

# GUÍA COMPLETA PFSENSE

## Introducción

PfSense es un firewall, basado en software libre, que tiene una gran cantidad de usuarios por todo el mundo. Utilizado como firewall en pequeñas y medianas empresas. Protegerá tus equipos de las amenazas y ataques cibernéticos. En este artículo te mostramos sus características técnicas y algunas funcionalidades que tiene este potente software.

## ¿Qué es un firewall o cortafuegos?

Un firewall es una herramienta de seguridad informática diseñada para proteger una red de computadoras al monitorear y controlar el tráfico de datos que entra y sale de la red. Funciona estableciendo reglas y filtros que determinan qué tipo de comunicación se permite y cuál se bloquea, con el objetivo de prevenir accesos no autorizados, ataques maliciosos o la propagación de malware. Los firewalls pueden operar a nivel de hardware o software y se utilizan comúnmente en entornos empresariales y domésticos para salvaguardar la integridad y la confidencialidad de la información almacenada en los sistemas conectados a la red. Además de actuar como una barrera defensiva, los firewalls también pueden generar registros detallados de actividad que ayudan a los administradores de red a supervisar posibles amenazas y mejorar continuamente la seguridad.

## ¿Qué es PFSENSE?

PfSense es un sistema operativo especializado de software libre, diseñado para montar servicios de cortafuegos y seguridad del más alto nivel para tu empresa basado en FreeBSD. Su portal de administración está basado en lenguaje PHP y en las últimas versiones cuenta con una interfaz amigable hecha en bootstrap, desde este mismo panel se puede acceder a todas las configuraciones administrativas del sistema, con lo que le facilita a tu empresa la administración de todos los permisos.

## ¿Porque PFSENSE es un firewall tan popular?

### Facilidad de uso

Lo que vuelve tan popular esta herramienta de seguridad empresarial es su facilidad de uso y configuración, destacando el hecho de que no es imprescindible los conocimientos avanzados en línea de comandos UNIX, para su manejo.

## Es software libre

Esta grandiosa herramienta es desarrollada en software libre, por lo que cuenta con una gran comunidad y actualizaciones frecuentes de seguridad, lo que pone a tu negocio en buenas manos.

## Mayor rendimiento de hardware

En sus últimas versiones se destacó por mucho sobre otros softwares en rendimiento del hardware, permitiéndole posicionarse como uno de los servicios de firewall más seguros y de mayor velocidad de procesamiento en el mercado.

## Funciones de reporte y monitoreo

Brinda reportes y es monitoreable en tiempo real, lo cual es una gran ventaja a la hora de tener control sobre los accesos a nuestra Red Privada, también a la hora de implementar cambios en las políticas de accesos y demás.

Todo esto vuelve al **pfSense** una de las herramientas **más recomendadas** por las grandes empresas para administrar la seguridad de sus sitios, además de ofrecerte una plusvalía sobre los demás Servicios **Firewall** en el mercado.

## Índice rápido

Como abrir y cerrar puertos en Pfsense, [click aquí](#)



Como Bloquear una dirección IP en Pfsense, [click aquí](#)

Como crear y eliminar un usuario de conexión VPN en Pfsense, [click aquí](#)



Como instalar la configuración VPN de Pfsense en Windows, [click aquí](#)



Como usar PfSense para configurar un servidor de DNS y DHCP, [click aquí](#)

Como reservar la dirección IP de un usuario específico con DHCP, [click aquí](#)



Como bloquear un sitio web con DNS resolver en Pfsense, [click aquí](#)

Como realizar un NAT en Pfsense, [click aquí](#)



Como Agregar una página en la lista blanca de PFBLOCKER, [click aquí](#)



Como gestionar el ancho de banda en Pfsense, [click aquí](#)

Como verificar el consumo de ancho de banda en Pfsense, [click aquí](#)

Uso de NTOPNG para monitorear el Tráfico en tiempo real, [click aquí](#)

Como redireccionar el tráfico entre diferentes proveedores de internet ISP, [click aquí](#)

Como cambiar de proveedor de internet ISP en Pfsense, [click aquí](#)

# Como abrir y cerrar puertos en el Pfsense

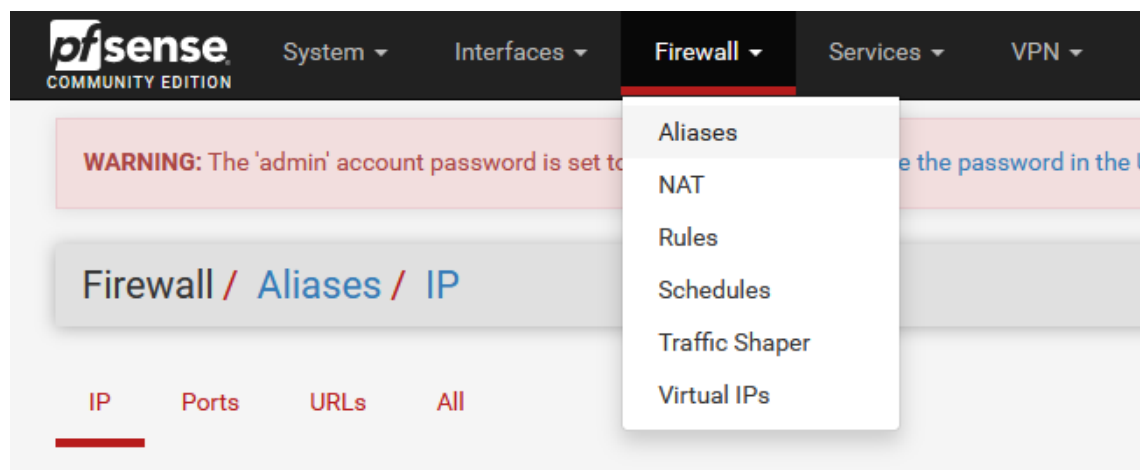
Si quieres mejorar la seguridad de red de tu Firewall, Pfsense cuentan una herramienta que se llama Reglas, que te permite habilitar solo los puertos que usas y bloquear los puertos que no necesitas:

## Habilitar puertos en Pfsense

Para realizar la actividad debes tener en cuentas que puertos se van a habilitar, más adelante si vas a requerir habilitar nuevos puertos se puede agregar en el Alias.

### Paso 1:

En el panel de Pfsense nos vamos al menú Firewall y escogemos la opción Aliases.



### Paso 2:

En menú de alias nos vamos a la pestaña de Puertos y para crear uno nuevo seleccionamos en el botón de Agregar.



### Paso 3:

Ahora le ponemos un nombre y una descripción, en tipo los dejamos por defecto en Puertos, mas abajo podemos agregar los numero de puertos, si quieres poner mas, seleccionas la opción de Agregar puerto, por ultimo seleccionamos en Guardar.

Firewall / Aliases / Edit

Properties

Name

OTROS\_PUERTOS

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

Description

OTROS\_PUERTOS

A description may be entered here for administrative reference (not parsed).

Type

Port(s)

Port(s)

Hint

Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port

10000

Description

Delete

8080

Description

Delete

Save

+ Add Port

**Paso 4:**

Una vez creado el Alias seleccionamos en el botón Aplicar cambios para que se aplique en el pfsense.

Firewall / Aliases / Ports

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

Apply Changes










IP

Ports

URLs

All

Firewall Aliases Ports

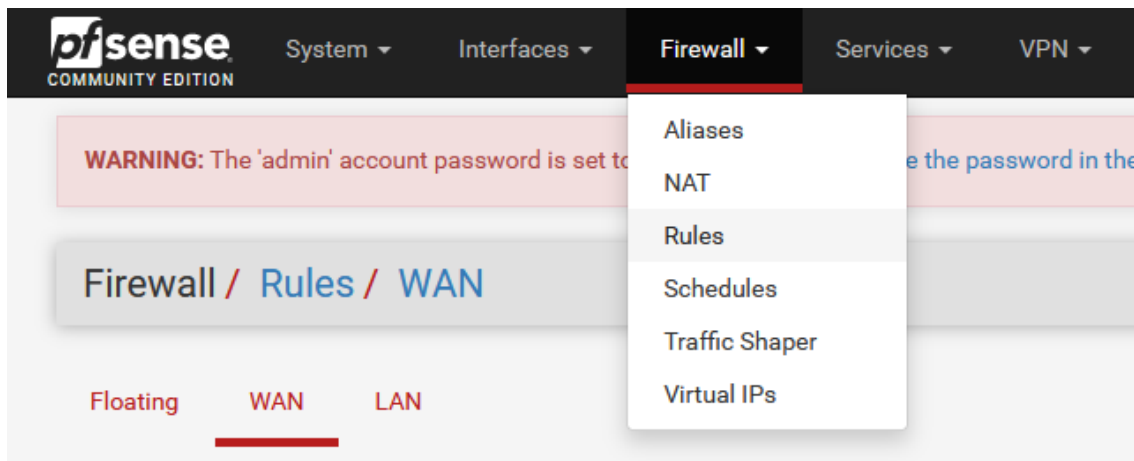
Name	Values	Description	Actions
OTROS_PUERTOS	10000, 8080	OTROS_PUERTOS	  
PUERTOS_MAIL	993, 465, 587, 443, 995, 143	PUERTOS_MAIL	  
PUERTOS_WEB	443, 80	PUERTOS_WEB	  

+ Add

Import

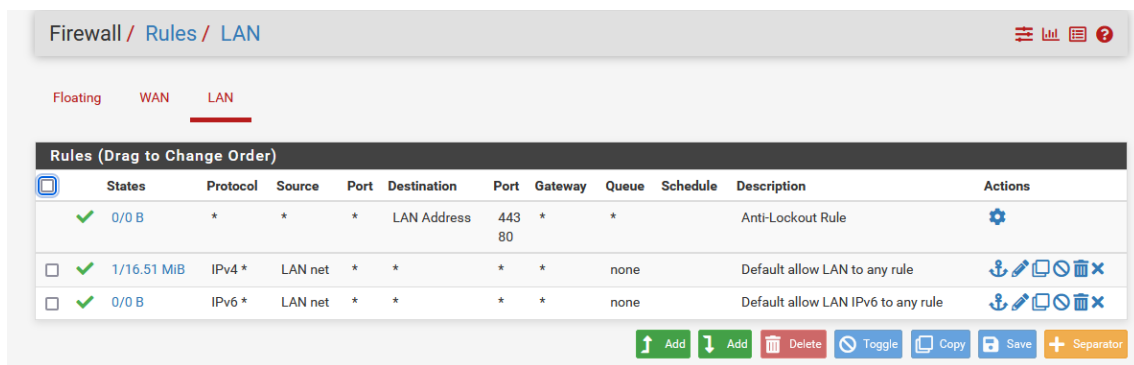
**Paso 5:**

Una vez creado el Alias, ahora nos toca crear la Regla para eso en pfsense nos vamos al menú firewall y seleccionamos la opción de Reglas.



### Paso 6:

Luego nos ubicamos en la pestaña de LAN y para crear la regla seleccionamos el botón de Agregar.



### Paso 7:

Ahora Definamos el tipo de regla, en acción escogemos la opción de Pass ya que vamos a permitir el acceso, la interface por defecto es LAN, y en protocolo TCP/UDP.

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/UDP

Choose which IP protocol this rule should match.

Paso 8:

En Source los dejamos por defecto los ajustes, en Destino ponemos en Any, en rango de puerto, escogemos para ambos casos en otros y agregamos el Alias que hemos creado anteriormente, en opciones extras habilitamos el log para poder hacerle seguimiento, por último, seleccionamos en Guardar.

Source

Source

☐ Invert match

any

Source Address

/

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

any

Destination Address

/

Destination Port Range

(other)

OTROS\_PUERTOS

(other)

OTROS\_PUERTOS

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).

Description

ACCESO A OTROS PUERTOS

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

Paso 9:

Una vez creada la regla nos va a pedir aplicar los cambios para que se guarde en el Pfsense.

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 checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	2/16.53 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	*	OTROS_PUERTOS	*	none		ACCESO A OTROS PUERTOS	

↑ Add

↓ Add

Delete

Toggle

Copy

Save

Separator

Bloquear puertos en Pfsense

Realizar el bloqueo de algunos puertos en Pfsense es caso similar a la apertura de puerto, se va a crear una regla bloqueo con un Alias.

Paso 1:



Primero creamos un alias para el bloqueo de puertos y en el mismo agregamos los puertos a bloquear.













Firewall / Aliases / Ports



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

Apply Changes

IP Ports URLs All

Firewall Aliases Ports

Name	Values	Description	Actions
BLOQUEO_PUERTOS	25, 22	BLOQUEO_PUERTOS	  
OTROS_PUERTOS	10000, 8080	OTROS_PUERTOS	  
PUERTOS_MAIL	993, 465, 587, 443, 995, 143	PUERTOS_MAIL	  
PUERTOS_WEB	443, 80	PUERTOS_WEB	  

 Add  Import






















Paso 2:








Podemos crear una nueva regla, o duplicar una regla existente, seleccionar el icono de Copiar.

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	 0/953 KIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	 0/0 B	IPv4 TCP/UDP	*	*	*	OTROS_PUERTOS	*	none		ACCESO A OTROS PUERTOS	    
<input type="checkbox"/>	 0/1.16 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	    
<input type="checkbox"/>	 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	    

 Add  Add  Delete  Toggle  Copy  Save  Separator

Paso 3:

Como es una regla de bloqueo, en el campo de acción seleccionamos la opción de Block, la interfaz LAN y el protocolo TCP/UDP.

Edit Firewall Rule

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.

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/UDP

Choose which IP protocol this rule should match.

Paso 4:

En Source dejamos por defecto y en Destino seleccionamos en Otros para ambos casos y agregamos también el alias que se creo anteriormente, por ultimo seleccionamos en guardar.

Source

Source

☐ Invert match

any

Source Address

/

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

any

Destination Address

/

Destination Port Range

(other)

BLOQUEO\_PUERTOS

(other)

BLOQUEO\_PUERTOS

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).

Description

REGLA BLOQUEO DE PUERTOS

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

Advanced Options

Display Advanced

Paso 5:

La regla de Bloqueo aparece con icono de X ya que es una restricción, aplicamos los cambios para que se guarde en el Pfsense.

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)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/953 KIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	*	BLOQUEO_PUERTOS	*	none		REGLA BLOQUEO DE PUERTOS	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	*	OTROS_PUERTOS	*	none		ACCESO A OTROS PUERTOS	
<input type="checkbox"/>	0/1.16 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

# Como Bloquear una dirección IP en el Pfsense

Si quieres bloquear algunas IP especificas en tu red, la herramienta pfsense te permite realizar el boqueo de 1 o varias IP a través de una regla.

