Practica Examen con PFSense

Configuración inicial.

Asignación de interfaces WAN Y LAN.

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em0 a or nothing if finished): em0

The interfaces will be assigned as follows:

WAN  -> em1
LAN  -> em0

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
```

IP del router(WAN).

```
Enter an option: 2

Available interfaces:

1 - WAN (em1 - static)
2 - LAN (em0)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 172.16.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

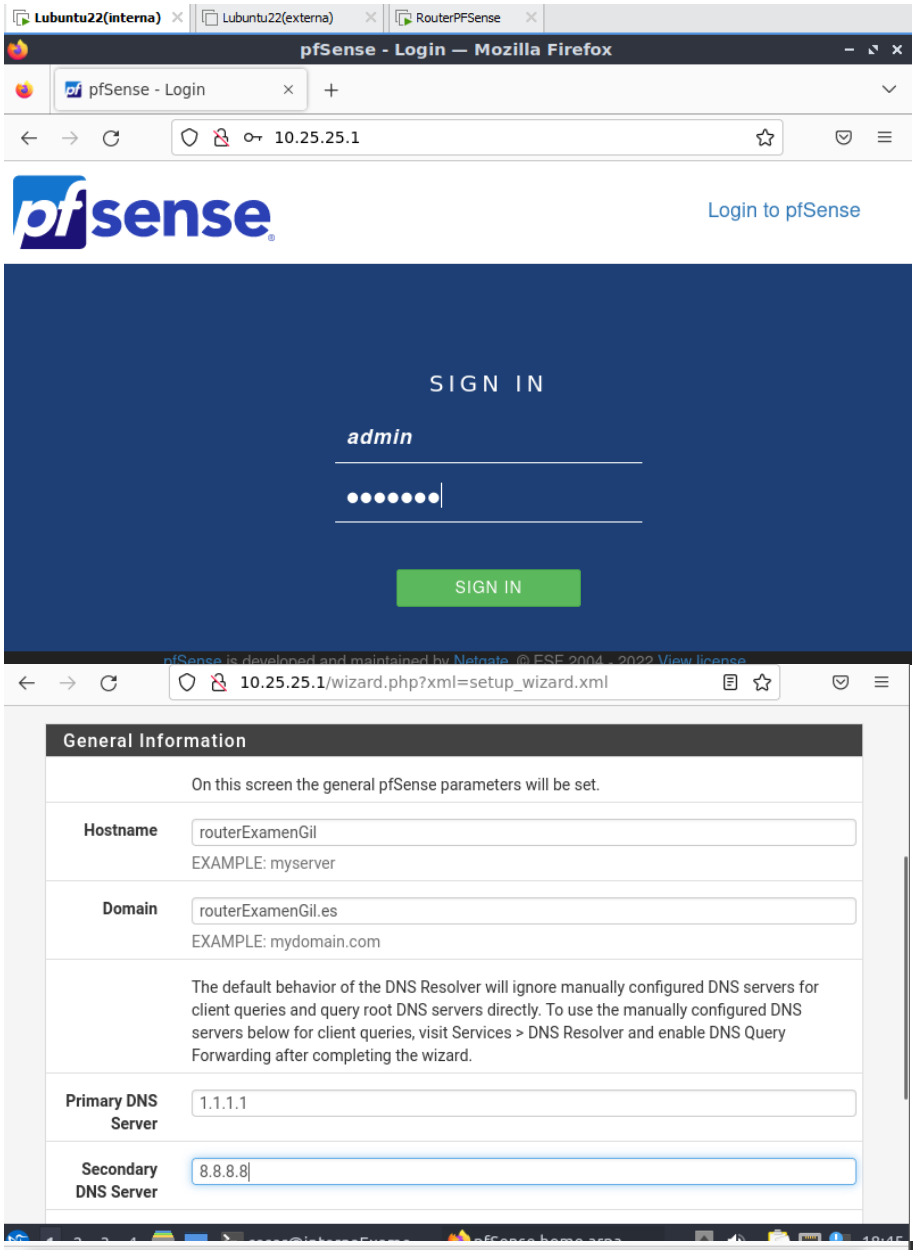
IP del router(WAN).

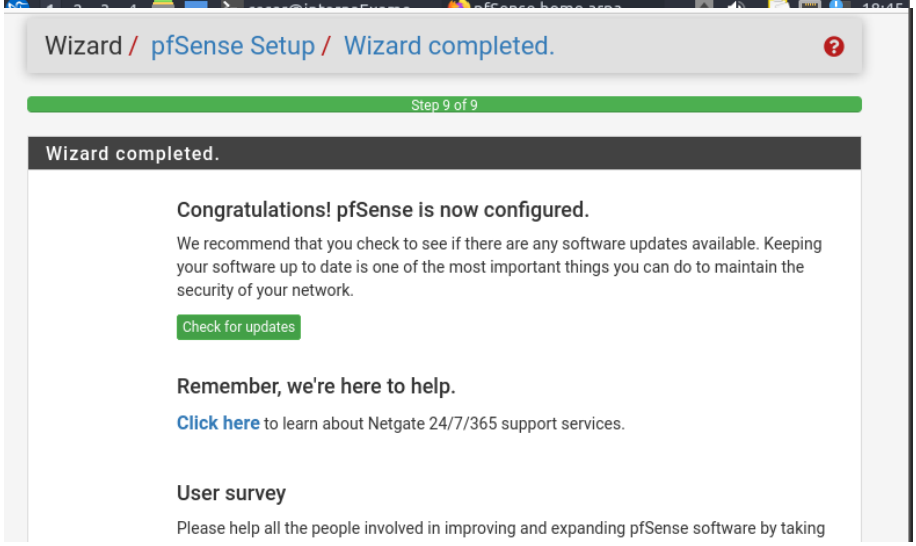
```
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em1 - static)
2 - LAN (em0)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.25.25.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 8

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

IP a la que hay que acceder desde el cliente interno para configurar el firewall con interfaz grafica.

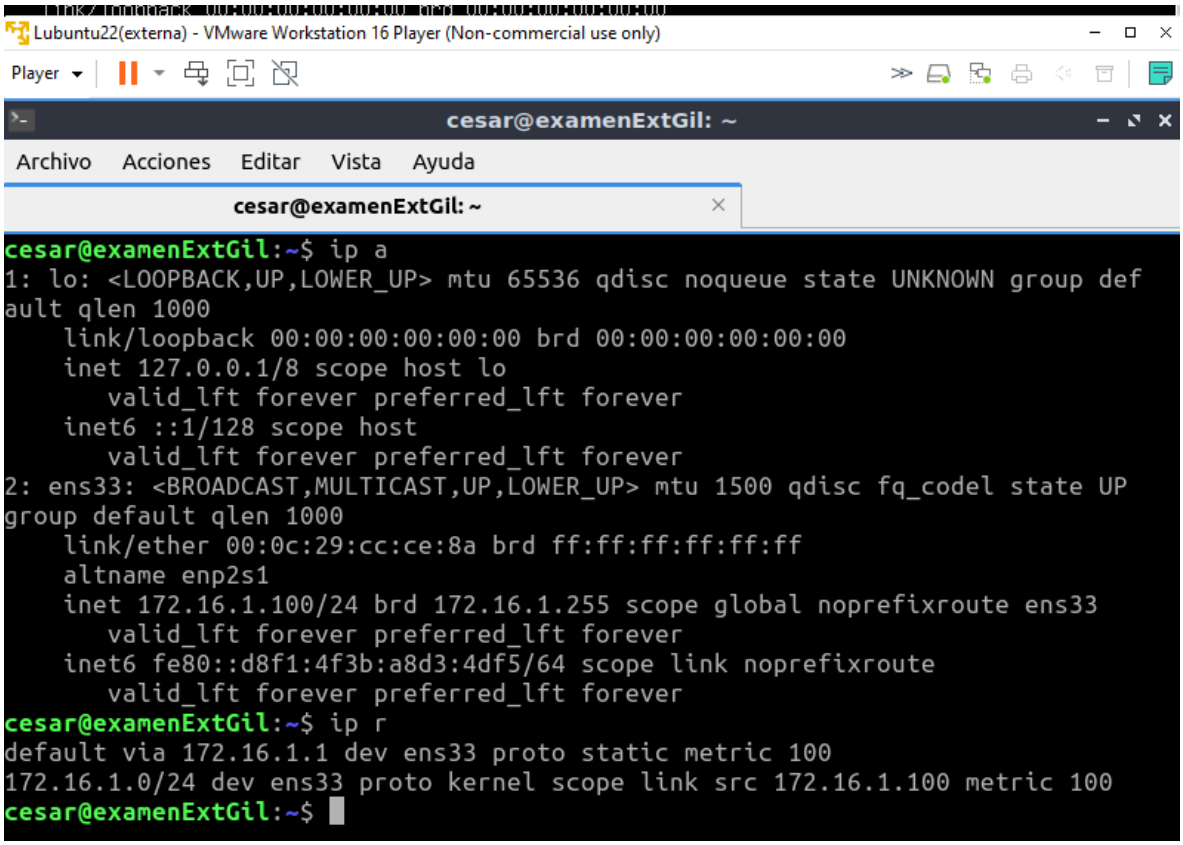
```
The IPv4 LAN address has been set to 10.25.25.1/8
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://10.25.25.1/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 63756e9ccd80a70693f5

