pfSense + DMZ

ESCENARIO:

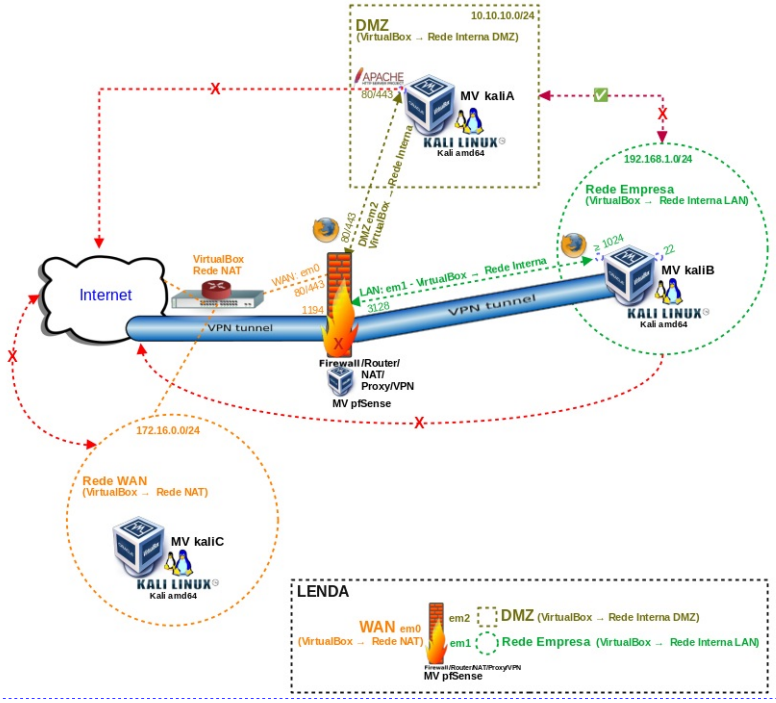
Máquinas virtuais:
- RAM ≥ 2048MB
- CPU ≥ 2
- PAE/NX habilitado
- BIOS: Óptica

DMZ ⊃ MV kaliA:
- ISO: Live Kali amd64
- Rede: Interna
- IP/MS: 10.10.10.10/24
- Servidor Web: apache2

Máquina virtual pfSense:
- ISO: pfSense
- BIOS: Óptica, HD
- HD Dinámico: 20GB
- Rede1: NAT Network (em0)
  - IP/MS: 172.16.0.7/24
- Rede2: Interna (em1)
  - IP/MS: 192.168.1.1/24
- Rede3: Interna (em1:0)
  - IP/MS: 10.10.10.1/24
- Firewall/Router/NAT/Proxy/VPN

Rede Empresa ⊃ MV kaliB:
- ISO: Live Kali amd64
- Rede:Interna
- IP/MS: 192.168.1.100/24
- Cliente Web + Cliente Proxy

Rede WAN ⊃ MV kaliC:
- ISO: Live Kali amd64
- Rede: NAT Network
- IP/MS: 172.16.0.8/24
- Cliente Web
- Cliente VPN



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTA: Documentación de interese
- **Cheat Sheet Apache2 Web Server**
- **Practica BRS Cifrado asimetrico Conexion SSH sen contrasinal**
- **Mecanismos de Control**

DMZ

A DMZ, ou zona desmilitarizada, utilízase habitualmente para aloxar servidores que ofrecen servizos á rede externa, xeralmente Internet. Estes servizos poden incluír servidores web, DNS, correo electrónico, etc.
En canto á conectividade, a DMZ está deseñada para permitir conexións dende a rede interna e a externa, pero restrinxir as conexións dende a DMZ unicamente á rede externa. Isto significa que:

- Os equipos da rede interna poden conectarse aos servidores da DMZ.
- Os equipos da rede externa (Internet) poden conectarse aos servidores da DMZ.
- Os equipos da DMZ non poden iniciar conexións coa rede interna.

Esta configuración ten como obxectivo protexer a rede interna no caso de que un atacante comprometa a seguridade dos equipos na DMZ. A DMZ actúa como unha especie de "amortiguador", impedindo que un atacante que accedese á DMZ poida acceder directamente á rede interna.

Que é Que é pfSense?

pfSense é unha solución de *firewall* e *router* de código aberto baseada no sistema operativo **FreeBSD**. É amplamente utilizada para xestionar e protexer redes, tanto pequenas como grandes, grazas á súa flexibilidade, robustez e facilidade de uso.

- ### Principais características de pfSense:
  - **Firewall avanzado:** Controla o tráfico da rede mediante regras configurables.
  - **Enrutador integrado:** Ofrece enrutamento estático e dinámico entre redes.
  - **VPN (Redes Privadas Virtuais):** Establece conexións seguras usando protocolos como OpenVPN e IPsec.
  - **Balanceo de carga e failover:** Mellora o rendemento e dispoñibilidade da conexión a Internet.
  - **Filtro de contido:** Bloquea sitios web ou categorías específicas.
  - **Interfaz web fácil de usar:** Configuración sinxela a través dun navegador.
- ### Vantaxes de usar pfSense:
  - **Gratuíto e de código aberto:** Sen custos de licenzas.
  - **Alta seguridade e estabilidade:** Ideal para redes críticas.
  - **Personalización:** Adaptable ás necesidades específicas.
  - **Actualizacións frecuentes:** Melloras continuas grazas á comunidade activa.
- ### Interfaces e Roles en pfSense:

  En **pfSense**, as interfaces como `em0`, `em1` e `em2` son asignadas automaticamente segundo a detección do hardware durante a instalación. A asignación de roles (**WAN**, **LAN**, **OPT1**) non está relacionada co nome físico (`emX`), senón coas decisións tomadas ao configurar o sistema.

  A. ### Asignación típica das interfaces:
     - **em0 (WAN):** A primeira interface detectada, normalmente asignada como **WAN**. Conecta a rede local a Internet ou a unha rede externa.
     - **em1 (LAN):** A segunda interface detectada, asignada como **LAN**. Utilízase para conectar dispositivos internos na rede local.
     - **em2 (OPT1):** A terceira interface detectada, configurada como **OPT1**. Pode usarse para redes adicionais, como unha DMZ ou redes de invitados.

  B. ### Explicación dos roles das interfaces:
     - **WAN (Wide Area Network):** Interface que conecta a rede local a Internet. Protexe a rede interna fronte a ameazas externas.
     - **LAN (Local Area Network):** Interface para conectar os dispositivos internos. Proporciona acceso a Internet aos equipos locais.
     - **OPT (Opcional):** Interfaces adicionais configurables para fins específicos, como VLANs ou DMZs.

En resumo:

1. **pfSense** é unha ferramenta versátil que permite mellorar a seguridade e o control dunha rede de forma profesional e eficiente.
2. Os nomes das interfaces (`em0`, `em1`, `em2`) son asignados automaticamente polo sistema en función do hardware dispoñible. Os roles (**WAN**, **LAN**, **OPT1**) son definidos polo usuario para especificar o uso de cada interface, permitindo unha configuración flexible e adaptada ás necesidades específicas.

Descarga fpSense

Resumo

Firewall: Regras Port Forwarding

- No **Exemplo1. Port Forwarding kaliC(WAN) $\overset{80}{\rightarrow}$ kaliA(DMZ)** imos redireccionar o porto TCP 80(HTTP) de pfSense ao porto TCP 80(HTTP) en kaliA se a petición de conectividade realízase dende a rede WAN(kaliC)
- No **Exemplo2. Port Forwarding kaliC(WAN) $\overset{443}{\rightarrow}$ kaliA(DMZ)** imos redireccionar o porto TCP 443(HTTPS) de pfSense ao porto TCP 443(HTTPS) en kaliA se a petición de conectividade realízase dende a rede WAN(kaliC)

Proxy: Squid

- No **Exemplo3. Proxy en pfSense** imos activar o proxy en pfSense para que as peticións web dende LAN(kaliB) saían a través deste proxy.

VPN: OpenVPN

- **No Exemplo4. OpenVPN en pfSense. Acceso remoto kaliC(WAN$\overset{1194}{)}$ → kaliA(DMZ) imos configurar acceso VPN para que dende kaliC(WAN) poidamos conectarnos a kaliB(LAN).**

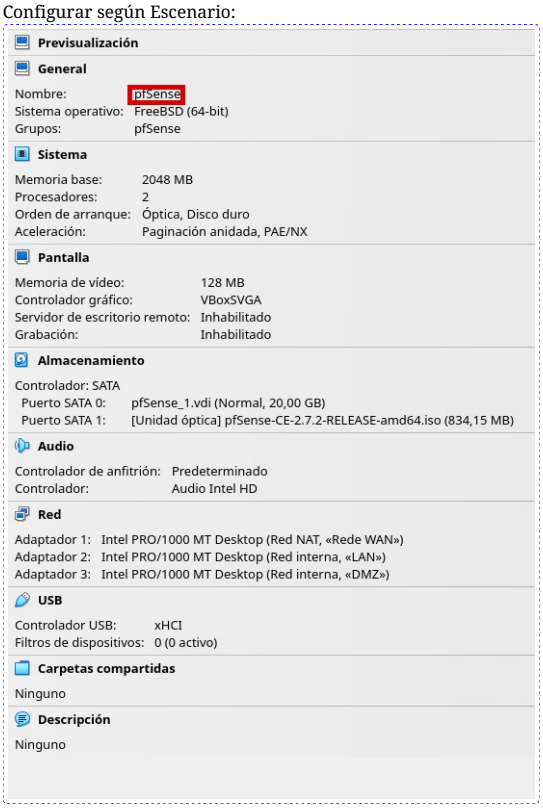
Firewall: Regras DMZ

- No **Exemplo5. Bloqueo tráfico de rede da DMZ á LAN** imos engadir a regra que impide o acceso da DMZ(kaliA) á LAN(kaliB).

Configuración Escenario

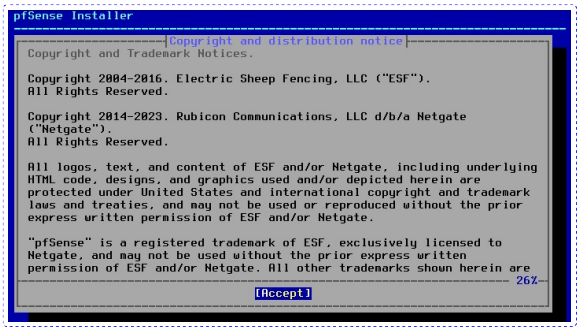
Firewall - Máquina virtual pfSense

1. Configurar según Escenario:



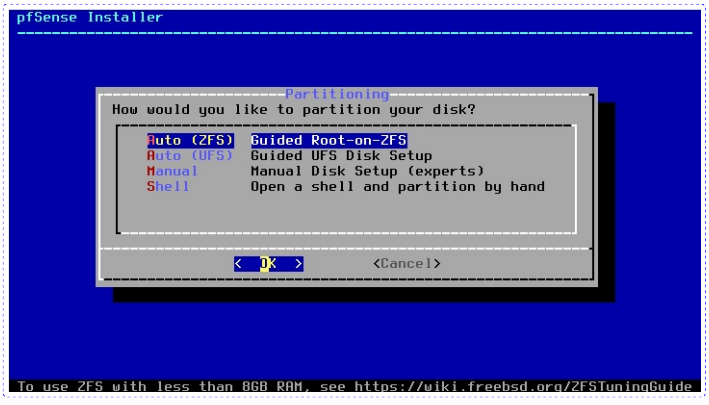
2. Arrancar a live pfSense para a instalación no HD dinámico de 20GB:

Moverse polas pantallas de instalación coas teclas frechas e tabulado. Unha vez elexido a opción desexada premer a tecla Enter.

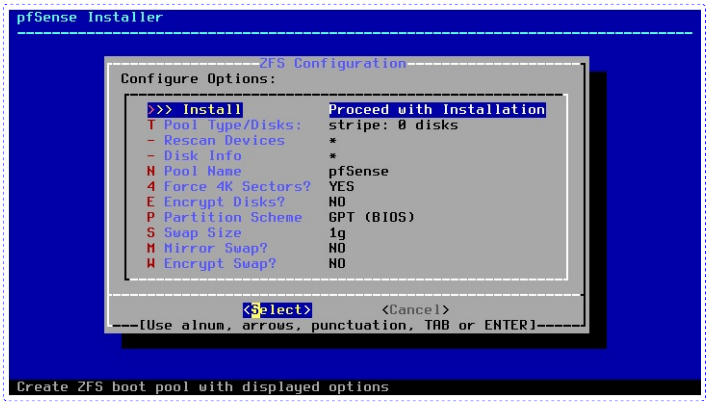


Premer a tecla Enter

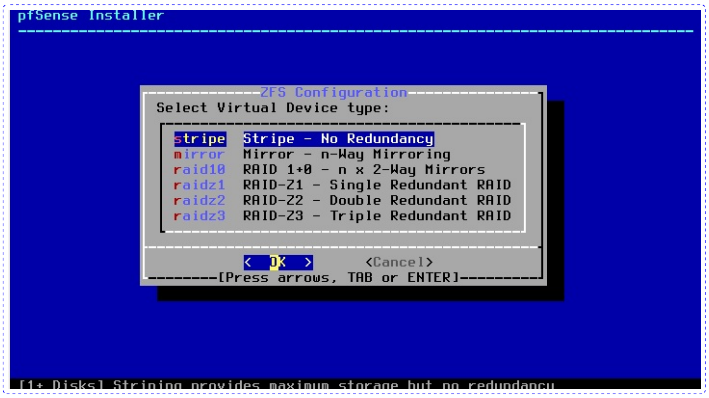
Escoller a opción Install e premer Enter



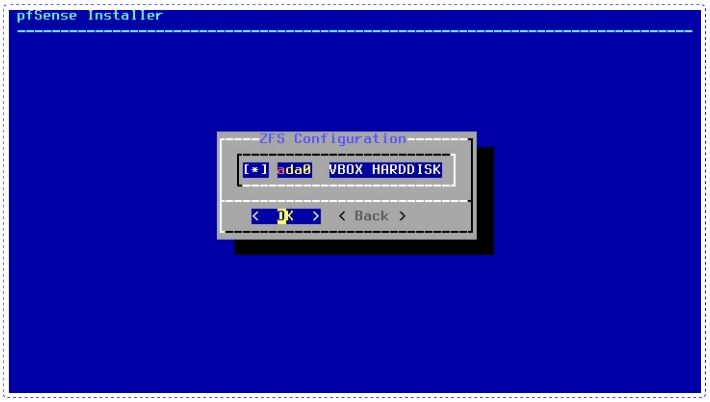
Escoller a opción Auto (ZFS) e premer Enter



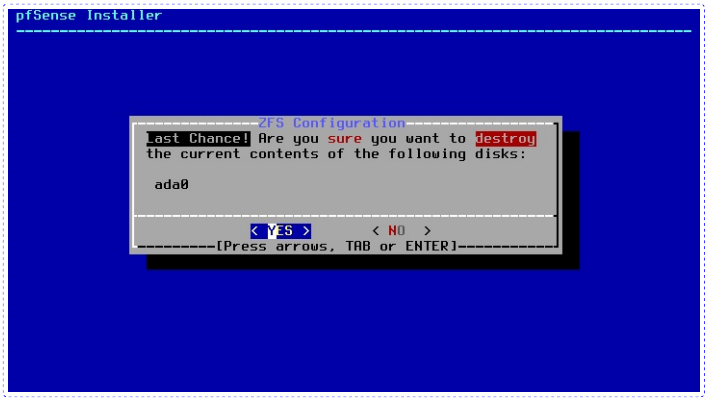
Premer a tecla Enter para proseguir coa instalación



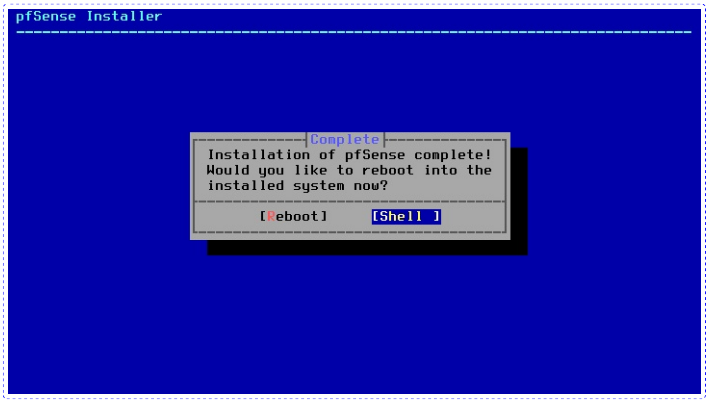
Premer a tecla Enter para proseguir coa instalación



Seleccionar o disco duro onde instalar pfSense premendo na tecla "barra espaciadora" e premer Enter.

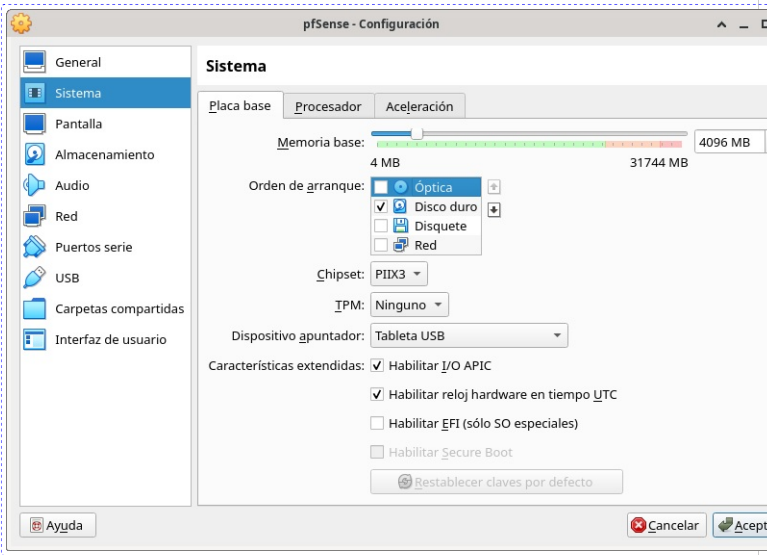


Premer a tecla Enter para proseguir coa instalación

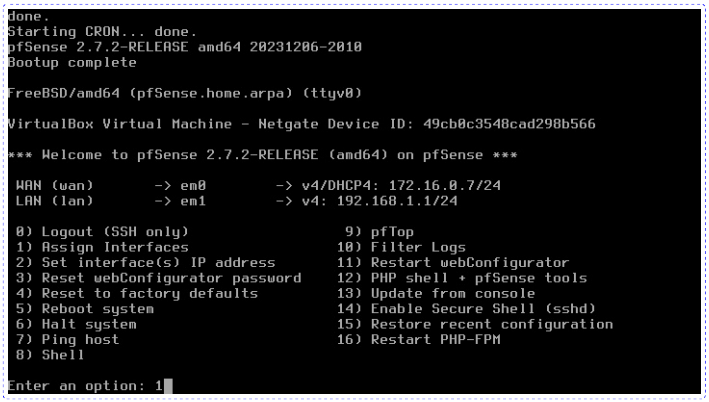


Elixir a opción Shell para proseguir coa instalación

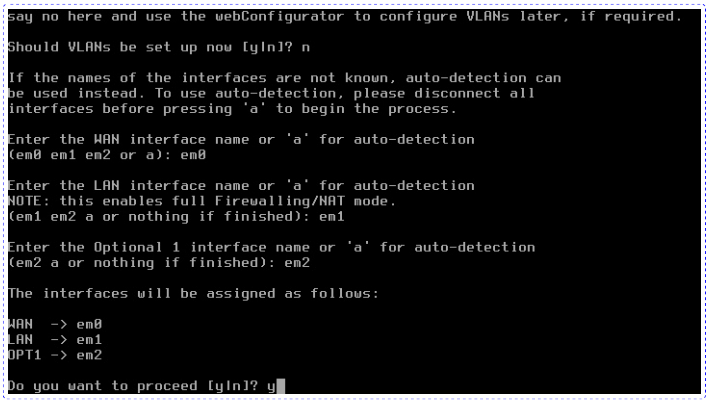
Apagar o equipo executando o comando: init 0



Modificar as opcións de arranque: deixar soamente disco duro



Arrancar a máquina virtual. Unha vez arrancado aparece un menú.



Elixir a opción 1 para determinar que rol posee cada interface de rede. Premer:
n → para non configurar VLANs
em0 → para escoller a interface em0 co rol WAN
em1 → para escoller a interface em1 co rol LAN

em2 → para escoller a interface em2 co rol OPT1
y → para confirmar as anteriores opcións escollidas.

```
OPT1 -> em2

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

Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: 49cb0c3548cad298b566

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.16.0.7/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        ->

 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: 2
```

Elixr a opción 2 para configurar a rede das interfaces em0, em1, em2

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.16.0.7/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        ->

 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: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3
```

Escoller a opción 3 para configurar a única interface que non posúe configuración de rede: em2

```
Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 10.10.10.1

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 OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y
```

Premer:
n → para non configurar a interface por DHCP e si de forma estática
10.10.10.1 → para configurar esa IPv4 estática
24 → para configurar esa máscara de subrede
Enter → para non configurar gateway para esta interface.
n → para non configurar IPv6 de forma dinámica
Enter → para non configurar IPv6 de forma estática
y → para confirmar as anteriores opcións escollidas.

```
For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y
Enter the start address of the IPv4 client address range: 10.10.10.10
Enter the end address of the IPv4 client address range: 10.10.10.50
Disabling IPv6 DHCPD...

Please wait while the changes are saved to OPT1...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT1 address has been set to 10.10.10.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://10.10.10.1/

Press <ENTER> to continue.
```

Efectuados os cambios premer Enter para continuar

```
The IPv4 OPT1 address has been set to 10.10.10.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://10.10.10.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 49cb0c3548cad298b566

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.16.0.7/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        -> v4: 10.10.10.1/24

 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:
```

Para poder continuar coa práctica verificar que está realizada a configuración de rede das 3 interfaces como se amosa na imaxe.

Igual as IP/MS non son as mesmas pero máis adiante na práctica resolverase esta cuestión.

Unha vez configuradas en pfSense as 3 tarxetas de rede: em0, em1, em2 imos configurar o resto de máquinas virtuais:

- kaliA para a DMZ(em2)
- kaliB para a LAN(em1)
- kaliC para a WAN(em0)

DMZ - Máquina virtual A: Kali amd64

3. Configurar según Escenario:

Previsualización

General

Nombre: kaliA
Sistema operativo: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)
Grupos: pfSense

Sistema

Memoria base: 2048 MB
Procesadores: 2
Orden de arranque: Óptica
Aceleración: Paginación anidada, PAE/NX, Paravirtualización KVM

Pantalla

Memoria de vídeo: 128 MB
Controlador gráfico: VBoxSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado

Almacenamiento

Controlador: SATA
Puerto SATA 1: [Unidad óptica] kali-linux-2024.3-live-amd64.iso (4,35 GB)

Audio

Controlador de anfitrión: Predeterminado
Controlador: Audio Intel HD

Red

Adaptador 1: Intel PRO/1000 MT Desktop (Red interna, «DMZ»)

USB

Controlador USB: xHCI
Filtros de dispositivos: 0 (0 activo)

Carpetas compartidas

Ninguno

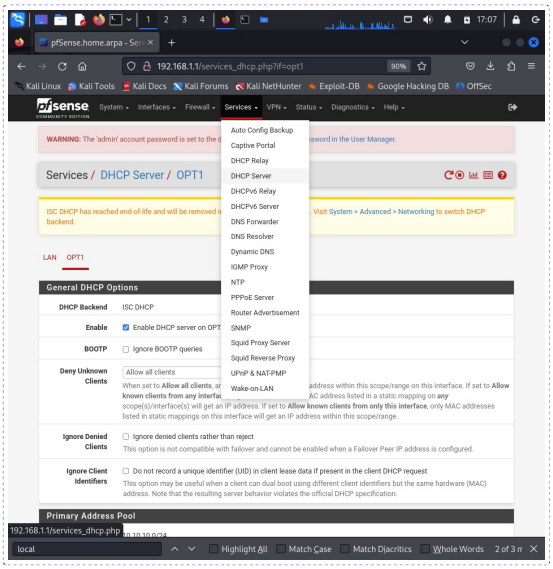
Descripción

Ninguno

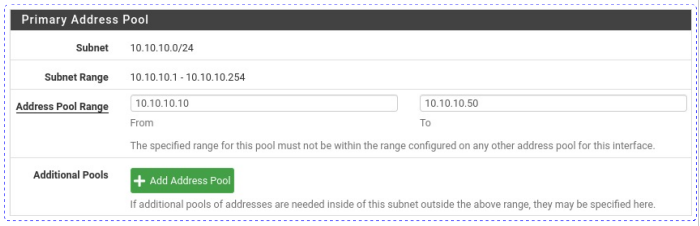
4. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal **DMZabc123.** (Ollo que o contrasinal ten un caracter punto final).

5. Configuración da rede:

kaliA será cliente DHCP, polo cal recollerá a configuración de rede do servidor DHCP de pfSense a través da súa interface em2



Imaxe que amosa a configuración DHCP para em2 en pfSense (máis adiante veremos como acceder a esta aplicación de configuración de pfSense)



Imaxe que amosa o rango de concesión DHCP: 10.10.10.10 - 10.10.10.50

Nesta práctica a IP/MS concedida polo servidor DHCP DMZ de pfSense para kaliB foi: 10.10.10.10/24. Esta IP/MS pode variar na execución desta práctica. Se se quere proceder coa configuración 10.10.10.10/24 débese cambiar a IP estática a interface eth0 de kaliB e manter as táboas de rutas e o ficheiro /etc/resolv.conf como se amosa a continuación.

kali@kali:~$ ip addr show eth0 #Amosar a configuración da tarxeta de rede interna(eth0) con IP/MS: 10.10.10.10/24 recollida polo DHCP (em2) de pfSense.
kali@kali:~$ ip route show || ip route list || ip route || ip r # Listar a táboa de enrutamento otorgada polo servidor DHCP.
kali@kali:~$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.

