

FACULTAD DE CIENCIA Y TECNOLOGÍA
CENTRO REGIONAL DE USULUTÁN
INGENIERÍA EN SISTEMAS Y REDES INFORMÁTICAS

SEGURIDAD INFORMÁTICA
CICLO II – 2025



ACTIVIDAD:

LABORATORIO 2 COMPUTO 3 – GUÍA PFSENSE.

DOCENTE:

ING. TIMOTEA GUADALUPE MENJIVAR.

ESTUDIANTES:

| | |
|----------------------------------|------------|
| ANA PATRICIA GAITÁN HERNÁNDEZ | USSF017122 |
| FREDY ADILSON CAMPOS HERNÁNDEZ | USSF017322 |
| JOSUÉ GABRIEL CAMPOS ESCOBAR | USIS006316 |
| LESLY CAROLINA BERMÚDEZ MEMBREÑO | USSF017722 |
| ROMEO ALEXANDER GARCIA CASTILLO | USIS000313 |

FECHA DE ENTREGA:

USULUTÁN, MIERCOLES 10 DE OCTUBRE DE 2025.

PFSENSE.

Es un firewall / router de código abierto, basado en FreeBSD. Se usa para:

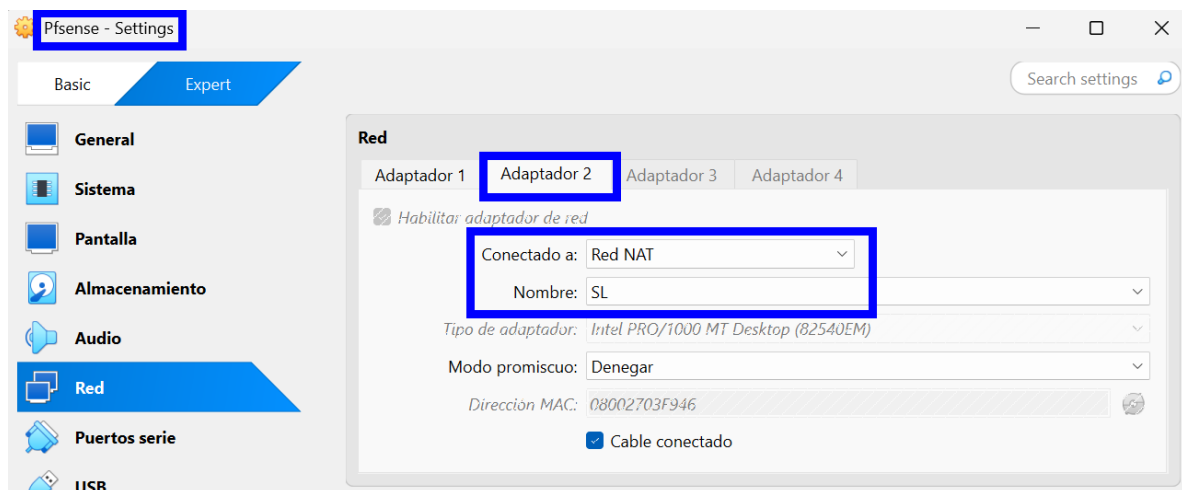
- Enrutamiento.
- Firewall (reglas de entrada y salida).
- NAT.
- VPN.
- DHCP.
- Creación de VLANs.
- Segmentación de red.

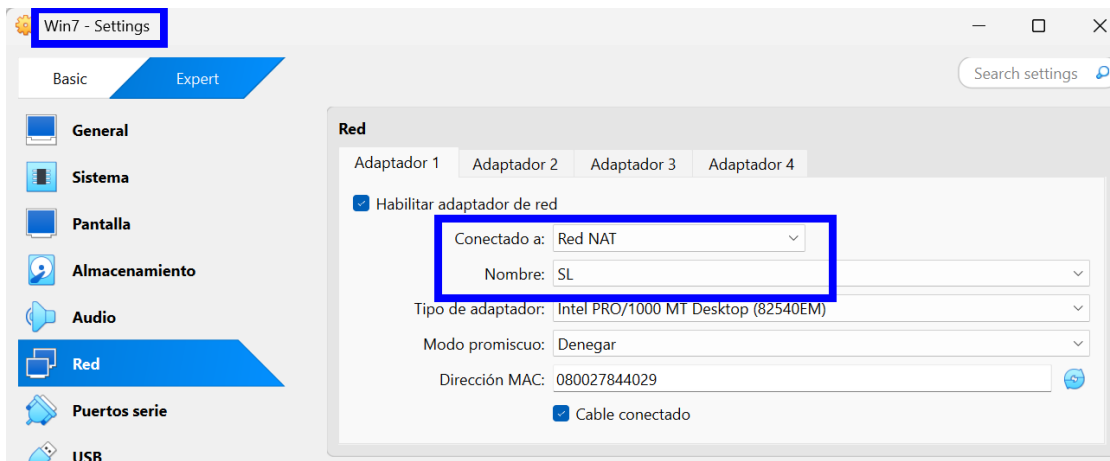
Las reglas creadas en PFSENSE, se evalúan de **ARRIBA HACIA ABAJO**.
La **primera regla que coincide SE APLICA**.

ACCESO DESDE EL CLIENTE.

Primero debemos verificar que este dentro del adaptador de red seleccionado para la conexión, por lo tanto, el cliente debe estar conectado la red NAT llamada "SL" que usa la **LAN de pfsense**.

Esto asegura que estén en el mismo segmento lógico.





Adaptador de Ethernet Conexión de área local:

```
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::100:4868:14d0:fa7f%12  
Dirección IPv4. . . . . : 192.168.1.4  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

Adaptador de túnel isatap.{688996FD-F5F3-40C5-9CC4-A278BA838A51}:

```
Estado de los medios. . . . . : medios desconectados  
Sufijo DNS específico para la conexión. . . :
```

Adaptador de túnel Conexión de área local*:

```
Estado de los medios. . . . . : medios desconectados  
Sufijo DNS específico para la conexión. . . :
```

C:\Users\Romeo García> ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

```
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64
```

Estadísticas de ping para 192.168.1.1:

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:

