

pfSense + DMZ

ESCUENARIO:

Máquinas virtuales:

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: 172.16.0.0/24

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:

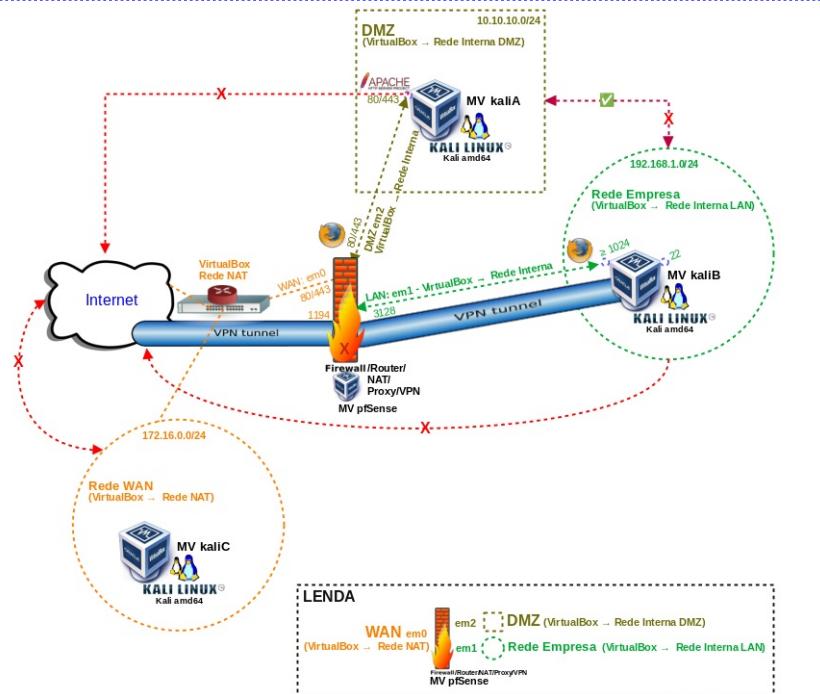
ISO: Live Kali amd64

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 fa 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, incluindo os posibles errores 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 das 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, utilizase habitualmente para aloxar servidores que ofrecen servizos á rede externa, xeralmente Internet. Estes servizos poden incluir 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 Virtuales):** Establece conexións seguras usando protocolos como OpenVPN e IPsec.
- **Balanceo de carga e failover:** Mellora o rendemento e disponibilidade da conexión a Internet.
- **Filtro de contenido:** Bloquea sitios web ou categorías específicas.
- **Interfaz web fácil de usar:** Configuración sinxela a través dun navegador.

■ Vantaxes de usar pfSense:

- **Gratuito e de código abierto:** Sen custos de licenzas.
- **Alta seguridad e estabilidade:** Ideal para redes críticas.
- **Personalización:** Adaptable ás necesidades específicas.
- **Actualizaciones 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 disponible. 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)** ⁸⁰ → **kaliA(DMZ)** imos redireccionar o porto TCP 80(HTTP) de pfSense ao porto TCP 80(HTTP) en kaliA se a petición de conectividade realizase dende a rede WAN(kaliC)
- No Exemplo2. Port Forwarding **kaliC(WAN)** ⁴⁴³ → **kaliA(DMZ)** imos redireccionar o porto TCP 443(HTTPS) de pfSense ao porto TCP 443(HTTPS) en kaliA se a petición de conectividade realizase dende a rede WAN(kaliC)

Proxy: Squid

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

VPN: OpenVPN

- No Exemplo4. OpenVPN en pfSense. Acceso remoto **kaliC(WAN)** 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

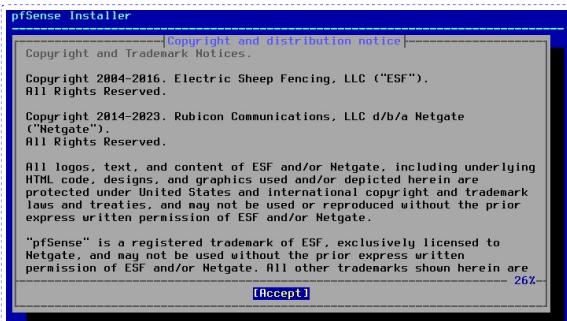
Firewall - Máquina virtual pfSense

1. Configurar según Escenario:



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

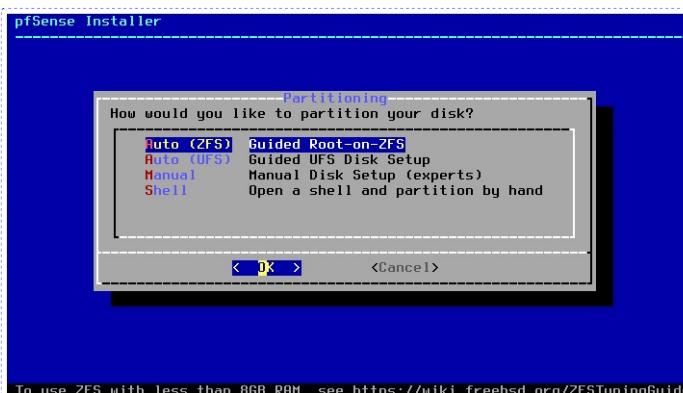
Móvese polas pantallas de instalación coas teclas frechas e tabulado. Unha vez elexido a opción desexada premer a tecla Enter.



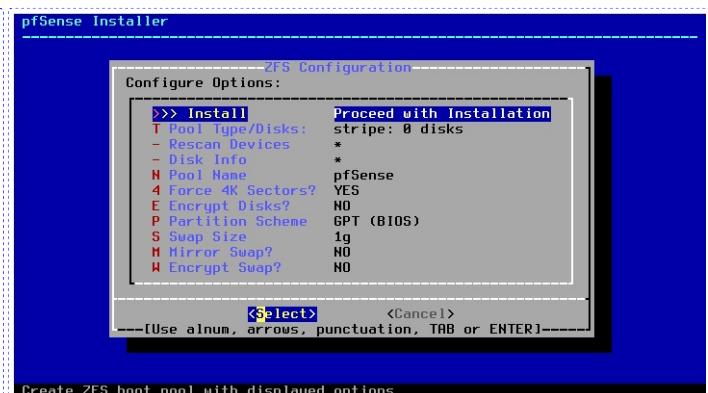
Premere a tecla Enter



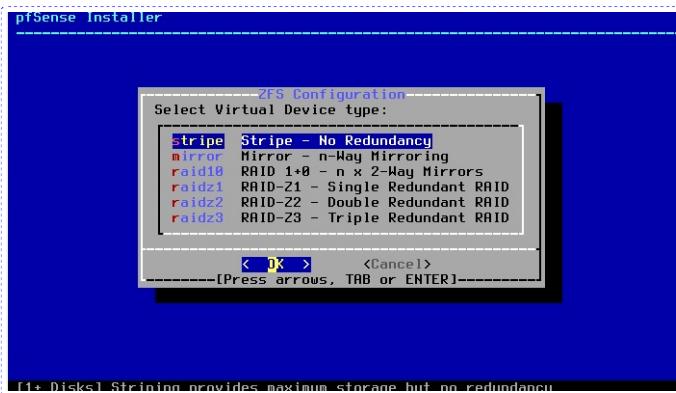
Escooller a opción Install e premer Enter



Escooller a opción Auto (ZFS) e premer Enter

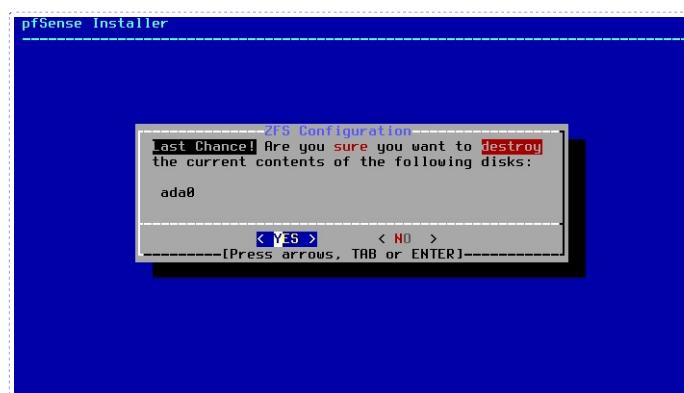


Premer a tecla Enter para proseguir coa instalación



[!] Disks! Stringing provides maximum storage but no redundancy.

Premer a tecla Enter para proseguir coa instalación



Premer a tecla Enter para proseguir coa instalación

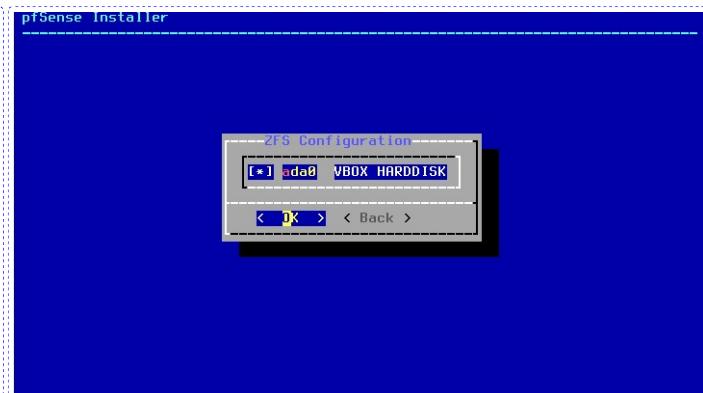


Apagar o equipo executando o comando: init 0



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

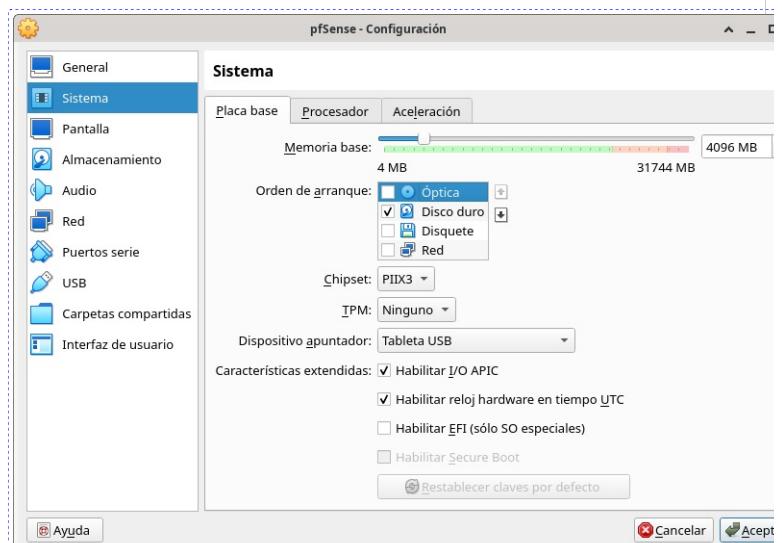
Enter an option: 1



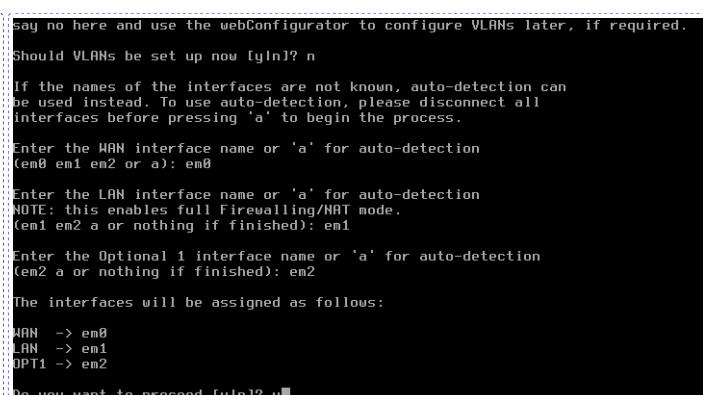
Seleccionar o disco duro onde instalar pfSense premendo na tecla "barra espaciadora" e premer Enter.