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em1        -> v4: 172.16.1.1/24
 LAN (lan)       -> em0        -> v4: 10.25.25.1/8

 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) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Login PFSense.

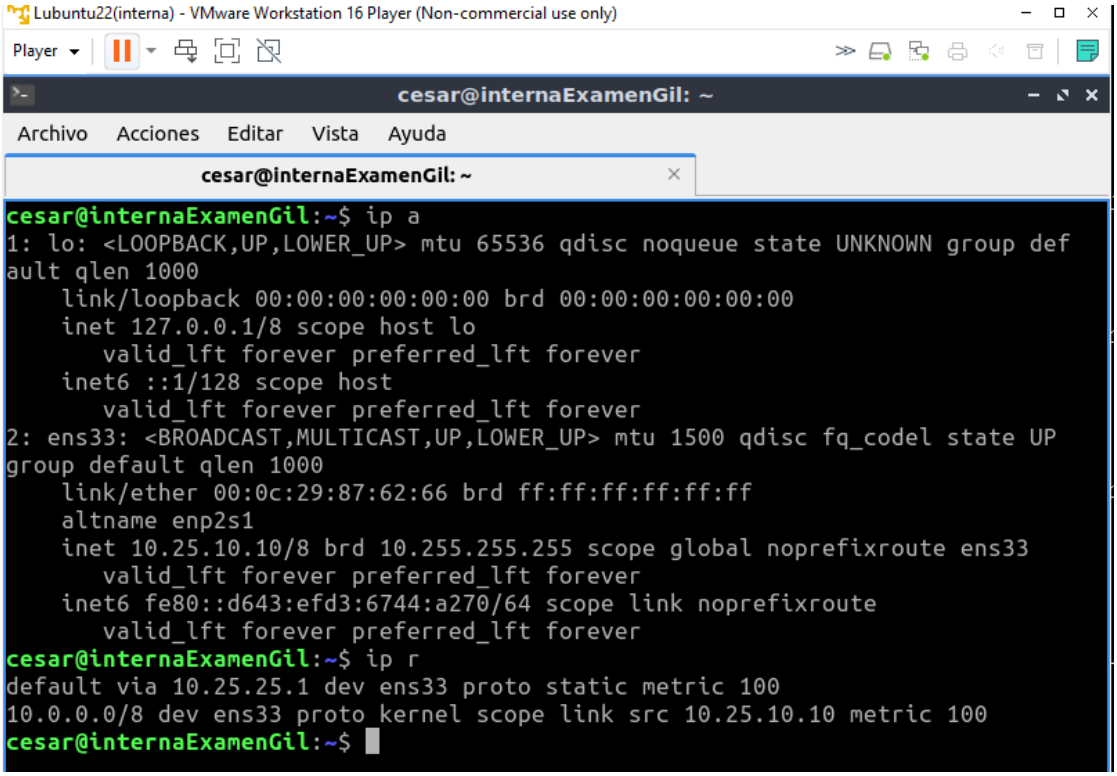




IP del cliente.

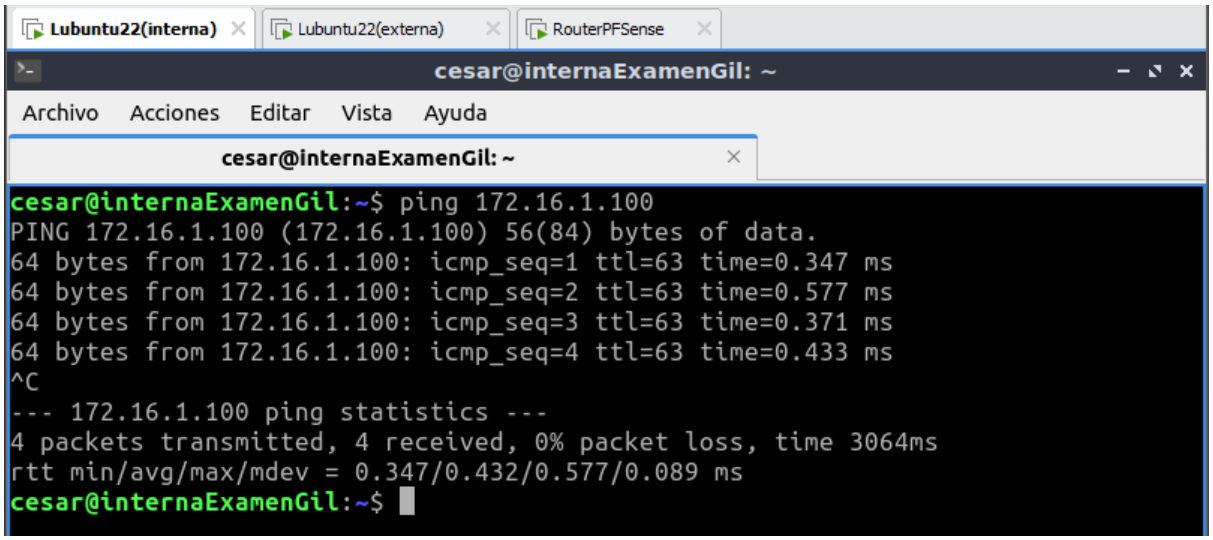


IP del servidor.



