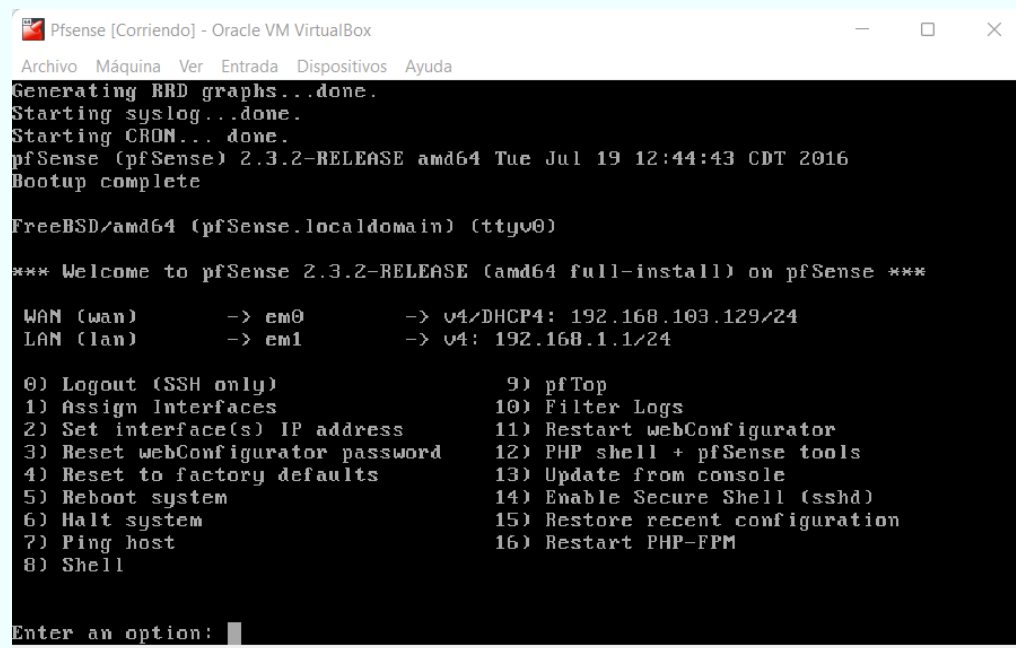


CONFIGURACIÓN DE AUTENTICACIÓN RADIUS



SEGURIDAD INFORMÁTICA
JUAN CARLOS NAVIDAD GARCÍA

1. Configuración de Pfsense:



Una vez iniciado **Pfsense**, nos encontraremos con que nos listará unas opciones, de las cuáles solo tocaremos la **segunda**.

La **segunda opción** sirve para **configurar y asignar las direcciones IP** a los adaptadores de red.

De los cuales tenemos dos, uno que nos proporcionará **conexión a internet y que está conectado mediante DHCP** y otro adaptador conectado a un **segmento de LAN que sería equivalente a una red NAT en VirtualBox**, este adaptador se configuraría con la **IP estática**.

Así que, como ya he dicho, escribiremos el número **dos** para seleccionar la opción.

Enter an option: 2

Nos preguntará por la interfaz de red que queremos configurar, en nuestro caso solo configuraremos la segundo, la **LAN**, está es la interfaz por la que va a salir el servidor **Pfsense**.

Seleccionaremos la interfaz también escribiendo el número **2**:

```
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

Continuando, nos pedirá la **dirección IP** que le queremos asignar a la interfaz, le podemos asignar cualquier dirección, en mi caso le he asignado la **192.168.1.1** que pertenece a la red interna.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1
```

Después, nos pedirá la **máscara de subred** en la que nos encontramos, como ya he dicho es la **/24**, así que escribiremos **24**:

```
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 31):
> 24
```

En las opciones **"For a LAN, press <Enter> for none"** y **"Enter the new LAN IPv6 address, press <Enter> for none"** pulsaremos **Enter** para saltar, ya que no a configurar las **direcciones IPv6**.

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

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

Por último, nos preguntará si queremos configurar el **servidor DHCP**, en nuestro caso lo necesitaremos para que funcione el **portal cautivo**, así que lo configuraremos.

