La idea es explicar en perfecto castellano, las opciones de configuración de este hack donde explico como crear un servidor OpenVPN con las opciones más seguras posibles. Tanto para la seguridad de los datos transmitidos, como para la fiabilidad de la conexión.

**Modo de servidor «Acceso remoto (SSL/TLS + Autenticación de usuario)»:** Requiere SSL/TLS y autenticación de usuario para conectarse. Esta es la opción más segura disponible. No solo aprovecha los beneficios de otras configuraciones SSL/TLS, sino que también exige un nombre de usuario y una contraseña por parte del cliente al conectarse. El acceso del cliente puede revocarse no solo anulando el certificado, sino también cambiando la contraseña. Además, si una clave comprometida no se detecta de inmediato, el riesgo se reduce, ya que es poco probable que el atacante tenga tanto las claves como la contraseña. El asistente de OpenVPN utiliza este modo cuando configura una VPN de acceso remoto.

**Protocolo TCP sólo en IPv4 o IPv6:** El uso de TCP para una VPN es más lento y puede generar más problemas. En algunos casos excepcionales, TCP puede superar limitaciones del entorno del cliente, como eludir cortafuegos al ejecutar un servidor OpenVPN en el puerto TCP 443. TCP es orientado a la conexión con entrega garantizada, lo que significa que cualquier paquete perdido se retransmite. Esto puede parecer una buena idea en principio, pero las retransmisiones de TCP provocan una degradación significativa del rendimiento en conexiones a Internet con alta carga o con pérdidas constantes de paquetes. El tráfico TCP a menudo existe dentro de túneles, y no es deseable retransmitir paquetes perdidos del tráfico VPN encapsulado. En casos donde TCP se encapsula dentro de TCP, como un túnel VPN que usa TCP como protocolo de transporte, si se pierde un paquete, tanto los paquetes TCP externos como los internos se retransmitirán. Aunque esto pueda pasar desapercibido ocasionalmente, una pérdida recurrente generará un rendimiento significativamente inferior al de UDP. Si el tráfico dentro del túnel requiere entrega confiable, usará un protocolo como TCP, que garantiza dicha confiabilidad y gestionará sus propias retransmisiones. Este modo se vincula a una única interfaz y limita a OpenVPN a aceptar exclusivamente IPv4 o IPv6, pero no ambos al mismo tiempo.

**Clave TLS:** Una clave TLS mejora la seguridad de una conexión OpenVPN al requerir que ambas partes tengan una clave común antes de que un par pueda realizar un handshake TLS. Esta capa de autenticación HMAC permite descartar los paquetes del canal de control que no posean la clave adecuada, protegiendo a los pares de ataques o conexiones no autorizadas. La clave TLS no tiene ningún efecto sobre los datos del túnel. Una clave TLS también protege contra algunos ataques basados en SSL, como Heartbleed, que de otro modo podrían comprometer la VPN a través del canal de control.

**Intercambio de claves mediante curva ECDH:** Configura una curva elíptica específica para su uso en intercambios de claves Elliptic Curve Diffie-Hellman (ECDH). Esto se aplica únicamente a la encriptación TLS con ECDH. Por defecto, OpenVPN utiliza la curva especificada en el certificado del servidor cuando está configurado con un certificado ECDSA. De lo contrario, OpenVPN utiliza secp384r1 como alternativa predeterminada.

**Algoritmo de cifrado:** Es la lista de algoritmos de cifrado de datos que OpenVPN puede usar para esta VPN, en orden de preferencia. La selección predeterminada incluye AES-GCM en versiones de 256 y 128 bits, así como ChaCha20-Poly135. La mejor práctica es utilizar cifrados AEAD (Authenticated Encryption with Associated Data) como AES-GCM y ChaCha20-Poly135. Estos cifrados combinan cifrado y autenticación, por lo que no requieren un algoritmo de hash separado. Además de ofrecer una seguridad robusta, suelen ser significativamente más rápidos que otros cifrados. Esta funcionalidad sólo es compatible con el modo cliente/servidor, lo que significa que únicamente funciona con modos SSL/TLS en los que la red del túnel es lo suficientemente grande para múltiples clientes (por ejemplo, más grande que una /30). En modo de clave compartida o al usar una red de túnel /30, OpenVPN utiliza únicamente el valor del algoritmo de cifrado de datos de reserva (Fallback Data Encryption Algorithm). Si hay compatibilidad AES-NI en el hardware del servidor o de los clientes, AES-256-GCM va muy bien. Si no la hay, CHACHA20-POLY1305 ofrece mejor rendimiento. Hay que tener en cuenta que el único algoritmo compatible con OpenVPN Data Channel Offload (DCO) es AES-256-GCM. Si se activa DCO, estas opciones se ocultan para evitar selecciones no válidas.

**Algoritmo de cifrado de reserva:** El algoritmo de cifrado de datos que OpenVPN utilizará cuando no pueda negociar un algoritmo automáticamente. OpenVPN emplea este valor para túneles de clave compartida y para configuraciones SSL/TLS que solo puedan admitir un único cliente (red de túnel /30). OpenVPN también utiliza este algoritmo para clientes heredados más antiguos que no solo no pueden negociar un algoritmo de cifrado de datos, sino que también han sido compilados para un «tamaño reducido», como dispositivos integrados.

**Algoritmo de Digestión de Autenticación:** Selecciona el algoritmo de digestión de mensajes que OpenVPN utiliza para la autenticación HMAC de los paquetes entrantes. Este algoritmo se usa en el canal de datos y también en el canal de control cuando el túnel utiliza una clave TLS. El valor predeterminado en la interfaz gráfica es SHA256, que ofrece un buen equilibrio entre seguridad y velocidad. Cuando se usan cifrados AEAD, como AES-GCM, OpenVPN ignora este valor para el canal de datos, ya que los cifrados AEAD ya realizan la autenticación. Sin embargo, incluso al usar un cifrado AEAD, OpenVPN sigue empleando este algoritmo para autenticar el canal de control si el túnel utiliza una clave TLS. OpenVPN utiliza SHA1 de forma predeterminada si esta opción no se especifica en su configuración. A menos que ambos lados estén configurados con un valor conocido, se recomienda usar SHA1 aquí.

**Profundidad del Certificado:** Esta opción limita la longitud válida de una cadena de certificados. El valor predeterminado restringe la

cadena a uno (Cliente + Servidor). Con este valor, si una Autoridad de Certificación (CA) intermedia no autorizada firma un certificado, los certificados firmados por esa CA intermedia no autorizada fallarán en la validación. En casos donde la estructura del certificado requiera encadenamiento con CAs intermedias, aumente este límite para permitir la cadena más larga requerida.

**Coincidencia estricta entre Usuario y CN:** Controla si el firewall aplicará una coincidencia estricta entre el nombre de usuario proporcionado por el usuario y el Common Name (CN) de su certificado al autenticarlo. Cuando está habilitado, la autenticación falla si estos dos valores no coinciden. Esto evita que los usuarios utilicen sus propias credenciales con el certificado de otro usuario y viceversa.

**Validación de Uso de Clave en Certificados de Cliente:** Cuando está habilitada, el proceso de autenticación verifica que el certificado proporcionado por un cliente contenga las propiedades adecuadas para actuar como cliente. Esto significa que el certificado debe incluir el atributo de uso de clave extendido para «Autenticación de Cliente TLS Web». Esto evita que se utilicen certificados diseñados para otros propósitos, como la firma de correos electrónicos o certificados destinados únicamente a actuar como servidor, como certificados de cliente VPN.