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, permet assegurar el tràfic d'informació sensible al llarg de xarxes desprotegides, com ara Internet, fent que la comunicació entre els extrems estigui aïllada de la resta del món. A la VPN hi intervenen conceptes com autenticació i encriptació (que s'han de negociar entre les dues parts), els quals asseguren la confidencialitat i integritat de les dades que viatgen pel túnel.

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 pertinents del seu tallafocs, etc). És a dir, fer: *PC_VPN=>ISP=>Servidor_VPN=>LAN_i_recursos_empresa* L'ús típic d´aquesta configuració seria el tele-treball.

  NOTA: El servidor corporatiu pot no tenir una IP pública, però llavors el "router" que li fa de porta d´enllaç haurà de tenir implementat el DNAT

* 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, LowendBox, 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 travessi l'ISP sense que aquest en sàpiga res d´ella (perquè està xifrada) i, un cop els paquets originals del client arribin al servidor VPN, aquest els desxifri i sigui qui consti a Internet com a originari d'aquest tràfic, ara ja sí, "normal". És a dir, fer: *PC_VPN => ISP => Servidor_VPN => Internet* (en comptes de simplement *PC => ISP => Internet*) D´aquesta manera, un observador extern d´Internet només veurà que les dades entren i surten a/de l'adreça IP del servidor VPN, mentre que l'ISP veurà que el PC del seu client està connectat a un servidor VPN però no podrà veure quines dades s´estan transmetent i rebent (gràcies a l´ús, com hem dit, d'encriptació entre el client i el servidor VPN). Un ús típic d´aquesta configuració seria, com ja s'ha dit, evitar ser espiat en xarxes locals insegures, com ara les Wifis obertes de cafeteries, etc

  NOTA: L'ús d'un servei VPN no substitueix la necessitat d'un proveïdor de serveis d'Internet, ja que és el nostre proveïdor d'Internet el que proporciona la nostra connexió a Internet en primer lloc

NOTA: En qualsevol dels casos anteriors, per establir una connexió VPN necessitarem, a més d´accedir a un servidor VPN concret, configurar a la nostra màquina un determinat client VPN. D´això en parlarem properament
NOTA: També hi hauria una altra implementació interessant a banda dels dos casos anteriors: connectar amb una VPN dos dispositius iguals (normalment dos "routers"), els quals tindrien cadascun d’ells una LAN per darrera, (permetent en aquest cas un túnel segur entre dues xarxes privades LAN senceres).

Així doncs, podem fer servir una VPN per ...:

*... garantir la nostra privadesa, ja que oculta la nostra activitat en Internet al nostre ISP (i al govern)
*... eludir la censura (realitzada a l´escola, a la feina, a l´ISP o al govern) ja que "sortim" a Internet des d´un altre lloc. D'altra banda també la podem fer servir per geolocalitzar falsament la nostra ubicació per accedir a serveis que no estan disponibles a la nostra ubicació geogràfica real
*... protegir-nos contra els pirates informàtics quan utilitzem un punt d'accés WiFi públic
*... poder descarregar P2P amb seguretat

Cal ser conscient, insistim, que un servidor VPN sí que pot "veure" tot el trànsit que hi passa: en els dos extrems del "túnel" els paquets tornen a ser "transparents". És a dir, amb una VPN només estem canviat qui pot veure el nostre tràfic: passem de l´ISP al servidor VPN. Per tant, si el servidor VPN mantingués algun registre d’aquest trànsit (registres), els pot lliurar a les autoritats. L’única manera d’assegurar-se que un servidor VPN no lliurarà les dades és només fent servir un servidor VPN que no mantingui registres, de manera que, en cas que se li demani o s’obligui, no tingui res a lliurar.

NOTA: Òbviament, si el paquet té algun tipus de xifratge integrat, com ara els de tipus HTTPS, el servidor VPN no podrà inspeccionar-los (a no ser que faci un atac MitM) però sí que podrà conèixer el valors de les seves capçaleres no xifrades (IP, TCP/UDP, etc), de manera que en podrà conèixer força metadades del trànsit igualment. En aquest sentit, el tràfic DNS sol ser el més perillós perquè no sol estar xifrat (tot i que actualment s´està intentant promoure el DNS over TLS o DNS over HTTPS que sí que ofereix aquesta característica) i aporta molta informació interessant sobre nosaltres.
NOTA: Una altra preocupació per als usuaris comuns quan es connecten mitjançant VPN és que disminueix la velocitat de la connexió a Internet. Les dades s'han d'enviar mitjançant l'ISP dels usuaris al servidor VPN, xifrar-les, anar a qualsevol lloc web que l'usuari visiti i, després, tornar de la mateixa manera. A la pràctica, si el servidor VPN no està massa geogràficament distant (per exemple, a qualsevol lloc d'Europa per a un usuari europeu), la desacceleració sol ser tan mínima que és improbable que es noti, però si algú es connecta a un servidor d'Europa a Califòrnia, llavors poden experimentar un retard considerable

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, depèn de OpenSSL per funcionar. Treballar en aquest nivell permet triar 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.