Para habilitarlo pulsaremos la tecla **"Y"**, e introduciremos el rango de **IPs** que puede asignar nuestro **servidor DHCP**:

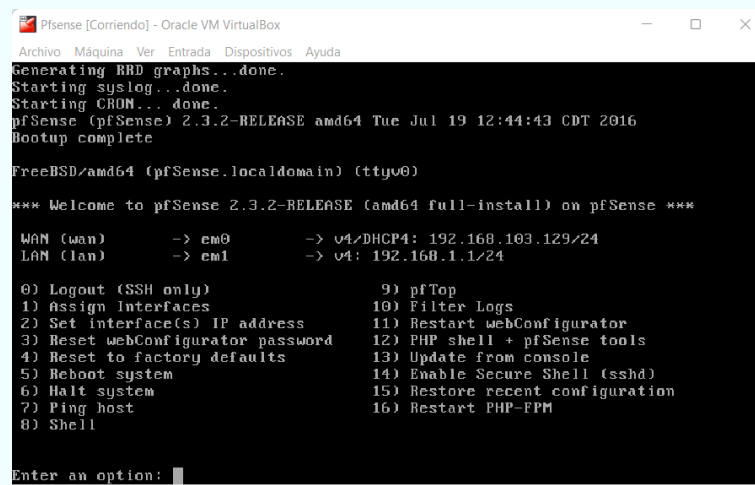
```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.100
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Finalmente, nos preguntará si queremos que el **protocolo Web** sea **HTTP** y le diremos que si dando a la tecla **"Y"**.

Después de todo, acabaremos con la configuración de la interfaz y podremos acceder a **Pfsense**.

```
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://192.168.1.1/
Press <ENTER> to continue.
```

Reiniciaremos la máquina para que se apliquen bien los cambios y nos daremos cuenta de que, al reiniciar, nos saldrá la dirección IP que le hemos asignado a la interfaz "**LAN**":



```
Pfsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Tue Jul 19 12:44:43 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.103.129/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

