# Proyecto Integrado:

# Implantación de un portal cautivo con autenticación Radius




Gemner Vanhe Diaz Rodriguez

2º ASIR

I.E.S. Juan de la Cierva

# ÍNDICE

# 1. INTRODUCCIÓN Y OBJETIVOS

## 1.1. Introducción / Propuesta detallada

Actualmente, en la empresa que trabajo hay una misma conexión Wi-Fi para trabajadores y visitantes (clientes), la contraseña de la red está a conocimiento de toda persona que se acerque a la empresa, puede verla y conectarse.

Yo veo esto muy desordenado y poco seguro, así que se me ha ocurrido la idea de crear una especie de "recepción" para que todo usuario que se quiera conectar, primero se autentique.

Sin embargo, según el tipo de usuario, me gustaría crear varios grupos.
Por ejemplo, según el usuario, crearía estos 5 grupos:

1) Para los técnicos que trabajan fuera
2) Para los técnicos que permanecen dentro de la empresa
3) Para el jefe y el personal de oficina
4) Para los practicantes y alumnos (como yo)
5) Para los clientes y visitantes

De esta manera, se puede tener un control exhaustivo de cada conexión a internet y de donde proviene. Pudiendo así, mejorar la seguridad de la empresa.

Todo esto lo puedo llevar a cabo por medio de un portal cautivo con autenticación RADIUS, en un sistema operativo basado en Linux (FreeBSD), llamado PfSense - versión 2.6.0.

En principio, desarrollaré el proyecto en una máquina virtual en VMWARE, para poder demostrar la eficacia y funcionalidad, y así, poder llevarlo a cabo en un entorno productivo.

## 1.2. ¿Qué es un portal cautivo?

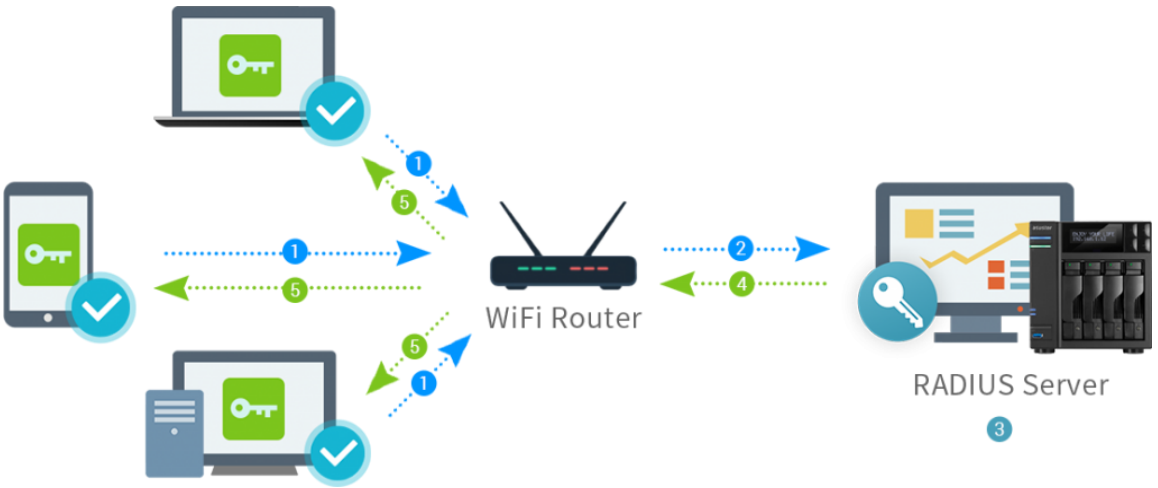
Un portal cautivo es una herramienta que permite controlar y gestionar el acceso a redes WiFi a través de un proceso de autenticación o login. Mediante este sistema es posible recoger información sobre los usuarios.




Esta imagen puede ser un ejemplo de cómo se vería un portal cautivo como yo quiero que quede.

## 1.3. ¿Qué es RADIUS?

RADIUS es un protocolo que destaca por ofrecer un mecanismo de seguridad, flexibilidad, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red. Es un protocolo de autenticación y autorización para el acceso a la red, este protocolo utiliza un esquema cliente-servidor. En la imagen se ve como funciona:



## 1.4. Objetivos:

El objetivo, es hacer que la red Wi-Fi de la compañía cuente con un portal cautivo y autenticación RADIUS para:

- Ofrecer una red segura, tanto a trabajadores como a clientes.
- Proteger la información personal, que es utilizada por la empresa.
- Monitoreo y control de cada usuario conectado en la red
- Hacer uso de soluciones que implementan la posibilidad de cifrado asimétrico con Transport Layer Security (TLS)
- Innovar con una implantación de un portal cautivo, con el que no cuenta la empresa actualmente.
- Evitar intrusos o personas que utilicen el internet sin medida y puedan causar fallos o ralentización del mismo.
- Si alguien comete un delito, queda registrado el usuario que lo hizo.

## 1.3 Justificación:

La justificación de mi proyecto se basa en que noto la inseguridad de tener una red Wi-Fi sin ningún tipo de control ni seguridad. Es vulnerable a cualquier ataque de cualquier "cliente" u otra persona que tenga malas intenciones. Incluso de una persona sin maldad que simplemente por falta de conocimiento pueda ocasionar problemas en la red de la compañía y esto desencadene problemas mayores.

Hace falta tener un mínimo de revisión y seguridad cuando se tiene una red de tamaño considerable. Al encontrarme con este panorama, decidí que quería ayudarles a monitorear su red con dicho portal.

## 1.4 Planificación temporal:

Mi proyecto lo voy a dividir en 3 fases, las cuales van a ser:

1) **FASE:** Desarrollo de la documentación inicial como esta, todo lo relacionado al comienzo del proyecto, como por ejemplo, los puntos [ 1 ] y [ 2 ]. Además quisiera empezar lo práctico con un par de capturas de pantalla y alguna anotación.
   Esto lo he de entregar en la primera revisión para mi tutor.

2) **FASE:** Desarrollar lo práctico y que esté casi terminado y a ser posible funcionando correctamente. Documentación de lo práctico explicado en la memoria con sus respectivas capturas de pantalla y demás información de interés adjuntada al documento.
   Esto lo he de entregar en la segunda revisión para mi tutor.

3) **FASE:** El proyecto está terminado y documentado, funciona correctamente y hace lo que quiero. Hecho en mi entorno y no en producción por la seguridad de mi empresa.
   Me gustaría desarrollar mi proyecto en producción pero necesito el consentimiento de mi empresa una vez esté terminado y aprobado por mi institución educativa.
   Además de las posibles mejoras que se me puedan ir ocurriendo a lo largo del proyecto.

| 1ª FASE | 2ª FASE | 3ª FASE |
|---|---|---|
| Documentación | Práctica | Funcionamiento |

# 2. DISEÑO DEL ENTORNO DE TRABAJO

## 2.1 Especificación de requisitos:

Para desarrollar mi proyecto solamente es necesario contar con lo siguiente:

- Conexión a internet - red Wi-Fi.
- Banda ancha mínima de 100Mb.
- Un ordenador, Raspberry Pi o una máquina virtual (VMware, VirtualBox...) con las siguientes características:
  - Mínimo 256Mb de memoria RAM
  - Mínimo 20Gb de disco duro
  - 1 o 2 tarjetas de red
- Una versión estable de **PfSense** (2.6.0) en mi caso.
- Un programa para editar código **HTML**.

## 2.2 Especificación de mis herramientas:

Voy a desarrollar mi proyecto en un ordenador con las siguientes características:

- Tipo: Laptop
- Marca: HP
- Modelo: 15-da0012ns
- Procesador: Intel(R) Celeron(R) N4000 CPU: @ 1.10GHz~1.1GHz
- Memoria RAM: 8,00 GB (7,83 GB usables)
- Disco duro: 1 TB HDD (913 GB usables)
- Sistema operativo: Windows 11 Home (21H2)
- Arquitectura de S.O. y procesador: x64 bits
- Gráfica: Intel(R) UHD Graphics 600

## 2.3 Seguridad y alta disponibilidad

En la medida de lo posible, desarrollaré el proyecto pensando como si estuviera en producción para ir con precaución y no dejar cabos sueltos.

- Dificultad en las contraseñas utilizadas cuando sean necesarias.
- No utilizar usuarios comunes que sean fáciles de atacar con un diccionario.
- Implementar RADIUS, obviamente.
- Uso exclusivo de 1 persona o 2 del S.O. que administra todo.
- Vigilar comportamientos extraños en la red.
- Limitar el ancho de banda para evitar desbalances.
- Contar con una copia de seguridad completa del sistema operativo, además de ir haciendo copias incrementales para tener seguros los usuarios que sean creados y el historial de estos.

## 2.4 Evaluación de costes

Desarrollar este proyecto no es nada caro, cualquier ordenador que ya poseas aunque sea antiguo sirve para esto, sin embargo si quieres desarrollarlo en una **Raspberry Pi**, puedes conseguir una con el hardware necesario entre 35€ y 50€ en internet.
El sistema operativo **PfSense** es gratuito y **VMware** en su versión de uso doméstico y/o estudiantil es gratuito. Si deseas comprar la licencia para el uso profesional en una compañía cuesta alrededor de $200 (175€).
Sin embargo, software de código abierto como **VirtualBox** es completamente gratuito.

| Servidor | Servidor | Servidor | Servidor | Servidor | S.O. | S.O. |
|---|---|---|---|---|---|---|
| PC propio | Raspberry Pi | VMware NO PRO | VMware PRO | Virtual Box | PfSense | UNIX |
| 0,00€ | 35,00€ - 50,00€ | 0,00€ | 175€ ($200) | 0,00€ | 0,00€ | 0,00€ |

En definitiva, como mínimo puedes no tener que gastar nada, **0,00€** para implementar este proyecto tanto en práctica como en producción.

O como máximo, comprando una Raspberry Pi y pagando la licencia de VMWARE, un máximo de **225,00€**.

### 2.5 Herramientas de desarrollo y/o software

- He de utilizar **Visual Studio Code** que es un editor de código fuente para crear o editar los documentos **HTML** del Portal C.
- **VMware 16.0** Workstation Player Evaluation (free), será el servidor que nos alojara el S.O. → PfSense

## 3. IMPLANTACIÓN / INSTALACIÓN

### 3.1 Descargas

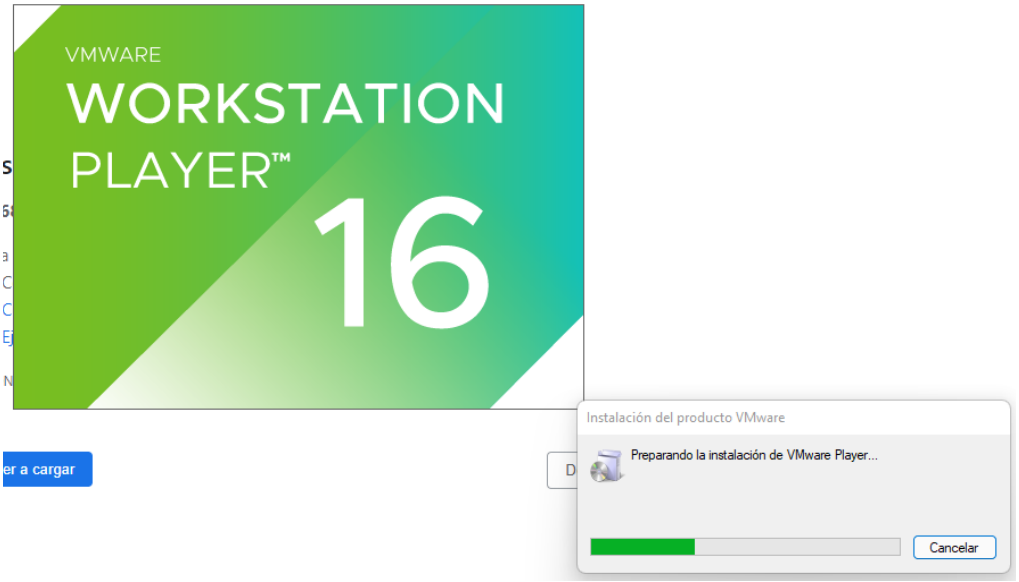
En primer lugar, y en mi caso que lo haré en una máquina virtual, he de descargar:

- VMware Workstation 16.0 o VirtualBox
- PfSense 2.6.0
- Visual Studio Code
- Imágenes para la estetica del código HTML

