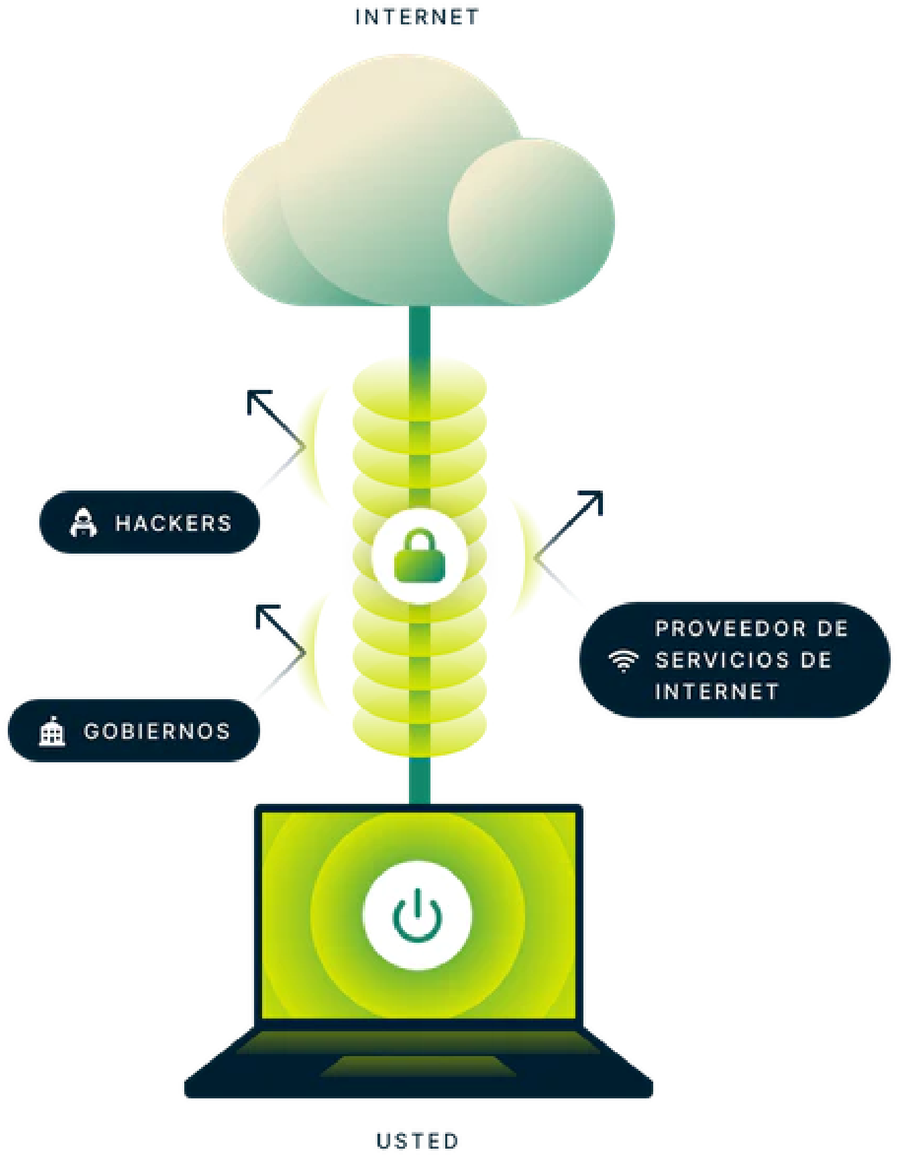
VIRTUAL PRIVATE NETWORK

VPN

Nara Abril Nanfara
Ticiana Cobresi

RED PRIVADA VIRTUAL

Una red privada virtual es una implementación o sistema que habilita una comunicación segura a través de un medio inseguro, siendo transparente para el usuario o aplicación que realiza y recibe la comunicación.