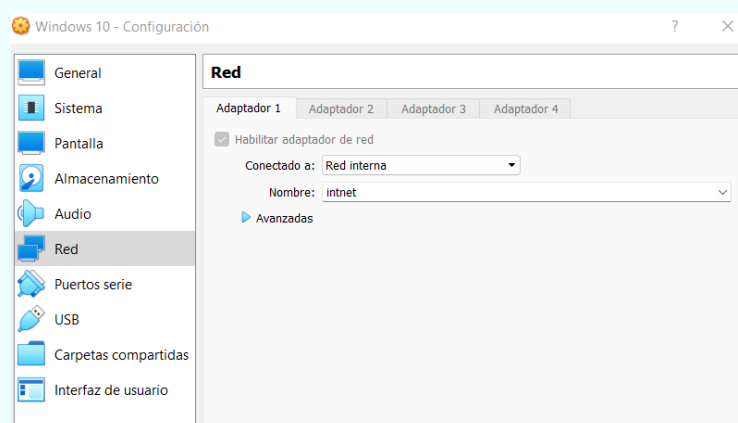
Enter an option:
```

Esta dirección IP será la que utilizaremos para acceder al **configurador Web de Pfsense**.

2. Configuración inicial de Pfsense:

Para crear el **portal cautivo** y realizar las diversas configuraciones que quedan en **Pfsense** necesitaremos otra máquina (cliente) en la misma red.

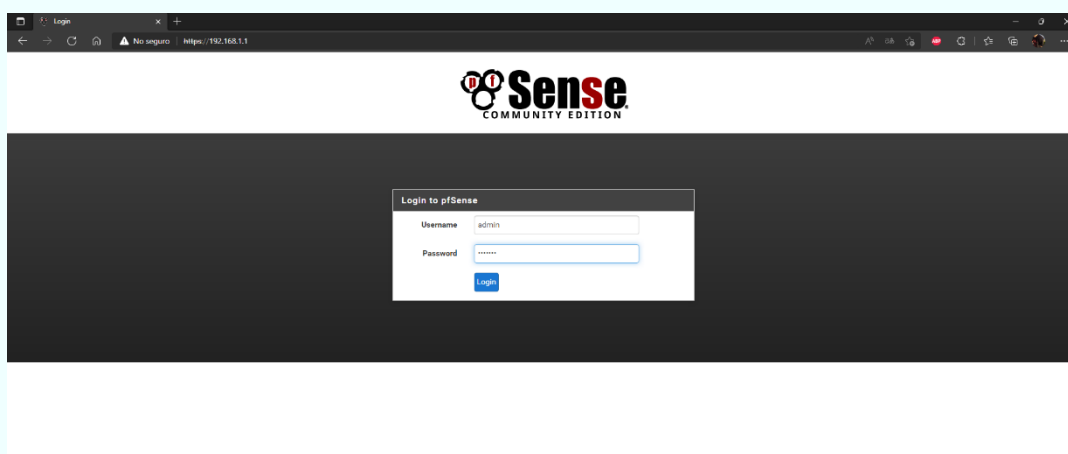
Para esto he utilizado una máquina virtual con **Windows 10** también configurada la red como **"Red Interna"**.



Iniciaremos la máquina virtual e ingresaremos en el navegador;

En la barra de búsqueda insertaremos la **IP configurada anteriormente**, en mi caso la **192.168.1.1**.

Una vez dentro nos pedirá **iniciar sesión**, el usuario y la contraseña por defecto son **usuario: admin ; contraseña: pfsense**

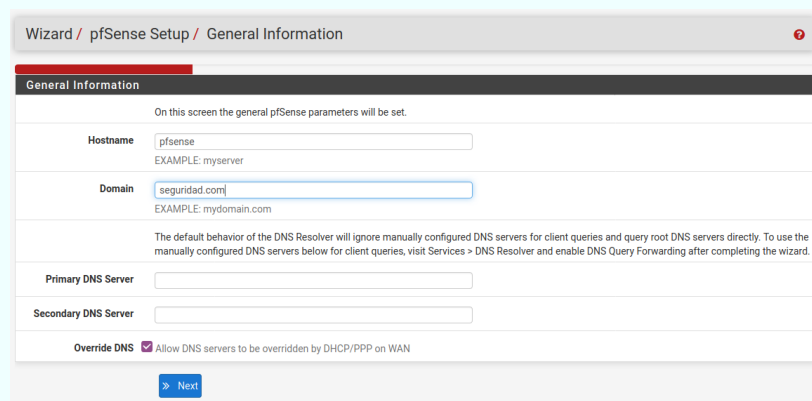


Una vez iniciada la sesión, comenzará el **setup** de la configuración web de **Pfsense**:



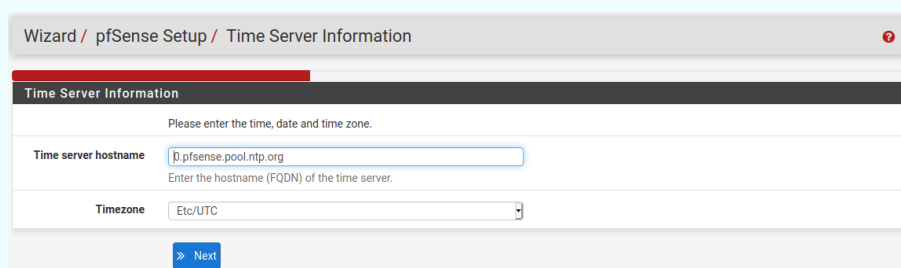
The screenshot shows the 'Wizard / pfSense Setup' window. The title bar includes a help icon. Below the title bar is a dark header with 'pfSense Setup'. The main content area has a light pink background and contains the following text: 'This wizard will provide guidance through the initial configuration of pfSense.' and 'The wizard may be stopped at any time by clicking the logo image at the top of the screen.' At the bottom, there is a blue button with a right arrow and the text 'Next'.

Lo primero sería darle un **nombre de dominio a Pfsense**, no tendríamos que tocar nada más de esa pantalla, aunque si queremos podemos añadir **direcciones DNS**, aunque no es necesario.



