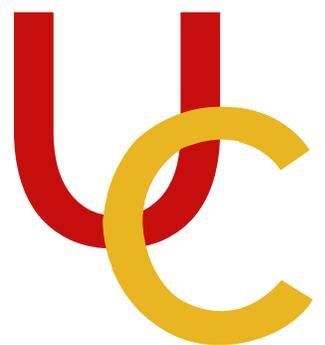


Conexion VPN mediante Pfsense

Manual de instalación y configuración



UNIDAD DE CÓMPUTO

DIVISIÓN DE INGENIERÍAS CIVIL Y GEOMÁTICA

FACULTAD DE INGENIERÍA, UNAM

Tel: 5622-8005 ext. 1037 | dicyg@ingenieria.unam.edu | dicyg.fi-c.unam.mx © 2022-1

Revisión: M. I. Tanya Itzel Arteaga Ricci

CONTENIDO

Pfsense	3
¿Qué es Pfsense?	3
Requisitos necesarios para utilizar Pfsense	3
Configuración de la VPN en Pfsense	8
Configuración	9
Creación del Cliente	17
Créditos	21

PFSENSE.

¿QUÉ ES PFSENSE?

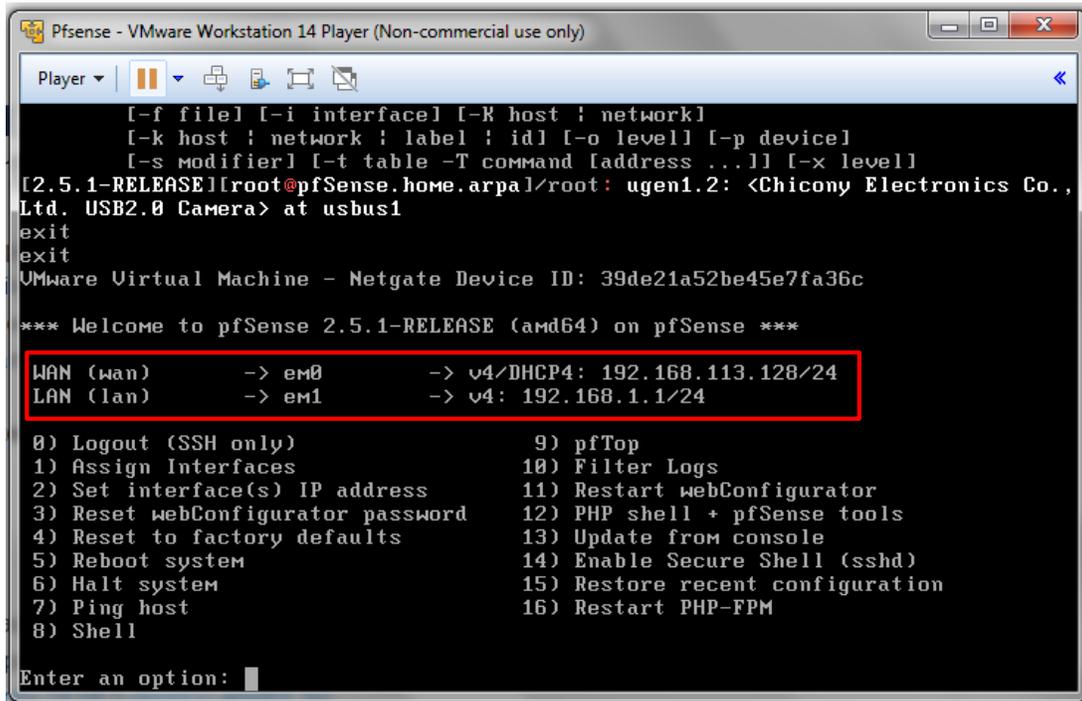
Es un Sistema Operativo orientado a firewall, open source basada en en FreeBSD lo que implica que se tiene la garantía de tener un sistema operativo estable, robusto y seguro.

REQUISITOS NECESARIOS PARA UTILIZAR PFSENSE.

Para poder utilizar el Sistema Operativo Pfsense, es necesario contar con una máquina virtual en la cual se hará la instalación de este mismo.

En la máquina virtual se debe de hacer la instalación del ISO de Pfsense, el cual se puede descargar desde la página oficial de [Pfsense](http://www.pfsense.org). Cuando se realiza la instalación se debe asignar la IP a la red WAN que se va a utilizar, la cual debe ir conectada a Internet y la otra que será una red LAN la cual nos permitirá conectar otra máquina virtual para acceder a Pfsense.

Al finalizar la instalación de Pfsense en la primera máquina virtual, aparecerá en pantalla el puerto que se asignó a cada una de las redes, así como la IP correspondiente. Así mismo aparecerá el menú en el cual podemos acceder a distintas características que posee el Sistema, esto se puede ver en la Figura 1.



```

PfSense - VMware Workstation 14 Player (Non-commercial use only)
Player
[-f file] [-i interface] [-R host ; network]
[-k host ; network ; label ; id] [-o level] [-p device]
[-s modifier] [-t table -T command [address ...]] [-x level]
[2.5.1-RELEASE][root@pfSense.home.arpal/root: ugen1.2: <Chicony Electronics Co., Ltd. USB2.0 Camera> at usb1
exit
exit
VMware Virtual Machine - Netgate Device ID: 39de21a52be45e7fa36c
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.113.128/24
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:

```

Fig. 1 Menú del Sistema Operativo Pfsense en la máquina virtual.

Otro requisito necesario para la utilización del Sistema Operativo Pfsense, es una segunda máquina virtual, la cual puede tener un Sistema Operativo como Linux que es más ligero y fácil de usar, o si se prefiere se puede instalar alguna de las versiones de Windows, aunque suelen requerir mayor espacio de almacenamiento para su ejecución.

En la segunda máquina virtual se deberá corroborar que la IP asignada a la máquina, pertenece a la red LAN del Pfsense, en caso contrario, se deberá asignar manualmente.

Una vez iniciada la segunda máquina virtual, abrimos el navegador con el que cuente la máquina virtual y se accederá a la red LAN del Pfsense mediante su dirección IP, como se muestra en la Figura 2.

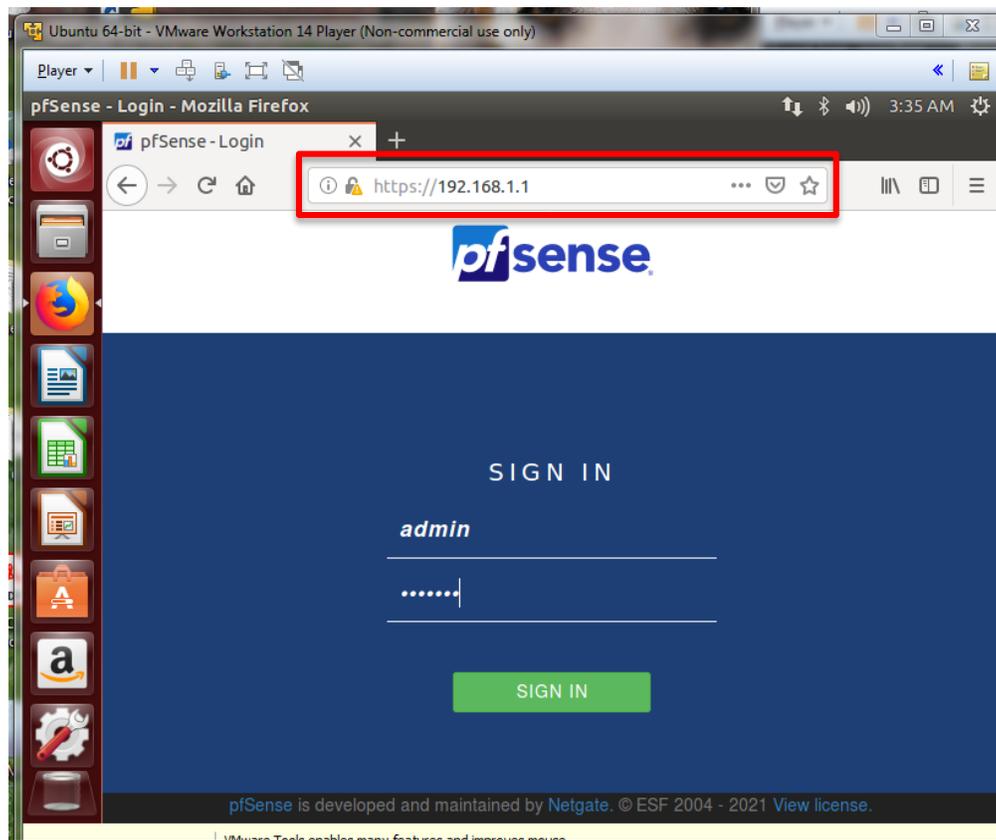


Fig. 2 Portal de Inicio del Pfsense en el navegador de la segunda máquina virtual.