## Paso 1:

Primero creamos el alias y dentro del mismo agregamos las direcciones IP que se quiere bloquear, en este caso el campo Tipo escogemos la opción de Hosts.

Firewall / Aliases / Edit

**Properties**

**Name** BLOQUEO\_IPS  
The name of the alias may only consist of the characters 'a-z, A-Z, 0-9 and \_'.

**Description** BLOQUEO\_IPS  
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	Description	
190.12.64.180		Delete
100.50.10.8		Delete

Save + Add Host

## Paso 2:

Una vez creado el alias aplicamos el cambio para que se guarde en el pfsense.

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	Values	Description	Actions
BLOQUEO_IPS	190.12.64.180, 100.50.10.8	BLOQUEO_IPS	

+ Add Import

## Paso 3:

Ahora creamos la Regla para el bloqueo, en el campo Action podemos poner Reject o Block, la interface es LAN y el protocolo es TCP.

Edit Firewall Rule	
<b>Action</b>	<div>Reject</div> <div>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.</div>
<b>Disabled</b>	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
<b>Interface</b>	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
<b>Address Family</b>	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
<b>Protocol</b>	<div>TCP</div> <div>Choose which IP protocol this rule should match.</div>

#### Paso 4:


En source ponemos que viene desde la LAN, en destino agregamos el Alias creado y el puerto ponemos en any para que bloquee los puertos de esas IP.

Source	
<b>Source</b>	<div><input type="checkbox"/> Invert match</div> <div>LAN net</div> <div>Source Address</div>
<div>Display Advanced</div> <div>The <b>Source Port Range</b> 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.</div>	
Destination	
<b>Destination</b>	<div><input type="checkbox"/> Invert match</div> <div>Single host or alias</div> <div>BLOQUEO_IPS</div>
<b>Destination Port Range</b>	<div>any</div> <div>From</div> <div>Custom</div> <div>any</div> <div>To</div> <div>Custom</div> <div>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</div>
Extra Options	
<b>Log</b>	<div><input checked="" type="checkbox"/> Log packets that are handled by this rule</div> <div>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 <a href="#">Status: System Logs: Settings</a> page).</div>
<b>Description</b>	<div>BLOQUEO IPS</div> <div>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.</div>
<b>Advanced Options</b>	<div>Display Advanced</div>

#### Paso 5:

























Una vez creada la regla, nos va a aparecer con un icono de una mano, aplicamos los cambios para que se guarde en el pfSense

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)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	 0/953 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	 0/0 B	IPv4 TCP	LAN net	*	BLOQUEO_IPS	*	*	none		BLOQUEO IPS	   
<input type="checkbox"/>	 0/0 B	IPv4 TCP/UDP	*	*	*	OTROS_PUERTOS	*	none		ACCESO A OTROS PUERTOS	    
<input type="checkbox"/>	 0/0 B	IPv4 TCP/UDP	*	*	*	BLOQUEO_PUERTOS	*	none		REGLA BLOQUEO DE PUERTOS	   
<input type="checkbox"/>	 0/1.16 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	    

# Como crear y eliminar un usuario de conexión VPN en el Pfsense

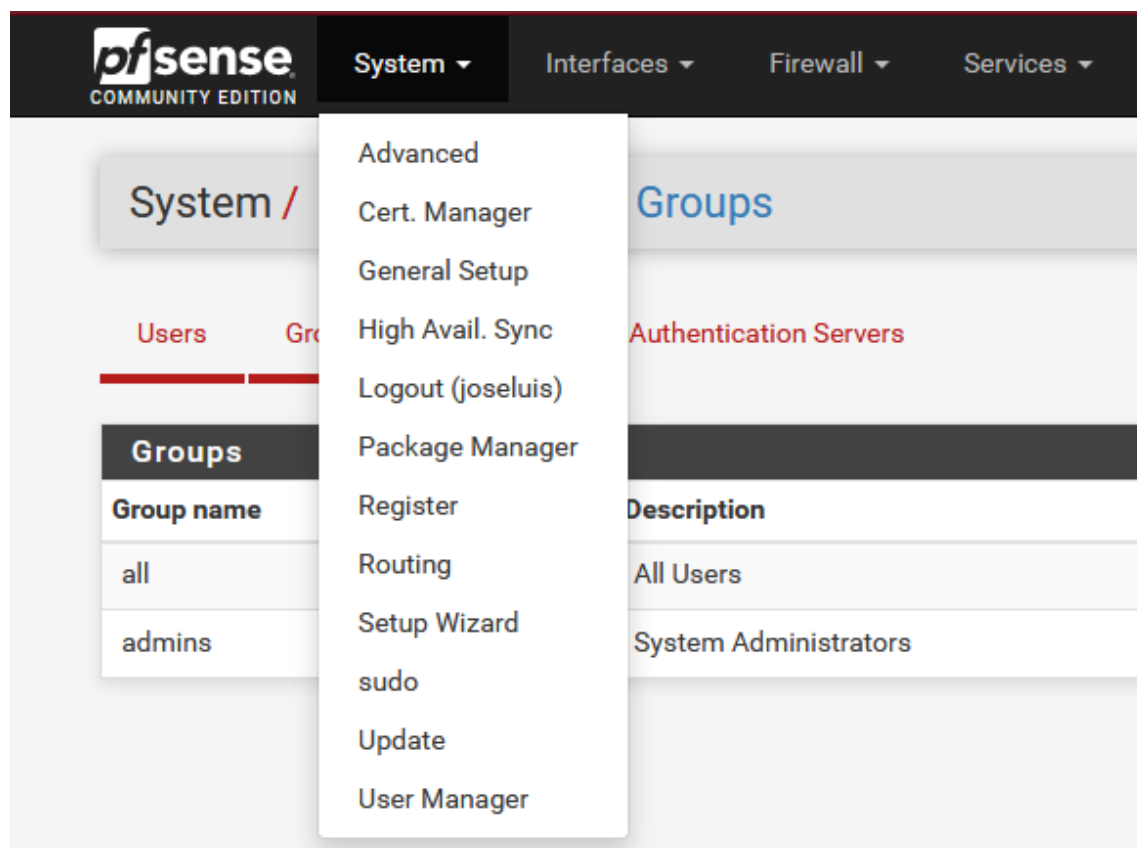
Si estas usando una conexión VPN en tu equipo Pfsense para tus usuarios. Te vamos a enseñar como crear nuevos accesos VPN como también desactivarlo o eliminar el acceso.

## Como crear un usuario de conexión VPN

Antes de realizar la creación del VPN, ya debes tener configurado el servicio VPN en tu Pfsense y haber realizado la configuración de conexión al servidor.

### Paso 1:

En el Pfsense nos vamos al Menu Sistema, escogemos la opción de User Manager, luego nos vamos a la pestaña de Users y seleccionamos el botón de agregar.



### Paso 2:

Al crear el nuevo acceso le asignamos un nombre de usuario y una contraseña, también le ponemos una descripción o un nombre de acceso, hacer click en la opción de Certifícate para que te genere el instalador.

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="demo"/>
Password	<input type="password" value="....."/> <input type="password" value="....."/>
Full name	<input type="text" value="Demo Nettix"/> <small>User's full name, for administrative information only</small>
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<div> <input type="text" value="admins"/> </div> <div> <input type="text"/> </div> <div> <small>Not member of</small> </div> <div> <small>Member of</small> </div> <div> <a href="#">» Move to "Member of" list</a> </div> <div> <a href="#">« Move to "Not member of" list</a> </div> <div> <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small> </div>
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate

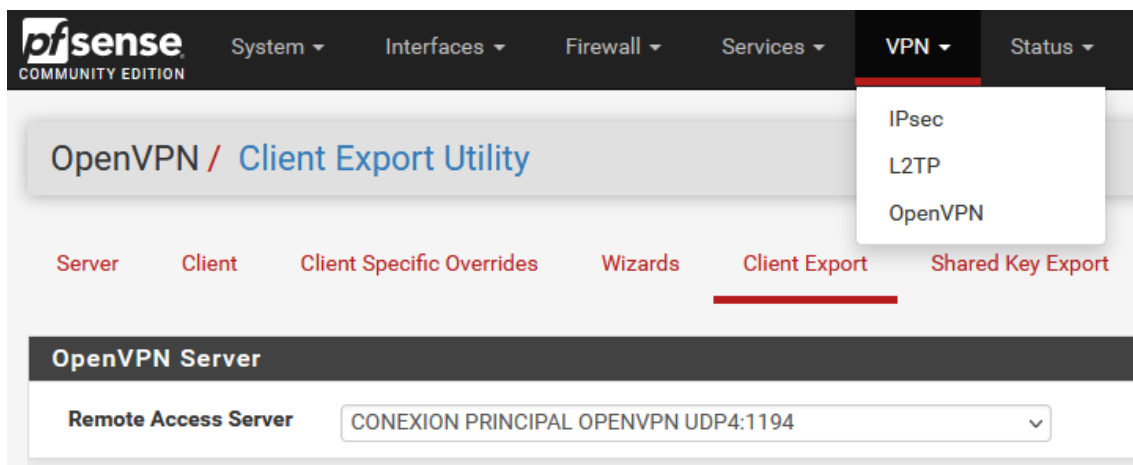
### Paso 3:

Al habilitar el Certificado, nos va a aparecer mas opciones, le ponemos el mismo nombre del usuario, en la opción de certificado si manejas varias conexión VPN debes seleccionar uno en específico, luego selección el botón guardar para que se cree el acceso.

Create Certificate for User	
Descriptive name	<input type="text" value="demo"/>
Certificate authority	<input type="text" value="CA_CONEXION_OPENVPN"/>
Key type	<input type="text" value="RSA"/>
	<input type="text" value="2048"/> <small>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</small>
Digest Algorithm	<input type="text" value="sha256"/> <small>The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid</small>
Lifetime	<input type="text" value="3650"/>
Keys	
Authorized SSH Keys	<div><input type="text"/></div> <div><small>Enter authorized SSH keys for this user</small></div>

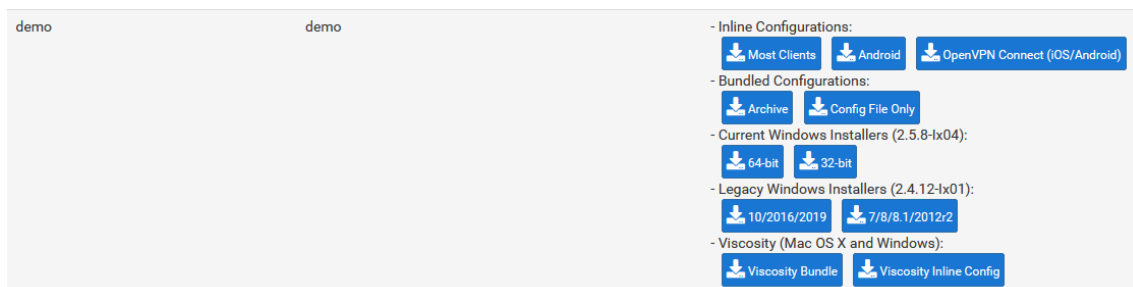
### Paso 4:

Ahora para descargar el instalador del VPN nos vamos al menú VPN y seleccionar la opción de OpenVPN.



### Paso 5:

Ahora buscamos el nombre del usuario que hemos creado y descargamos el instalador en este caso el Windows de 64 bits.



## Como Eliminar o desactivar un usuario de conexión VPN

Si quieres eliminar o desactivar una conexión VPN de un usuario, la herramienta pfsense te permite aplicar este cambio desde su panel User manager.

### Paso 1:

Si solo quieres desactivar de forma temporal el acceso VPN de un usuario, primero seleccionas el usuario a Editar y activas en el Campo de Disabled, al realizar este cambio el Pfsense va a rechazar el acceso VPN del usuario configurado en su Equipo.



**User Properties**

Defined by

USER

Disabled

☒ This user cannot login

Username

demo

Password

Password

Confirm Password

Full name

Demo Nettix

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings

☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

admins

Not member of

Member of

>> Move to "Member of" list

<< Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

## Paso 2:

Si quieres Eliminar el acceso VPN de un usuario, al Editar el mismo primero debes eliminar el Certificado para que se elimine el instalador, luego guardas los cambios.

**Effective Privileges**

Inherited from	Name	Description	Action
			<div>+ Add</div>

**User Certificates**

Name	CA	
demo	CA_CONEXION_OPENVPN	<div></div>
		<div>+ Add</div>

**Keys**

Authorized SSH Keys

Enter authorized SSH keys for this user

## Paso 3:

Luego en el panel de Users seleccionas el usuario y haces click en el icono de Eliminar, al aplicar este cambio se va a borrar toda la configuración VPN del usuario.

Users

Groups

Settings

Authentication Servers

Users

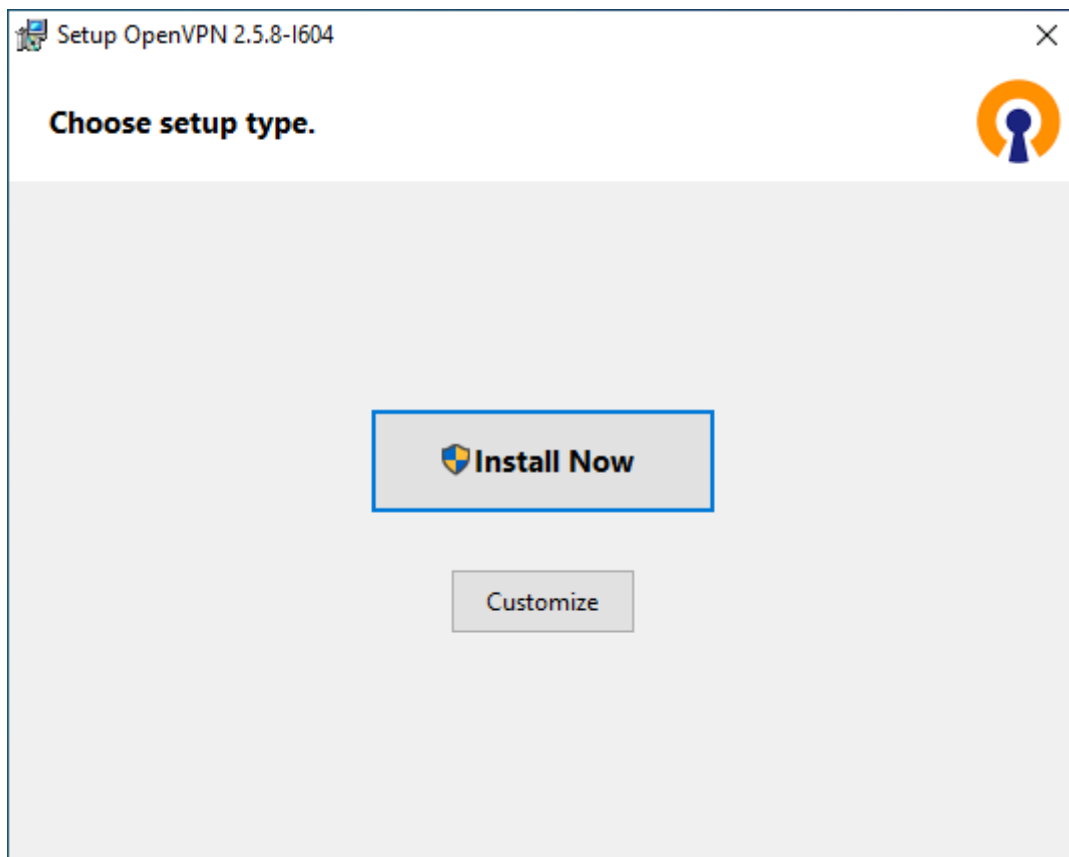
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator		admins	
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input checked="" type="checkbox"/>	demo	Demo Nettix			

# Como instalar la configuración VPN de Pfsense en Windows

Una vez creado el Acceso VPN en el Pfsense ahora toca instalar el cliente vpn en el equipo del Usuario, para eso debes tener el usuario y contraseña de la conexión VPN y el instalador generado.