Elixir a opción Shell para proseguir coa instalación



Modificar as opciones de arranque: deixar soamente disco duro



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      ->
 8) 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      ->
 8) 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

 8) 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 más 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:



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

Primary Address Pool	
Subnet	10.10.10.0/24
Subnet Range	10.10.10.1 - 10.10.10.254
Address Pool Range	From: 10.10.10.10 To: 10.10.10.50
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	
+ Add Address Pool	
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

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

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

Nesta práctica a IP/MS concedida polo servidor DHCP DMZ de pfSense 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 dos 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  
    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:bfc1: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|kaliA' >> /etc/hosts #Engadir o hostname kaliA en /etc/hosts
root@kali:~# exit #Sair da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kali:~$ exit #Pesar 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|kaliA' >> /etc/hosts #Engadir o hostname kaliA en /etc/hosts
root@kali:~# exit #Sair da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kali:~$ exit #Pesar 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 más 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 #Reinic平ar 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 más 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 poderíamos 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 #Reinic平ar 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.arpal/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.arpal/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.arpal/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=1.106 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 = 1.106/1.242/1.298/0.056 ms
[2.7.2-RELEASE][root@pfSense.home.arpal/root: nc -46DdEfhk1NnrStUuvz1 [-e policy1] [-l length] [-i interval] [-t timeout]
usage: nc [-46DdEfhk1NnrStUuvz1] [-e policy1] [-l length] [-i interval] [-t timeout]
        [-no-tcpopt] [-scpt]
        [-P proxy_username] [-p source_port] [-s source] [-T ToS]
        [-tun tundev] [-V rtable] [-u timeout] [-X proxy_protocol]
        [-x proxy_address[:port]] [destination] [port]
[2.7.2-RELEASE][root@pfSense.home.arpal/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.arpal/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.arpal/root:
```

LAN - Máquina virtual B: Kali amd64

9. Configurar según Escenario:

The screenshot shows the 'General' tab where the VM name is 'kaliB'. Under 'System', memory is set to 2048 MB and processor count to 2. In the 'Storage' tab, a SATA controller is selected and a 4.35 GB ISO image is assigned to the first drive. The 'Audio' tab shows an Intel HD audio adapter. The 'USB' tab has 'xHCI' selected. There are no shared folders or descriptions defined.

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

The left screenshot shows the pfSense web interface at 192.168.1.1/services_dhcp.php. It displays a warning about the admin account password being set to the default. The right screenshot shows the 'Primary Address Pool' configuration for the LAN interface, setting the subnet to 192.168.1.0/24 and the address pool from 192.168.1.10 to 192.168.1.245.

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

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

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:d30: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 #Sair da consola local sudo na que estábamos 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 set-hostname kaliB || hostnamectl #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 #Sair da consola local sudo na que estábamos a traballar para voltar á consola local de kali.
kali@kali:~$ exit #Pecchar 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㉿kali)-[~]
└─$ 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㉿kali)-[~]
└─$ ping -c2 www.google.es
PING www.google.es (142.250.200.131) 56(84) bytes of data.
64 bytes from mad4lis14-in-f3.1e100.net (142.250.200.131): icmp_seq=1 ttl=103 time=32.3 ms
64 bytes from mad4lis14-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㉿kali)-[~]
└─$ 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㉿kali)-[~]
└─$ 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㉿kali)-[~]
└─$ 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.

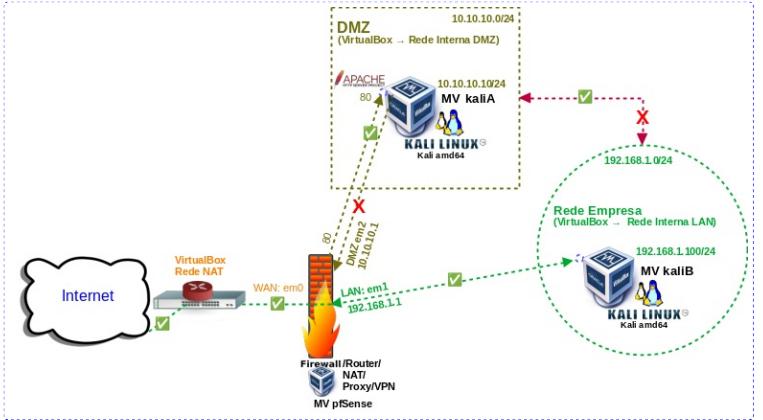
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1014ms

(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
```

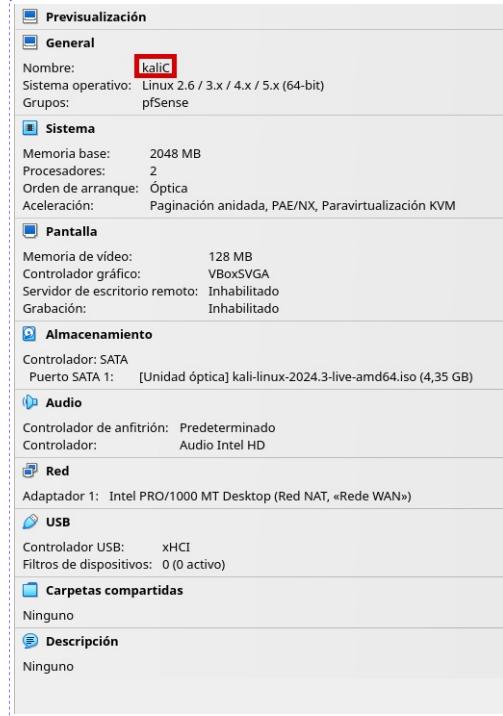
Resumo Escenario Actual

	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㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default 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:eb0:df5:ad97/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$ 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㉿kali)-[~]
└─$ 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|kaliC' >> /etc/hosts #Engadir o hostname kaliC en /etc/hosts
root@kali:~# exit #Sair da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kali:~$ exit #Pesar 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|kaliC' >> /etc/hosts #Engadir o hostname kaliC en /etc/hosts
root@kali:~# exit #Sair da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kali:~$ exit #Pesar 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.arp1]# 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 = 1.279/1.685/1.931/0.326 ms
[2.7.2-RELEASE][root@pfSense.home.arp1]# 

└─(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

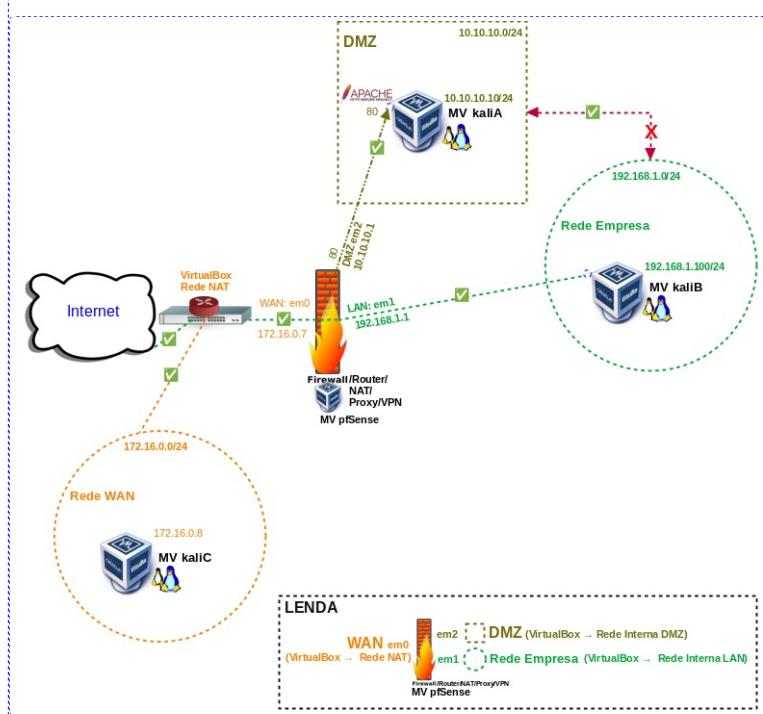
O que desexamos

	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 conseguir o deseñado temos que configurar novas regras de firewall en pfSense.

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.

The screenshot shows the pfSense Login page. It has a blue header with the pfSense logo. Below it is a dark blue background area with the text "SIGN IN". There are two input fields: one for "admin" and another for "pfSense". A green "SIGN IN" button is at the bottom. At the very bottom, there is a small footer note: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license".

Acceder coas credenciais: admin/pfSense

The screenshot shows the pfSense Setup Wizard Step 1 of 9. The title bar says "Wizard / pfSense Setup /". The main content area is titled "pfSense Setup" and "Welcome to pfSense® software!". It includes a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.". A "Learn more" button and a "» Next" button are at the bottom.

Premer en Next

The screenshot shows the pfSense Setup Wizard Step 2 of 9. The title bar says "Step 2 of 9". The main content area is titled "General Information". It asks for the host name ("Hostname") and domain ("Domain"). It also includes sections for DNS servers and an "Override DNS" checkbox. A "» Next" button is at the bottom.

Premer en Next

The screenshot shows the pfSense Setup Wizard Step 3 of 9. The title bar says "Step 3 of 9". The main content area is titled "Time Server Information". It asks for the time server's hostname ("Time server hostname") and timezone ("Timezone"). A "» Next" button is at the bottom.

Premer en Next

The screenshot shows the pfSense Setup Wizard Step 4 of 9. The title bar says "Step 4 of 9". The main content area is titled "Configure WAN Interface". It includes sections for "General configuration" (MAC address, MTU, MSS), "Static IP Configuration" (IP Address, Subnet Mask, Upstream Gateway), and "DHCP client configuration". A "» Next" button is at the bottom.

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

Premer en Reload

Proceso finalizado. Premer en Finish.

Recargando...

Copyright and Trademark Notices.

Copyright® 2004-2016, Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.
Copyright® 2014-2023, Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

pfSense® software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate software is allowed without the prior written consent of ESF and/or Netgate.

Regulatory Rights Legend.

No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply

Baixar para ler a licenza.

Restricted Rights Legend.

No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferating weapons of mass destruction; a U.S. party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Accept!

Aceptar licenza. Premer en Accept.

Thank you!

Netgate, as well as many community members, work hard to make pfSense CE software an excellent secure networking solution. As well, Netgate strives to deliver even greater value through our pfSense Plus software. Would you take a moment to answer this brief (and anonymous) survey to help us guide those efforts?

User survey

Close

Licenza aceptada. Premer en Close.