En la Figura 2 podemos observar que para poder iniciar sesión en Pfsense, es necesario introducir el usuario y contraseña, los cuales ya están predeterminados por el mismo sistema, los cuales son:

Usuario: admin

Contraseña: pfsense

Y posteriormente damos clic en **SIGN IN**.

Se recomienda cambiar la contraseña predeterminada por otra con mayor seguridad.

Una vez iniciada sesión en el portal de Pfsense, se desplegará en pantalla el estado del Sistema Operativo Pfsense que se ha instalado en la primera máquina virtual, esto lo podemos observar en la Figura 3 que se encuentra a continuación.

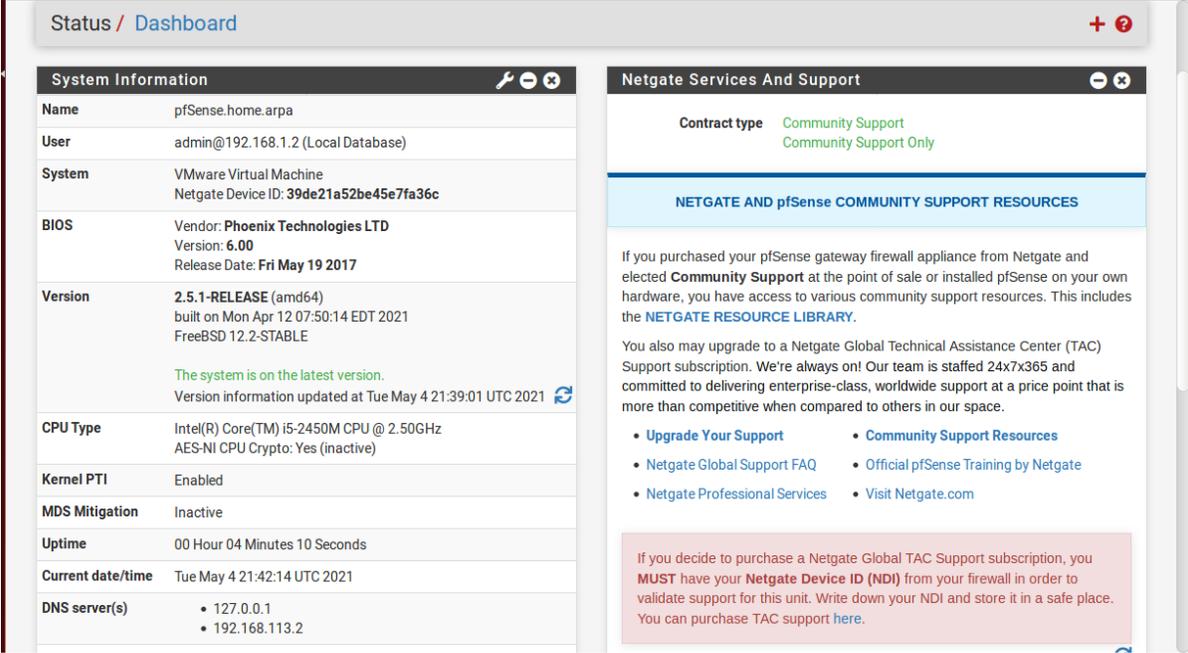


Fig. 3 Información del Sistema desplegado en el portal de Pfsense.

En la Figura 4 se muestra el apartado de **Interfaces** donde podemos encontrar la dirección IP asignada a la red WAN y la IP asignada a la red LAN, así como el estado de ambas.

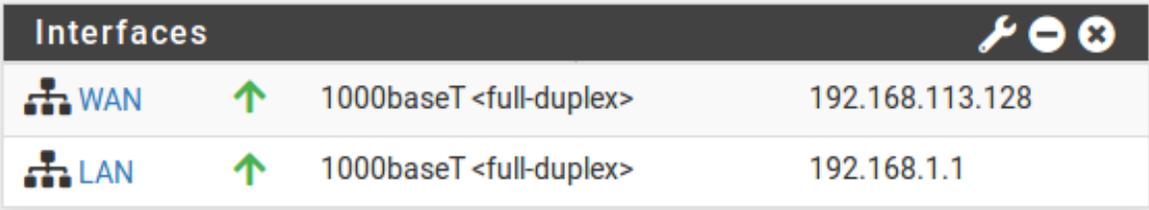


Fig. 4 Sección Interfaces en la Información del Sistema.

Hasta el momento podemos saber que tenemos dos máquinas virtuales, la primera tiene nuestro Sistema Operativo Pfsense y es ahí donde se asignó la dirección IP para la red WAN y otra dirección IP para nuestra red LAN; de igual forma la red LAN está asignado una dirección IP a

nuestra segunda máquina virtual desde la cual accederemos al Pfsense para realizar la configuraciones que requerimos.

Antes de realizar la configuración de la VPN (Virtual Personal Network), es necesario corroborar que se tiene conexión a internet desde el portal de Pfsense; para poder realizarlo, buscamos en el menú principal la opción **DIAGNOSTICS**, damos clic y se desplegará el menú de este apartado, después damos clic en la opción **PING**. (Observe Figura 5)

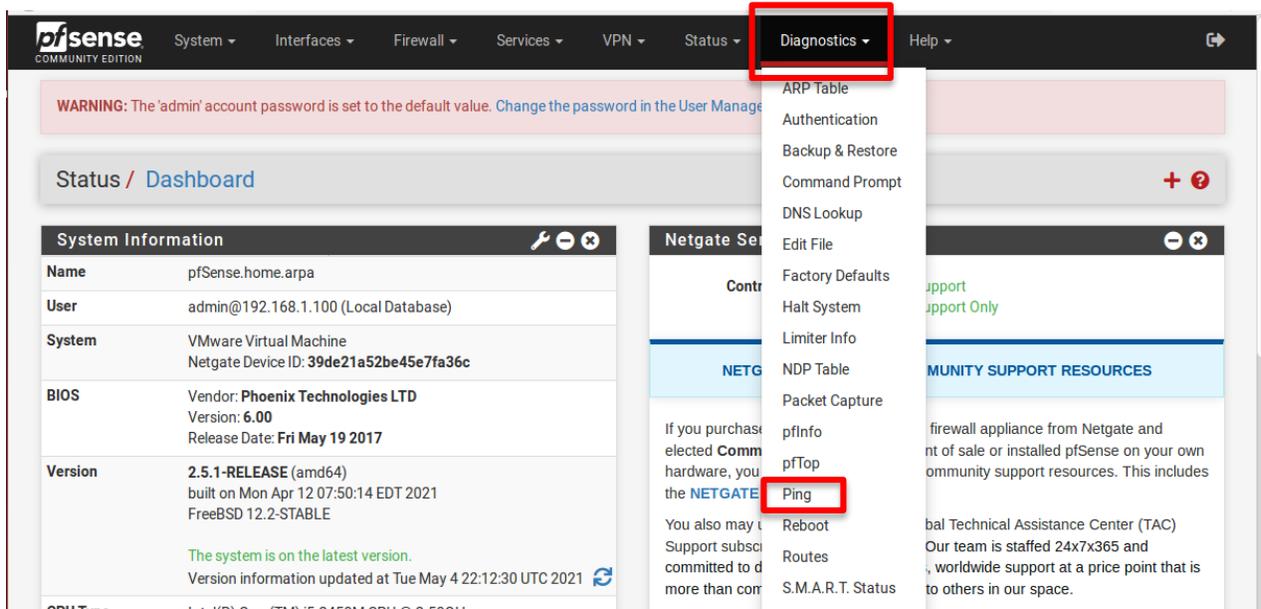


Fig. 5 Despliegue del menú al seleccionar la opción *Diagnostics*.

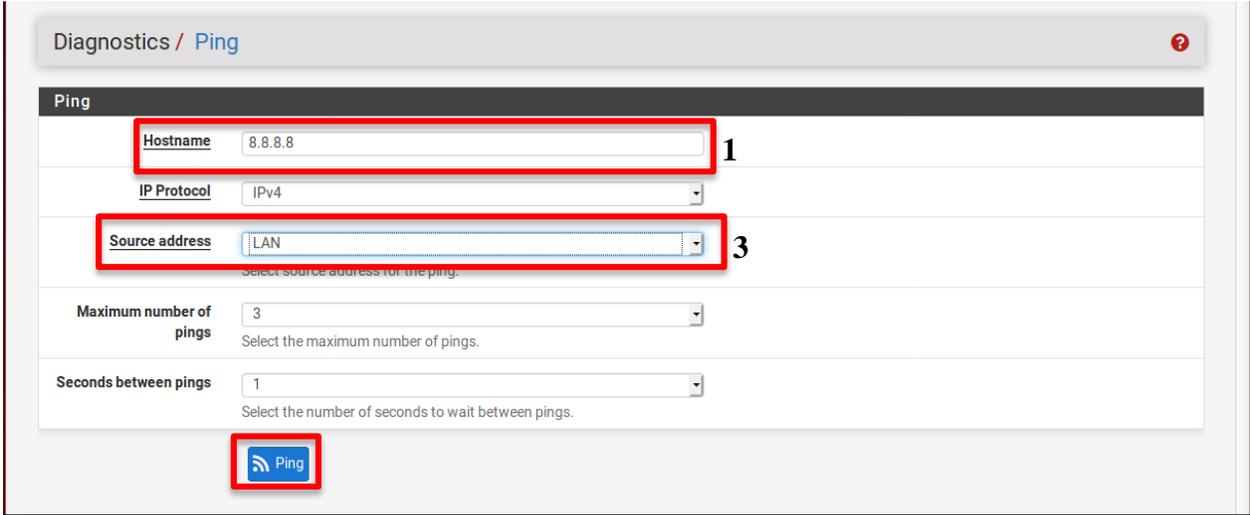
La herramienta Ping nos permite comprobar la conectividad de nuestra máquina con un determinado equipo de la red (o servidor externo) y, además, nos medirá el tiempo que tardan los paquetes en llegar.

