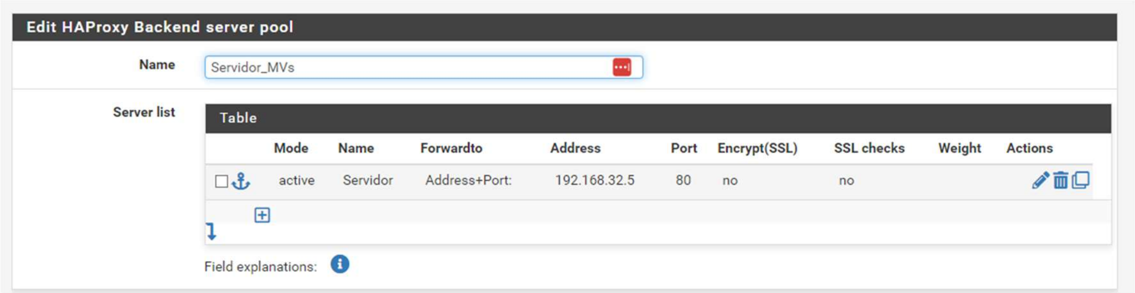
Carp monitor Disabled

Monitor carp interface and only run haproxy on the firewall which is MASTER.

Stats tab, 'internal' stats port

3.1. Backend

Creamos un nuevo backend que apunte al servidor de MVs, con IP 192.168.32.5.



Edit HAProxy Backend server pool

Name Servidor_MVs

Server list

Table

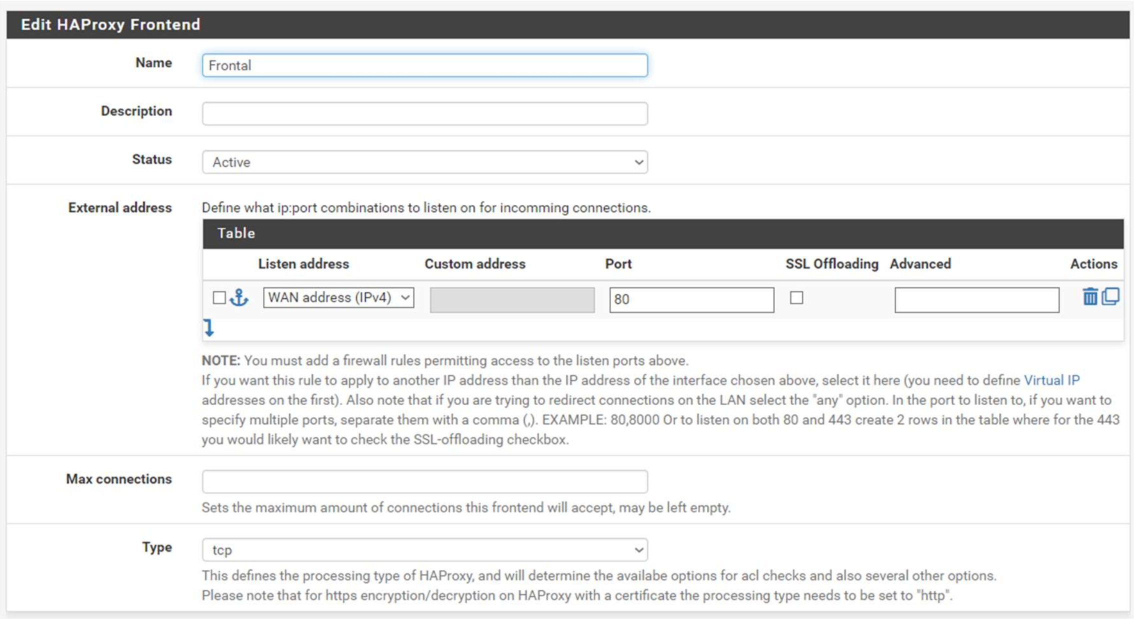
	Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
☐	active	Servidor	Address+Port:	192.168.32.5	80	no	no		

Field explanations:

Establecemos un nombre a la pool de servers, el nombre del servidor en modo activo, la dirección y puerto.

3.2. Frontend

Creamos el frontend, que apuntará a la interfaz WAN por el puerto 80.



Edit HAProxy Frontend

Name	Frontal
Description	
Status	Active
External address	Define what ip:port combinations to listen on for incomming connections.