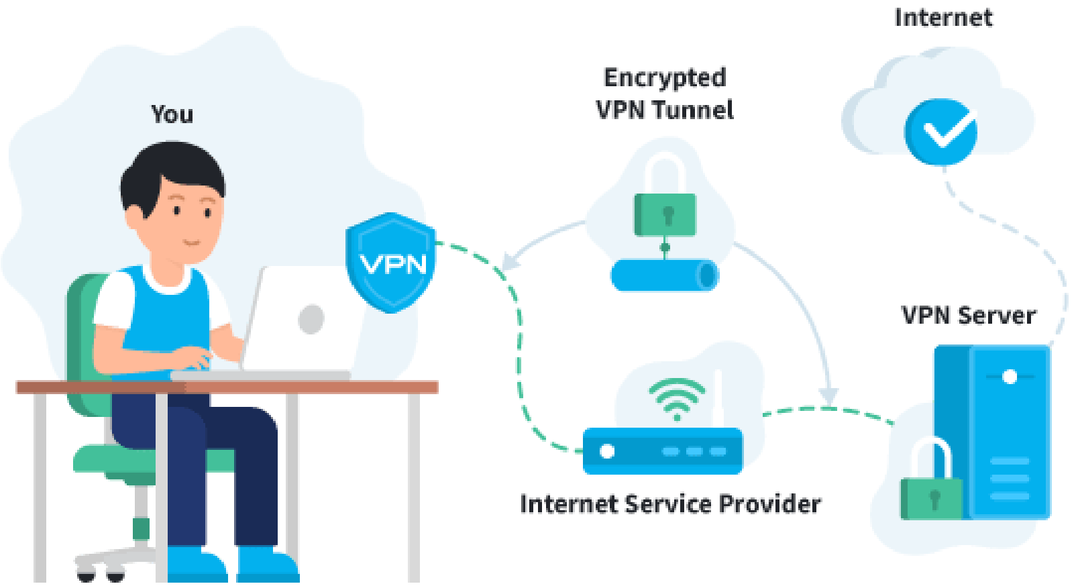
¿COMO FUNCIONA?

Sin VPN vs con VPN

- El software VPN en su computadora encripta su tráfico de datos y lo envía (a través de su proveedor de servicios de Internet) al servidor VPN a través de una conexión segura.

- El servidor VPN descifra los datos cifrados de su computadora.

- El servidor VPN enviará sus datos a Internet y recibirá una respuesta, que es para usted, el usuario.



CONCEPTOS

PROXY

VPN tiene como fin velar por la seguridad de sus usuarios, el proxy es simplemente un intermediario.

ENCRIPTACION

Esto mantiene completamente oculto al contenido de su tráfico en internet

KILL SWITCH

Si su VPN no funciona bien mientras navega, el interruptor de apagado apagará su conexión a Internet por completo

AUTENTICACION

el cliente VPN y el servidor VPN pueden estar seguros de que solo están hablando entre sí y nadie más

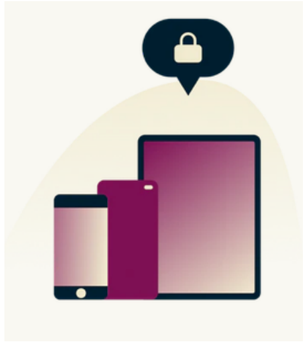
TUNELIZACIÓN

Proceso mediante el cual cada paquete de datos es encapsulado dentro de otro paquete de datos