Al seleccionar la opción de Ping, aparecerá en pantalla las opciones que se muestran en la Figura 6. La cuales incluye:

1. **Hostname**, en este caso se hizo la prueba con la dirección al DNS de Google la cual es 8.8.8.8
2. **IP Protocol**.
3. **Source address**, donde se puede seleccionar la red WAN o la red LAN, en ambos casos se debe de tener conectividad.
4. **Maximum numbers of pings**, aquí se seleccionara el número de paquetes de datos que queremos que se envíen.
5. **Seconds between pings**.

Los únicos dos parámetros que se modificaron fueron el 1 y el 3, al dar clic en el botón Ping, se realiza la prueba de conectividad; el resultado se muestra en la Figura 7, la cual se comprobó que

en la red LAN del PfSense se tiene conexión a internet, lo que implica que nuestra segunda máquina virtual tiene conexión a internet.



Diagnosics / Ping

Ping

Hostname 8.8.8.8 1

IP Protocol IPv4

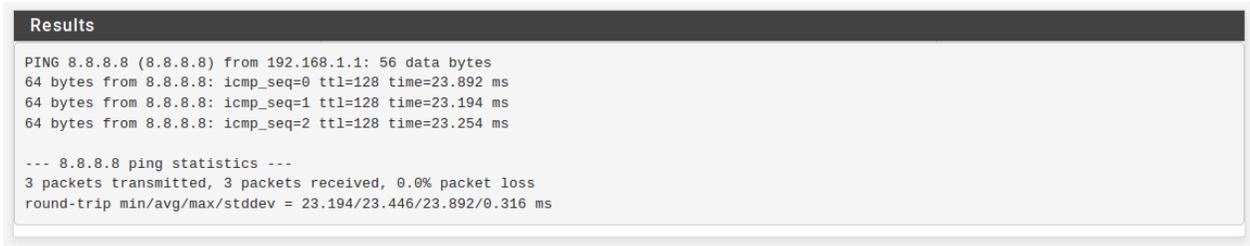
Source address LAN 3
Select source address for the ping.

Maximum number of pings 3
Select the maximum number of pings.

Seconds between pings 1
Select the number of seconds to wait between pings.

Ping

Figura 6. Comprobación de conectividad mediante la opción de Ping.



```
Results
PING 8.8.8.8 (8.8.8.8) from 192.168.1.1: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=23.892 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=23.194 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=23.254 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 23.194/23.446/23.892/0.316 ms
```

Figura 7. Resultados de la prueba de Ping al DNS de Google.

CONFIGURACIÓN DE LA VPN EN PFSENSE.

Para poder realizar la configuración de la VPN en Pfsense, primero debemos descargar el Package Manager de OpenVPN, para ello en el menú principal damos clic en la opción **System**, posteriormente en la opción **Package Manager** y por ultimo seleccionamos el apartado de **Available Package**.

Como podemos observar en la Figura 8, en el buscador de términos escribimos open y damos clic en el botón **Search**; en el listado que aparecerá, buscamos **openvpn-client-export** y damos clic en el botón **+Install**, para que inicie la instalación de este paquete.

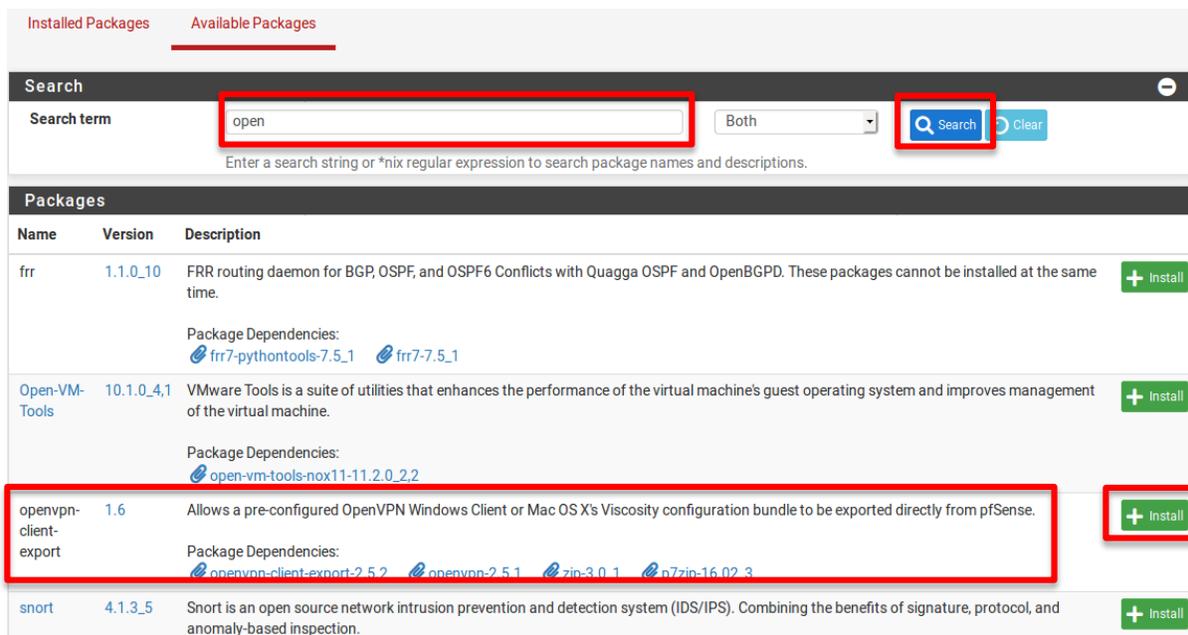


Figura 8. Instalación de Package Manager de OpenVPN.

Al iniciar la instalación del **openvpn-client-export**, nos desplazara a la pestaña **Package Installer** y solo deberemos dar clic en **Confirm** (Figura 9).

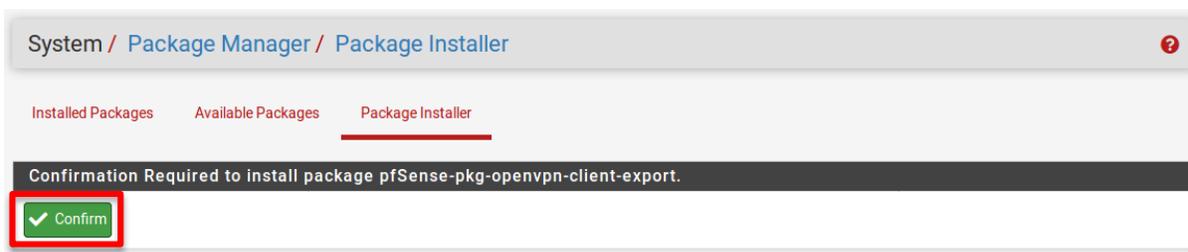


Figura 9. Confirmación de la instalación del Package Manager de OpenVPN

Cuando la instalación del Package Manager de OpenVPN haya finalizado, nos aparecerá un mensaje en verde, que la instalación se hizo completada con éxito, como lo podemos ver en la Figura 10.

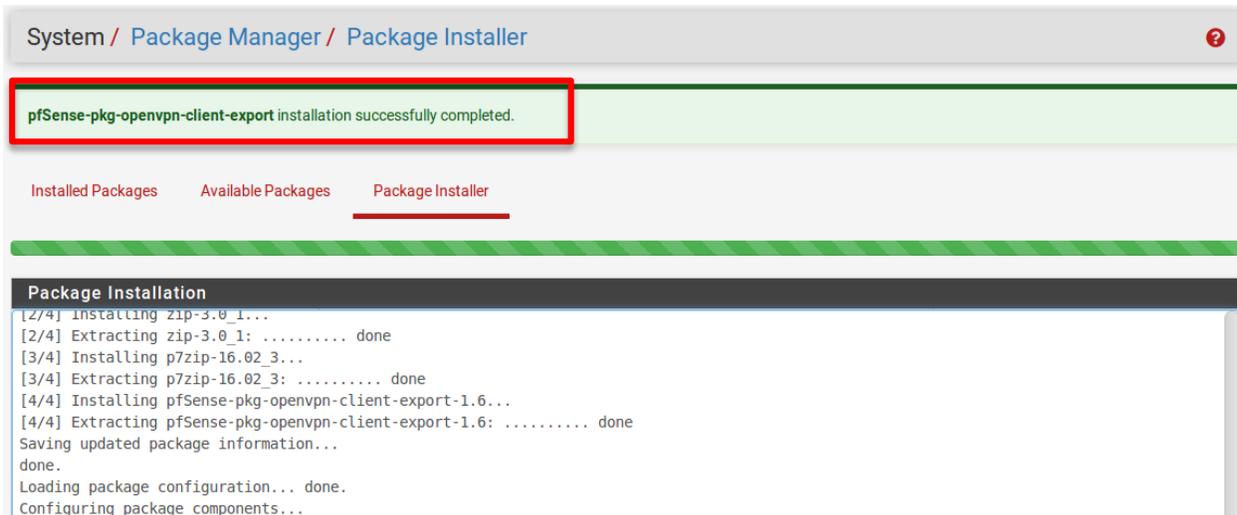


Figura 10. Finalización de la instalación del Package Manager de OpenVPN.