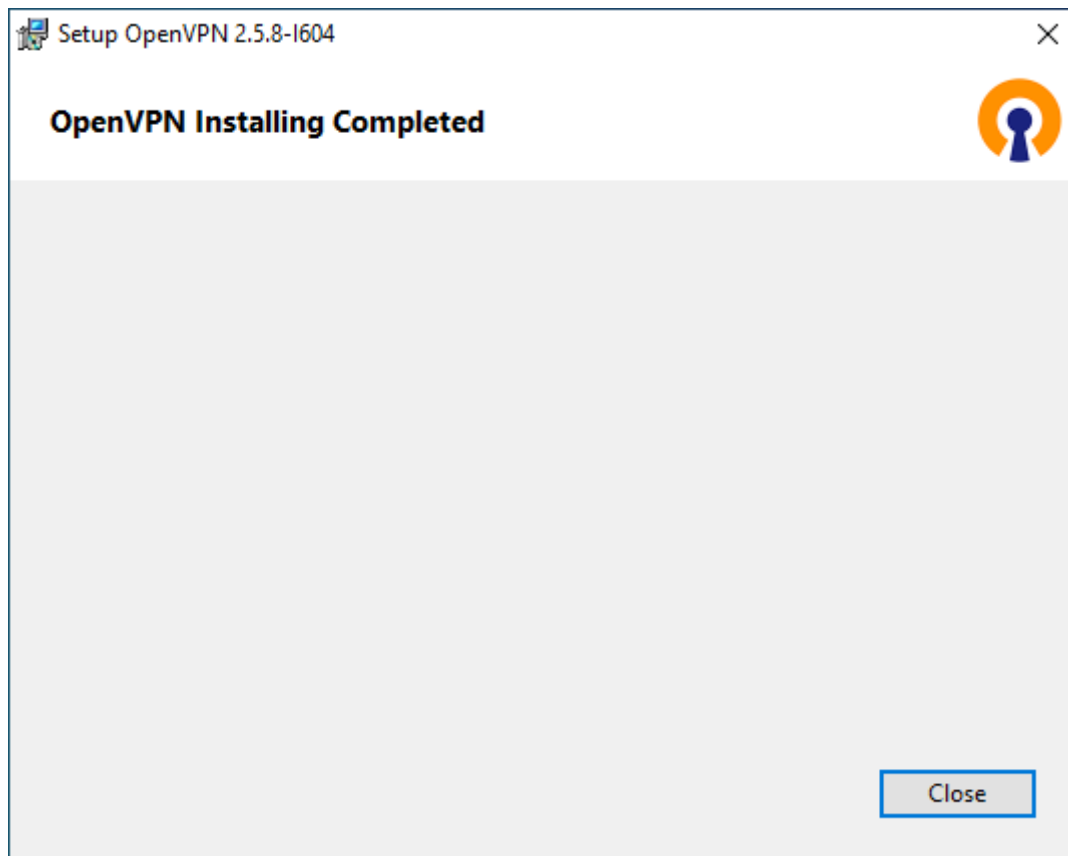
## Paso 1:

Lo primero a realizar es ejecutar el instalar el Windows, ahora va a iniciar el asistente de instalación Openvpn, ahora seleccionas el botón de Instalar ahora.



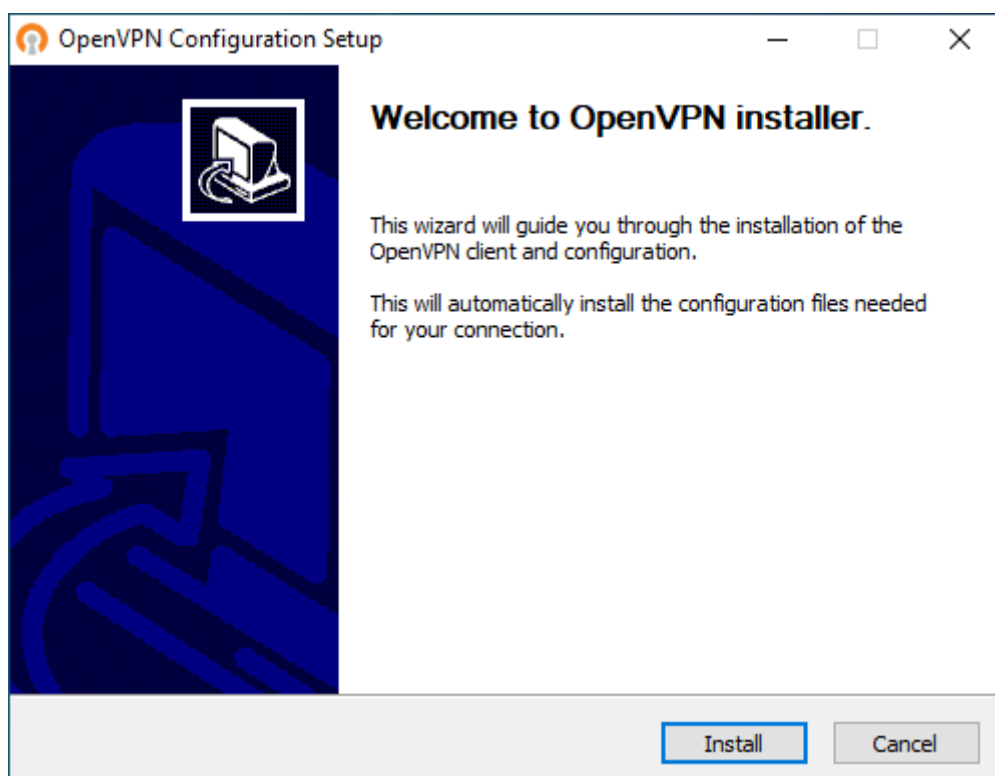
## Paso 2:

Va a comenzar con el proceso de instalación, una vez finalizado te va a aparecer el mensaje de instalación finalizada, seleccionamos en el botón de cerrar.



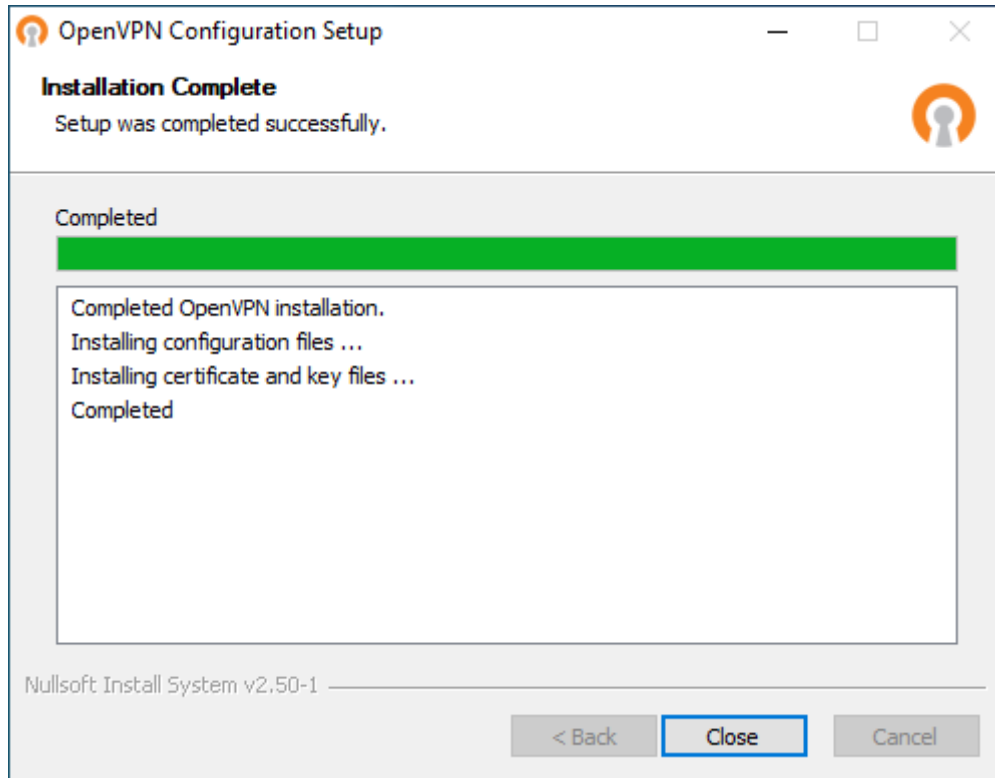
### Paso 3:

Ahora te va a mostrar un asistente para instalar los archivos de configuración, el cual seleccionamos el botón de instalar.



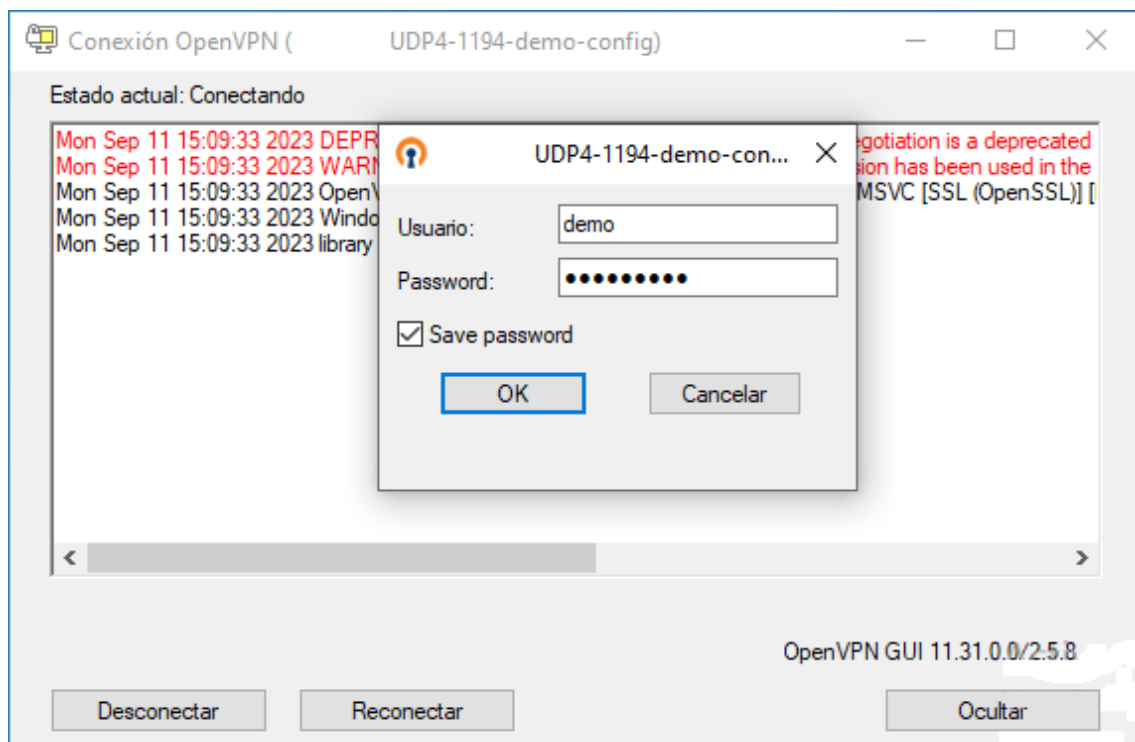
#### Paso 4:

Esperamos unos minutos que instale los archivos hasta que aparezca el mensaje de Completed, ahora seleccionamos en el botón de cerrar.



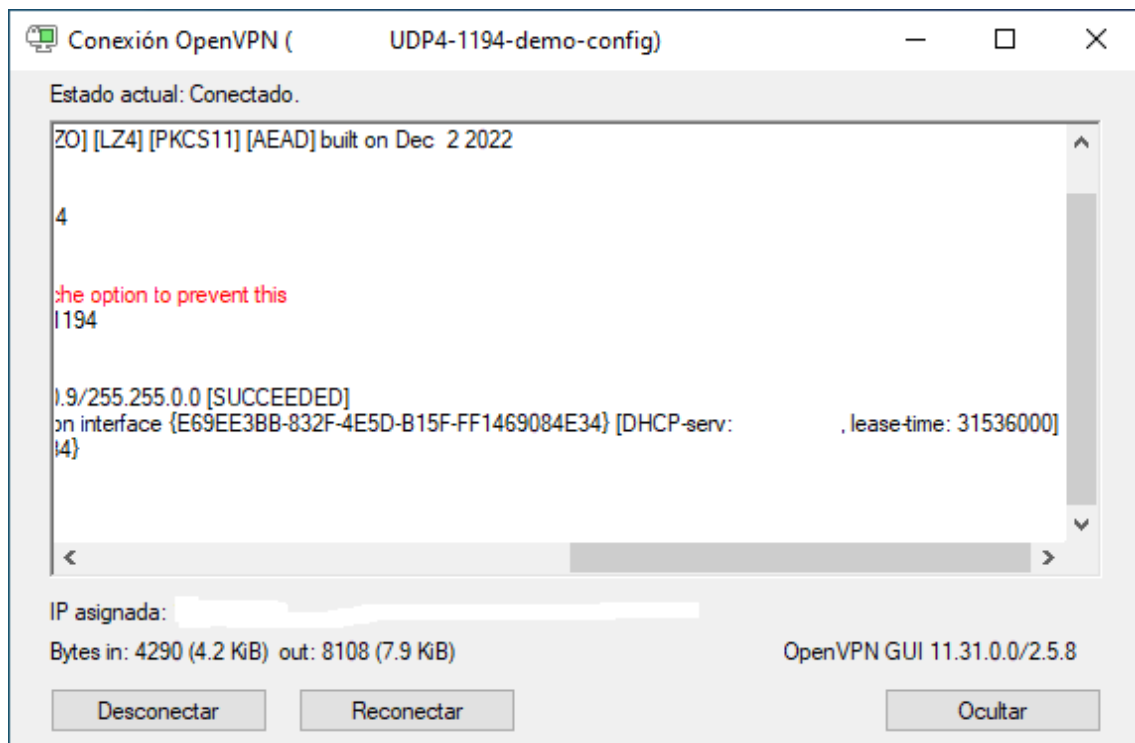
#### Paso 5:

Al iniciar la VPN nos va a pedir las credenciales de acceso (Usuario y Contraseña) luego seleccionamos en el botón de OK para que inicie la conexión.