VENTAJAS DE USAR VPN

Tu dirección IP real está oculta

El tráfico de datos se cifra



Mayor seguridad

Evite las restricciones geográficas

Descargar de forma segura y anónima

Evitar la censura del gobierno

Las VPN mejoran los juegos en línea

Comprar en línea por menos

ISP limite su conexión a Internet

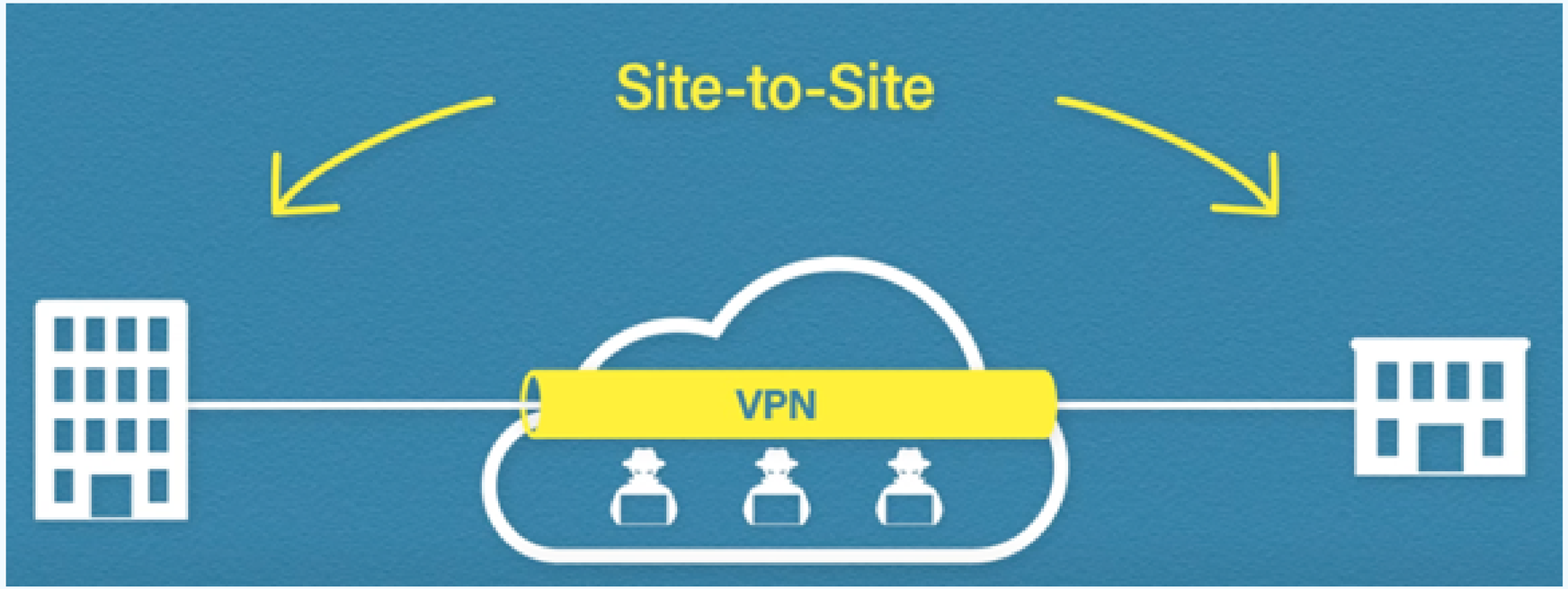
DESVENTAJAS DE USAR VPN

- Una VPN puede disminuir su velocidad
- Puede correr el riesgo de ser bloqueado por ciertos servicios
- Una VPN no es legal en todos los países
- Es difícil para los consumidores comprobar la calidad del cifrado
- La conexión se rompe
- Una sensación injustificada de impunidad en línea
- VPN gratuitas: a veces peor que ninguna
- El registro y la posible reventa de sus hábitos de Internet a terceros