```
Mínimo = 3ms, Máximo = 4ms, Media = 3ms
```

C:\Users\Romeo García>

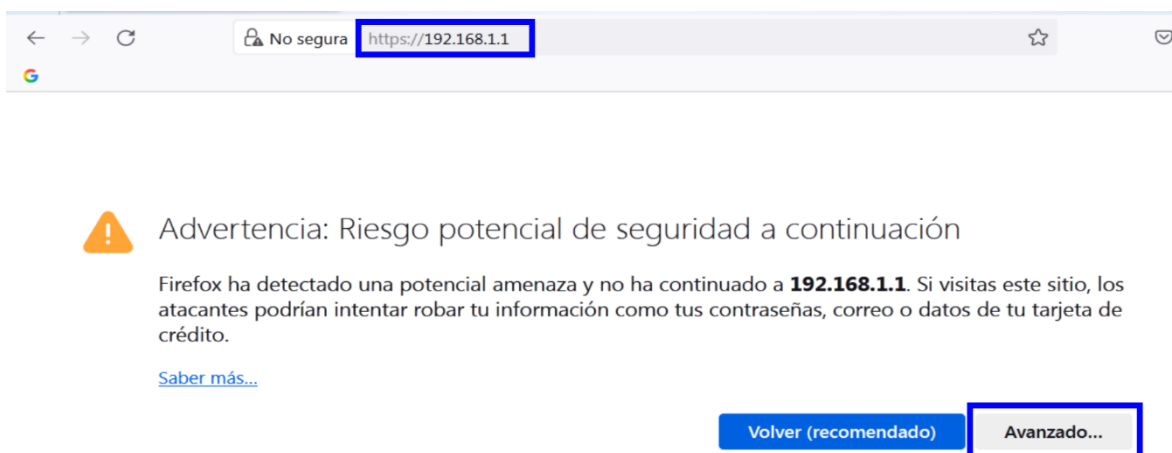
Verificando que el cliente ve a pfsense a nivel de capa 2.

```
C:\Users\Romeo Garcia>arp -a

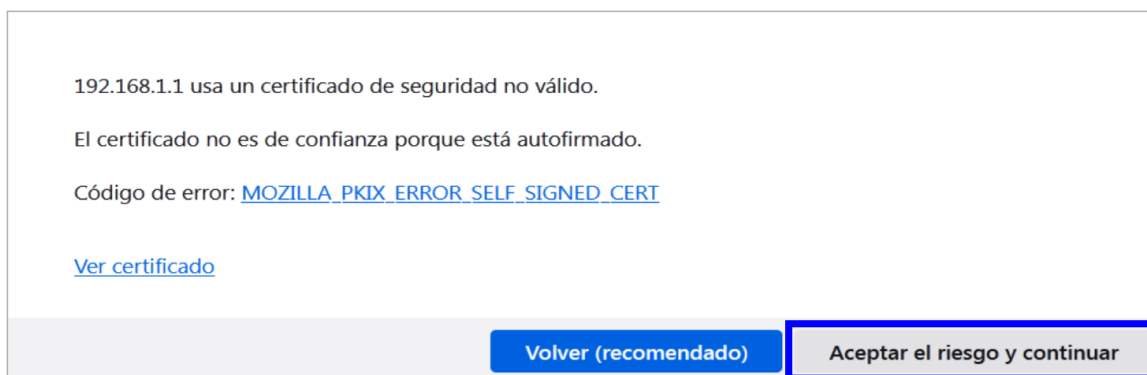
Interfaz: 192.168.1.4 --- 0xc
Dirección de Internet      Dirección física      Tipo
192.168.1.1                08-00-27-03-f9-46    dinámico
192.168.1.3                08-00-27-5b-e9-4c    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

