



RFID TRAFFIC ANALYST

 **pfSense**
– GUIA DE USUARIO –

Xavi Conde
Gerard Soteras



Índice

Índice.....	2
¿Qué es pfSense?.....	3
Configuración inicial.....	3
Configuración de las redes en pfSense.....	3
Configuración de la red WAN PortForward.....	6
Configuración del servicio Nginx.....	6
Comprobación.....	7
Configuración OpenVPN.....	8
Instalar el plugin OpenVPN client.....	8
Certificados digitales propios de pfSense.....	9
Creación de CA (Autoridad de Certificación).....	9
Creación de Certificado del servidor OpenVPN.....	9
Configuración del servidor OpenVPN.....	11
Reglas que permitan el acceso al firewall desde el VPN.....	12
Clientes autorizados para usar la VPN.....	14
Conexión VPN desde móvil.....	16



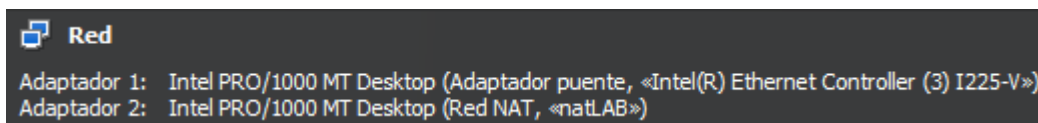
¿Qué es pfSense?

pfSense es una distribución de software basada en FreeBSD utilizada para la implementación de cortafuegos y enrutadores. Se caracteriza por su flexibilidad, seguridad y facilidad de uso, permitiendo a los administradores de red gestionar configuraciones avanzadas a través de una interfaz web intuitiva. Gracias a su amplia compatibilidad con múltiples plataformas y su soporte para plugins y extensiones, pfSense es una solución robusta para redes empresariales y domésticas.

Configuración inicial

Para la instalación de pfSense utilizaremos VirtualBox. Antes de iniciar la máquina virtual, es necesario configurar los adaptadores de red. En esta configuración inicial, agregaremos dos adaptadores:

- Red WAN: Adaptador puente.
- Red LAN: Red NAT.



Configuración de las redes en pfSense

Al iniciar la máquina virtual, aparecerán las direcciones IP asignadas en ambas redes y una lista de opciones numeradas. Para poder entrar en las configuraciones del firewall de manera gráfica antes tenemos que configurar las direcciones IP de las interfaces para poder acceder desde un equipo virtual que se encuentre dentro de la misma red LAN.

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.22/24
LAN (lan)      -> em1      -> v4: 10.20.30.100/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```



Configuración de la interfaz LAN: Para entrar a la configuración LAN pulsamos **2** y nos saldrá una ventana que nos preguntará qué red queremos configurar. Pulsamos nuevamente el **2**. En esta configuración le estamos diciendo que tenga la IP 192.168.56.2, con la que accederemos más adelante desde otro equipo. También vamos a hacer que sea un servidor DHCP para la red.

```
Enter an option: 2

Available interfaces:

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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.20.30.100

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

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

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.20.30.1

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.20.30.150
Enter the end address of the IPv4 client address range: 10.20.30.160
Disabling IPv6 DHCPD...
```

Una vez configuradas las interfaces de red, podemos acceder a la interfaz gráfica de administración de pfSense. Para ello, es necesario utilizar una máquina con entorno gráfico conectada a la red LAN.