El caso de Onavo Protect

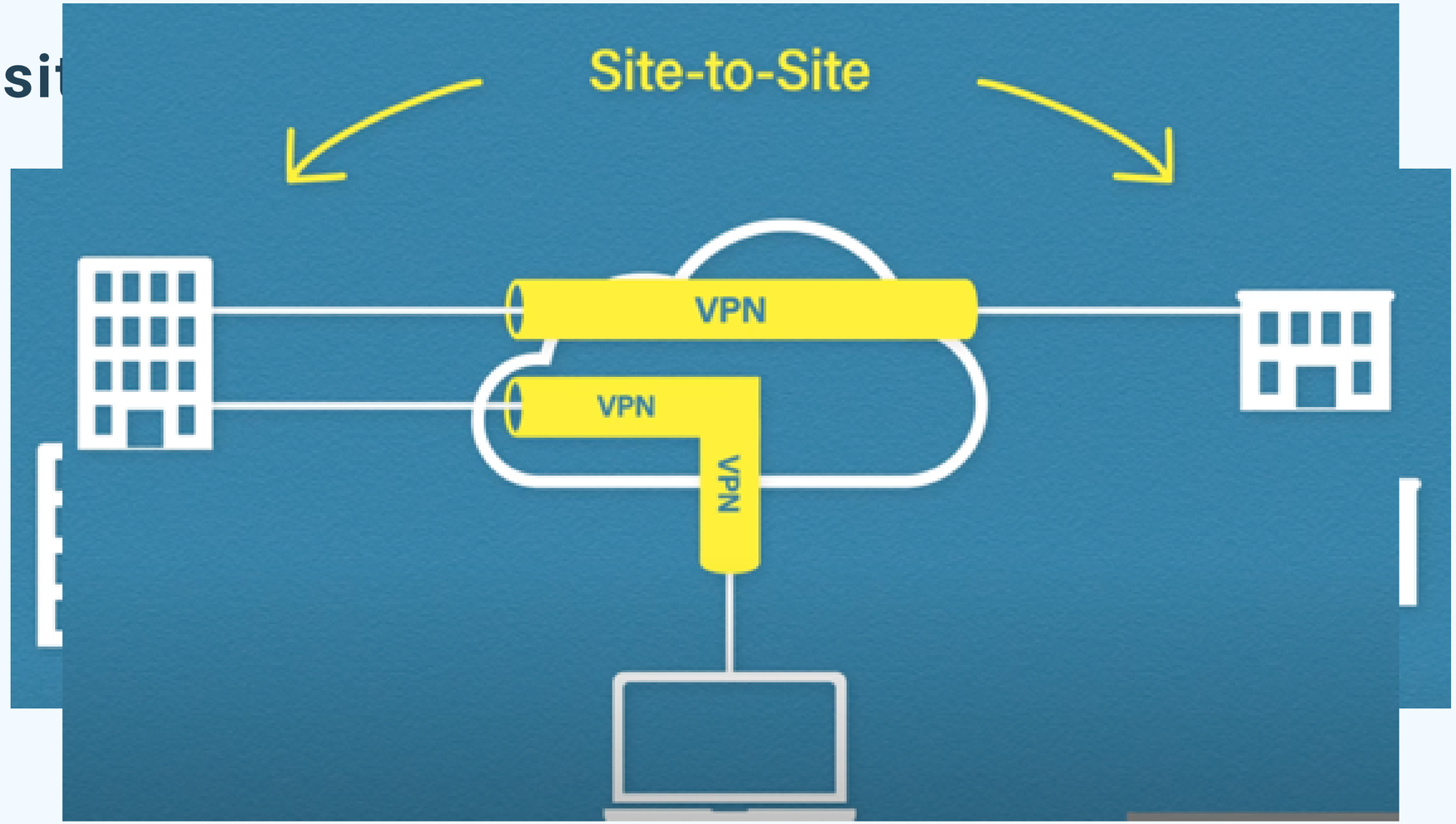
TIPOS DE VPN

Site-to-site VS acceso remoto



TIPOS DE VPN

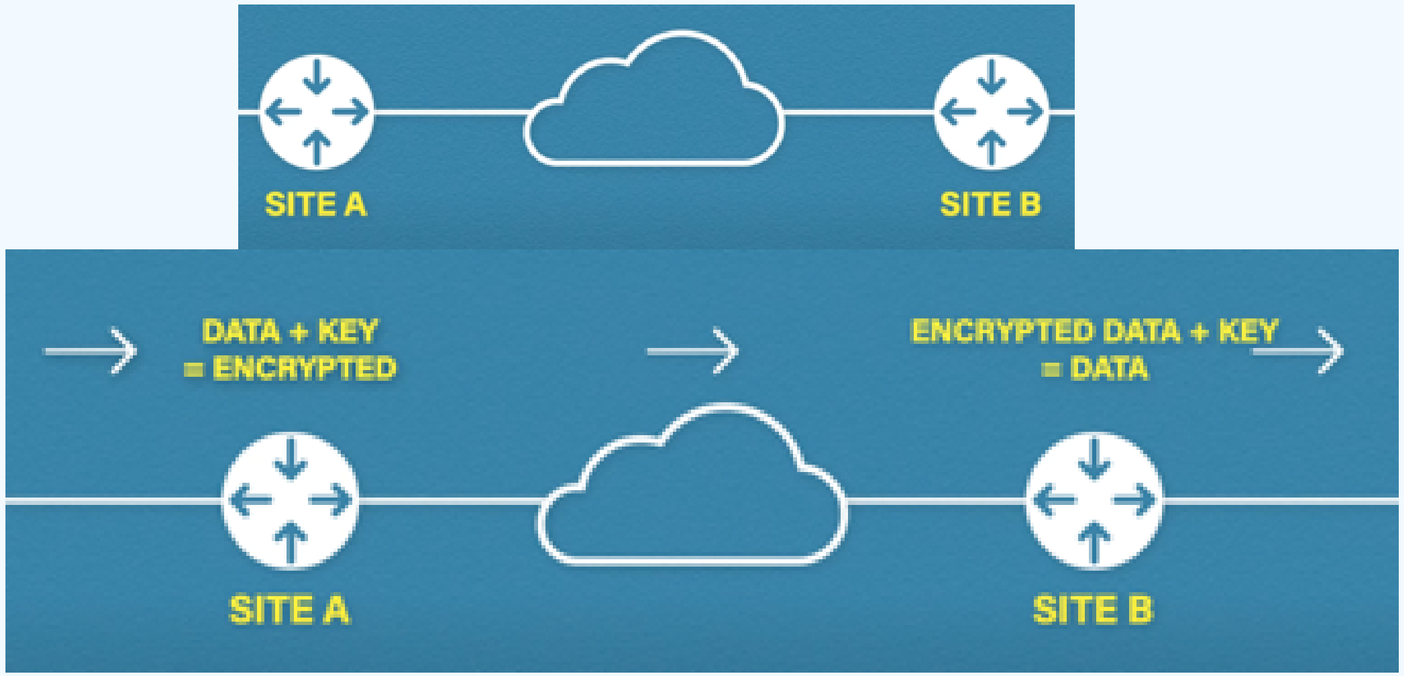
Site-to-sit



TIPOS DE VPN

VPN SITE-TO-SITE

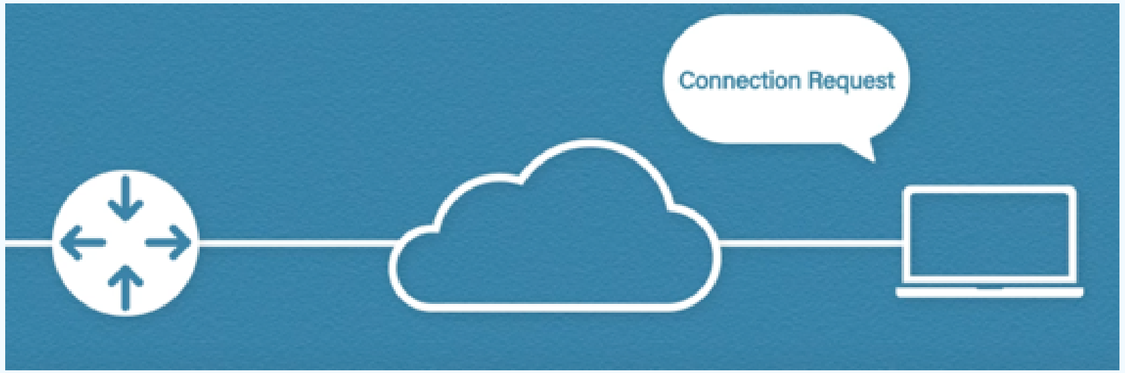
Esta arquitectura nos permite intercomunicar diferentes sedes para compartir los recursos a través de una red segura, protegida con cifrado punto a punto. Este tipo de VPN nos permite interconectar oficinas, sedes de empresas etc.

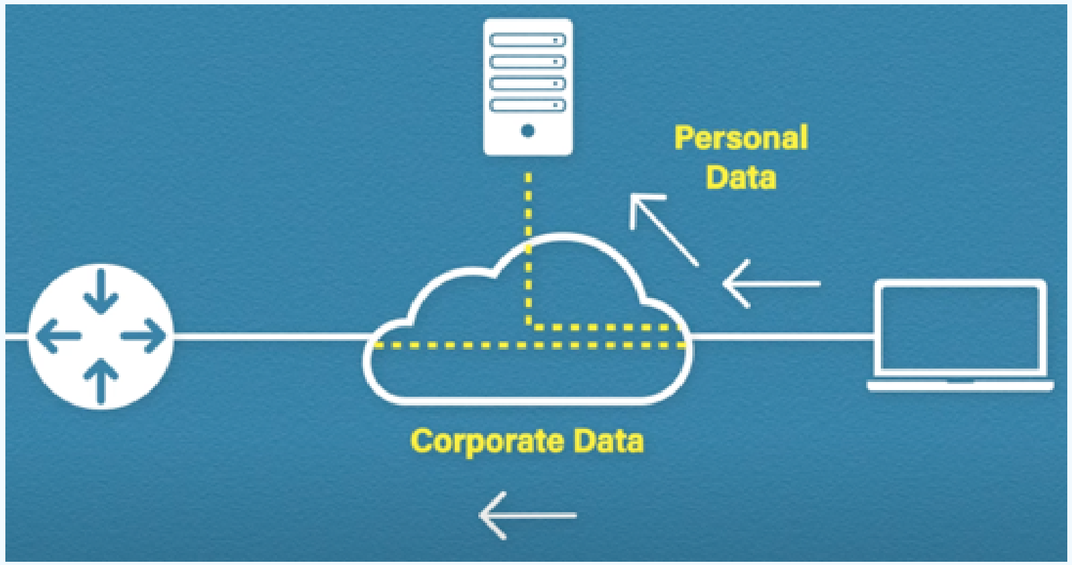


TIPOS DE VPN

VPN ACCESO REMOTO

Tenemos un servidor VPN central, y varios clientes VPN con el software instalado en su ordenador, smartphone, tablet u otro dispositivo, y todos se conectan de manera centralizada al servidor VPN.





PROTOCOLOS VPN

PPTP

- Es uno de los protocolos VPN más antiguos en uso
- PPTP es uno de los más comunes, más fáciles de configurar, y computacionalmente rápidos
- Sus protocolos de autenticación típicamente MS-CHAP-v1/v2 y de encriptación RSA RC4 con un máximo de claves de sesión de 128 bits. Son inseguros

IPsec

- Proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores, como TCP y UDP
- IPsec integra un sistema de negociación para que los equipos finales negocien el mejor cifrado posible que soporten
- Dependiendo de la cabecera de IPsec usada (AH o ESP), podremos comprobar solamente la autenticidad del paquete, o cifrar la carga útil de todo el paquete IP y comprobar también su autenticidad.