The screenshot shows the 'Wizard / pfSense Setup / General Information' window. The title bar includes a help icon. Below the title bar is a dark header with 'General Information'. The main content area has a light pink background and contains the following text: 'On this screen the general pfSense parameters will be set.' Below this, there are two input fields: 'Hostname' with the value 'pfsense' and 'Domain' with the value 'seguridad.com'. Below these are two more input fields: 'Primary DNS Server' and 'Secondary DNS Server'. At the bottom, there is a checkbox labeled 'Override DNS' which is checked, and a blue button with a right arrow and the text 'Next'.

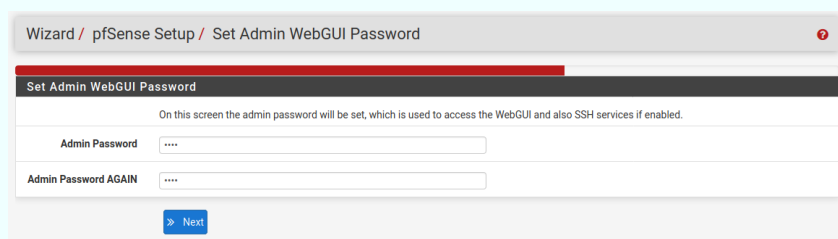
A continuación, nos aparecerá la selección del **servidor de horario** y nuestra **zona horaria**, todo lo dejaremos **por defecto**, no tocaremos nada.



The screenshot shows the 'Wizard / pfSense Setup / Time Server Information' window. The title bar includes a help icon. Below the title bar is a dark header with 'Time Server Information'. The main content area has a light pink background and contains the following text: 'Please enter the time, date and time zone.' Below this, there are two input fields: 'Time server hostname' with the value 'p.pfsense.pool.ntp.org' and 'Timezone' with the value 'Etc/UTC'. At the bottom, there is a blue button with a right arrow and the text 'Next'.

Los siguientes dos apartados serán sobre la **configuración de las interfaces de red**, las cuales ya hemos configurado **manualmente** en pasos anteriores. Así que también se dejará todo tal cual está.

Para finalizar, nos hará introducir una **nueva contraseña para el usuario administrador**, para que no se quedé la contraseña por defecto.



Wizard / pfSense Setup / Set Admin WebGUI Password

Set Admin WebGUI Password

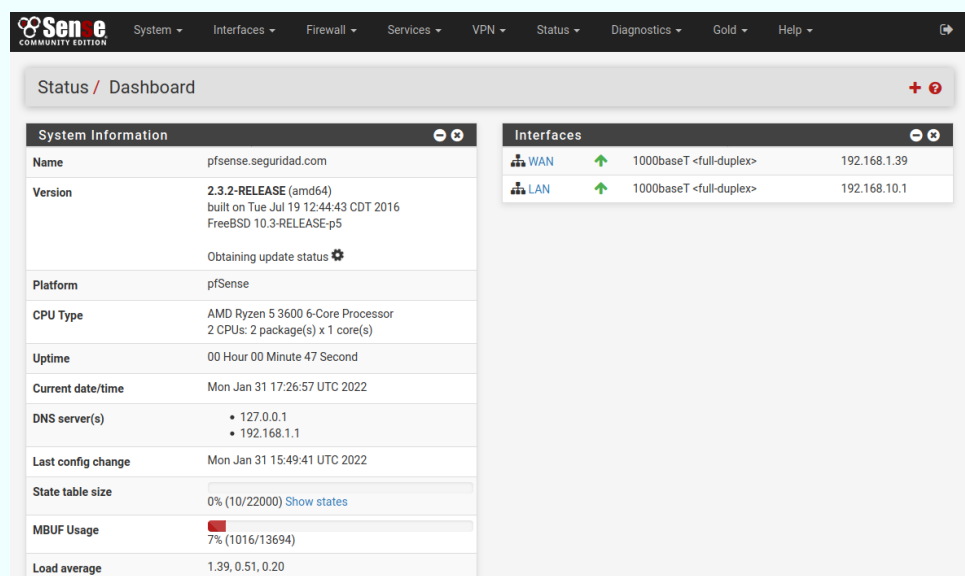
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

Admin Password AGAIN:

[Next](#)

Una vez introducida la nueva contraseña, se nos abrirá el **panel principal de Pfsense**:



Status / Dashboard

System Information

Name	pfSense.seguridad.com
Version	2.3.2-RELEASE (amd64) built on Tue Jul 19 12:44:43 CDT 2016 FreeBSD 10.3-RELEASE-p5 Obtaining update status
Platform	pfSense
CPU Type	AMD Ryzen 5 3600 6-Core Processor 2 CPUs: 2 package(s) x 1 core(s)
Uptime	00 Hour 00 Minute 47 Second
Current date/time	Mon Jan 31 17:26:57 UTC 2022
DNS server(s)	• 127.0.0.1 • 192.168.1.1
Last config change	Mon Jan 31 15:49:41 UTC 2022
State table size	0% (10/22000) Show states
MBUF Usage	7% (1016/13694)
Load average	1.39, 0.51, 0.20

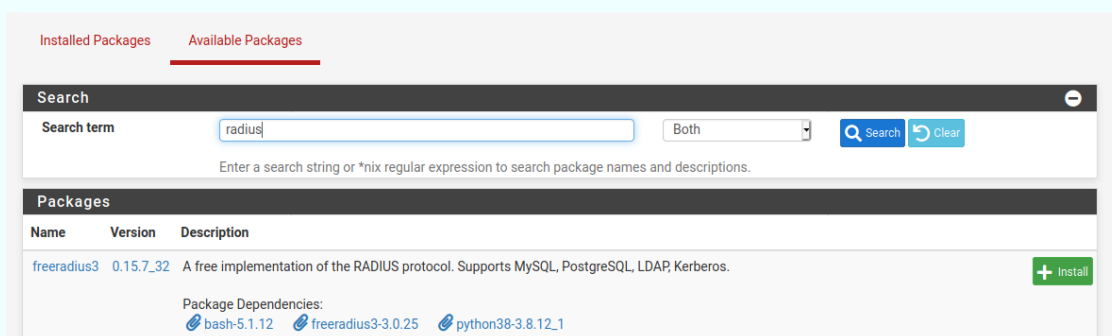
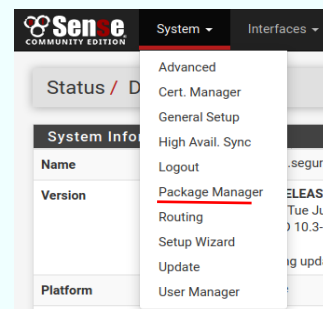
Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.1.39
LAN	↑	1000baseT <full-duplex>	192.168.10.1

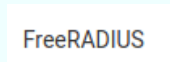
3. Instalación del paquete FreeRADIUS

FreeRADIUS no viene directamente incluido en **Pfsense**, por lo que hay que instalarlo desde el administrador de paquetes.

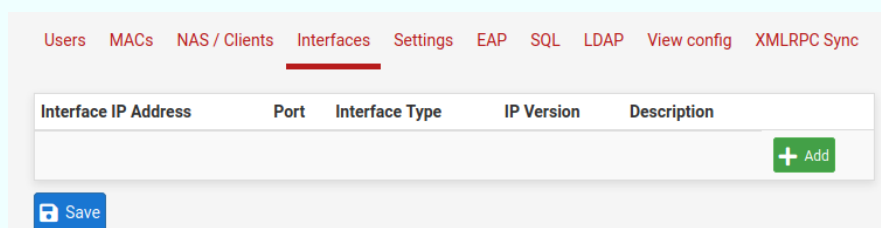
Entonces nos iremos a **sistema** → **Administrador de paquetes**. Y dentro del administrador de paquetes nos iremos a paquetes disponibles. Buscaremos **RADIUS** y le daremos a instalar:



Una vez esté instalado, el **FreeRadius** se va a encontrar en el apartado de Servicios como **FreeRadius**.



Cuando estemos dentro del **FreeRadius**, lo primero que haremos será añadir una nueva interfaz desde el apartado de interfaces:



En la dirección IP, debemos de poner la de nuestro servidor, todo lo demás lo dejamos tal cual viene, por último, le daremos a **Save**.

The screenshot shows the 'General Configuration' form for an interface. The form has a light gray header with the title 'General Configuration'. Below the header, there are several input fields and dropdown menus. The 'Interface IP Address' field is set to '192.168.1.1'. The 'Port' field is set to '1812'. The 'Interface Type' dropdown is set to 'Authentication'. The 'IP Version' dropdown is set to 'IPv4'. The 'Description' field is empty. At the bottom of the form, there is a blue 'Save' button.