C:\Users\Romeo Garcia>
```

Debemos acceder al panel web, por medio de la ip: 192.168.1.1 y dar clic en el botón “Avanzado”.



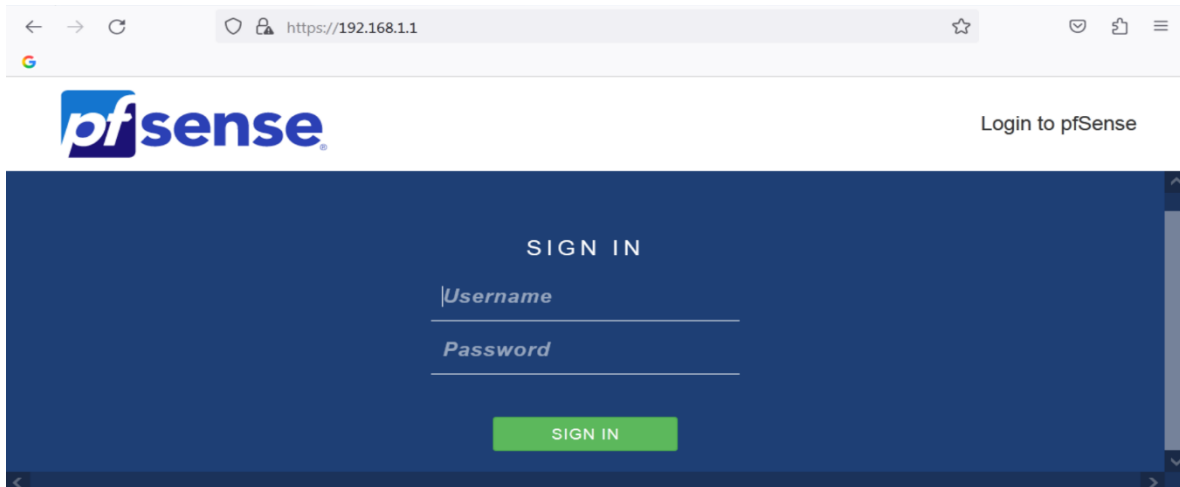
Luego debemos dar clic en el botón “Aceptar el riesgo y continuar”.



Nos abre el panel de inicio de sesión de Pfsense, las credenciales para iniciar sesión son las siguientes:

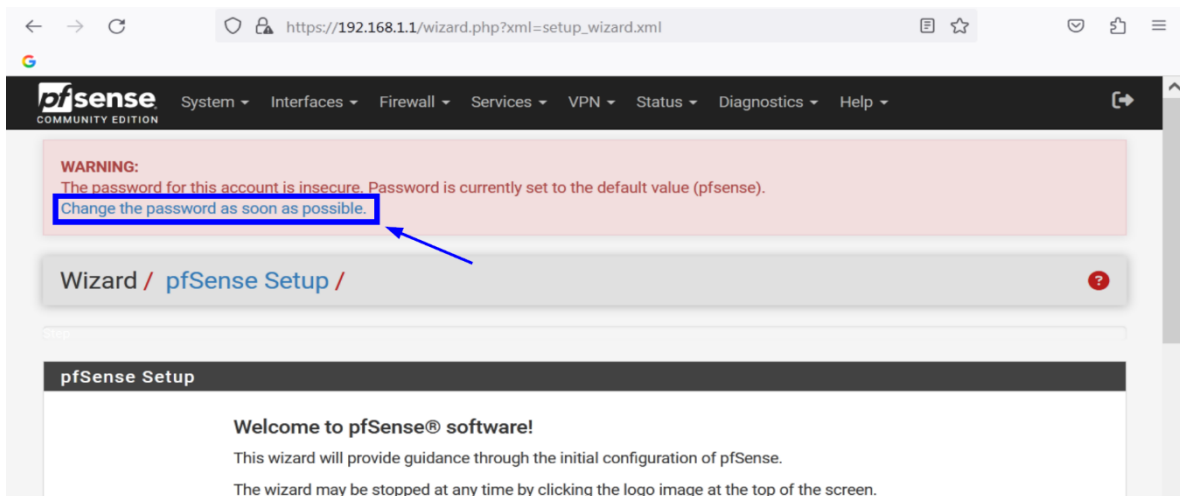
Usuario: admin

Contraseña: pfsense

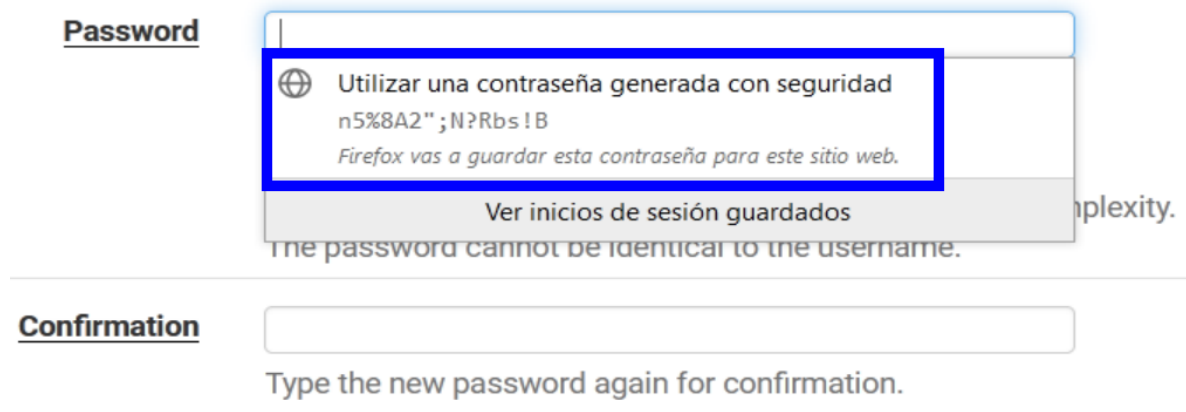


Una vez entrando al panel, debemos cambiar la contraseña:

Para ello debemos dar clic en el link que nos dice cambiar contraseña.



Una vez dentro, le daremos una contraseña segura, de hecho, el mismo sistema nos dice que debemos utilizar una contraseña generada con seguridad. Para efectos prácticos nosotros generamos una con la web [lastpass](#), esta es de un mínimo de 18 caracteres.



Password

Utilizar una contraseña generada con seguridad
n5%8A2";N?Rbs!B
Firefox vas a guardar esta contraseña para este sitio web.

Ver inicios de sesión guardados

complexity.

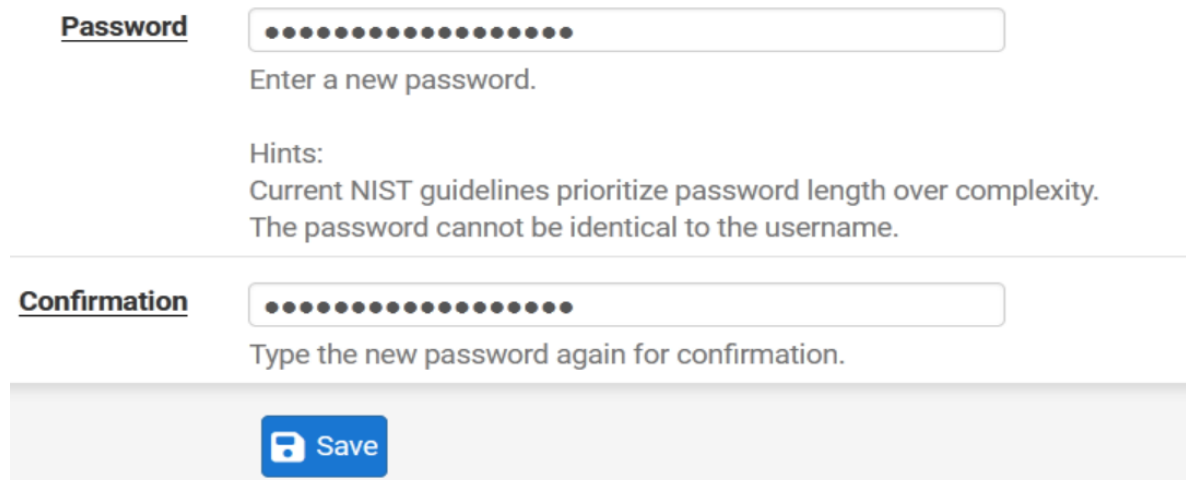
The password cannot be identical to the username.

Confirmation

Type the new password again for confirmation.

Por ser destinado a la práctica, mostraremos la contraseña utilizada, sin embargo, debemos aclarar que, en un entorno real, nunca debemos mostrar la contraseña.

Contraseña generada: 1e7&3u80>4GwrrN|Sy



Password

Enter a new password.

Hints:
Current NIST guidelines prioritize password length over complexity.
The password cannot be identical to the username.

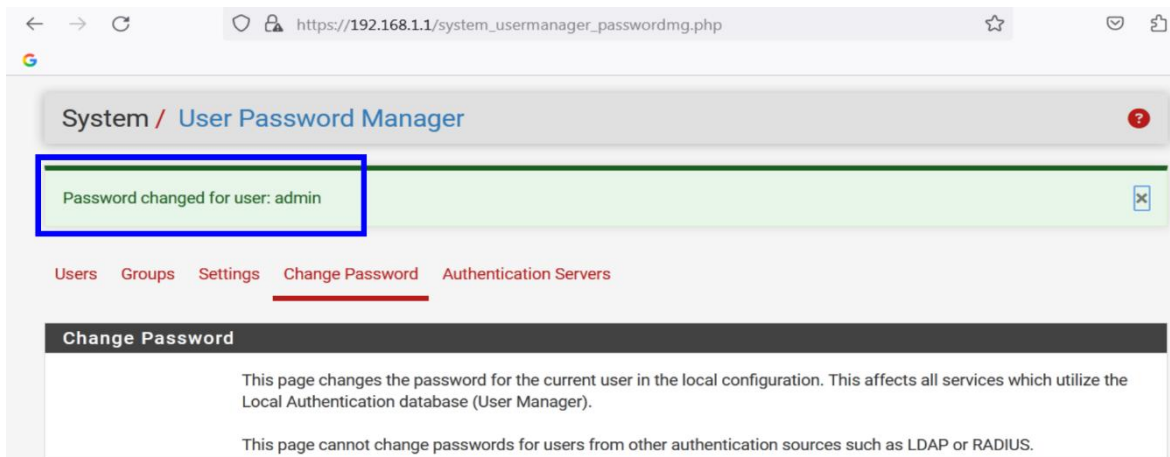
Confirmation

Type the new password again for confirmation.

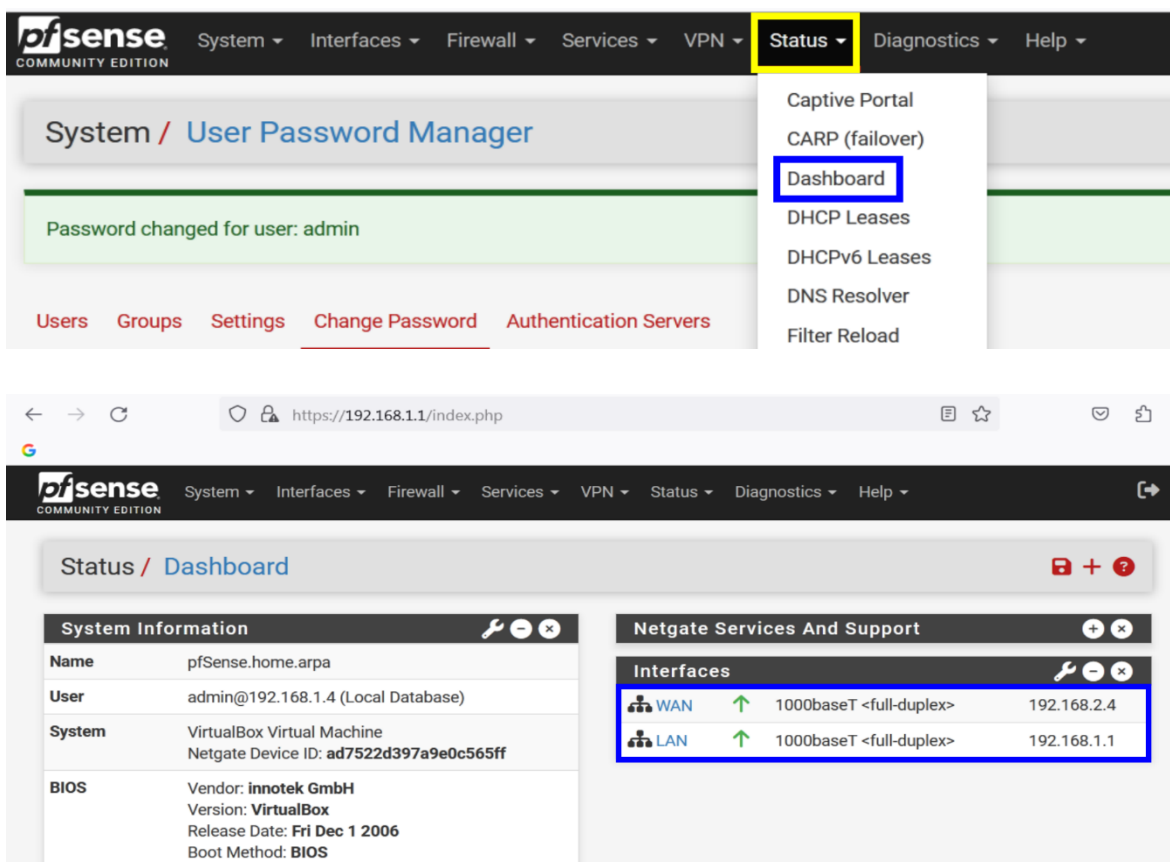
Save

Por último, daremos clic en el botón “Save”, para guardar los cambios.

Nos mostrará un mensaje indicándonos que la contraseña ha sido cambiada exitosamente.



Ahora, debemos ir al menú status en la opción dashboard para visualizar la configuración del sistema. Entre ellas la configuración de nuestro firewall que es la WAN y la configuración de red de los clientes en la LAN.



CONFIGURACIÓN INICIAL DE PFSENSE.

Crear alias y reglas.

Debemos describir que es un alias en pfsense para una mejor comprensión de la herramienta.

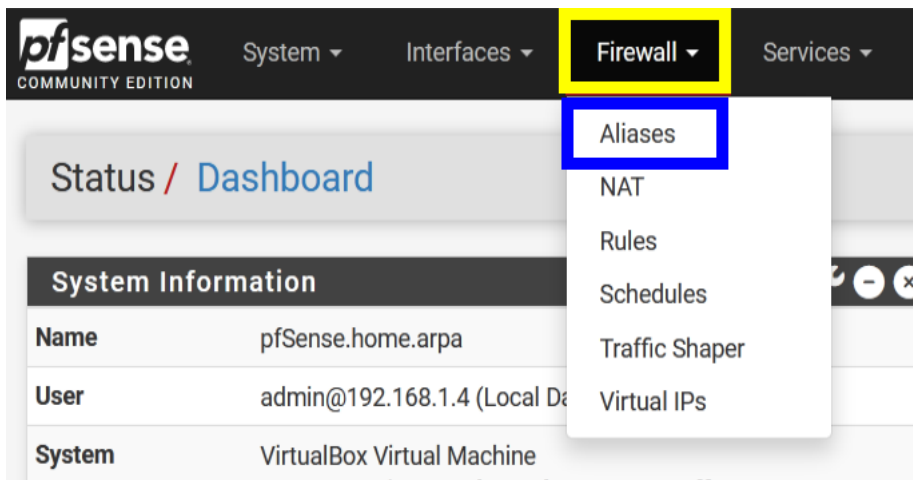
Un alias es un nombre que agrupa varios elementos de red (dominios, direcciones IP o redes).

En lugar de escribir muchos dominios uno por uno en una regla, se agrupan bajo un alias y se utilizan como si fuera un solo objeto.

Para crearlo debemos realizar los siguientes pasos:

Paso 1:

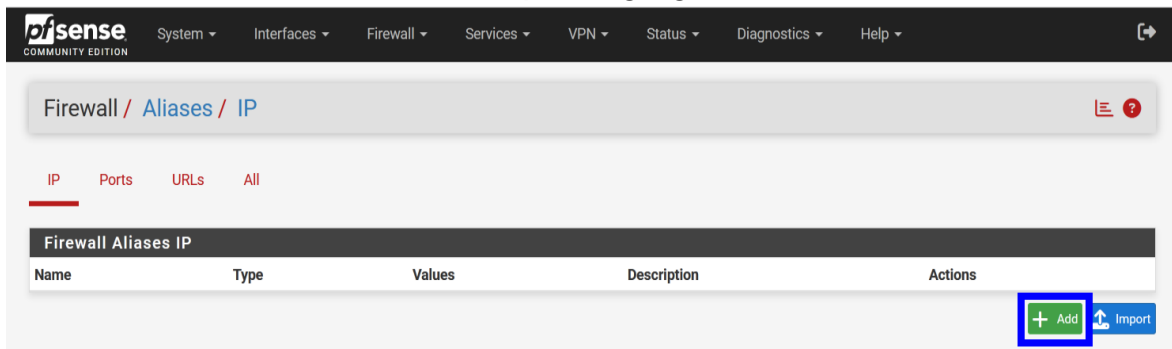