PROTOCOLOS VPN

OpenVPN

- Es de codigo abierto
- Algunos fabricantes de routers lo están incorporando en sus equipos
- Está basado en SSL/TLS
- Más fácil de configurar que IPsec y parte gracias al soporte de la comunidad
- Algoritmos criptográficos como 3DES, AES, RC5, Blowfish

IKEv2

- IKEv2: Internet Key Exchange Version 2
- El resultado es una asociación de seguridad.
- Ofrece beneficios de seguridad de IPsec con velocidades y estabilidad IKEv2
- MOBIKE en IKEv2.
- Protocolos de seguridad subyacentes como: ISAKMP, SKEME y Oakley
- Solo disponible a través de UDP

PROTOCOLOS VPN

Wireguard

- Más rápida que IPsec y OpenVPN.
- Linus Torvalds lo llamó "work of art". Trabaja en el kernel de Linux.
- Primera versión estable en marzo 2020.
- Solo 4k líneas de código.
- Las direcciones de IP de VPN se combinan con llaves de cifrado públicas.

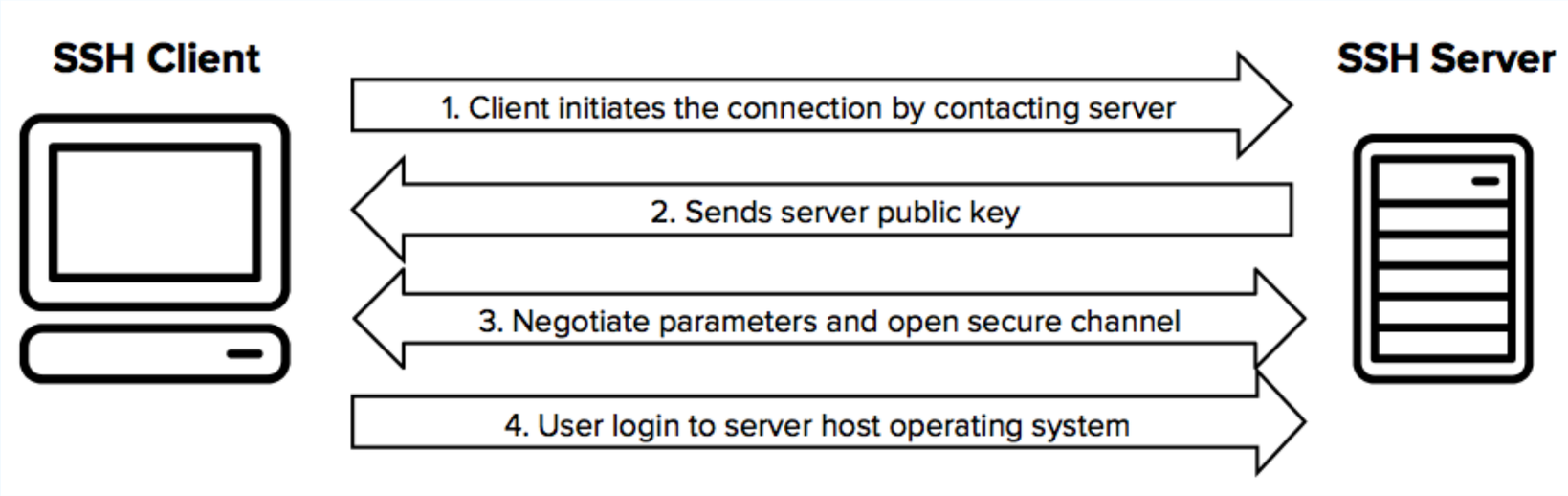
SSL/TLS

- Junto a HTTP da lugar a HTTPS
- Lo podemos utilizar en servidores VPN de tipo SSL/TLS, como en el caso de OpenVPN
- SSL se encuentra en la capa de sesión, mientras TLS en la de transporte y es el sucesor de SSL.
- SSL/TLS VPNs conecta sesiones de aplicaciones de usuario a servicios dentro de una red protegida.

PROTOCOLOS VPN

SSH

- SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.
- SSH encripta la sesión de conexión
- El protocolo funciona en el modelo cliente-servidor lo que significa que la conexión la establece el cliente SSH que se conecta al servidor SSH



CRIPTOGRAFÍA EN VPN

Es el eslabón que se intenta romper para vulnerar nuestra VPN

- ➜ Clave de cifrado larga (>= 128 bits)
- ➜ Protocolos confiables de intercambio de llaves (ECDH, RSA-2048)
- ➜ Protocolos potentes (OpenVPN, IKEv2)
- ➜ Hash SHA-2 para autenticación HMAC
- ➜ Perfect Forward Secrecy
- ➜ Cifrados fuertes (AES, Twofish o Camellia)