Posteriormente nos iremos al apartado de **NAS / Clients**, en el configuraremos los clientes y añadiremos un cliente:

The screenshot shows the 'NAS / Clients' table. The table has a light gray header with the title 'NAS / Clients'. Below the header, there is a table with the following columns: 'Client IP Address', 'Client IP Version', 'Client Shortname', 'Client Protocol', 'Client Type', 'Require Message Authenticator', 'Max Connections', and 'Description'. The table is currently empty. At the bottom of the table, there is a green '+ Add' button. Below the table, there is a blue 'Save' button.

En la dirección IP también ponemos la de nuestro servidor, en el nombre corto del cliente le asignamos uno cualquiera y por último, le asignaremos una contraseña, eso es lo único que habría que hacer:

The screenshot shows the 'General Configuration' section for a new client in the FreeRADIUS web interface. The navigation bar at the top includes: Users, MACs, **NAS / Clients**, Interfaces, Settings, EAP, SQL, LDAP, View config, and XMLRPC Sync. The configuration fields are as follows:

- Client IP Address:** 192.168.1.1. Description: Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).
- Client IP Version:** IPv4.
- Client Shortname:** jnav. Description: Enter a short name for the client. This is generally the hostname of the NAS.
- Client Shared Secret:** Description: Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret. Warning: Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\).

Cuando tengamos configurados los clientes, configuraremos los usuarios desde el mismo apartado de usuarios.

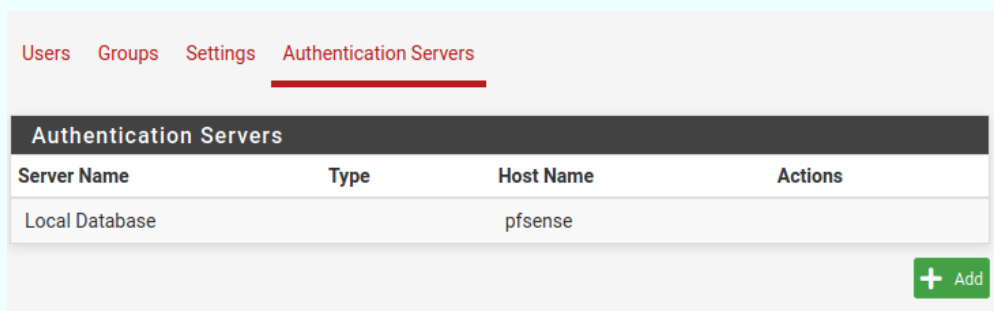