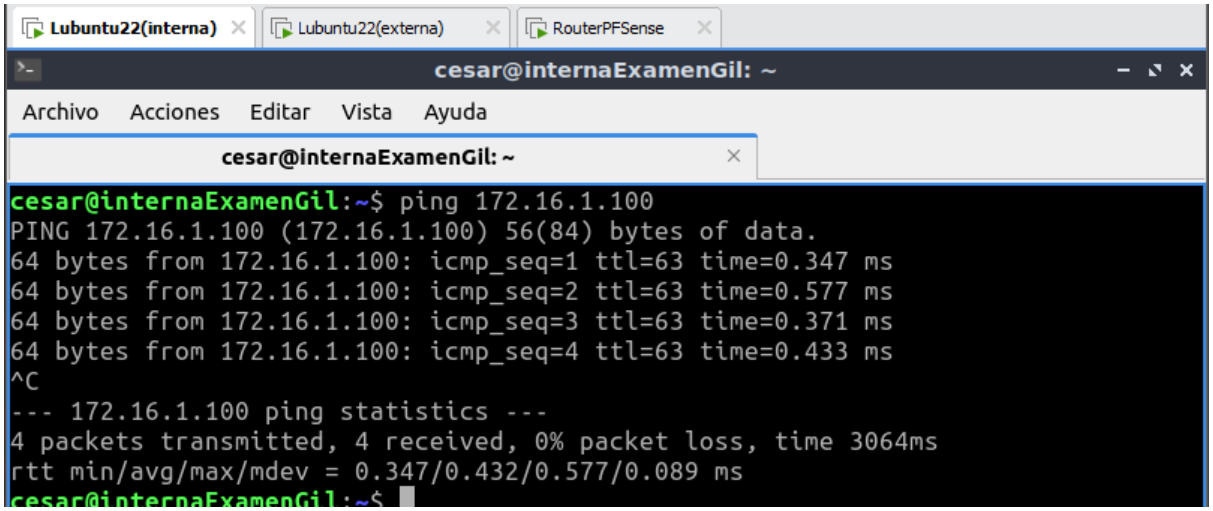
Ping interno a externo con todo en ACCEPT.

Captura del ping.

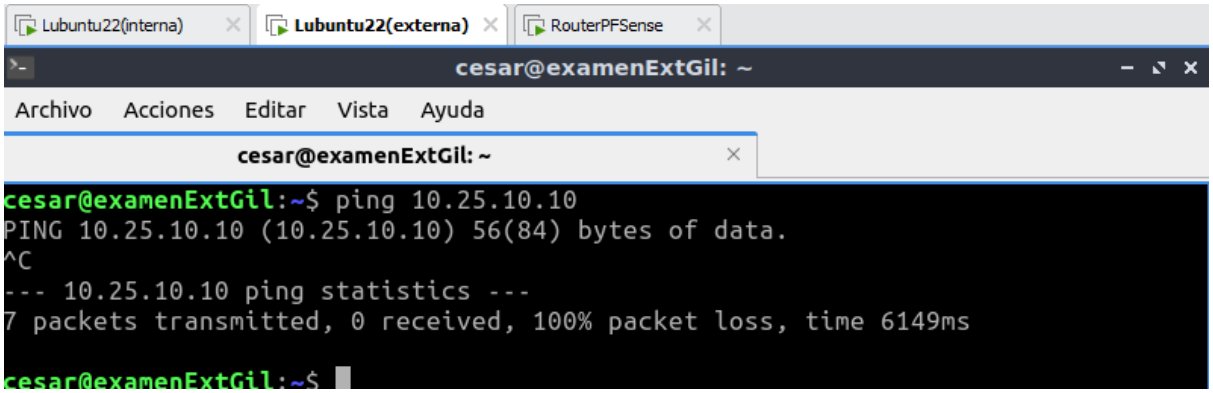


Con todo en DROP,Ping interno a externo pero al revés no.

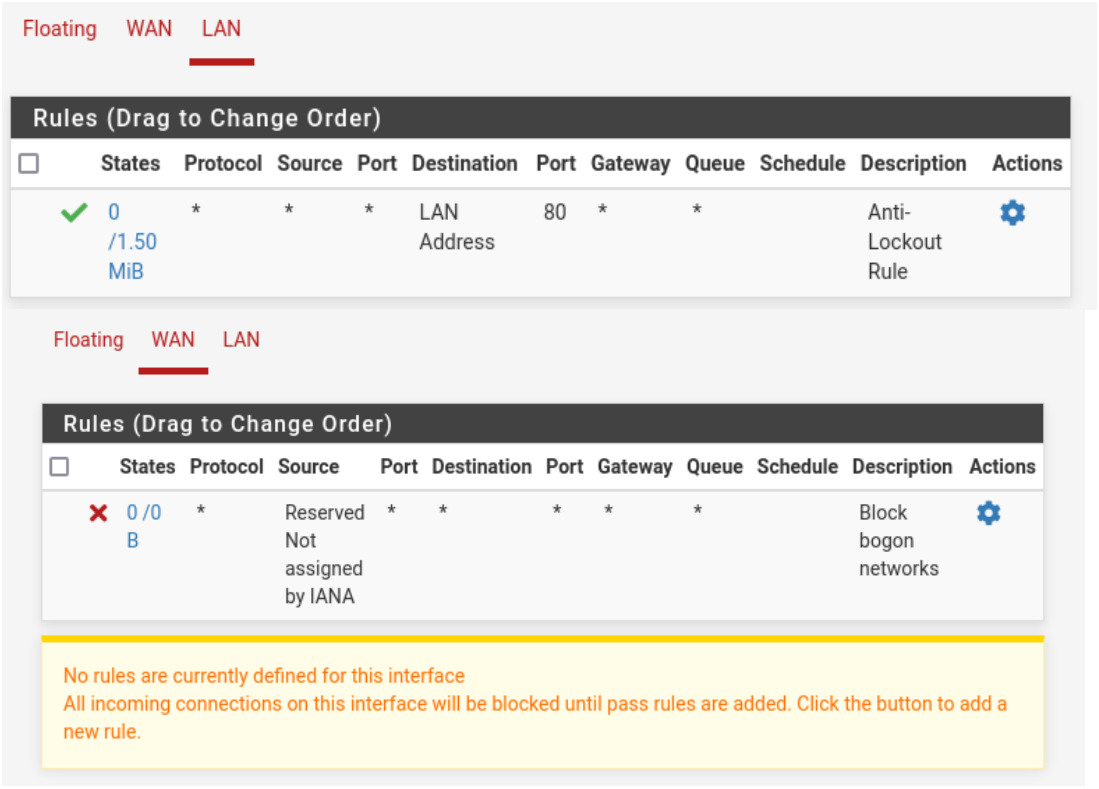
Captura del ping.



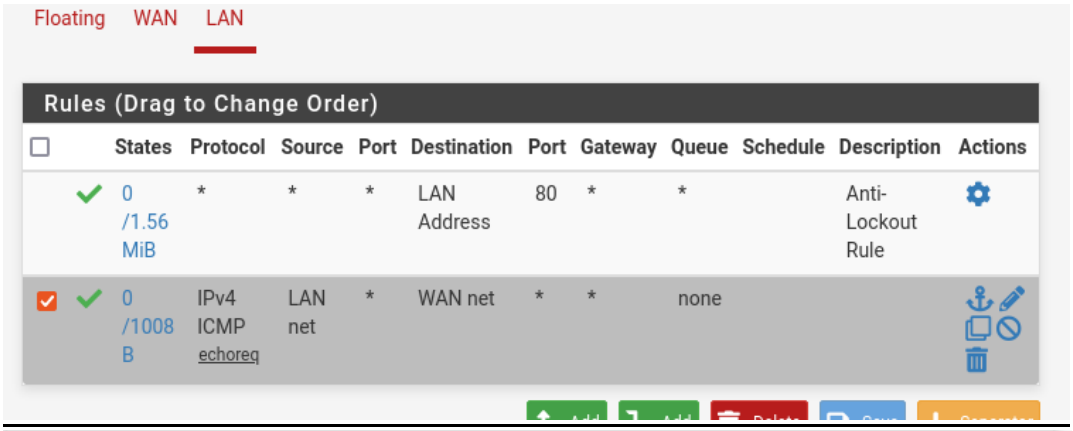
Ping fallido externo-interno.