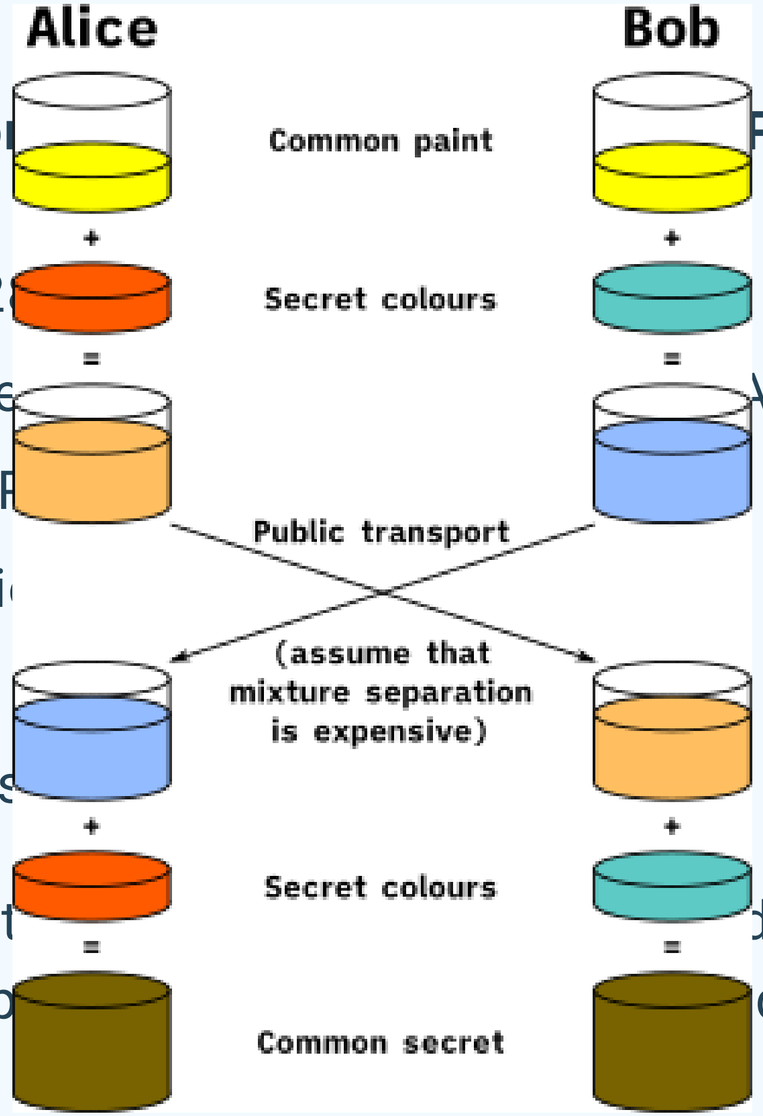
«El cifrado funciona. Los sistemas de cifrado fuertes debidamente implementados son una de las pocas cosas en las que se puede confiar».

Edward Snowden

CRIPTOGRAFÍA EN VPN

Es el eslabón que se intenta ro PN

- ➜ Clave de cifrado larga (>= 12
- ➜ Protocolos confiables de inte -2048)
- ➜ Protocolos potentes (OpenV
- ➜ Hash SHA-2 para autenticaci
- ➜ Perfect Forward Secrecy
- ➜ Cifrados fuertes (AES, Twofis



«El cifrado funciona. Los sist damente implementados son una de las p de confiar».

CRIPTOGRAFÍA EN VPN

Es el eslabón que se intenta romper para vulnerar nuestra VPN

- ➜ Clave de cifrado larga (>= 128 bits)
- ➜ Protocolos confiables de intercambio de llaves (ECDH, RSA-2048)
- ➜ Protocolos potentes (OpenVPN, IKEv2)
- ➜ Hash SHA-2 para autenticación HMAC
- ➜ Perfect Forward Secrecy
- ➜ Cifrados fuertes (AES, Twofish o Camellia)

«El cifrado funciona. Los sistemas de cifrado fuertes debidamente implementados son una de las pocas cosas en las que se puede confiar».

Edward Snowden

CRIPTOGRAFÍA EN VPN

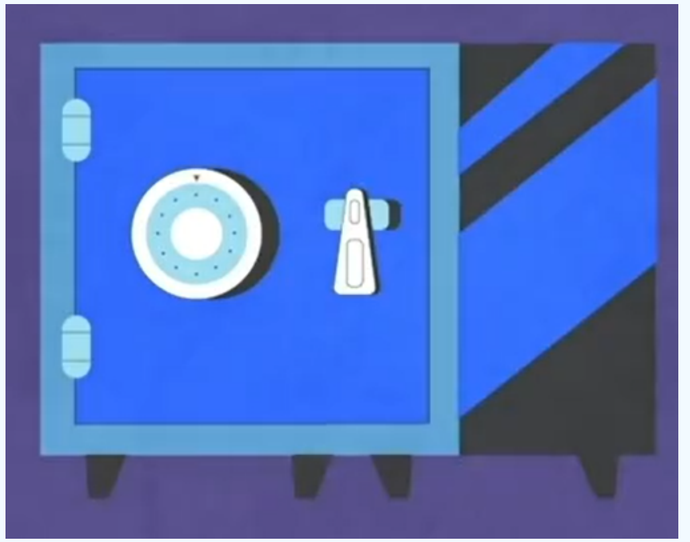
Algoritmos de cifrado según protocolo

➜ **PPTP**: protocolo MPPE, algoritmo de cifrado RSA RC4 con un máximo de claves de sesión de 128 bits.