```
┌──(kali㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
    link/ether 08:00:27:de:f1:6e brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.10/24 brd 10.10.10.255 scope global dynamic noprefixroute eth0
       valid_lft 6796sec preferred_lft 6796sec
    inet6 fe80::9811:bfcb:deac:4a01/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ip route
default via 10.10.10.1 dev eth0 proto dhcp src 10.10.10.10 metric 100
10.10.10.0/24 dev eth0 proto kernel scope link src 10.10.10.10 metric 100

┌──(kali㉿kali)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
search home.arpa
nameserver 10.10.10.1
```

6. Cambiar hostname da máquina virtual A. Por kaliA como hostname:

OPCIÓN A:

kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kali:~# echo 'kaliA' > /etc/hostname #Indicar ao sistema o valor do hostname.
root@kali:~# echo 'kernel.hostname=kaliA' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
root@kali:~# echo -e '10.10.10.10\tkaliA' >> /etc/hosts #Engadir o hostname kaliA en /etc/hosts
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

OPCIÓN B:

kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kali:~# hostnamectl hostname kaliA || hostnamectl set-hostname kaliA #Modificar o hostname do sistema a kaliA.
root@kali:~# echo -e '10.10.10.10\tkaliA' >> /etc/hosts #Engadir o hostname kaliA en /etc/hosts
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

7. Activar Servidor Web Apache:

kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kaliA:~# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
root@kaliA:~# /etc/init.d/apache2 start #Iniciar o servidor web Apache.
root@kaliA:~# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
root@kaliA:~# nc -vz 10.10.10.10 80 #Mediante o comando nc(netcat) comprobar se o porto 80 do servidor web Apache está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 80 é o porto TCP a escanear.
root@kaliA:~# a2ensite default-ssl #Habilitar o VirtualHost default-ssl, que configura o acceso a través de https (porto TCP 443)
root@kaliA:~# a2enmod ssl #Habilitar o módulo ssl que permite activar a configuración do VirtualHost default-ssl, que configura o acceso a través de https (porto TCP 443)
root@kaliA:~# /etc/init.d/apache2 restart #Reiniciar a configuración do servidor web Apache.
root@kaliA:~# nc -vz 10.10.10.10 443 #Mediante o comando nc(netcat) comprobar se o porto 443 do servidor web Apache está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 443 é o porto TCP a escanear.

> No caso da distribución Kali xa temos instalado o servidor web Apache, pero nunha distribución baseada en Debian poderiamos instalalo do seguinte xeito:
> # apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
> # apt search apache2 #Buscar calquera paquete que coincida co patrón de búsqueda apache2
> # apt -y install apache2 #Instalar o paquete apache2, é dicir, instalar o servidor HTTP apache2. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.

8. Permisos apache:

root@kaliA:~# chown -R www-data: /var/www/html/ #Cambiar usuario propietario www-data e grupo propietario www-data a toda a árbore de ficheiros e directorios que colgan do directorio DocumentRoot de Apache: /var/www/html
root@kaliA:~# chmod 444 /var/www/html/index.html #Cambiar a só lectura os permisos **ugo** do ficheiro index.html situado en /var/www/html, é dicir, establecer os permisos r--r--r-- (soamente lectura para o usuario propietario, o grupo propietario e o resto do mundo)
root@kaliA:~# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
root@kaliA:~# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.

	pfSense → kaliA	kaliA → pfSense	kaliA → Internet
ping	SI	NON	NON
nc (ports TCP 80/443)	SI		

Agora podemos comprobar que dende pfSense si é posible establecer conectividade cun ping a kaliA(10.10.10.10), pero que dende kaliA non é posible establecer conectividade cun ping a pfSense(10.10.10.1) nin a Internet.

```
WAN (wan)       -> em0        -> v4/DHCP4: 172.16.0.7/24
LAN (lan)       -> em1        -> v4: 192.168.1.1/24
OPT1 (opt1)     -> em2        -> v4: 10.10.10.1/24

 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: 8

[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping -c2 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=64 time=1.311 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=1.883 ms

--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.311/1.597/1.883/0.286 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

```
┌──(kali㉿kaliA)-[~]
└─$ ping -c2 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.

--- 10.10.10.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1032ms
```

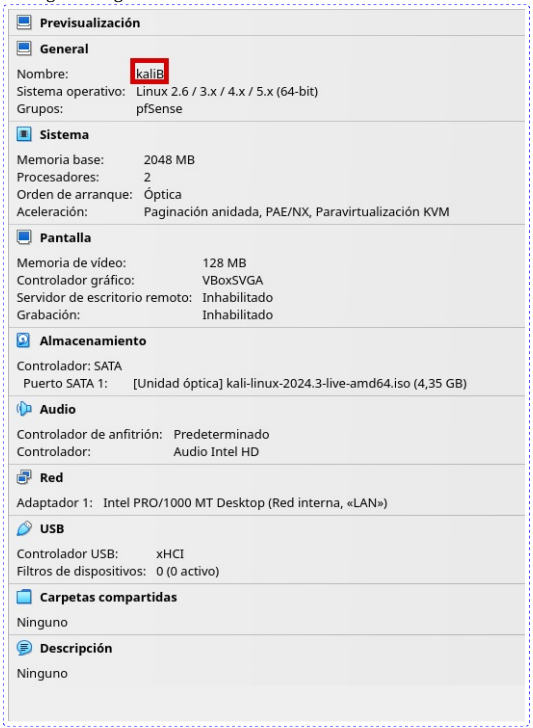
```
┌──(kali㉿kaliA)-[~]
└─$ ping -c2 www.google.es
ping: www.google.es: Temporary failure in name resolution
```

Tamén podemos observar que dende pfSense somos quen de chegar ao portos TCP 80 e 443(servizo web apache2) de kaliA.

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping -c2 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=64 time=1.186 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=1.298 ms

--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.186/1.242/1.298/0.056 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: nc
usage: nc [-46DdEFhklNnrStUuvz] [-e policy] [-I length] [-i interval] [-O length
]
          [--no-tcpopt] [--sctp]
          [-P proxy_username] [-p source_port] [-s source] [-T ToS]
          [--tun tundev] [-V rtable] [-w timeout] [-X proxy_protocol]
          [-x proxy_address[:port]] [destination] [port]
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: nc -vz 10.10.10.10 80
Connection to 10.10.10.10 80 port [tcp/http] succeeded!
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: nc -vz 10.10.10.10 443
Connection to 10.10.10.10 443 port [tcp/https] succeeded!
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

LAN - Máquina virtual B: Kali amd64

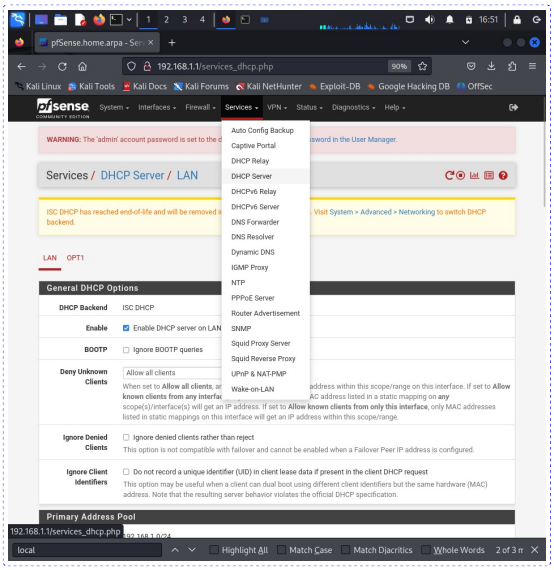
9. Configurar según Escenario:



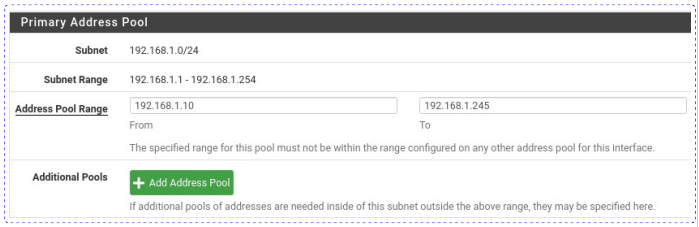
10. Na contorna gráfica abrir un terminal e executar:
    kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
    kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal **LANabc123**. (Ollo que o contrasinal ten un caracter punto final).

11. Configuración da rede:

kaliB será cliente DHCP, polo cal recollerá a configuración de rede do servidor DHCP de pfSense a través da súa interface em1



Imaxe que amosa a configuración DHCP para em1 en pfSense (máis adiante veremos como acceder a esta aplicación de configuración de pfSense)



Imaxe que amosa o rango de concesión DHCP: 192.168.1.10 - 192.168.1.245

Nesta práctica a IP/MS concedida polo servidor DHCP LAN de pfSense para kaliB foi: 192.168.1.100/24. Esta IP/MS pode variar na execución desta práctica. Se se quere proceder coa configuración 192.168.1.100/24 débese cambiar a IP estática a interface eth0 de kaliB e manter as táboas de rutas e o ficheiro /etc/resolv.conf como se amosa a continuación.

kali@kali:~$ ip addr show eth0 #Amosar a configuración da tarxeta de rede interna(eth0) con IP/MS: 192.168.1.100/24 recollida polo DHCP (em1) de pfSense.
kali@kali:~$ ip route show || ip route list || ip route || ip r # Listar a táboa de enrutamento otorgada polo servidor DHCP.
kali@kali:~$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.

```
┌──(kali㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
    link/ether 08:00:27:88:c0:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 6881sec preferred_lft 6881sec
    inet6 fe80::13af:c4:dd30:f89/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ip route
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.100 metric 100
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.100 metric 100

┌──(kali㉿kali)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
search home.arpa
nameserver 192.168.1.1
```

12. Cambiar hostname da máquina virtual B. Por kaliB como hostname:

OPCIÓN A:

kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kali:~# echo 'kaliB' > /etc/hostname #Indicar ao sistema o valor do hostname.
root@kali:~# echo 'kernel.hostname=kaliB' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
root@kali:~# echo -e '192.168.1.100\tkaliB' >> /etc/hosts #Engadir o hostname kaliB en /etc/hosts
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

OPCIÓN B:

kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kali:~# hostnamectl hostname kaliB || hostnamectl set-hostname kaliB #Modificar o hostname do sistema a kaliB.
root@kali:~# echo -e '192.168.1.100\tkaliB' >> /etc/hosts #Engadir o hostname kaliB en /etc/hosts
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

	pfSense → kaliB	kaliB → pfSense	kaliB → Internet	kaliA → kaliB	kaliB → kaliA
ping	SI	SI	SI	NON	SI
nc (ports TCP 80/443)					SI

Agora podemos comprobar que dende kaliB **SI** é posible establecer conectividade cun ping a pfSense(192.168.1.1) e viceversa; e que tamén dende kaliB é posible a saída a Internet

```
┌──(kali㉿kaliB)-[~]
└─$ ping -c2 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.72 ms

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.104/1.411/1.719/0.307 ms

┌──(kali㉿kaliB)-[~]
└─$ ping -c2 www.google.es
PING www.google.es (142.250.200.131) 56(84) bytes of data.
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=1 ttl=103 time=32.3 ms
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=2 ttl=103 time=32.3 ms

--- www.google.es ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 32.251/32.298/32.346/0.047 ms
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping -c2 192.168.1.100
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=64 time=1.669 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=2.364 ms

--- 192.168.1.100 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.669/2.017/2.364/0.347 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

Tamén podemos observar que dende kaliB **SI** é posible establecer conectividade cun ping a kaliA e que somos quen de chegar aos portos TCP 80 e 443(servizo web apache2) de kaliA.

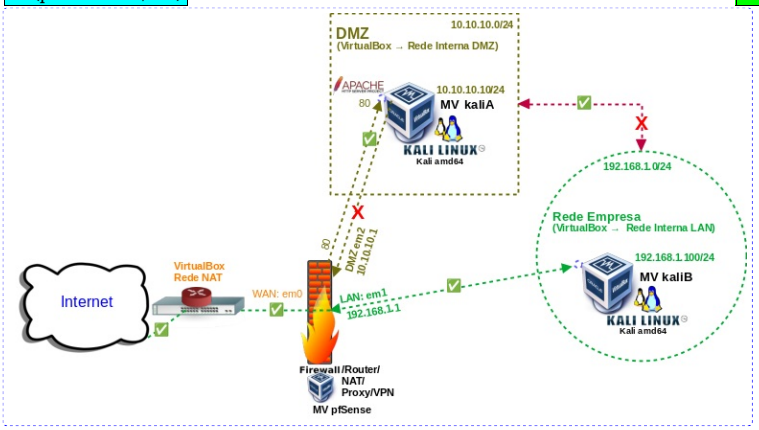
```
└─$ ping -c2 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=1.78 ms

--- 10.10.10.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.253/1.516/1.780/0.263 ms

┌──(kali㉿kaliB)-[~]
└─$ ping -c2 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=3.14 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=63 time=3.04 ms

--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 3.036/3.087/3.139/0.051 ms

┌──(kali㉿kaliB)-[~]
└─$ nc -vz 10.10.10.10 80 443
10.10.10.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.10] 80 (http) open
(UNKNOWN) [10.10.10.10] 443 (https) open
```

Tamén que dende kaliA **NON** é posible establecer conectividade cun ping a pfSense nin a kaliB

```
┌──(kali㉿kaliA)-[~]
└─$ ping -c2 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.

--- 10.10.10.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1034ms


┌──(kali㉿kaliA)-[~]
└─$ ping -c2 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1014ms


┌──(kali㉿kaliA)-[~]
└─$ ping -c2 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.

--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1004ms
```

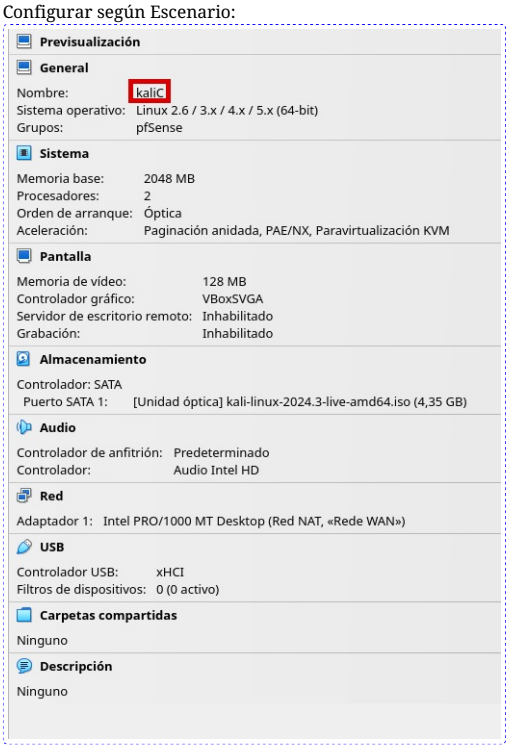
Resumo Escenario Actual

	pfSense → kaliB	kaliB → pfSense	kaliB → Internet	kaliA → kaliB	kaliB → kaliA
ping	SI	SI	SI	NON	SI
nc (ports TCP 80/443)					SI



WAN - Máquina virtual C: Kali amd64

13. Configurar según Escenario:



14. Na contorna gráfica abrir un terminal e executar:
    kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
    kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal **WANabc123.** (Ollo que o contrasinal ten un caracter punto final).

15. Configuración da rede:

kaliC será cliente DHCP, polo cal recollerá a configuración de rede da propia **Rede NAT de VirtualBox(Rede WAN)** a través da súa interface eth0

> Nesta práctica a IP/MS concedida por VirtualBox para kaliC foi: 172.16.0.8/24. Esta IP/MS pode variar na execución desta práctica. Se se quere proceder coa configuración 172.16.0.8/24 débese cambiar a IP estática a interface eth0 de kaliC e manter as táboas de rutas e o ficheiro /etc/resolv.conf como se amosa a continuación.

kali@kali:~$ ip addr show eth0 #Amosar a configuración da tarxeta de rede interna(eth0) con IP/MS: 172.16.0.8/24 recollida polo DHCP (eth0) de VirtualBox.
kali@kali:~$ ip route show || ip route list || ip route || ip r # Listar a táboa de enrutamento otorgada polo servidor DHCP.
kali@kali:~$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.

```
┌──(kali㉿kaliC)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 08:00:27:67:b8:c7 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.8/24 brd 172.16.0.255 scope global dynamic noprefixroute eth0
       valid_lft 538sec preferred_lft 538sec
    inet6 fe80::5de9:e4b0:dff5:ad97/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kaliC)-[~]
└─$ ip route
default via 172.16.0.1 dev eth0 proto dhcp src 172.16.0.8 metric 100
172.16.0.0/24 dev eth0 proto kernel scope link src 172.16.0.8 metric 100

┌──(kali㉿kaliC)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 8.8.8.8
```

16. Cambiar hostname da máquina virtual C. Por kaliC como hostname:

OPCIÓN A:
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
    root@kali:~# echo 'kaliC' > /etc/hostname #Indicar ao sistema o valor do hostname.
    root@kali:~# echo 'kernel.hostname=kaliC' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
    root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
    root@kali:~# echo -e '172.16.0.8\tkaliC' >> /etc/hosts #Engadir o hostname kaliC en /etc/hosts
    root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

OPCIÓN B:
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
    root@kali:~# hostnamectl hostname kaliC || hostnamectl set-hostname kaliC #Modificar o hostname do sistema a kaliC.
    root@kali:~# echo -e '172.16.0.8\tkaliC' >> /etc/hosts #Engadir o hostname kaliC en /etc/hosts
    root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

	pfSense → kaliC	kaliC → pfSense	kaliC → Internet	kaliA → kaliC	kaliC → kaliA	kaliB → kaliC	kaliC → kaliB
ping	SI	NON	SI	NON	NON	SI	NON
nc (ports TCP 80/443)					NON		

Agora podemos comprobar que dende pfSense **SI** é posible establecer conectividade cun ping a kaliC(172.16.0.8), pero que dende kaliC non é posible establecer conectividade cun ping a pfSense(en calquera das interfaces em0,em1,em2) e **SI** con Internet.

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping -c2 172.16.0.8
PING 172.16.0.8 (172.16.0.8): 56 data bytes
64 bytes from 172.16.0.8: icmp_seq=0 ttl=64 time=1.279 ms
64 bytes from 172.16.0.8: icmp_seq=1 ttl=64 time=1.931 ms

--- 172.16.0.8 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.279/1.605/1.931/0.326 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

```
┌──(kali㉿kalic)-[~]
└─$ ping -c2 172.16.0.7
PING 172.16.0.7 (172.16.0.7) 56(84) bytes of data.

── 172.16.0.7 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1012ms


┌──(kali㉿kalic)-[~]
└─$ ping -c2 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.

── 10.10.10.1 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1028ms


┌──(kali㉿kalic)-[~]
└─$ ping -c2 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.

── 192.168.1.1 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1016ms


┌──(kali㉿kalic)-[~]
└─$ ping -c2 www.google.es
PING www.google.es (216.58.215.163) 56(84) bytes of data.
64 bytes from mad41s07-in-f3.1e100.net (216.58.215.163): icmp_seq=1 ttl=114 time=24.9
 ms
64 bytes from mad41s07-in-f3.1e100.net (216.58.215.163): icmp_seq=2 ttl=114 time=22.1
 ms

── www.google.es ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 22.129/23.508/24.888/1.379 ms
```

Tamén podemos observar que dende kaliC **NON** é posible establecer conectividade cun ping a kaliA e kaliB

```
┌──(kali㉿kalic)-[~]
└─$ ping -c2 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.

── 10.10.10.10 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1021ms


┌──(kali㉿kalic)-[~]
└─$ ping -c2 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
From 192.168.1.38 icmp_seq=1 Destination Host Unreachable
From 192.168.1.38 icmp_seq=2 Destination Host Unreachable

── 192.168.1.100 ping statistics ──
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1015ms
pipe 2
```

E dende kaliB **SI** temos conectividade con kaliC.

```
┌──(kali㉿kaliB)-[~]
└─$ ping -c2 172.16.0.8
PING 172.16.0.8 (172.16.0.8) 56(84) bytes of data.
64 bytes from 172.16.0.8: icmp_seq=1 ttl=63 time=1.69 ms
64 bytes from 172.16.0.8: icmp_seq=2 ttl=63 time=3.41 ms

── 172.16.0.8 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 1.693/2.549/3.405/0.856 ms
```

E dende kaliA **NON** temos conectividade con kaliC.

```
File  Actions  Edit  View  Help
┌──(kali㉿kaliA)-[~]
└─$ ping -c2 172.16.0.8
PING 172.16.0.8 (172.16.0.8) 56(84) bytes of data.

── 172.16.0.8 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1006ms
```

Tamén podemos observar que dende kaliB **SI** é posible chegar ao porto TCP 80(servizo web apache2) de kaliA; cousa que non acontece dende kaliC.