## 3.2 Instalación

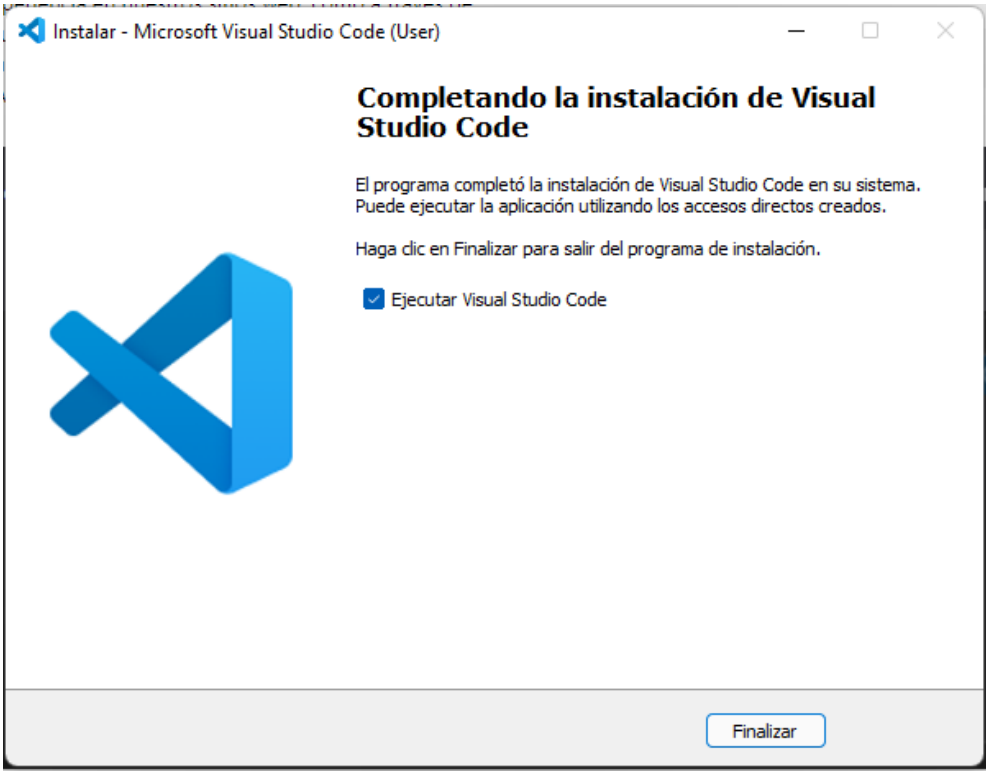
En primer lugar instalamos,

**1) VMware 16.0 Workstation:**

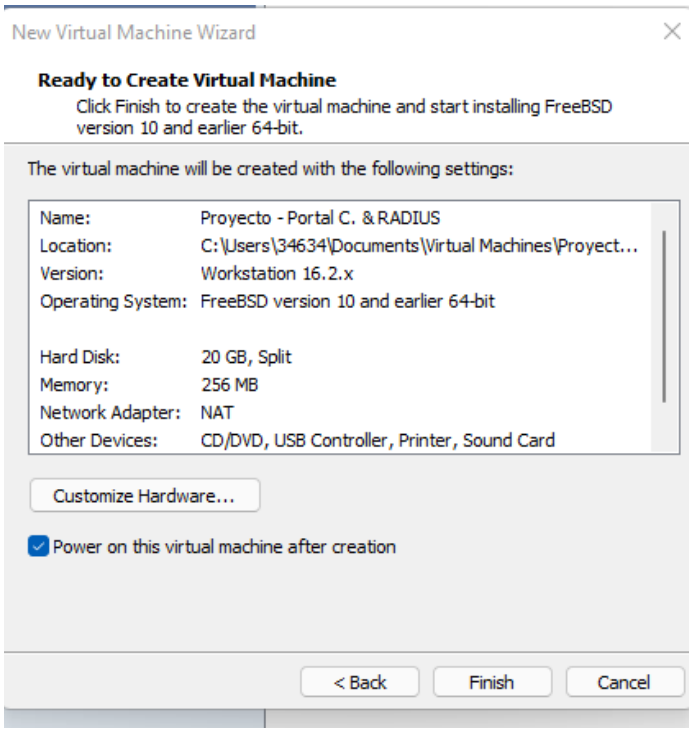


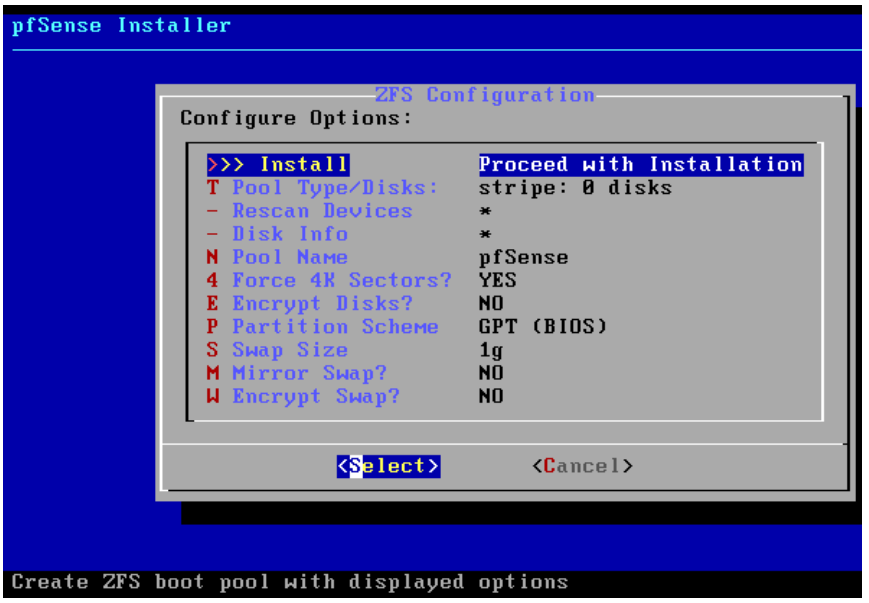

Luego instalamos,

**2) Visual Studio Code:**

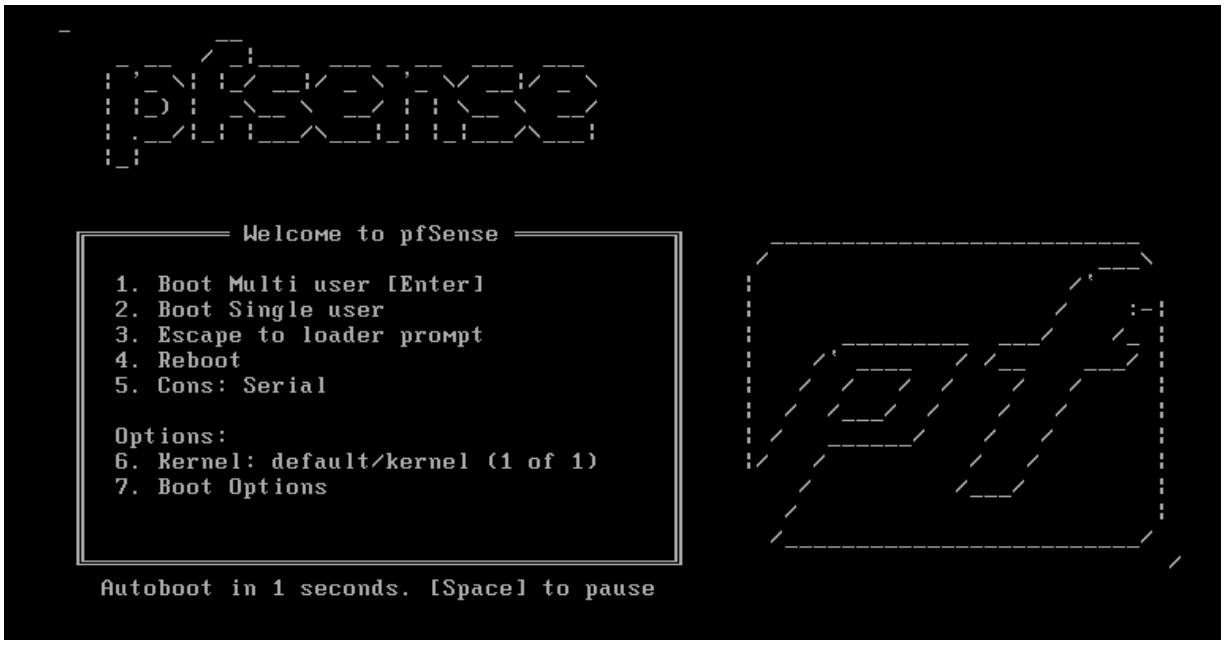


3) **PfSense**, que lo instalamos como ISO en VMware:




Ya instalado, veremos la siguiente ventana y por defecto es el **[1]**.



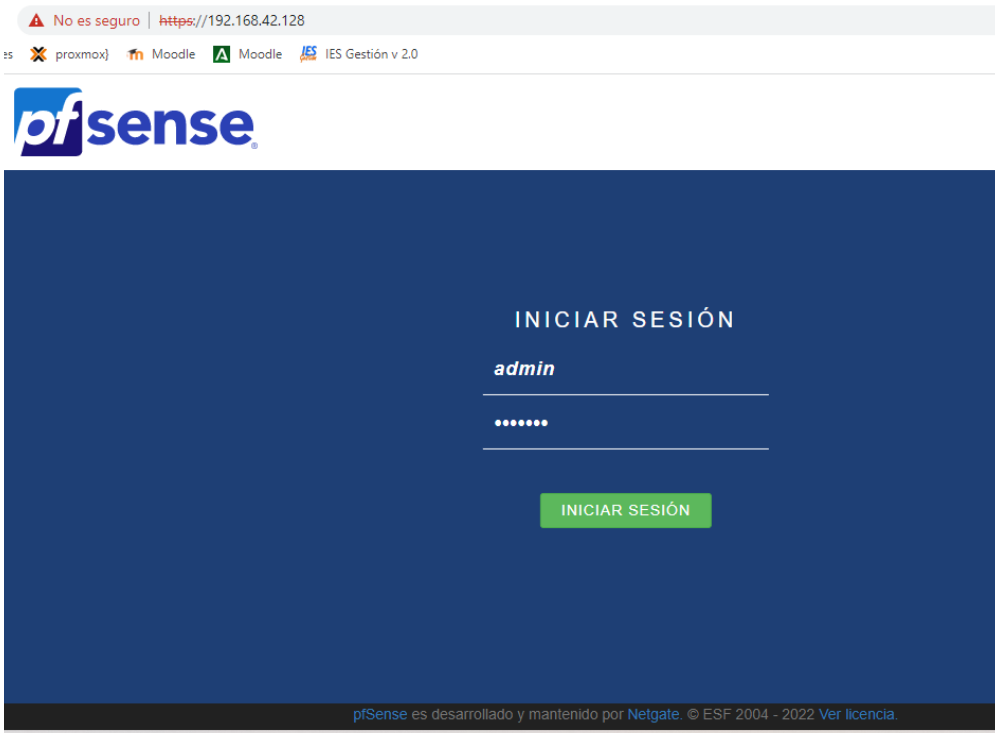
## 3.3 Configuración previa del S.O. PfSense

Ahora debemos ver la dirección IP que nos ha dado en nuestro S.O. PfSense para acceder desde el navegador de mi máquina local:

```
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=81009b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,VLAN_HW
FILTER>
        ether 00:0c:29:55:ef:8b
        inet6 fe80::20c:29ff:fe55:ef8b%em0 prefixlen 64 scopeid 0x1
        inet 192.168.42.128 netmask 0xffffff00 broadcast 192.168.42.255
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
        nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
enc0: flags=0<> metric 0 mtu 1536
        groups: enc
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
        inet 127.0.0.1 netmask 0xff000000
        groups: lo
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
pflog0: flags=100<PROMISC> metric 0 mtu 33160
        groups: pflog
pfsync0: flags=0<> metric 0 mtu 1500
        groups: pfsync
[2.6.0-RELEASE][root@pfSense.home.arpa]/root:
```

Nos ha asignado la **IP → 192.168.42.128**

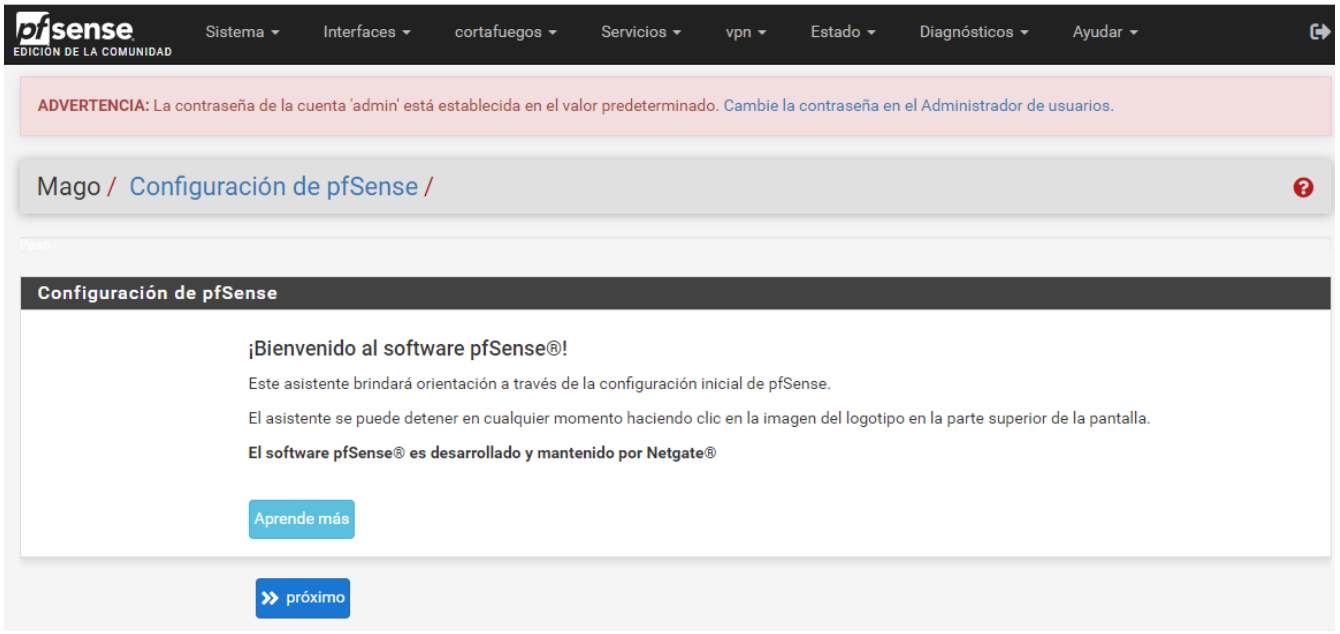
Voy al navegador de la máquina local, funciona, y ponemos los datos que vienen por defecto:




→ La IP como URL

→ admin
→ pfsense
Click en
INICIAR SESIÓN

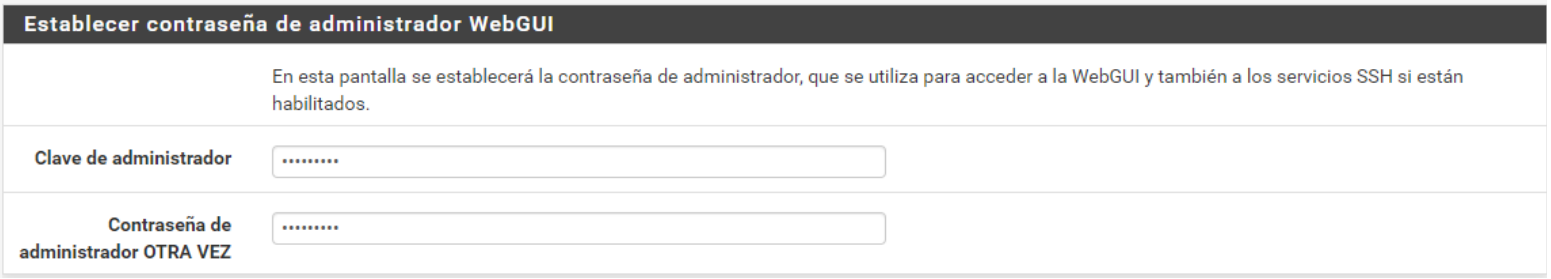
Ya dentro seguimos los pasos para una configuración previa...

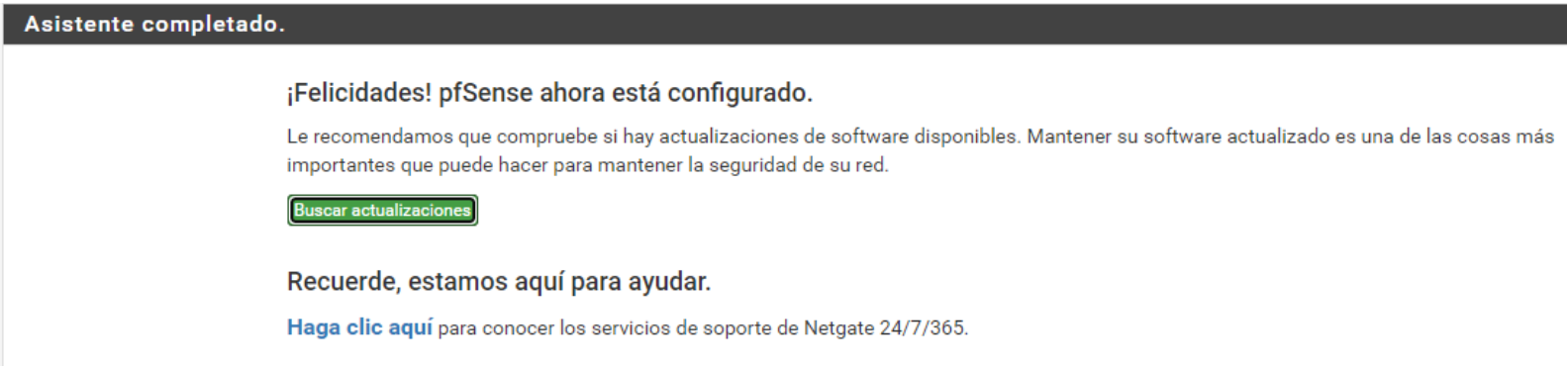



Ajusto algunos datos como el host, dominio, quizás DNS...