Si se requiere acceso desde la red WAN, es posible desactivar temporalmente las restricciones de seguridad utilizando el siguiente comando en pfSense (opción 8 para abrir el terminal):

```
pfctl -d
```

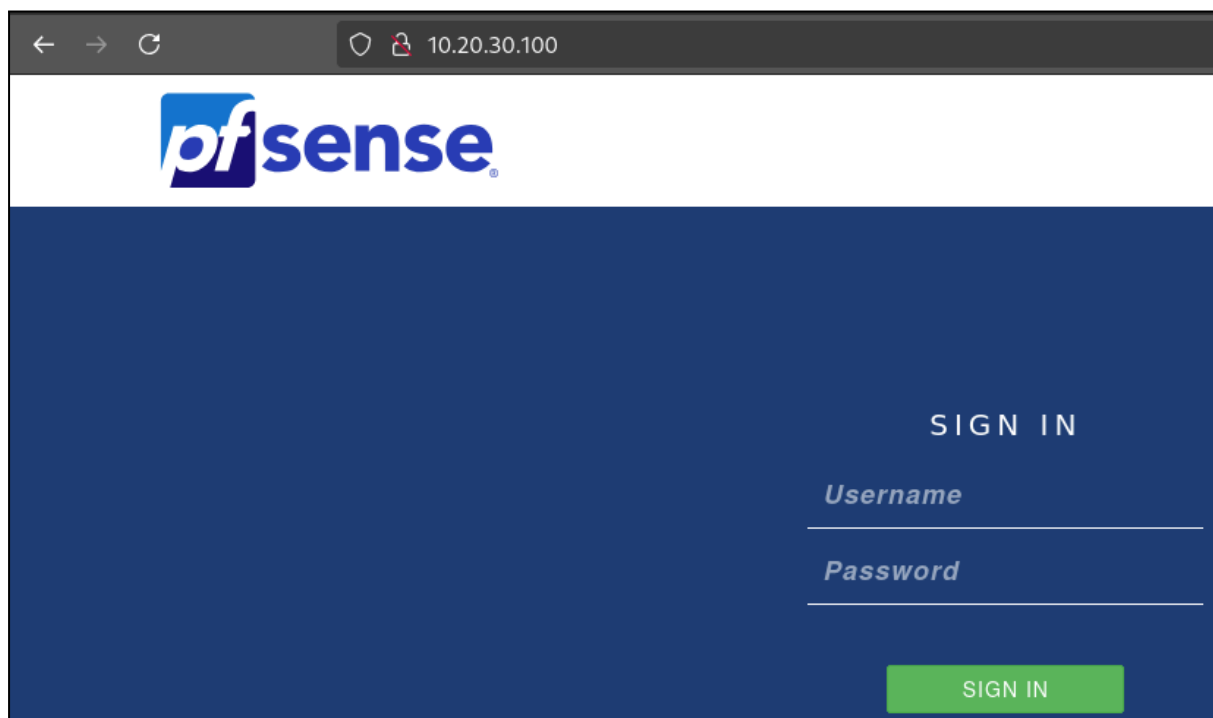
Este comando permite acceder a la interfaz de configuración desde la WAN ingresando la dirección IP correspondiente. Sin embargo, esto representa un riesgo de seguridad, ya que puede abrir una puerta de acceso a usuarios no autorizados.



Desde una máquina en la red LAN, al ingresar la dirección IP de pfSense en un navegador, se mostrará la página de inicio de sesión. Por defecto, las credenciales son:

- **Usuario:** admin
- **Contraseña:** pfsense

Se recomienda cambiar la contraseña inmediatamente después del primer inicio de sesión para mejorar la seguridad del sistema.





Configuración de la red WAN PortForward

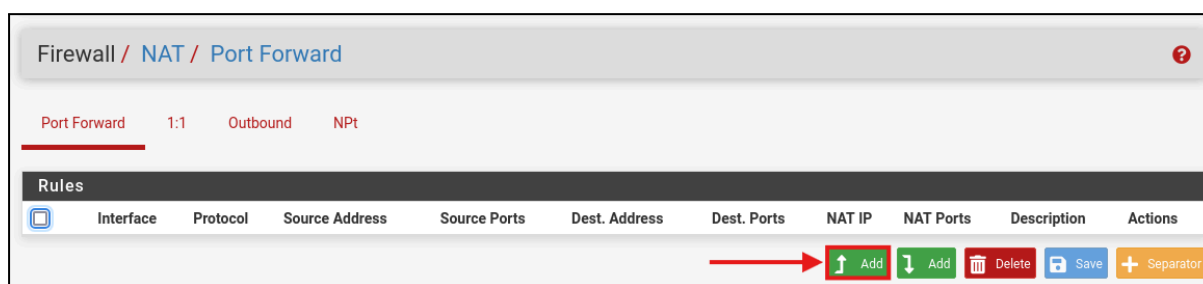
Para configurar la red WAN y poder hacer PortForward, gracias a esto podemos ver una página web alojada en un servidor de nuestra red LAN introduciendo la IP del firewall desde la WAN. Es un reenvío de puertos.