```
┌──(kali㉿kaliB)-[~]
└─$ nc -vz 10.10.10.10 80 443
10.10.10.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.10] 80 (http) open
(UNKNOWN) [10.10.10.10] 443 (https) open
```

```
┌──(kali㉿kalic)-[~]
└─$ nc -vz 10.10.10.10 80 443
10.10.10.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.10] 80 (http) : Connection timed out
(UNKNOWN) [10.10.10.10] 443 (https) : Connection timed out
```

Resumo Estado Actual

kaliA ∈ DMZ | kaliB ∈ LAN | kaliC ∈ WAN

O que temos

	pfSense → kaliA	kaliA → pfSense	pfSense → kaliB	kaliB → pfSense	pfSense → kaliC	kaliC → pfSense
ping	SI	NON	SI	SI	SI	NON

	kaliA → Internet	kaliB → Internet	kaliC → Internet
ping	NON	SI	SI

	kaliA → kaliB	kaliB → kaliA	kaliA → kaliC	kaliC → kaliA	kaliB → kaliC	kaliC → kaliB
ping	NON	SI	NON	NON	SI	NON

	pfSense → kaliA	kaliB → kaliA	kaliC → kaliA
nc (ports TCP 80/443)	SI	SI	NON

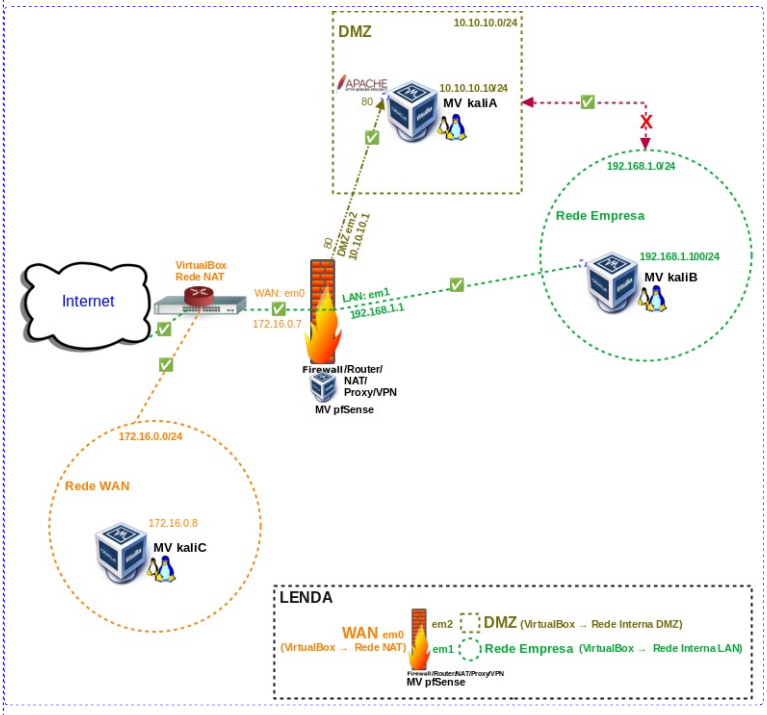
O que desexamos

	pfSense → kaliA	kaliA → pfSense	pfSense → kaliB	kaliB → pfSense	pfSense → kaliC	kaliC → pfSense
ping	SI	NON	SI	SI	SI	NON

	kaliA → Internet	kaliB → Internet	kaliC → Internet
ping	NON	SI	SI

	kaliA → kaliB	kaliB → kaliA	kaliA → kaliC	kaliC → kaliA	kaliB → kaliC	kaliC → kaliB
ping	NON	SI	NON	NON	SI	NON

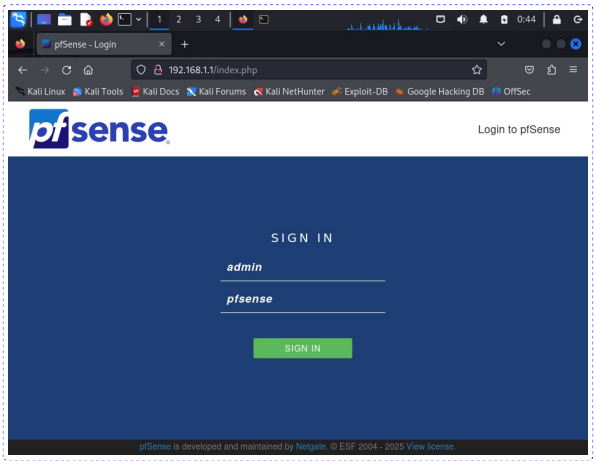
	pfSense → kaliA	kaliB → kaliA	kaliC → kaliA
nc (ports TCP 80/443)	SI	SI	SI



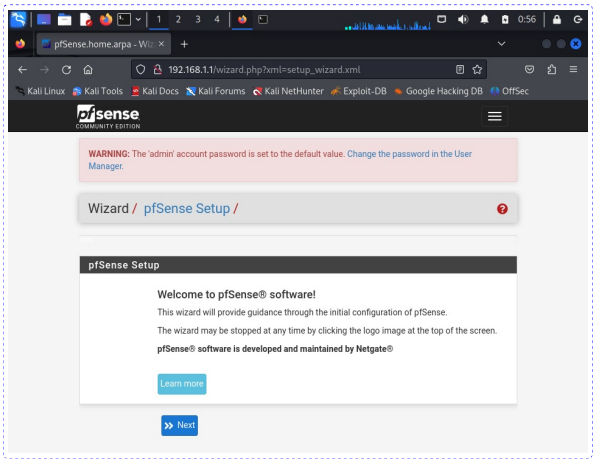
Entón, para consiguir o desexado temos que configurar novas regras de firewall en pfSense.

17. **Configuración Inicial**

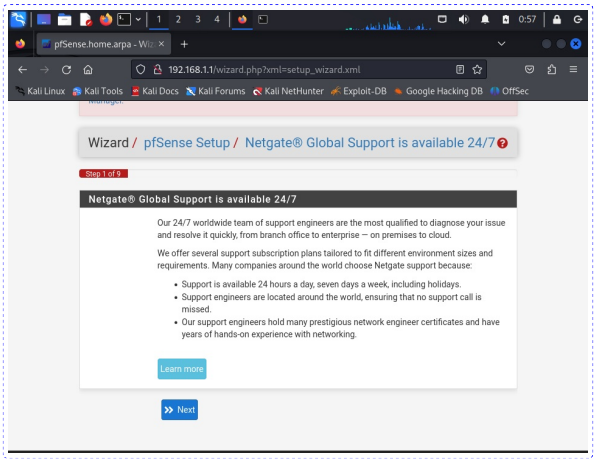
Antes de xerar as regras debemos acceder a aplicación de pfSense(http://192.168.1.1) e proceder coa configuración inicial de pfSense.
Este procedemento farase dende kaliB.



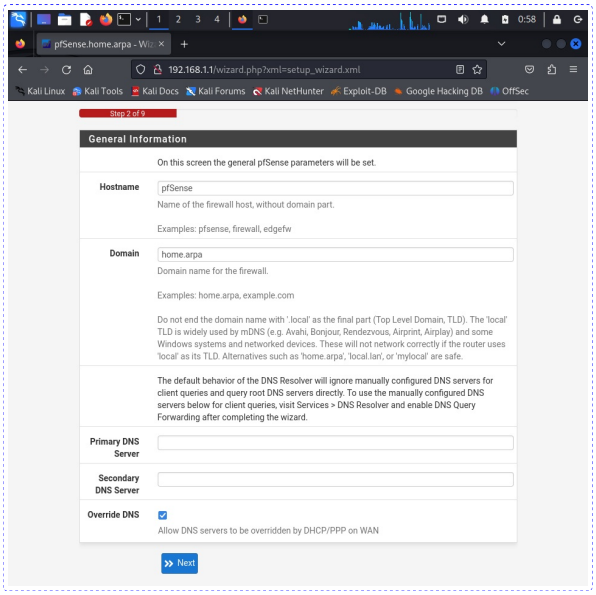
Acceder coas credenciais: admin/pfSense



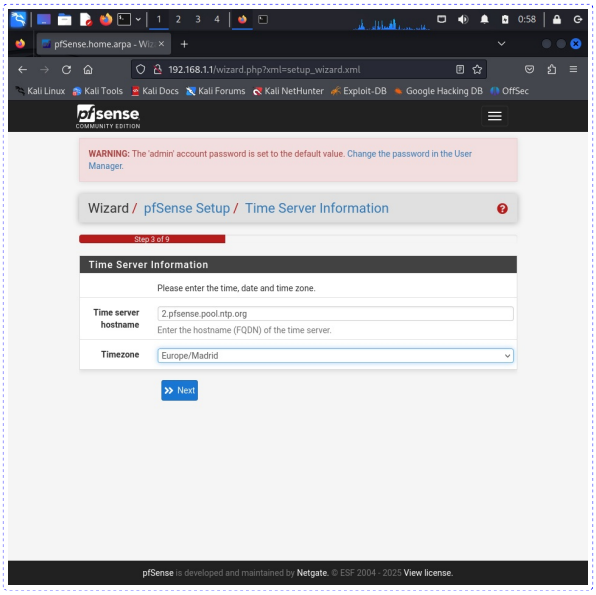
Premer en Next



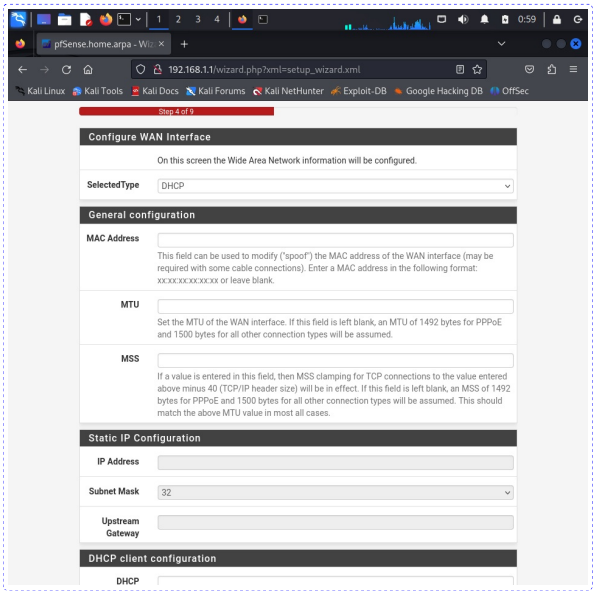
Premer en Next



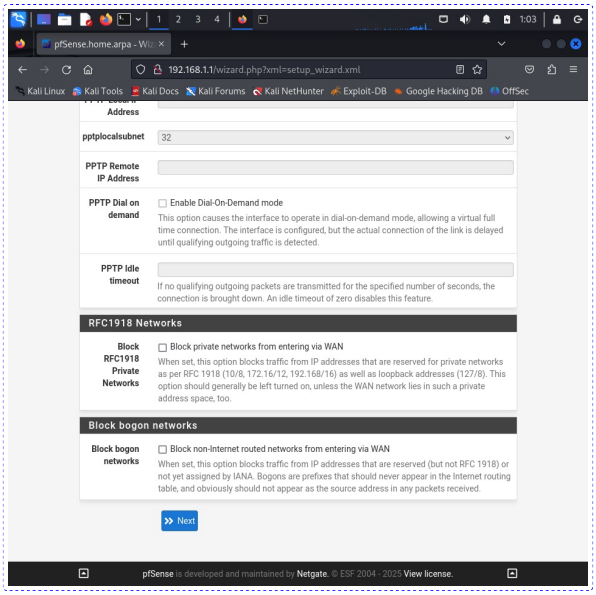
Premer en Next



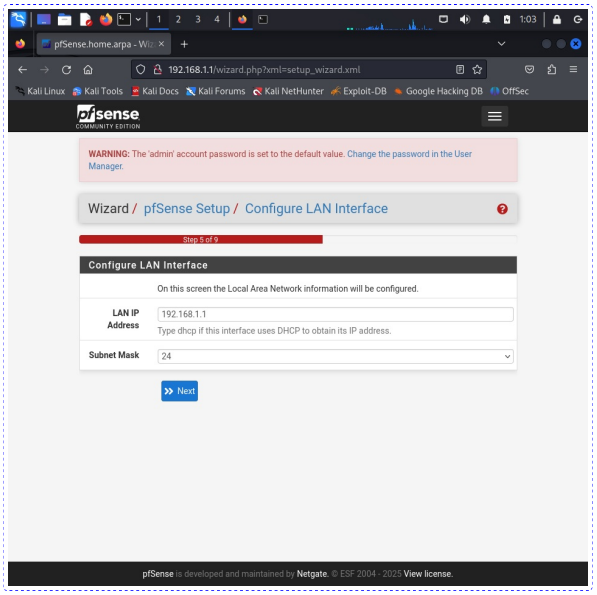
Premer en Next



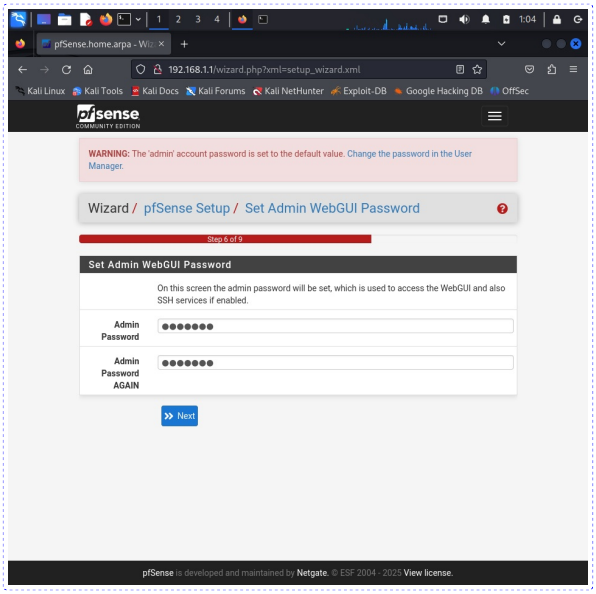
Baixar para chegar ao botón Next



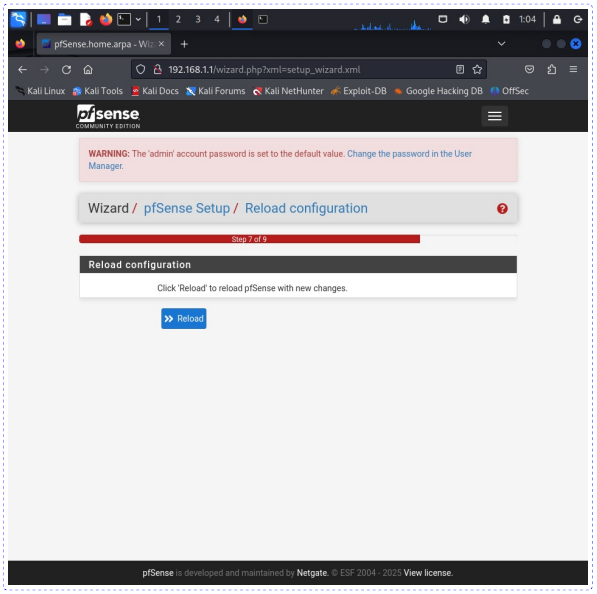
Antes de premer en Next asegurarse que non están activadas as 2 opcións **Block**



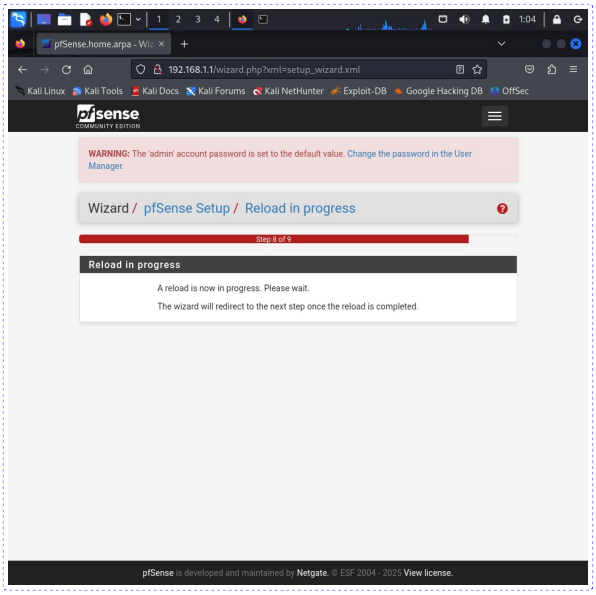
Confirmar que LAN posúe a configuración IPv4: 192.168.1.1/24 e premer en Next



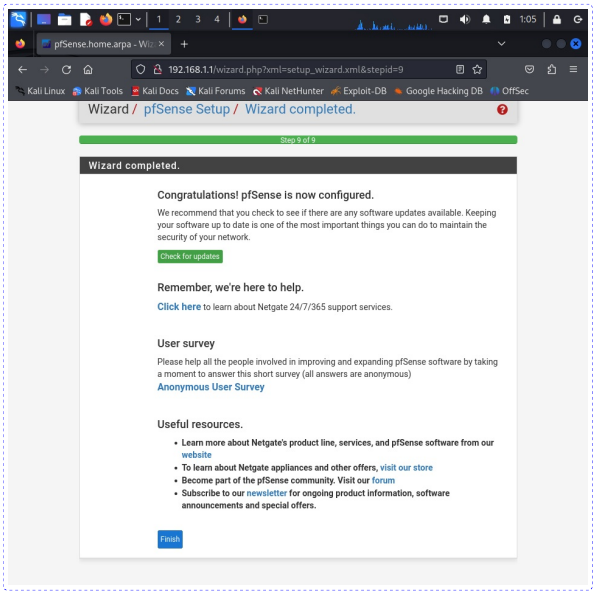
Débese modificar o contrasinal de admin -aínda que nesta práctica non se faga-, e logo premer en Next



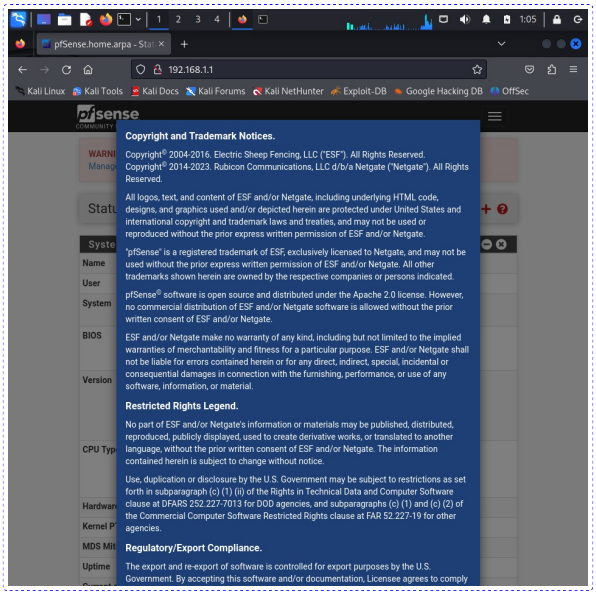
Premer en Reload



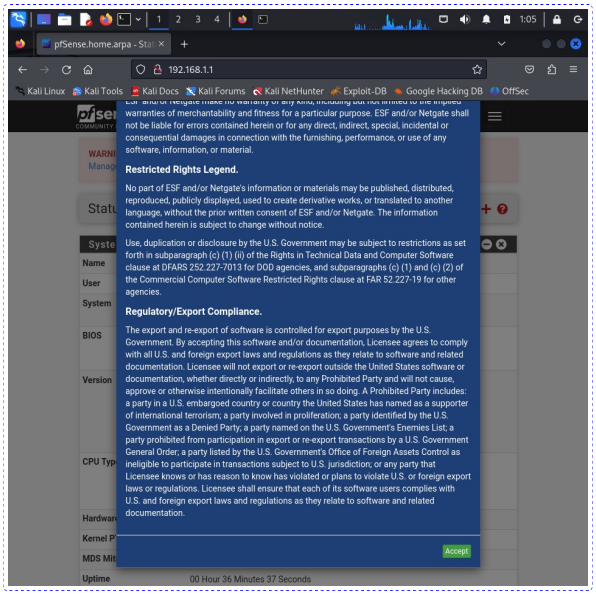
Recargando...



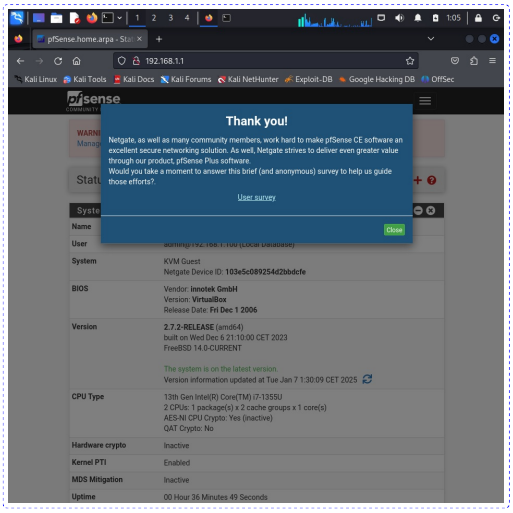
Proceso finalizado. Premer en Finish.



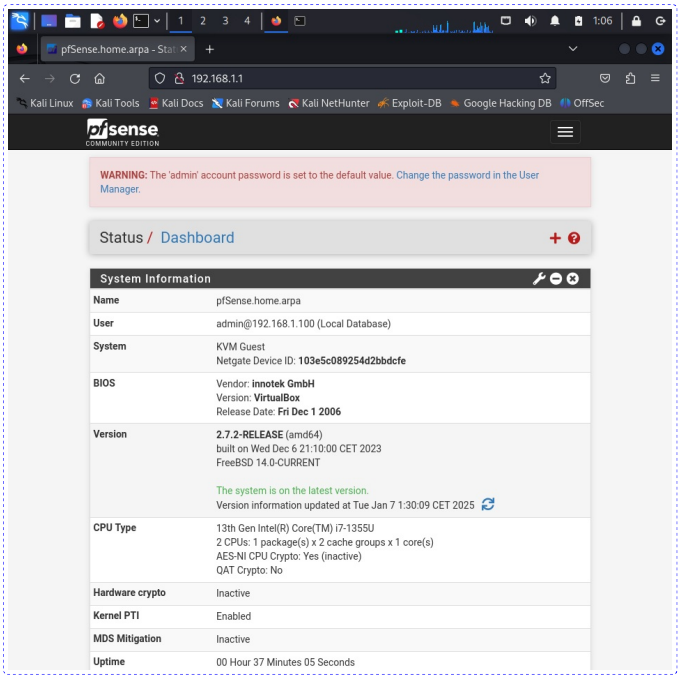
Baixar para ler a licenza.



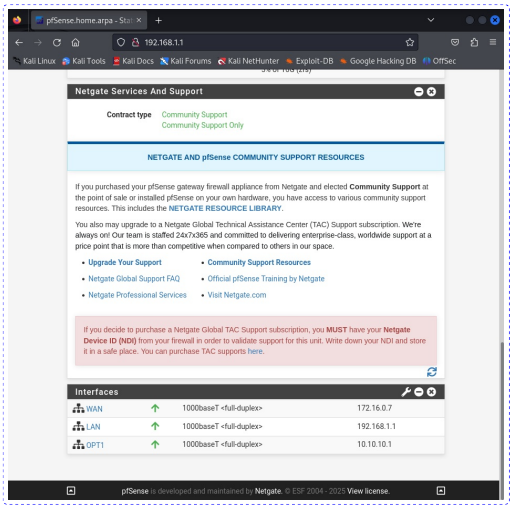
Aceptar licenza. Premer en Accept.



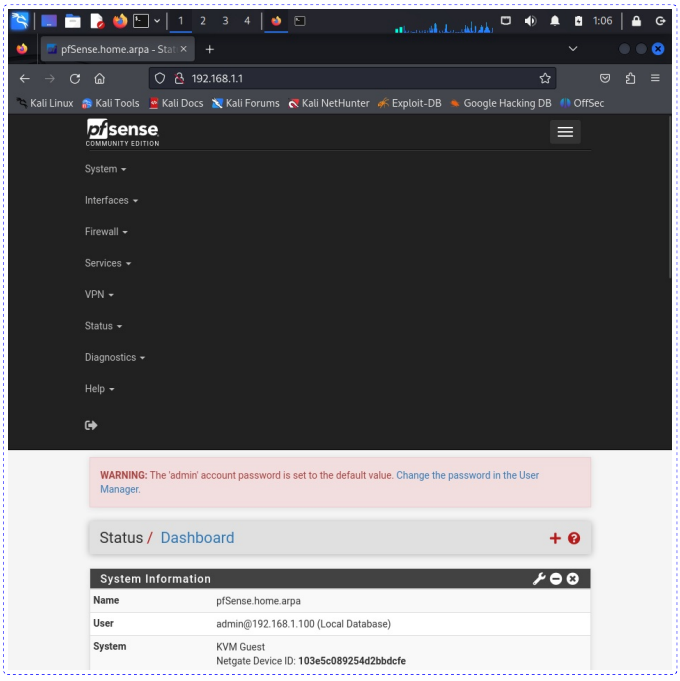
Licenza aceptada. Premer en Close.



Amósase información do sistema pfSense.



Baixando a pantalla vemos un resumo das Interfaces.



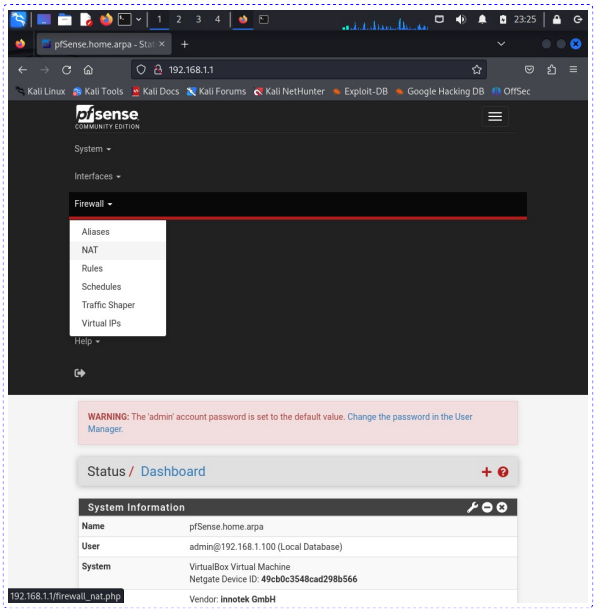
Menú de pfSense. Dependendo das dimensións da pantalla verase en vertical(picar no botón) ou verase en horizontal de forma predeterminada.

Firewall: Regras Port Forwarding.

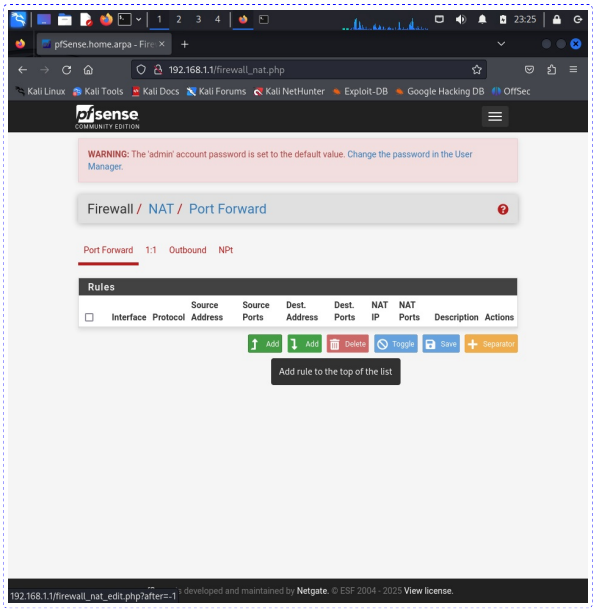
Imos engadir a seguintes regras en pfSense:

1. Permitir(pass) redirección(NAT) kaliC → kaliA ao servidor Web Apache (port tcp 80)
2. Permitir(pass) redirección(NAT) kaliC → kaliA ao servidor Web Apache (port tcp 443)

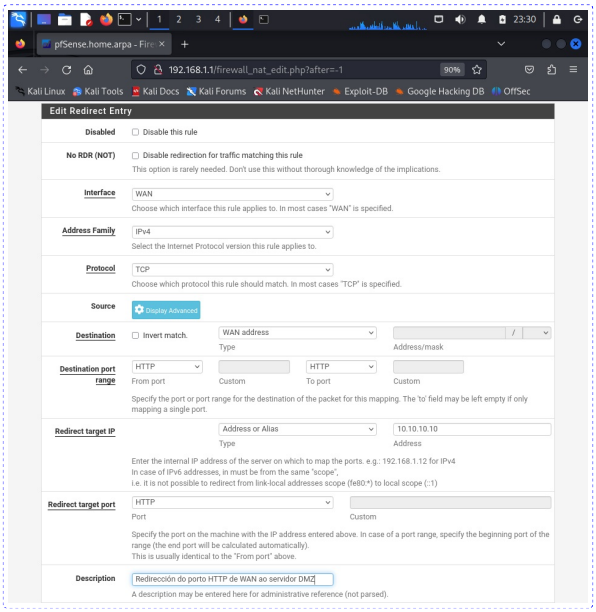
18. **Exemplo1. Port Forwarding kaliC(WAN) $\xrightarrow{80}$ kaliA(DMZ)**



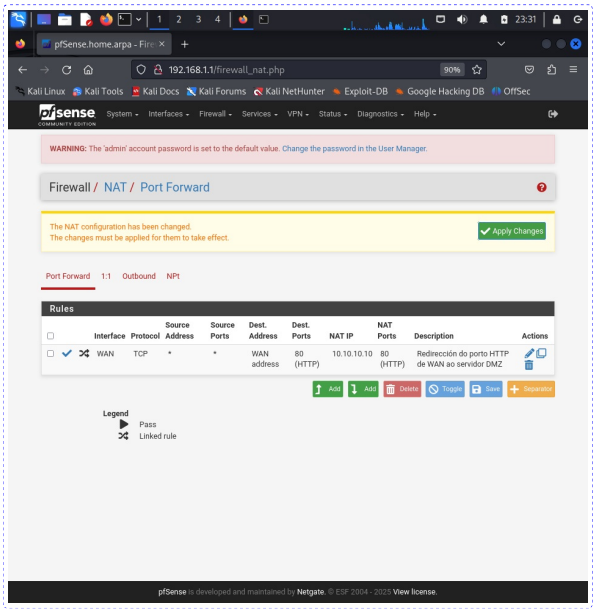
Para crear a primeira regra NAT escoller no menú a opción:
Firewall → NAT



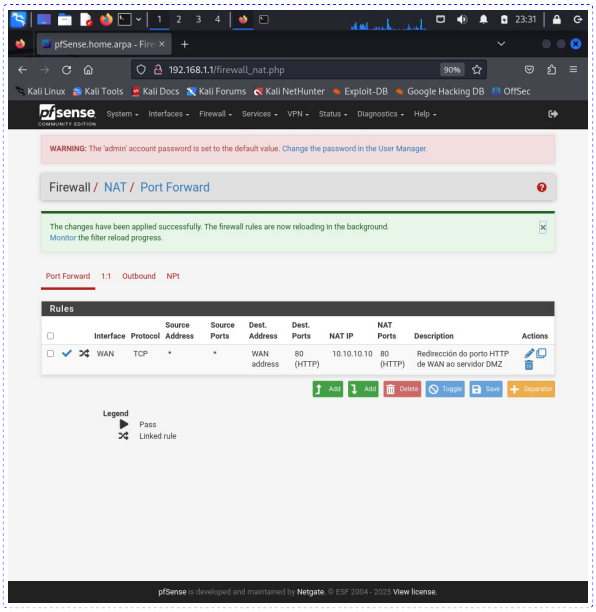
Premer en 



Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer en Save.



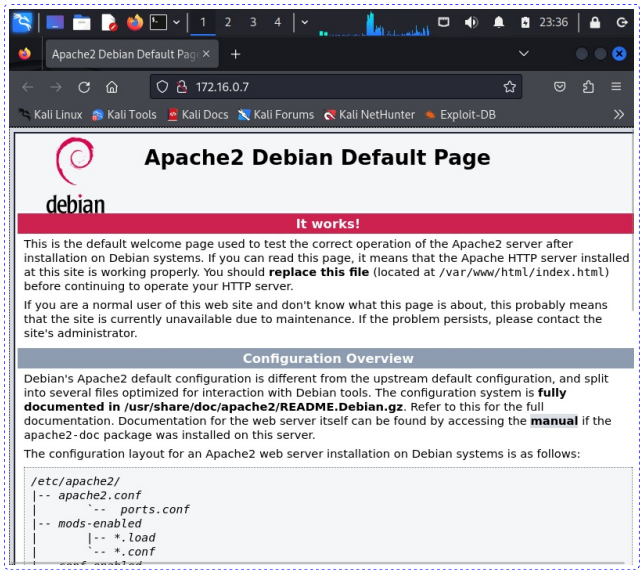
Para aplicar os cambios premer en "Apply Changes"



Cambios aplicados e regra xerada.

Probamos agora que **SI** é posible acceder dende kaliC ao servidor web da DMZ:

```
┌──(kali㉿kaliC)-[~]
└─$ nc -vz 10.10.10.10 80
10.10.10.10 [10.10.10.10] 80 (http) : Connection timed out

┌──(kali㉿kaliC)-[~]
└─$ nc -vz 172.16.0.7 80
172.16.0.7 [172.16.0.7] 80 (http) open
```

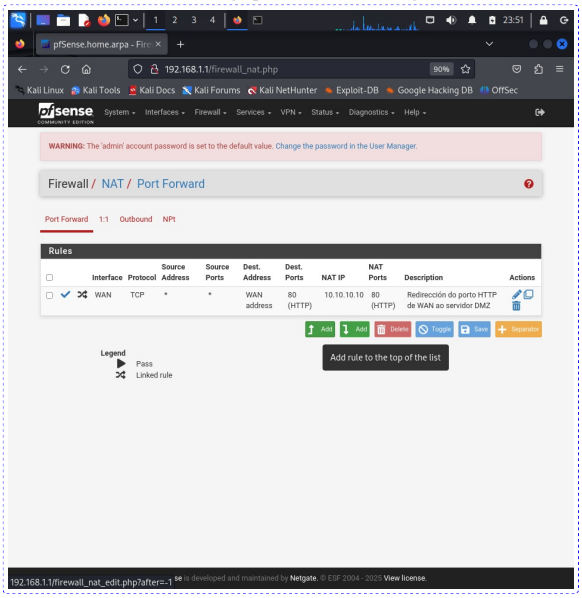


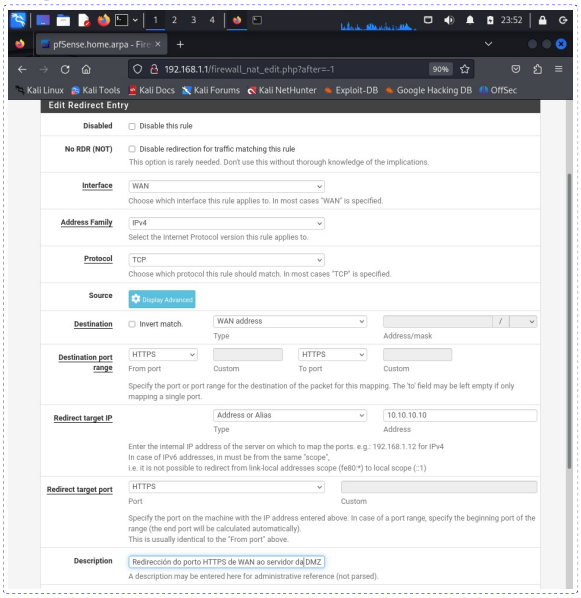
Comprobamos que seguimos sen poder ter conectividade dende kaliC(WAN) a kaliB(LAN)

```
┌──(kali㉿kaliC)-[~]
└─$ ping -c2 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
From 192.168.1.38 icmp_seq=1 Destination Host Unreachable
From 192.168.1.38 icmp_seq=2 Destination Host Unreachable

--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1030ms
pipe 2
```

19. **Exemplo2. Port Forwarding kaliC(WAN) → kaliA(DMZ) 443**

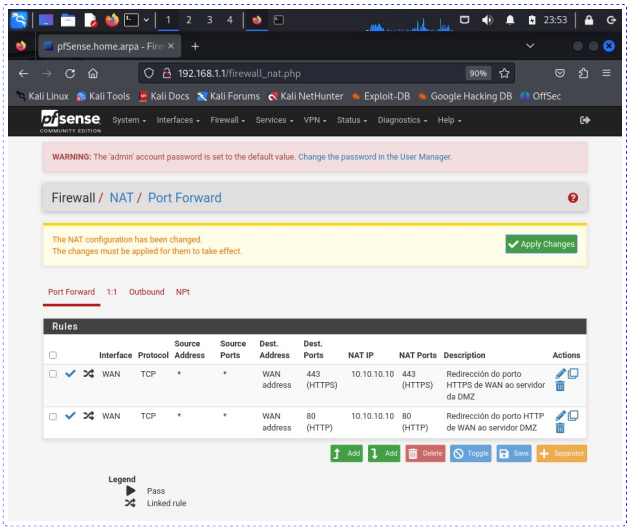
Procedemos de forma análoga para xerar unha regra de Port Forwarding para o porto 443(https):





Premer en 

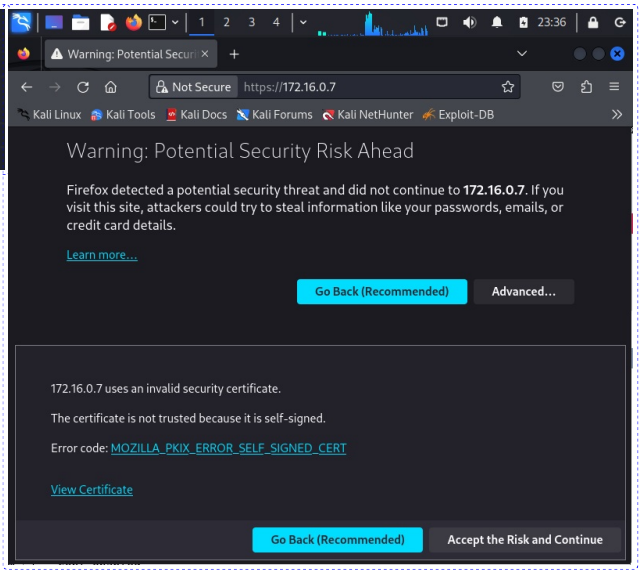
Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer en Save.

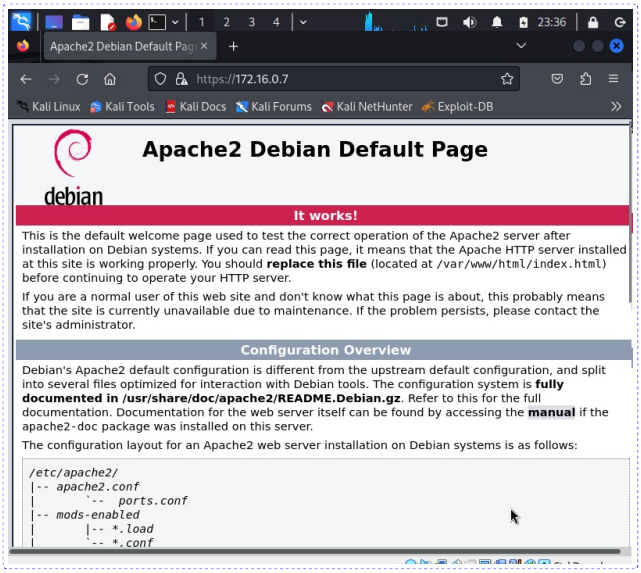


Para aplicar os cambios premer en "Apply Changes"

Probamos agora que **SI** é posible acceder dende kaliC ao servidor web, mediante https, da DMZ:

```
┌──(kali㉿kaliC)-[~]
└─$ nc -vz 10.10.10.10 80 443
10.10.10.10 [10.10.10.10] 80 (http) : Connection timed out
10.10.10.10 [10.10.10.10] 443 (https) : Connection timed out

┌──(kali㉿kaliC)-[~]
└─$ nc -vz 172.16.0.7 80 443
172.16.0.7 [172.16.0.7] 80 (http) open
172.16.0.7 [172.16.0.7] 443 (https) open
```





Comprobamos que seguimos sen poder ter conectividade dende kaliC(WAN) a kaliB(LAN)

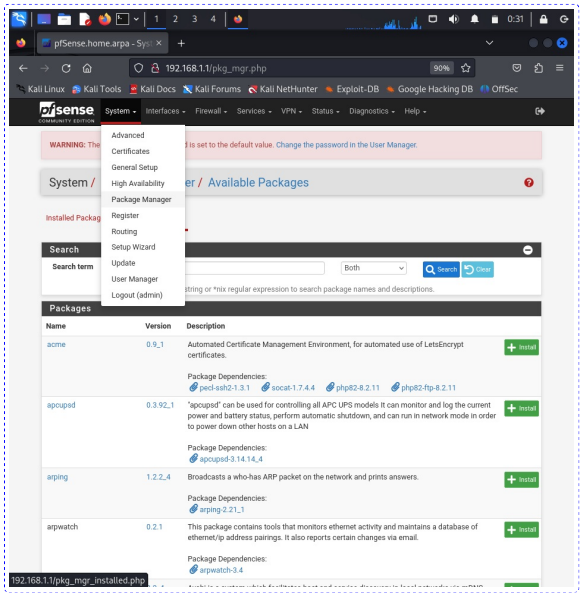
```
┌──(kali㉿kaliC)-[~]
└─$ ping -c2 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
From 192.168.1.38 icmp_seq=1 Destination Host Unreachable
From 192.168.1.38 icmp_seq=2 Destination Host Unreachable