System Information

Name	pfSense.home.apa
User	admin@192.168.1.100 (Local Database)
System	KVM Guest Netgate Device ID: 103e5c089254d2bbdcfe
BIOS	Vendor: Innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT
CPU Type	13th Gen Intel(R) Core(TM) i7-1355U 2 CPUs; 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 36 Minutes 49 Seconds

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

Amósase información do sistema pfSense.

NETGATE AND pfSENSE COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more competitive than compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.

Interfaces

WAN	1000baseT <full-duplex>	172.16.0.7
LAN	1000baseT <full-duplex>	192.168.1.1
OPT1	1000baseT <full-duplex>	10.10.10.1

pfSense is developed and maintained by Netgate. © 2004 - 2025 View license.

Baixando a pantalla vemos un resumo das Interfaces.

System Information

Name	pfSense.home.apa
User	admin@192.168.1.100 (Local Database)
System	KVM Guest Netgate Device ID: 103e5c089254d2bbdcfe

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

Menú de pfSense. Dependendo das dimensíons 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) → kaliA(DMZ)

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Port Forward' tab. In the 'Rules' section, there is a table with columns: Interface, Protocol, Source Address, Source Ports, Dest. Address, Dest. Ports, NAT IP, NAT Ports, Description, and Actions. A single row is selected, showing 'WAN' as the interface, 'TCP' as the protocol, and '80' as the source port. The destination is '10.10.10.10' on port '80'. The NAT IP is '10.10.10.10' and the NAT port is '80'. The description is 'Redirección do porto HTTP de WAN ao servidor DMZ'.

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Port Forward' tab. The 'Rules' table now contains two rows. The first row is identical to the one in the previous screenshot. A second row has been added, showing 'WAN' as the interface, 'TCP' as the protocol, and '80' as the source port. The destination is '10.10.10.10' on port '80'. The NAT IP is '10.10.10.10' and the NAT port is '80'. The description is 'Redirección do porto HTTP de WAN ao servidor DMZ'. A message at the bottom states: 'The NAT configuration has been changed. The changes must be applied for them to take effect.'

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

The screenshot shows the 'Edit Redirect Entry' configuration page. It includes fields for 'Interface' (WAN), 'Address Family' (IPv4), 'Protocol' (TCP), 'Source' (WAN address), 'Destination' (HTTP port 80), 'Destination port range' (HTTP port 80), 'Redirect target IP' (10.10.10.10), 'Redirect target port' (HTTP port 80), and a 'Description' field ('Redirección do porto HTTP de WAN ao servidor DMZ').

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Port Forward' tab. The 'Rules' table now contains two rows. The first row is identical to the one in the previous screenshots. A second row has been added, showing 'WAN' as the interface, 'TCP' as the protocol, and '80' as the source port. The destination is '10.10.10.10' on port '80'. The NAT IP is '10.10.10.10' and the NAT port is '80'. The description is 'Redirección do porto HTTP de WAN ao servidor DMZ'. A message at the bottom states: 'The changes have been applied successfully. The firewall rules are now reloading in the background.'

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

The screenshot shows the 'Edit Redirect Entry' configuration page for port 443. It includes fields for 'Interface' (WAN), 'Address Family' (IPv4), 'Protocol' (TCP), 'Source' (WAN address), 'Destination' (HTTP port 443), 'Destination port range' (HTTP port 443), 'Redirect target IP' (10.10.10.10), 'Redirect target port' (HTTP port 443), and a 'Description' field ('Redirección do porto HTTPS de WAN ao servidor DMZ').

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Port Forward' tab. The 'Rules' table now contains three rows. The first two rows are identical to the ones in the previous screenshots. A third row has been added, showing 'WAN' as the interface, 'TCP' as the protocol, and '443' as the source port. The destination is '10.10.10.10' on port '443'. The NAT IP is '10.10.10.10' and the NAT port is '443'. The description is 'Redirección do porto HTTPS de WAN ao servidor DMZ'. A message at the bottom states: 'The changes have been applied successfully. The firewall rules are now reloading in the background.'

Cambios aplicados e regra xerada.

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

```
(kali㉿kali)-[~]
$ nc -vz 10.10.10.80
10.10.10.10 [10.10.10.10] 80 (http) : Connection timed out
(kali㉿kali)-[~]
$ 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㉿kali)-[~]
$ 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)

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

Premir en Add

Escolher 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㉿kali)-[~]
$ 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㉿kali)-[~]
$ 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
```

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 172.16.0.7. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more... Go Back (Recommended) Advanced...

172.16.0.7 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate Go Back (Recommended) Accept the Risk and Continue

Apache2 Debian Default Page

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP Server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|--- ports.conf
|-- mods-enabled
|--- *.load
|--- *.conf
```

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