Por seguridad, un cambio de clave:



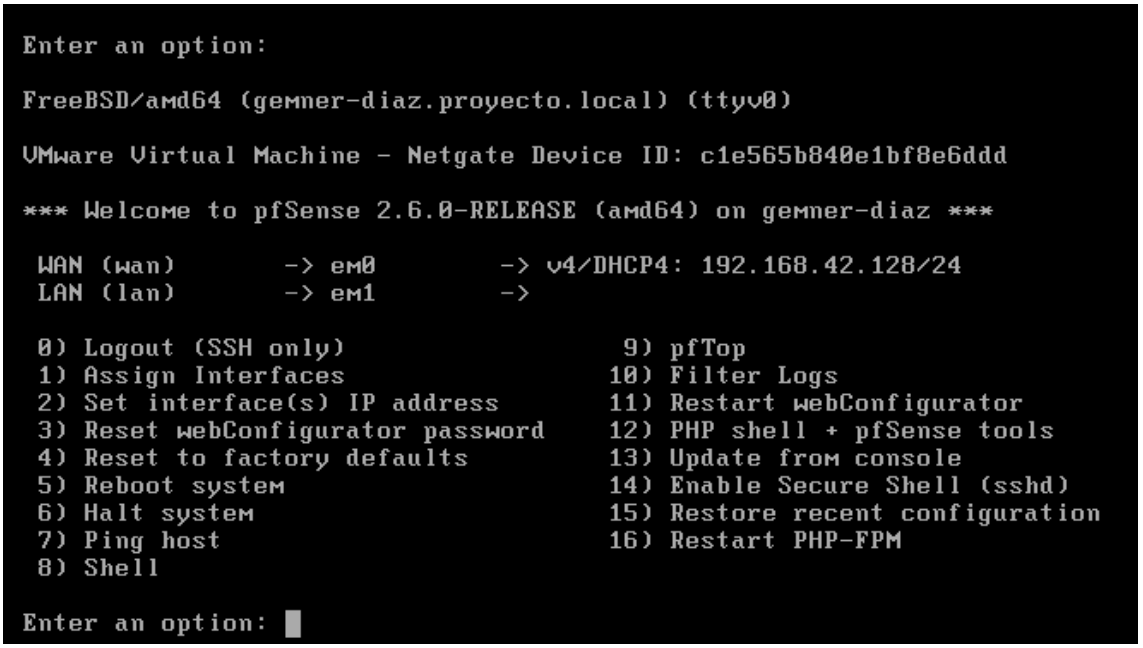




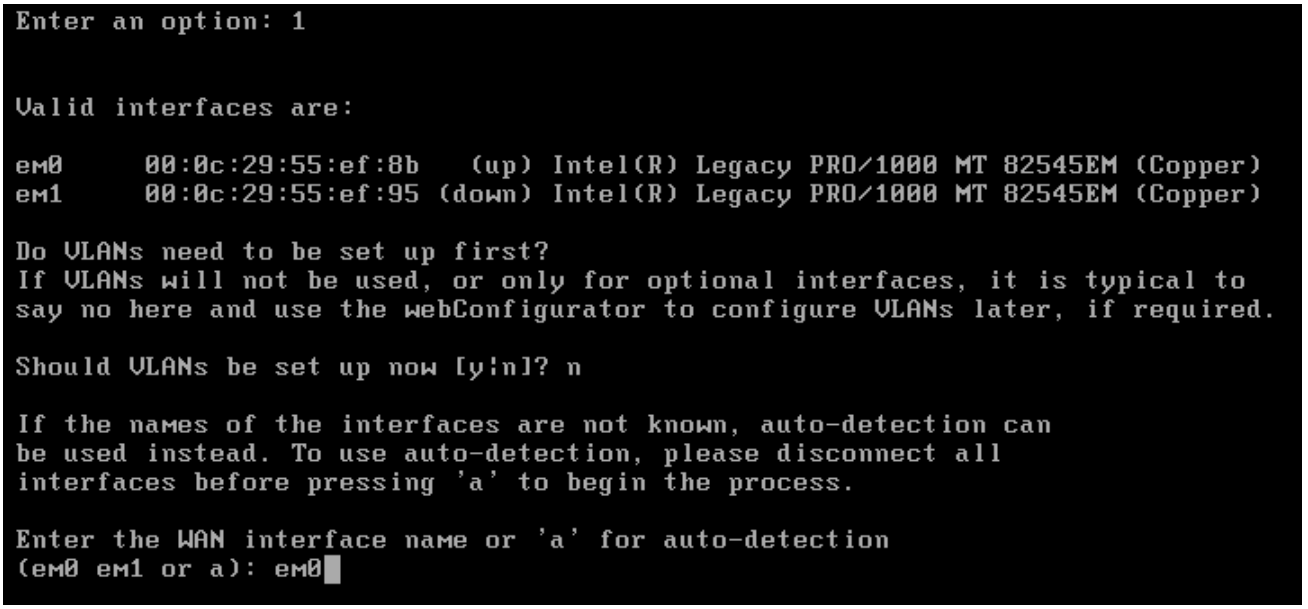
Y listo, tenemos PfSense configurado para empezar a trabajar nuestro portal cautivo.

# 4. CONFIGURACIÓN DEL PORTAL CAUTIVO + RADIUS

## 4.1 Configuro las interfaces de red ( WAN / LAN ):

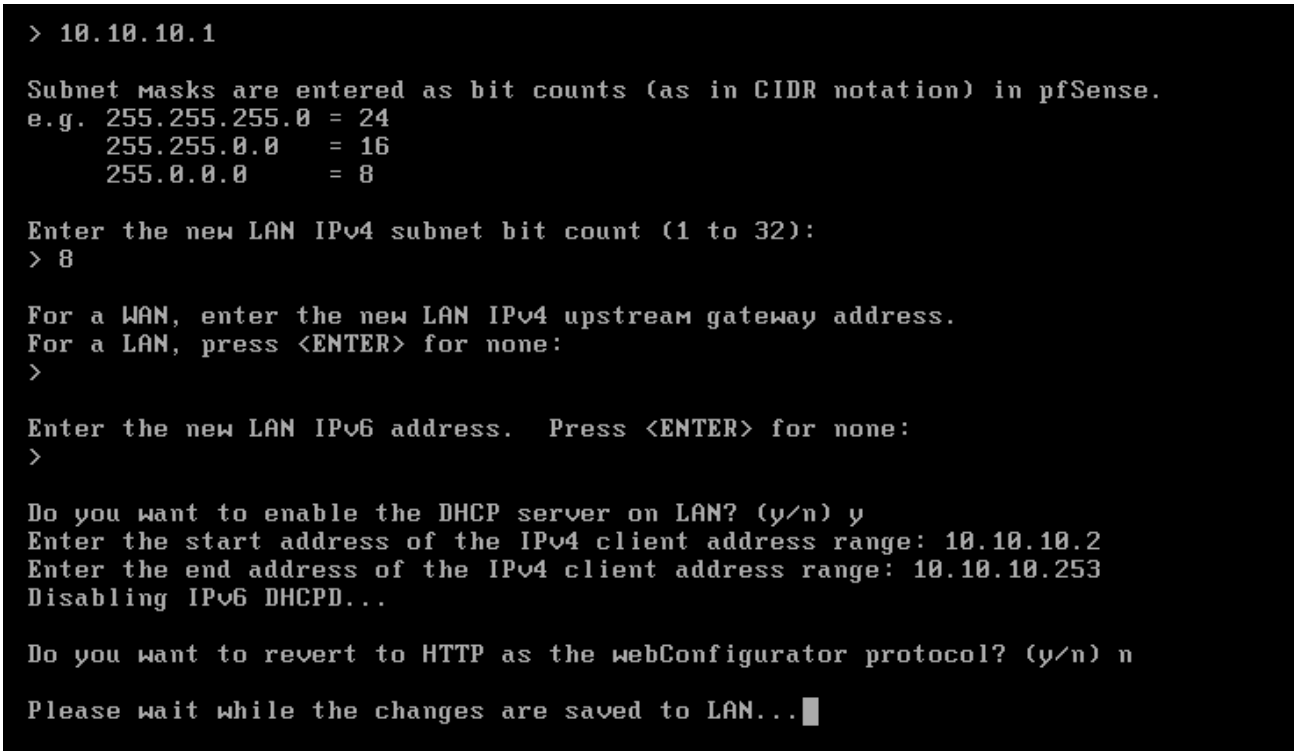



Desde la consola de la máquina PfSense, en el menú principal, seleccionamos la opción 1)



**em0** → para la red WAN por DHCP ( IP = 192.168.42.128 )

Para **em1** le damos la IP → 10.10.10.1/8 en LAN y con DHCP para que le asigne direcciones IP a los usuarios que se conecten con una IP de estas características.



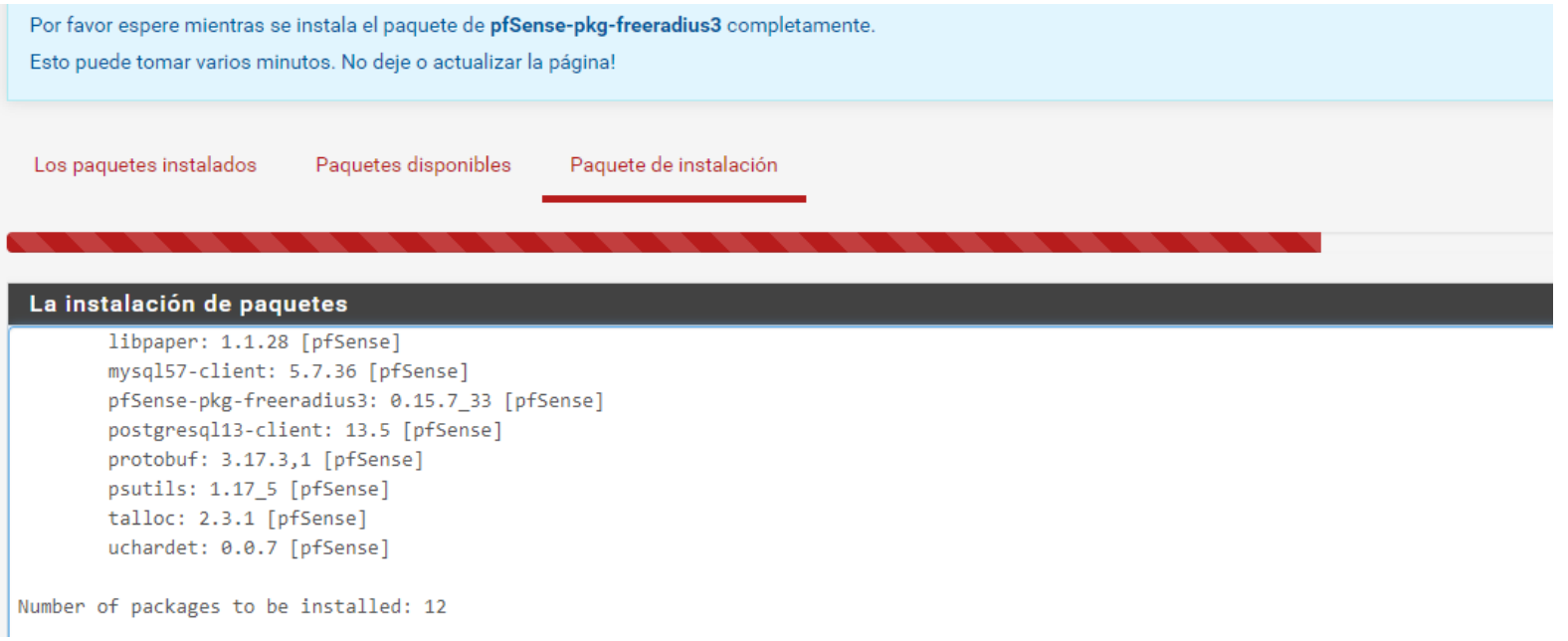

Cuando los cambios están hechos, damos click en < enter > y esperamos...

## 4.2 Instalamos los paquetes referentes a Radius

Debemos ir a → Sistema → Gestor de paquetes → paquetes disponibles → y buscamos por "Freeradius":

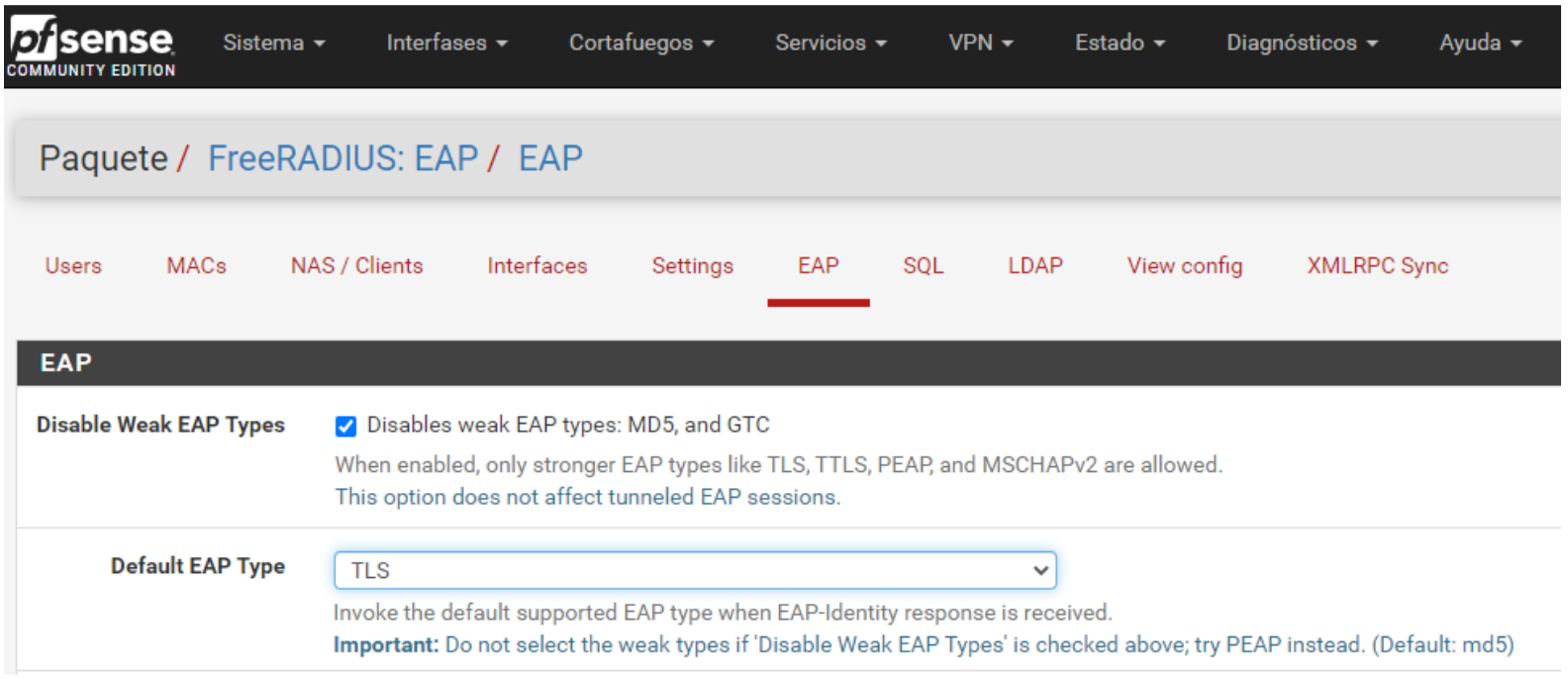



Ya aquí, le damos click a **< Install >** , confirmamos y esperamos...

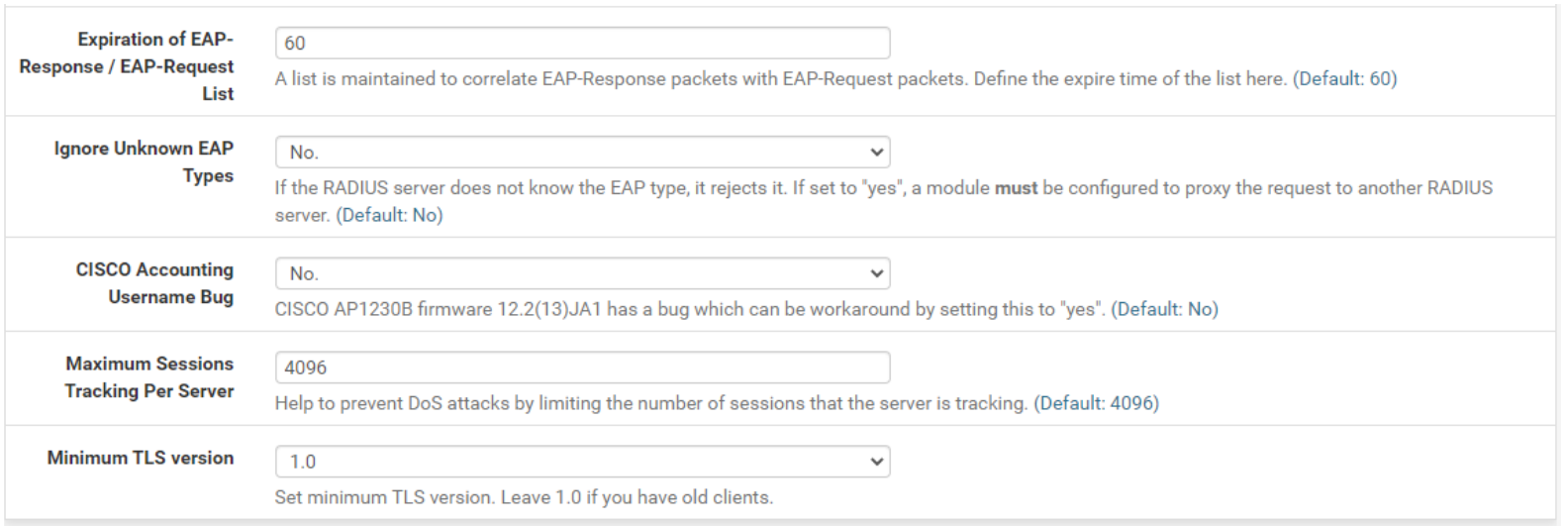


## 4.3 Configuramos RADIUS:

En primer lugar, vamos a → Servicios → FreeRadius → EAP:

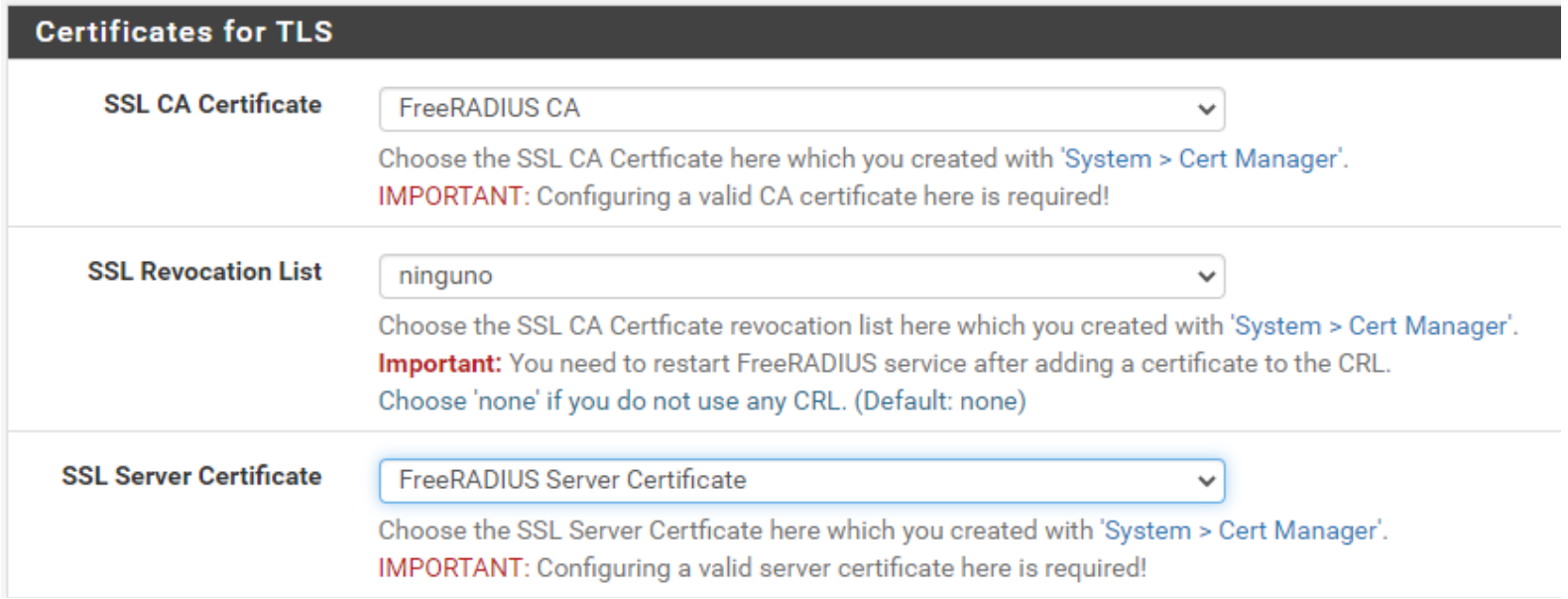



En EAP, desactivamos los métodos de encriptación débiles, y seleccionamos TLS.

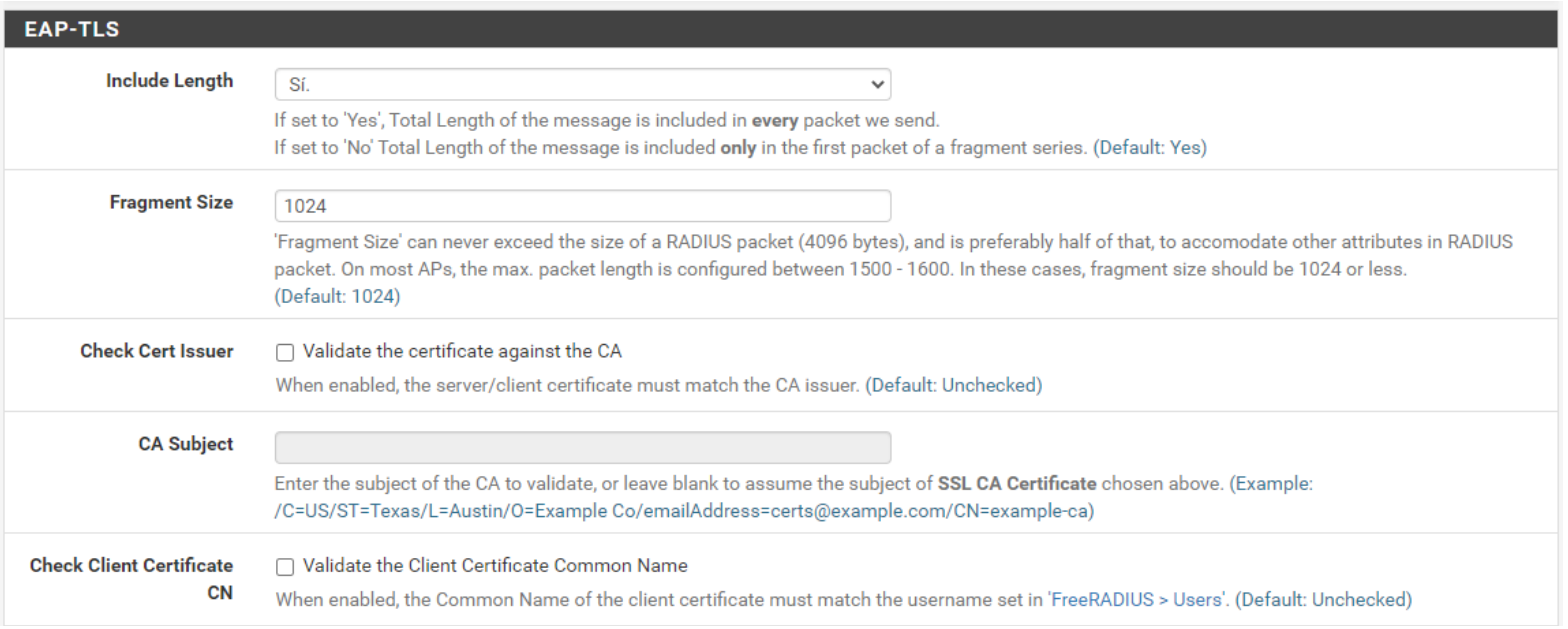



Estos 5 recuadros se dejan por defecto, ya que es buena configuración.

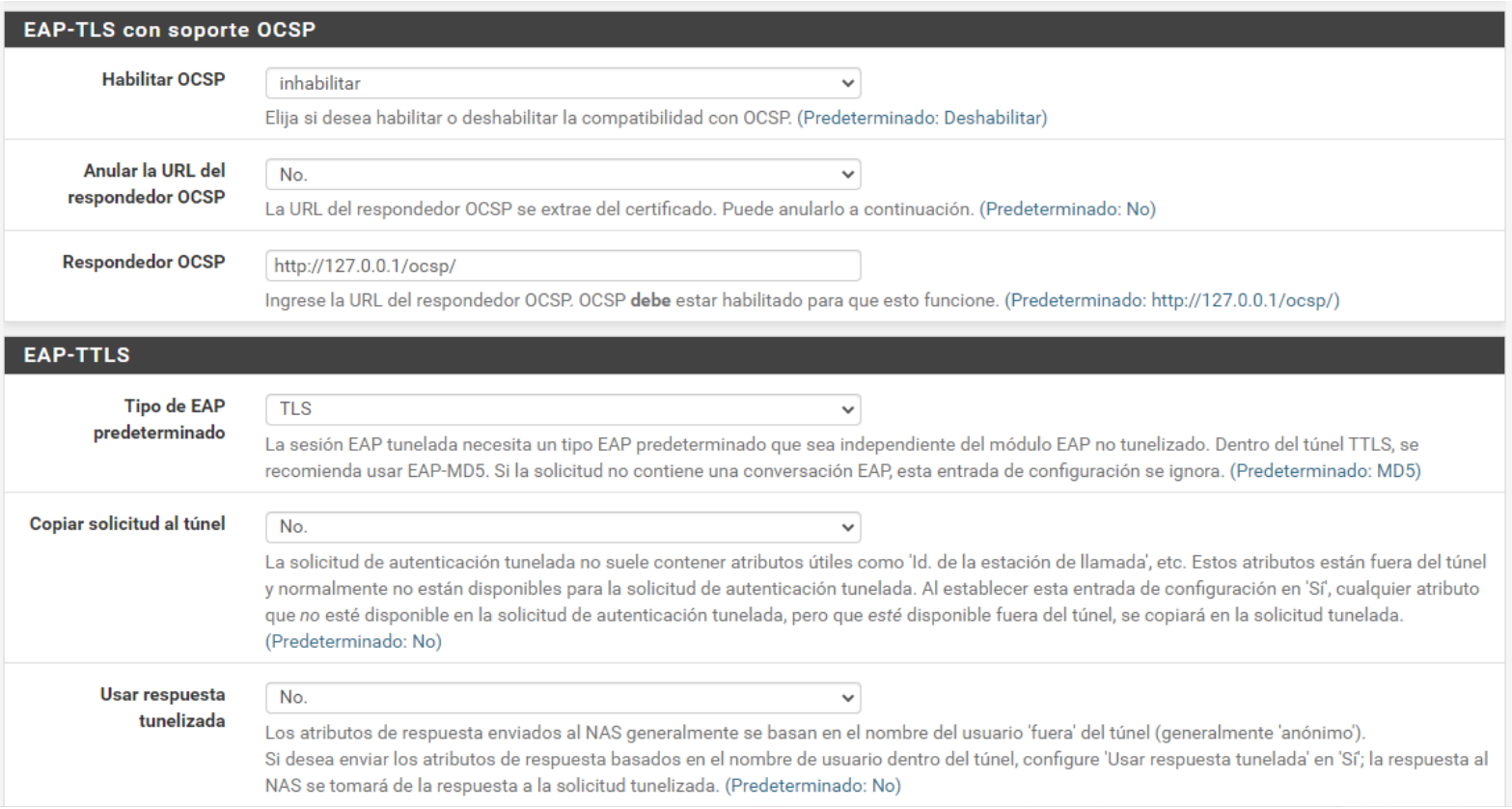
En Certificates for TLS → SSL... seleccionamos un certificado que trae por defecto el paquete de FreeRadius y en SSL Server también.




Seguimos dejando estos otros por defecto

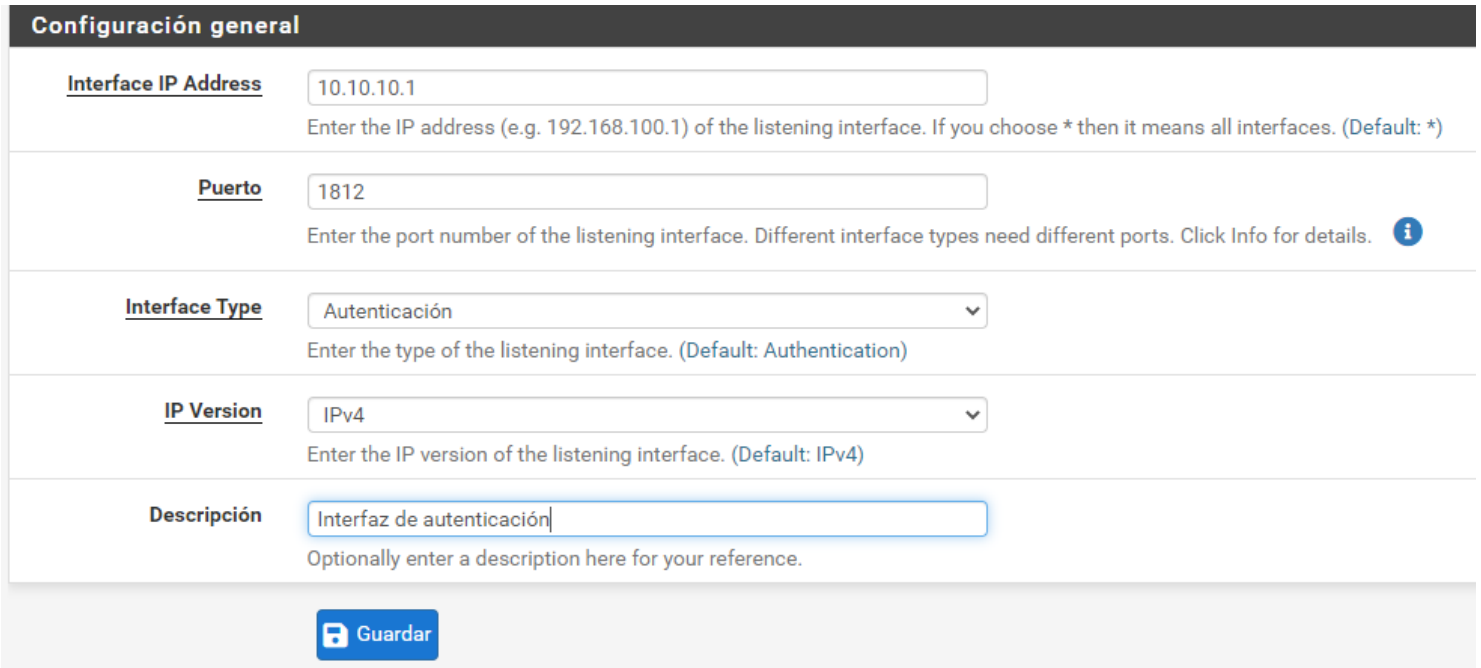



Todos los demás recuadros hacia abajo se siguen dejando por defecto...

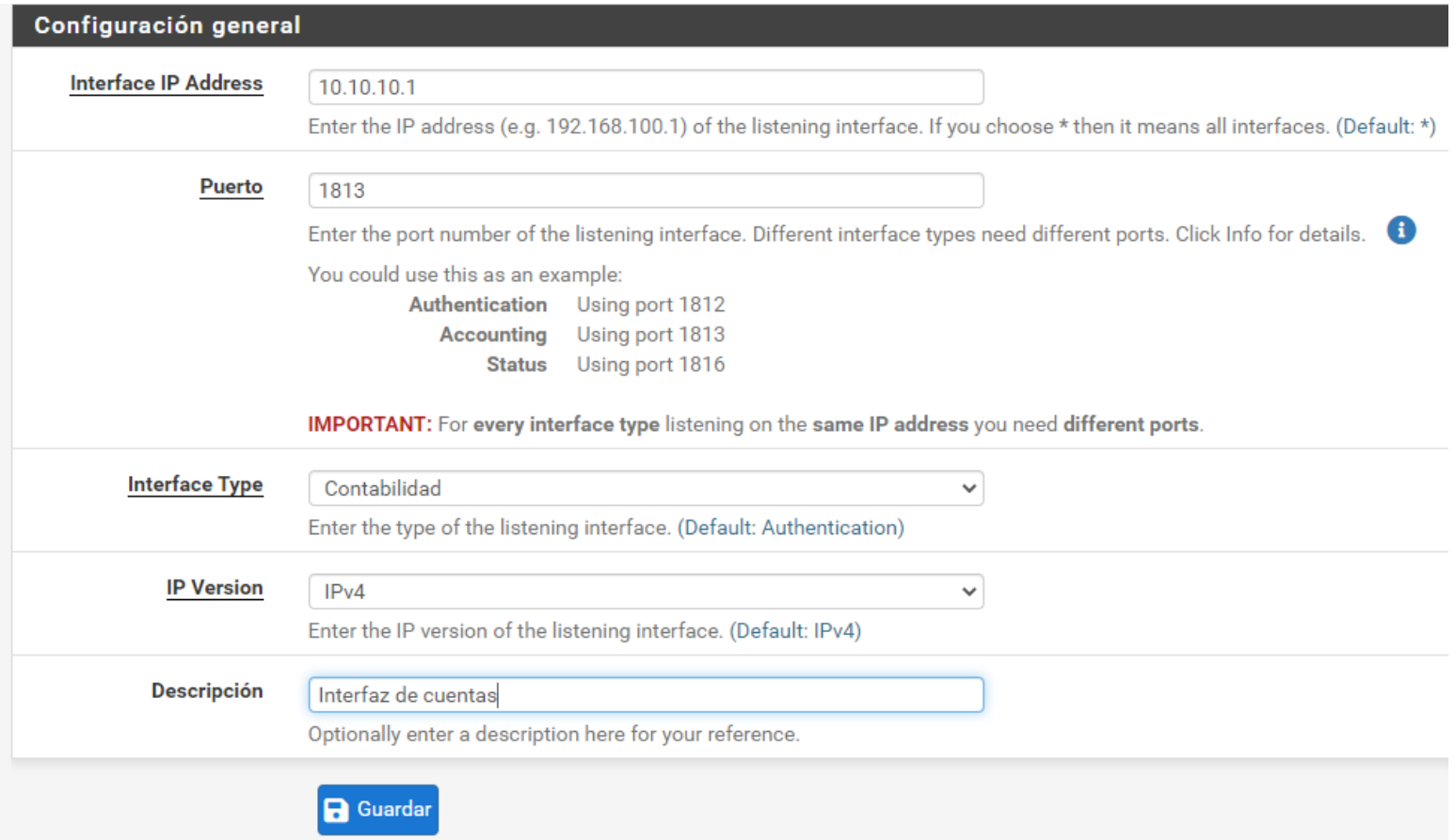



Por defecto dejamos también todo esto.
Y damos click en < Guardar >.