Debemos ir al panel Firewall → Aliases.



Paso 2:

Creamos el alias para bloquear algunos dominios. Este alias se asociará a una regla de firewall.

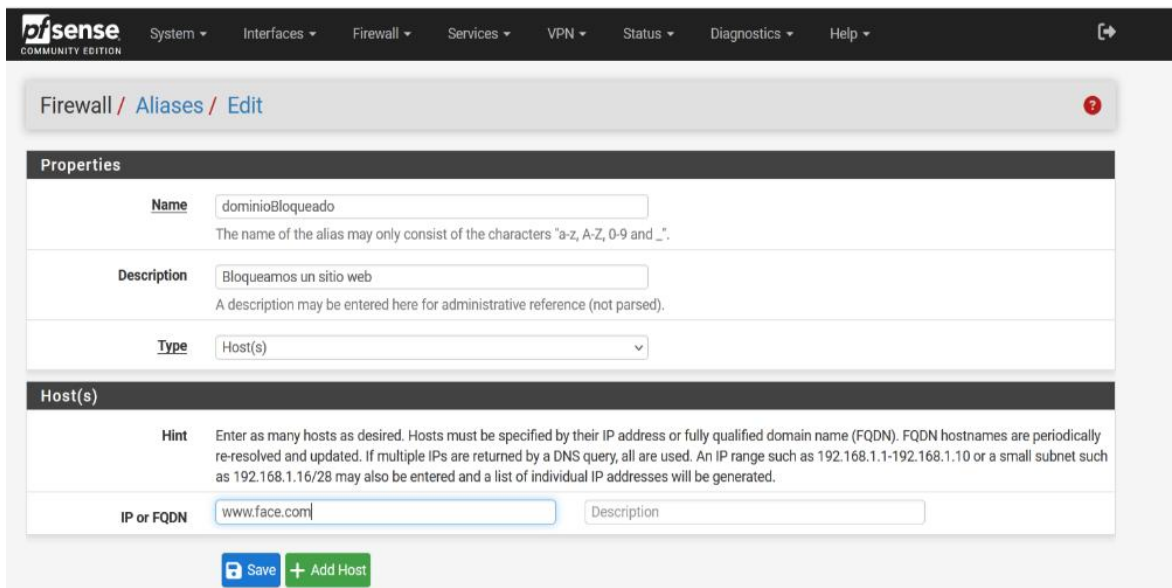
Vamos a dar clic en el botón **add** para agregar un nuevo alias.



Nos saldrá el siguiente panel:

The screenshot shows the 'Edit' page for a Firewall Alias in PfSense. The breadcrumb trail is 'Firewall / Aliases / Edit'. The 'Properties' section contains three fields: 'Name' (with a hint: 'The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _"'), 'Description' (with a hint: 'A description may be entered here for administrative reference (not parsed).'), and 'Type' (set to 'Host(s)'). Below the 'Properties' section is the 'Host(s)' section, which includes a 'Hint' explaining that hosts must be specified by IP address or FQDN, and a table with columns 'IP or FQDN' and 'Description'. At the bottom, there are 'Save' and '+ Add Host' buttons.

Vamos a configurar de la siguiente manera y por último daremos clic en el botón “Save”



Firewall / Aliases / Edit

Properties

Name dominioBloqueado
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description Bloqueamos un sitio web
A description may be entered here for administrative reference (not parsed).

Type Host(s)

Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

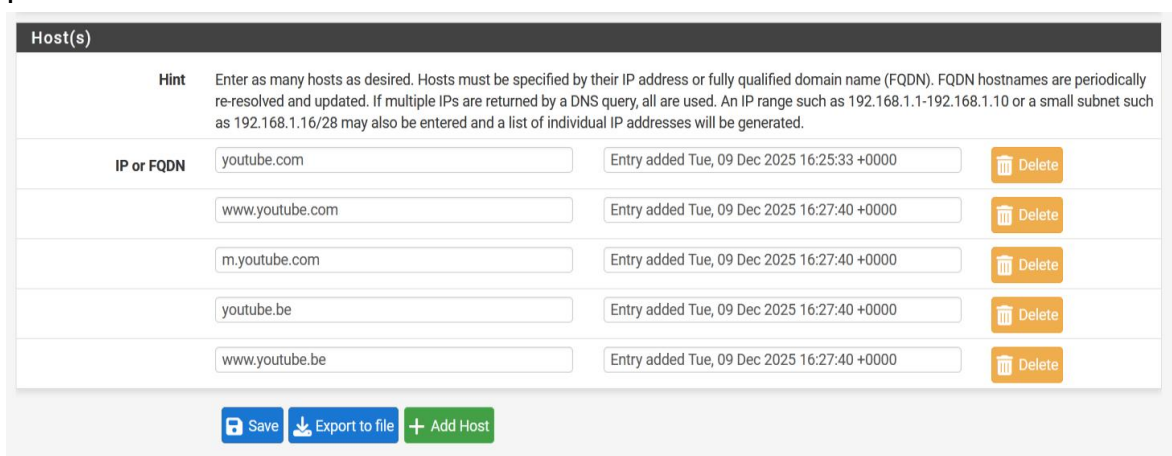
IP or FQDN www.facebook.com

Description

Save **+ Add Host**

Paso 3:

Procedemos a configurar de la siguiente manera. Debemos agregar todos los hostname debido a que youtube tiene varios y si no se agrega el bloqueo puede fallar.



Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

| IP or FQDN | Entry added | Delete |
|-----------------|---------------------------------|--------|
| youtube.com | Tue, 09 Dec 2025 16:25:33 +0000 | Delete |
| www.youtube.com | Tue, 09 Dec 2025 16:27:40 +0000 | Delete |
| m.youtube.com | Tue, 09 Dec 2025 16:27:40 +0000 | Delete |
| youtube.be | Tue, 09 Dec 2025 16:27:40 +0000 | Delete |
| www.youtube.be | Tue, 09 Dec 2025 16:27:40 +0000 | Delete |

Save **Export to file** **+ Add Host**

Paso 4:

Solo falta dar clic en save, el cual nos dirigirá al panel anterior, y daremos clic en el botón verde que dice “Apply Change”, para que aplique los cambios.

Firewall / Aliases / IP

The alias list has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes




IP

Ports

URLs

All

Firewall Aliases IP

| Name | Type | Values | Description | Actions |
|------------------|---------|---|---------------------------------------|---|