Configuración del servicio Nginx

Si en la red LAN existe un servidor web con Nginx, podemos configurar pfSense para redirigir el tráfico de la WAN hacia dicho servidor. Para ello, realizamos la configuración en la sección de PortForward del firewall:

1. Accedemos a **Firewall** → **NAT** → **PortForward**.
2. Configuramos una nueva regla con los siguientes parámetros:
 - **Interfaz:** WAN
 - **Address family:** IPv4
 - **Protocol:** TCP
 - **Destination:** WAN address
 - **Destination port:** HTTP (puerto 80 por defecto)
 - **Redirect target IP:** single host - (IP donde esté SERVIDOR WEB)
 - **Redirect target port:** HTTP (puerto 80 por defecto)
 - **Description:** regla NAT en WAN

Esta misma regla se creará automáticamente en **Firewall** → **Rules** → **WAN**
Con esta configuración, cualquier solicitud HTTP que llegue a la IP de pfSense en la WN será redirigida al servidor Nginx en la LAN.





Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination ☐ Invert match.
Type Address/mask

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



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



Comprobación

Para verificar que la configuración ha salido correctamente, tendremos que ver la misma página web que se ve en la LAN introduciendo la IP del firewall en la WAN.

Comprobación de la IP del servidor Nginx

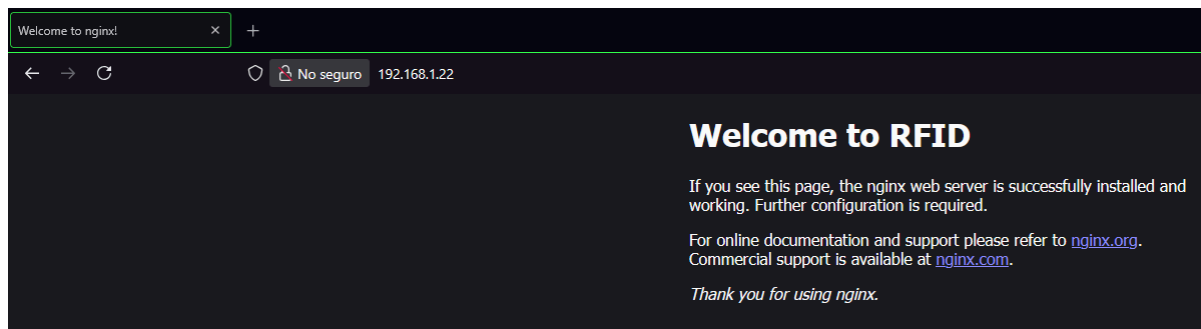
```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e9:ff:89 brd ff:ff:ff:ff:ff:ff
    inet 10.20.30.151/24 brd 10.20.30.255 scope global dynamic enp0s3
        valid_lft 6950sec preferred_lft 6950sec
    inet6 fe80::a00:27ff:fee9:ff89/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```



Comprobación del servicio Nginx activo.

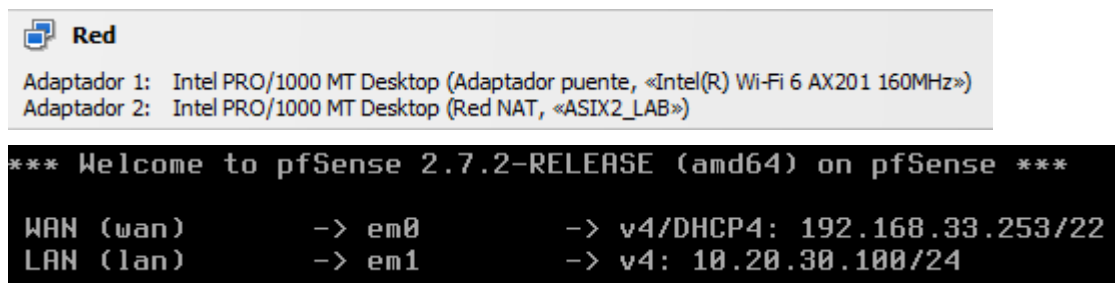
```
• nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-03-09 18:46:06 CET; 2h 34min ago
```

Accedemos a la web desde la red WAN introduciendo la IP WAN de pfSense.



Configuración OpenVPN

Para tener OpenVPN en nuestro firewall debemos instalar el plugin correspondiente a la herramienta VPN y crear un usuario autorizado que pueda establecer conexión. Para este ejemplo cambiaremos el adaptador al del WiFi para poder conectarse por VPN desde el móvil.



Instalar el plugin OpenVPN client

Para instalar el paquete tenemos que ir a **System** → **Package Manager** → **Available Packages**. Aquí buscaremos el paquete llamado: **openvpn-client-export**



System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.

Package Dependencies: [openvpn-client-export-2.6.7](#) [openvpn-2.6.4](#) [zip-3.0_1](#) [7-zip-22.01](#)