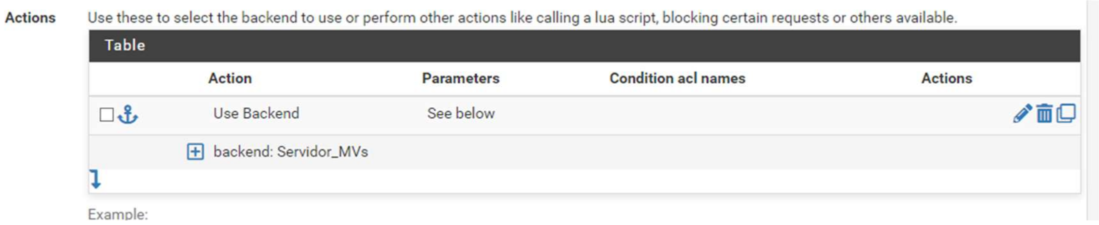
Table

	Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
□ ⚓	WAN address (IPv4)		80	□		

NOTE: You must add a firewall rules permitting access to the listen ports above.
If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define Virtual IP addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections	Sets the maximum amount of connections this frontend will accept, may be left empty.
Type	tcp This defines the processing type of HAProxy, and will determine the availabe options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

Importante seleccionar el tipo de frontend, en este caso tcp, ya que si no, no funcionará. Y en acciones, elegir USE BACKEND, y seleccionamos el servidor backend.



Actions — Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

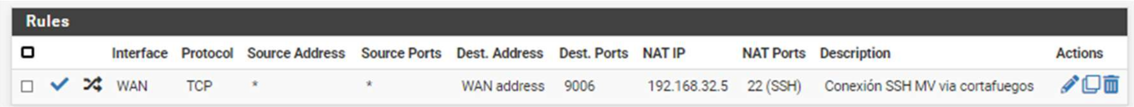
Table

	Action	Parameters	Condition acl names	Actions
□ ⚓	Use Backend	See below		
	⊞ backend: Servidor_MVs			

Example:

4. Redirección puerto pfSense

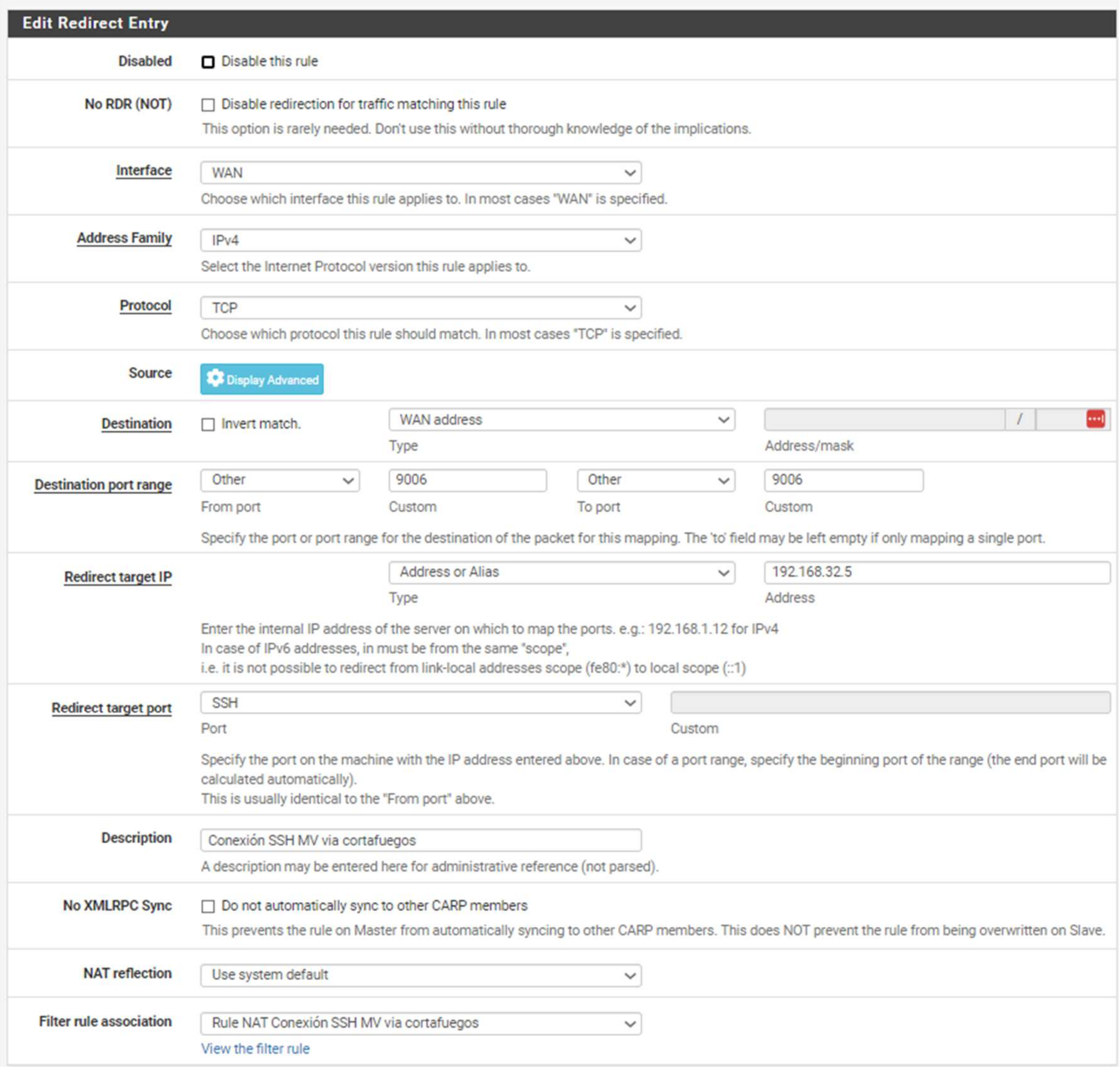
Para la redirección de puertos basta con acceder al apartado port forward en la configuración NAT, en firewall.