➜ **IPSec/IKEv2**: gran grupo incluidos 3DES, AES, Blowfish, Camellia.

➜ **OpenVPN**: utiliza la biblioteca OpenSSL para proporcionar cifrado.

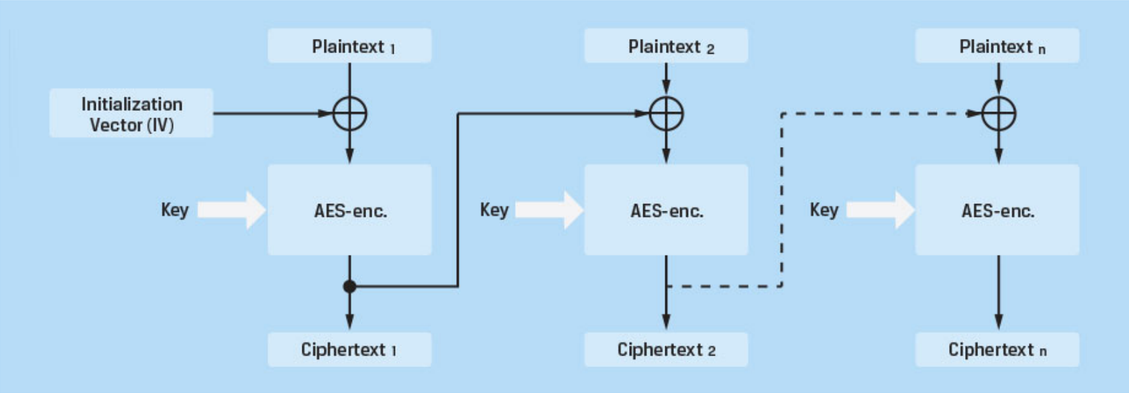
➜ **WireGuard**: ChaCha20 para cifrado simétrico.



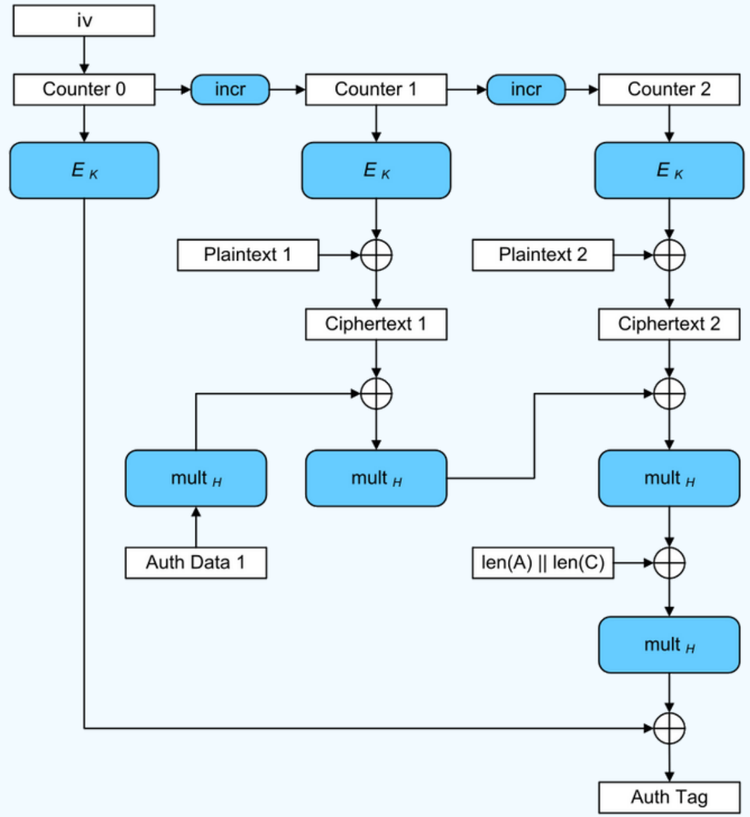
CRIPTOGRAFÍA EN VPN

Modos de procesamiento AES - 256

Cipher Block Chaining (CBC)



Galois/Counter Mode (GCM)



PRODUCTOS VPN EMPRESARIALES

Casi el 43% de las pequeñas empresas fueron víctimas de ciberdelito y se espera que éste le cueste al mundo $6 billones de dólares para el 2021

Perimeter 81

ExpressVPN

NordVPN