Una vez instalado, tendremos que crear certificados digitales para los usuarios.

Certificados digitales propios de pfSense

Para que un usuario pueda acceder por VPN a la red, tendremos que crear unos certificados digitales y configurar una serie de reglas.

Creación de CA (Autoridad de Certificación)

- Nos dirigimos a: **System** → **Certificate Manager**
- Creamos un certificado nuevo
- Rellenamos los datos
- Guardamos

Create / Edit CA

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

Internal Certificate Authority

Common Name

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN_CA	✓	self-signed	2	CN=OpenVPN_CA		

Valid From: Thu, 27 Feb 2025 15:47:02 +0100
Valid Until: Sun, 25 Feb 2035 15:47:02 +0100

Creación de Certificado del servidor OpenVPN

- Nos dirigimos a: **System** → **Certificate Manager** → **Certificates**
- Creamos uno nuevo



- Rellenamos los datos (los de ubicación no son obligatorios)
- Guardamos

Add/Sign a New Certificate

Method

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

Internal Certificate

Certificate authority

Key type

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.

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

Lifetime (days)
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name

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

Country Code

State or Province

City

Organization

Organizational Unit

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. The selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on the certificate.

Alternative Names
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically signing CA may ignore or change these values.

Add SAN Row

OpenVPN_Certificates	OpenVPN_CA	CN=OpenVPN_Certificates		OpenVPN Server	
Server Certificate					
CA: No				Valid From: Thu, 27 Feb 2025 16:02:12 +0100	
Server: Yes				Valid Until: Sun, 25 Feb 2035 16:02:12 +0100	



Configuración del servidor OpenVPN

Nos dirigimos a **VPN** → **OpenVPN** → **Servers**

Añadimos un nuevo certificado.

General Information	
Description	<input type="text" value="OPENVPN_Server"/> <small>A description of this VPN for administrative reference.</small>
Disabled	<input type="checkbox"/> Disable this server <small>Set this option to disable this server without removing it from the list.</small>
Mode Configuration	
Server mode	<input type="text" value="Remote Access (SSL/TLS + User Auth)"/>
Backend for authentication	<input type="text" value="Local Database"/>