The screenshot shows the 'Users' section of the FreeRADIUS web interface. The navigation bar is the same as the previous screenshot. Below the navigation bar, there is a filter section with a dropdown for 'Filter by:' (showing A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z), a 'Filter field:' dropdown (set to 'Username'), and a 'Filter text:' input field. Below this is a table with columns: Username, Password, Use One Time, Simult. Connections, IP Address, Expiration Date, Session Timeout, Possible Login Times, VLAN ID, and Description. There is a '+ Add' button at the bottom right of the table and a 'Save' button at the bottom left.

The screenshot shows the 'General Configuration' section for a new user in the FreeRADIUS web interface. The navigation bar is the same as the previous screenshots. The configuration fields are as follows:

- Username:** jnav. Description: Enter the username. Whitespace is allowed. Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.
- Password:** Description: Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.
- Password Encryption:** Cleartext-Password. Description: Select the password encryption for this user. If the (pre-hashed) options are used, the password should already be hashed by the expected hash function. Note that not all authentication protocols are compatible with all types of hashed passwords. Default: Cleartext-Password.

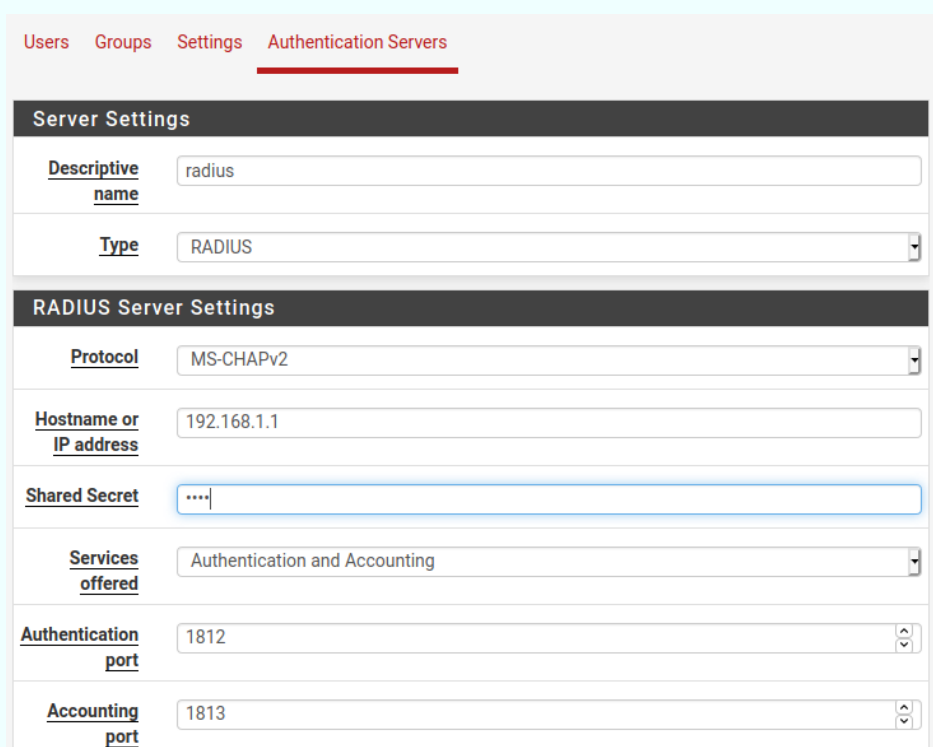
Únicamente pondremos el nombre de usuario y la contraseña, todo lo demás se deja por defecto.

Vamos a añadir un servidor, para ello accedemos a **system** → **user manager** → **authentication servers**.



Users Groups Settings Authentication Servers			
Authentication Servers			
Server Name	Type	Host Name	Actions
Local Database		pfsense	
			+ Add