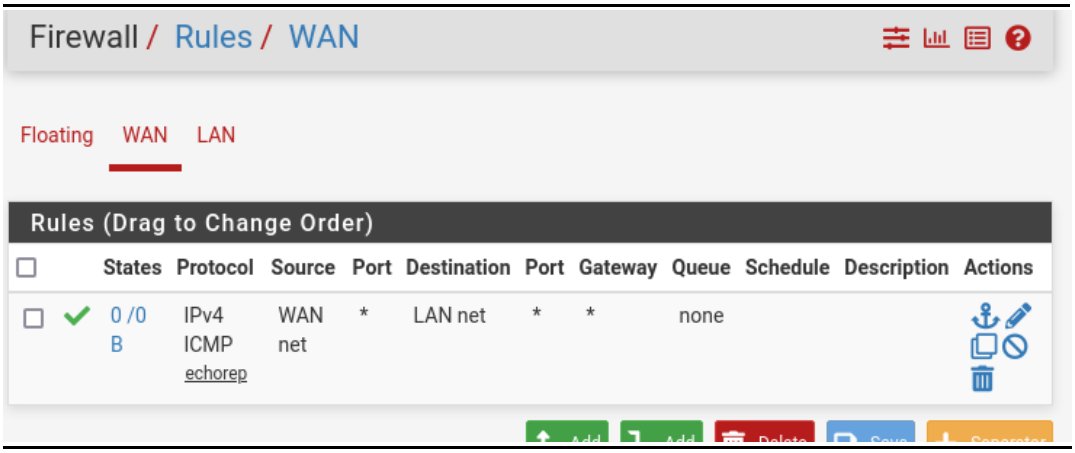


Normas a drop(se ponen por defecto, es decir, todo lo que no este especificado se filtra a drop).



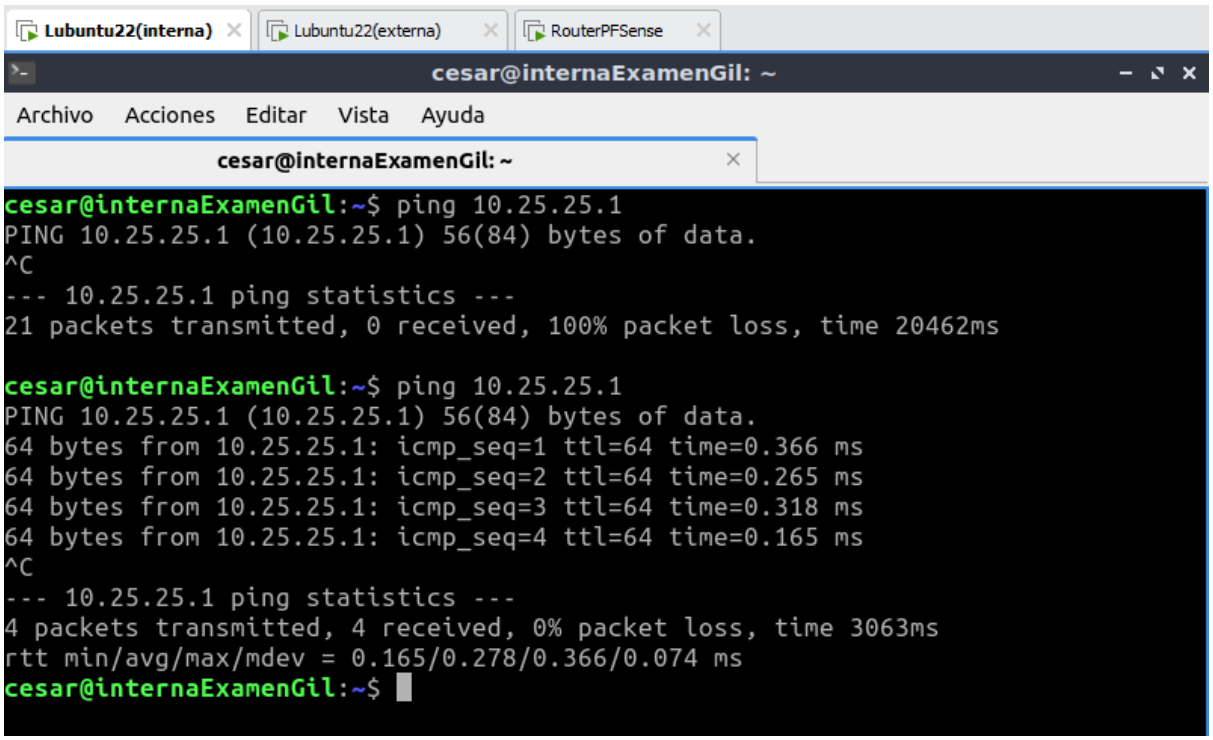
Reglas para permitir el ping.



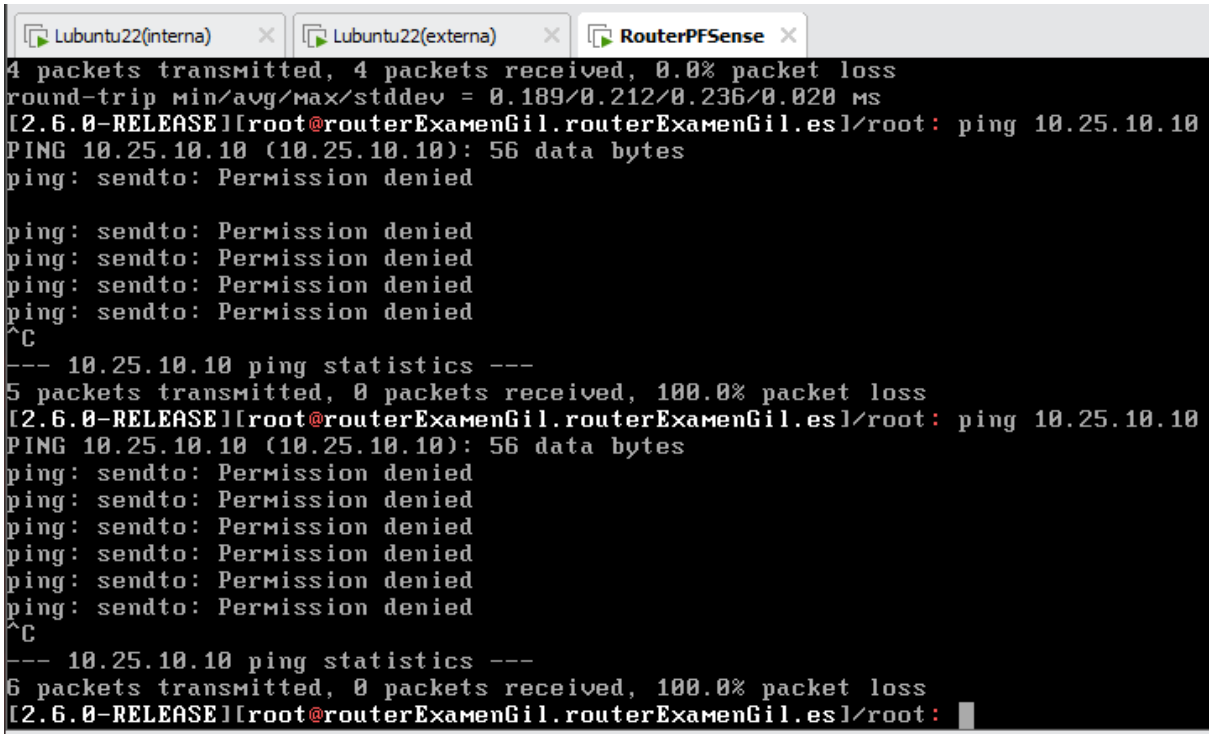


Ping interno a router pero al revés no.