Ahora nos dirigimos a la sección de Interfaces
Y con nuestra IP de la red LAN, creamos en el puerto 1812 la interfaz de tipo - autenticación. click en < Guardar >.

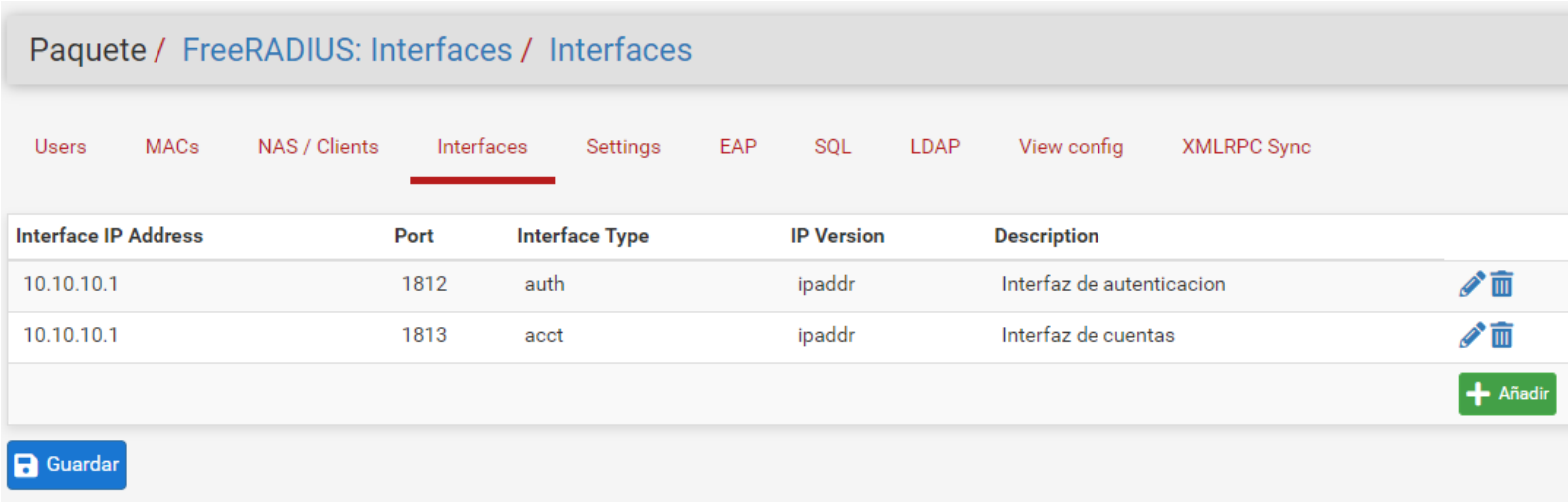


Ahora creamos otro pero en el puerto 1813 para las cuentas:



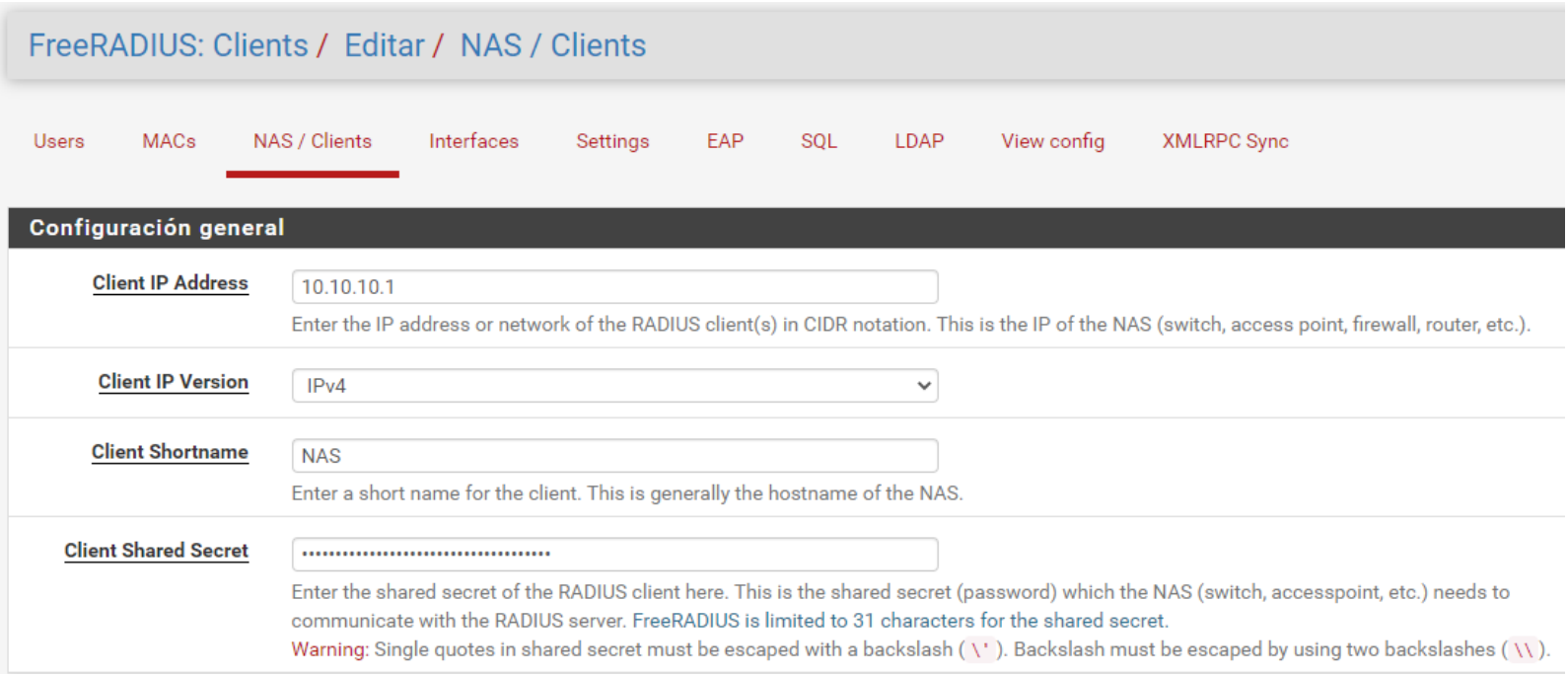

Click en < Guardar >

Quedaría de esta manera:

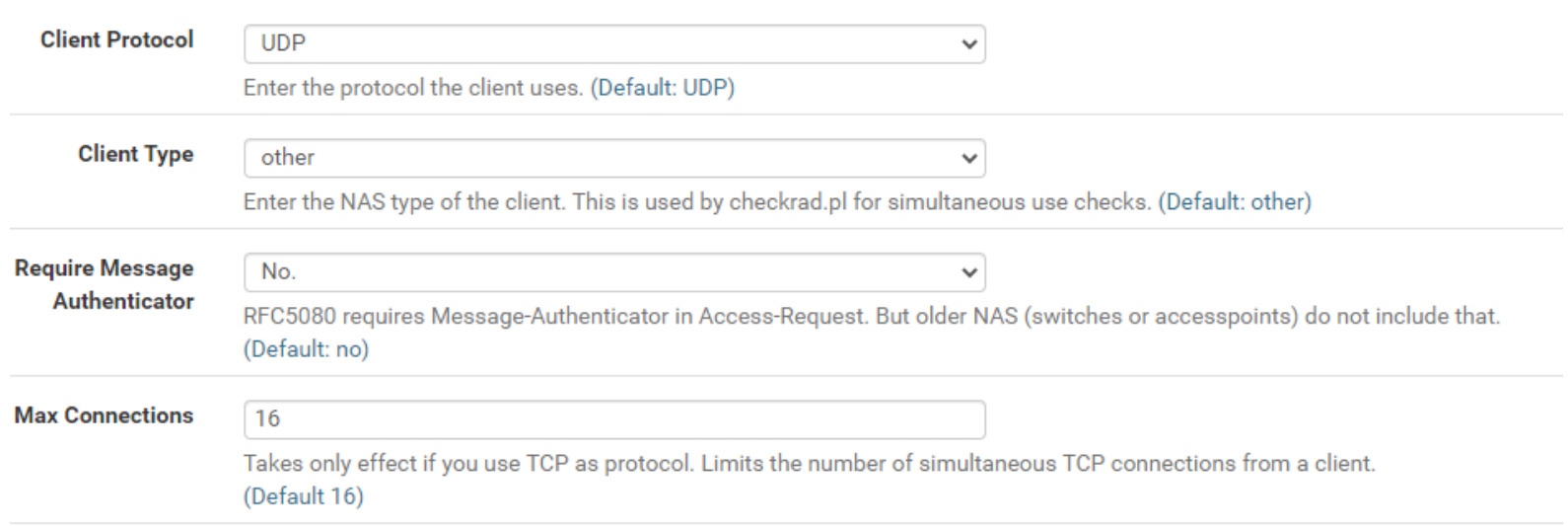



Click en < Guardar >.

Ahora nos dirigimos a NAS / Clients y creamos uno de esta manera:
Siendo el cliente la dirección IP LAN → 10.10.10.1
En Client IP Versión, siempre → IPv4
En Client Shortname, seleccionamos un nombre.
Y en Client Shared Secret, creamos una contraseña fuerte, puesto que la función de esto es comunicar el servidor RADIUS con el NAS

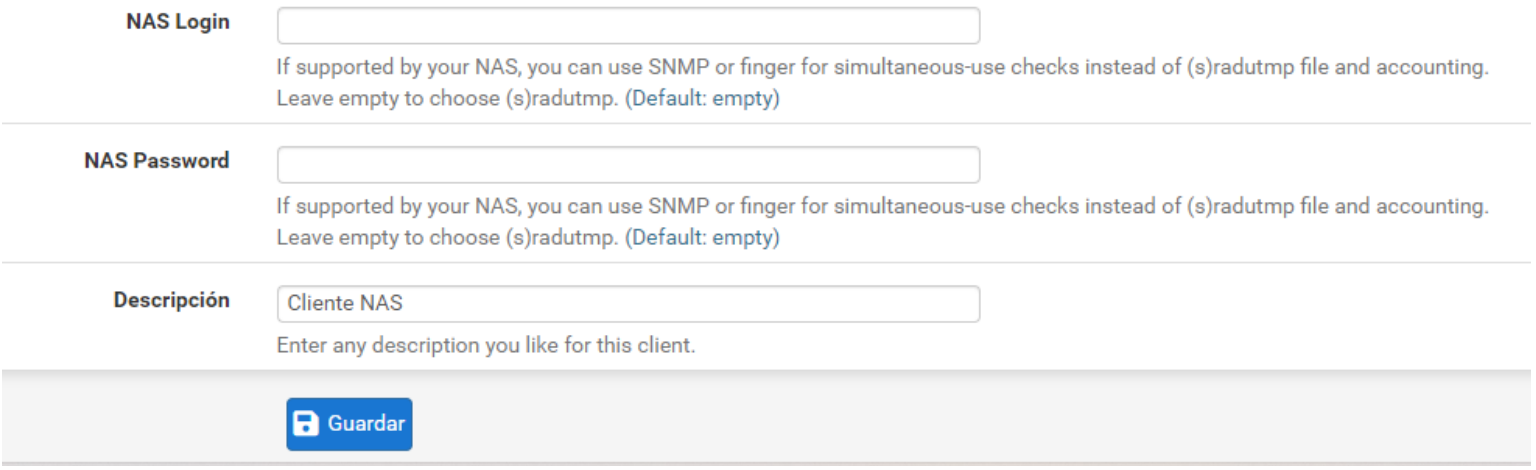



Seguimos...

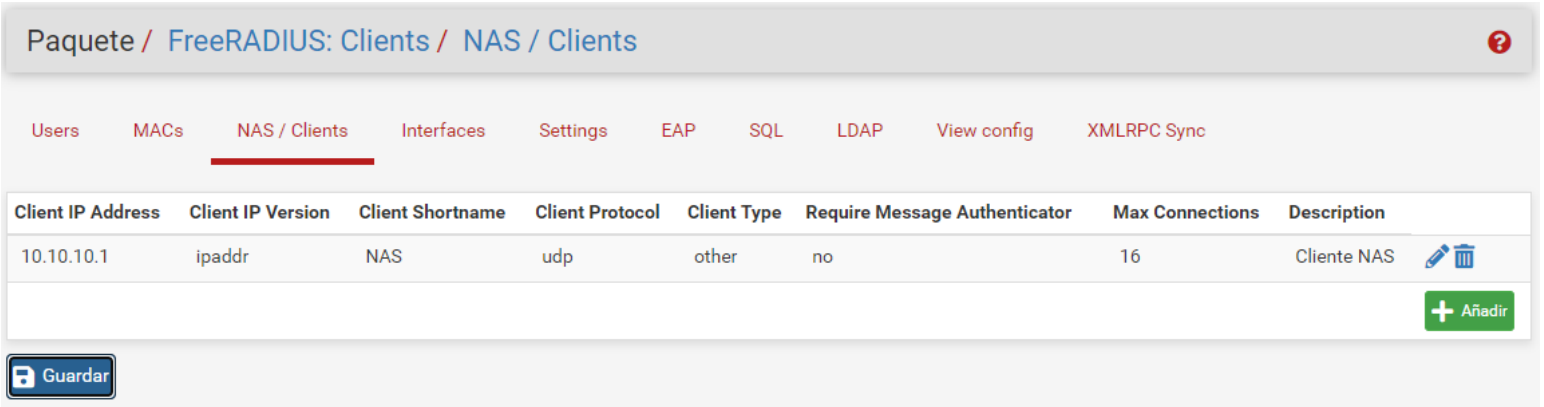



Importante que el protocolo del cliente sea → UDP

Dejamos por defecto lo demás y click en < Guardar >.