Una vez finalizada la instalación del Package Manager de OpenVPN, obsérvese la Figura 11, en la cual nos dirigimos al menú y seleccionamos la opción VPN, ahí se desplegará un submenú en el cual seleccionaremos la opción OpenVPN.

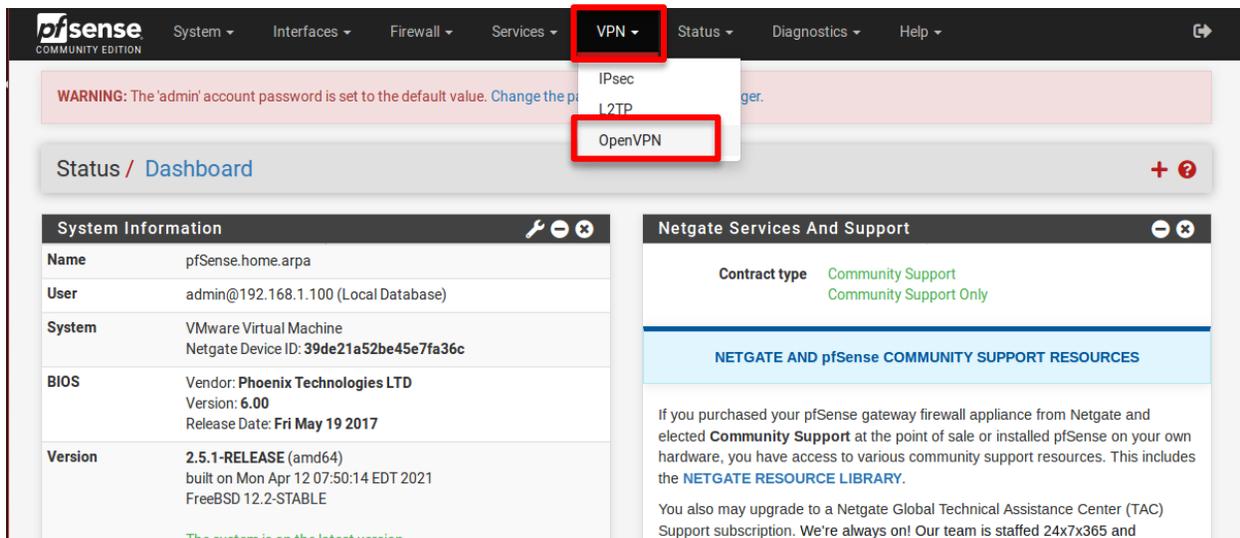


Figura 11. Selección de la opción OpenVPN en el submenú de VPN.

Cuando se haya seleccionado la opción de **OpenVPN** aparecerá en pantalla las opciones que tenemos así como los servidores que hemos creado en **OpenVPN**, como podemos ver en la Figura 12, no tenemos ningún servidor, por lo cual se creará uno para poder utilizar el **OpenVPN**. Seleccionamos la opción **Wizards** para ello.

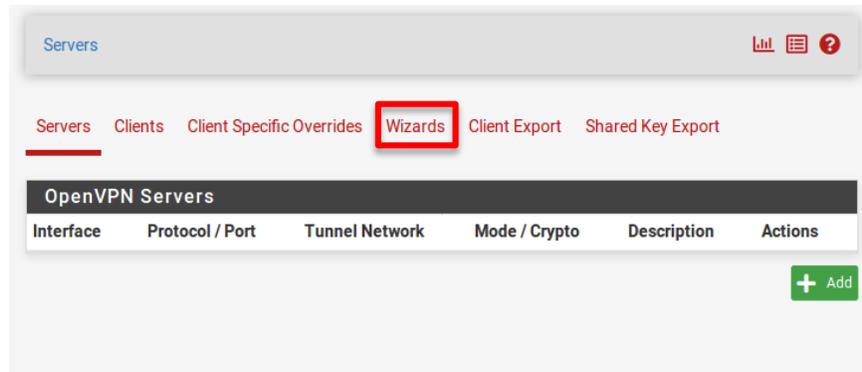


Figura 12. Selección de la opción *Wizards* para la creación de un servidor para OpenVPN.

Una vez seleccionada la opción de Wizards, aparecerá en la pantalla los apartados que podemos ver en la Figura 13, en la cual se seleccionara el Tipo de Servidor que vamos a ocupar, en este caso se ocupará un **Local User Access**, lo que significa que solo permitira acceder al servidor de OpenVPN que crearemos a aquellos usuarios locales, por consiguiente, sería solamente aquellos pertenecientes a nuestra red LAN que tenemos en el Pfsense. Y se da clic en el boton Next para continuar con la configuración del servidor.

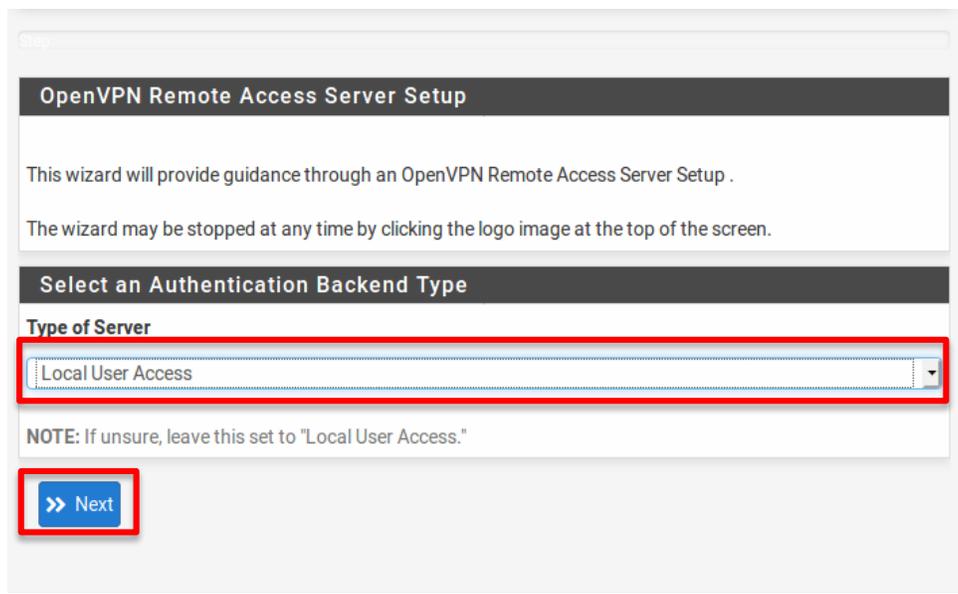
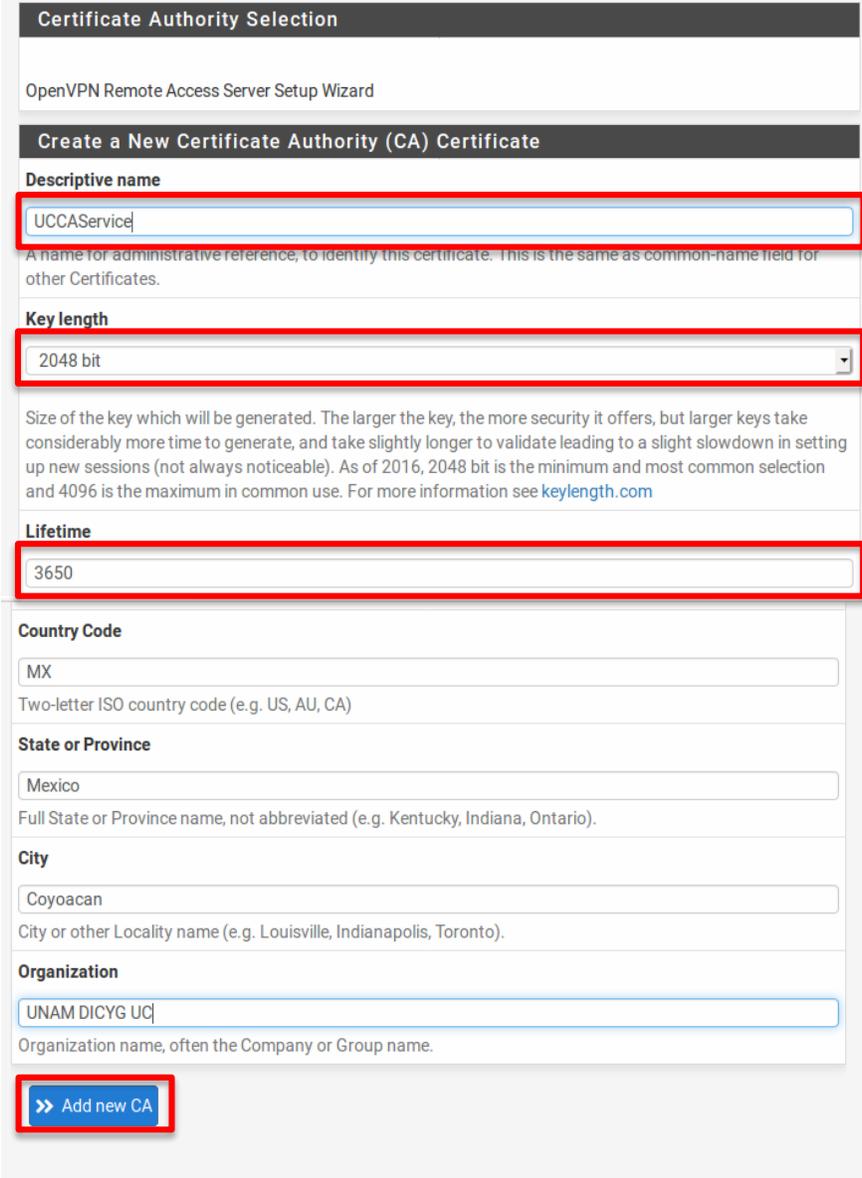