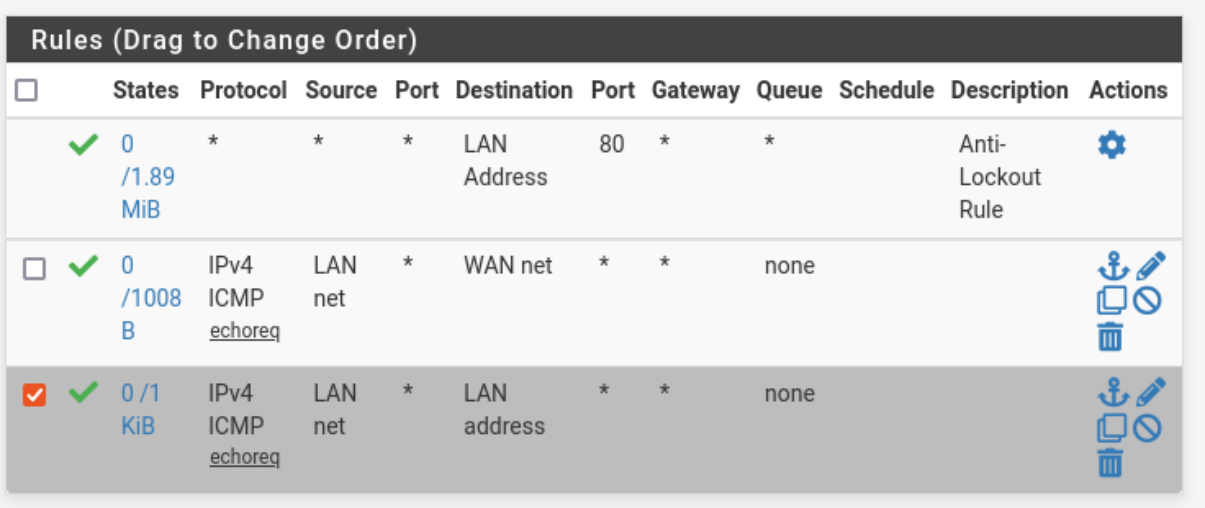
Captura del ping.



Captura del ping fallido router-interno.



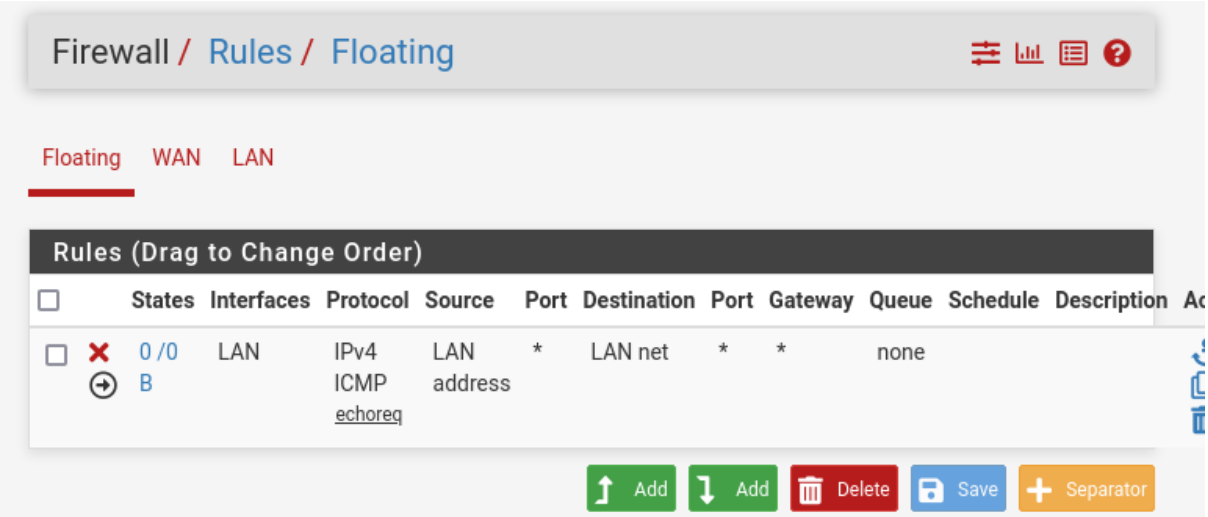
Reglas para permitir el ping del interno al router.



Rules (Drag to Change Order)

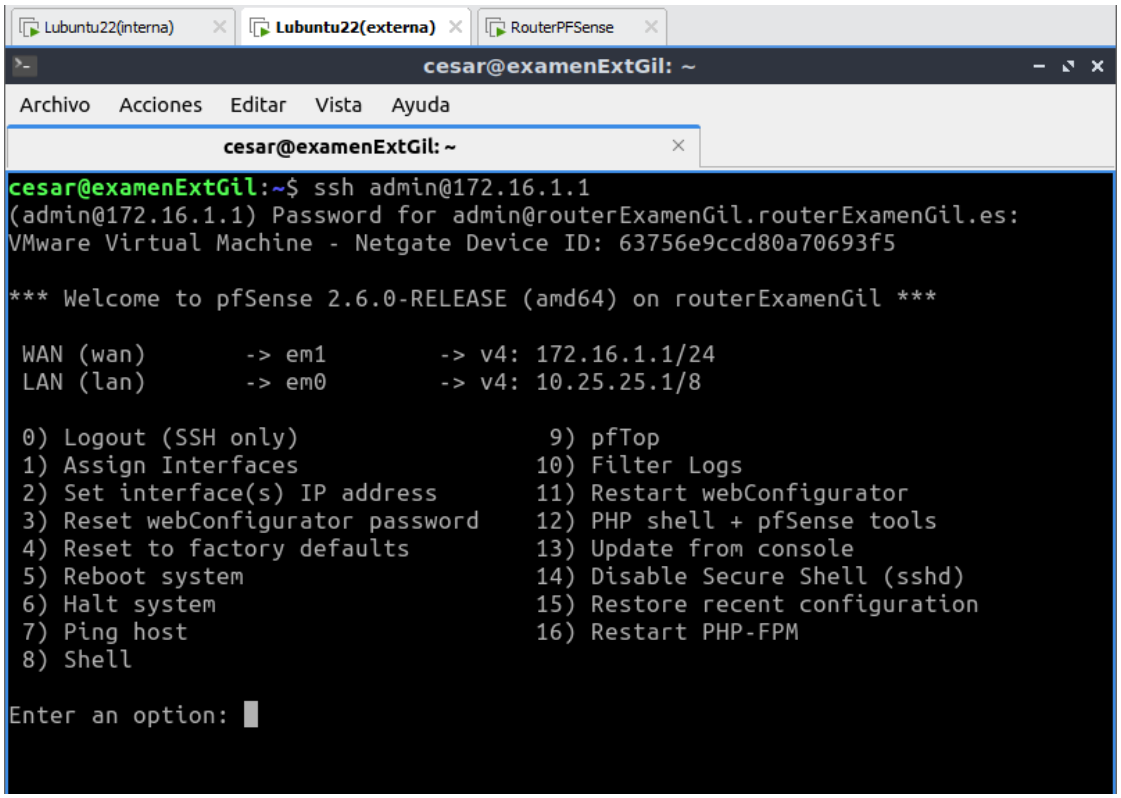
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /1.89 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
☐ ✓	0 /1008 B	IPv4 ICMP echoreq	LAN net	*	WAN net	*	*	none			⚓ ✎ ⧉ ⊘ 🗑
☑ ✓	0 /1 KiB	IPv4 ICMP echoreq	LAN net	*	LAN address	*	*	none			⚓ ✎ ⧉ ⊘ 🗑

