VPNs

Una VPN és una “Virtual Private Network”. Utilitzant un medi públic i obert, la VPN crea un túnel privat (“private”) entre un client i un servidor remot confiable, de manera que entre ells sembli (“virtual”) que hi hagi una connexió de tipus LAN privada. És a dir, ofereix seguretat i confidencialitat al tràfic d'informació sensible al llarg de xarxes desprotegides com ara Internet. A la VPN hi intervenen conceptes com autenticació i encriptació, que s'han de negociar entre les dues parts, i que asseguren la confidencialitat i integritat de les dades que viatgen pel túnel.

Concretament, VPNs provide privacy by hiding your internet activity from your ISP (and government), allows you to evade censorship (by school, work, your ISP, or government), allows you to “geo-spoof” your location in order to access services unfairly denied to you based on your geographical location (or when you are on holiday), protects you against hackers when using a public WiFi hotspot, allows you to P2P download in safety, etc.

Una VPN pot implementar-se de vàries formes, segons l'ús que se'n vulgui fer:

*Des d’un client darrera un NAT (un portàtil domèstic, per exemple) fins un servidor corporatiu privat amb IP pública (el qual, opcionalment, podria permetre o no la connexió simultània de múltiples clients i/o donar accés a la resta de recursos de la seva LAN mitjançant les regles Iptables pertinents, etc). És a dir, fer: *PC_VPN => Internet => Servidor_VPN => LAN_i_recursos_empresa* L'ús típic seria el tele-treball.

*Des d'un client darrera un NAT (un portàtil o un telèfon mòbil, per exemple) fins un servidor públic contractat (o bé funcionant de forma ja predefinida per realitzar tasques de VPN gràcies a què aquest servei específic és ofert per alguna empresa, o bé havent-lo de configurar manualment fent ús de sistemes IaaS generalistes de tipus AWS, Linode, DigitalOcean, etc), el qual, al seu torn, accedirà als destins demanats pel client a mode de "trampolí". La idea és que la connexió entre client i servidor atravessa l'ISP sense que aquest sàpiga res i, un cop els paquets originals del client arribin al servidor VPN, aquest sigui qui consta a Internet com a originari d'aquest tràfic. És a dir, en comptes de fer: *PC => ISP => Internet* , fer: *PC_VPN => ISP => Servidor_VPN => Internet* so an external observer will only see data entering and leaving the IP address of the VPN server, but will not be able to determine any details about the computer at the other end of the tunnel, while the ISP can see that a customer’s computer is connected to a VPN server, but cannot see what requests and data are being transmitted thanks to the encryption used. Un ús típic seria, com ja s'ha dit, evitar ser espiat en xarxes locals insegures, com ara les Wifis obertes de cafeteries, etc
NOTA: Using a VPN service does not replace the need for an Internet Service Provider, as it is your ISP that provides your internet connection in the first place.

*Entre dos dispositius iguals -normalment dos routers-, els quals tindran cadascun d’ells una LAN per darrera, (permetent en aquest cas un túnel segur entre dues xarxes privades senceres).

En tots els casos, la idea és generar en els dos sistemes dels extrems una tarja de xarxa virtual (que normalment s’anomena *tunX*), la qual tindrà una IP privada pertanyent a una xarxa diferent de les xarxes a les que les eventuals tarjes de xarxa reals poguessin pertànyer en ambdós costats. Les tarjes *tunX* es comuniquen entre elles mitjançant un túnel segur mentre que les tarjes reals continuen mantenint en paral.lel la seva comunicació no segura.

The weak points coming at either end of the encrypted data tunnel. The user end is usually secure enough as data cannot be traced to it. More important is the fact that a VPN server can see the traffic that passes through it. If any record of this traffic is kept (logs) then it can be handed over to authorities. The only way to ensure that an VPN Server will not hand over data is to only use an VPN Server that keeps no logs, so that in the event it is asked or forced to, it has nothing to hand over.