Figura 13. Selección del tipo de servidor.

Una vez seleccionado el Tipo de Servidor, se continuara con la creacion del **Certificate Authority (CA)**, para ello es necesario llenar los recuadros que aparecen en la Figura 14, en la cual nos piden el nombre que le daremos a la unidad certificadora (**Descriptive name**), es quien va a emitir los certificados; lo siguiente es la longitud de la llave (**Key length**), en este caso se escogio una longitud de 2048bits, por cuestiones de seguridad no se recomienda que tenga un longitud menor a esta; por ultimo está el lifetime nos dice cuantos dias quremos que sea valida esta unidad

certificadora, lo indicado es un tiempo razonable, los administrativos son los que deciden este tiempo.

Los demas espacios son solo datos de información, una vez que se han llenado, damos clic en el boton **Add New CA**.



Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name
UCCAServic
A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Key length
2048 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime
3650

Country Code
MX
Two-letter ISO country code (e.g. US, AU, CA)

State or Province
Mexico
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City
Coyoacan
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization
UNAM DICYG UC
Organization name, often the Company or Group name.

>> Add new CA

Figura 14. Creación del Certificate Authority.

Ahora se creara el certificado del servidor de la red VPN, con el cual se utilizara para identificar que es el mismo. Aquí podemos observar en la Figura 15 que son los mismos datos utilizados para la creación del *Certificate Authority* (Figura 14). Por ultimo se da clic en el boton de **Create new Certificate**.

Create a New Server Certificate

Descriptive name

A name for administrative reference, to identify this certificate. This is also known as the certificates "Common Name."

Key length

Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime

Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Country Code

Two-letter ISO country code (e.g. US, AU, CA)

State or Province

Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City

City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization

Organization name, often the Company or Group name.

[» Create new Certificate](#)

Figura 15. Creación del certificado de la red VPN.

Ya se creó la Unidad Certificadora (Figura 14) y ya se creó el certificado del servidor (Figura 15), ahora vamos a hacer la configuración del Servidor de OpenVPN.

Como podemos ver en la Figura 16, el primer recuadro nos pide seleccionar el tipo de **Interface** y debajo del recuadro nos dice “*The interface where OpenVPN will listening for incoming connections (typically WAN)*”, en este caso se seleccionara nuestra red WAN porque es la que tiene salida a internet.

Después seleccionaremos el tipo de **protocolo**, lo normal es utilizar UDP pero aquí seleccionaremos **TCP** porque nos garantiza la entrega de paquetes y podemos rastrear problemas en la conexión VPN.

En la selección del puerto por el cual OpenVPN escuchará las conexiones (**Local Port**), el puerto por default es el 1194, el cual es un puerto ya reservado para OpenVPN pero se puede utilizar otro para ocultar este ya existente.

Y por último en el recuadro de **Description**, solo agregamos un nombre para el Servidor OpenVPN.



General OpenVPN Server Information

Interface
WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)

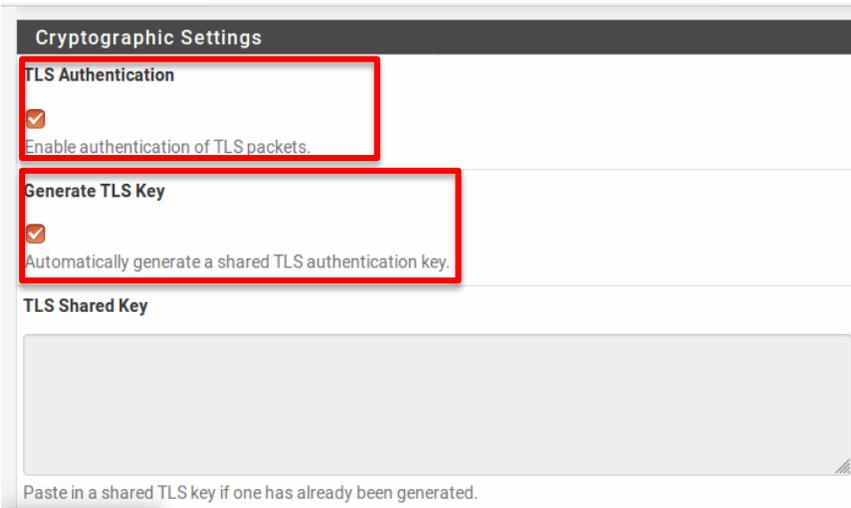
Protocol
TCP on IPv4 only
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Local Port
1201
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Description
VPN1Admin
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Figura 16. Información general de la creación del Servidor OpenVPN.

Continuando con la configuración del Servidor OpenVPN, encontramos el apartado de Configuración Criptográfica (**Cryptographic Settings**), en la cual seleccionaremos **TLS Authentication** y **Generate TLS Key**, esto nos ayudará a que el servidor genere las llaves TLS. (Figura 17).



Cryptographic Settings

TLS Authentication

Enable authentication of TLS packets.

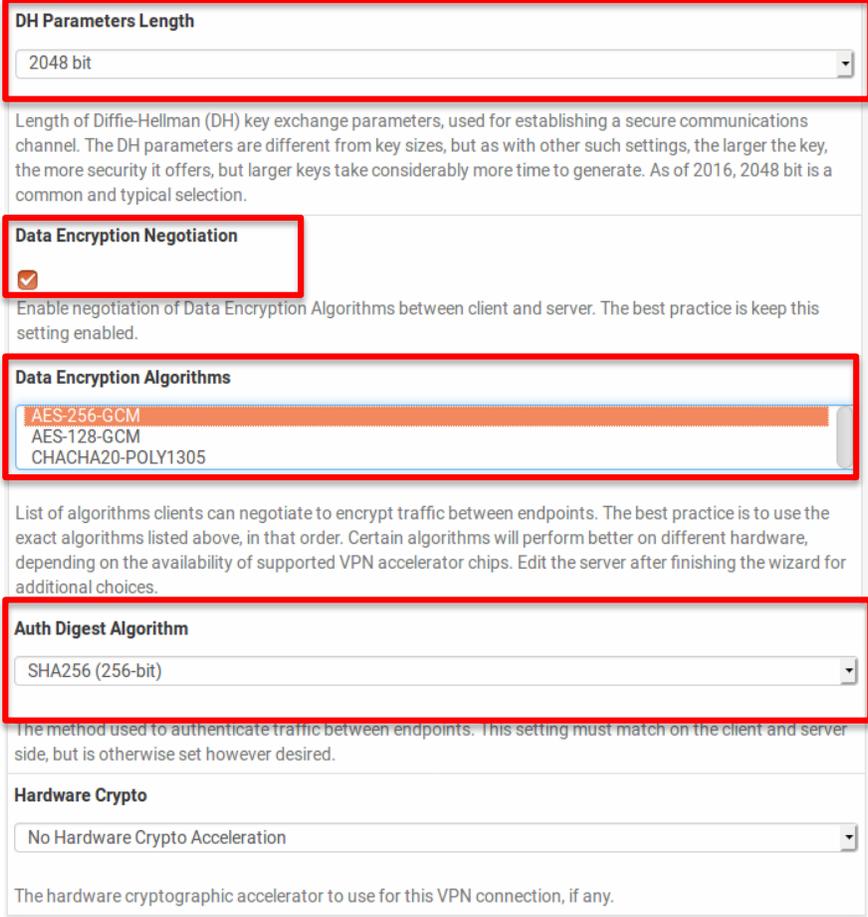
Generate TLS Key

Automatically generate a shared TLS authentication key.