Reglas para denegar el ping del servidor al router.

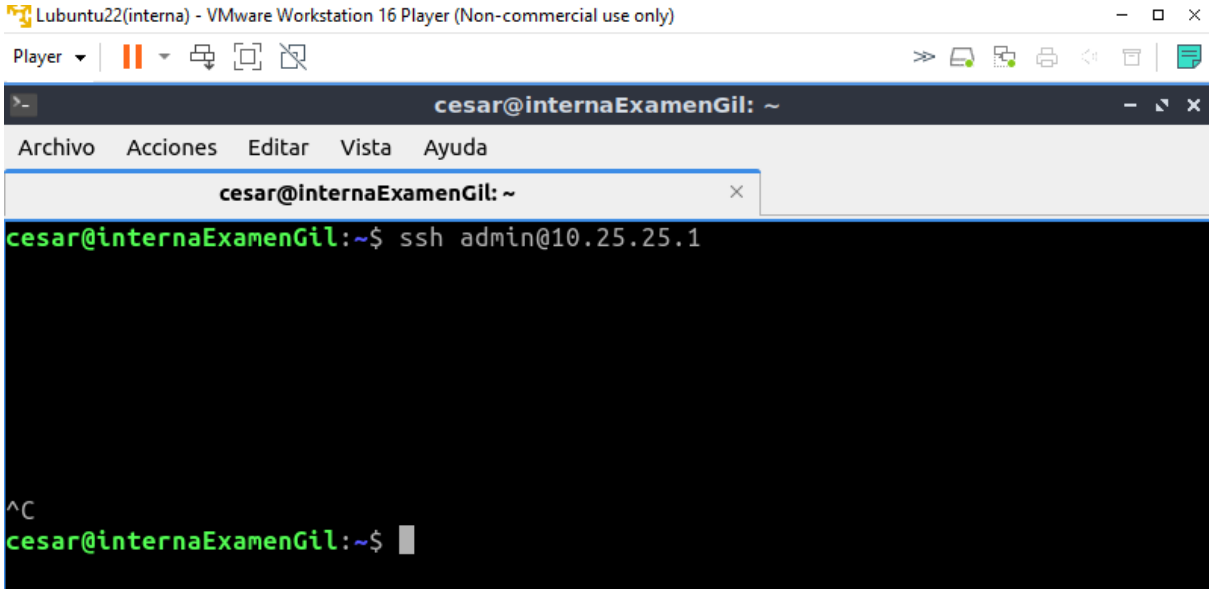


SSH a router desde externo pero no desde el interno.

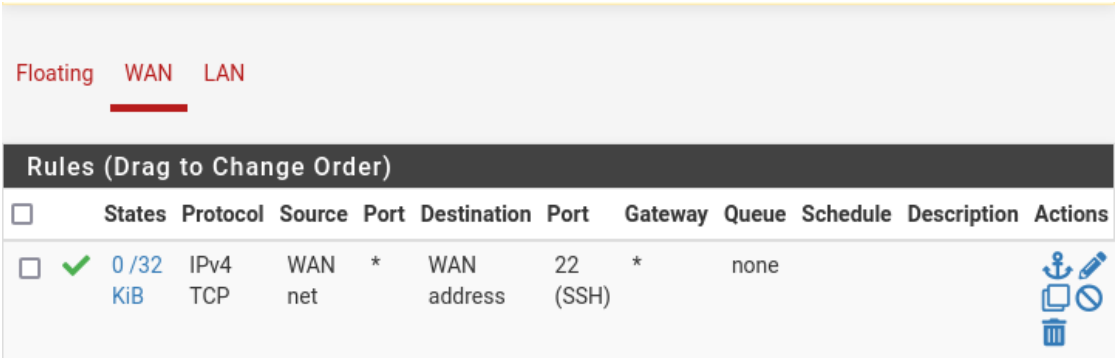
Captura del ssh.

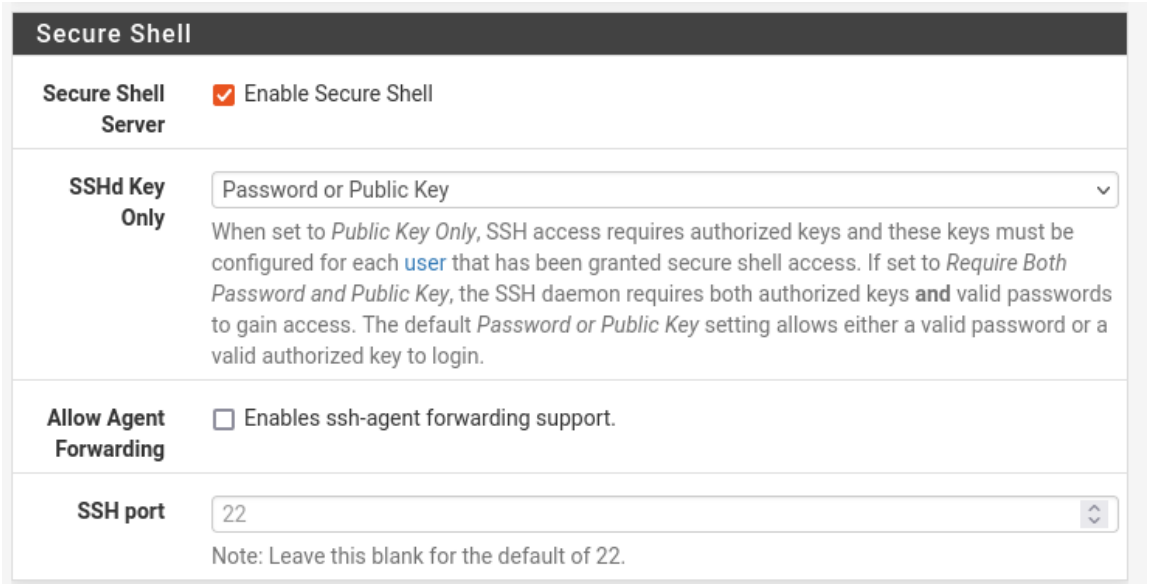


Captura del ssh fallido desde el interno.

