

El objetivo de este hack (contrario a este) es crear el servidor OpenVPN en PFSense con la menor seguridad posible, para realizar una conexión lo más rápida posible, pero sin utilizar el wizard. Vamos a ello.

1 - CREAR LA AUTORIDAD CERTIFICADORA

Vamos al menú «System» >> «Certificate», pestaña «Authorities» y hacemos click en «Add».

• Descriptive Name: Nombre para la CA.

• Resto: Dejar todo por defecto.

2 - CREAR UN CERTIFICADO PARA EL SERVIDOR

Vamos al menú «System» >> «Certificate», pestaña «Certificates» y hacemos click en «Add».

• Method: Create an Internal Certificate.

• Descriptive Name: OpenVPNServer.

• Certificate Authority: La Autoridad certificadora creada en el paso 1.

• Common Name: El FQDN con el sobdominio

• Certificate Authority: Server Certificate.

• Resto: Dejar todo por defecto.

3 - CONFIGURAR EL SERVIDOR

Vamos al menú «VPN» >> «OpenVPN», pestaña «Servers» y hacemos click en «Add».

• Description: SimpleOpenVPN

• Server Mode: Remote Access (User Auth).

• Backend for authentiction: Local database.

• Device Mode: tun (Layer 3).

• **Protocol:** TCP on IPv4 only.

• Interface: WAN.

• Local port: 1194 (O cualquier otro).

• TLS Configuration: Use a TLS key desmarcado.

• Peer Certificate Authority: La que creamos en el paso 1.

• Server certificate: El que creamos en el paso 2.

• Client Certificate Key Usage Validation: Enforce key usage desmarcado.

• IPv4 Tunnel Network: La dirección de subred del tunel.

• IPv4 Local networks: La subred de la lan, la de la DMZ, etc.

• Gateway creation: IPv4 only (en el caso de que sóno necesitemos IPv4).

4 - CREACIÓN DE USUARIOS

Vamos a Menú >> «System» >> «User Manager» y hacemos click en «Add».



- Username: ovpn (o cualquier otro).
- Password: OpenVPN (o cualquier otro).

Guardamos los cambios para crear el usuario.

5 - CREACIÓN DEL CERTIFICADO PARA EL USUARIO

Con el usuario ya creado, lo editamos, bajamos hasta «User Certificates» y le damos al botón «Add».

- Method: Create an internal certificate.
- Descriptive name: usuario-ovpn.
- Certificate authority: La que creamos antes.
- Common name: usuario-ovpn
- Certificate type: User Certificate.

Nos volverá a la ventana donde estábamos configurando el usuario. Le damos a guardar.

6 - REGLAS DEL CORTAFUEGOS

Vamos al menu «Firewall» >> «Rules», pestaña «WAN» y agregamos una regla con destino en «WAN address» y «Destination port range» en «OpenVPN (1194)».

Ahora vamos a la pestaña OpenVPN y agregamos una regla para pemitir TCP/UDP y otra para permitir ICMP.

7 - EXPORTACIÓN DEL ARCHIVO .ovpn

Vamos al menú «System» >> «Package Manager», pestaña «Available Packages», en el campo de texto del buscador buscamos «**openvpn-client-export**» y lo instalamos. Nos pedirá confirmación y procederá con la instalación.

Una vez instalado vamos a menú «VPN» >> «OpenVPN», pestaña «Client export» y rellenamos con los siguientes datos:

- Remote access server: SimpleOpenVPN TCP4:1194
- Host name resolution: Other.
- Host name: el FQDN.
- Verify Server CN: Do not verify the server CN.
- Bind mode: Do not bind to the local port.

Bajamos hasta el botón que dice «Most Clients» y descargamos la configuración.

Ya estaríamos en condiciones de conectarnos al servidor con el archivo de configuración descargado e indicando ovpn como usuario y OpenVPN como contraseña.