TLS Shared Key

Paste in a shared TLS key if one has already been generated.

Figura 17. Configuración Criptográfica Parte I.



DH Parameters Length

2048 bit

Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.

Data Encryption Negotiation

Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.

Data Encryption Algorithms

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.

Auth Digest Algorithm

SHA256 (256-bit)

The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.

Hardware Crypto

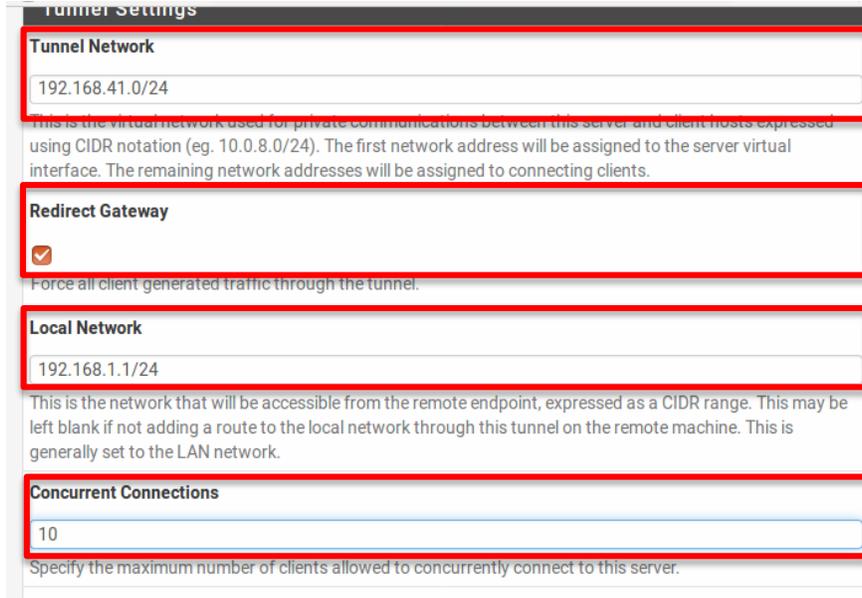
No Hardware Crypto Acceleration

The hardware cryptographic accelerator to use for this VPN connection, if any.

Figura 18. Configuración Criptográfica Parte II.

En la Figura 18 continuamos con los parámetros de la Configuración Criptográfica, en la cual tenemos *DH Parameters Length*, que como se mencionó anteriormente (Figura 14) la longitud mínima recomendada es de 2048 bits y aquí podemos ver qué tipo de algoritmo usa para la generación de llaves. Así mismo seleccionamos en la parte de *Data Encryption Algorithms*, la opción AES-256-GCM y en *Auth Digest Algorithm* la opción SHA256 (256-bit).

A continuación se deberá realizar la configuración del túnel, en el *Tunnel Network* se escribirá la dirección IP por la cual queremos que pase nuestra conexión y nuestros datos, la cual creamos nosotros mismo, por ello también se debe marcar la opción de *Redirect Gateway* para que todo esto pase por el túnel y en el apartado de *Local Network* deberemos introducir la dirección IP a la cual queremos conectarnos desde afuera, en este caso será nuestra red LAN del Pfsense. Por último escribimos cuantas conexiones concurrentes queremos permitir (clientes al mismo tiempo que se permiten) en el apartado de *Concurrent Connections*. (Figura 19).



Tunnel Settings

Tunnel Network
192.168.41.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect Gateway

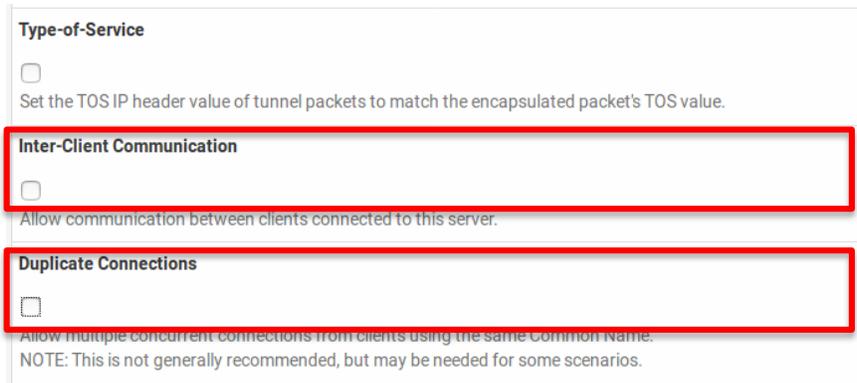
Force all client generated traffic through the tunnel.

Local Network
192.168.1.1/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent Connections
10
Specify the maximum number of clients allowed to concurrently connect to this server.

Figura 19. Configuración del Túnel Parte I.

Es importante **NO** seleccionar la opción *Inter-Client Communication* si no deseamos que los clientes se comuniquen entre sí, así mismo la opción **Duplicate Connections**, **NO** se debe seleccionar, porque como su nombre lo indica, permitiría que se duplicaran las conexiones y esto puede deberse al robo del certificado del cliente o la llave del cliente, lo que provocaría robo de información. (Figura 20).



Type-of-Service

Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

Inter-Client Communication

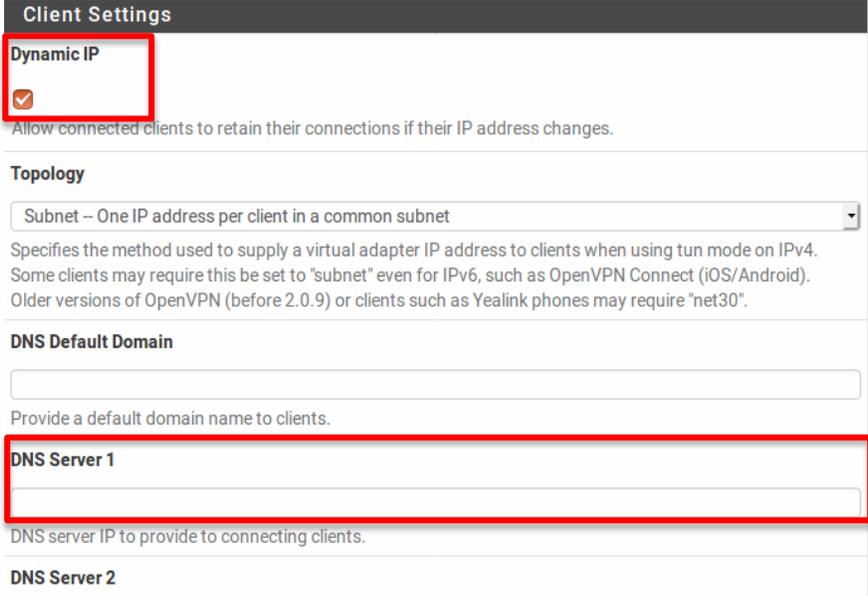
Allow communication between clients connected to this server.

Duplicate Connections

Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.

Figura 20. Configuración del Túnel Parte II.

En la Figura 21, se muestra la configuración de los clientes en la cual seleccionamos *Dynamic IP* y en *DNS Server 1* utilizaremos la dirección IP 192.168.1.1



Client Settings

Dynamic IP

 Allow connected clients to retain their connections if their IP address changes.

Topology
 Subnet – One IP address per client in a common subnet
 Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

DNS Default Domain

 Provide a default domain name to clients.

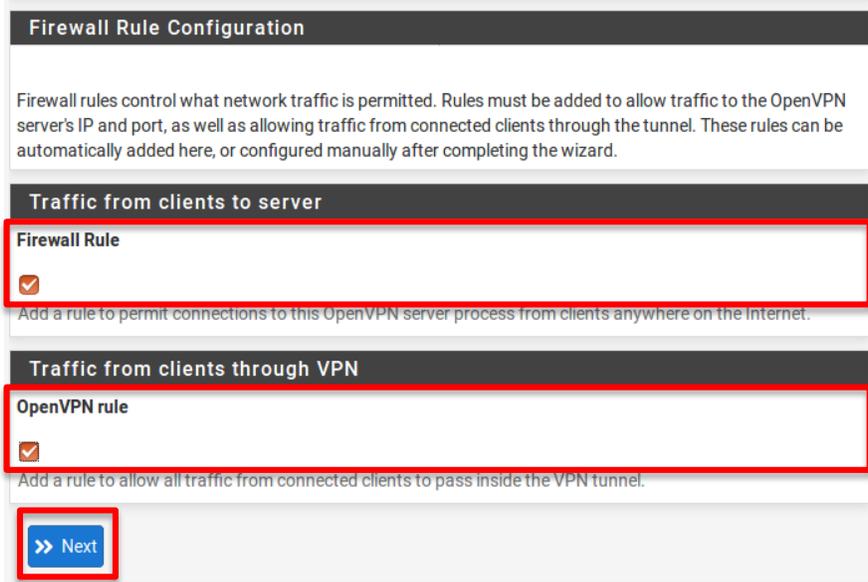
DNS Server 1

 DNS server IP to provide to connecting clients.