```
(kali㉿kali)-[~]
$ 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
```

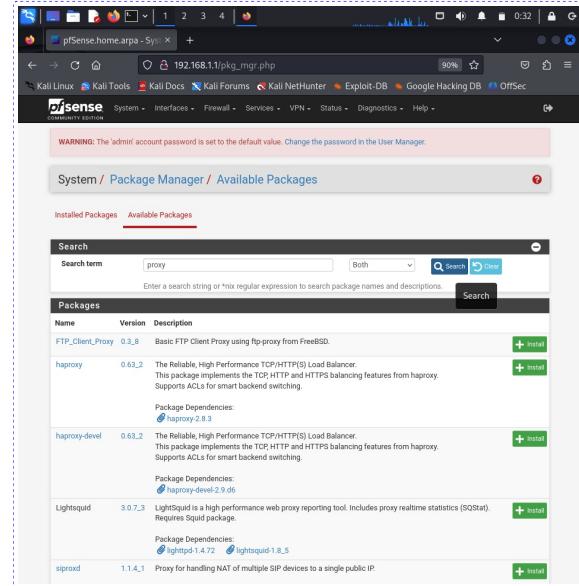
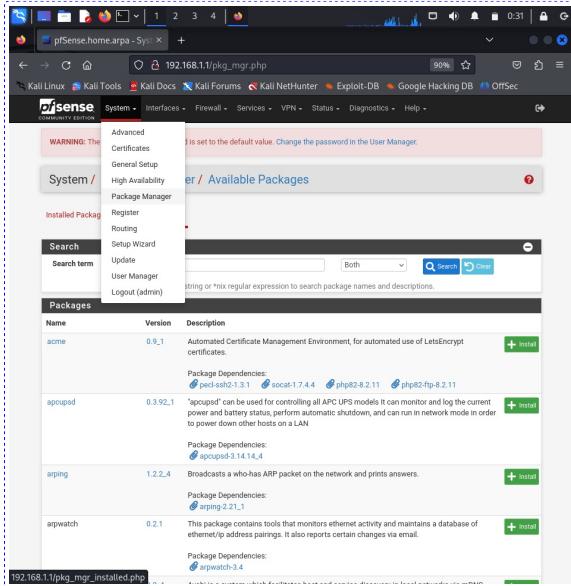
Proxy: Squid

20. Exemplo3. Proxy en pfSense

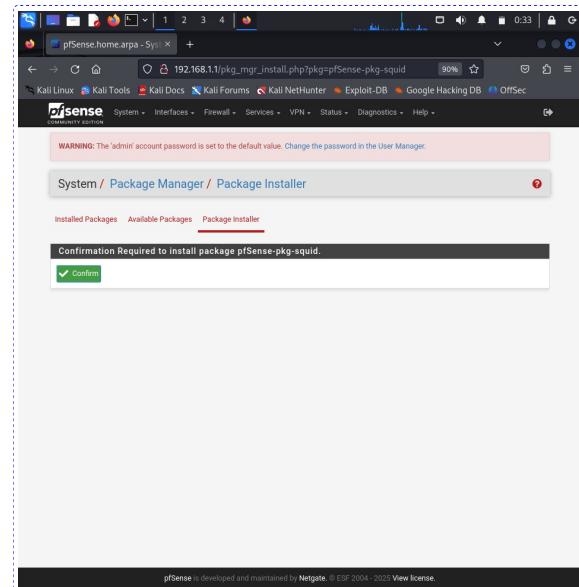
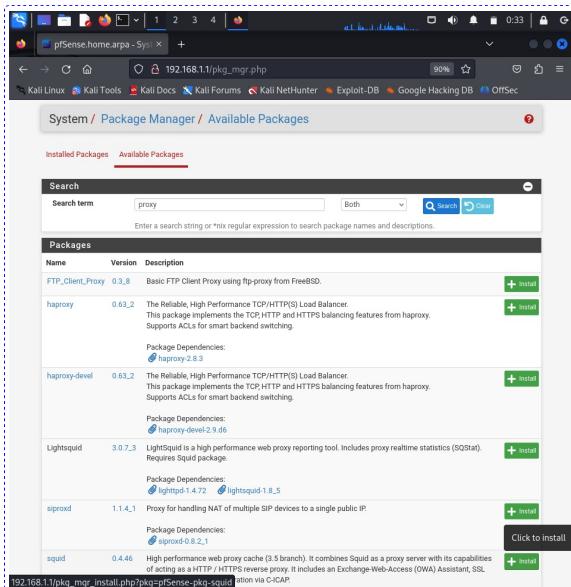
Imos activar o proxy en pfSense para que as petições web dende LAN(kaliB) saíam a través deste proxy.

Procedemento:

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

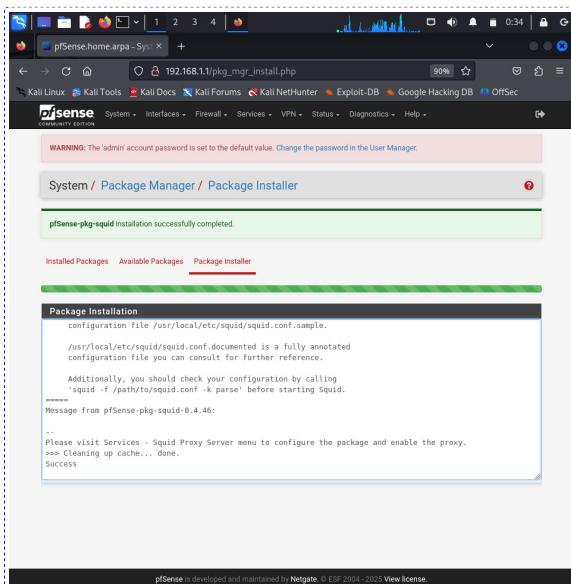


Abrir System → Package Manager



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):

The screenshot shows the pfSense Firewall Rules WAN tab. There are two entries in the 'Rules (Drag to Change Order)' table:

- Row 1: State: 0/0/B, Protocol: IPv4, Source: *, Port: 10.10.10. 80 (HTTP), Destination: *, Port: none. Description: NAT Redirección do porto HTTP de WAN ao servidor DMZ.
- Row 2: State: 0/0/B, Protocol: IPv4, Source: *, Port: 10.10.10. 443 (HTTPS), Destination: *, Port: none. Description: NAT Redirección do porto HTTPS de WAN ao servidor da DMZ.

Buttons at the bottom include Add, Add, Delete, Toggle, Copy, Save, and Separate.

Abrir Firewall → Rules

The screenshot shows the pfSense Firewall Rules LAN tab. There are three entries in the 'Rules (Drag to Change Order)' table:

- Row 1: State: 3/3/MIB, Protocol: LAN Address, Source: *, Port: 80, Destination: *, Port: none. Description: Anti-Lockout Rule.
- Row 2: State: 0/16/09 MIB, Protocol: IPv4, Source: LAN subnets, Port: *, Destination: *, Port: none. Description: Default allow LAN to any rule.
- Row 3: State: 0/0/B, Protocol: IPv6, Source: LAN subnets, Port: *, Destination: *, Port: none. Description: Default allow LAN IPv6 to any rule.

Buttons at the bottom include Add, Add, Delete, Toggle, Copy, Save, and Separate. A tooltip says "Add rule to the top of the list".

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

The screenshot shows the 'Edit Rule' dialog for a new rule. The 'Action' dropdown is set to 'Block'. Other fields include:

- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Invert match, Any, Source Address: /
- Destination:** Invert match, Any, Destination Address: /
- Extra Options:** Log, Description: Impedir acceso http sen proxy

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

The screenshot shows the pfSense Firewall Rules LAN tab after adding a new rule. The table now includes the new rule from the previous screenshot, and a green 'Apply Changes' button is visible.

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

The screenshot shows the 'Edit Rule' dialog for a new rule. The 'Action' dropdown is set to 'Block'. Other fields include:

- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Invert match, Any, Source Address: /
- Destination:** Invert match, Any, Destination Address: /
- Extra Options:** Log, Description: Impedir acceso https sen proxy

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

The screenshot shows the pfSense Firewall Rules LAN tab after applying changes. The table now includes the new rule from the previous screenshot, and a green 'Apply Changes' button is visible.

Para aplicar os cambios premer en "Apply Changes"

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/3 21 MIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Impedir acceso https sen proxy	
✗ 0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Impedir acceso http sen proxy	
✓ 2/16 13 MIB	IPv6*	LAN subnets	*	*	*	*	*		Default allow LAN to any rule	
✓ 0/0 B	IPv6*	LAN subnets	*	*	*	*	*		Default allow LAN IPv6 to any rule	

Add **Save** **Separator**

pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

Cambios aplicados e regras xeradas.

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

System / Certificates / Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions

192.168.1.1/system_cmanager.php pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

Abrir System → Certificates

System / Certificate / Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions

192.168.1.1/system_cmanager.php act=new pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

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

Create / Edit CA

Descriptive name: Cert-Proxy
This name will be displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, <, >, &, ;, \, /, ^.

Method: Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: Use random serial numbers when signing certificates
When enabled, if this CA is capable of issuing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type: RSA
2048
The length to use when generating a new RSA key on save.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm: sha256
The digest method used when the CA is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days): 3650
The time to live when generating a new RSA key on save.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Common Name: internal-ca
The following certificate authority subject components are optional and may be left blank.

Country Code: ES
State or Province: Pontevedra
City: A Estrada
Organization: IES Pl. Anton Losada Dieguez
Organizational Unit: Informática

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

System / Certificate / Authorities

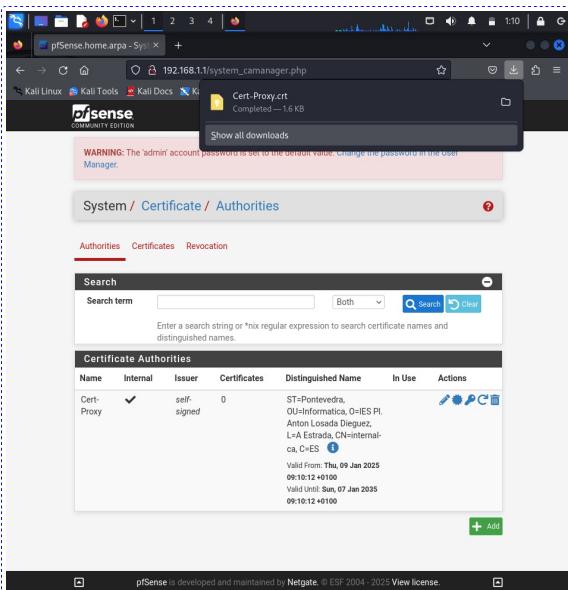
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Cert-Proxy	✓	self-signed	0	ST=Pontevedra, OU=Informática, O=IES Pl. Anton Losada Dieguez, L=A Estrada, CN=internal- ca, C=ES		

Valid From: Thu, 09 Jan 2025
09:16:12 +0100
Valid Until: Thu, 07 Jan 2035
09:10:12 +0100

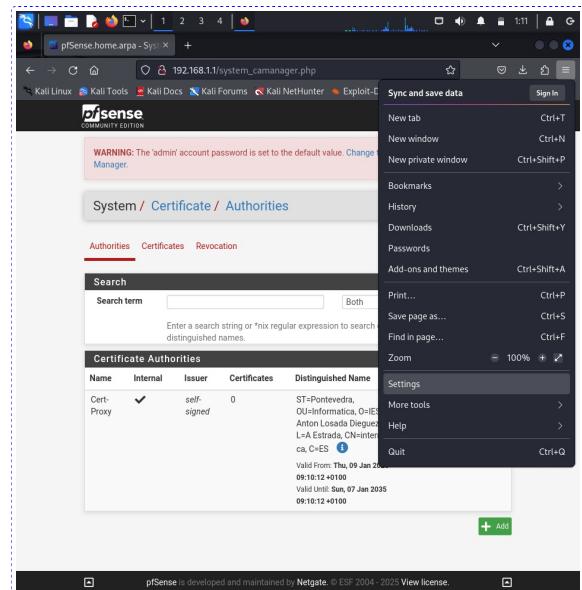
Export CA

192.168.1.1/system_cmanager.php?act=exp&id=677f8463e2e5a ned by Netgate. © ESF 2004–2025 View license.

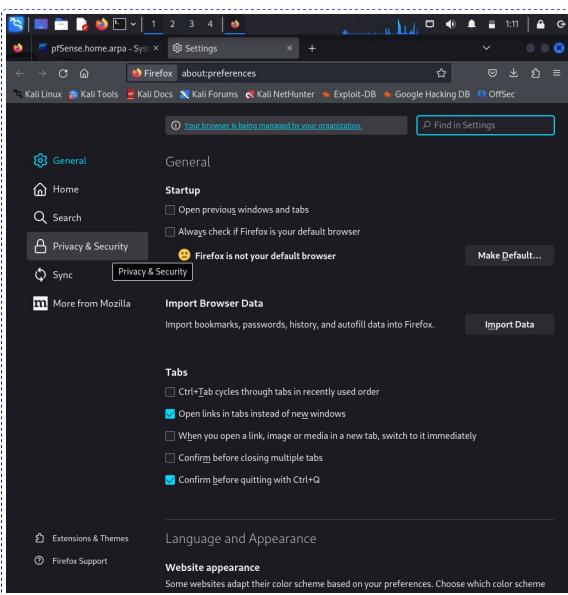
Premer no botón para exportar o certificado xerado.



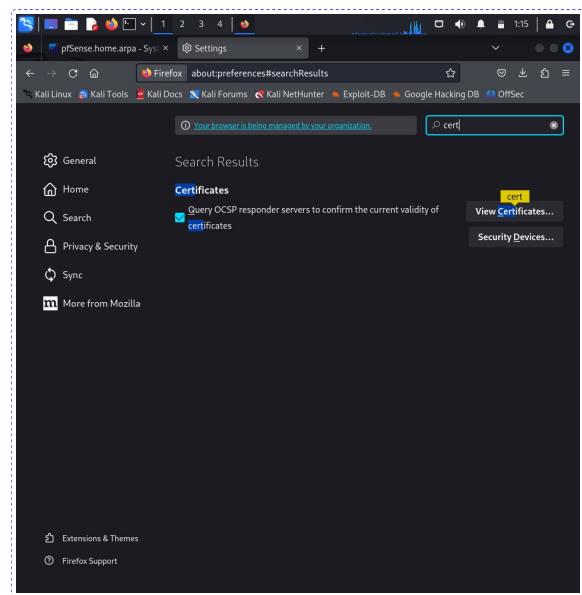
Certificado descargado (/home/kali/Downloads/Cert-Proxy.crt)



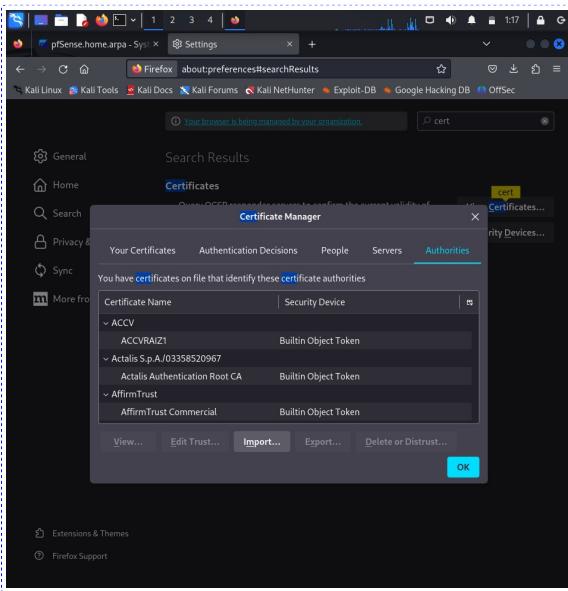
Ir á configuración(Settings) do navegador



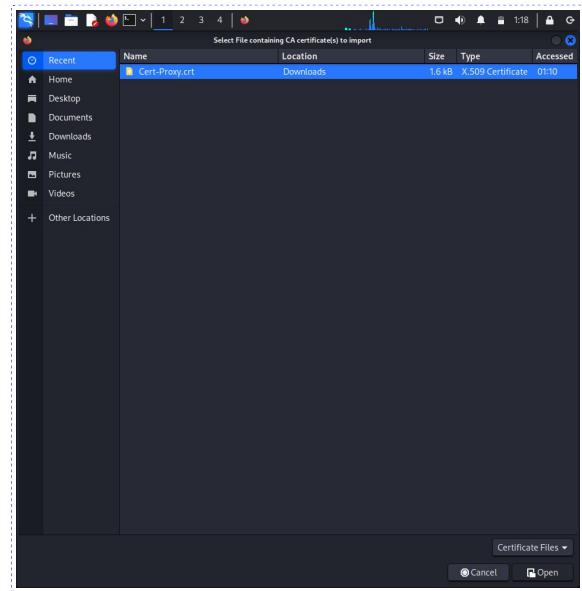
Escoller Privacy & Security



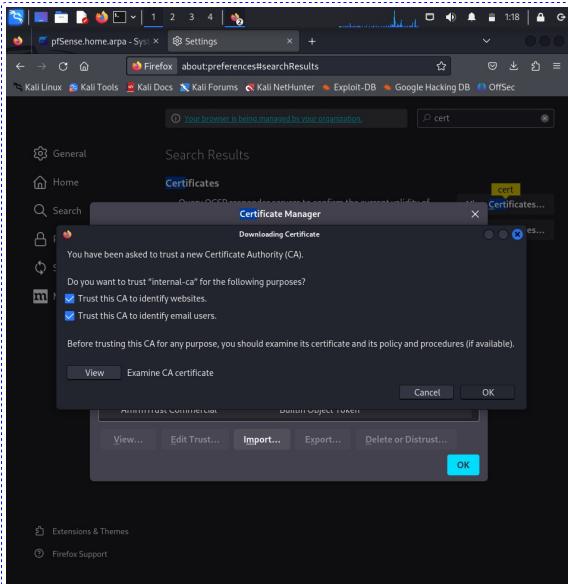
Ir á sección Certificates



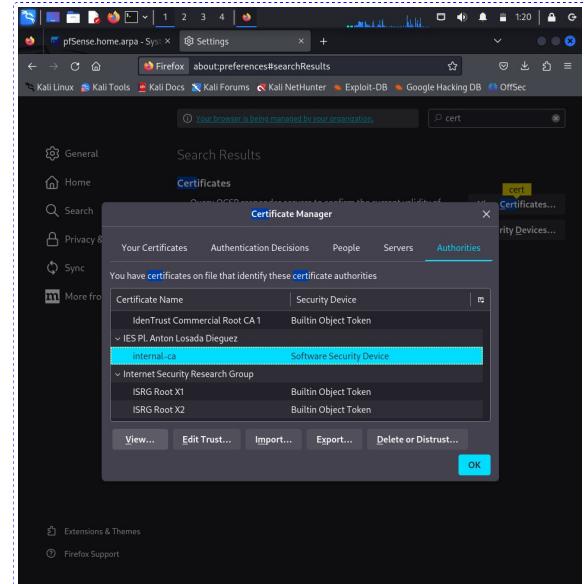
Importar o Certificado descargado na sección Authorities.



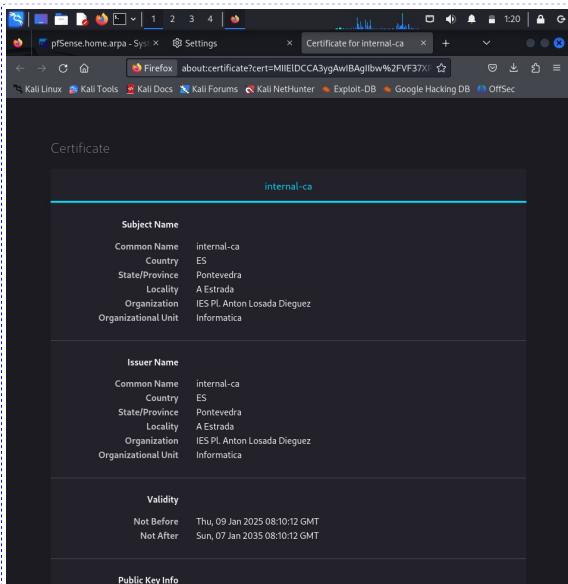
Escoller o certificado na ruta de descarga



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

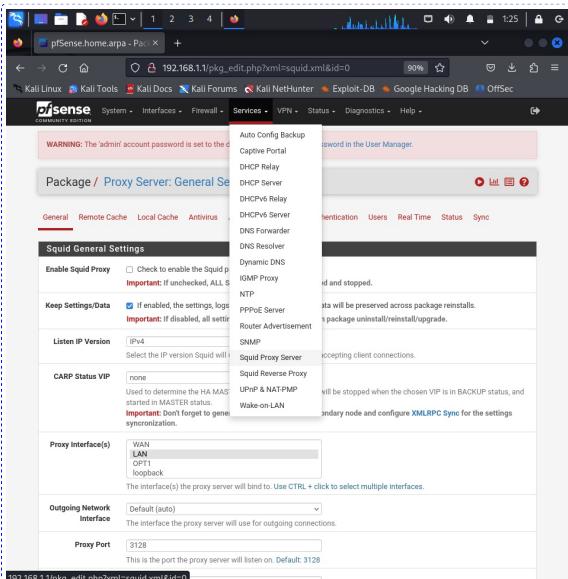


Certificado importado.

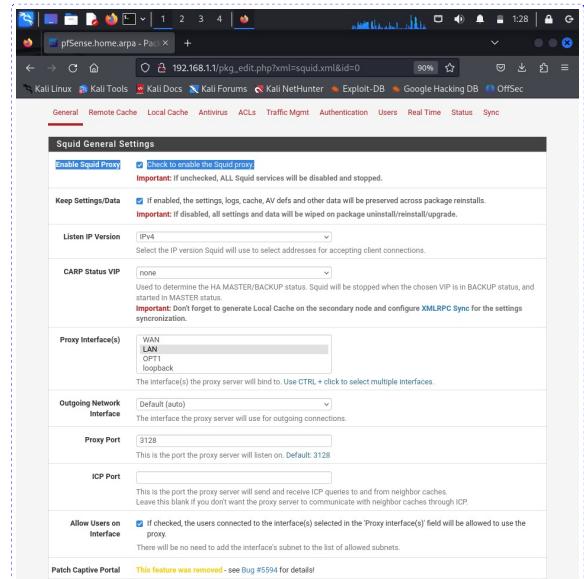


Ver as propiedades do certificado importado (premer na imaxe anterior en View co certificado seleccionado).

4. Configuración SQUID



Abrir Services → Squid Proxy Server



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

Transparent Proxy Settings

Transparent HTTP **Enable transparent mode to forward all requests from destination port 80 to the proxy server.**

Transparent proxy mode works without any additional configuration being necessary on clients.

Important: Transparent mode will filter SSL (port 443) if you enable HTTPS/SSL Intercept below.

Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s) WAN LAN OPT1

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Bypass Proxy for Private Address Destination **Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations.**

Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

Bypass Proxy for These Source IPs **Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.**

Applies only to transparent mode. Separate entries by semi-colons (;)

Bypass Proxy for These Destination IPs **Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.**

Applies only to transparent mode. Separate entries by semi-colons (;)

SSL Man in the Middle Filtering

HTTPS/SSL Interception **Enable SSL filtering.**

SSL/MITM Mode **Splice Whitelist, Bump Otherwise**

The SSL/MITM mode determines how SSL interception is treated when 'SSL Man in the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. Click Info for details.

SSL Intercept Interface(s) WAN LAN OPT1

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

Logging Settings

Enable Access **This will enable the access log.**

Warning: Do NOT enable if available disk space is low.

Log Store Directory /var/squid/logs

The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs

Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs

Defines how many days of logs will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard

Makes it possible for SquidGuard denied log to be included on Squid logs.

Click Info for detailed instructions.