#### Paso 6:

Si has realizado los pasos correctamente al ver el estado del VPN nos va a aparecer con Estatus Conectado y ahora vamos a poder acceder a nuestro servidor de forma segura.



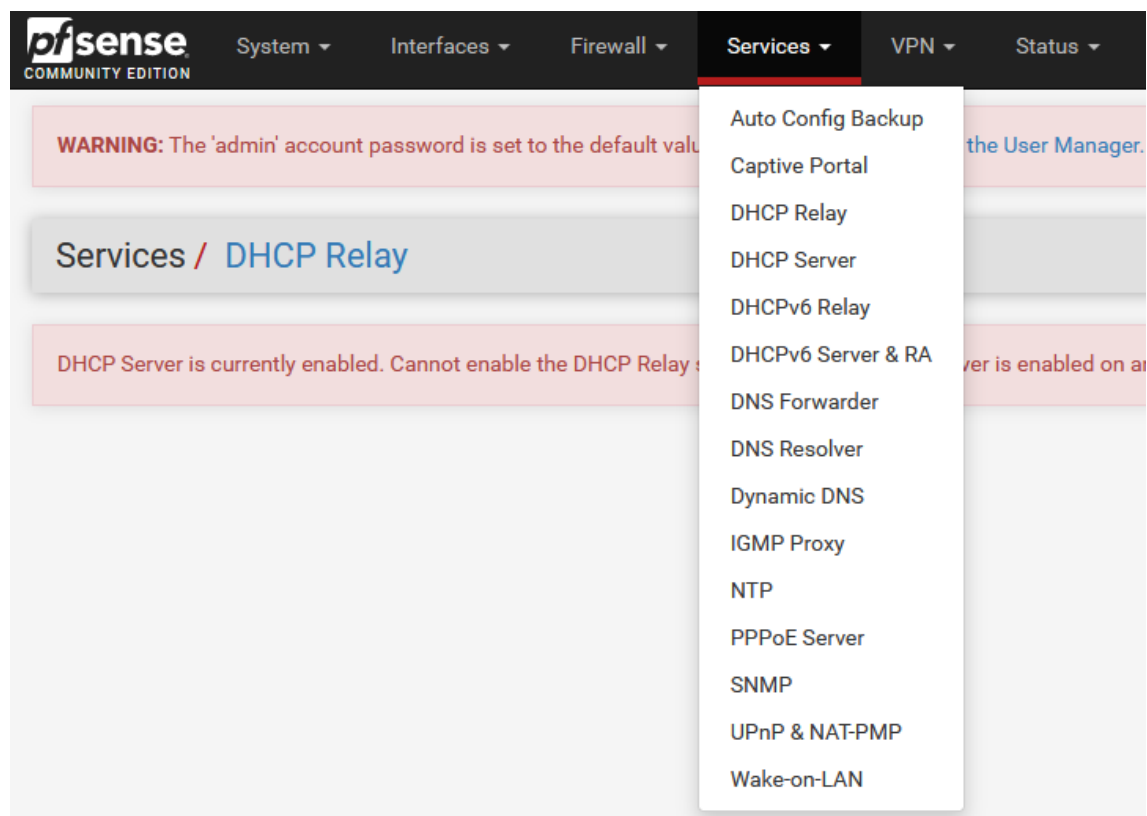
# Como usar PfSense para configurar un servidor de DNS y DHCP

Si quieres aplicar DHCP a los equipos de los usuarios, la Herramienta Pfsense cuenta con esta característica, también te permite configurar los DNS para que puedan conectarse a un servidor o dispositivos de red.

Antes de configurar el DHCP debes tener conectado la salida del dispositivo Pfsense a un swicht y este repartir a los usuarios, también puedes conectar a un dispositivo Wifi de modo Brigde y en las interfaces del Pfsense seleccionar cual va a ser tu LAN por defecto.

## Paso 1:

En el panel Pfsense nos vamos al menú de Servicio y seleccionamos la opción de DHCP Server.



## Paso 2:

La interfaz por defecto va a estar con el nombre de LAN, si tienes más interfaces de salida estas deben ser declaradas en el PfSense para que se muestren en el Panel DHCP. En el panel General primero habilitamos el DHCP en la opción de Enable, mas abajo nos va a indicar la subred y el rango disponible de IPs, podemos personalizar el rango y dejar unos libres para IPs Fijas.

LAN

General Options

Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<div>Allow all clients</div> <p>When set to <b>Allow all clients</b>, any DHCP client will get an IP address within this scope/range on this interface. If set to <b>Allow known clients from any interface</b>, any DHCP client with a MAC address listed in a static mapping on <b>any</b> scope(s)/interface(s) will get an IP address. If set to <b>Allow known clients from only this interface</b>, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</p>
Ignore denied clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	<div>192.168.1.100</div> <div>192.168.1.199</div> <div>FromTo</div>

Paso 3:

En el campo de Server podemos agregar los DNS que pueden ser hasta 4, los cuales nos va a permitir conectarnos con otros servicios, por último seleccionamos en Guardar.

Additional Pools

Add

+ Add pool

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Actions
------------	----------	-------------	---------

Servers

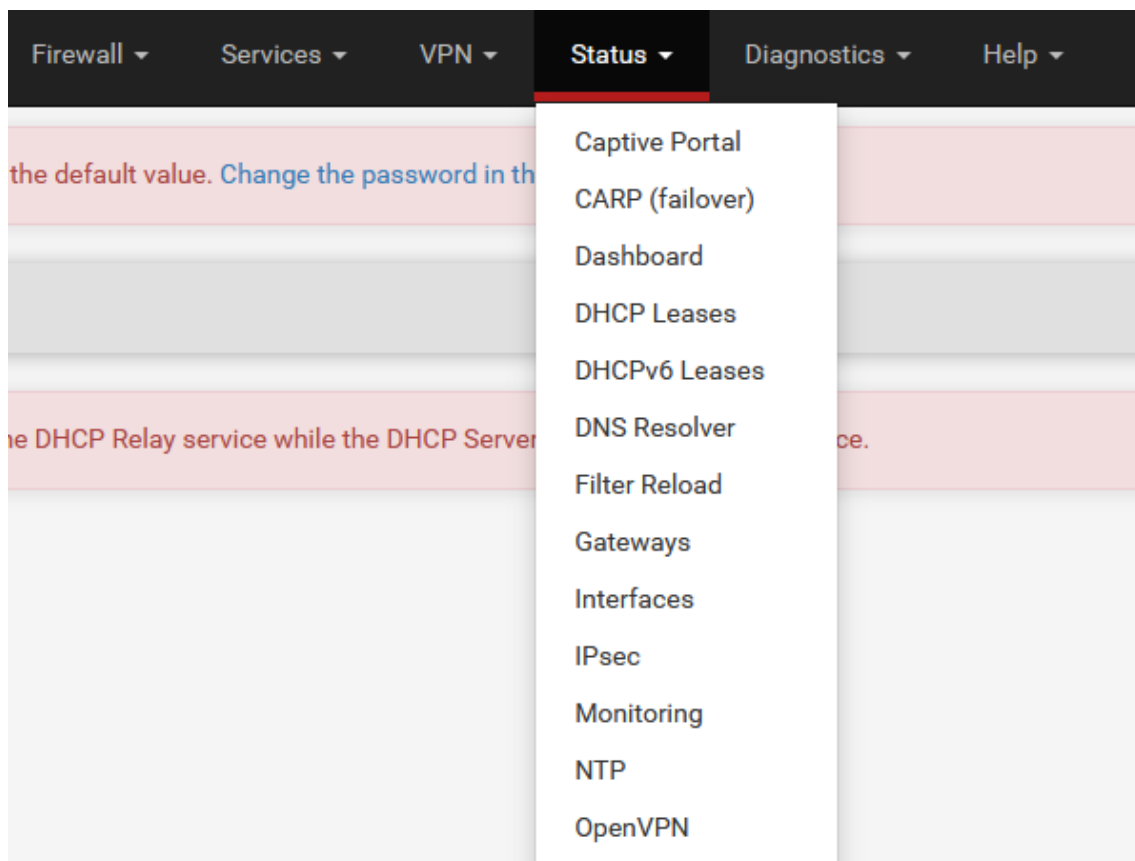
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	192.168.1.1
	DNS Server 2
	DNS Server 3
	DNS Server 4

Leave blank to use the system default DNS servers: The IP address of this firewall interface if DNS Resolver or Forwarder is enabled, otherwise the servers configured in General settings or those obtained dynamically.

Paso 4:

Una vez que el Servicio DHCP este activado conectamos los equipos y vamos a ver que automáticamente va a tomas el rango de IPs configurados y también los DNS, para verificar esto nos vamos al menú de Estatus y seleccionamos la opción de DHCP Leases.





## Paso 5:

En el panel de DHCP Leases vas a poder visualizar los Equipo con sus direcciones IP y dirección MAC, los cuales vas a poder administrarlo.

Status / DHCP Leases									
<div>Search</div> <div>Search term <input type="text"/> All <span>Search</span> <span>Clear</span></div> <div>Enter a search string or *nix regular expression to filter entries.</div>									
Leases									
	IP address	MAC address	Client Id	Hostname	Description	Start	End	Online	Lease Type
	192.168.1.101	00:0c:29:61:e5:13		DESKTOP-R1RMO61		2023/09/12 13:40:04	2023/09/12 15:40:04	active	active
Leases in Use									
	Interface	Pool Start	Pool End	# of leases in use					
	LAN	192.168.1.100	192.168.1.199	1					

# Como reservar la dirección IP de un usuario específico con DHCP

Si quieres reservar unos equipos con una dirección IP estática, la herramienta DHCP del Pfsense te permite aplicar esta configuración, pero para poder realizar debes tener primero la dirección MAC del equipo.


## Paso 1:

En el panel de configuración debe tener un pool de IP libres que no esté dentro del rango del DHCP.

Subnet	192.168.1.0	
Subnet mask	255.255.255.0	
Available range	192.168.1.1 - 192.168.1.254	
Range	<input type="text" value="192.168.1.100"/>	<input type="text" value="192.168.1.199"/>
	From	To

## Paso 2:


En la parte final del panel de configuración DHCP vamos a tener un campo donde van a estar las direcciones IPS estáticas, seleccionamos en el botón de Agregar.

 Save

DHCP Static Mappings for this Interface				
Static ARP	MAC address	IP address	Hostname	Description
<div>+ Add</div>				

## Paso 3:

Ahora agregamos la dirección MAC del equipo, la dirección IP que le queremos poner y una descripción para identificar el Equipo, seleccionamos en botón guardar para aplicar los cambios.

Static DHCP Mapping on LAN	
MAC Address	<input type="text" value="00:0c:29:61:e5:13"/> 
MAC address of the client to match (6 hex octets separated by colons).	
Client Identifier	<input type="text"/>
An optional identifier to match based on the value sent by the client (RFC 2132)	
IP Address	<input type="text" value="192.168.1.90"/>
IPv4 address to assign this client.	
Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool. The same IP address may be assigned to multiple mappings.	
Hostname	<input type="text"/>
Name of the client host without the domain part.	
Description	<input type="text" value="Equipo IP estatico"/>
A description for administrative reference.	

#### Paso 4:

Una vez creado el DHCP estático, reiniciamos el equipo para que se aplique el cambio.

DHCP Static Mappings for this Interface (total: 1)				
Static ARP	MAC address	IP address	Hostname	Description
	00:0c:29:61:e5:13	192.168.1.90		Equipo IP estatico
<a href="#">+ Add</a>				

#### Paso 5:

Para ver si se ha aplicado el cambio nos vamos al DHCP Leases y vemos que el equipo tomo la dirección IP configurada y que esta con DHCP estático.

Status / DHCP Leases

Search

Search term

All

Search

Clear

Enter a search string or \*nix regular expression to filter entries.