DNS Server 2

Figura 21. Configuración del cliente.

Para finalizar la configuración del Servidor OpenVPN, en el apartado de *Traffic from clients to server*, seleccionamos la opción de **Firewall Rule**, lo que nos permite que se cree automáticamente la regla de Firewall y no tengamos que hacerlo manualmente, también seleccionamos la opción **OpenVPN rule** para que permita el tráfico a través de la VPN; y finalizamos dando clic en el botón **Next**. (Figura 22).



Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule

 Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule

 Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

>> Next

Figura 22. Apartados finales de la configuración del servidor OpenVPN.

En la Figura 23 tenemos la finalización de la configuración del Servidor OpenVPN y lo único que se debe hacer es dar clic en el botón **Finish**.

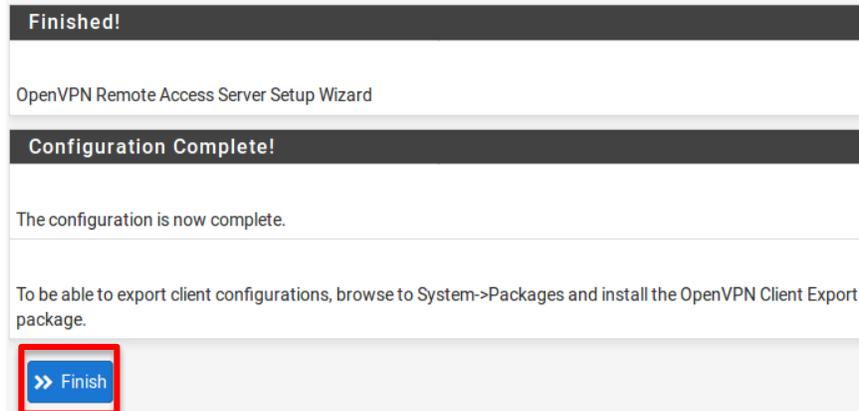


Figura 23. Finalización de la configuración del Servidor de OpenVPN.

Si seleccionamos en el menú **VPN > OpenVPN > Servers**, deberá aparecer el Servidor OpenVPN que acabamos de crear, así como el tipo de protocolo y puerto que seleccionamos, la dirección del túnel junto con configuración criptográfica, la descripción del servidor, y por último tenemos la opción de editarlo o eliminarlo. (Ver Figura 24).

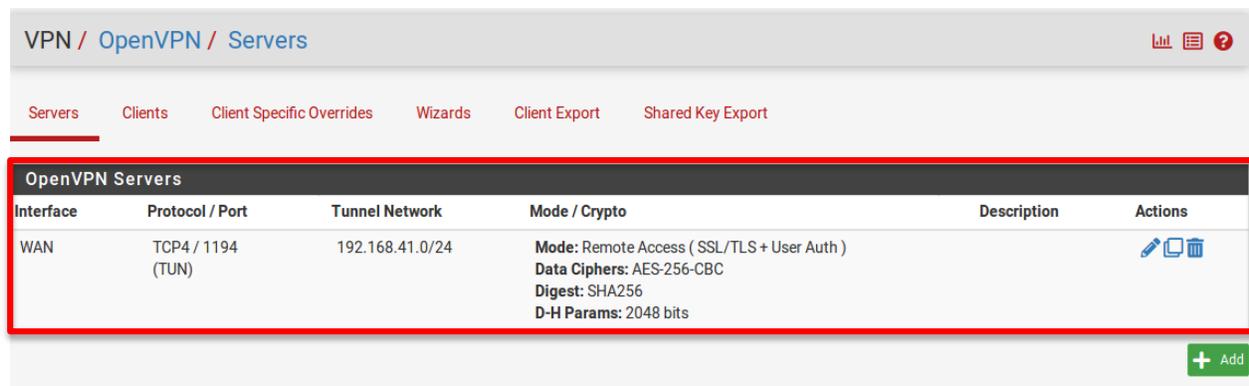


Figura 24. Comprobación de la creación del Servidor OpenVPN con la configuración deseada.

CREACIÓN DEL CLIENTE

Como se decidió que el Servidor OpenVPN sería del tipo Local User, para crear nuestros clientes, accedemos al menú principal y seleccionamos la opción System y en el submenú damos clic en User Manager, esto se muestra en la Figura 25.

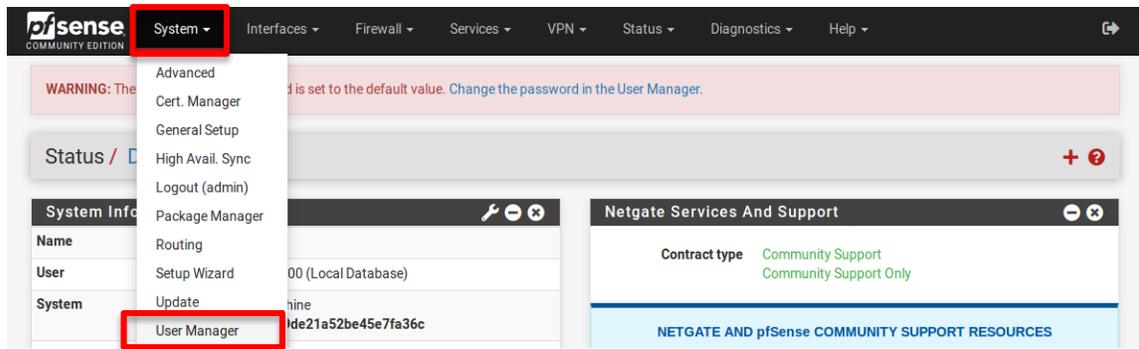


Figura 25. Creación del cliente Parte I.

En la Figura 26 se muestra lo que nos aparecerá en pantalla, así que para crear al cliente, damos clic en el botón + **Add**.

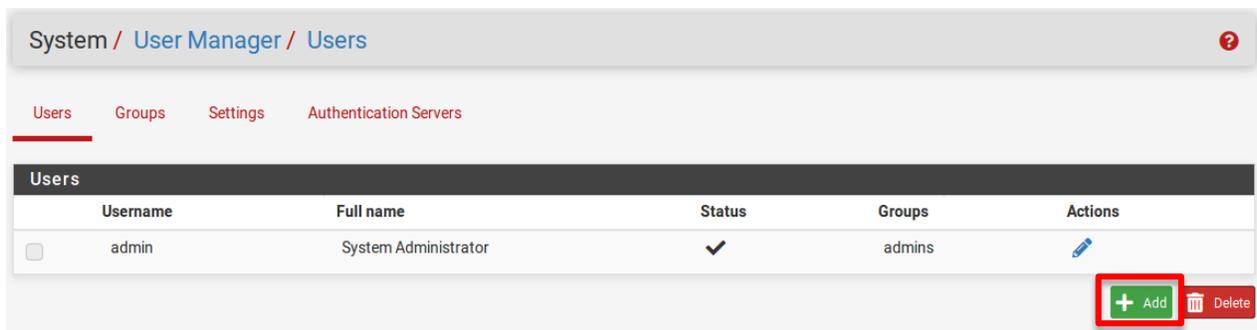
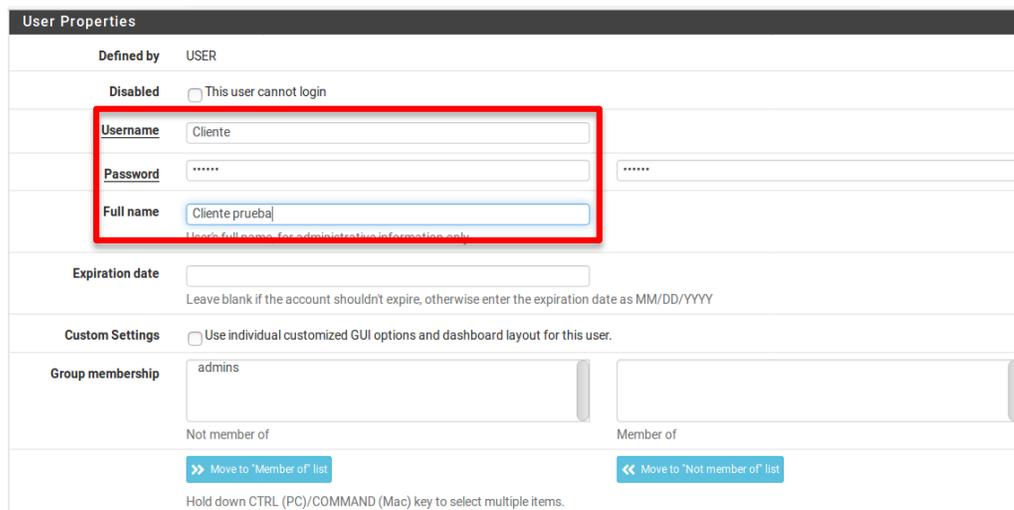


Figura 26. Creación del cliente Parte II.