Headers Handling, Language and Other Customizations

Visible Hostname localhost

This is the hostname to be displayed in proxy server error messages.

Administrator's Email admin@localhost

This is the email address displayed in error messages to the users.

Error Language en

Starts the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode (on)

Choose how to handle X-Forwarded-For headers. Default: on.

Disable VIA Header If not set, Squid will include a Via header in requests and replies as required by RFC2616.

URI Whitespace Characters Handling strip

Choose how to handle whitespace characters in URLs. Default: strip.

Suppress Squid Version Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

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

Minimum Object Size 0

Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum).

Maximum Object Size 4

Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB).

Squid Memory Cache Settings

Memory Cache Size 64

Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-Cached objects. Minimum value: 1 (MB). Default: 64 (MB).

Maximum Object Size in RAM 256

Objects greater than this size (in kilobytes) will not be attempted to be kept in the memory cache. Default: 256 (KB).

Memory Replacement Policy **Heap GDSF**

The memory replacement policy determines which objects are purged from memory when space is needed. Default: heap GDSF.

Dynamic and Update Content

Cache Dynamic Content Select to enable caching of dynamic content.

With dynamic cache enabled, you can also apply refresh_patterns to sites like Windows Updates.

Custom refresh_patterns

Enter custom refresh_patterns for better dynamic cache usage.

Note: These refresh_patterns will only be included if 'Cache Dynamic Content' is enabled.

Esta imaxe amosa o botón Save comentado na imaxe anterior.

SSL Man in the Middle Filtering

HTTPS/SSL Interception **Enable SSL filtering.**

SSL/MITM Mode **Splice Whitelist, Bump Otherwise**

The SSL/MITM mode determines how SSL interception is treated when 'SSL Man in the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. Click Info for details.

SSL Intercept Interface(s) WAN LAN OPT1

The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port 3129

This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode Modern

The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details.

DHParams Key Size 2048 (default)

DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA none **Cert-Proxy** **enabled.**

Applies only to transparent mode. Separate entries by semi-colons (;).

SSL Certificate Daemon Children 5

This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

Remote Cert Checks **Accept remote server certificate with errors**

Do not verify remote certificate

Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

Certificate Adapt Sets the "Not After" (setValidAfter)

Sets the "Not Before" (setValidBefore)

Sets CN property (setCommonName)

See [salproxy_cert_adapt](#) directive documentation and [Mimic original SSL server certificate](#) wiki article for details.

Escooller as opcións según aparece na imaxe para habilitar a incepción HTTPS/SSL. Baixar a pantalla.

WARNING: The admin account password is set to the default value. Change the password in the User Manager.

Package / Proxy Server: General Settings / General

General **Remote Cache** **Local Cache** **Antivirus** **ACLs** **Traffic Mgmt** **Authentication** **Users** **Real Time** **Status** **Sync**

The following input errors were detected:

- Please configure and save Local Cache settings first.

Squid General Settings

Enable Squid Proxy **Check to enable the Squid proxy.**

Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data **If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.**

Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version IPv4

Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP none

Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.

Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.

Proxy Interface(s) WAN LAN OPT1 loopback

The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Outgoing Network Default (auto)

The interface the proxy server will use for outgoing connections.

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"

WARNING: The admin account password is set to the default value. Change the password in the User Manager.

Package / Proxy Server: General Settings / General

General **Remote Cache** **Local Cache** **Antivirus** **ACLs** **Traffic Mgmt** **Authentication** **Users** **Real Time** **Status** **Restart Service**

Squid General Settings

Enable Squid Proxy **Check to enable the Squid proxy.**

Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data **If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.**

Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version IPv4

Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP none

Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.

Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.

Proxy Interface(s) WAN LAN OPT1 loopback

The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Outgoing Network Default (auto)

The interface the proxy server will use for outgoing connections.

Proxy Port 3128

This is the port the proxy server will listen on. Default: 3128

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 realizaase a través do proxy e como a comunicación establecese 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)

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:

The screenshot shows the pfSense certificate authorities list. A single certificate named 'Cert-Proxy' is listed. It is self-signed, issued by 'pfSense', and has a common name of 'OU=Infomatica, O=IES PI. Anton Losada Dieguez, L=A Estrada, CN=Cert-Proxy.ca, C=ES'. The certificate is valid from Jan 09, 2023, to Jan 07, 2035. There is a green 'Edit CA' button next to it.

The screenshot shows the 'Create / Edit CA' form for 'Cert-Proxy'. In the 'Description name' field, 'OpenVPN Server' is typed. In the 'Certificate data' field, a PEM certificate is pasted. In the 'Certificate Private Key (optional)' field, a PEM private key is pasted. In the 'Next Certificate Serial' field, the value '1' is entered. At the bottom, there is a 'Save' button.

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

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

The screenshot shows the pfSense certificates list. A new certificate named 'OpenVPN Server' is listed. It is self-signed, issued by 'Cert-Proxy', and has a common name of 'OpenVPN Server'. The certificate is valid from Jan 09, 2023, to Feb 09, 2026. There is a green 'Add/Sign' button next to it.

The screenshot shows the 'Add a New Certificate' form. In the 'Method' dropdown, 'Create an internal certificate' is selected. In the 'Description name' field, 'OpenVPN Server' is typed. In the 'Internal Certificate' section, 'Cert-Proxy+VPN' is selected as the certificate authority, 'RSA' as the key type, and '2048' as the key length. Other fields like 'Lifetime (days)', 'Common Name', and 'Organization' are filled with their respective values. At the bottom, there is a 'Save' button.

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

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

The screenshot shows the 'Certificate Attributes' form for the 'OpenVPN Server' certificate. In the 'Common Name' field, 'openvpnserver' is typed. In the 'Country Code' dropdown, 'ES' is selected. In the 'State or Province' field, 'Pontevedra' is typed. In the 'City' field, 'A Estrada' is typed. In the 'Organization' field, 'IES PI. Anton Losada Dieguez' is typed. In the 'Organizational Unit' field, 'Informatica' is typed. In the 'Attribute Notes' section, it says 'The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.' Under 'Certificate Type', 'Server Certificate' is selected. In the 'Alternative Names' section, 'FQDN or Hostname' is selected, and 'Value' is typed. At the bottom, there is a 'Save' button.

The screenshot shows the pfSense certificates list. The 'OpenVPN Server' certificate is now listed as 'In Use'. It is self-signed, issued by 'Cert-Proxy+VPN', and has a common name of 'OpenVPN Server'. The certificate is valid from Jan 09, 2023, to Feb 09, 2026. There is a green 'Add/Sign' button next to it.

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

Certificado OpenVPN-Server xerado.

e premer en Save.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Certificates / Certificates

Created internal certificate OpenVPN-Server

Authorities Certificates Certificate Revocation