| dominioBloqueado | Host(s) | youtube.com, www.youtube.com, m.youtube.com, youtube.be, www.youtube.be | Restrinja el acceso a varios dominios |    |

+ Add

Import

Una vez dando clic en Apply Change se verá así:

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.




IP

Ports

URLs

All

Firewall Aliases IP

| Name | Type | Values | Description | Actions |
|------------------|---------|---|---------------------------------------|---|
| dominioBloqueado | Host(s) | youtube.com, www.youtube.com, m.youtube.com, youtube.be, www.youtube.be | Restrinja el acceso a varios dominios |    |

+ Add

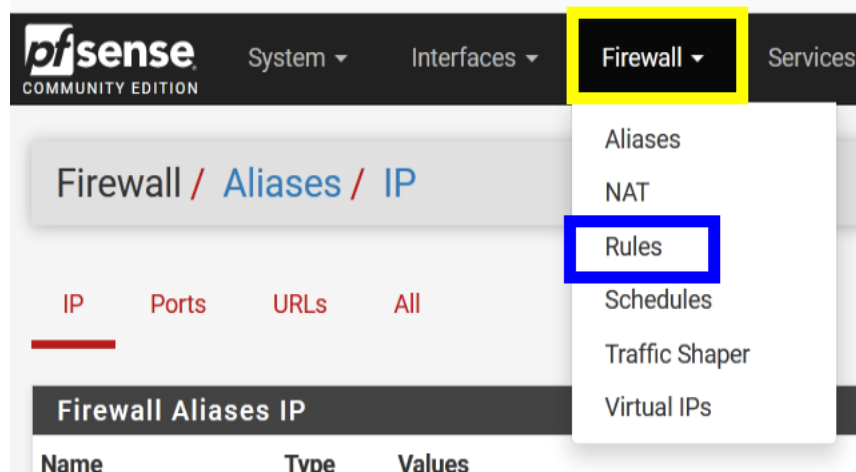
Import

Creamos la regla del firewall en la LAN.

Este paso es crítico para que Youtube quede bloqueado.

Para ello nos dirigiremos a:

Firewall → Rules → LAN



Veremos 3 reglas creadas automáticamente en este panel, estas son:

1. Anti-Lockout Rule:

Evita que nos bloqueemos a nosotros mismos del panel web. (No se toca).

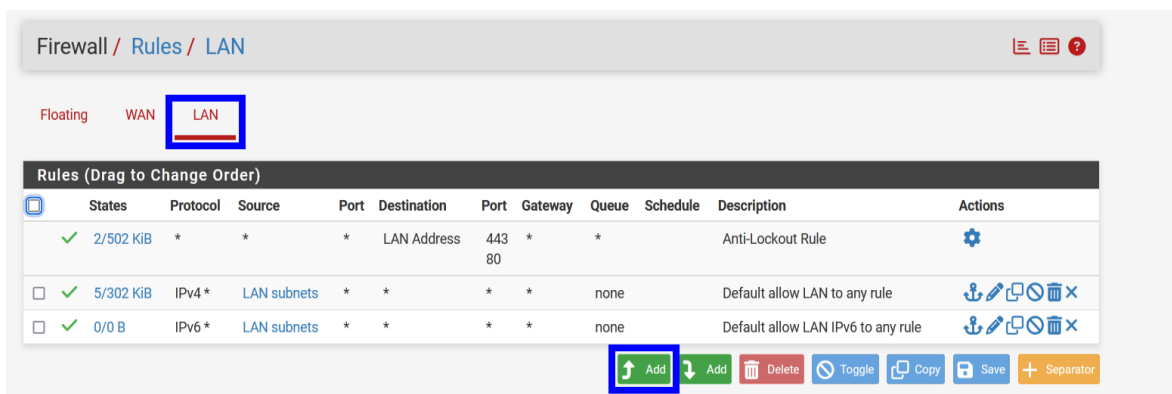
2. Default allow LAN to any rule (IPv4):

Permite que la LAN salga a internet. En este caso la regla de bloqueo de los sitios web debe colocarse **encima de esta**.

3. Default allow LAN IPv6:

Permite tráfico IPV6. Si no se está usando IPV6 no afecta.

Debemos estar en la parte de **LAN**, y luego dar clic en el botón con la flecha hacia arriba que dice “Add”.



Firewall / Rules / LAN

Floating WAN **LAN**

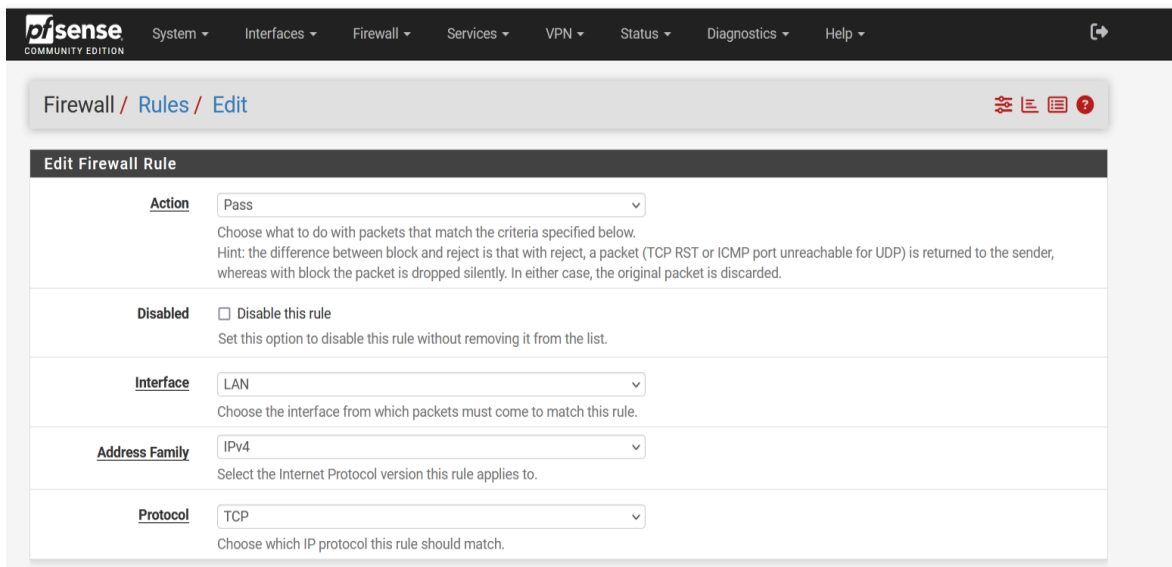
Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------------------------------|-----------|----------|-------------|------|-------------|--------|---------|-------|----------|------------------------------------|---------|
| <input checked="" type="checkbox"/> | 2/502 KiB | * | * | * | LAN Address | 443-80 | * | * | | Anti-Lockout Rule | |
| <input type="checkbox"/> | 5/302 KiB | IPv4 * | LAN subnets | * | * | * | * | none | | Default allow LAN to any rule | |
| <input type="checkbox"/> | 0/0 B | IPv6 * | LAN subnets | * | * | * | * | none | | Default allow LAN IPv6 to any rule | |

Add Add Delete Toggle Copy Save Separator

Al hacer eso, nos manda a un panel como el siguiente, el cual vamos a tener que configurar porque pfsense los coloca por defecto.

Configuración por defecto:



pfSense COMMUNITY EDITION

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

Firewall / Rules / Edit

Edit Firewall Rule

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

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

Interface LAN
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 TCP
Choose which IP protocol this rule should match.

Configuración correcta para bloquear sitios web:

- Action:


Cambiaremos de “Pass” a “Block”.

Action Block 

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

- Interface:


“LAN” (Ya está configurada como LAN).

Interface LAN 

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

- Address Family:


“IPv4” (Ya está configurada como IPV4).

Address Family IPv4 

Select the Internet Protocol version this rule applies to.

- Protocol:

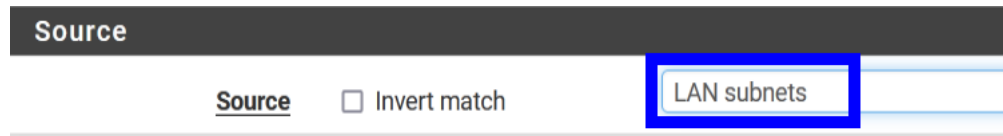
Cambiamos de “TCP” a “ANY”.

Protocol Any 

Choose which IP protocol this rule should match.

- Source:

Cambiaremos “ANY” a “LAN subnet. Para que aplique a toda la red LAN, todos los dispositivos dentro de esa red, todo el tráfico generado por ellos.



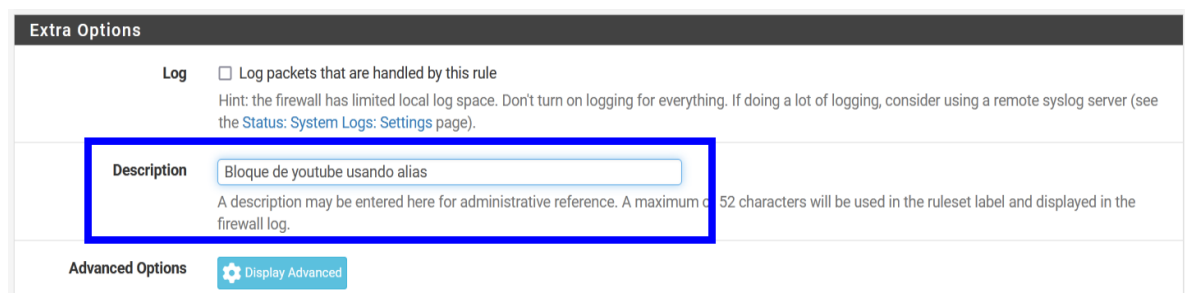
- Destination:

Cambiaremos “Any” a “Address or Alias”. Al seleccionar esta opción se desbloquea un cuadro a la derecha. En ese cuadro se escribe o selecciona: DominioBloqueado (Este es mi alias con todos los dominios de Youtube).



- Descripción:

Agregamos una descripción para saber qué hace esta regla.



- Guardamos los cambios.

Para ello debemos dar clic en el botón azul que dice “save”. Una vez hecho esto nos dirigirá nuevamente, donde están todas las reglas de LAN.

Extra Options

Log ☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

- Aplicamos los cambios.

Debemos dar clic en el botón verde que dice “Apply Changes”.

Firewall / [Rules](#) / [LAN](#)

The firewall rule configuration has been changed.
 The changes must be applied for them to take effect.

[Apply Changes](#)

Floating [WAN](#) [LAN](#)

Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------------------------|--------------|----------|-------------|------|------------------|--------|---------|-------|----------|------------------------------------|---|
| <input type="checkbox"/> | ✓ 1/546 KiB | * | * | * | LAN Address | 443 80 | * | * | | Anti-Lockout Rule | Settings |
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 * | LAN subnets | * | dominioBloqueado | * | * | none | | Bloque de youtube usando alias | Anchor Edit Copy Delete |
| <input type="checkbox"/> | ✓ 14/443 KiB | IPv4 * | LAN subnets | * | * | * | * | none | | Default allow LAN to any rule | Anchor Edit Copy Delete X |
| <input type="checkbox"/> | ✓ 0/0 B | IPv6 * | LAN subnets | * | * | * | * | none | | Default allow LAN IPv6 to any rule | Anchor Edit Copy Delete X |

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

Al aplicar los cambios, quedará de la siguiente manera:

1. Anti-Lockout Rule.
2. Nuestra regla de bloqueo (Bloqueo de youtube usando alias).