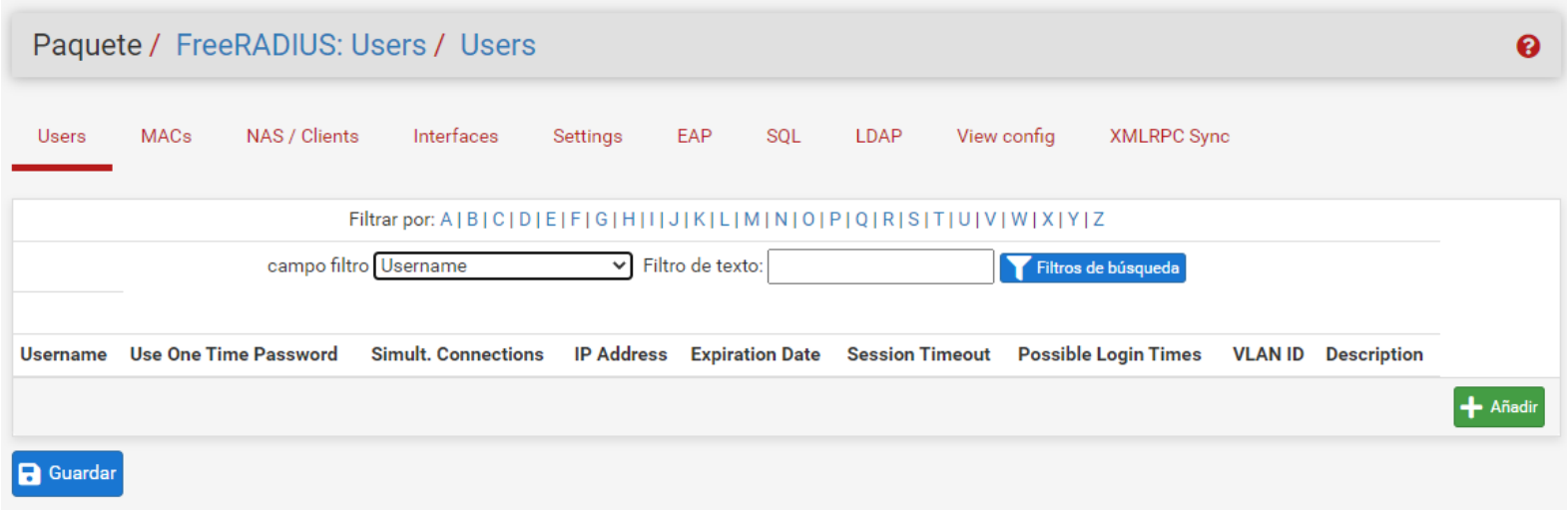

Quedaría de esta manera:




Hecho esto, es el momento de crear los diferentes tipos de usuarios deseados:

- Técnicos que trabajan fuera
- Técnicos que permanecen dentro de la empresa
- Jefe y el personal de oficina
- Practicantes y alumnos (como yo)
- Clientes y visitantes

Vamos a la pestaña de “Users” y damos click en < Añadir >:

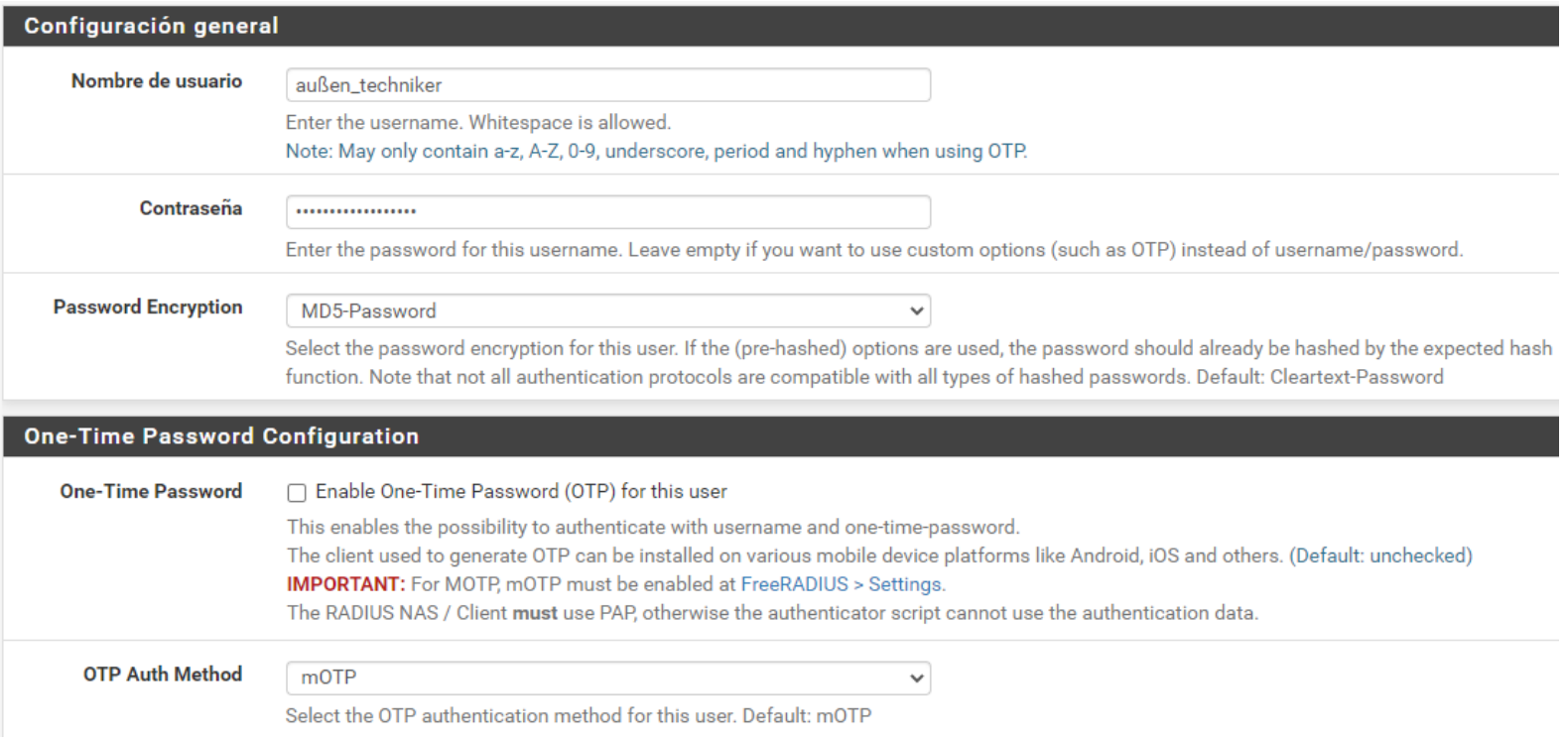



Ahora, vamos a crear al tipo [ 1 ] → Técnicos de instalaciones y reparaciones (fuera de la empresa) es una plantilla de 12 técnicos y el usuario será:

- außen_techniker ( Técnicos de fuera)

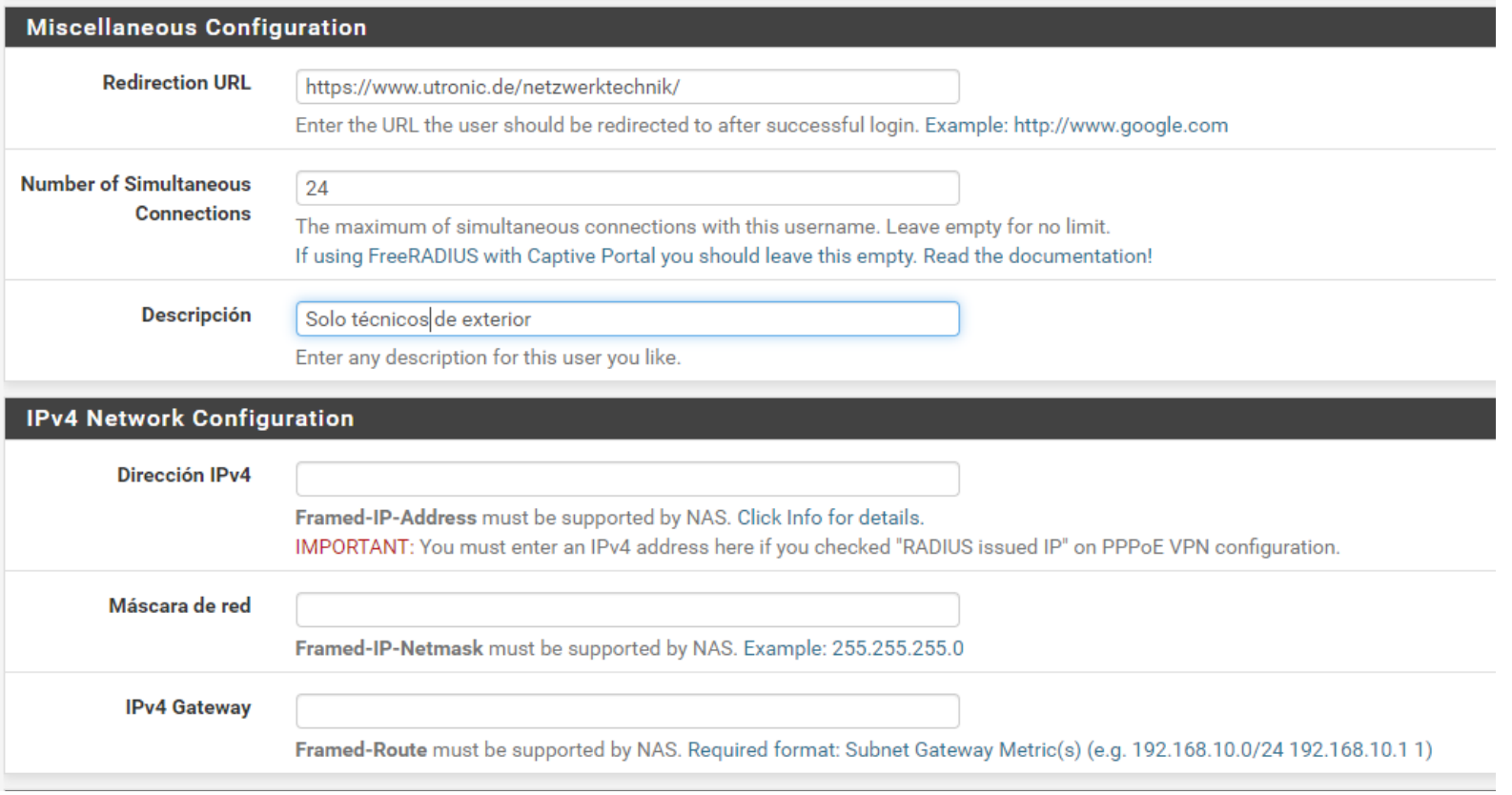
y la contraseña:

- au_tech_12-utronic

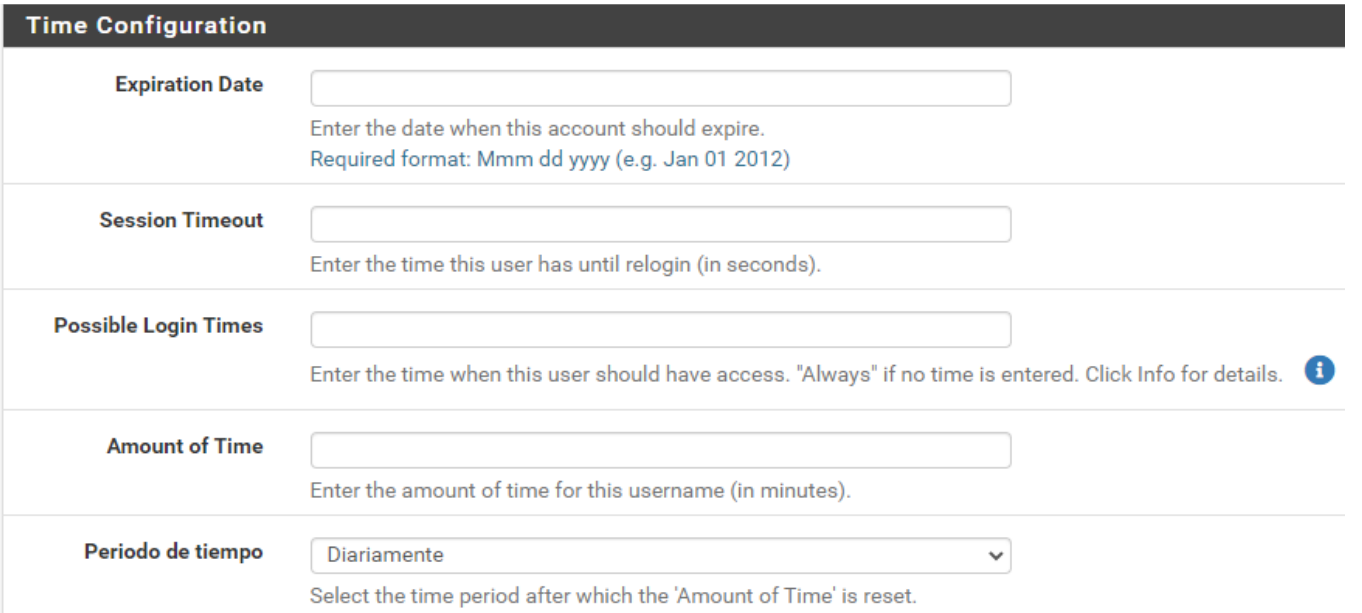



Password Encryption → MD5 Password

Dejamos las siguientes 2 opciones por defecto y seguimos: Redireccionamos a estos usuarios a la URL correspondiente con un máximo de 24 conexiones simultaneas - 2 para cada técnico, las opciones de IPv4 se dejan por defecto.

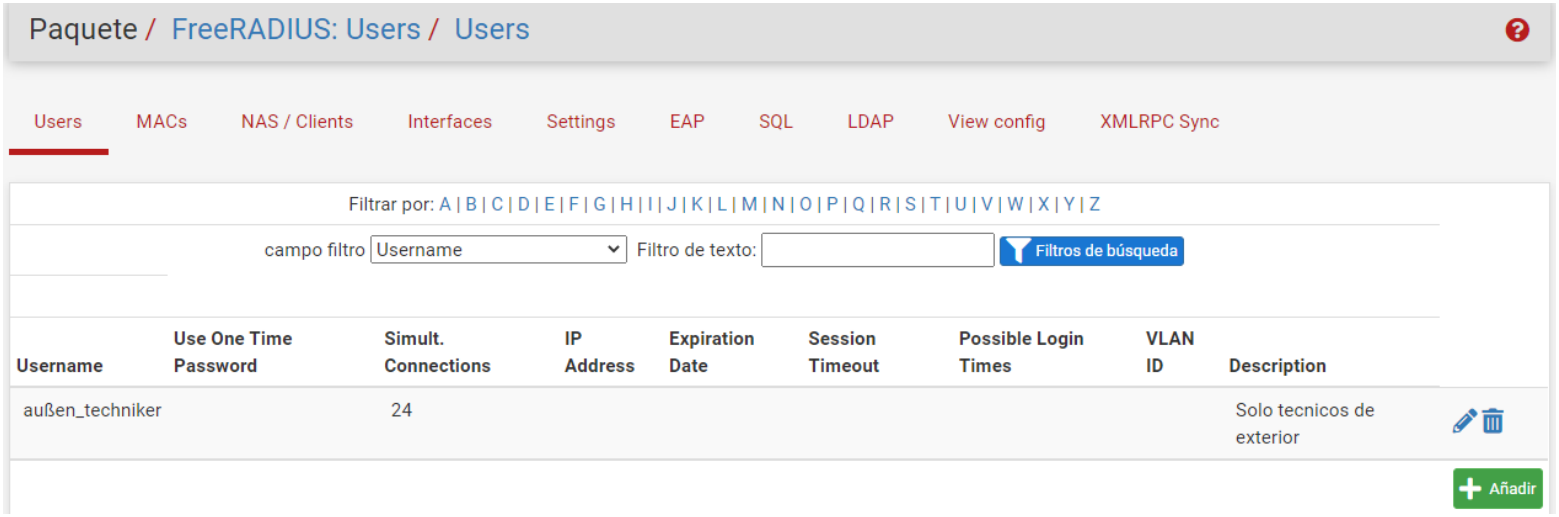



Por último nos pregunta si queremos establecer algún tipo de límite en minutos para el tipo de usuario, lo cual dejaremos en blanco para no entorpecer el trabajo de los técnicos.



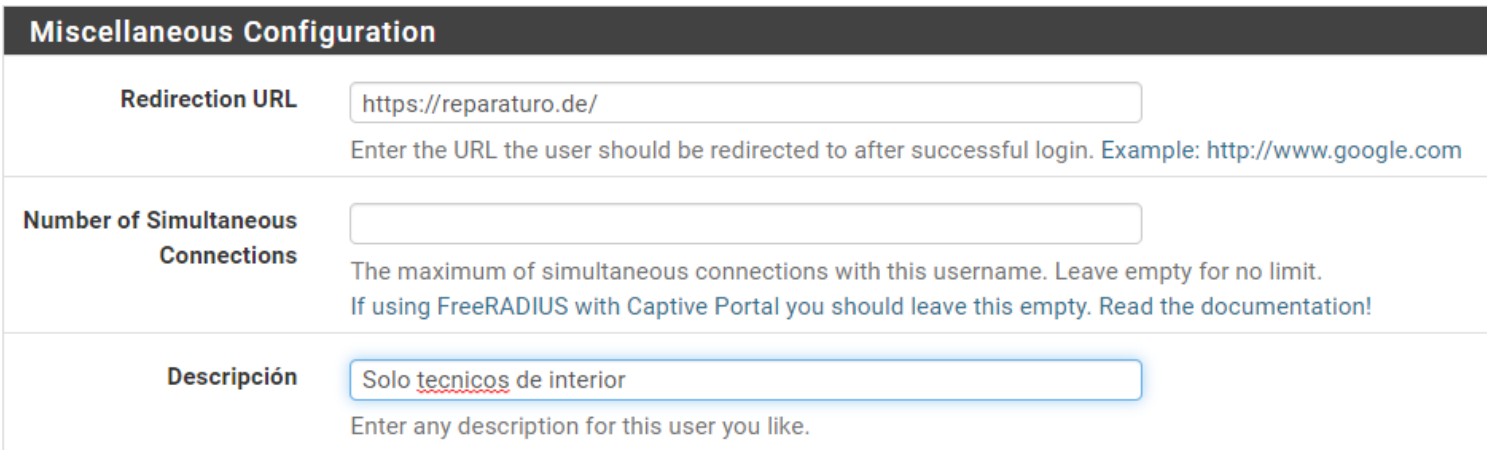
Luego en los apartados de tráfico y ajustes avanzados dejamos de nuevo la configuración por defecto y click en < Guardar >.