Other concern for ordinary users when connecting by VPN is that is does slow down an internet connection. The data has to be sent via the users ISP to the VPN server, be encrypted, go to whatever websites etc. the user is visiting, and then return by the same way. In practice, if the VPN server is not too geographically distant (e.g. anywhere in Europe for a European user), then the slowdown is usually so minimal it’s unlikely to be noticed, but if someone is connecting to a server in California from Europe, then they may experience considerable lag

Tecnologies

OpenVPN (capa 7): implementa la VPN a nivell d'aplicació. Per tant, és transparent a qualsevol tipus de tràfic inferior (TCP, UDP, ICMP). De fet, depén de OpenSSL per funcionar. Treballar en aquest nivell permet escollir els ports a utilitzar per crear la VPN (TCP o UDP, com es vulgui), cosa que fa molt difícil bloquejar-la (això no passa amb les altres tecnologies de nivell inferiors al 4, on els ports i els protocols de transport utilitzats són fixes) . No obstant, treballar en el nivell d'aplicació obliga a que tant el client (que pot ser el nostre PC però també el nostre router domèstic) com el servidor remot tinguin instal.lada l'aplicació pertinent, però això no sol ser problema (si es té privilegis d'administrador) perquè aquesta és multiplataforma

Wireguard (capa 3): protocol incorporat nativament al kernel Linux. Criptogràficament és molt segur perquè només utilitza una cipher suite molt específica, a diferència d'altres protocols que permeten escollir (concretament, utilitza Curve25519 per l'intercanvi de claus, ChaCha20+Poly1305 per l'encriptació i autenticació de dades i BLAKE2 pel hashing). A més, ofereix un rendiment excel.lent en termes de velocitat, fiabilitat i consum de bateria (fent-lo ideal per mòbils). No obstant, té alguns inconvenients:

*Encara està sota desenvolupament i no ha estat auditat
*Encara no està clar si es pot utilitzar sense haver de generar logs (per garantir la privadesa).
*Encara no hi ha un suport generalitzat a la indústria VPN (és un protocol molt nou)
*Funciona sobre UDP només (per tant, és més fàcil de bloquejar)

IPSec (capa 3): Representa un conjunt de protocols de comunicació dissenyats per autenticar i encriptar les dades transmeses per una VPN (oferint confidencialitat -és a dir, secret-, integritat -és a dir, protecció a la manipulació dels paquets- i assegurament de les comunicacions passades). IPSec fa servir diferents mètodes per oferir cadascuna d'aquestes característiques: per exemple, pot oferir AES per la confidencialitat, SHA-512 (HMAC) per la integritat, etc. En qualsevol cas, IPSec és depenent de la infrastructura de mòduls del kernel de tots els elements de capa 3 involucrats a la comunicació (dispositius finals i routers)

Tiene dos métodos de trabajo principales: el modo tunnel, donde todos los paquetes IP son encapsulados en un nuevo paquete y enviados a través del túnel siendo desempaquetados en el otro extremo (así se protegen las direcciones IP del emisor y receptor además de los metadatos del paquete); o el modo transporte, donde sólo la carga útil de la sección de datos es cifrada y encapsulada. Por otro lado, integra dos protocolos de seguridad a elegir internamente:

*AH: Provides authentication and antireplay services, without encryption, by adding a digital signature (in form of a own security header) to the original IP packet
*ESP: Provides authentication, encryption, and antireplay services. It encrypts the data within the packet and then adds its own security header to the original IP packet. Because ESP headers don't authenticate the outer IP header as AH headers do, AH and an ESP are often used in combination with each other

PPTP (capa 2): protocolo inseguro diseñado por Microsoft. Encapsula datagramas de cualquier protocolo de red en datagramas IP usando una versión extendida del protocolo GRE (permitiendo así que cualquier protocolo pueda ser enrutado a través de una red IP, como Internet). Para la autentificación, PPTP tiene dos opciones: CHAP ó PAP (texto plano). Para la encriptación suele apoyarse en el protocolo MPPE. Obsoleto.
NOTA: Microsoft también es propietario de otro protocolo alternativo (privativo) llamado **SSTP**, el cual trabaja en la capa 7 sobre TLS (al igual que OpenVPN) y por defecto utiliza el puerto 443 TCP (por lo que es menos fácil de bloquear)

L2TP (capa 2): protocolo evolución de L2F propuesto por Cisco pero estandarizado en el RFC 3193. Encapsula tramas PPP sobre cualquier medio, no necesariamente redes IP. Como no ofrece mecanismos de seguridad, para su uso deberá ser combinado con otros mecanismos que sí proporcionen confidencialidad, autenticación e integridad, como IPSec (de capa 3). L2TP/IPSec suele utilizar cifrado AES.

. NOTA: Una alternativa a L2TP/Ipsec es **IKEv2/Ipsec**, estandarizada en el RFC 7296. IKEv2 proporciona la funcionalitat d'intercanvi de claus simètriques (a partir d'un túnel construït prèviament amb criptografia asimètrica) A diferencia de OpenVPN, no obstante, su implementación recae en el uso de puertos UDP fijos, por lo que es más fácil de bloquear. No necesita instalación de ningún software cliente.