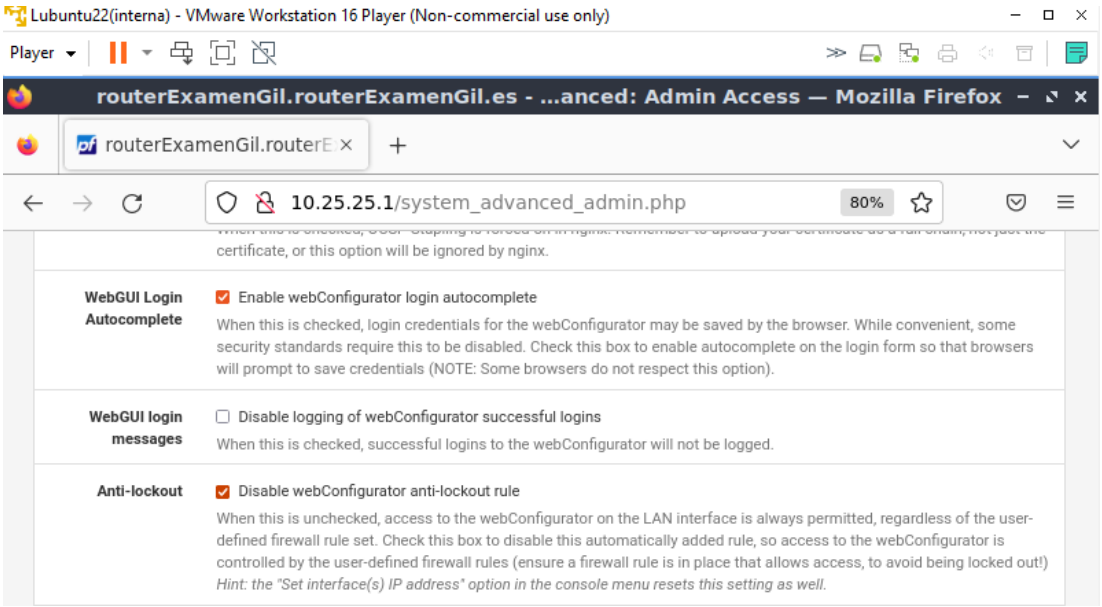


Regla para permitir el ssh.



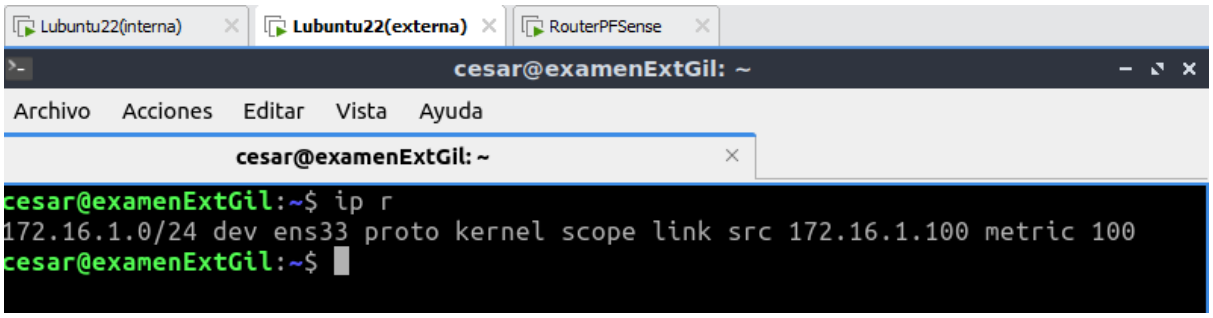


Para denegar el ssh desde el interno, desde la misma pestaña donde habilitamos el secure shell, hay que deshabilitar el anti-lockout. Antes de hacerlo,recordar habilitar la conexión http o si no, no podremos seguir usando el interfaz web.

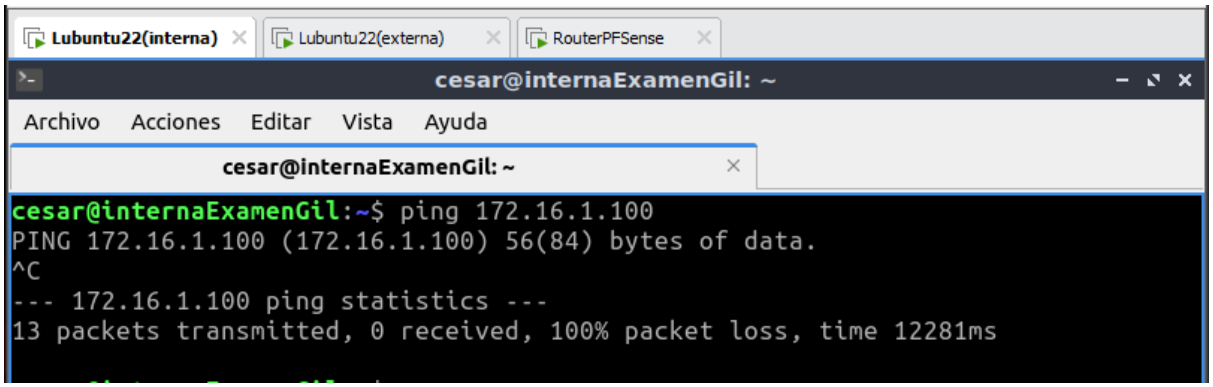


Externo sin puerta de enlace.

Captura del ip r.

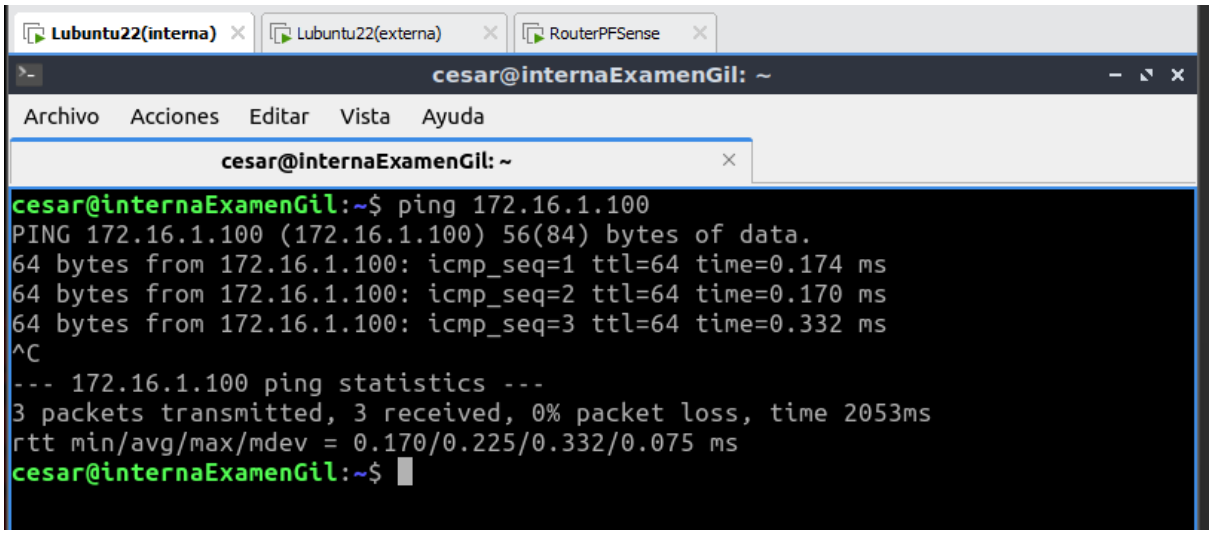


Ping fallido interno-externo.