Leases

IP address	MAC address	Client Id	Hostname	Description	Start	End	Online	Lease Type	Actions
<div><div></div>192.168.1.90</div>	00:0c:29:61:e5:13			Equipo IP estatico	n/a	n/a	<div><div></div>active</div>	static	<div><div></div><div></div></div>

Leases in Use

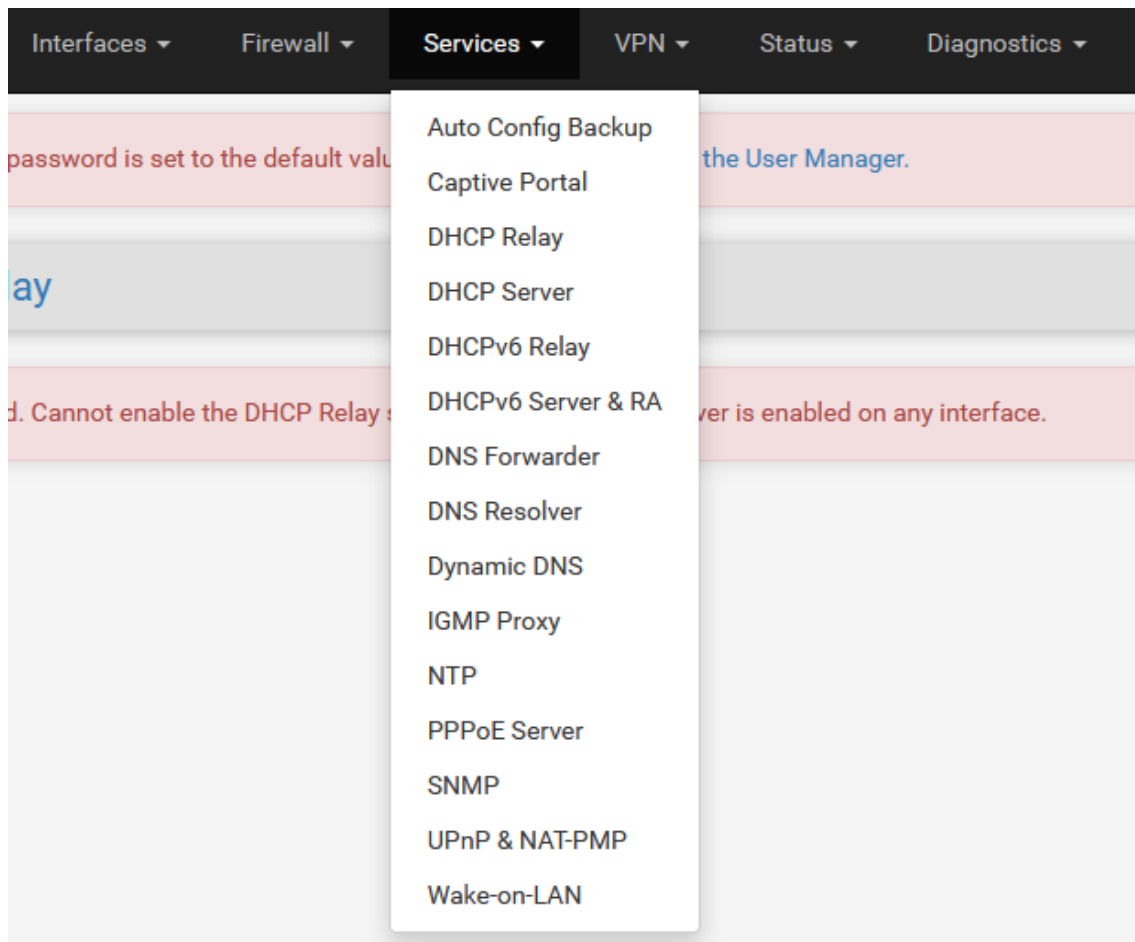
Interface	Pool Start	Pool End	# of leases in use
No leases are in use			

## Como bloquear un sitio web con DNS resolver en Pfsense

Si quieres bloquear algunas paginas web especificas a tus usuarios la herramienta Pfsense cuenta con un módulo DNS Resolver que te permite administrar el bloqueo de las páginas.

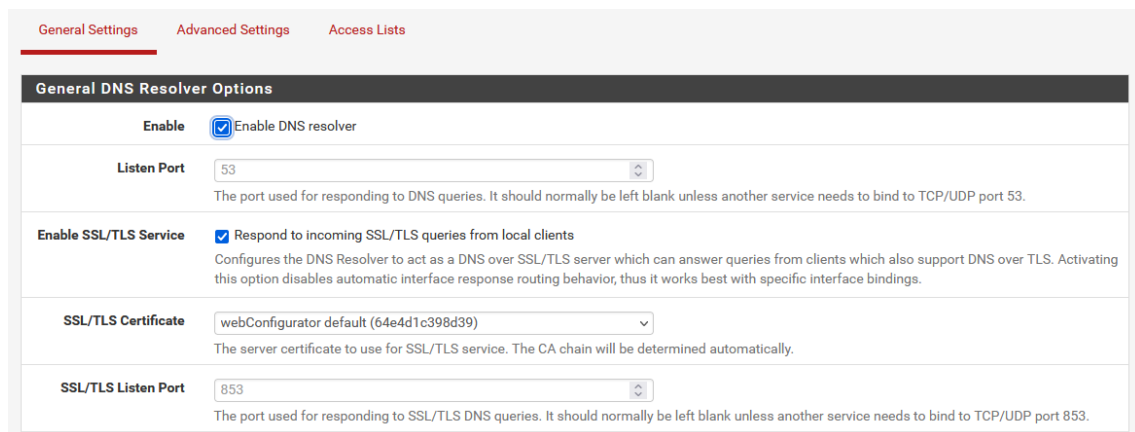
#### Paso 1:

Primero nos Vamos al menú de Servicios y escogemos la opción de DNS Resolver.



## Paso 2:

En la Configuración General debe estar habilitado el DNS Resolver, también de activar el servicio SSL/TLS.



## Paso 3:

Puedes también personalizar donde se va a aplicar el bloqueo (LAN, WAN, etc), pero por defecto le ponemos en Todos.

<b>Network Interfaces</b>	<div> <div>All</div> <div> <div>WAN</div> <div>LAN</div> <div>WAN IPv6 Link-Local</div> <div>LAN IPv6 Link-Local</div> </div> </div>
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.	
<b>Outgoing Network Interfaces</b>	<div> <div>All</div> <div> <div>WAN</div> <div>LAN</div> <div>WAN IPv6 Link-Local</div> <div>LAN IPv6 Link-Local</div> </div> </div>
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.	
<b>Strict Outgoing Network Interface Binding</b>	<input type="checkbox"/> Do not send recursive queries if none of the selected Outgoing Network Interfaces are available. By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.
<b>System Domain Local Zone Type</b>	<div>Transparent</div> <div>The local-zone type used for the pfSense system domain (System   General Setup   Domain). Transparent is the default.</div>
<b>DNSSEC</b>	<input checked="" type="checkbox"/> Enable DNSSEC Support

#### Paso 4:

Ahora en la opción de Custom Options podemos personalizar el Bloqueo de las paginas y poner las siguientes opciones

Primero Declaramos el control de acceso con el pool de IPs y le ponemos un nombre que se llama bloqueo.

server:

access-control-view: 192.168.1.0/24 bloqueo

Luego declaramos el acceso con el nombre de bloqueo y dentro de ello agregamos las paginas que queremos bloquear.

view:

name: "bloqueo"  
 view-first: yes  
 local-zone: "youtube.com" inform\_deny  
 local-zone: "facebook.com" inform\_deny

Para el caso del PFBlocker también puedes declararlo esto para hacer una exclusión.

view:

name: "dnsbl"  
 view-first: yes  
 include: /var/unbound/pfb\_dnsbl.\*conf

Al terminar la configuración, seleccionamos en el botón de Guardar para aplicar los cambios.

Display Custom Options

Hide Custom Options

Custom options

```
server:
  access-control-view: 192.168.1.0/24 bloqueo
#IPS CON ACCESO#

view:
  name: "bloqueo"
  view-first: yes
  local-zone: "youtube.com" inform_deny
  local-zone: "m.youtube.com" inform_deny
  local-zone: "youtube.com.pe" inform_deny
  local-zone: "facebook.com" inform_deny
  local-zone: "netflix.com" inform_deny
  local-zone: "mail.google.com" inform_deny
  include: /var/unbound/pfb_dnsbl.*conf

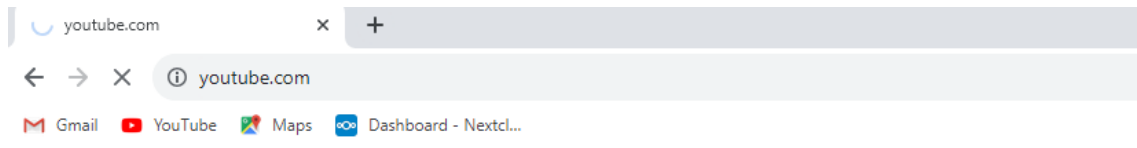
view:
  name: "dnsbl"
  view-first: yes
  include: /var/unbound/pfb_dnsbl.*conf
```

Enter any additional configuration parameters to add to the DNS Resolver configuration here, separated by a newline.

Save

## Paso 5:

Por para validar el bloqueo de páginas probamos en uno de los equipos de los usuarios y vemos que la página web ya no se muestra.



## No se puede acceder a este sitio web

Comprueba si hay un error de escritura en youtube.com.

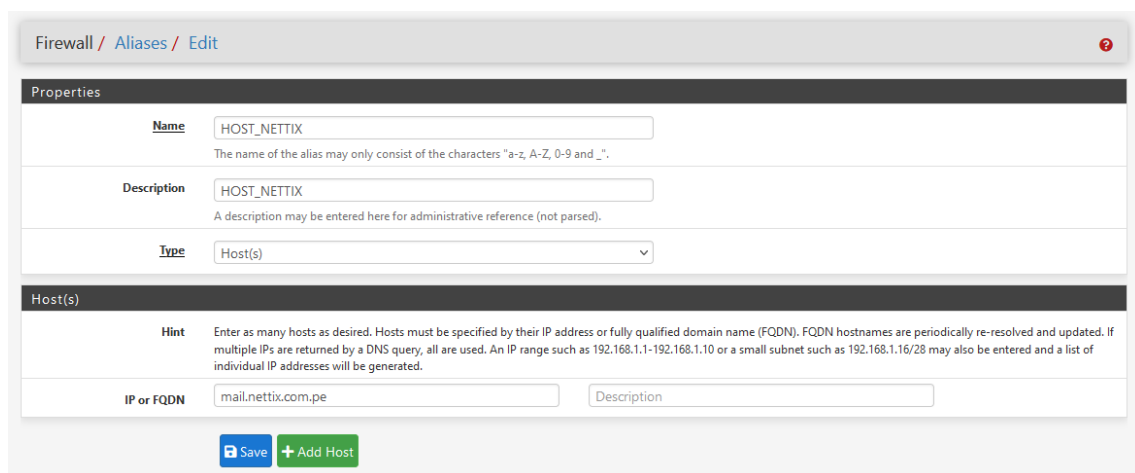
Si está escrito correctamente, [prueba a ejecutar el diagnóstico de red de Windows](#).

DNS\_PROBE\_FINISHED\_NXDOMAIN

# Como realizar un NAT en Pfsense

Un servicio NAT sirve para habilitar los servicios externos que vienen de internet y especificar con que IP y Puerto se van a conectar los usuarios internos, esto te permitirá administrar tus conexiones externas, como también seguridad en su red interna, la Herramienta Pfsense cuenta con un módulo de NAT en donde puedes realizar esta configuración.

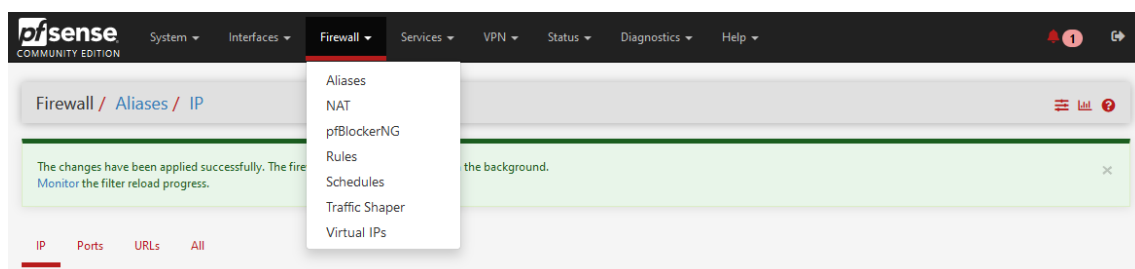
**Paso 1:** Puedes aplicar el NAT ya sea con una IP Fija o con un Alias, en este caso vamos a crear un Alias en donde se va a incluir el Host externo.



The screenshot shows the 'Firewall / Aliases / Edit' configuration page in Pfsense. The 'Properties' section includes fields for 'Name' (HOST\_NETTIX), 'Description' (HOST\_NETTIX), and 'Type' (Host(s)). Below this is the 'Host(s)' section with a 'Hint' explaining that hosts can be specified by IP or FQDN. The 'IP or FQDN' field contains 'mail.nettix.com.pe' and there is an empty 'Description' field. At the bottom are 'Save' and '+ Add Host' buttons.

**Paso 2:**

Una Vez creado el Alias nos vamos al menú Firewall y escogemos la opción de NAT.



**Paso 3:**

En el panel de NAT vamos a poder ver nuestras reglas aplicadas para conexiones Externas, para crear uno nuevo seleccionamos el botón de Agregar.

Firewall / NAT / Port Forward										
Port Forward 1:1 Outbound NPT										
Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	200	100.5.5.1	400	Redireccion servicio	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	10000	127.0.0.1	443 (HTTPS)	ACCESO ADMINSTRACION DESDE WAN PFSENSE PORT 443	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	10001	127.0.0.1	80 (HTTP)	ACCESO ADMINSTRACION DESDE WAN PFSENSE PORT 80	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	3000 (HBCI)	127.0.0.1	3000 (HBCI)	ACCESO ADMINSTRACION NTOP WAN PFSENSE PORT 3000	
<input type="checkbox"/>	WAN	TCP	HOST_ZABBIX_NETTIX	*	WAN address	10050	127.0.0.1	10050	ACCESO NAT DESDE zabbix.nettix.com.mx HACIA ZABBIX PORT 10050	
Add            Add            Delete            Toggle            Save            Separator										

#### Paso 4:

La interface por Defecto es WAN al que la IP, el protocolo escogemos el tipo como en nuestro caso es una web, seleccionamos en TCP, Ahora en Source agregamos el Alias creado, el puerto lo dejamos en Any.

Firewall / NAT / Port Forward / Edit										
Edit Redirect Entry										
Disabled <input type="checkbox"/> Disable this rule										
No RDR (NOT) <input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.										
Interface <span>WAN</span> Choose which interface this rule applies to. In most cases "WAN" is specified.										
Address Family <span>IPv4</span> Select the Internet Protocol version this rule applies to.										
Protocol <span>TCP</span> Choose which protocol this rule should match. In most cases "TCP" is specified.										
Source  Hide Advanced										
Source <input type="checkbox"/> Invert match. <span>Single host or alias</span> <span>HOST_NETTIX</span> Type Address/mask										
Source port range <span>Any</span> From port Custom To port Custom										
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.										

#### Paso 5:

En Destino decimos que viene por la WAN, agregamos el puerto específico, en la redirección ponemos la IP del localhost para que vengan del mismo host y el puerto por donde va a conectarse, por último, le ponemos una Descripción y guardamos el NAT.



**Destination** ☐ Invert match. WAN address Type Address/mask

**Destination port range** Other 10000 Other 10000  
 From port Custom To port Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP** Single host 127.0.0.1  
 Type Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
 In case of IPv6 addresses, it must be from the same "scope",  
 i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

**Redirect target port** Other 10000  
 Port Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).  
 This is usually identical to the "From port" above.

**Description** ACCESO NAT DESDE NETTIX PORT 10000  
 A description may be entered here for administrative reference (not parsed).