En el apartado de **User Properties** nos aparecerá la información que debemos llenar, de los cuales definiremos: **Username**, **Password**, **Full name**, con los datos de nuestro cliente. Esto lo podemos ver en la Figura 27 que se muestra a continuación.



User Properties

Defined by: USER

Disabled: This user cannot login

Username:

Password:

Full name:

Expiration date:

Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Not member of:

Member of:

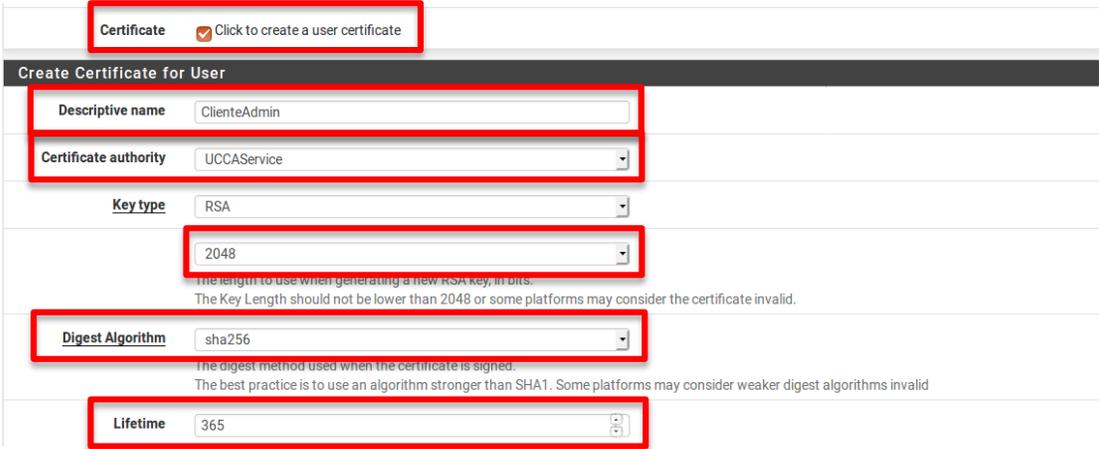
Move to 'Member of' list:

Move to 'Not member of' list:

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

Figura 27. Propiedades de Usuario.

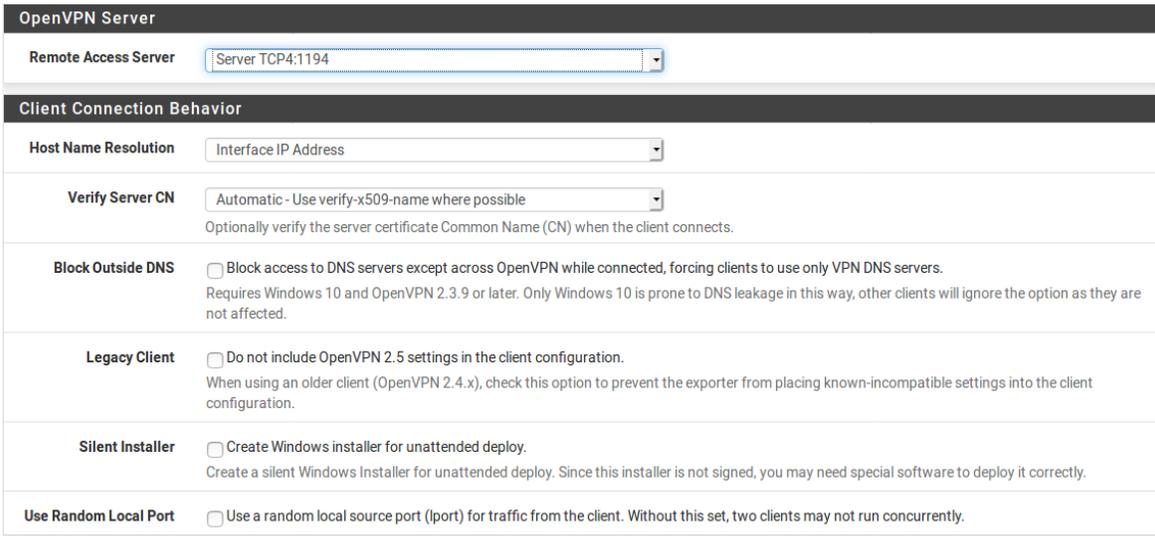
Una vez que hemos escrito los datos de nuestro cliente, ahora se creará un certificado de usuario, para ello seleccionaremos la opción de **Certificate** y aparecerá el apartado de **Create Certificate for User**, en donde hay que escribir un nombre para el certificado, posteriormente asignaremos el Certificado que ya hemos creado y que es el único que hay en sistema, el cual es **UCCAService**, e igual que en la creación de los certificados anteriores, utilizaremos una longitud de llave (**Key Length**) de 2048 y un **Digest Algorithm** SHA256, también modificaremos el **Lifetime** para solo dejarlo en un año (365 días). Todo esto lo podemos observar en la Figura 28.



The screenshot shows the 'Create Certificate for User' form. A red box highlights the 'Certificate' checkbox, which is checked and labeled 'Click to create a user certificate'. Below this, the form fields are: 'Descriptive name' (ClienteAdmin), 'Certificate authority' (UCCAService), 'Key type' (RSA), 'Key length' (2048), 'Digest Algorithm' (sha256), and 'Lifetime' (365). Each of these fields is also highlighted with a red box. Small text below the key length and digest algorithm fields provides additional context: '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.' and '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.'

Figura 28. Creación del certificado para el cliente.

Ahora se debe exportar al cliente para ello nos vamos al menú principal y seleccionamos la opción **VPN** y posteriormente **OpenVPN** y **Client Export**. Deberá aparecer en la pantalla la información como en la Figura 29.



The screenshot shows the 'OpenVPN Server' configuration page. The 'Remote Access Server' is set to 'Server TCP4:1194'. Under the 'Client Connection Behavior' section, the following settings are visible: 'Host Name Resolution' (Interface IP Address), 'Verify Server CN' (Automatic - Use verify-x509-name where possible), 'Block Outside DNS' (unchecked), 'Legacy Client' (unchecked), 'Silent Installer' (unchecked), and 'Use Random Local Port' (unchecked). Each setting includes a brief description of its function.

Figura 29. Exportación de cliente.

Todo la información se va por default, no debemos modificar nada y nos desplazamos hasta la parte final donde esta **OpenVPN Clients**, ahí vamos a la opción de **Current Windows Installers** y dependiendo de la máquina del cliente, ya sea 32 o 64 bits, descargamos el archivo correspondiente.

Este archivo es el que deberá instalar nuestro cliente para poder conectarse mediante OpenVPN.

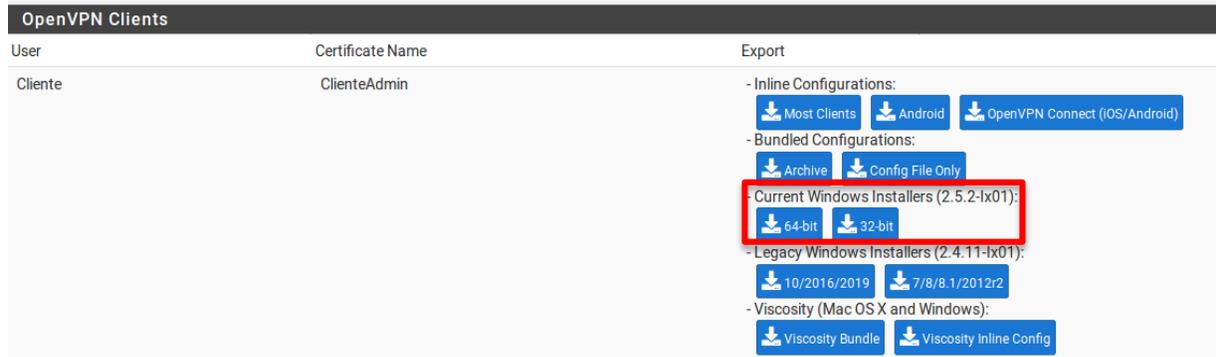


Figura 30. Opciones de descarga para la exportación de cliente OpenVPN.

Siguiendo las instrucciones anteriores paso a paso, se lograra realizar la instalación y configuración de una conexión VPN mediante Pfsense de manera exitosa.

CRÉDITOS

Nombre del Manual

Fecha de creación: *Mayo 13, 2021*

Versión: *1.0*

Última actualización: *Agosto 19, 2021*

Revisión: *1.0.0*

Autores

Ocaña Sandoval Vanessa Guadalupe.
Servicio Social.
Infraestructura.
1.0.0

Revisión y aprobación del documento

Arteaga Ricci Tanya Itzel.
Jefa de Unidad de Computo.
Unidad de Computo.
1.0.0

Bonilla Pastor Abraham
Ayudante de Profesor.
Infraestructura.
1.0.0