Search Search term Both Search Clear

Enter a search string or *mix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default	self-signed	OrpionSense GUI default Self-Signed Certificate, CN=pfSense-677da9fbbe3d3		
OpenVPN-Server	Cert-Proxy+VPN	ST=Pontevedra, O=IIES Pl. Anton Losada Dieguez, L=A Estrada, CN=openvpnServer, C=ES		

Valid From: Tue, 07 Jan 2025 23:43:03 +0100
Valid Until: Mon, 09 Feb 2026 23:43:03 +0100

Valid From: Thu, 09 Jan 2025 17:26:49 +0100
Valid Until: Sun, 07 Jan 2035 17:26:49 +0100

+ Add/Sig

192.168.1.1/system_certmanager.php?act=new developed and maintained by Netgate © ESF 2004 - 2025 View license

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

The following certificate subject components are optional and may be left blank.

Common Name openvpnClient

Country Code ES

State or Province Pontevedra

City A Estrada

Organization IES Pl. Anton Losada Dieguez

Organizational Unit Informatica

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

Certificate Type User Certificate

Alternative Names FQDN or Hostname Value

Add SAN Row + Add SAN Row

Save

pfSense is developed and maintained by Netgate © ESF 2004 - 2025 View license

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

Method Create an internal Certificate

Descriptive name OpenVPN-Client-1

The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, %

Internal Certificate

Certificate authority Cert-Proxy+VPN

Key type RSA

Key length 2048

Digest algorithm sha256

Lifetime (days) 3650

The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Common Name openvpnClient1

The following certificate subject components are optional and may be left blank.

Country code ES

State or Province Pontevedra

City A Estrada

Organization IES Pl. Anton Losada Dieguez

Organizational Unit Informatica

192.168.1.1/system_certmanager.php?act=new developed and maintained by Netgate © ESF 2004 - 2025 View license

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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Certificates / Certificates

Created internal certificate OpenVPN-Client-1

Authorities Certificates Certificate Revocation

Search Search term Both Search Clear

Enter a search string or *mix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default	self-signed	OrpionSense GUI default Self-Signed Certificate, CN=pfSense-677da9fbbe3d3		
OpenVPN-Server	Cert-Proxy+VPN	ST=Pontevedra, O=IIES Pl. Anton Losada Dieguez, L=A Estrada, CN=openvpnServer, C=ES		
OpenVPN-Client-1	Cert-Proxy+VPN	ST=Pontevedra, O=IIES Pl. Anton Losada Dieguez, L=A Estrada, CN=openvpnClient1, C=ES		

Valid From: Tue, 07 Jan 2025 23:43:03 +0100
Valid Until: Mon, 09 Feb 2026 23:43:03 +0100

Valid From: Thu, 09 Jan 2025 17:26:49 +0100
Valid Until: Sun, 07 Jan 2035 17:26:49 +0100

+ Add/Sig

192.168.1.1/system_certmanager.php?act=new developed and maintained by Netgate © ESF 2004 - 2025 View license

Certificado OpenVPN-Client-1 xerado.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Interfaces / Firewall / Services / VPN / Status / Diagnostics / Help

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions

192.168.1.1/vpn_openvpn_server.php?act=new pfSense is developed and maintained by Netgate © ESF 2004 - 2025 View license

Ir a VPN → OpenVPN

Na sección Servers premer o botón Add

General Information

Description: openVPN-Server
A description of this VPN for administrative reference.

Disabled: Disable this server
Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode: Remote Access (SSL/TLS)
Device mode: tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2).

Endpoint Configuration

Protocol: UDP on IPv4 only
Interface: WAN
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port: 1194
The port used by OpenVPN to receive client connections.

Cryptographic Settings

TLS Configuration: Use a TLS Key

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

Cryptographic Settings

TLS Configuration

Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key

Peer Certificate Authority

No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

OCSP Check

Check client certificates with OCSP

Server certificate

OpenVPN-Server (Server Yes, CA: Cert-Proxy+VPN)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length

2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.

ECDH Curve

Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

AES-128-CBC (128 bit key, 128 bit block)	AES-256-GCM AES-128-GCM CHACHA20-POLY1305
AES-128-CFB (128 bit key, 128 bit block)	
AES-128-ECB (128 bit key, 128 bit block)	
AES-128-OCB (128 bit key, 128 bit block)	
AES-128-OFB (128 bit key, 128 bit block)	
AES-192-CFB (192 bit key, 128 bit block)	
AES-192-ECB (192 bit key, 128 bit block)	
AES-192-OFB (192 bit key, 128 bit block)	
AES-256-CFB (256 bit key, 128 bit block)	
AES-256-ECB (256 bit key, 128 bit block)	
AES-256-OFB (256 bit key, 128 bit block)	

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
The order of the selected data encryption algorithms is respected by OpenVPN. This list is ignored in shared key mode.

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

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.0.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining available addresses will be assigned to connecting clients.
A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including **Box Notify** and **Inactive**.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fd00::/64). The :1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IPv4/NETMASK or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections

3
Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance.
Compression can potentially increase performance but may allow an attacker to extract secrets if they can control compression and intercept the VPN (e.g. HTTPS). Before enabling compression, consult information about the VOLCANO, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Push Compression

Push the selected compression setting to connecting clients.

Type-of-Service

Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication

Allow communication between clients connected to this server

Duplicate Connection

Allow multiple concurrent connections from the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

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

Client Settings

Dynamic IP

Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet - One IP address per client in a common subnet
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this to be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Ping settings

Inactive

300
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Ping method

keepalive - Use keepalive helper to define ping config
ping = interval ping-restart = timeout#
push ping = interval
push ping-restart = timeout

Interval

10

Timeout

60

Advanced Client Settings

DNS Default Domain

Provide a default domain name to clients

DNS Server enable

Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1

8.8.4.4

DNS Server 2

8.8.8.8

DNS Server 3

DNS Server 4

Block Outside DNS

Make Windows 10 Clients Block access to DNS servers except those OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Force DNS cache update

Run "net stop dnscache", "net start dnscache", "pconfig flushdns" and "pconfig registerdns" on connection initiation.
This is known to kick Windows into recognizing pushed DNS servers.

NTP Server enable

Provide an NTP server list to clients

NetBIOS enable

Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

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

Advanced Client Settings

DNS Default Domain

Provide a default domain name to clients

DNS Server enable

Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1

8.8.4.4

DNS Server 2

8.8.8.8

DNS Server 3

DNS Server 4

Block Outside DNS

Make Windows 10 Clients Block access to DNS servers except those OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Force DNS cache update

Run "net stop dnscache", "net start dnscache", "pconfig flushdns" and "pconfig registerdns" on connection initiation.
This is known to kick Windows into recognizing pushed DNS servers.

NTP Server enable

Provide an NTP server list to clients

NetBIOS enable

Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push route 10.0.0.255 255.255.255.0

UDP Fast I/O

Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

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

Cryptographic Settings

TLS Configuration

Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

TLS Key