**No XMLRPC Sync** ☐ Do not automatically sync to other CARP members  
 This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**NAT reflection** Use system default

**Filter rule association** Rule NAT ACCESO NAT DESDE NETTIX PORT 10000

## Paso 6:

Una vez creada el NAT aplicamos el Cambio para que se guarde en el Pfsense, ahora al realizar la consulta del Host con el puerto definido vamos a poder conectarnos al servicio.

The NAT configuration has been changed.  
 The changes must be applied for them to take effect. ✓ Apply Changes

**Port Forward** 1:1 Outbound NAT

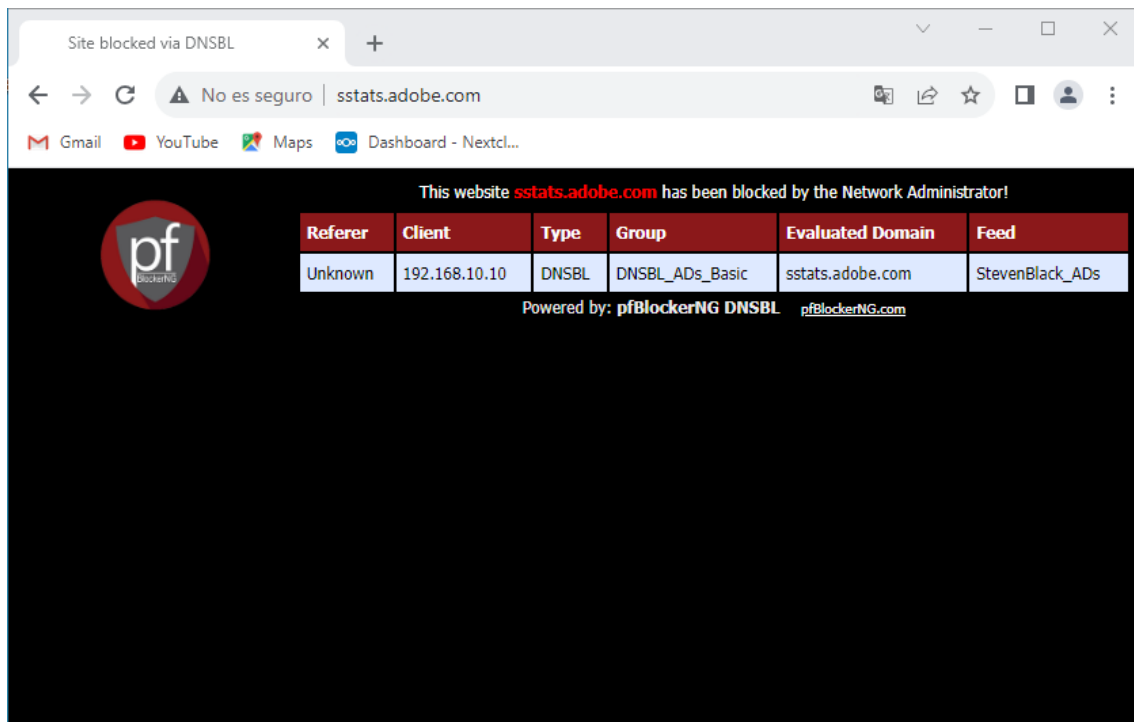
Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	200	100.5.5.1	400	Redireccion servicio	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	10000	127.0.0.1	443 (HTTPS)	ACCESO ADMINSTRACION DESDE WAN PFSense PORT 443	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	10001	127.0.0.1	80 (HTTP)	ACCESO ADMINSTRACION DESDE WAN PFSense PORT 80	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	3000 (HBCI)	127.0.0.1	3000 (HBCI)	ACCESO ADMINSTRACION NTOP WAN PFSense PORT 3000	
<input type="checkbox"/>	WAN	TCP	HOST_ZABBIX_NETTIX	*	WAN address	10050	127.0.0.1	10050	ACCESO NAT DESDE zabbix.nettix.com.mx HACIA ZABBIX PORT 10050	
<input type="checkbox"/>	WAN	TCP	HOST_NETTIX	*	WAN address	10000	127.0.0.1	10000	ACCESO NAT DESDE NETTIX PORT 10000	

# Como Agregar una página en la lista blanca del PFBLOCKER

PfBlocker es un complemento que se puede integrar en el Pfsens, esta herramienta te permite analizar y bloquear paginas no seguras para los usuarios. En el caso que una página que usas haya sido bloqueada, el PfBlocker tiene un campo con nombre WhiteList donde puedes agregar las páginas que no quieres que se bloquee.

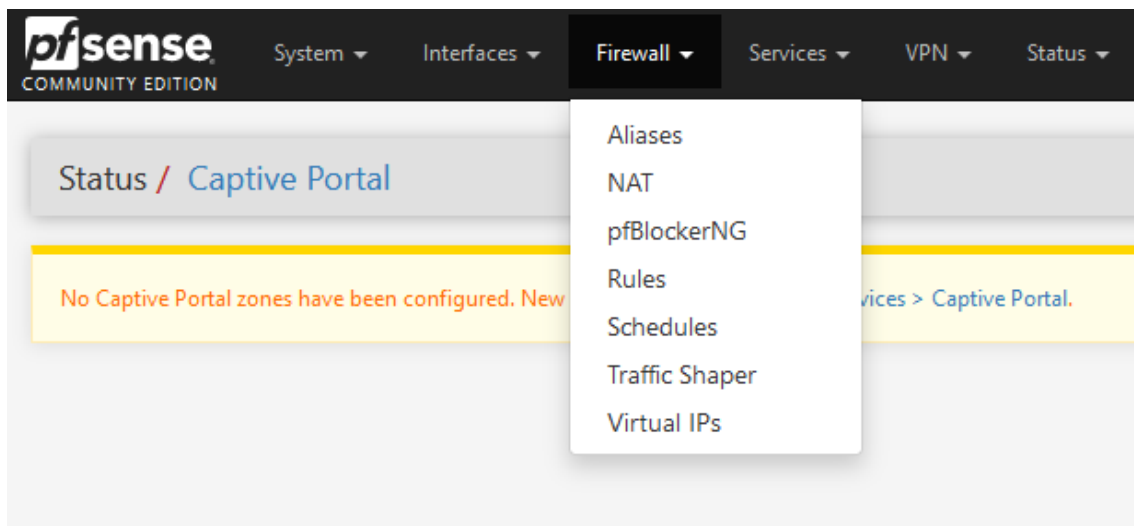
## Paso 1:

En este caso al consultar una página o servicio de Adobe nos muestra el sitio ha sido bloqueado por el Pfblocker.



## Paso 2:

Copiamos la dirección URL de la página bloqueada y nos vamos al menú de Firewall y en la opción de PfBlockerNG.



## Paso 3:

Al ingresar al Panel de PfBlocker vemos varias funciones, para la Whitelist nos vamos a la pestaña de DNSBL.

Firewall / pfBlockerNG / DNSBL

General IP **DNSBL** Update Reports Feeds Logs Sync

DNSBL Groups DNSBL Category DNSBL SafeSearch

### DNSBL

**Links** Firewall Aliases Firewall Rules Firewall Logs

**DNSBL** ☒ **Enable DNSBL**  
 This will enable DNS Block List for Malicious and/or unwanted Adverts Domains  
 To Utilize, **Unbound DNS Resolver** must be enabled. Also ensure that pfBlockerNG is enabled. ⓘ

**DNSBL Mode** Unbound mode   
 Select the DNSBL mode. ⓘ

#### Paso 4:

Ahora en la parte inferior hay un campo con nombre DNSBL Whitelist, es ahí donde vamos a agregar la URL de la página Bloqueada, ahora seleccionamos en el botón de Guardar.

DNSBL Whitelist

```
control.kochava.com
secure-gl.imrworldwide.com
pbs.twimg.com # twitter images
www.pbs.twimg.com # twitter images
cs196.wac.edgecastcdn.net # CNAME for (pbs.twimg.com)
cs2-wac-apr-8315.edgecastdns.net # CNAME for (pbs.twimg.com)
cs2-wac-us-8315.ecdns.net # CNAME for (pbs.twimg.com)
cs45.wac.edgecastcdn.net # CNAME for (pbs.twimg.com)
cs2-wac-apr-8315.edgecastdns.net # CNAME for (pbs.twimg.com)
cs2-wac-us-8315.ecdns.net # CNAME for (pbs.twimg.com)
cs45.wac.edgecastcdn.net # CNAME for (pbs.twimg.com)
.pfsense.org
.netgate.com
chrome.google.com
.nettix.com.mx
sstats.adobe.com
```

No Regex Entries Allowed! ⓘ

#### Paso 5:

Luego de ello nos va a pedir actualizar los cambios para eso nos vamos la pestaña de Update, hacemos Check en la opción de Reload y escogemos en All, ahora esperamos unos minutos para que actualice los cambios.

Firewall / pfBlockerNG / Update

General IP DNSBL **Update** Reports Feeds Logs Sync

### Update Settings

**Links** Firewall Aliases Firewall Rules Firewall Logs

**Status** NEXT Scheduled CRON Event will run at 15:00 with 00:18:22 time remaining.  
 Refresh to update current status and time remaining.

**Force Options** **\*\* AVOID \*\*** Running these "Force" options - when CRON is expected to RUN! ⓘ

Select 'Force' option ☐ Update ☐ Cron ☒ Reload

Select 'Reload' option ☒ All ☐ IP ☐ DNSBL

Una vez finalizado al volver a cargar la página vemos que ya se puede mostrar.

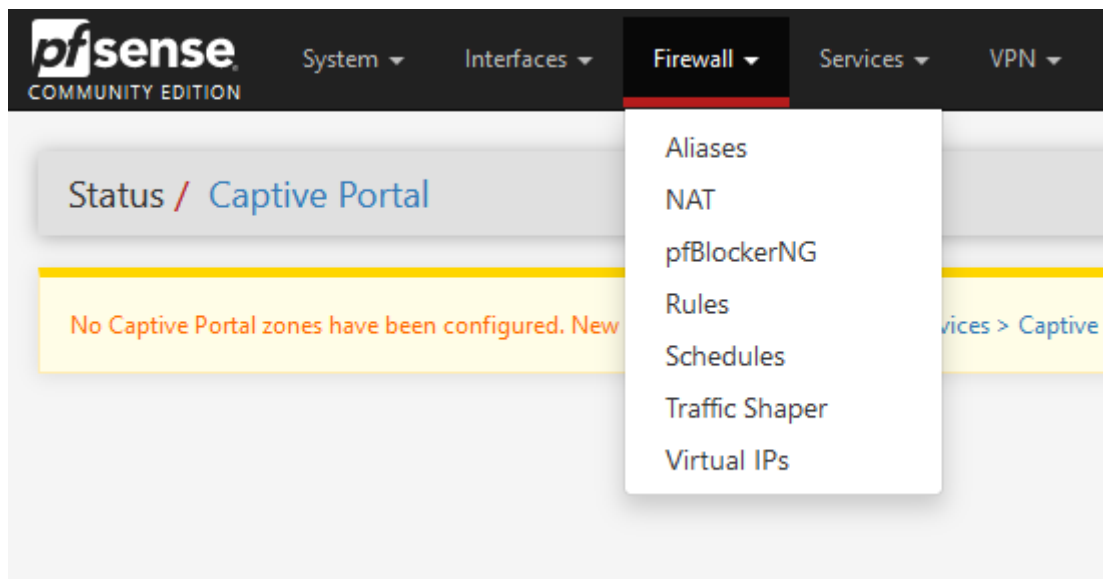


# Como gestionar el ancho de banda en el Pfsense

Si cuentas con un servidor de archivos en donde consultan los usuarios, El modulo Traffic Shaper te permite limitar el ancho de banda de descarga y subida esto para que tu servido no se sature con las constantes peticiones.

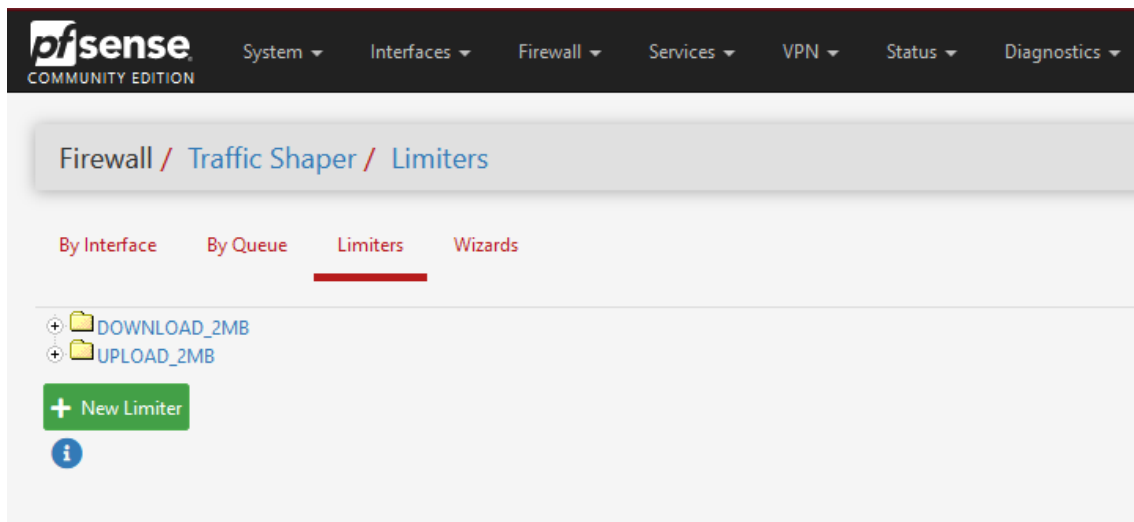
## Paso 1:

En el Pfsense nos vamos al Menu de Firewall y escogemos la opción de Traffic Shaper.



## Paso 2:

En el panel de Traffic shaper nos ubicamos en la pestaña de Limiters y ahí es donde vamos a crear la regla para la subida y descarga del ancho de banda, seleccionamos en el Boton de New Limiter.



### Paso 3:

Le ponemos un nombre en este caso DMZ Descargas, luego le asignamos el limite máximo ancho de banda que es 40 Mb, Definimos que es un Source Addresses y la máscara que es 32, le ponemos una descripción y guardamos los cambios.