Rules

□			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP	*	*	WAN address	9006	192.168.32.5	22 (SSH)	Conexión SSH MV via cortafuegos	

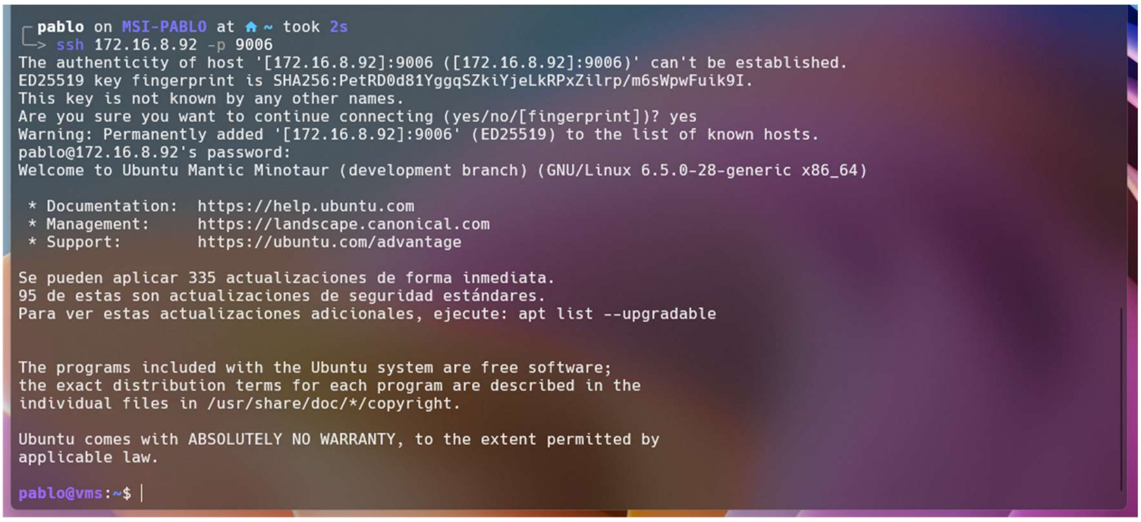
En este caso he configurado la regla para que desde el puerto 9006 de la WAN acceda al 22 de la máquina de red de MVs.



Edit Redirect Entry

Disabled	□ Disable this rule
No RDR (NOT)	□ Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface	WAN Choose which interface this rule applies to. In most cases "WAN" is specified.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which protocol this rule should match. In most cases "TCP" is specified.
Source	Display Advanced
Destination	□ Invert match. · Type: WAN address · Address/mask: /
Destination port range	From port: Other · Custom: 9006 · To port: Other · Custom: 9006 Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP	Type: Address or Alias · Address: 192.168.32.5 Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, in must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)
Redirect target port	Port: SSH · Custom: Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.
Description	Conexión SSH MV via cortafuegos A description may be entered here for administrative reference (not parsed).
No XMLRPC Sync	□ Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	Use system default
Filter rule association	Rule NAT Conexión SSH MV via cortafuegos View the filter rule

Si hacemos un ssh al puerto 9006 del pfsense, nos abrirá el acceso:



```
┌ pablo on MSI-PABLO at ⌂ ~ took 2s
└─> ssh 172.16.8.92 -p 9006
The authenticity of host '[172.16.8.92]:9006 ([172.16.8.92]:9006)' can't be established.
ED25519 key fingerprint is SHA256:PetRD0d81YggqSZkiYjeLkRPxZilrp/m6sWpwFuik9I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.16.8.92]:9006' (ED25519) to the list of known hosts.
pablo@172.16.8.92's password:
Welcome to Ubuntu Mantic Minotaur (development branch) (GNU/Linux 6.5.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Se pueden aplicar 335 actualizaciones de forma inmediata.
95 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

pablo@vms:~$ |
```