Ya tenemos nuestro primer tipo de usuario:




Creamos el mismo tipo para los técnicos de reparaciones en el interior, con la diferencia de que son 4 técnicos.
Su nombre de usuario será:
- drinner_techniker ( Técnicos de fuera)
y la contraseña:
- dr_tech_04-reparaturo

En redirección URL, la web es diferente porque tienen una propia:




No les creo restricciones de conexiones simultáneas porque requieren un número desconcertado.

Todo lo demás igual que el primer tipo o por defecto y guardamos.
Ahora voy a crear el tipo de Jefe y el personal de oficina.
Su usuario será:

- Büro ( Oficina )

Y su contraseña:

- bü_ro_4-utronic

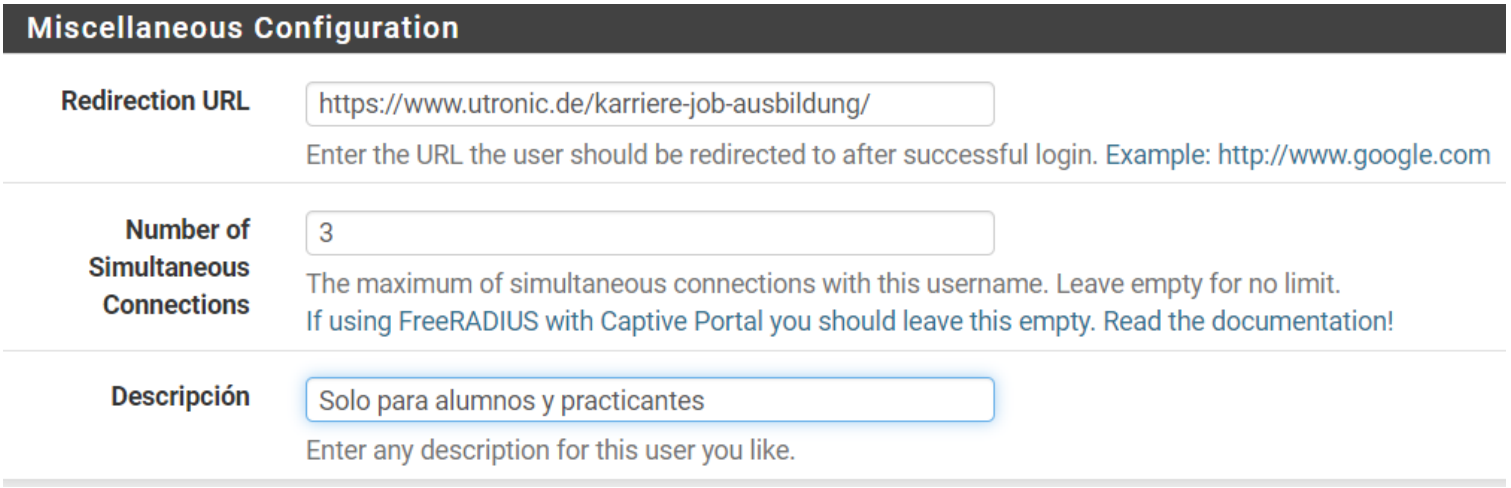
Creamos este tipo sin ninguna restricción de tiempo, tráfico, conexiones simultáneas ya que se desconoce la necesidad del número de conexiones.

Ahora vamos a crear al tipo → Practicantes y alumnos
Su usuario será:

- Praktiker ( Practicante )

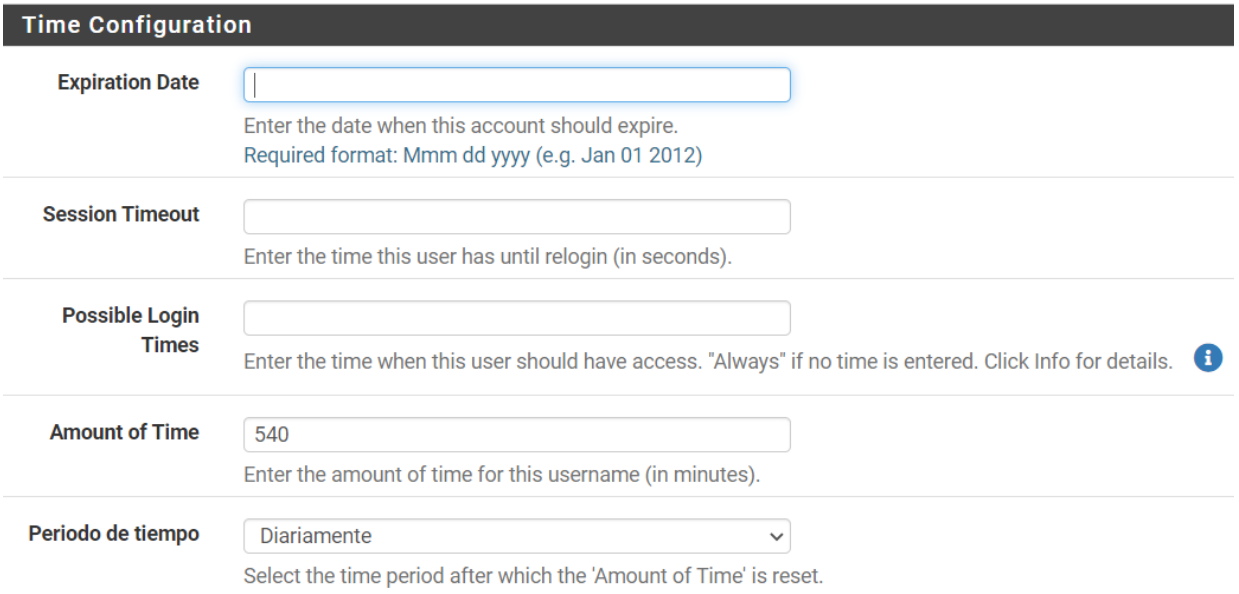
Y su contraseña:

- prak_03-utronic_reparaturo




Cómo URL, elijo la dirección de contacto para nuevas prácticas.
Conexiones simultáneas 3, porque somos 3 alumnos en prácticas, un practicante por conexión simultánea.

Les asigno un máximo de **540 minutos de conexión diarios** (8 horas), ya que por ley, es el máximo de una jornada de un alumno en prácticas.

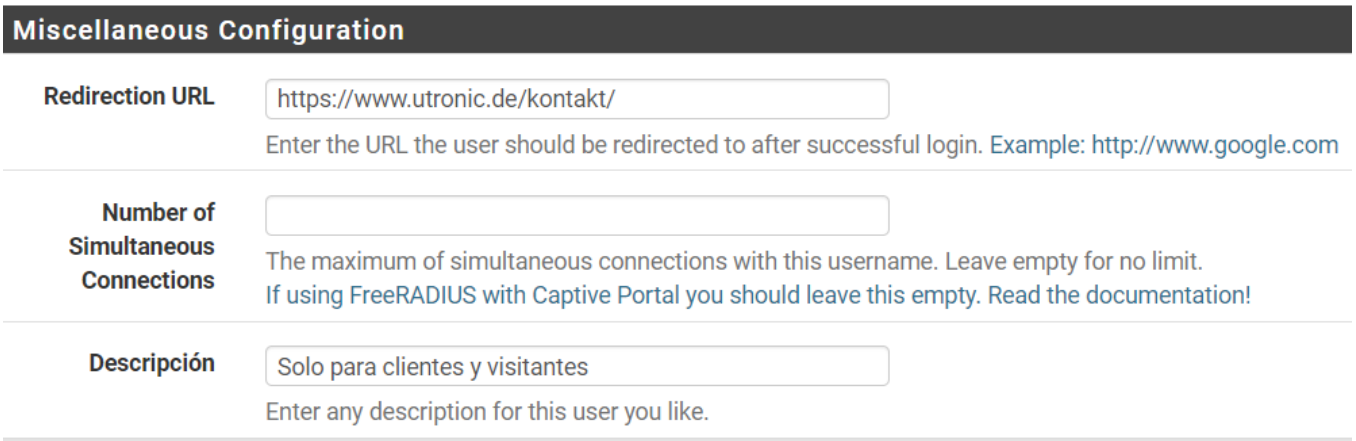



En tráfico lo dejamos sin límites, guardamos y pasamos al último tipo de usuario, → clientes y visitantes:
Su usuario será:

- kunden_besuch ( Cliente_visita )

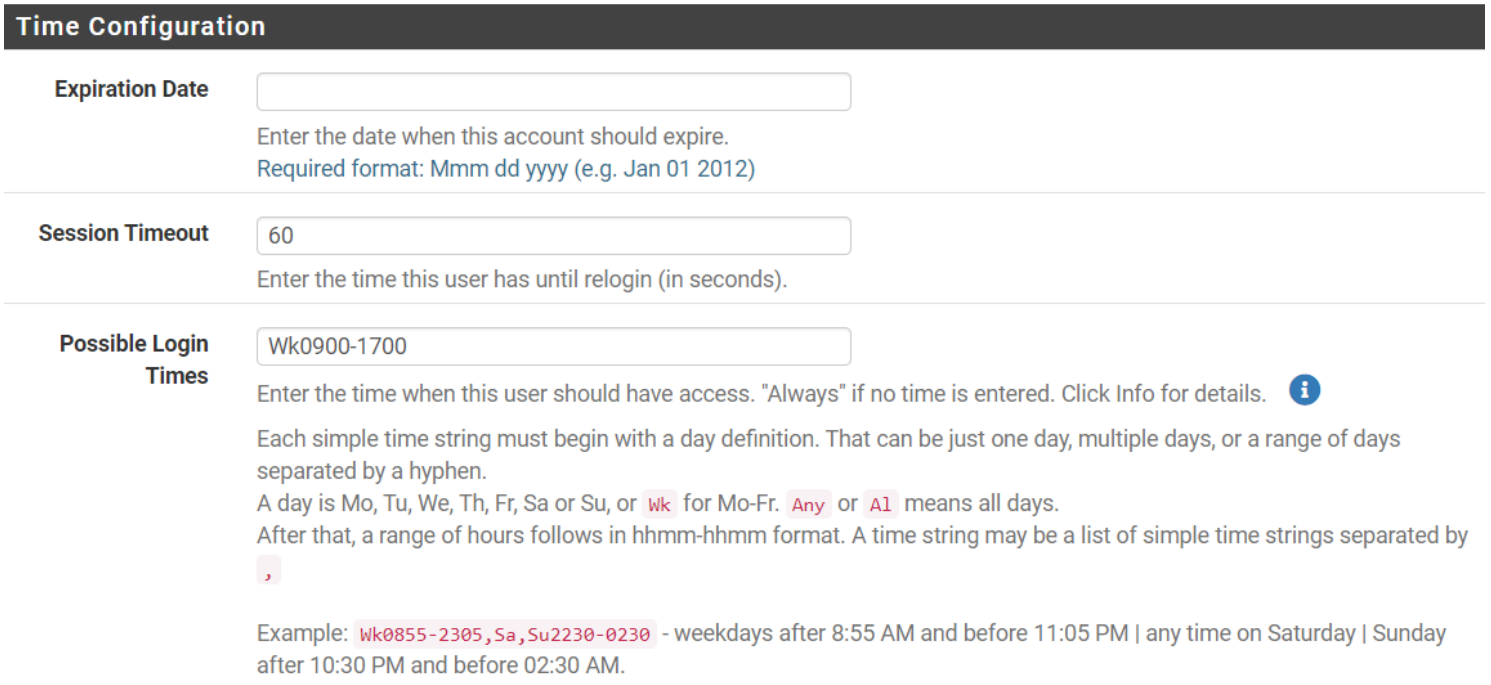
Y su contraseña:

- kund_besu_2022



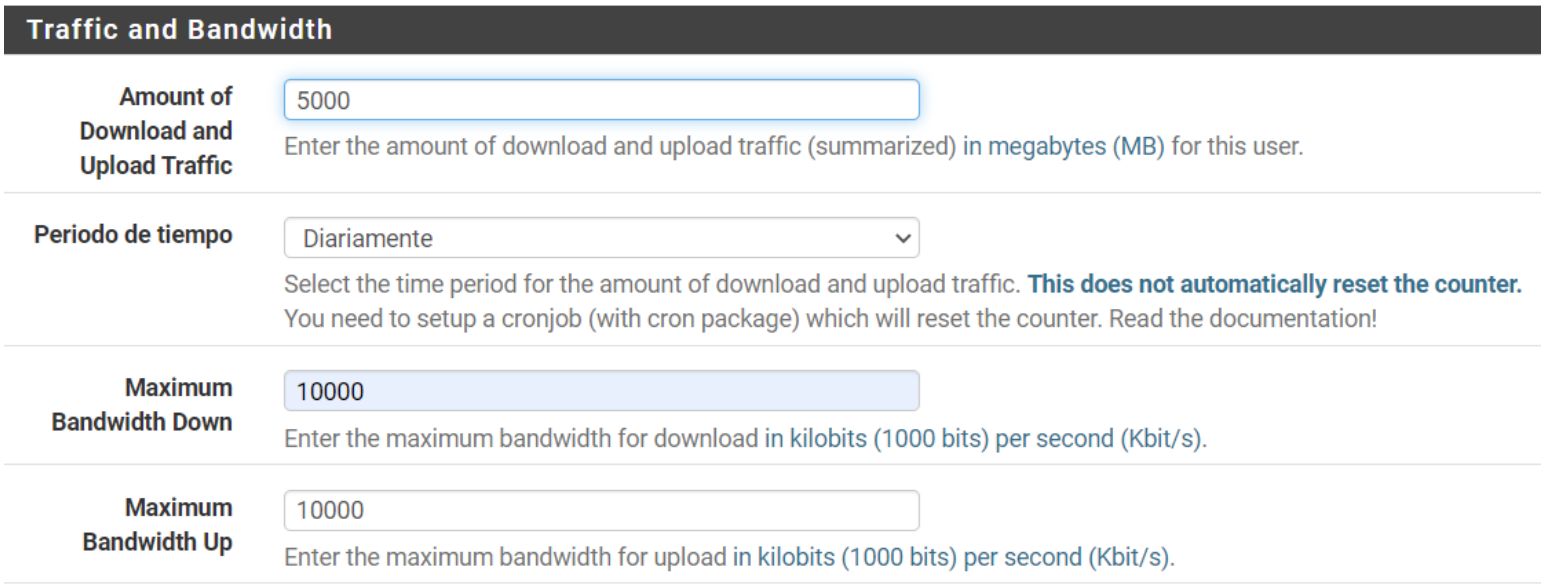

En la URL, los redirigimos a la sección de contacto, conexiones simultáneas ilimitadas porque no conocemos la cantidad de usuarios que usarán este tipo.

Ahora creo un ajuste en el que solo podrán conectarse de lunes a viernes de 9:00 a 17:00 que es el horario de clientes / visitas.