--- 192.168.1.100 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1030ms
pipe 2
```

Proxy: Squid

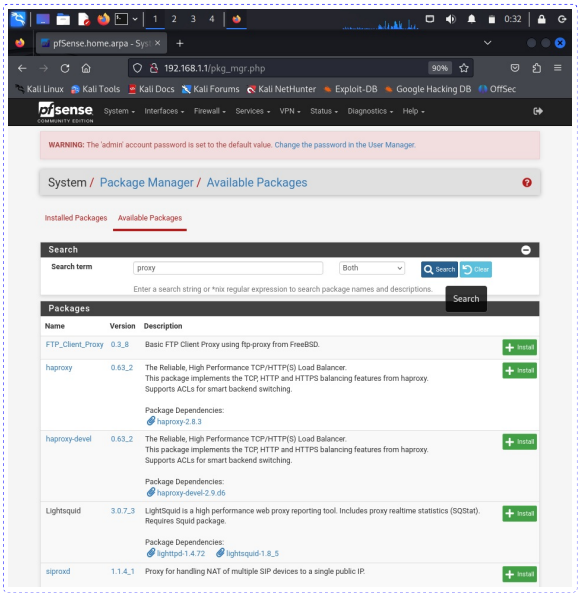
20. **Exemplo3. Proxy en pfSense**
Imos activar o proxy en pfSense para que as peticións web dende LAN(kaliB) saían a través deste proxy.

Procedemento:

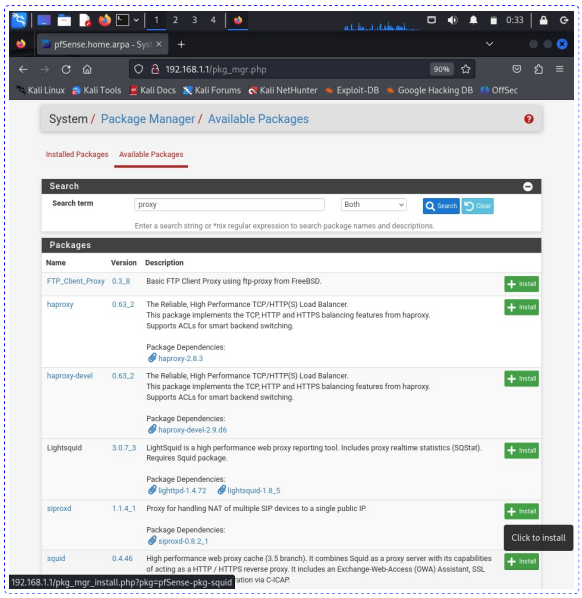
1. **Instalación do paquete squid en pfSense**. Entón, dende kaliB acceder ao panel de configuración de pfSense e proceder como segue:



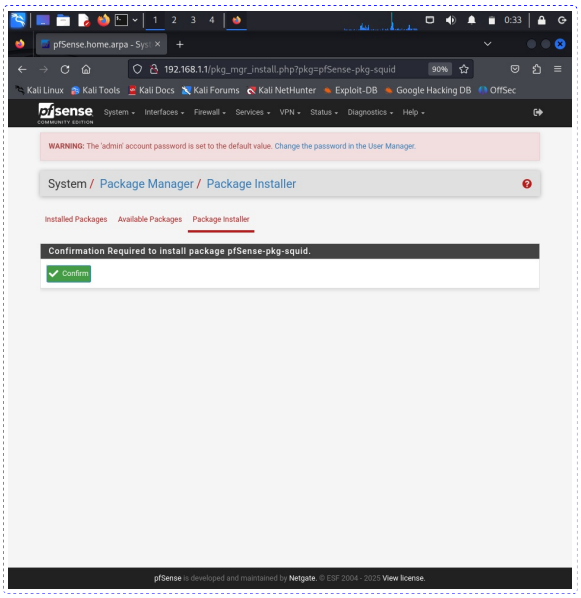
Abrir System → Package Manager



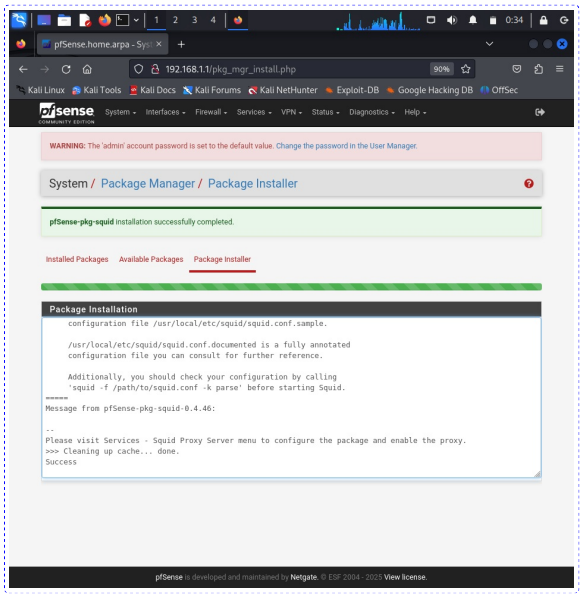
Buscar o patrón "proxy" os paquetes posibles a instalar.



Premer no botón Install do paquete squid para proceder a instalalo.

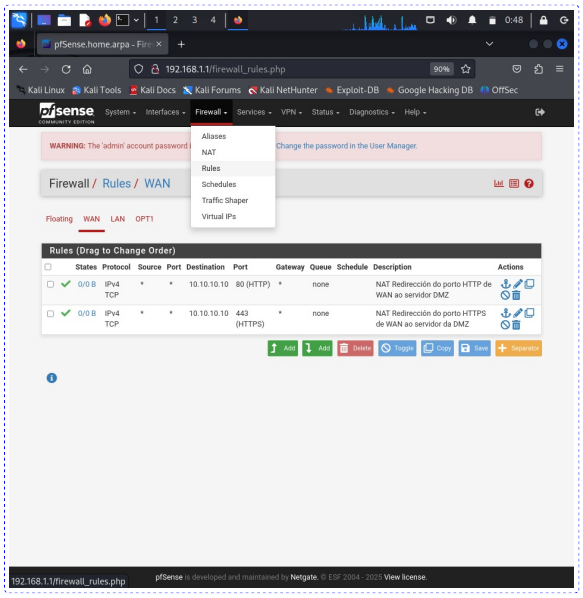


Premer no botón Confirm para confirmar a instalación requerida.

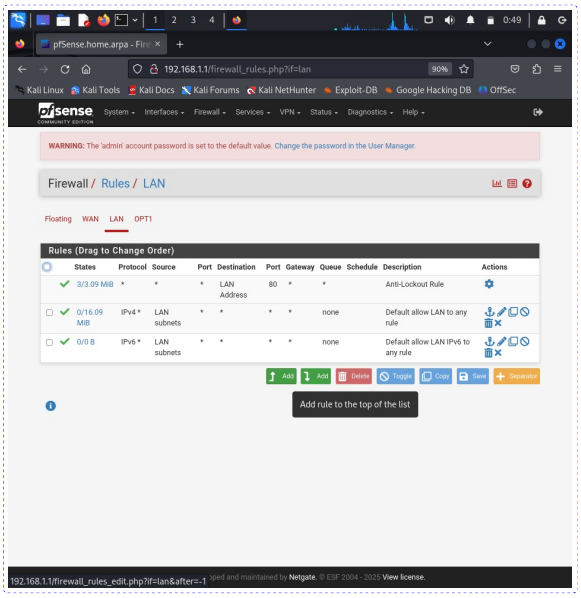


Instalación do paquete squid realizada.

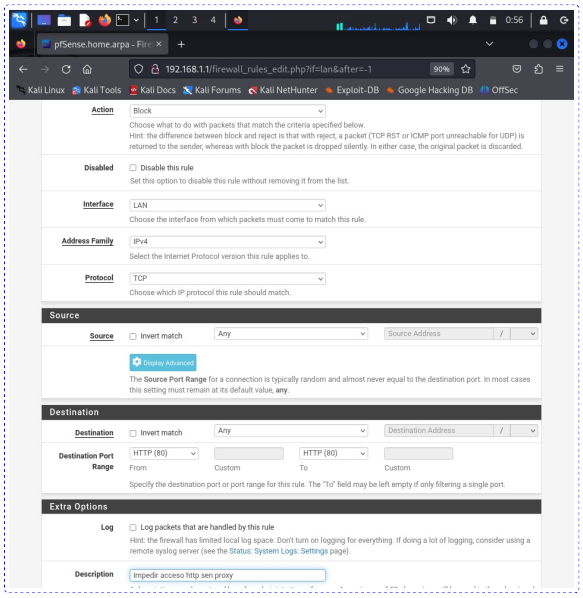
2. **Firewall: Regras LAN.** Imos xerar as regras que impiden dende a LAN(kaliB) as peticións de saída dos portos tcp 80(HTTP) e 443(HTTPS):



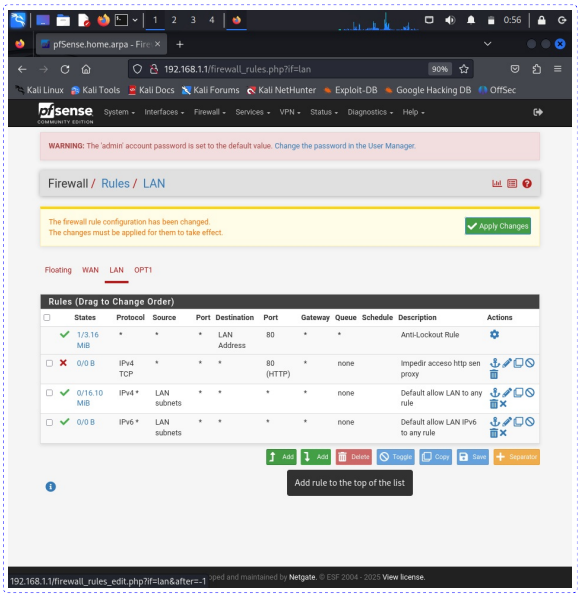
Abrir Firewall → Rules



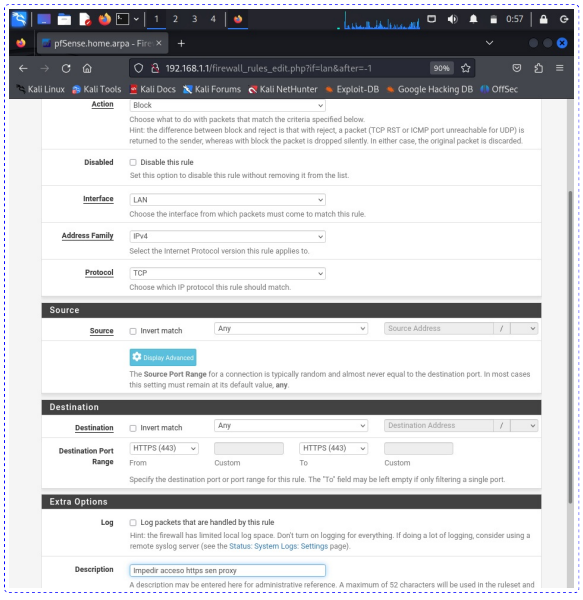
Escoller a opción LAN e premer en Add para engadir unha nova regra de firewall.



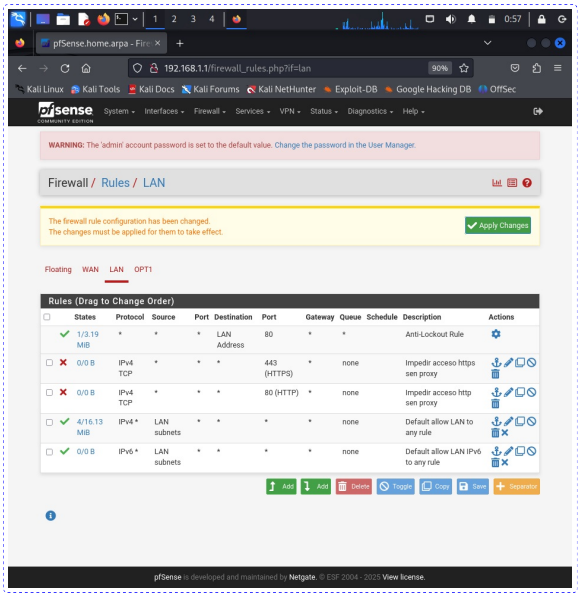
Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer en Save.



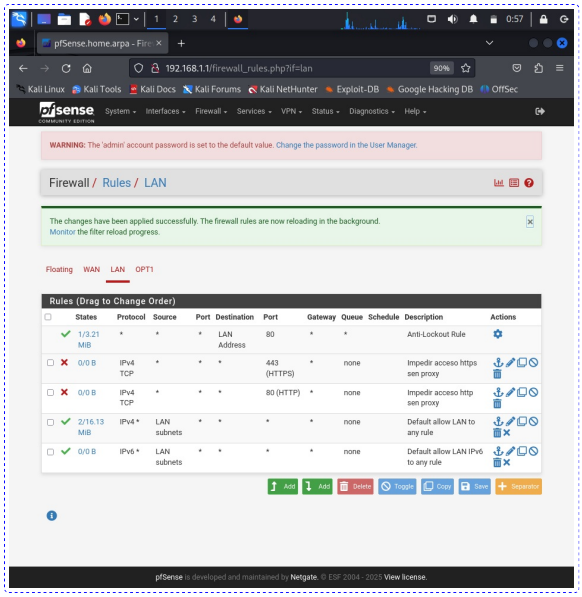
Premer de novo en Add para engadir unha nova regra de firewall.



Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer en Save.

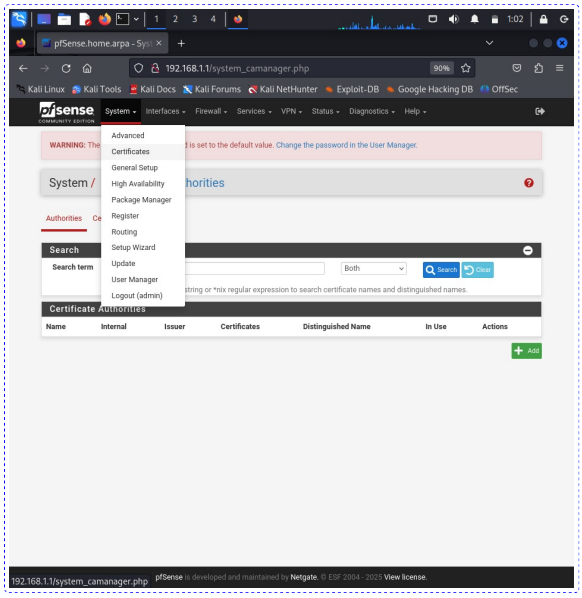


Para aplicar os cambios premer en "Apply Changes"

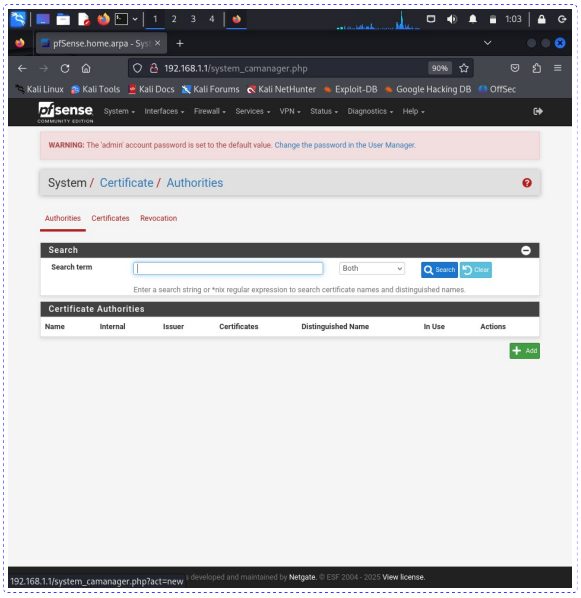


Cambios aplicados e regras xeradas.

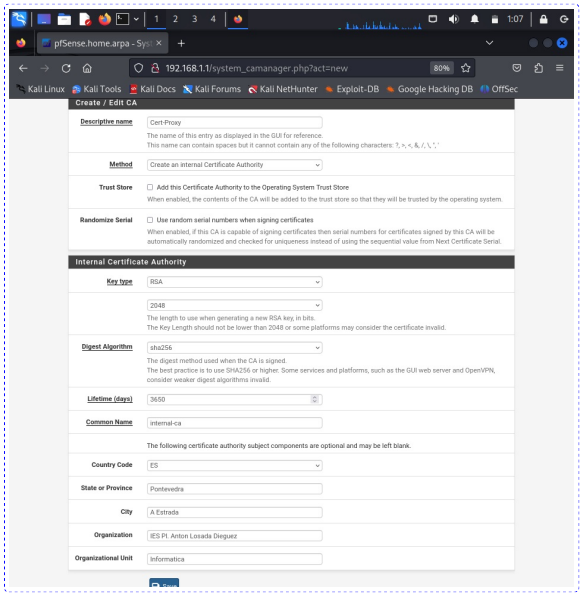
3. **Certificado SSL**: Imos xerar un certificado SSL para permitir o acceso ás páxinas web HTTPS.



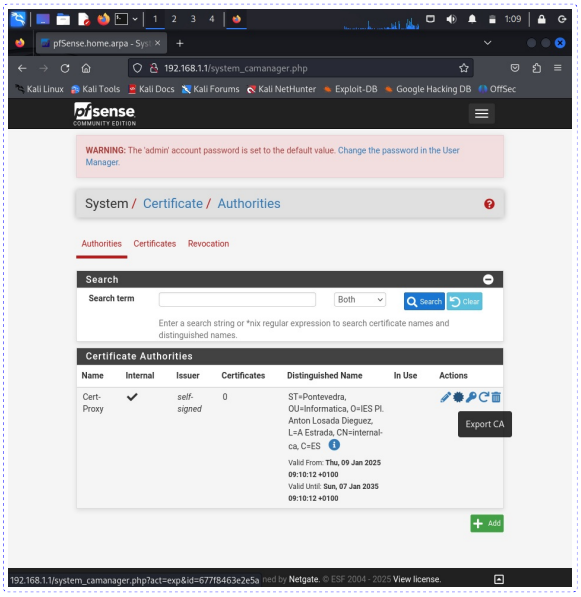
Abrir System → Certificates



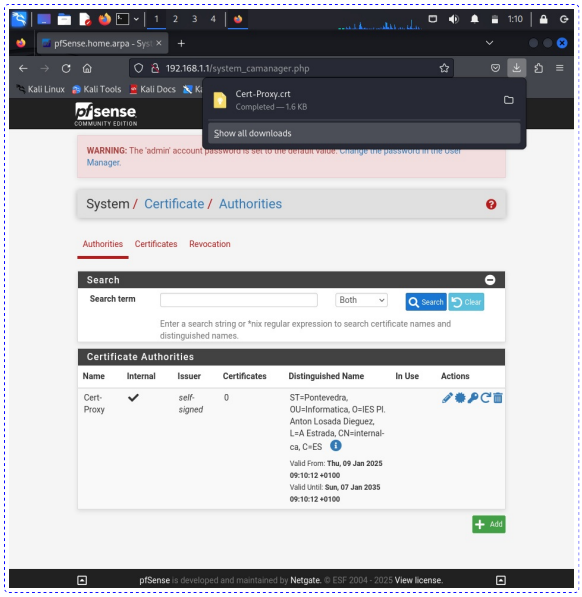
Premer en Add para xerar unha CA(Autoridade de Certificación) para que poidamos asinar/expedir certificados.



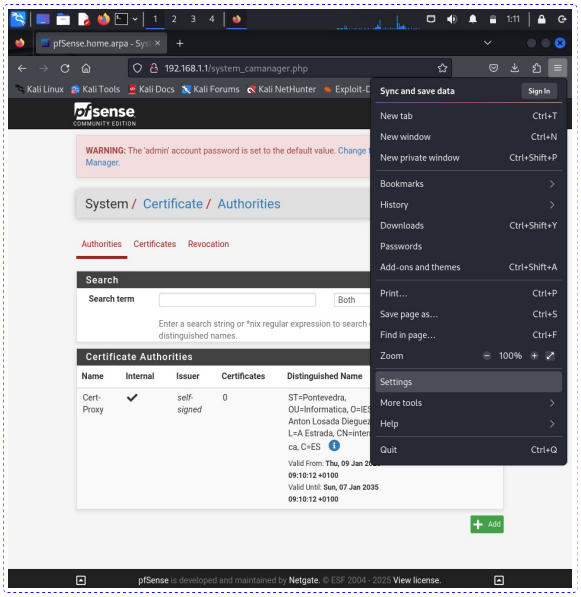
Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer en Save.



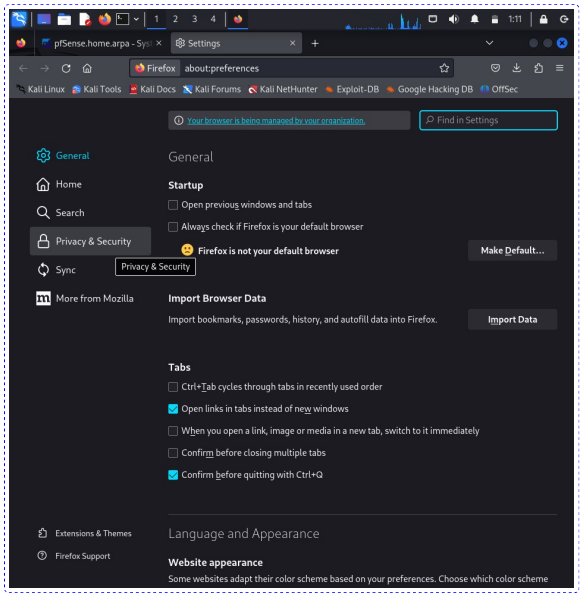
Premer no botón ⚙ para exportar o certificado xerado.



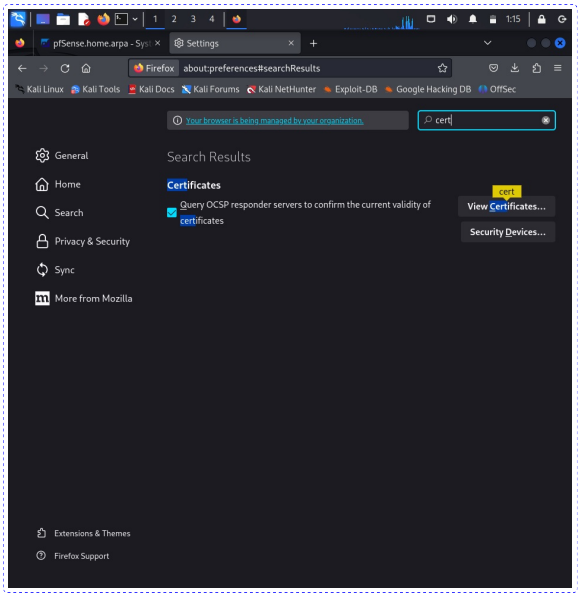
Certificado descargado (/home/kali/Downloads/Cert-Proxy.crt)



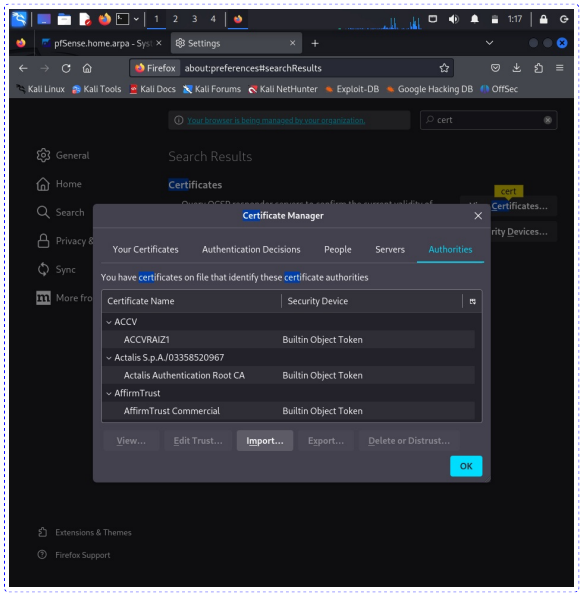
Ir á configuración(Settings) do navegador



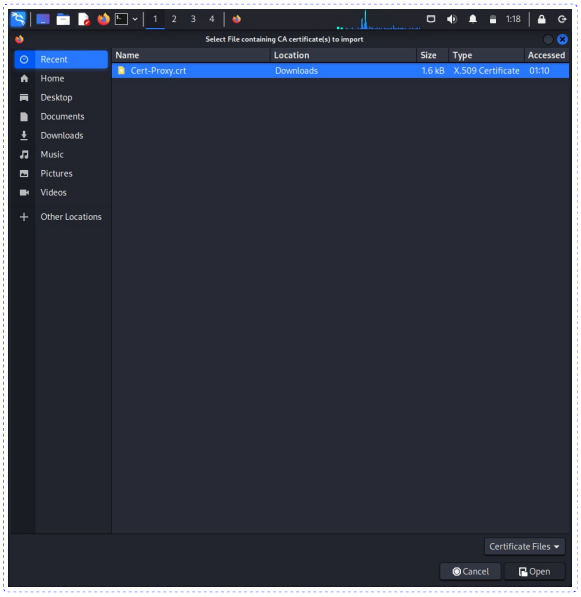
Escoller Privacy & Security



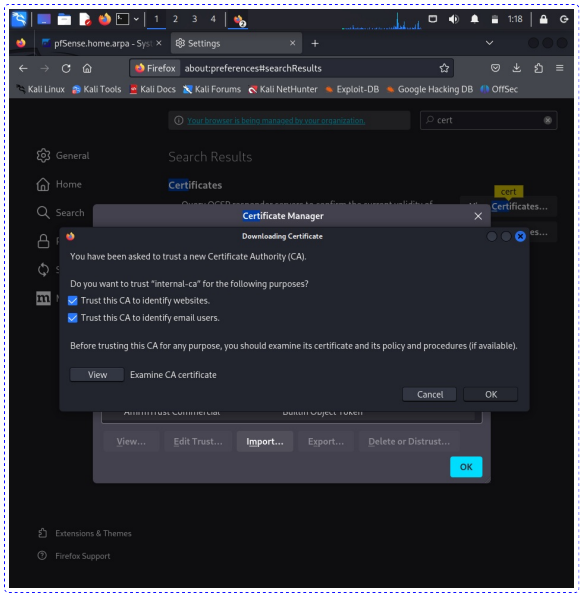
Ir á sección Certificates



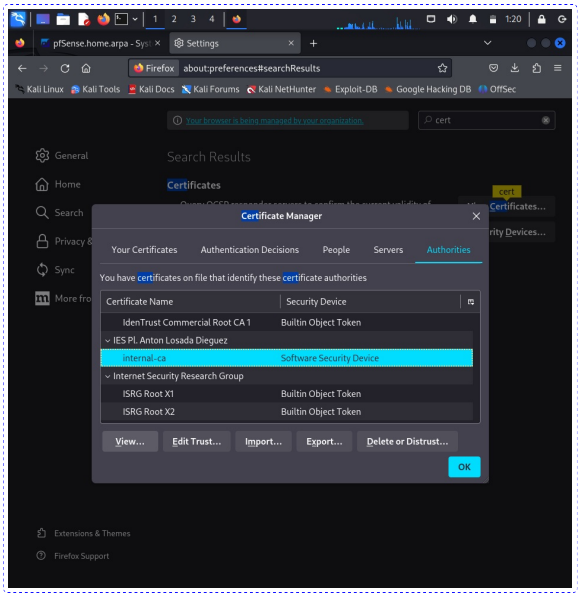
Importar o Certificado descargado na sección Authorities.



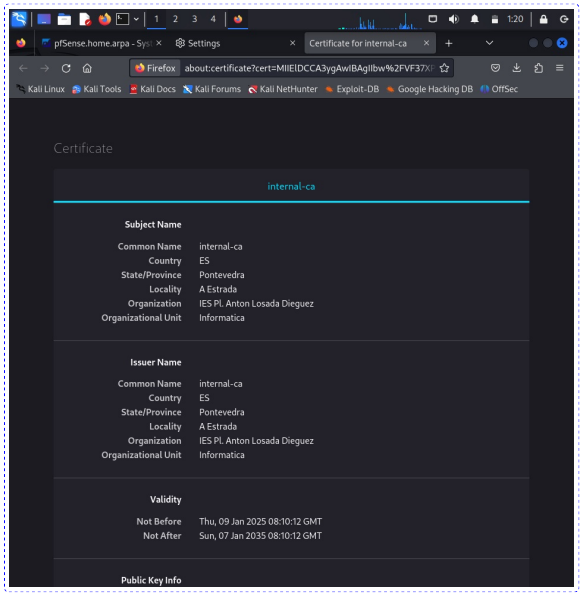
Escoller o certificado na ruta de descarga