Le asignaremos un nombre al servidor, le diremos que es de tipo **RADIUS**, le pondremos nuestra dirección IP de servidor y por último, una contraseña..



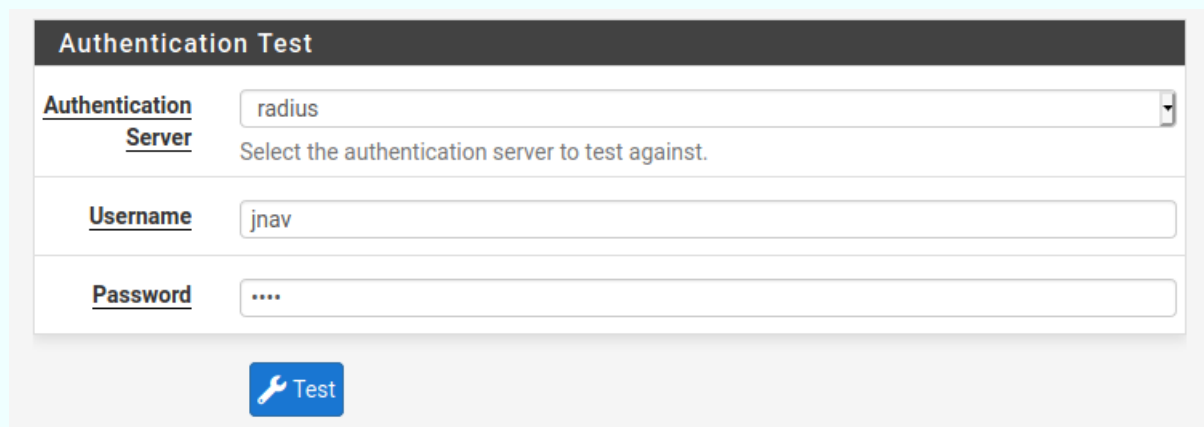
Users Groups Settings Authentication Servers	
Server Settings	
<u>Descriptive name</u>	radius
<u>Type</u>	RADIUS
RADIUS Server Settings	
<u>Protocol</u>	MS-CHAPv2
<u>Hostname or IP address</u>	192.168.1.1
<u>Shared Secret</u>
<u>Services offered</u>	Authentication and Accounting
<u>Authentication port</u>	1812
<u>Accounting port</u>	1813

Con todo esto ya hecho, le daremos a guardar para que todo funcione correctamente.

4. Comprobación:

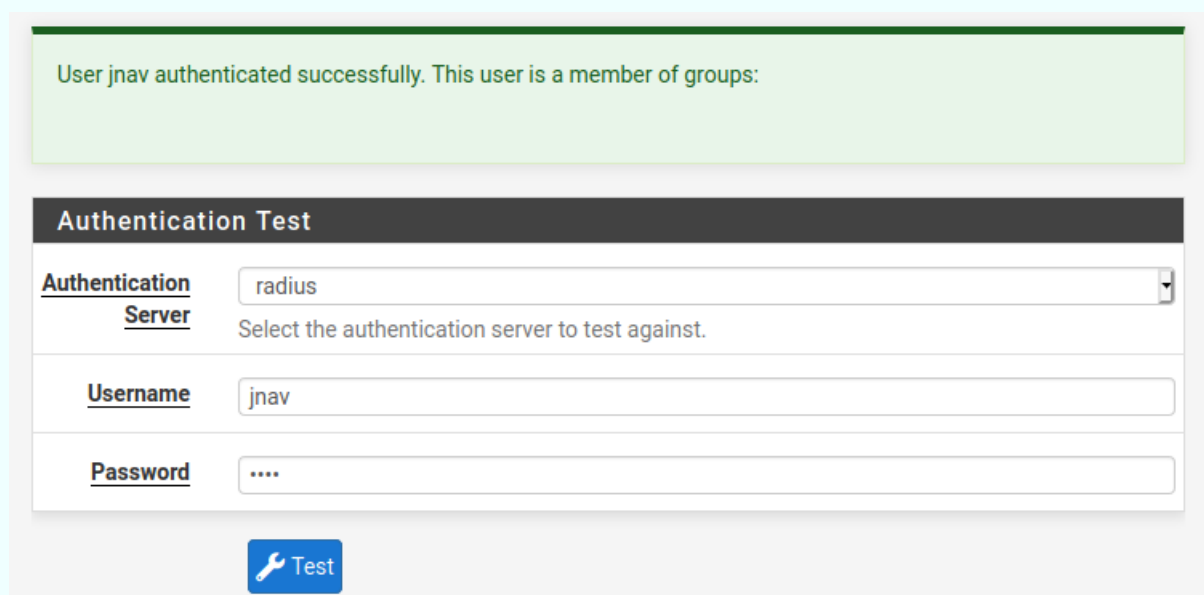
Para comprobar que el **Radius** funciona, nos iremos al apartado **Diagnostics** → **Authentication**-

Desde ahí podemos hacer las pruebas de inicio de sesión con **Radius**, así en **Authentication Server** seleccionaremos **RADIUS** y más abajo el nombre y contraseña que hemos configurado anteriormente.



The screenshot shows the 'Authentication Test' window. It has a dark header with the title 'Authentication Test'. Below the header, there are three input fields: 'Authentication Server' with a dropdown menu showing 'radius', 'Username' with the text 'jnav', and 'Password' with masked characters '....'. Below these fields is a blue button with a wrench icon and the text 'Test'. A small instruction text 'Select the authentication server to test against.' is located below the 'Authentication Server' dropdown.

Si todo está correcto, nos saldrá un mensaje que nos dirá que nuestro usuario está **autenticado**:



This screenshot shows the same 'Authentication Test' window as before, but with an additional green message box at the top. The message box contains the text: 'User jnav authenticated successfully. This user is a member of groups:'. The form fields and the 'Test' button remain the same as in the previous screenshot.