Device mode	<input type="text" value="tun - Layer 3 Tunnel Mode"/> <small>"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)</small>
Endpoint Configuration	
Protocol	<input type="text" value="UDP on IPv4 only"/>
Interface	<input type="text" value="WAN"/> <small>The interface or Virtual IP address where OpenVPN will receive client connections.</small>
Local port	<input type="text" value="5194"/> <small>The port used by OpenVPN to receive client connections.</small>
Cryptographic Settings	
TLS Configuration	<input checked="" type="checkbox"/> Use a TLS Key <small>A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from unauthorized connections. The TLS Key does not have any effect on tunnel data.</small>
	<input checked="" type="checkbox"/> Automatically generate a TLS Key.
Peer Certificate Authority	<input type="text" value="OpenVPN_CA"/>
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	<input type="checkbox"/> Check client certificates with OCSP
Server certificate	<input type="text" value="OpenVPN_Certificates (Server: Yes, CA: OpenVPN_CA, In Use)"/> <small>Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA digest algorithms.</small>



Tunnel Settings

IPv4 Tunnel Network

Redirect IPv4 Gateway ☒ Force all client-generated IPv4 traffic through the tunnel.

Inter-client communication ☒ Allow communication between clients connected to this server

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

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security may be necessary in some environments.

Advanced Configuration

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

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TAP packets.
6-11: Debug info range

Una vez configurado, se debe ver algo así:

VPN / OpenVPN / Servers

[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#) [Client Export](#)

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 5194 (TUN)	10.4.44.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OPENVPN_Server	

Reglas que permitan el acceso al firewall desde el VPN

Nos dirigimos a **Firewall** → **Rules** → **WAN** y creamos una nueva regla.



Firewall / Rules / WAN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	10.20.30.20	80 (HTTP)	*	none	NAT portForward de WAN a LAN

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

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

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)

5194

(other)

5194

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

OpenVPN_Rules

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.

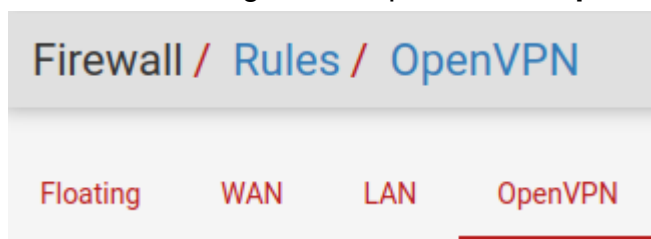
Advanced Options