```
# 2048 bit OpenVPN static key
#-----BEGIN OpenVPN Static key V1-----
#-----END-----#
Paste the TLS key here.  
This key is used to sign control packets with an HMAC signature for authentication when establishing the tunnel.
```

TLS Key Usage Mode

TLS Encryption and Authentication
In authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections.
Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction

Use default direction
The TLS key direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority

Cert-Proxy+VPN

Peer Certificate Revocation List

No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

OCSP Check

Check client certificates with OCSP

Server certificate

OpenVPN-Server (Server Yes, CA: Cert-Proxy+VPN In U)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length

2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.

ECDH Curve

Use Default

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

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push route 10.0.0.0 255.255.255.0

Use fast I/O operations with UDP writes to tun/tap. Experimental.

Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPNv2 bandwidth limiting.

Exit Notify

Reconnect to this server / Retry once

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server mode, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /39 tunnel network as it will cause the server to exit and not restart.

Send/Receive Buffer

Default

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network upload speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 128KB and test higher and lower values.

Gateway creation

Both IPv4 only IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level

default

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None Only fatal
0: Default strength - Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

Save

pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

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

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	Mode: Remote Access (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	openVPN-Server	

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

Add

pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

Servidor OpenVPN configurado.

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

Firewall / Rules / WAN

Floating WAN LAN OPT1 OpenVPN

Rules (Drag to Change Order)

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> 0/0/B	IP4	*	*	10.10.10.10	80 (HTTP)	*	none		NAT Redirección do porto HTTP de WAN ao servidor DMZ	
<input type="checkbox"/> 0/0/B	IP4	*	*	10.10.10.10	443 (HTTPS)	*	none		NAT Redirección do porto HTTPS de WAN ao servidor da DMZ	

Add **1** **Delete** **Log** **Copy** **Save** **+ Separator**

192.168.1.1/firewall_rules_edit.php?if=wan&after=-1

pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

Ir a Firewall → Rules → WAN e premer no botón **Add**

Edit Firewall Rule

Action: Pass

What to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP/RST or ICMP port unreachable for UDP) is returned to the sender whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface: WAN (IPv4)

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

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: UDP

Choose which IP protocol this rule should match.

Source

Source: Invert match Any

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination: Invert match WAN address

Destination Address: /

Destination Port Range: OpenVPN (1194) From: Custom To: Custom

Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Save

pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

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

Firewall / Rules / WAN

Floating WAN LAN OPT1 OpenVPN

Rules (Drag to Change Order)

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> 0/0/B	IP4	*	*	WAN	1194	*	none			
<input type="checkbox"/> 0/0/B	IP4	*	*	10.10.10.10	80 (HTTP)	*	none		NAT Redirección do porto HTTP de WAN ao servidor DMZ	
<input type="checkbox"/> 0/0/B	IP4	*	*	10.10.10.10	443 (HTTPS)	*	none		NAT Redirección do porto HTTPS de WAN ao servidor da DMZ	

Add **1** **Delete** **Log** **Copy** **Save** **+ Separator**

pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

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

The firewall rule configuration has been changed.

The changes must be applied for them to take effect.

Apply Changes

Firewall / Rules / WAN

Floating WAN LAN OPT1 OpenVPN

Rules (Drag to Change Order)

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> 0/0/B	IP4	*	*	WAN	1194	*	none			
<input type="checkbox"/> 0/0/B	IP4	*	*	10.10.10.10	80 (HTTP)	*	none		NAT Redirección do porto HTTP de WAN ao servidor DMZ	
<input type="checkbox"/> 0/0/B	IP4	*	*	10.10.10.10	443 (HTTPS)	*	none		NAT Redirección do porto HTTPS de WAN ao servidor da DMZ	

Save

pfSense is developed and maintained by Netgate. © ESF 2004–2025 View license.

Para aplicar os cambios premer en "Apply Changes"

The screenshot shows the pfSense Firewall / Rules / WAN interface. It displays three rules for floating IP traffic:

- Rule 0/0 B: IPv4 UDP to WAN address (OpenVPN) port 1194, Action: none.
- Rule 0/0 B: IPv4 TCP to 10.10.10.10 port 80 (HTTP), Action: NAT Redirección do porto HTTP de WAN ao servidor DMZ.
- Rule 0/0 B: IPv4 TCP to 10.10.10.10 port 443 (HTTPS), Action: NAT Redirección do porto HTTPS de WAN ao servidor da DMZ.

Buttons at the bottom include Add, Add, Delete, Toggle, Copy, Save, and Separate.

Cambios aplicados e regra xerada.

The screenshot shows the pfSense Firewall / Rules / OpenVPN interface. A message states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." Below the message are buttons for Add, Delete, Toggle, Copy, Save, and Separate.

Ir a Firewall → Rules → OpenVPN e premer no botón

The screenshot shows the pfSense Edit Firewall Rule dialog for the OpenVPN interface. The Action dropdown is set to "Pass". Other settings include Interface: OpenVPN, Address Family: IPv4, and Protocol: Any. The Source and Destination sections are empty. Under Extra Options, there is a Log checkbox and a Description field. The Advanced Options section includes a "Save Advanced" button.

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

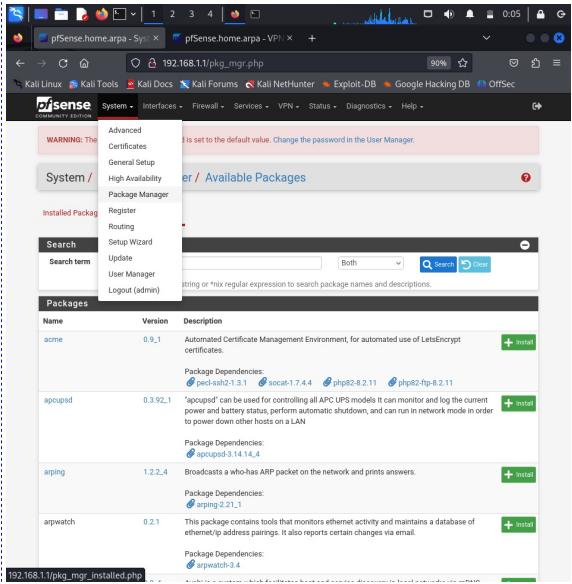
The screenshot shows the pfSense Firewall / Rules / OpenVPN interface. A message indicates: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." Below the message is a green "Apply Changes" button.

Para aplicar os cambios premer en "Apply Changes"

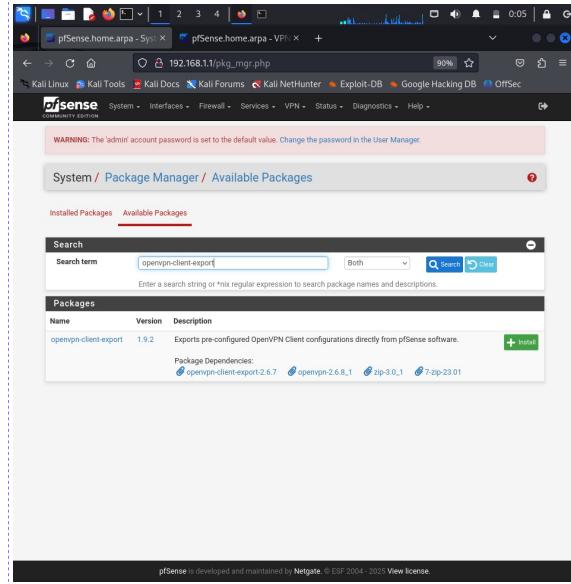
The screenshot shows the pfSense Firewall / Rules / WAN interface. A message states: "The changes have been applied successfully. The firewall rules are now reloading in the background." The interface lists the same three rules as the first screenshot, with the new rule added to the top of the list.

Cambios aplicados e regra xerada.

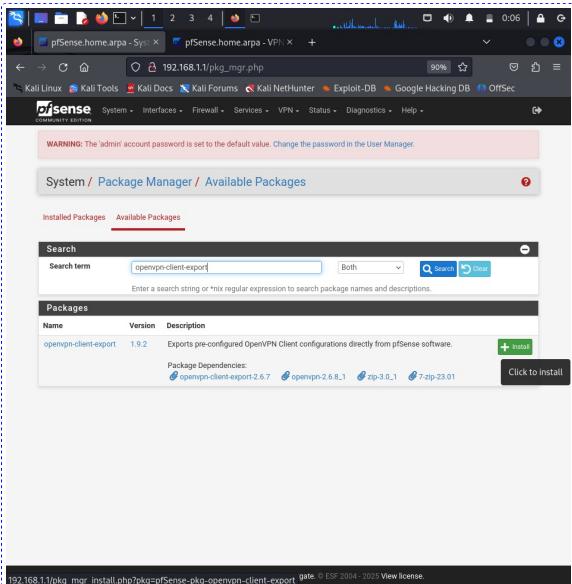
4. Exportar o arquivo de configuração OpenVPN para os clientes:



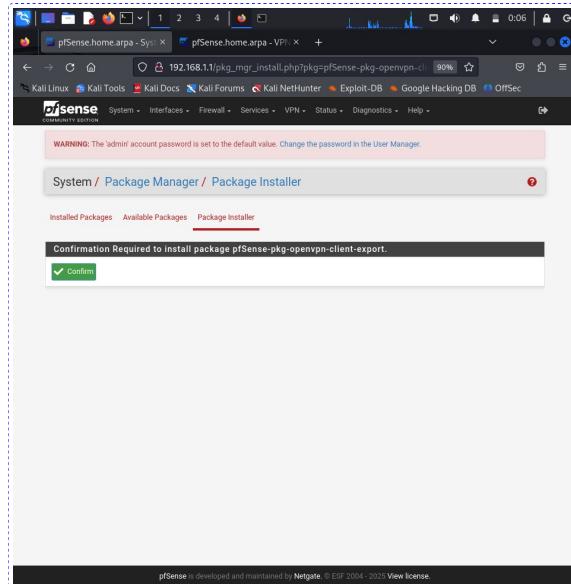
Abrir System → Package Manager



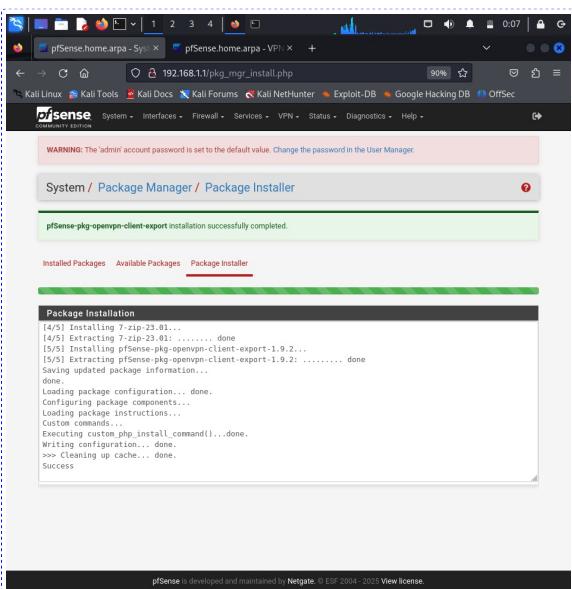
Buscar o padrão "openvpn-client-export" os paquetes possíveis a instalar.



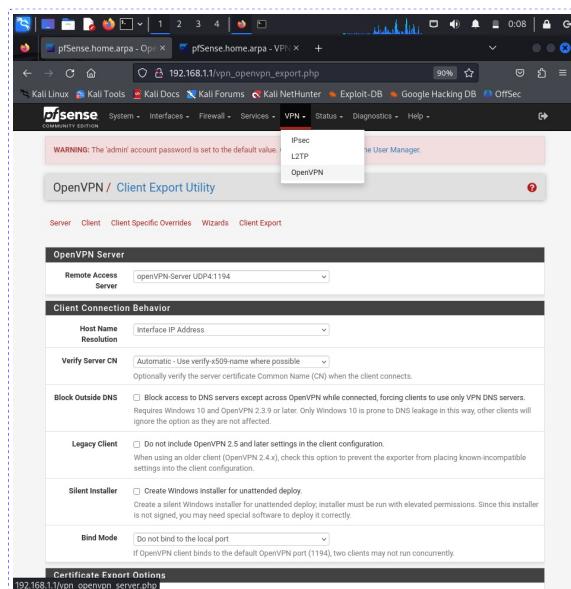
Premir no botón Install do paquete openvpn-client-export para proceder a instalalo.



Premir no botón Confirm para confirmar a instalación requerida.



Instalación do paquete openvpn-client-export realizado.



Abrir VPN → OpenVPN

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

OpenVPN Server

Remote Access Server openVPN-Server UDP4:1194

Client Connection Behavior

Host Name Resolution Interface IP Address

Verify Server CN Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way; other clients will ignore the option as they are not affected.

Legacy Client Do not include OpenVPN 2.5 and later settings in the client configuration.
When using a legacy client (OpenVPN 2.4.X), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer Create Windows installer for unattended deploy.
Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode Use a random local source port
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Certificate Export Options

PKCS#11 Certificate Storage Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage Use Microsoft Certificate Storage instead of local files.

Only OpenVPN-compatible user certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

Using clients with OpenSSL 3.0 may not work with older or weaker ciphers and hashes, such as SHA1, including when those were used to sign CA and certificate entries.

OpenVPN 2.4.8+ requires Windows 7 or later

Links to OpenVPN clients for various platforms:

- OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above the Windows installers
- OpenVPN For Android - Recommended client for Android
- OpenVPN Connect (Android (Google Play) or iOS (App Store)) - Recommended client for iOS
- Mac OS X and Windows

`javascript:download_begin('configfile', '1.0')`

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

Only OpenVPN-compatible user certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

Clients using OpenSSL 3.0 may not work with older or weaker ciphers and hashes, such as SHA1, including when those were used to sign CA and certificate entries.

OpenVPN 2.4.8+ requires Windows 7 or later

Links to OpenVPN clients for various platforms:

- OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above in the Windows installers
- OpenVPN For Android - Recommended client for Android
- OpenVPN Connect (Google Play) or iOS [App Store] - Recommended client for iOS
- javascript:download_begin('config1.ovpn') for Mac OS X and Windows

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

5. Conectar o cliente mediante VPN:

```
[kali㉿kali: ~]
$ ls
[ kali@kali: ~]
$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
    link-layer brd 00:00:00:00:00:00
inet 172.16.0.2/16 brd 172.16.0.255 scope global dynamic noprefixroute et
    valid_lft 343sec preferred_lft 343sec
    link-layer brd ff:ff:ff:ff:ff:ff
inet 172.16.0.2/24 brd 172.16.0.255 scope link link-layer brd ff:ff:ff:ff
    valid_lft forever preferred_lft forever

[ kali@kali: ~]
$ 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@kali: ~]
$ netplan apply
[ kali@kali: ~]
$ cat /etc/netplan/01-netcfg.yaml
# Generated by NetworkManager
nameserver 192.168.1.1

[ kali@kali: ~]
$
```

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 serviço SSH em kaliB

```

kali㉿kali: ~
$ sudo openvpn pfSense-UDP4-1194-uservpn-config.ovpn
2025-01-10 15:34:29 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD]
2025-01-10 15:34:29 LZO lib version: OpenSSL 3.2.2 4 Jun 2024, LZO 2.0
2025-01-10 15:34:29 TCP/UDP: Preserving recently used remote address: [AF_INET]172.16.0.7:1194
2025-01-10 15:34:29 UDPv4 link remote: [AF_INET]172.16.0.7:1194
2025-01-10 15:34:29 [openvpnServer] Peer Connection Initiated with [AF_INET]172.16.0.7:1194
2025-01-10 15:34:29 Options error: Unrecognized option or missing or extra parameter(s) in [PUSH
OPTIONS]4: block
2025-01-10 15:34:29 TUN/TAP device tun0 opened
2025-01-10 15:34:29 net_iface_atu_set: mtu 1500 for tun0
2025-01-10 15:34:29 net_iface_up: set tun0 up
2025-01-10 15:34:29 net_addr_v4_Addr: 10.6.8.3/24 dev tun0
2025-01-10 15:34:29 Initialization Sequence Completed

```

Establecer a conexión VPN con kaliB dende kaliC

```

kali㉿kali: ~
$ sudo openvpn pfSense-UDP4-1194-uservpn-config.ovpn
2025-01-10 15:34:29 [MH/PKTINFO] [~]
11 [MH/PKTINFO] [~]
2025-01-10 15:34:29 [~]
2025-01-10 15:34:29 ip link show
2025-01-10 15:34:29 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
2025-01-10 15:34:29 ault qlen 1000
2025-01-10 15:34:29 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2025-01-10 15:34:29 inet 127.0.0.1/8 scope host lo
2025-01-10 15:34:29 valid_lft forever preferred_lft forever
2025-01-10 15:34:29 2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
2025-01-10 15:34:29 ault qlen 1000
2025-01-10 15:34:29 link/ether 00:00:27:67:b0:c7 brd ff:ff:ff:ff:ff:ff
2025-01-10 15:34:29 inet 172.16.0.24 brd 172.16.0.255 scope global dynamic noprefixroute et
2025-01-10 15:34:29      valid_lft 457sec preferred_lft 457sec
2025-01-10 15:34:29 3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group none
2025-01-10 15:34:29 ault qlen 500
2025-01-10 15:34:29 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
2025-01-10 15:34:29      valid_lft forever preferred_lft forever
2025-01-10 15:34:29      inet 10.6.8.3/24 scope global tun0
2025-01-10 15:34:29          valid_lft forever preferred_lft forever
2025-01-10 15:34:29          inet6 fe80::53ef:6e7a:e874:5082/64 scope link stable-privacy proto kernel
2025-01-10 15:34:29              valid_lft forever preferred_lft forever

```

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

Aparece unha nova NIC: tun0

```

kali㉿kali: ~
$ sudo openvpn pfSense-UDP4-1194-uservpn-config.ovpn
2025-01-10 15:34:29 [MH/PKTINFO] [~]
2025-01-10 15:34:29 [~]
2025-01-10 15:34:29 File Actions Edit View Help
2025-01-10 15:34:29 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
2025-01-10 15:34:29 ault qlen 1000
2025-01-10 15:34:29 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2025-01-10 15:34:29      valid_lft forever preferred_lft forever
2025-01-10 15:34:29 2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
2025-01-10 15:34:29 ault qlen 1000
2025-01-10 15:34:29 link/ether 00:00:27:67:b0:c7 brd ff:ff:ff:ff:ff:ff
2025-01-10 15:34:29      valid_lft 457sec preferred_lft 457sec
2025-01-10 15:34:29 3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group none
2025-01-10 15:34:29 ault qlen 500
2025-01-10 15:34:29 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
2025-01-10 15:34:29      valid_lft forever preferred_lft forever
2025-01-10 15:34:29      inet 172.16.0.24 brd 172.16.0.255 scope global tun0
2025-01-10 15:34:29          valid_lft forever preferred_lft forever
2025-01-10 15:34:29          inet6 fe80::53ef:6e7a:e874:5082/64 scope link stable-privacy proto kernel
2025-01-10 15:34:29              valid_lft forever preferred_lft forever

```

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

```

kali㉿kali: ~
$ sudo openvpn pfSense-UDP4-1194-uservpn-config.ovpn
2025-01-10 15:34:29 [MH/PKTINFO] [~]
2025-01-10 15:34:29 [~]
2025-01-10 15:34:29 File Actions Edit View Help
2025-01-10 15:34:29 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
2025-01-10 15:34:29 ault qlen 1000
2025-01-10 15:34:29 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2025-01-10 15:34:29      valid_lft forever preferred_lft forever
2025-01-10 15:34:29 2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
2025-01-10 15:34:29 ault qlen 1000
2025-01-10 15:34:29 link/ether 00:00:27:67:b0:c7 brd ff:ff:ff:ff:ff:ff
2025-01-10 15:34:29      valid_lft 457sec preferred_lft 457sec
2025-01-10 15:34:29 3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group none
2025-01-10 15:34:29 ault qlen 500
2025-01-10 15:34:29 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
2025-01-10 15:34:29      valid_lft forever preferred_lft forever
2025-01-10 15:34:29      inet 10.6.8.3/24 scope global tun0
2025-01-10 15:34:29          valid_lft forever preferred_lft forever
2025-01-10 15:34:29          inet6 fe80::53ef:6e7a:e874:5082/64 scope link stable-privacy proto kernel
2025-01-10 15:34:29              valid_lft forever preferred_lft forever

```

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.

openvpn: openVPN-Server UDP4:1194 / Client Connections: 1						
Common Name	Real Address	Virtual Address	Last Change	Bytes Sent	Bytes Received	Cipher
uservpn	172.16.0.84986	10.6.8.3	2025-01-10 16:34:29	11 kB	10 kB	AES-256-GCM

Show Routing Table - Display OpenVPN's internal routing table for this server.

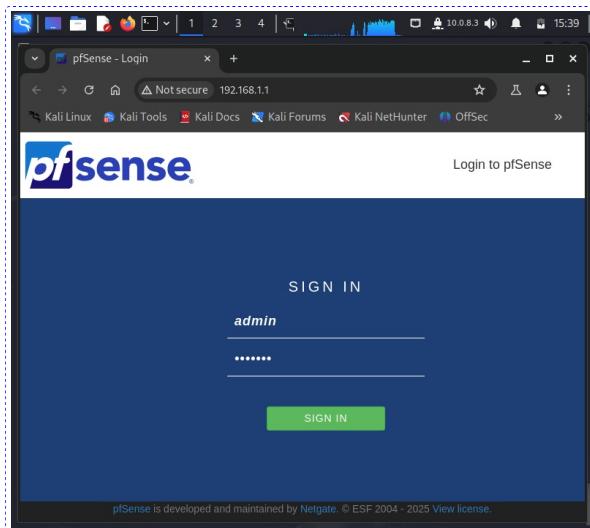
Comprobar en Status → OpenVPN que existe unha conexión VPN establecida. Premir en "Show Routing Table"

openVPN-Server UDP4:1194 / Client Connections: 1			
Common Name	Real Address	Virtual Address	Last Change
uservpn	172.16.0.84986	10.6.8.3	2025-01-10 16:34:29

openVPN-Server UDP4:1194 Routing Table		
Common Name	Real Address	Target Network
uservpn	172.16.0.84986	10.6.8.3

An IP address followed by C indicates a host currently connected through the VPN.

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

Ainda 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).

The screenshot shows the pfSense Firewall Rules / OPT1 interface. At the top, there is a warning about the admin password. Below it, the interface is titled 'Firewall / Rules / OPT1'. A table header 'Rules (Drag to Change Order)' is shown with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A message below the table states: 'No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.' At the bottom, there are several action buttons: Add, Edit, Delete, Toggle, Copy, Save, and Separator.

This screenshot shows the same pfSense Firewall Rules / OPT1 interface after a new rule has been added. The message at the bottom now says: 'The firewall rule configuration has been changed. The changes must be applied for them to take effect.' A green 'Apply Changes' button is visible. The table now contains one row: '0/0 B IPv4 * OPT1 subnets * LAN subnets * * none Bloquear comunicación da rede DMZ a LAN'. The 'Add' button is highlighted in green.

Escoler no menú a opción: Firewall → Rules → OPT1

Premre en para xerar unha nova regra.

This screenshot shows the 'Edit Firewall Rule' dialog for a new rule. It includes sections for Action (Block), Disabled (unchecked), Interface (OPT1), Address Family (IPv4), Protocol (Any), Source (OPT1 subnets), Destination (LAN subnets), Extra Options (Log checkbox unchecked, Description 'Bloquear comunicación da rede DMZ a LAN'), and Advanced Options (Display Advanced). A 'Save' button is at the bottom.

This screenshot shows the pfSense Firewall Rules / OPT1 interface after saving the new rule. A message at the top says: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below it, a yellow box says: 'The firewall rule configuration has been changed. The changes must be applied for them to take effect.' A green 'Apply Changes' button is present. The table now shows the new rule: '0/0 B IPv4 * OPT1 subnets * LAN subnets * * none Bloquear comunicación da rede DMZ a LAN'. The 'Add' button is highlighted in green.

Para aplicar os cambios premre en "Apply Changes"

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

This screenshot shows the pfSense Firewall Rules / OPT1 interface after changes have been applied. A green message box at the top says: 'The changes have been applied successfully. The firewall rules are now reloading in the background.' Below it, the interface shows the new rule: '0/0 B IPv4 * OPT1 subnets * LAN subnets * * none Bloquear comunicación da rede DMZ a LAN'. The 'Add' button is highlighted in green.

Cambios aplicados e regra xerada.