Habilitar as opcións de confianza(Trust) e premer en OK.

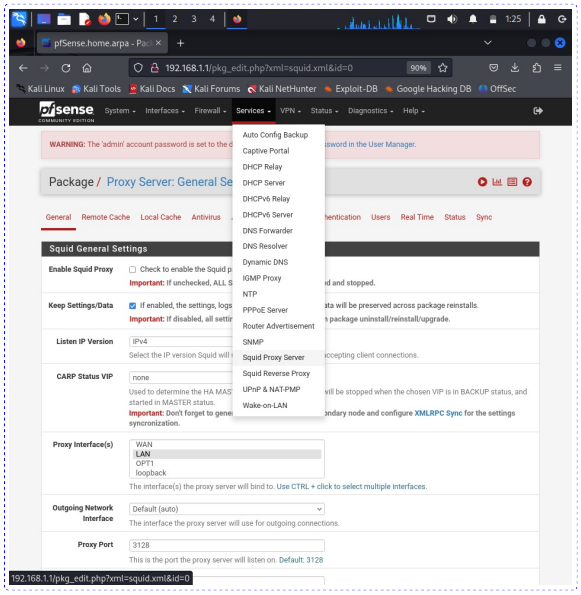


Certificado importado.

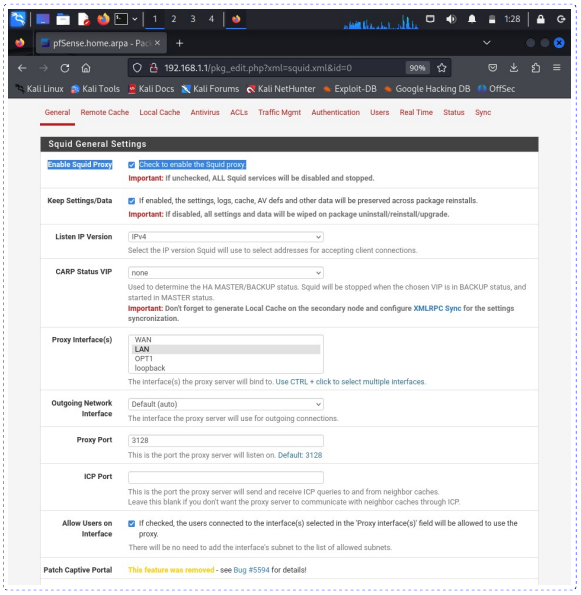


Ver as propiedades do certificado importado (premer na imaxe anterior en View co certificado seleccionado).

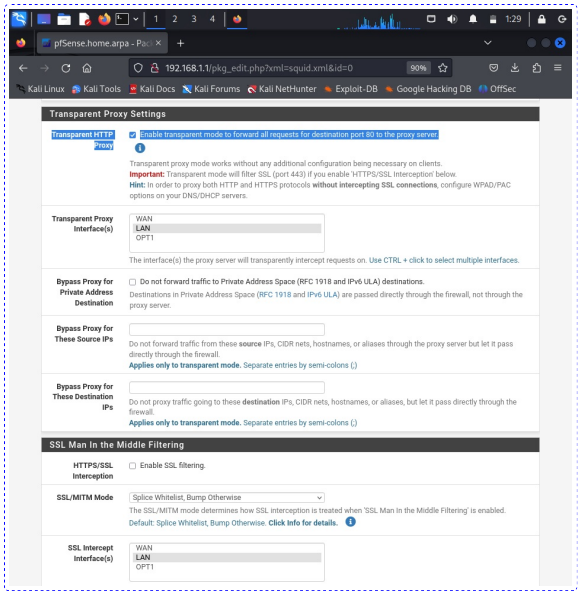
4. **Configuración SQUID**



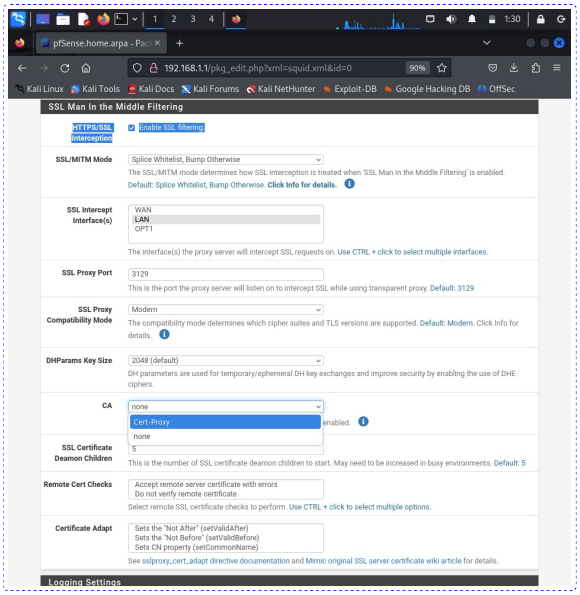
Abrir Services → Squid Proxy Server



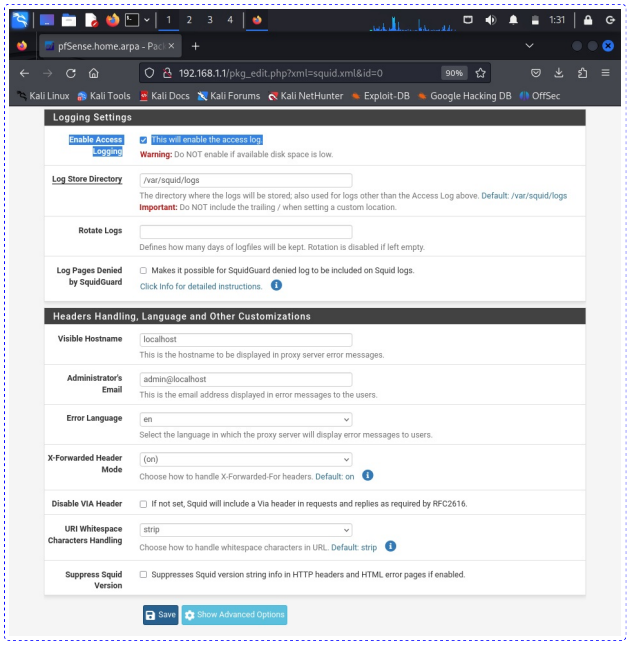
Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla.



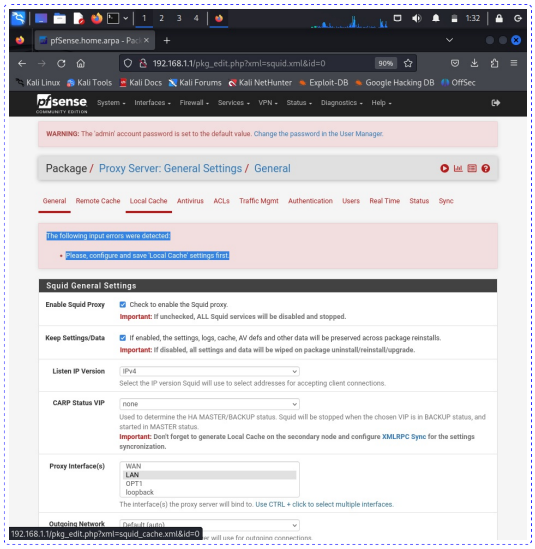
Escoller as opcións según aparece na imaxe para habilitar o modo transparente do proxy. Baixar a pantalla.



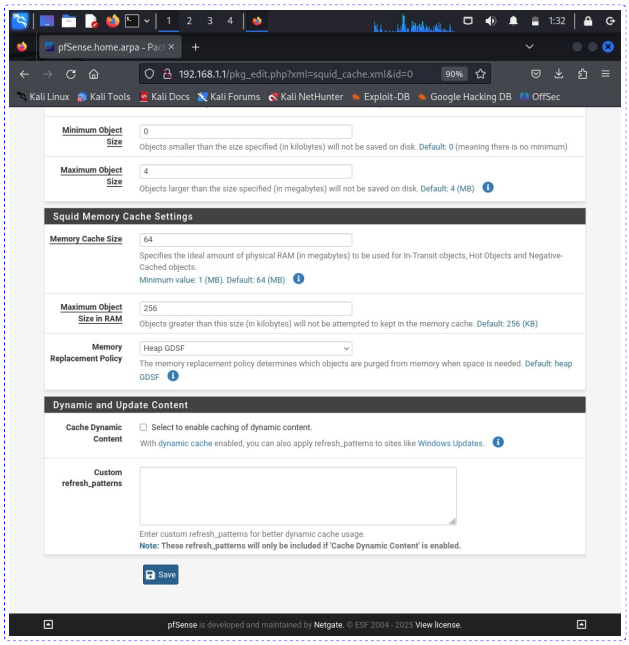
Escoller as opcións según aparece na imaxe para habilitar a intecepción HTTPS/SSL. Baixar a pantalla.



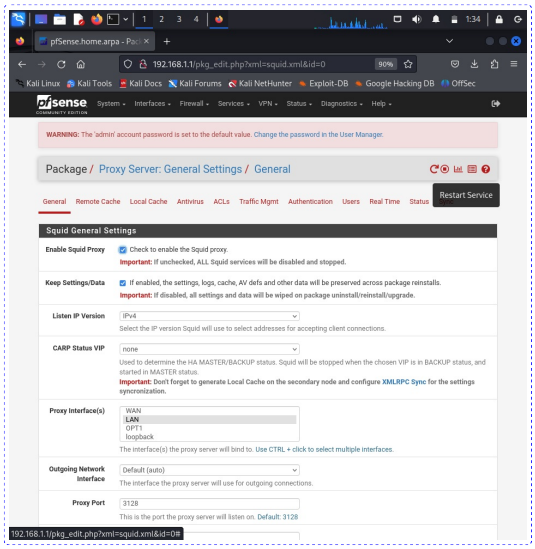
Escoller as opcións según aparece na imaxe para habilitar o rexistro. Baixar a pantalla e premer no botón Save.



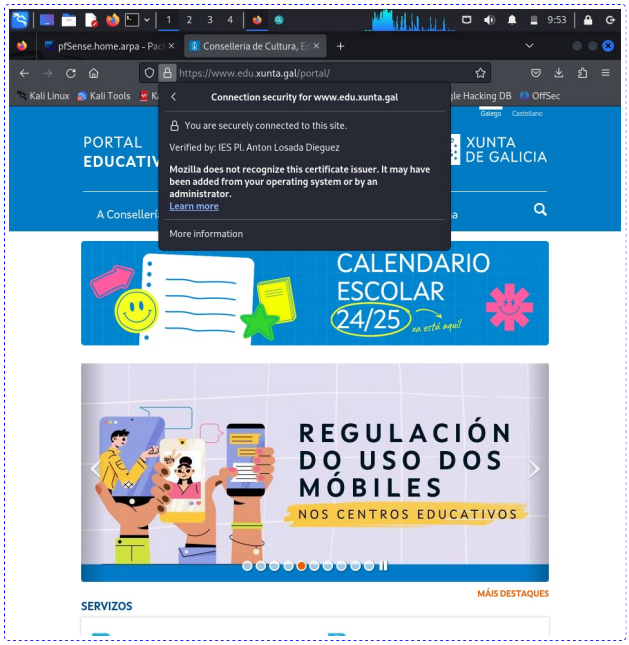
Ao intentar gardar premendo no botón Save o sistema de configuración de pfSense avisa que non é posible gardar a configuración porque primeiro debemos configurar e gardar a sección "Local Cache'



Esta imaxe amosa o botón Save comentado na imaxe anterior.



Entón, debemos dirixirnos "Local Cache", premer no botón Save e voltar a realizar a configuración SQUID (paso 4.)



Unha vez realizada a configuración do SQUID comprobamos que o acceso a Internet realízase a traveś do proxy e como a comunicación establécese mediante https é verificada co certificado escollido/xerado (IES Pl. Antón Losada Diéguez)

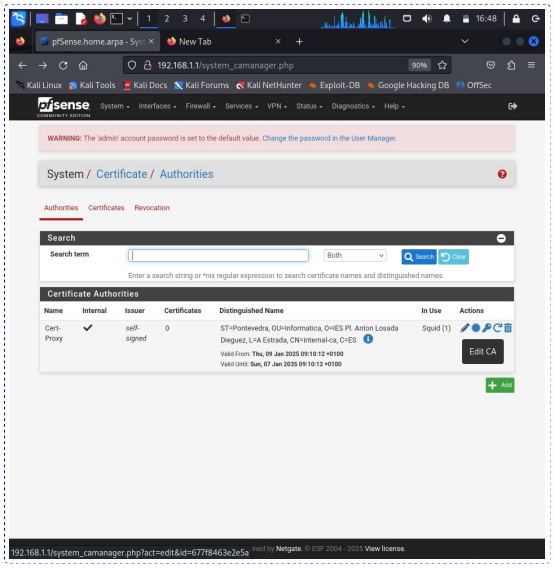
VPN: OpenVPN

21. Exemplo4. OpenVPN en pfSense. Acceso remoto kaliC(WAN) → kaliA(DMZ)[1194]

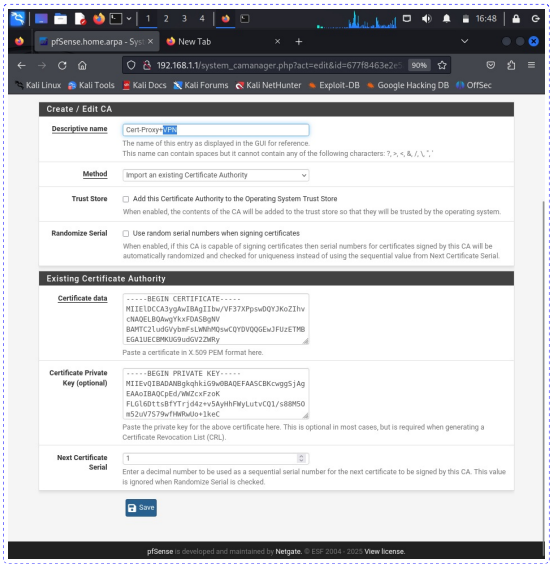
Imos configurar acceso VPN para que dende kaliC(WAN) poidamos conectarnos a través da VPN de pfSense a kaliB(LAN).

Procedemento:

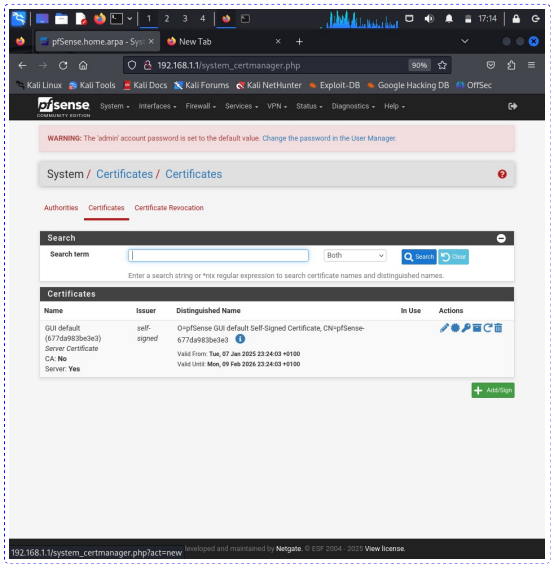
1. **Modificación da descripción do certificado da CA, creación do certificado do servidor VPN e de un cliente VPN**.
   Entón, dende kaliB acceder ao panel de configuración de pfSense e proceder como segue:



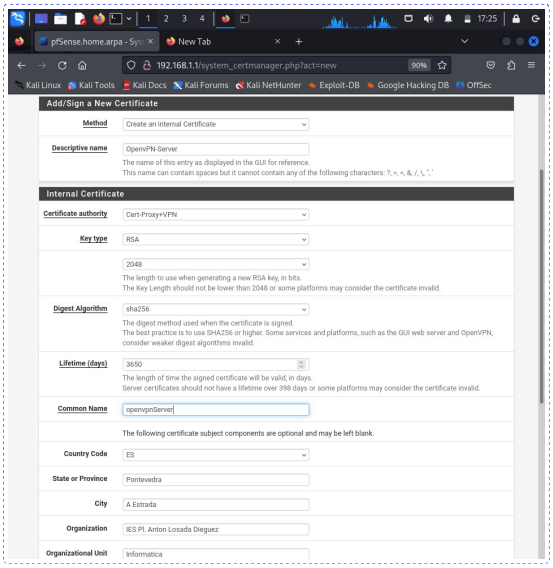
En System → Certificate → Authorities premer no botón  para editar o certificado anteriormente xerado.



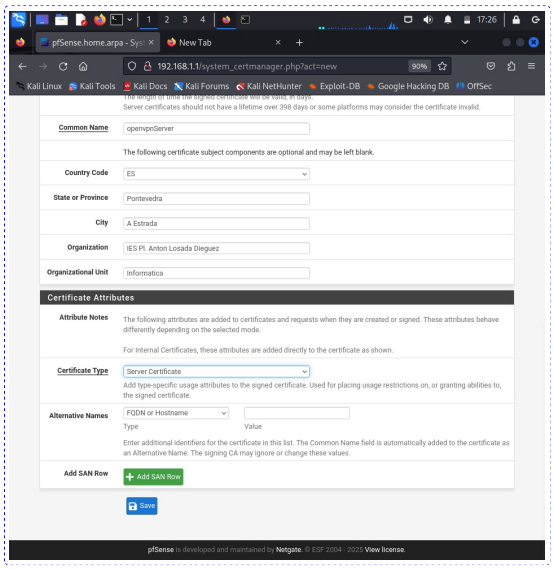
Modificar o campo "Description Name" e premer no botón Save.



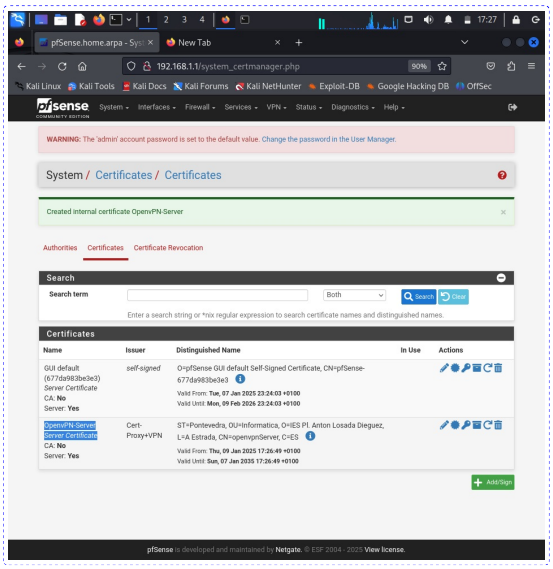
Na sección Certificates premer no botón "Add/Sign" para xerar o certificado para o servidor VPN.



Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla.

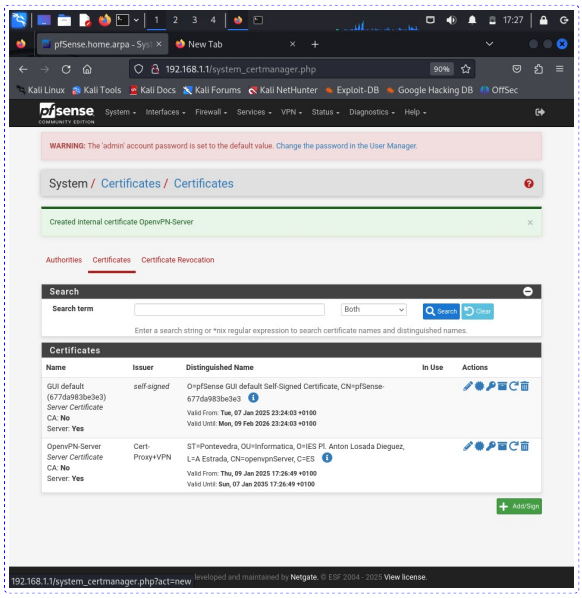


Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla

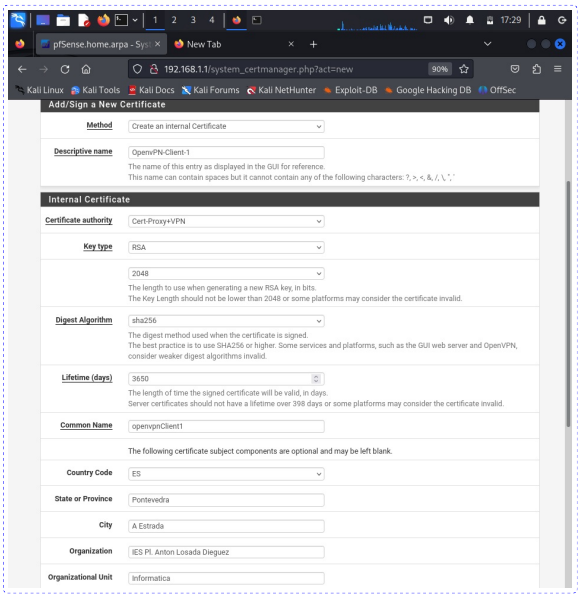