Display Advanced

Save



Ahora debemos crear otra regla para que se permita todo el tráfico de la VPN.
Para ello nos dirigimos al apartado de **OpenVPN**



Añadimos una nueva regla.

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 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 OpenVPN
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 Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Any Source Address

Destination

Destination ☐ Invert match Any Destination Address

Veremos algo así:

Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	none		OpenVPN_OpenVPN

Cientes autorizados para usar la VPN

Para crear usuarios autorizados nos dirigimos a:

System → User Manager



Lo más importante de este paso es activar la opción:

- Click to create a user certificate

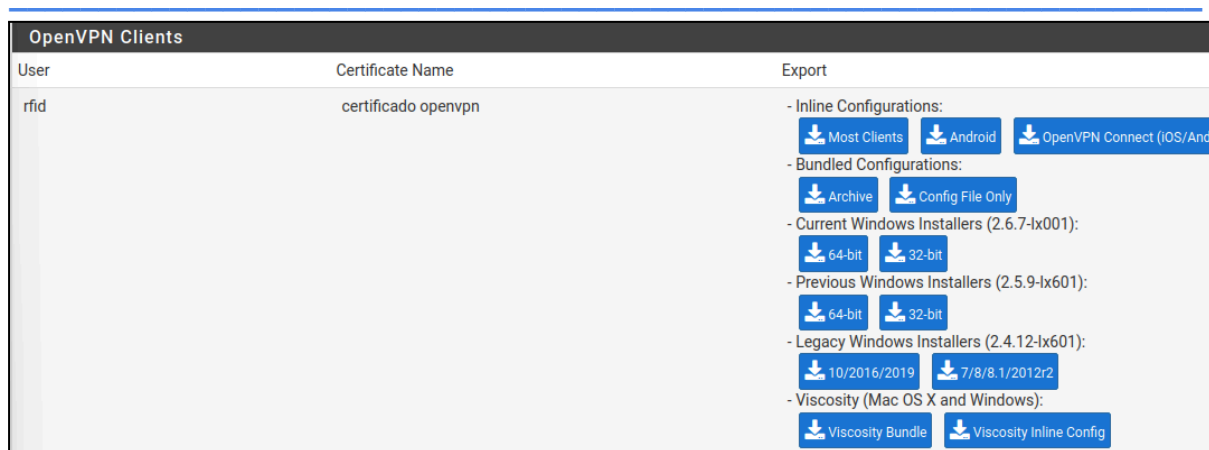
User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="rfid"/>
Password	<input type="password" value="*****"/> <input type="password" value="*****"/>
Full name	<input type="text" value="rfid"/> <small>User's full name, for administrative 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"/> Not member of</div> <div><input type="text"/> Member of</div>
<div><input type="button" value="» Move to 'Member of' list"/> <input type="button" value="« Move to 'Not member of' list"/></div> <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>	
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate

Create Certificate for User	
Descriptive name	<input type="text" value="certificado openvpn"/>
Certificate authority	<input type="text" value="OpenVPN_CA"/>
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"/>

Una vez creado el usuario, tendremos que exportar el archivo del cliente.

Para ello nos dirigimos **VPN → OpenVPN → Client Export**

Buscamos por el final de la página hasta el apartado **OpenVPN Clients**

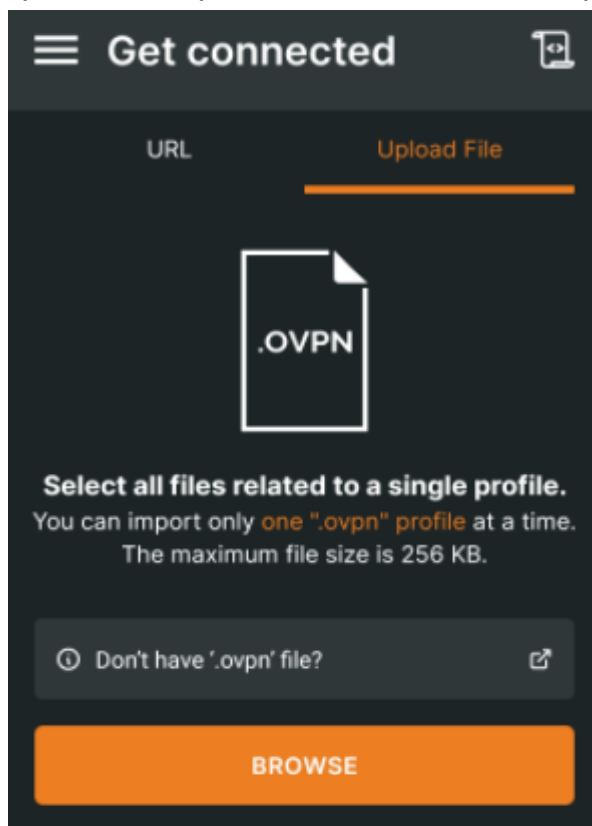


Descargamos el archivo que más convenga. En este caso descargamos el de Android y haremos la conexión a través del móvil. Para ello tendremos que descargar en el dispositivo la aplicación **OpenVPNConnect**.



Conexión VPN desde móvil

Una vez pasamos el archivo que se nos descarga al móvil e instalamos la aplicación, importamos el archivo en el apartado **Upload File** → **Browse**





Cuando añadimos el archivo, introducimos el nombre y contraseña del usuario autorizado. Para verificar que todo funciona correctamente, podemos buscar la IP WAN de pfSense. Si logramos ver la pantalla de acceso del firewall, podremos concluir con las configuraciones.