3. Default allow LAN to any rule.

The screenshot shows the pfSense Firewall Rules configuration page for the LAN interface. A green notification bar at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, the "Rules (Drag to Change Order)" table is displayed. The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The rules listed are:

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------|----------|-------------|------|------------------|--------|---------|-------|----------|------------------------------------|--------------|
| ✓ 2/561 KIB | * | * | * | LAN Address | 443 80 | * | * | | Anti-Lockout Rule | ⚙️ |
| ✗ 0/0 B | IPv4 * | LAN subnets | * | dominioBloqueado | * | * | none | | Bloque de youtube usando alias | 🔗 🖋️ 🔄 🗑️ |
| ✓ 3/446 KIB | IPv4 * | LAN subnets | * | * | * | * | none | | Default allow LAN to any rule | 🔗 🖋️ 🔄 🗑️ ✖️ |
| ✓ 0/0 B | IPv6 * | LAN subnets | * | * | * | * | none | | Default allow LAN IPv6 to any rule | 🔗 🖋️ 🔄 🗑️ ✖️ |

At the bottom of the table are buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

Esto indica que la regla quedo bien configurada y el hecho que aparezca una “x” en color rojo, no es un error, esto nos está indicando que **aún no ha pasado ningún paquete que haga match con esa regla.**

Verificando que el sitio está bloqueado.

The screenshot shows a web browser window with the address bar displaying "https://youtube.com". The page title is "Problemas al cargar la página". The browser is displaying a connection error message.

La conexión ha caducado

Un error ocurrió durante una conexión a youtube.com.

- El sitio podría estar temporalmente fuera de servicio o muy ocupado. Intenta nuevamente en un momento.
- Si no puedes cargar ninguna página, verifica la conexión de red de tu computadora.
- Si la red o tu computadora están protegidas por un firewall o proxy, asegúrate que Firefox pueda acceder a internet.

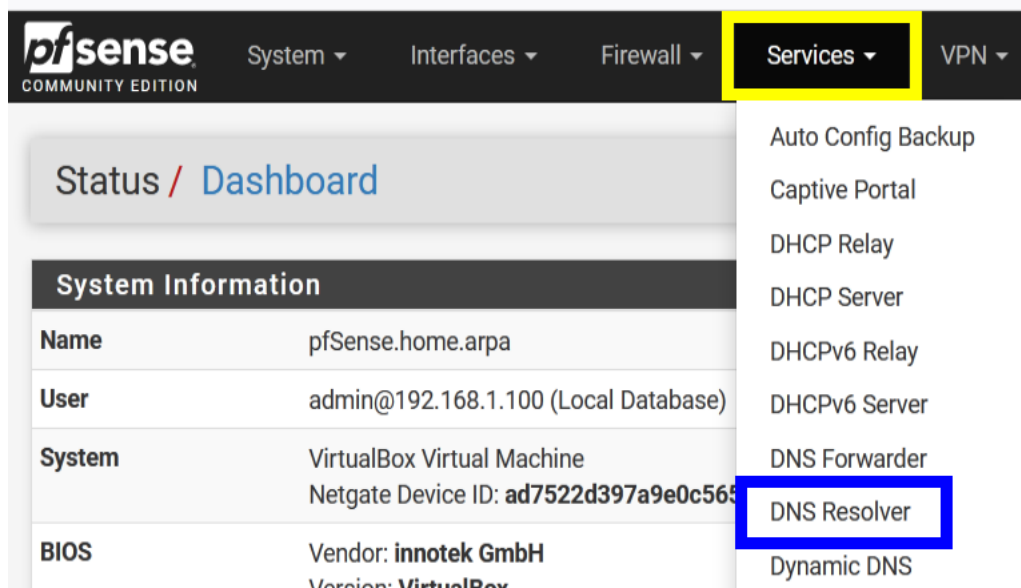
Intentar de nuevo

APLICANDO HERRAMIENTAS DE AYUDA A BLOQUEO.

Paso 1:

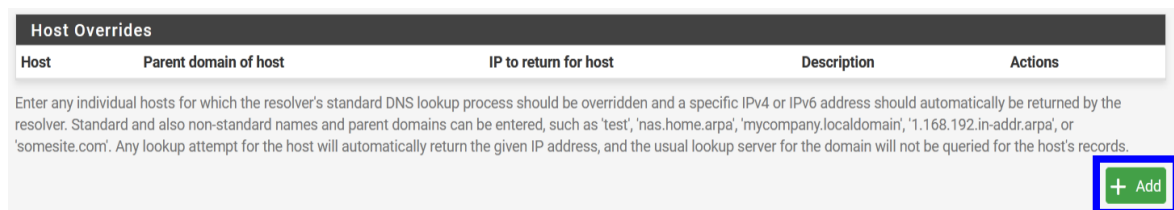
En pfsense entramos a:

Service → DNS Resolver.



Paso 2:

Una vez estemos en este panel, debemos bajar hasta la sección que dice: **Host Overrides**. En este apartado, debemos dar clic en el botón “Add”.



Paso 3:

Completaremos los campos de acuerdo a la red que queremos bloquear, en este caso bloquearemos x.com. Damos clic en el botón azul “Save”.

| Host Override Options | |
|-----------------------|--|
| Host | <input type="text" value="x"/> Nombre de la red social o web a bloquear por DNS |