Limiters			
Enable	<input checked="" type="checkbox"/> Enable limiter and its children		
Name	<input type="text" value="DMZ_DESCARGAS"/>		
Bandwidth	Bandwidth	Bw type	Schedule
	<input type="text" value="40"/>	<input type="text" value="Mbit/s"/>	<input type="text" value="none"/>
			<input type="button" value="Delete"/>
	<input type="button" value="+ Add Schedule"/>		
Mask	<input type="text" value="Source addresses"/>		
	If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.		
	<input type="text" value="32"/>	<input type="text" value="128"/>	
	IPv4 mask bits 255.255.255.255/?	IPv6 mask bits ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?	
Description	<input type="text" value="Limite de Descarga DMZ"/>		
	A description may be entered here for administrative reference (not parsed).		

### Paso 4:

Aplicamos la misma configuración ahora para la subida, en este caso le asignamos un ancho de banda de 20 Mb, le ponemos una descripción y guardamos los cambios.

Limiters			
<b>Enable</b>	<input checked="" type="checkbox"/> Enable limiter and its children		
<b>Name</b>	<input type="text" value="DMZ_SUBIDAS"/>		
<b>Bandwidth</b>	<b>Bandwidth</b>	<b>Bw type</b>	<b>Schedule</b>
	<input type="text" value="20"/>	<input type="text" value="Mbit/s"/>	<input type="text" value="none"/>
	<input type="button" value="+ Add Schedule"/>		
<b>Mask</b>	<input type="text" value="Source addresses"/>		
	If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.		
	<input type="text" value="32"/>	<input type="text" value="128"/>	
	IPv4 mask bits 255.255.255.255/?	IPv6 mask bits ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?	
<b>Description</b>	<input type="text" value="Limite de Subida DMZ"/>		
	A description may be entered here for administrative reference (not parsed).		

## Paso 5:

Ahora Creamos la Regla en donde se va a aplicar el límite de ancho de Banda, la interface es la LAN, en protocolo le damos en Any, ahora en source ponemos la dirección IP del servidor.

Edit Firewall Rule			
<b>Action</b>	<input type="text" value="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.		
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
<b>Interface</b>	<input type="text" value="LAN"/>		
	Choose the interface from which packets must come to match this rule.		
<b>Address Family</b>	<input type="text" value="IPv4"/>		
	Select the Internet Protocol version this rule applies to.		
<b>Protocol</b>	<input type="text" value="Any"/>		
	Choose which IP protocol this rule should match.		
<b>Source</b>			
<b>Source</b>	<input type="checkbox"/> Invert match	<input type="text" value="Single host or alias"/>	<input type="text" value="192.168.88.19"/>
<b>Destination</b>			
<b>Destination</b>	<input type="checkbox"/> Invert match	<input type="text" value="any"/>	<input type="text" value="Destination Address"/>

## Paso 6:

Desglosamos las opciones avanzadas y en el campo In/Out pipe asignamos los límites que se han creado, ahora seleccionamos en el botón de Guardar.

**Schedule** none  
 Leave as 'none' to leave the rule enabled all the time.

**Gateway** Default  
 Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.  
 Gateway selection is not valid for "IPv4+IPv6" address family.

**In / Out pipe** DMZ\_SUBIDAS DMZ\_DESCARGAS  
 Choose the Out queue/Virtual interface only if In is also selected. The Out selection is applied to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface.  
 If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out the selections are reversed, Out is for incoming and In is for outgoing.

**Ackqueue / Queue** none none  
 Choose the Acknowledge Queue only if there is a selected Queue.

## Paso 7:

Una vez que este la regla creada guardamos los cambios para que se aplique el límite de ancho de banda.

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** OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	*	*	*	LAN Address	443 80 2222	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	192.168.88.19	*	*	*	*	none			⬇️ ⚙️ ⏏️ 🗑️
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4	⬇️ ⚙️ ⏏️ 🗑️
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	pfB_BinaryDefense_v4	*	*	none		pfB_BinaryDefense_v4	⬇️ ⚙️ ⏏️ 🗑️

Ahora cuando vas a consultar a tu servidor de archivos vas a ver que el límite máximo de descarga es de 40 Mb y de subida 20 Mb.

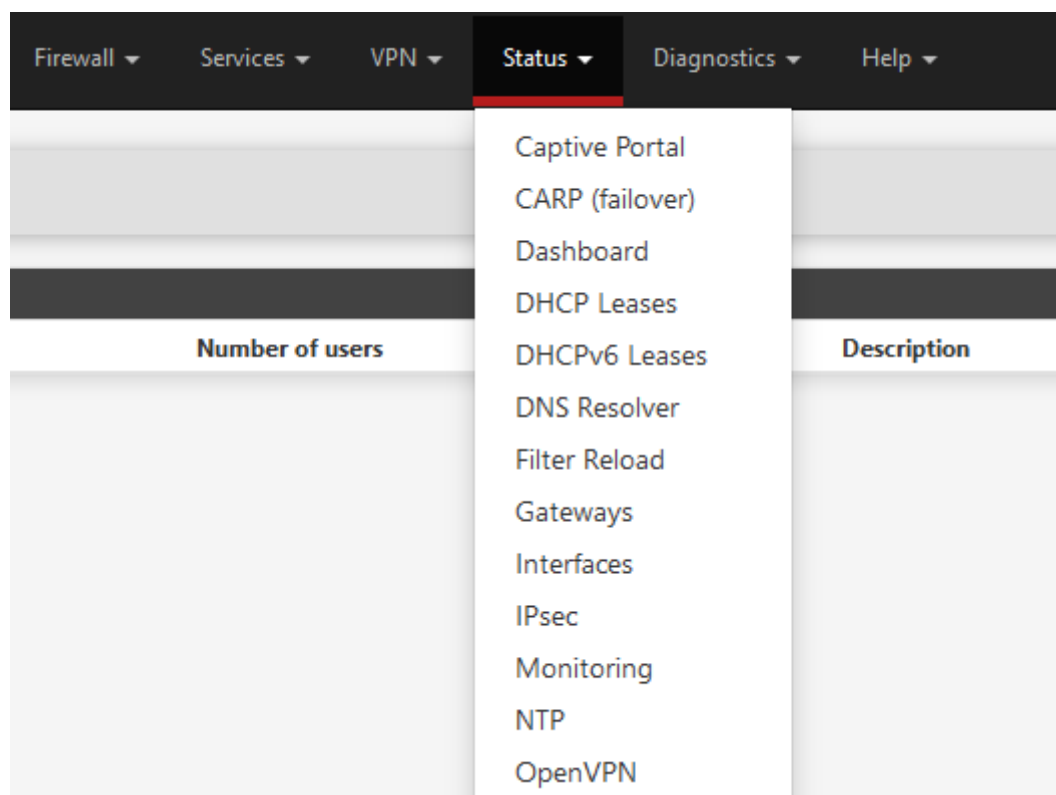


# Como verificar el consumo de ancho de banda en el Pfsense

Si quieres verificar el consumo del ancho de banda ya sea de la WAN o la LAN, la Herramienta Monitoring del Pfsense te permite visualizar el consumo de Red en tiempo Real

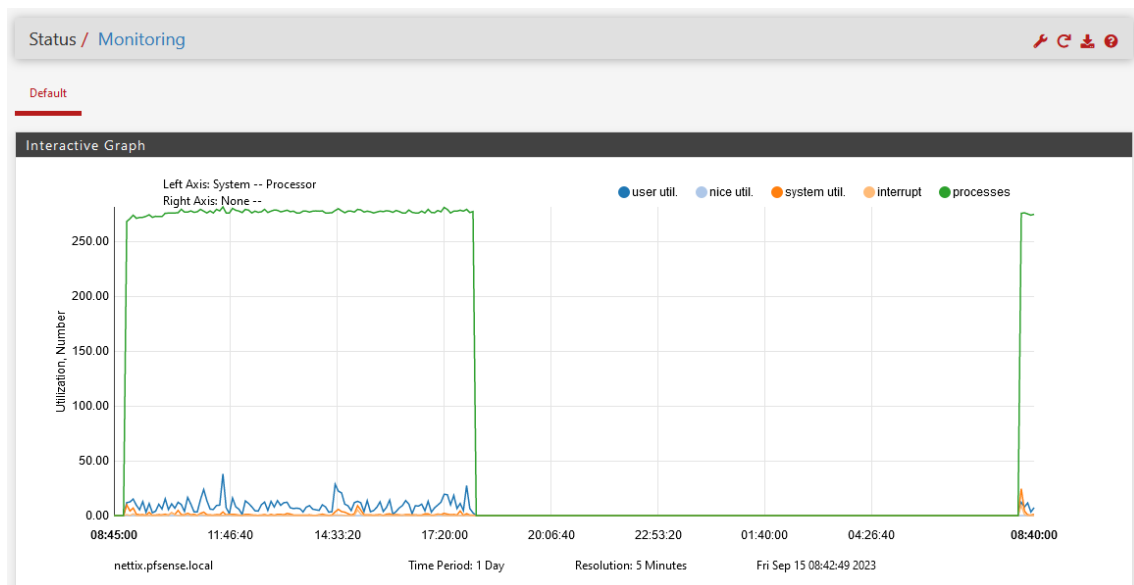
## Paso 1:

En el Panel Pfsense nos vamos al menú de Status y seleccionamos la opción de Monitoring.



## Paso 2:

Al ingresar al panel nos va a mostrar un resumen del consumo de red, pero si quieres ver más detalles seleccionamos en el icono de la tuerca que se encuentra en la parte superior derecha.



### Paso 3:

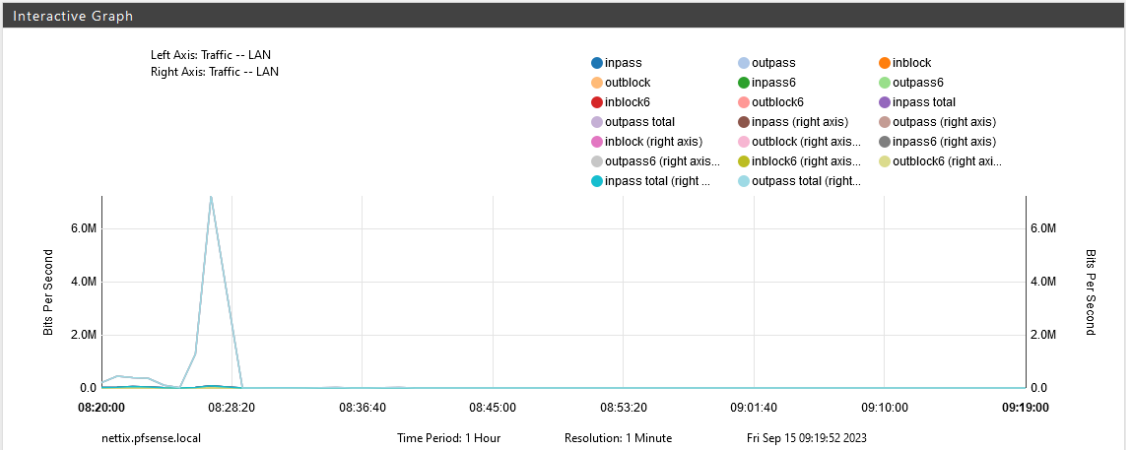
Ahora vas a poder personalizar con más detalles, en categoría escogemos la opción de Traffic y en Graph poner la interfaz que se quiere visualizar que puede ser la LAN, la WAN etc, luego en opciones puedes poner el intervalo de tiempo que puede ser 1 hora, 1 día etc, también poner el tipo de gráfico o si se quiere invertir el mismo, por último seleccionamos en el Boton Update Graphs.

The screenshot shows the Mikrotik WinBox Monitoring Settings page. The 'Settings' tab is selected. The page contains several configuration options:
 

- Left Axis:** A dropdown menu set to 'Traffic'.
- Right Axis:** A dropdown menu set to 'Traffic'.
- Options:** A section with five dropdown menus:
  - Time Period:** Set to '1 Hour'.
  - Resolution:** Set to '1 Minute'.
  - Graph Type:** Set to 'Line'.
  - Inverse:** Set to 'Off'.
  - Refresh Interval:** Set to 'Never'.
- Settings:** A section with two buttons: 'Display Advanced' (with a gear icon) and 'Update Graphs' (with a refresh icon).

### Paso 4:

Según lo que hayamos configurado en las opciones del Filtro vamos a visualizar el Gráfico del consumo de Ancho de Banda.

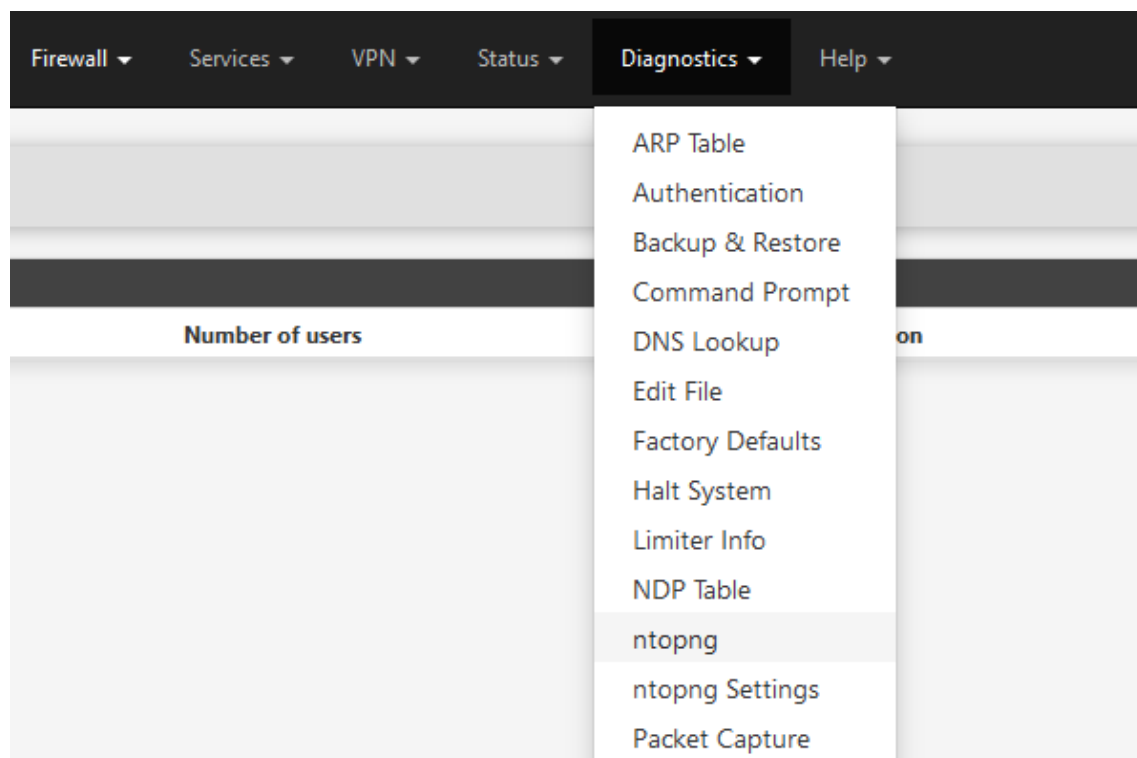


# Uso de NTOPNG para monitorear el Tráfico en tiempo real

Si quieres monitorear en tiempo Real el consumo del ancho de banda de los usuarios y que servicio o páginas web están peticionando, la Herramienta Ntopng te permite realizar seguimiento.