Certificado OpenvPN-Server xerado.

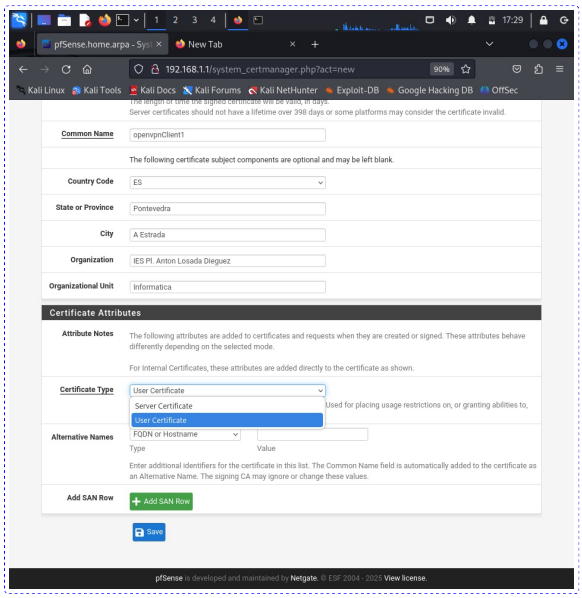
e premer en Save.



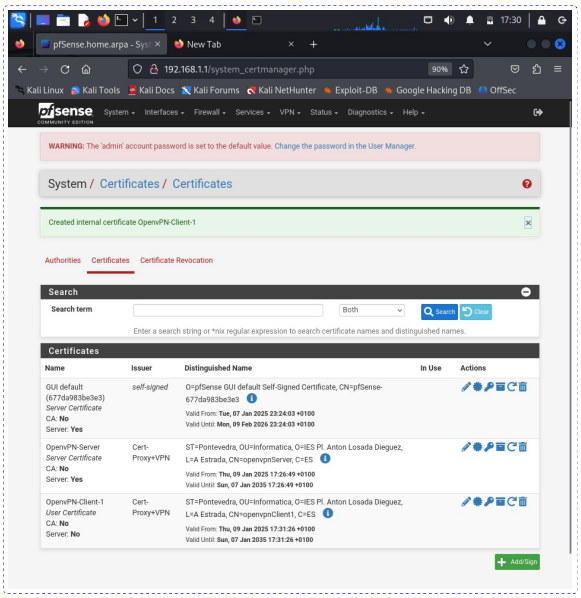
Na sección Certificates premer no botón "Add/Sign" para xerar un certificado para un cliente VPN.



Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla.

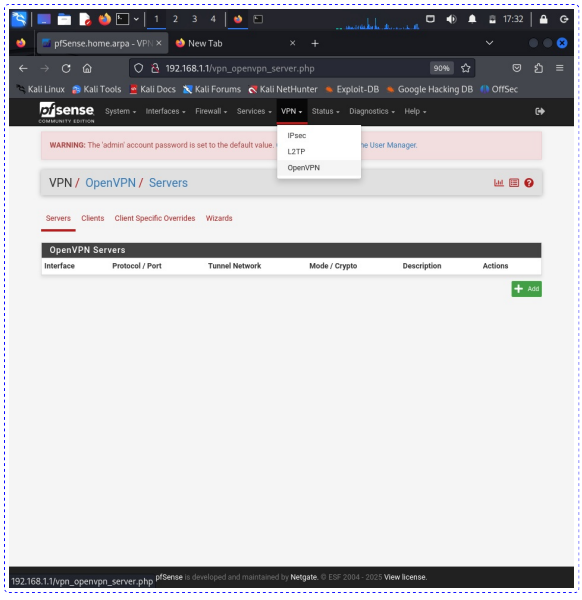


Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer en Save.

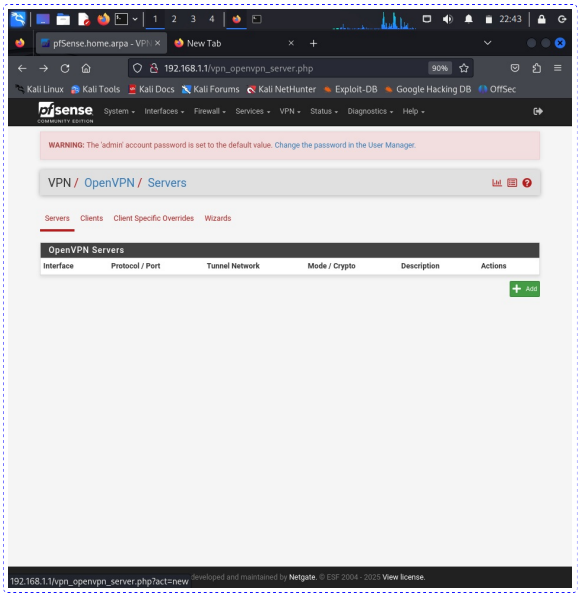


Certificado OpenvpnVPN-Client-1 xerado.

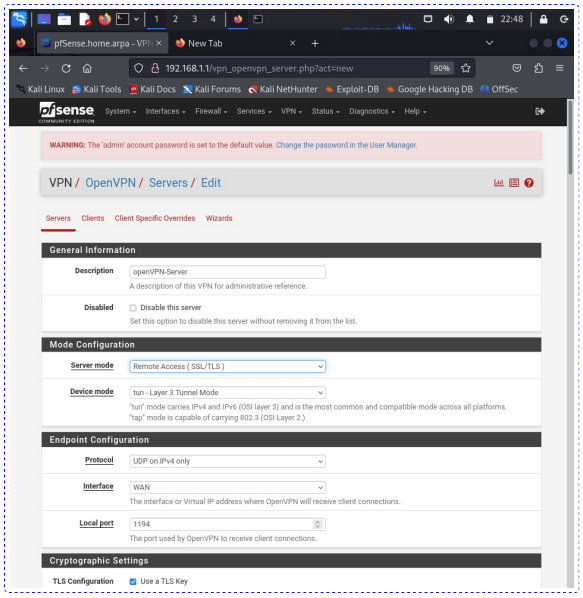
2. **Configuración OpenVPN**:



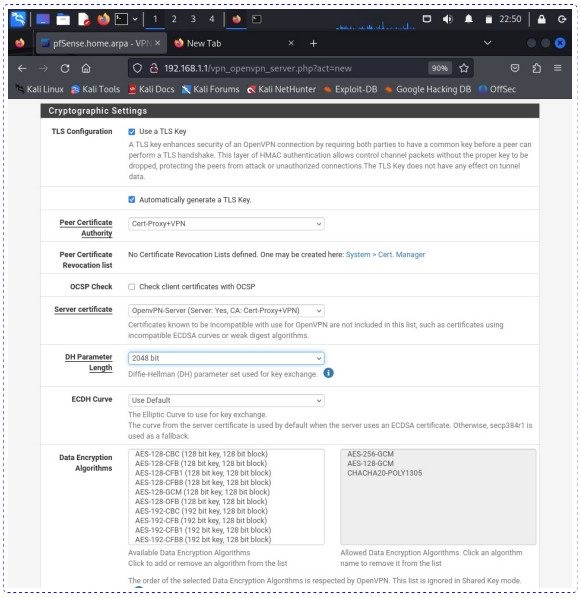
Ir a VPN → OpenVPN



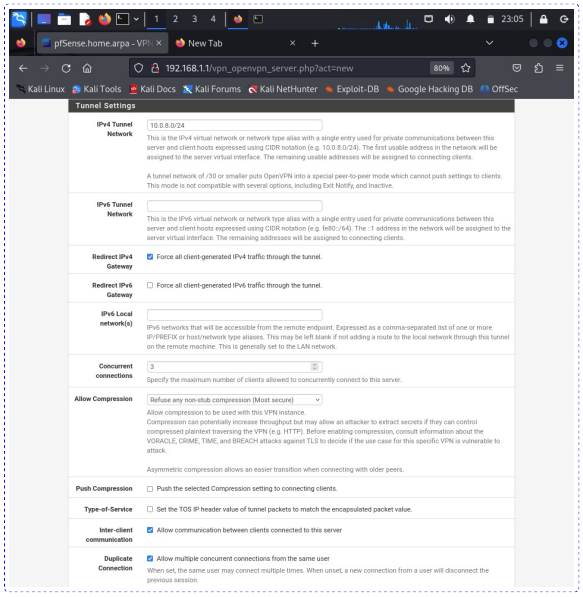
Na sección Servers premer o botón Add



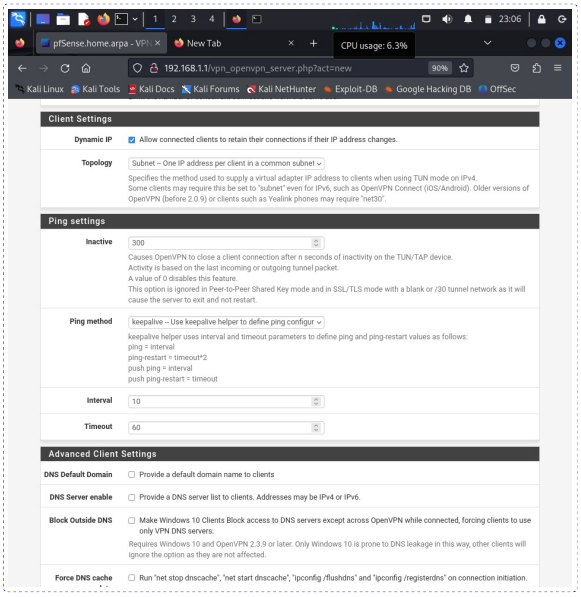
Escolleir as opcións e escribir o que aparece na imaxe. Baixar a pantalla.



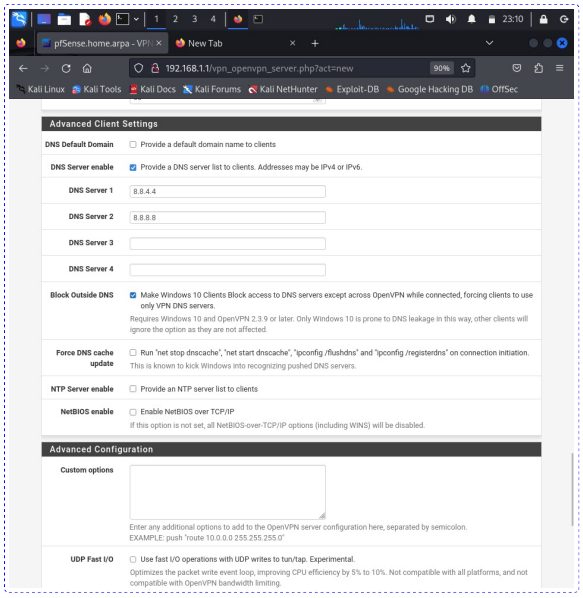
Escolleir as opcións e escribir o que aparece na imaxe. Baixar a pantalla.



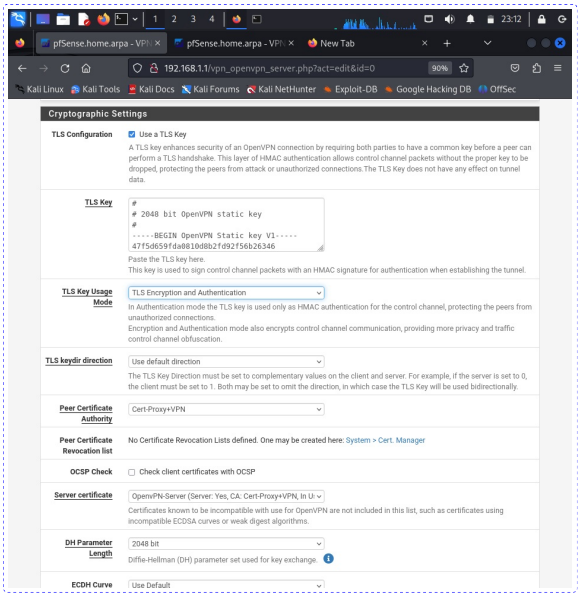
Escolleir as opcións e escribir o que aparece na imaxe. Baixar a pantalla.



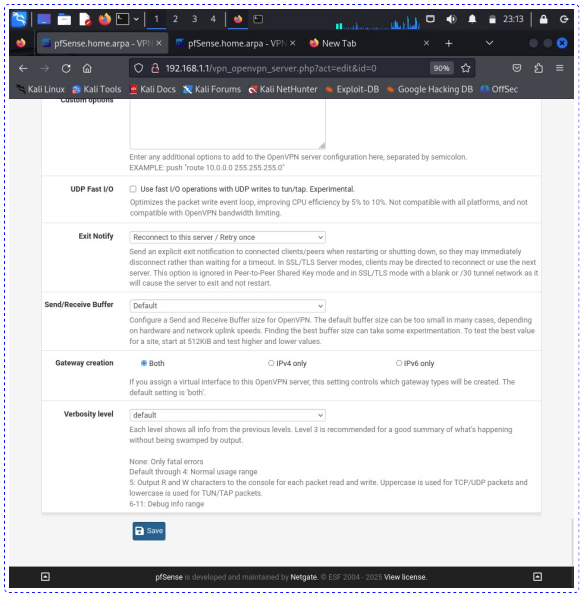
Escolleir as opcións e escribir o que aparece na imaxe. Baixar a pantalla.



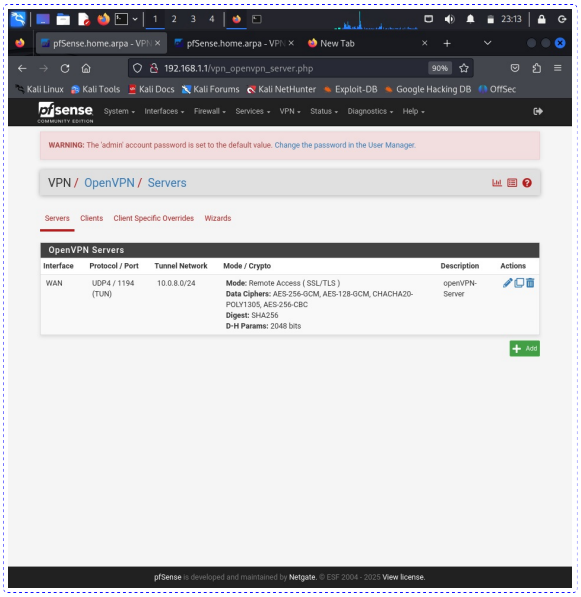
Escolleir as opcións e escribir o que aparece na imaxe. Baixar a pantalla.



Escolleir as opcións e escribir o que aparece na imaxe. Baixar a pantalla.

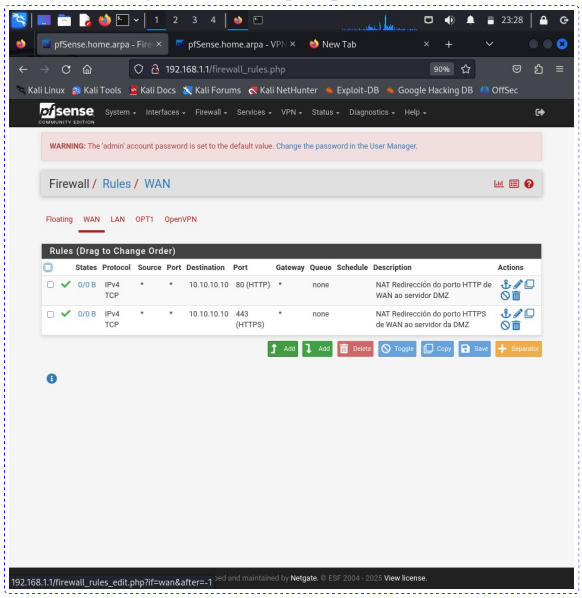


Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer o botón Save.

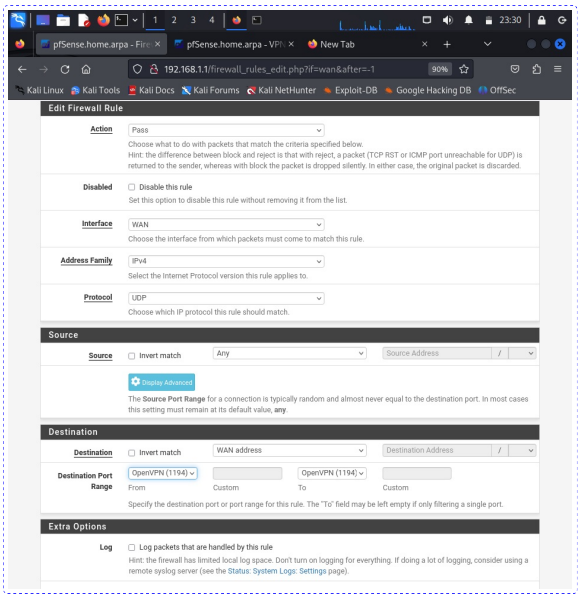


Servidor OpenVPN configurado.

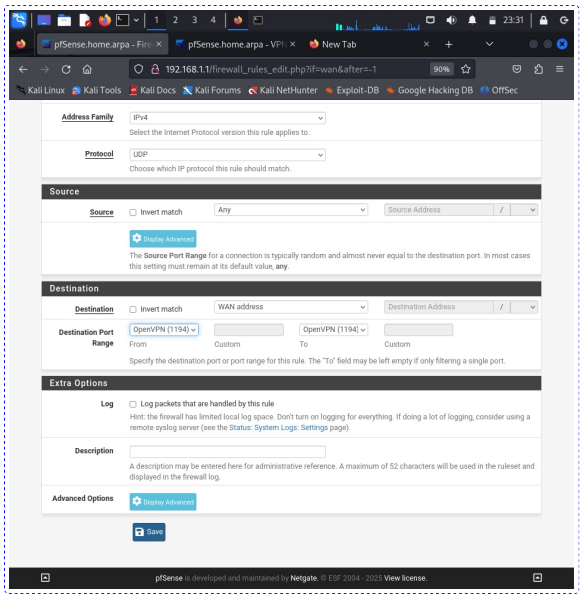
3. **Configurar as regras de firewall para permitir o acceso VPN**:



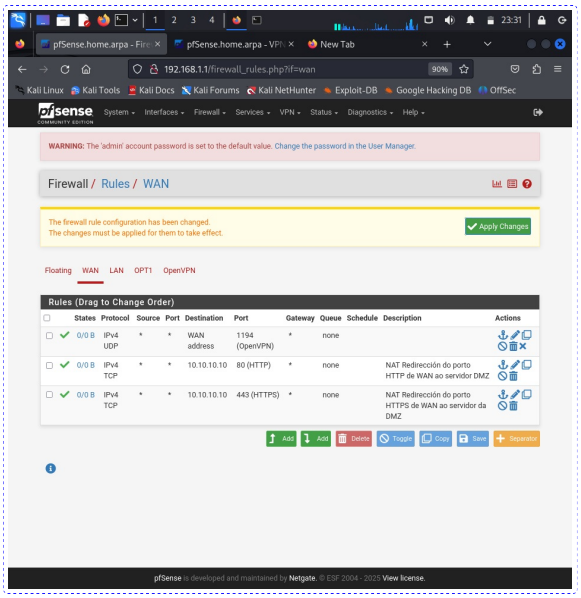
Ir a Firewall → Rules → WAN e premer no botón 



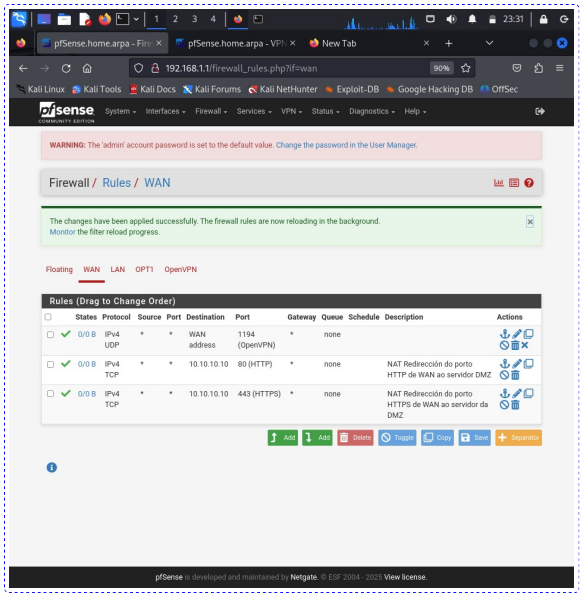
Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla.



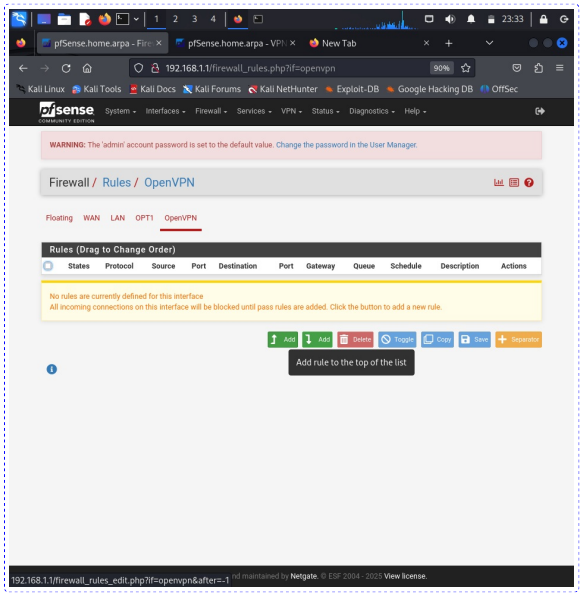
Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer no botón Save.



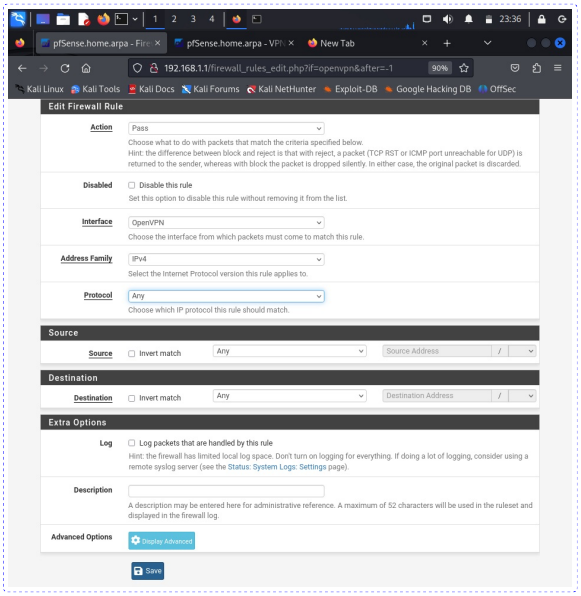
Para aplicar os cambios premer en "Apply Changes"



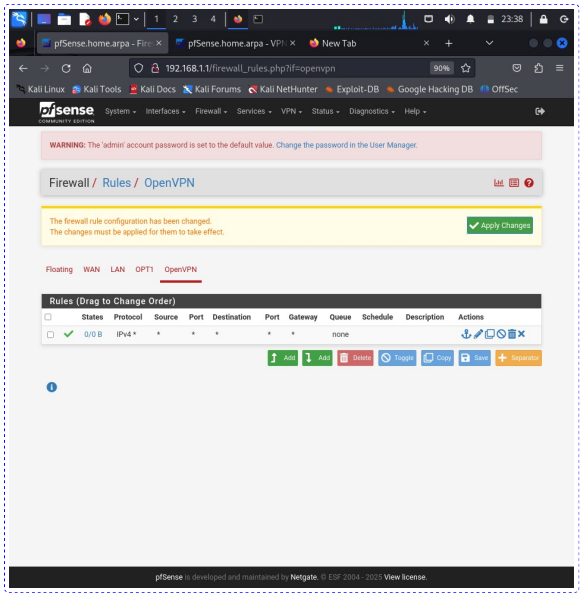
Cambios aplicados e regra xerada.



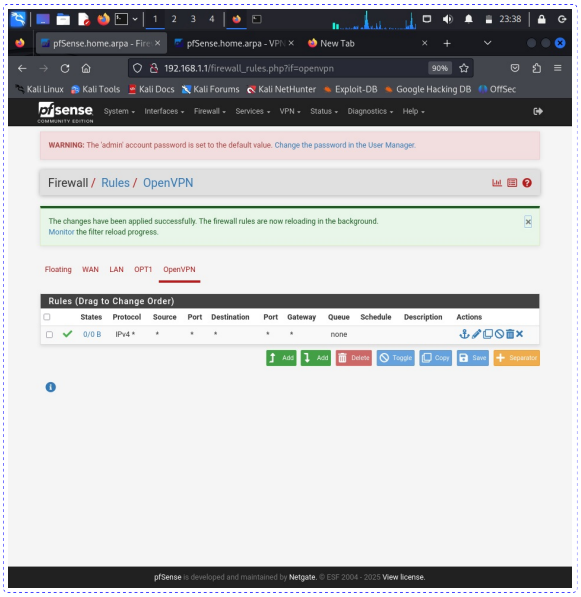
Ir a Firewall → Rules → OpenVPN e premer no botón 



Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer no botón Save.

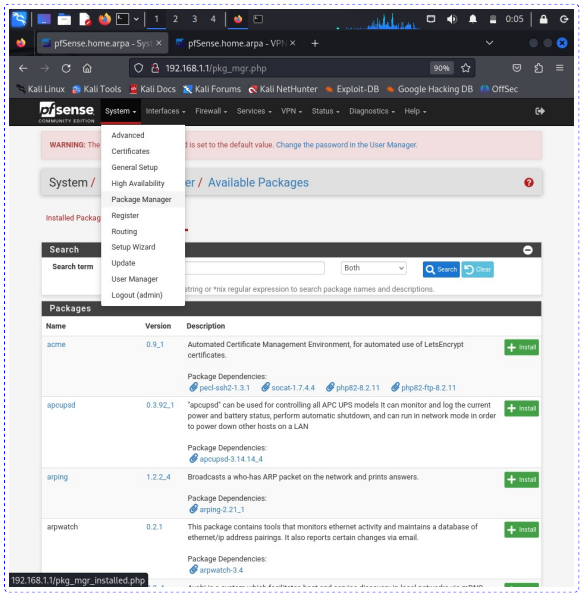


Para aplicar os cambios premer en "Apply Changes"

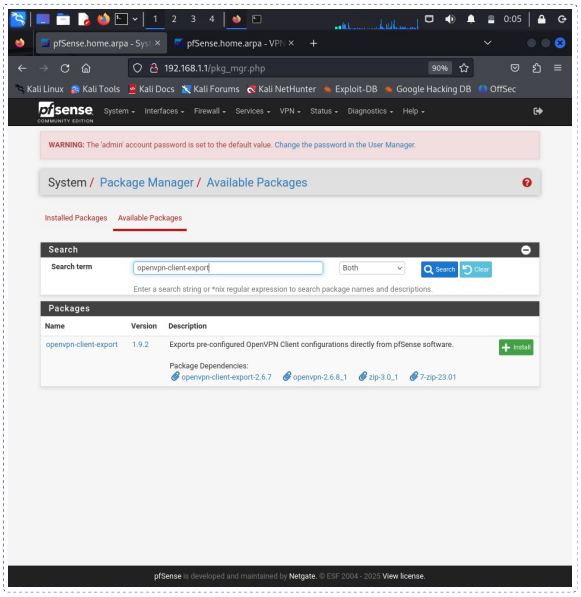


Cambios aplicados e regra xerada.

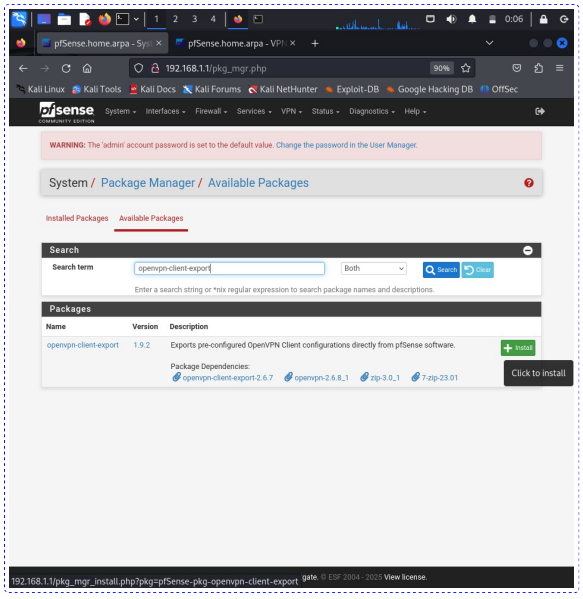
4. **Exportar o arquivo de configuración OpenVPN para os clientes**:



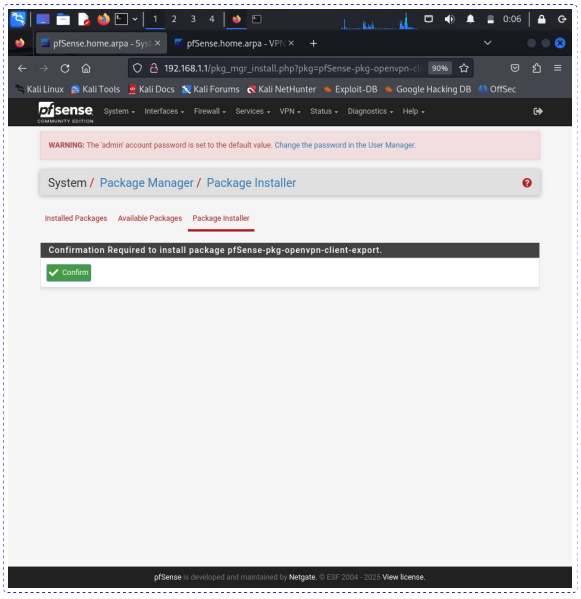
Abrir System → Package Manager



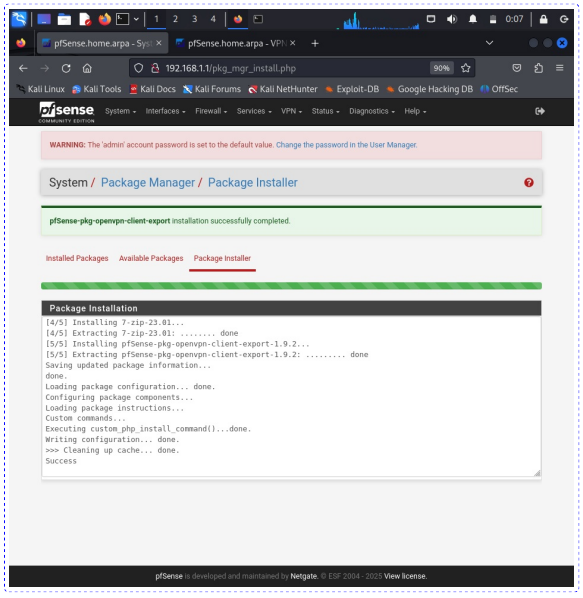
Buscar o patrón "openvpn-client-export" os paquetes posibles a instalar.



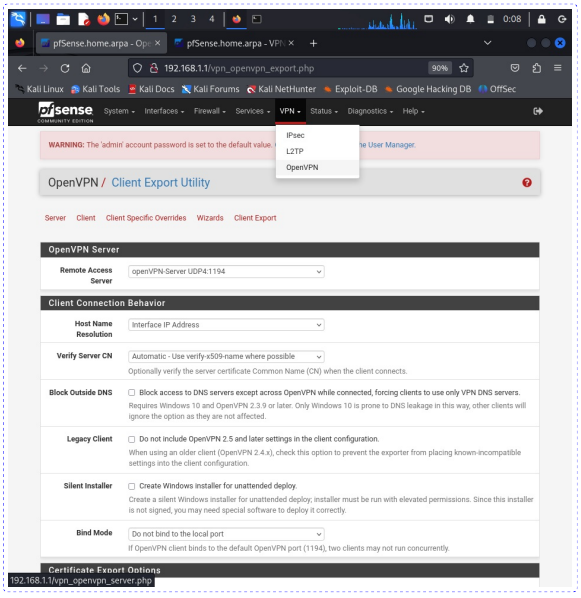