| Domain | <input type="text" value="com"/> Esta parte es la finalización de la red, pero no debemos poner "." ya que pfsense lo completa por sí mismo |
| IP Address | <input type="text" value="127.0.0.1"/> Dirección recomendada porque no lleva a ningún sitio ya que es la ip local |
| Description | <input type="text" value="Bloqueo de x.com mediante DNS"/> Texto descriptivo de lo que hace este tipo de bloqueo |

A description may be entered here for administrative purposes.

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., 'somesite.google.com' is entered as host='somesite' and parent domain='google.com'). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable names such as 'www' or 'google.co.uk'.

Por último, nos sacará de ese panel y nos mostrará un mensaje al cual debemos dar clic en “Apply Changes”.

pfSense COMMUNITY EDITION

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

Services / DNS Resolver / General Settings

The DNS resolver configuration has been changed.
The changes must be applied for them to take effect.

☒ Apply Changes

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.































Nos saldrá un mensaje que dice: cambios aplicados con éxito.

Services / DNS Resolver / General Settings

The changes have been applied successfully.

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

Quedando de la siguiente manera:

| Host Overrides | | | | |
|----------------|-----------------------|-----------------------|--------------------------------------|---|
| Host | Parent domain of host | IP to return for host | Description | Actions |
| | youtu.be | 127.0.0.1 | Variante de youtube a bloquear |   |
| | yting.com | 127.0.0.1 | Variante de youtube a bloquear |   |
| | googlevideo.com | 127.0.0.1 | Variante de youtube a bloquear |   |
| facebook | com | 127.0.0.1 | Bloqueo de facebook.com mediante DNS |   |
| i | yting.com | 127.0.0.1 | Variante de youtube a bloquear |   |
| m | youtube.com | 127.0.0.1 | Variante de youtube a bloquear |   |
| redirector | googlevideo.com | 127.0.0.1 | Variante de youtube a bloquear |   |
| s | youtube.com | 127.0.0.1 | Variante de youtube a bloquear |   |
| www | youtube.com | 127.0.0.1 | Variante de youtube a bloquear |   |
| www | youtu.be | 127.0.0.1 | Variante de youtube a bloquear |   |
| www | youtube.be | 127.0.0.1 | Variante de youtube a bloquear |   |
| x | com | 127.0.0.1 | Bloqueo de x.com mediante DNS |   |
| youtube | com | 127.0.0.1 | Bloqueo de youtube mediante DNS |   |
| youtube | be | 127.0.0.1 | Variante de youtube a bloquear |   |
| youtubei | googleapis.com | 127.0.0.1 | Variante de youtube a bloquear |   |