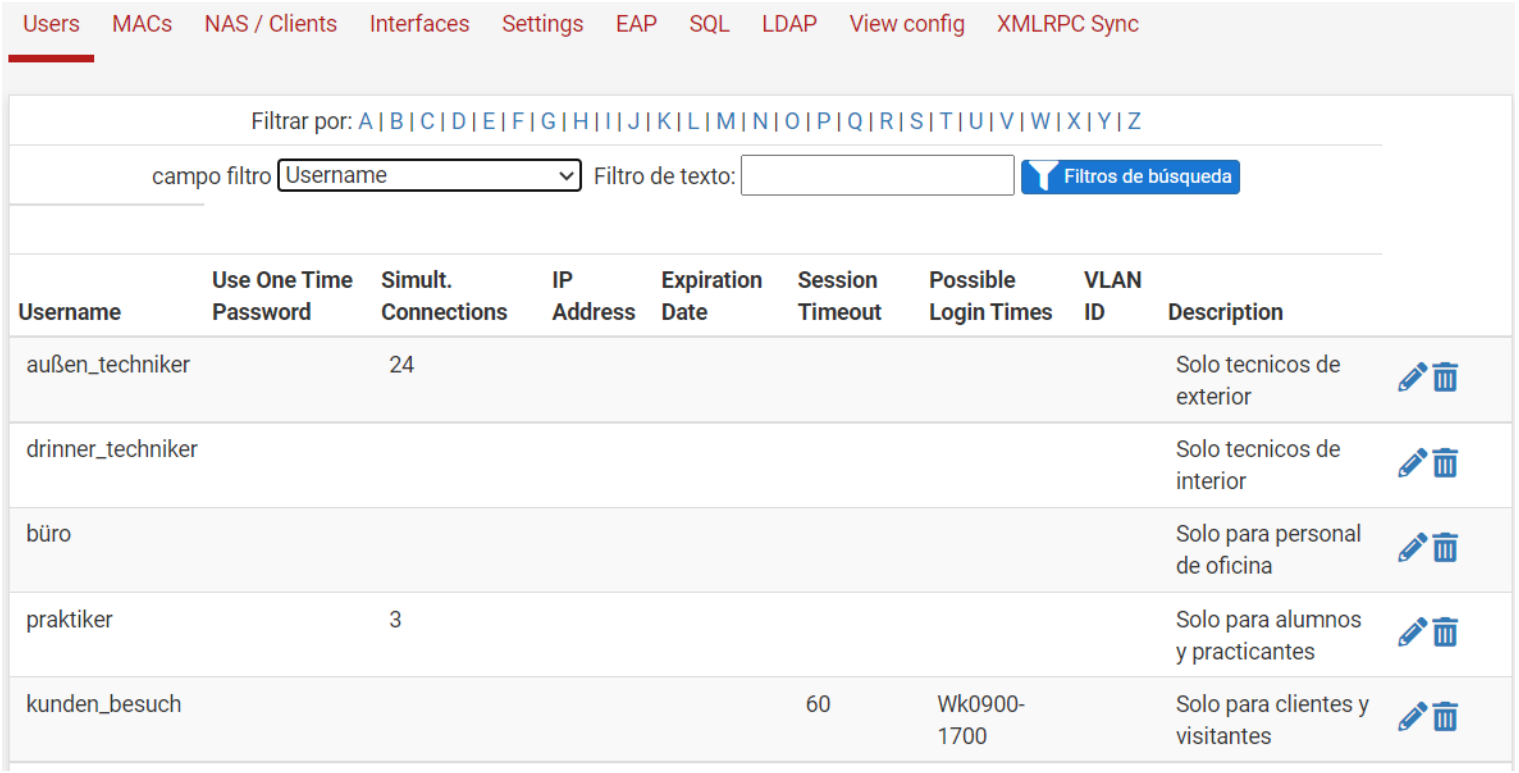



Además de un relogeo cada 60 minutos, o sea, el usuario será automáticamente desconectado, sin embargo, podrá volver a conectarse inmediatamente. (Session Timeout)

A continuación, en tráfico, limito a 5 Gb el consumo de este tipo de usuario al día y un máximo de 10000 Kbit/s que vendría siendo algo más de 1 Mb por segundo. Tanto de subida como de bajada, esto es para evitar movimientos extraños en la red y/o saturación.

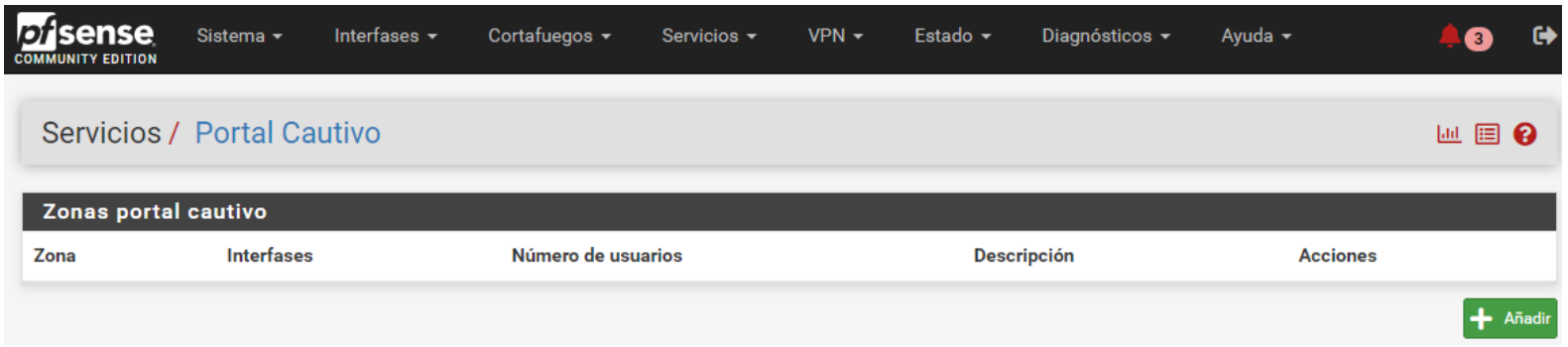


No hacemos más ediciones y guardamos.
Y de esta manera tendríamos ya creados nuestros 5 tipos de usuarios en nuestro servidor RADIUS:



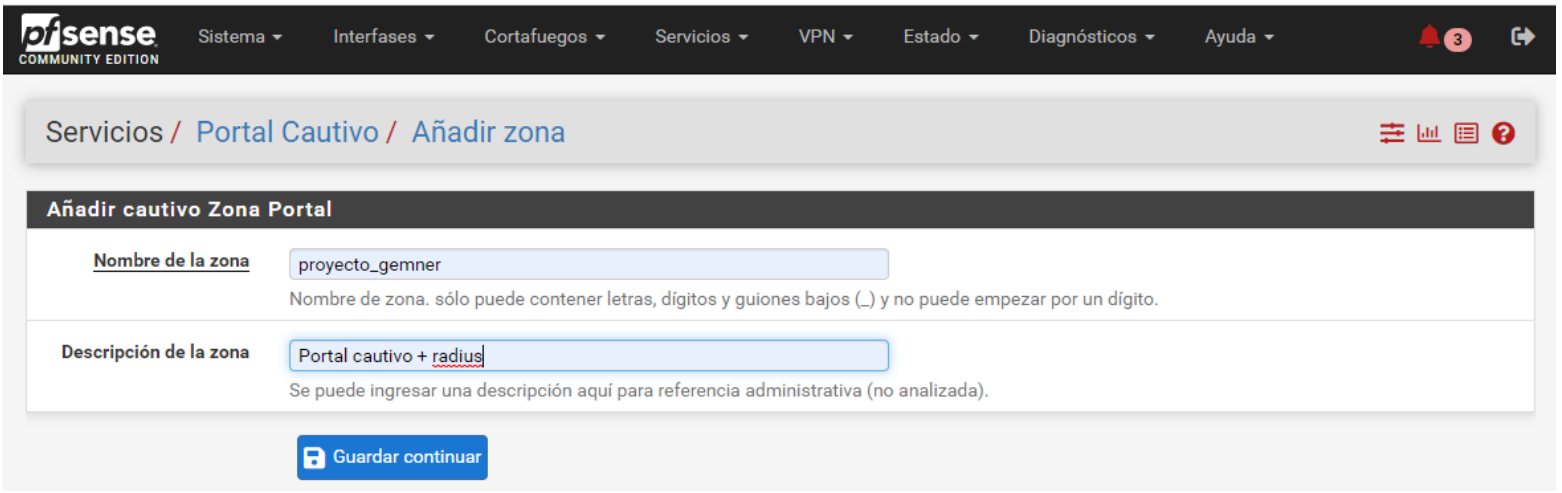
## 4.4 Configuro el portal cautivo

Primero vamos a → Servicios → Portal Cautivo:



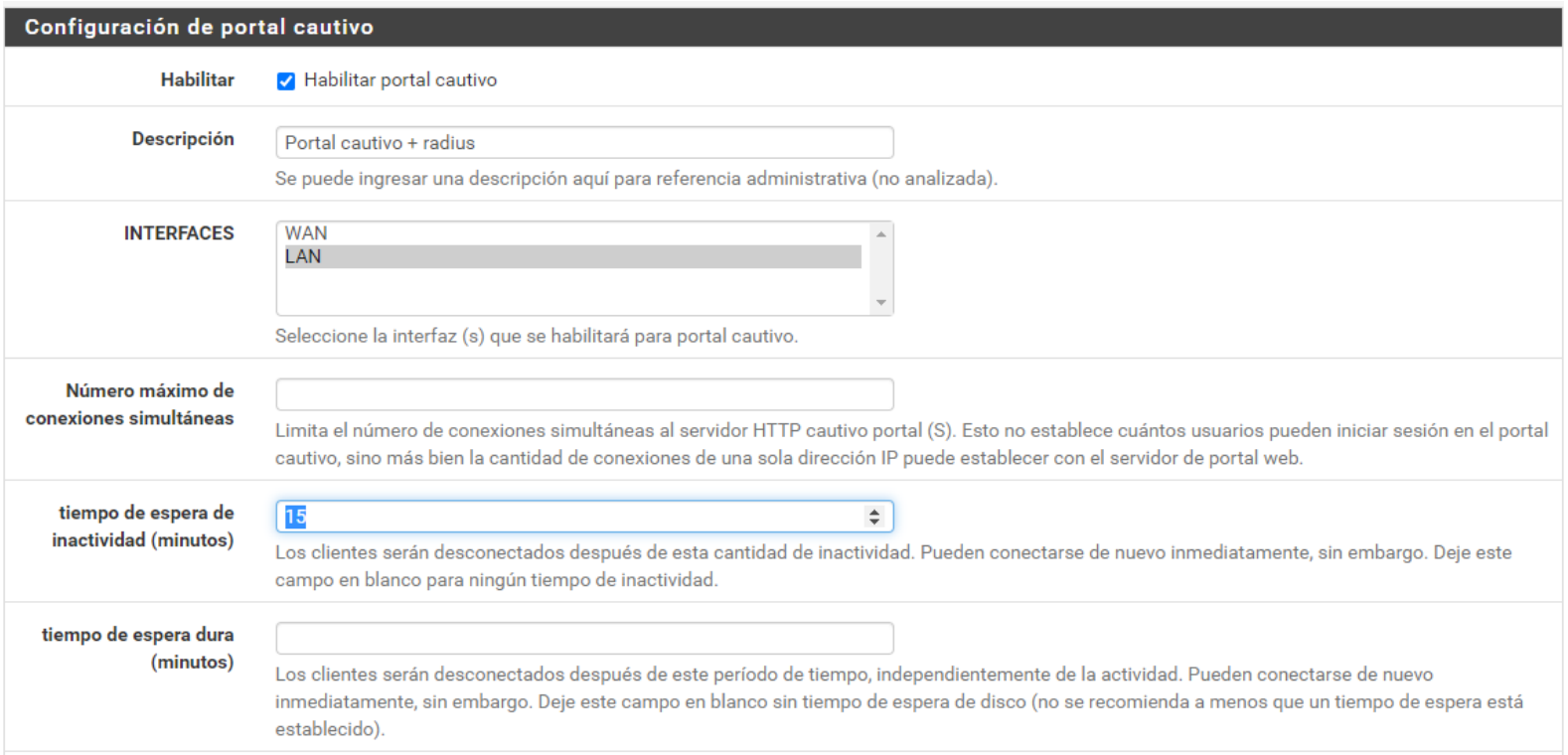

Damos click en < Añadir > ...

Creamos un nombre para la zona: proyecto_gemner
y una descripción: Portal cautivo + radius

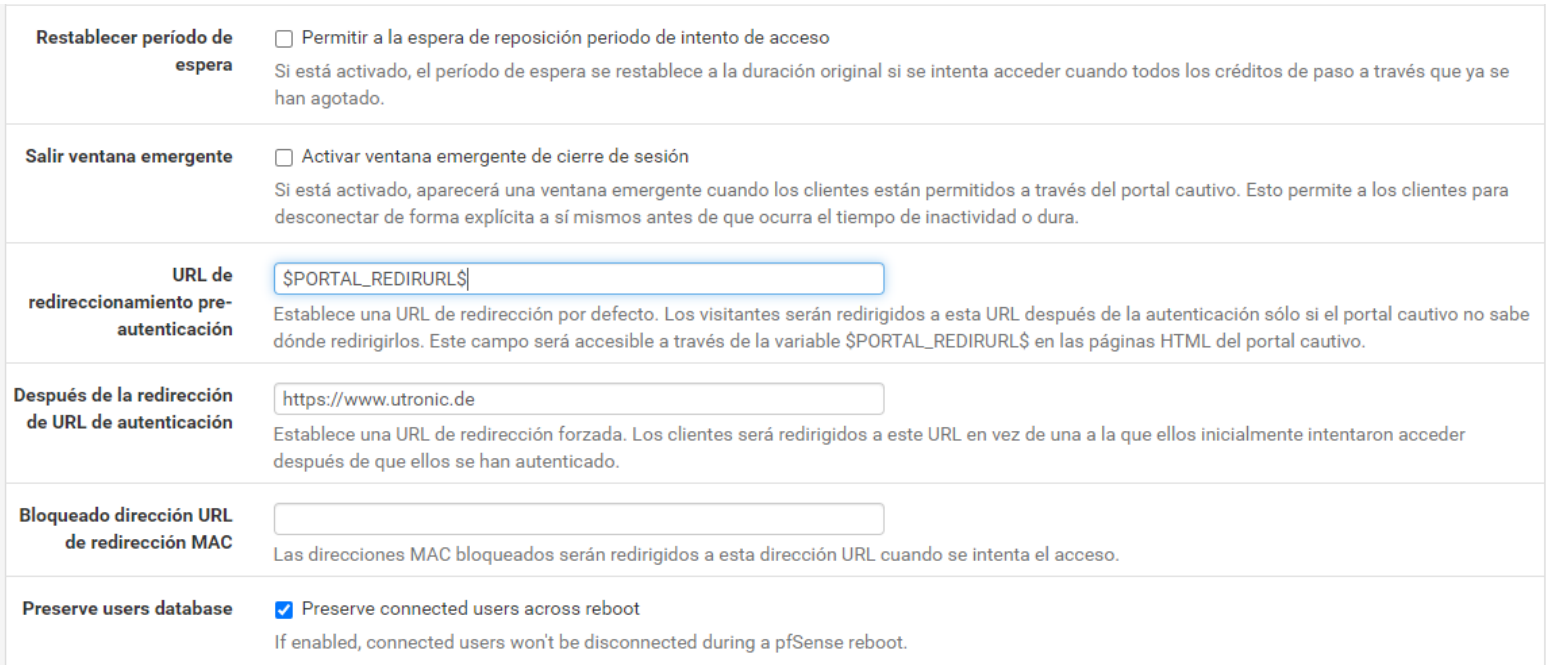



Guardamos y continuamos...

Ahora habilitamos el portal cautivo y en interfaces seleccionamos LAN, luego en tiempo de espera de inactividad, ponemos 15 (minutos) si el usuario en ese tiempo no tiene actividad en la red es desconectado automáticamente por su propia seguridad.




Seguimos rellenando...
En URL después de redirección pongo la página web de mi empresa aquí en Alemania. (https://utronic.de)



Damos click en “Preserve users database”, esto hará que al reiniciar PfSense por cualquier motivo, no saque ni desconecte a ningún usuario conectado a la red

**¡AQUÍ VOY!**

## Webgrafía / Bibliografía:

Descargar VMWare, la versión Player que es gratuita:
https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

Descargar la ISO de PfSense 2.6.0
https://www.pfsense.org/download/

Obtener información sobre instalación de paquetes:
https://forum.netgate.com/topic/98740/any-way-to-install-nano-on-2-3/14