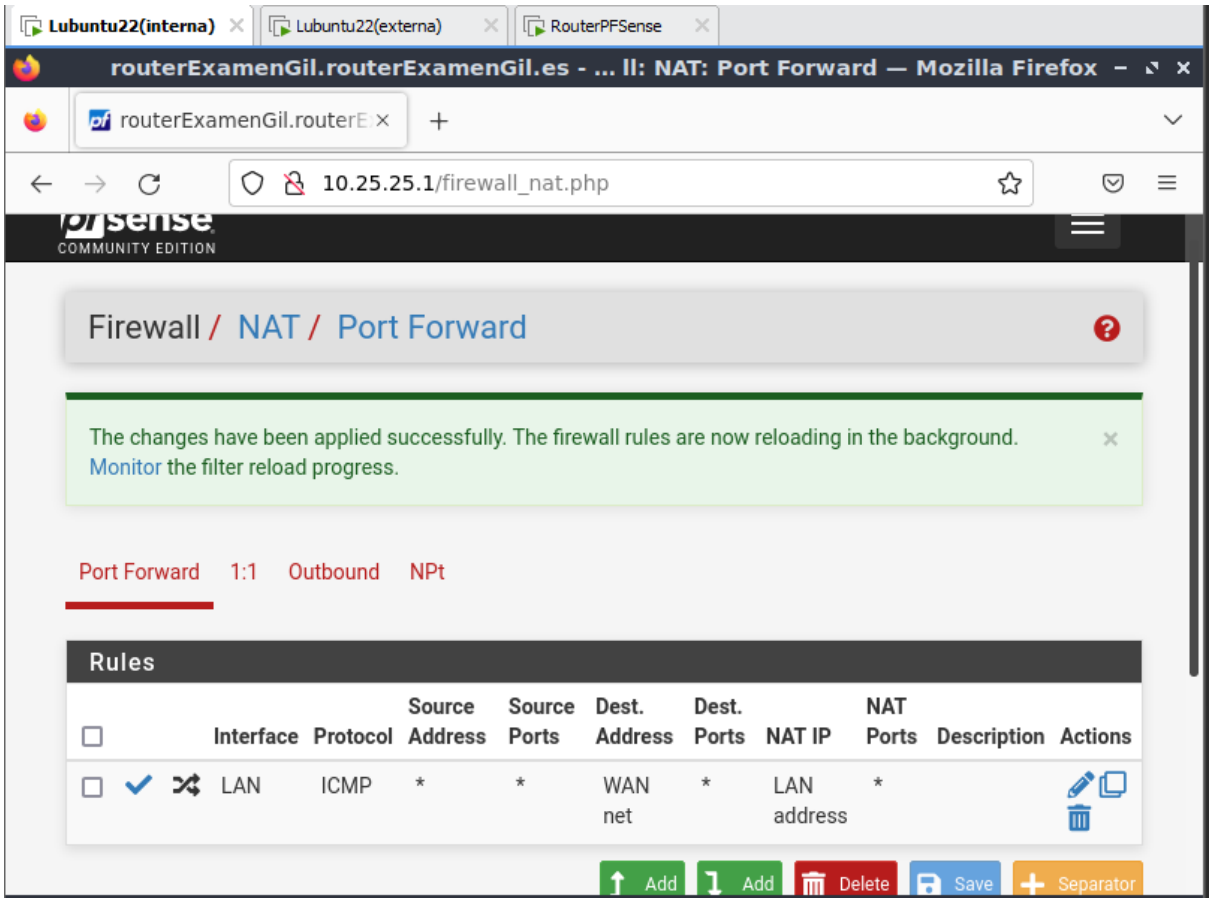


POSTROUTING para que el ping vuelva a funcionar.

Captura del ping.



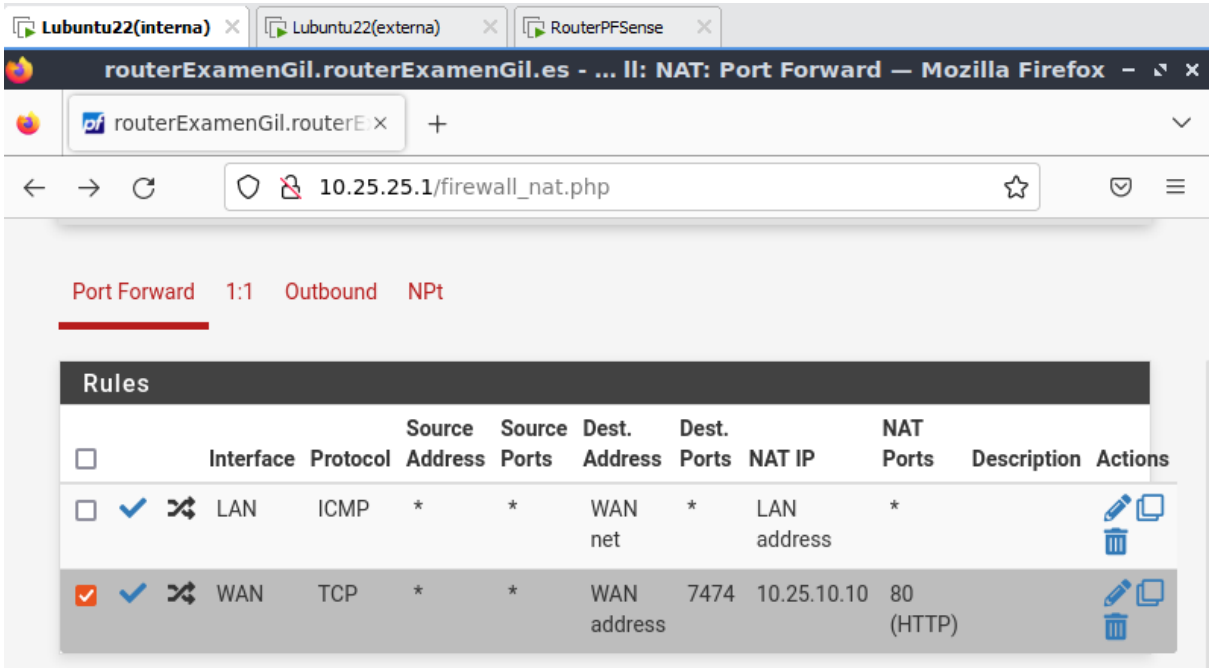
Norma para activar el postrouting.



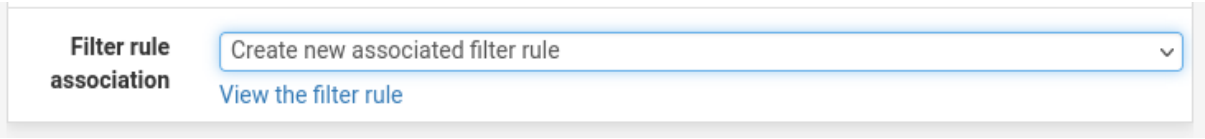
PREROUTING para permitir el HTTP desde el externo.

Captura de la conexión HTTP.

Captura de la regla.



A la hora de crear la regla existe la posibilidad de activar la siguiente opción para que PFSense cree automáticamente una regla en la tabla filter para permitir el forwarding entre la externa y la interna. De lo contrario habría que crearla manualmente.



Regla del forward creada automáticamente por el S.O del router.