## Paso 1:

Para acceder nos vamos al Menú de Diagnóstico y escogemos la opción de Ntopng.



## Paso 2:

Al ingresar al portal de Ntopng te va a pedir que ingrese con tus credenciales de acceso.

# Welcome to ntopng

Username (default admin)  
admin

Password (default admin)  
●●●●●●●●●●●●●●●●

Login

Unable to login?

[User's Guides](#) | [Community](#) | [Support](#) | [FAQ](#) | [Code](#) | [Contact Us](#)

© 1998-23 - ntop  
ntopng is released under [GPLv3](#).

### Paso 3:

Al ingresar nos va a mostrar un Dashboard con el consumo total de la red LAN, para ver el seguimiento de los usuarios nos vamos el menú Flows y la opción de Live.

Shortcuts

Dashboard

Alerts

Flows

Hosts

Interface

Settings

Developer

em1

↕

92.80 Mbps  
2.00 Mbps

3

4

15 (1)

2

55

Dashboard

Talkers

Hosts

Ports

Applications

Top Flow Talkers

Live

























192.168.10.10

### Paso 4:

En el panel de Flows vas a poder revisar todas las peticiones del usuario y que servicios web están ingresando, también se puede ver el consumo del ancho de banda, si quieres ver más detalles del servicio a que están consultando debes darle click al nombre de la aplicación, si quieres ver más detalles del usuario deber darle click en el nombre del equipo.


### Live Flows

Flow Idle Timeout: 60 sec ⓘ

Serial	Application	Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes
🔍	TLS.UbuntuON... 	TCP	desktop-r1mo61  :50100	releases.ubuntu.com  :https	02:22	 Server	64.20 Mbps ↑	1.2 GB ↑
🔍	G+ TLS.Google 	TCP	desktop-r1mo61  :50074	www.google.com  :https	02:22	 Server	0 bps —	1.5 MB —
🔍	G+ TLS.Google 	TCP	desktop-r1mo61  :50080	www.gstatic.com  :https	02:16	 Server	0 bps —	172.39 KB —
🔍	TLS 	TCP	desktop-r1mo61  :49674	186.233.185.64  :https	01:49:18	 Client	0 bps —	109.73 KB ↑
🔍	TLS 	TCP	desktop-r1mo61  :50086	res.cloudinary.com  :https	02:24	 Server	0 bps —	71.29 KB —
🔍	G+ TLS.Google 	TCP	desktop-r1mo61  :50075	id.google.com  :https	02:37	 Client	0 bps ↓	12.03 KB —

### Paso 5:

Al ingresar al nombre de la aplicación vas a poder ver más detalles de sitio web o servicio y también saber que usuario están consultando al mismo.





Live Flows |  Analysis

TLS.UbuntuONE Live Flows

1.40 Mbps  
80.10 Mbps

Total Bytes: 2.01 GB  
Total Throughput: 93.70 Mbps

Flow Idle Timeout: 60 sec ⓘ

Serial	Application	Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
🔍	TLS.UbuntuON... 	TCP	desktop-r1mo61  :50100	releases.ubuntu.com  :https	03:54	 Server	70.70 Mbps ↑	1.97 GB ↑	releases.ubuntu.

Showing 1 to 1 of 1 rows



ntopng Community v.5.6.230701 (FreeBSD 14.0) ⓘ






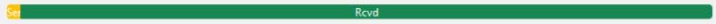
© 1998-23 - ntop

🕒 10:08:10 -0500 UTC | Uptime: 01:51:12

### Paso 6:

Si ingresas al Detalle del equipo vas a poder visualizar toda la información del usuario, el consumo del ancho de banda del equipo entre otras cosas.

Host: desktop-r1mo61  |  Traffic Packets Ports Peers Apps DNS TLS HTTP ⓘ ⚙️

Router/AccessPoint MAC Address	Vmware_27:8B:1D	
Host MAC Address	Vmware_61:E5:13	 Computer ⓘ
IP Address	192.168.10.10 [ 192.168.10.0/24 ]	Host Pool: Default ⓘ
OS	 Windows	
Name	desktop-r1mo61   	
Active Monitoring	Add ICMP Monitor +	
Active Alerted Flows	1 —	
First / Last Seen	15/09/2023 08:17:13 [01:51:53 ago]	15/09/2023 10:09:06 [< 1 sec ago]
Sent vs Received Traffic Breakdown	 Rcvd	
Traffic Sent / Received	702,552 Pkts / 43.4 MB ↑	1,829,223 Pkts / 2.5 GB ↑

# Como redireccionar el tráfico entre diferentes proveedores de internet ISP

Si tienes 2 proveedores de internet y quieres optimizar el consumo de ancho de banda de tu Red, la herramienta PfSense te permite redireccionar el tráfico de algunas páginas web o servicios por tu proveedor secundario de internet de manera que puedas liberar el consumo de tu proveedor principal.

## Paso 1:

Primero creamos una Alias en donde vamos a agregar las páginas que van a salir por el segundo proveedor.

Properties		
Name	WEBSGWAN2	
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".		
Description	Webs que salen por la Wan2	
A description may be entered here for administrative reference (not parsed).		
Type	Host(s)	

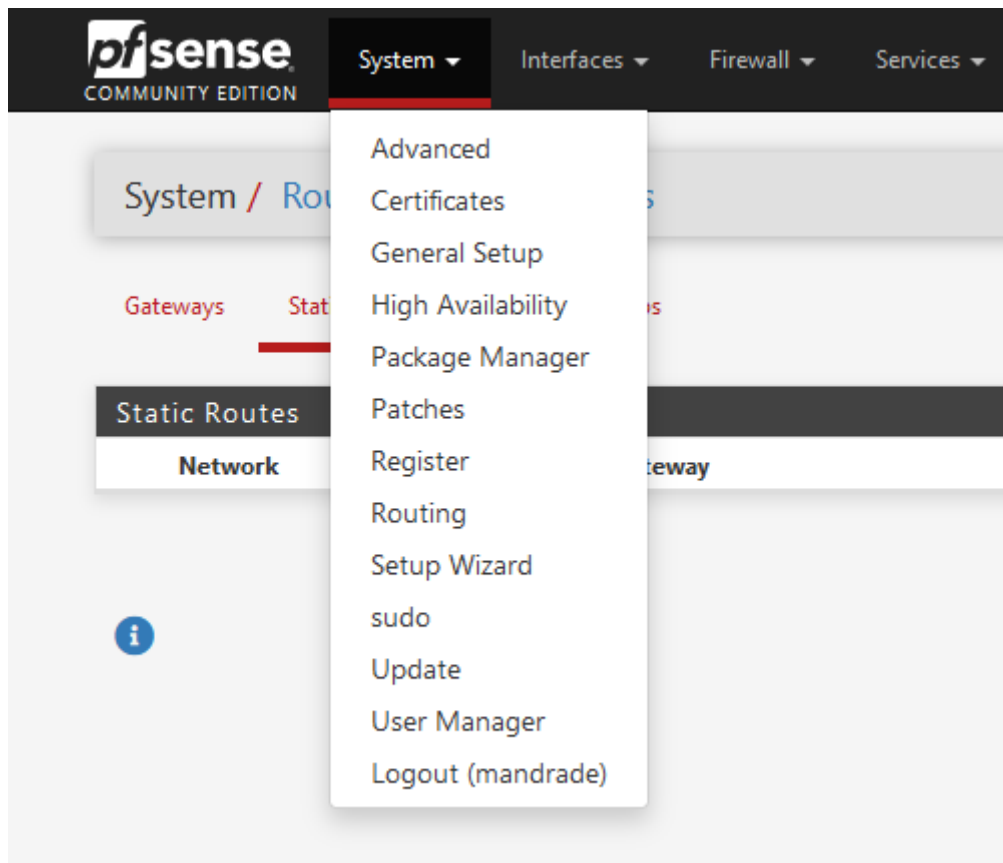
  

Host(s)		
Hint	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small 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	mxtoolbox.com	Entry added Mon, 18 Sep 2023 17:05:28 -0500 <span>Delete</span>
	dnschecker.org	Entry added Mon, 18 Sep 2023 17:05:28 -0500 <span>Delete</span>
	sitecheck.sucuri.net	Entry added Mon, 18 Sep 2023 17:05:28 -0500 <span>Delete</span>

Save Export to file + Add Host

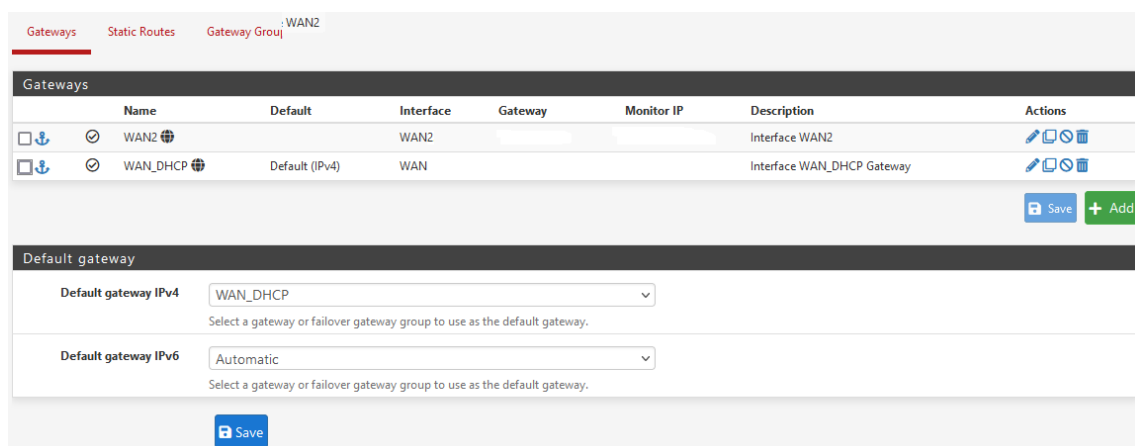
## Paso 2:

Luego en el panel de PfSense nos vamos al Menú de System y escogemos la opción de Routing.



### Paso 3:

En la pestaña de Gateway vas a poder ver las 2 interfaces WAN de los 2 proveedores de internet, puedes seleccionar uno de ellos para que sea tu Gateway por Defecto, ahora nos vamos a la pestaña de Static Routes para crear las rutas y seleccionamos en el botón de Agregar.



### Paso 4:

Ahora agregamos el nombre del Alias creado anteriormente donde están la paginas web, el Gateway selecciona la Wan del segundo proveedor, también agregamos una descripción, por último seleccionamos en el botón Save.



Edit Route Entry

Destination network

WEBSGWN2

/
32

Destination network for this static route

Gateway

WAN2

Choose which gateway this route applies to or [add a new one first](#)

Disabled

☐ Disable this static route

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

Description

SALIDA DE PAGINAS WEB POR WAN2

A description may be entered here for administrative reference (not parsed).

Save

## Paso 5:

Una vez creado la ruta estática seleccionas en Aplicar los cambios para que se guarde en el Pfsense, ahora al consultar la página vas a poder ver que internamente sale por el segundo proveedor, de igual manera puedes crear más rutas estáticas que pueden ir a la WAN principal o a la WAN secundaria.

The static route configuration has been changed.  
The changes must be applied for them to take effect.

Apply Changes

Gateways
Static Routes
Gateway Groups

Static Routes

Network	Gateway	Interface	Description	Actions
websgwan2	WAN2	WAN2	SALIDA DE PAGINAS WEB POR WAN2	
correo_netix	WAN_DHCP	WAN	SALIDA DE CORREO WEB POR WAN_DHCP	

Add

# Como cambiar de proveedor de internet ISP en el Pfsense

Si vas a realizar el cambio en uno de tus proveedores de internet, para no afectar a tus usuarios puedes configurar para que el todo tráfico de red vaya para una sola Wan.

## Paso 1:

En el panel de GateWay si la Red que vas a cambiar es la Wan principal puedes realizar el cambio de Default Gateway para que tu segunda Wan sea ahora el principal, para ellos en el campop Default GateWay Ipv4 seleccionamos la Wan a cambiar luego hacemos click en el botón de Save.

Gateways Static Routes Gateway Groups

Gateways

	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
	WAN2		WAN2			Interface WAN2	
	WAN_DHCP		Default (IPv4)	WAN		Interface WAN_DHCP Gateway	

Save Add

Default gateway

Default gateway IPv4 WAN2  
Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6 Automatic  
Select a gateway or failover gateway group to use as the default gateway.

Save

## Paso 2:

Al aplicar el cambio vemos que la segunda Wan ahora es el Default Gateway, ahora la Wan ya está listo para hacer el cambio de proveedor, también puedes desactivarlo de forma temporal.

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

Apply Changes

Gateways Static Routes Gateway Groups

Gateways

	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
	WAN2		Default (IPv4)	WAN2		Interface WAN2	
	WAN_DHCP		WAN			Interface WAN_DHCP Gateway	

Save Add

Default gateway

Default gateway IPv4 WAN2  
Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6 Automatic  
Select a gateway or failover gateway group to use as the default gateway.

Save

**Paso 3:**

Si tienes Ruta estáticas a la Wan que vas a hacer el cambio de proveedor se sugiere desactivarlo los mismo para en el panel de Static routes seleccionamos en el icono respectivo, ahora la regla va a estar de forma transparente y las paginas se van a redirigir al Wan que se haya declarado como Default Gateway.

System / Routing / Static Routes

The static route configuration has been changed.  
The changes must be applied for them to take effect.

Apply Changes

Gateways

Static Routes

Gateway Groups

Static Routes

	Network	Gateway	Interface	Description	Actions
⊙	websgwan2	WAN2 - 192.168.100.1	WAN	SALIDA DE PAGINAS WEB POR WAN2	<div><div></div><div></div><div></div><div></div></div>
⊙	correo_netix	WAN_DHCP - 192.168.100.1	WAN	SALIDA DE CORREO WEB POR WAN_DHCP	<div><div></div><div></div><div></div><div></div></div>

+ Add