El objetivo de este hack (contrario a este) es crear un servidor OpenVPN en PFSense con la mayor seguridad posible, pero sin perder funcionalidad. 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.
- **Key Method:** ECDSA (Curva elíptica)
- **Curve:** secp384r1 [HTTPS] [IPSec] [OpenVPN]
- **Digest Algorithm:** SHA-512.
- **Common Name:** El FQDN.

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.
- **Key Type:** ECDSA (Curva elíptica)
- **Curve:** secp384r1 [HTTPS] [IPSec] [OpenVPN]
- **Digest Algorithm:** SHA-512.
- **Common Name:** El FQDN con el sobdominio
- **Certificate Type:** Server Certificate.

3 – CONFIGURAR EL SERVIDOR

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

- **Server Mode:** Remote Access (SSL/TLS + User Auth).
- **Device Mode:** tun (Layer 3).
- **Protocol:** TCP on IPv4 only.
- **Interface:** WAN.
- **Local port:** 1194 (O cualquier otro).
- **TLS Authentication:** Use a TLS Key, marcada. Automatically generate a TLS KEY, marcada.
- **Peer Certificate Authority:** La que creamos en el paso 1.
- **Server certificate:** El que creamos en el paso 2.
- **DH Parameter Lenght:** 8192.
- **ECDH Curve:** secp384r1.
- **Data Encryption Algorithms:** Primero CHACHA20-POLY1305 y luego AES-256-GCM.

- **Fallback Data Encryption Algorithm**: AES-256-GCM.
- **Auth digest algorithm:** SHA3-512.
- **Hardware Crypto:** Si hay alguno, lo seleccionamos.
- **Certificate Depth:** One (Client+Server).
- **Strict User-CN Matching:** Enforce match, marcada.
- **Client Certificate Key Usage Validation:** Enforce key usage, marcada.
- **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

EN PROCESO ...