Premer no botón Install do paquete openvpn-client-export para proceder a instalalo.



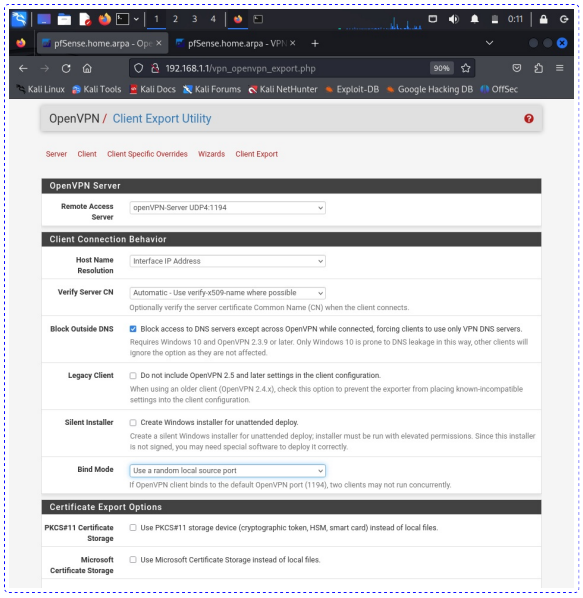
Premer no botón Confirm para confirmar a instalación requerida.



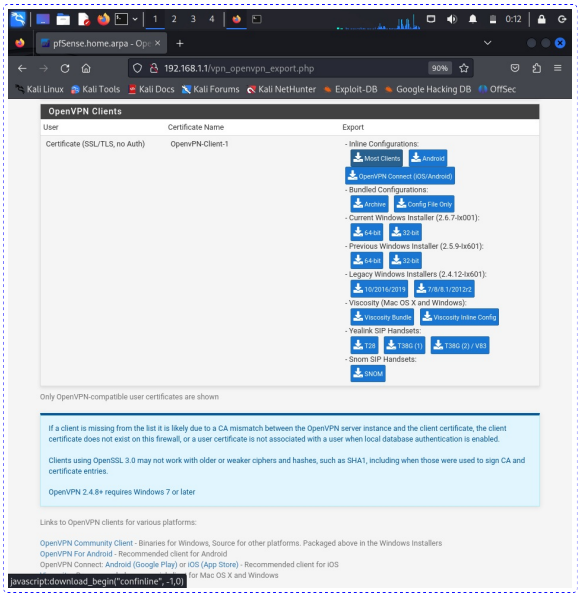
Instalación do paquete openvpn-client-export realizado.



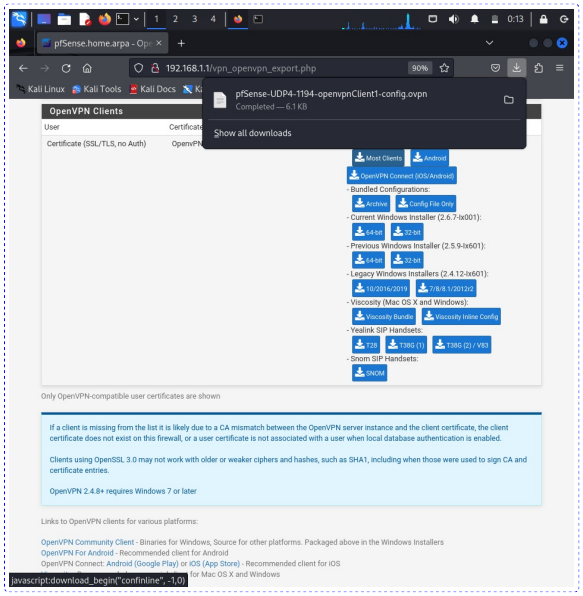
Abrir VPN → OpenVPN



Elixir a opción "Client Export". Baixar a pantalla.

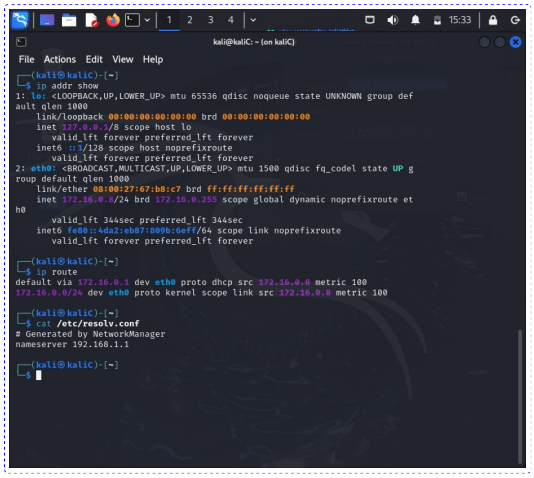


No certificado OpenvPN-Client-1 premer no botón "Most Clients"

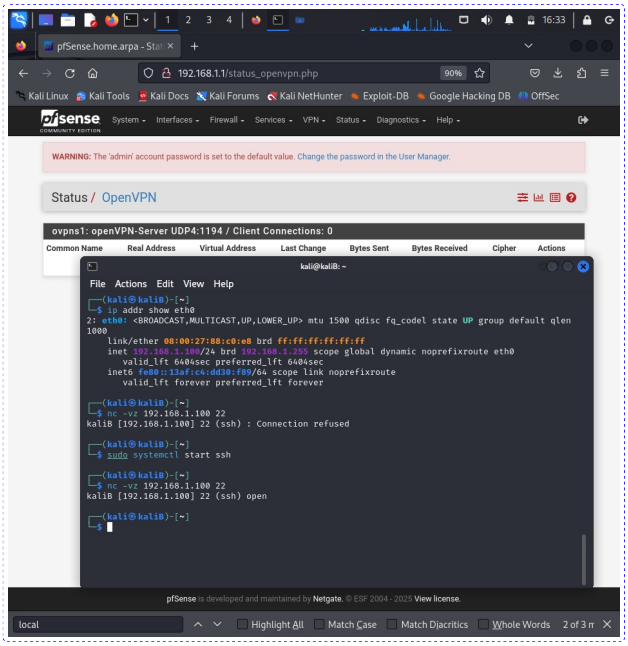


Certificado descargado (/home/kali/Downloads/pfSense-UDP4-1194-openvpnClient1-config.ovpn

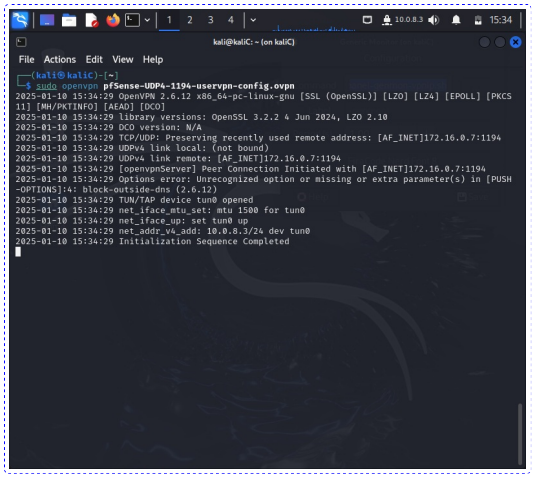
5. **Conectar o cliente mediante VPN**:



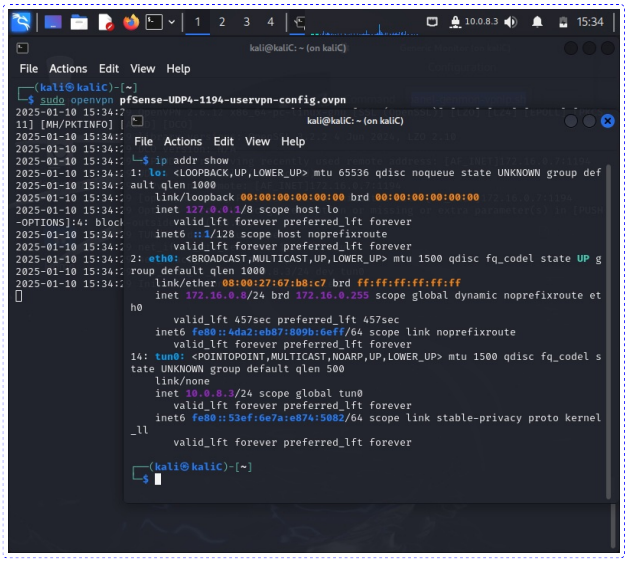
Revisar a configuración actual de rede en kaliC antes da conexión VPN con kaliB



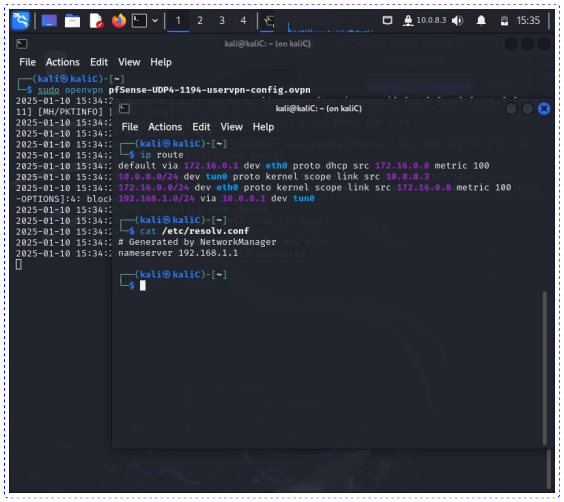
Revisar a configuración actual de rede en kaliB antes da conexión VPN e habilitar o servizo SSH en kaliB.



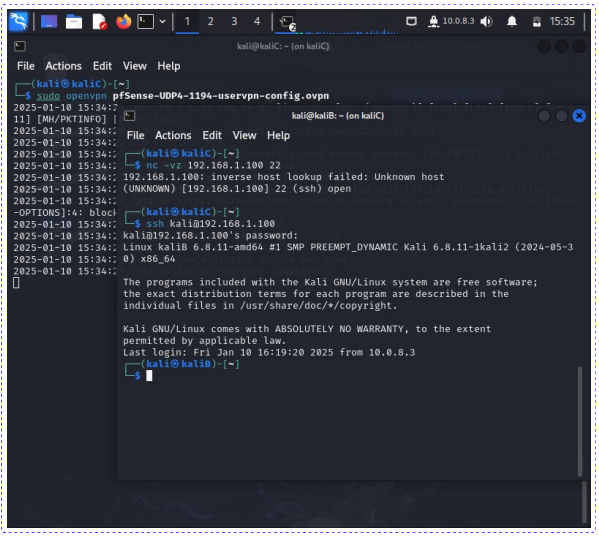
Establecer a conexión VPN con kaliB dende kaliC



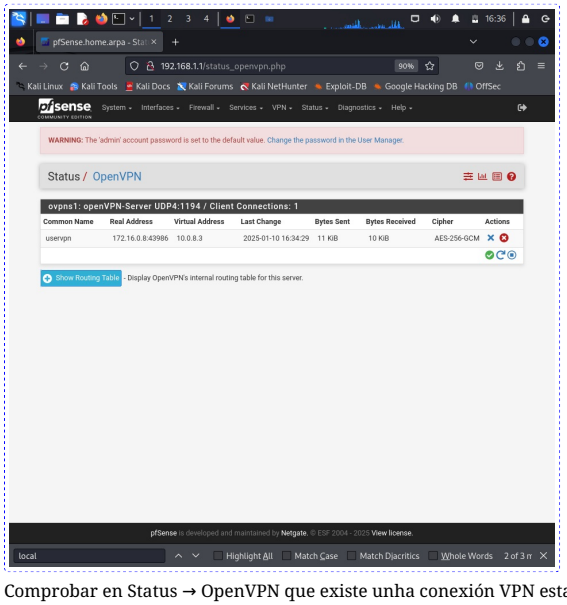
Revisar a configuración actual de rede en kaliC logo da conexión VPN con kaliB
Aparece unha nova NIC: tun0



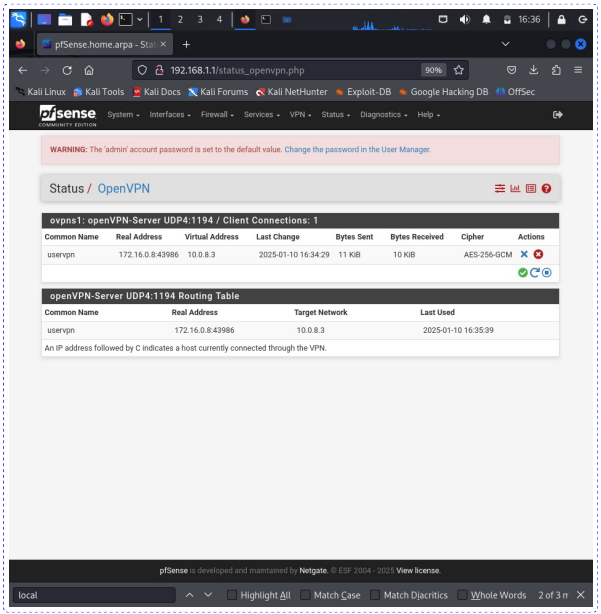
Revisar a configuración actual de rede en kaliC logo da conexión VPN con kaliB



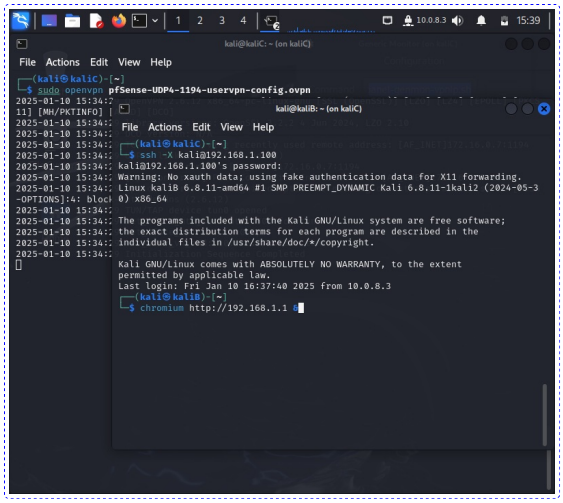
Acceder dende kaliC a kaliB mediante ssh.
Isto é posible debido á conexión VPN.
Notar que non é necesario xerar unha nova regra para chegar ao servizo SSH en kaliB.



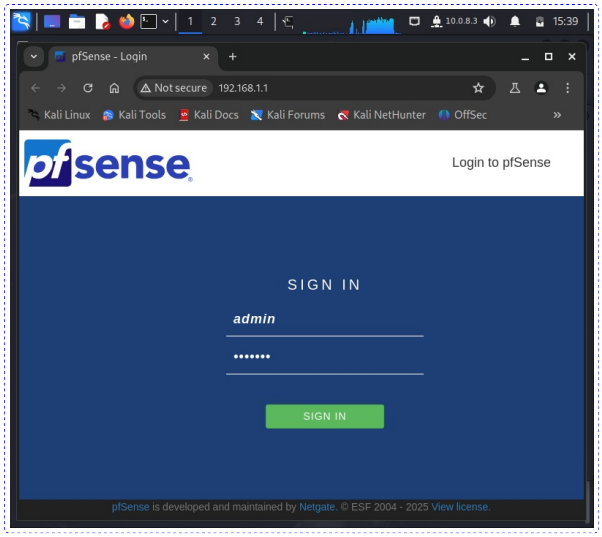
Comprobar en Status → OpenVPN que existe unha conexión VPN establecida.
Premer en "Show Routing Table"



Amosar tamén a táboa de rutas na conexión VPN establecida.



Acceder dende kaliC a kaliB mediante ssh exportando o display gráfico.
Abrir o navegador chromium
Isto é posible debido á conexión VPN.

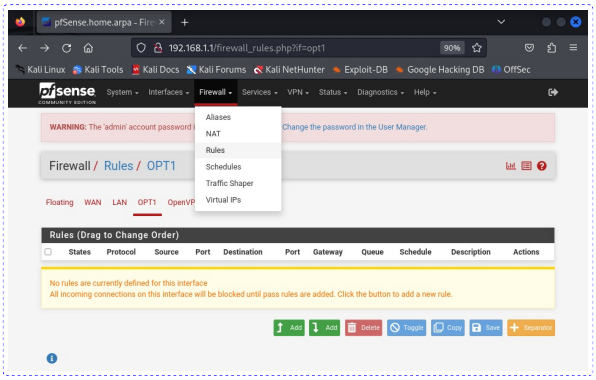


Recibir o navegador na páxina requerida en kaliC, debido a exportación do display por ssh e a conexión VPN establecida.

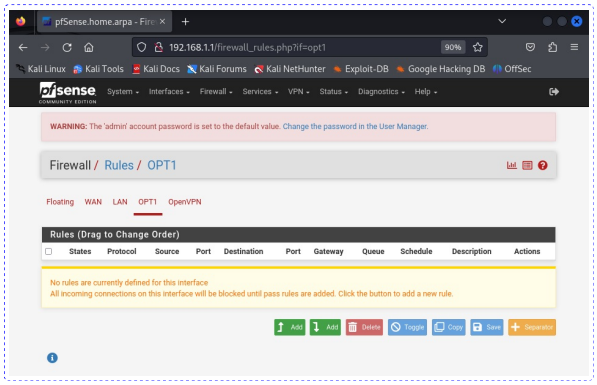
Firewall: Regras DMZ

22. **Exemplo5. Bloqueo tráfico de rede da DMZ á LAN**

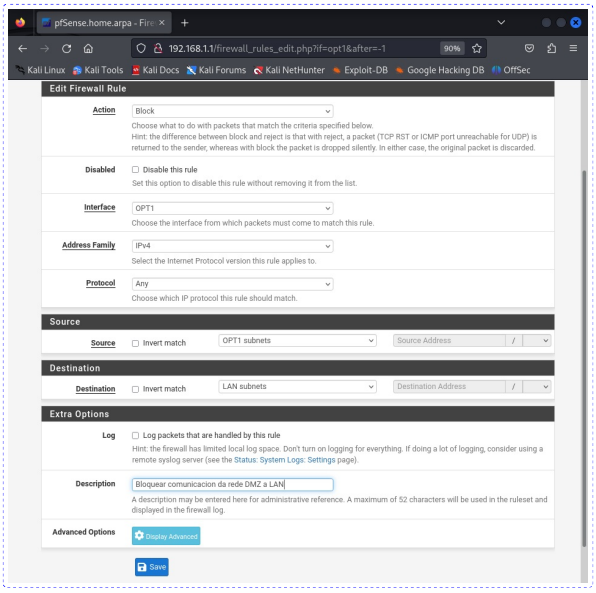
Aínda que tal como está configurado o Escenario a rede DMZ xa non posee conectividade hacia a LAN imos engadir a regra que impide ese acceso: o da DMZ(kaliA) á LAN(kaliB).



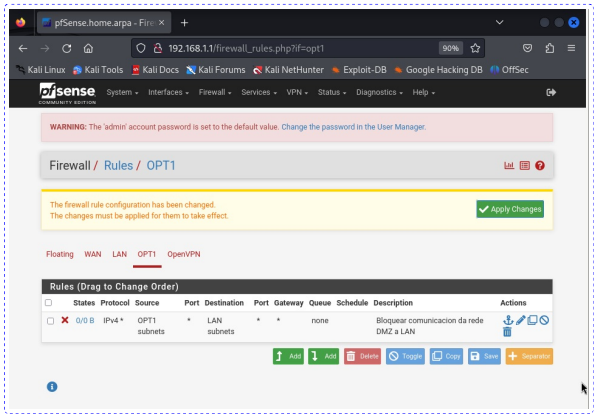
Escoller no menú a opción: Firewall → Rules → OPT1



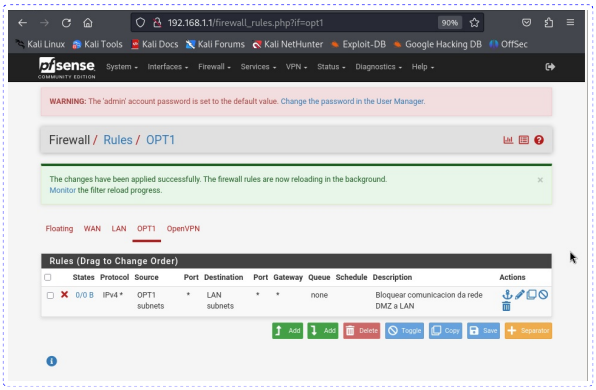
Premer en Add para xerar unha nova regra.



Escoller as opcións e escribir o que aparece na imaxe. Baixar a pantalla e premer en Save.



Para aplicar os cambios premer en "Apply Changes"



Cambios aplicados e regra xerada.

Ricardo Feijoo Costa