NOTA: A la pràctica, el software OpenVPN ofereix dos modes de funcionament: el mode "routing", que treballa a nivell de capa 3 (com Wireguard o IPSec), i que és el mode per defecte, o el mode "bridging", que treballa a nivell de capa 2 (com PPTP o L2TP)

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 triar-la (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 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, el bon funcionament d´IPSec depèn de què tots els elements de capa 3 involucrats a la comunicació (dispositius finals i routers) l'implementin.

IPSec té dos mètodes de treball principals: el mode "tunnel", on tots els paquets IP són encapsulats en un nou paquet i enviats a través del túnel essent desempaquetats a l´altre extrem (així es protegeixen les adreces IP de l´emissor i el receptor a més de les metadades del paquet); o en mode "transport", on només la càrrega útil de la secció de dades (el "payload") és xifrada i encapsulada. D'altra banda, integra dos protocols de seguretat a triar internament:

*AH *(Authentication Header)*: Proporciona serveis d'autenticació i d'"antireplay" (sense xifratge, però) afegint una signatura digital (en forma de capçalera de seguretat pròpia) al paquet IP original. D´aquesta manera es poden detectar atacs MitM.
*ESP *(Encapsulating Security Payload)*: Proporciona serveis d'autenticació, d'"antireplay" i xifratge. Encripta les dades del paquet i, a continuació, afegeix la seva pròpia capçalera de seguretat al paquet IP original. No obstant, com que les capçaleres ESP no autentiquen la capçalera IP externa tal com ho fan les capçaleres AH, AH i ESP sovint s'utilitzen en combinació entre si.

PPTP (capa 2): Protocol insegur (i obsolet) dissenyat per Microsoft. Encapsula datagrames de qualsevol protocol de xarxa en datagrames IP usant una versió extesa del protocol GRE (permetent així que qualsevol protocol pugui ser enrutat a través d'una xarxa IP, com Internet). Per l'autentificació, PPTP té dues opcions: CHAP ó PAP (text pla). Per l'encriptació sol usar el protocol MPPE.

NOTA: Microsoft també és propietari d´un altre protocol alternatiu (privatiu) anomenat **SSTP**, el qual treballa a la capa 7 sobre TLS (a l'igual que OpenVPN) i per defecte utilitza el port 443 TCP (essent doncs menys fàcil de bloquejar)

L2TP (capa 2): Protocol evolució de L2F proposat per Cisco però estandarditzat en el RFC 3193. Encapsula trames PPP sobre qualsevol mitjà, no necessàriament xarxes IP. Com no ofereix mecanismes de seguretat, per al seu ús haurà de ser combinat amb altres mecanismes que sí proporcionin confidencialitat, autenticació i integritat, com IPSec (de capa 3). L2TP/IPSec sol utilitzar xifrat AES.

NOTA: Una alternativa a L2TP/Ipsec és **IKEv2/Ipsec**, estandaritzada en el RFC 7296. IKEv2 proporciona la funcionalitat d'intercanvi de claus simètriques (a partir d'un túnel construït prèviament amb criptografia asimètrica), i és el protocol que es fa servir més amb Ipsec, de fet. A diferència de OpenVPN, no obstant, la seva implementació recau en l´ús de ports UDP fixes (essent, doncs, més fàcil de bloquejar). No necessita instal·lació de cap tipus de software client.

En tots els casos, la idea és generar en els dos sistemes dels extrems una tarja de xarxa virtual que 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. Aquestes tarjes virtuals es comuniquen entre elles mitjançant un túnel segur mentre que les tarjes reals continuen mantenint en paral.lel la seva comunicació no segura.

Ús de VPNs comercials

Existeixen molts serveis comercials que ofereixen servidors VPNs per poder-s´hi connectar. Normalment, aquests serveis són accessibles mitjançant la instal·lació al nostre sistema d´algun software client específic (tot i que també, depenent del servei, pot fer-se servir un software genèric com és OpenVPN i llavors només haver d´emprar la configuració pertinent disponible per descarregar de l´empresa en qüestió). D´aquesta manera, un cop registrat com a usuari i instal·lat/configurat el client pertinent al nostre ordinador, ja podrem disposar d´un canal segur fins el servidor VPN que haguem escollit.

A l´hora de triar una empresa concreta de les moltes que hi ha (tot seguit mostrarem un llistat) que ens ofereixen servidors VPN, cal tenir en compte diversos factors:

*¿Què sap aquesta empresa sobre mi (només una adreça correu o també el nombre tarja de crèdit...)? En aquest sentit, ¿permet pagament anònim via Bitcoin o similar?
*¿Qui és el propietari de l´empresa? ¿En quin país i sota quina jurisdicció (en relació a les lleis de privacitat) es troben els seus servidors (cal saber quants són i on estan ubicats geogràficament)? ¿L'empresa responsable col·labora amb el govern de torn a l´hora de facilitar informació sobre els seus clients? En aquest sentit, la pregunta clau: ¿els servidors VPN utilitzats guarden en un registre l'activitat del seus clients? (resposta: això no ho podrem saber mai, diguin el que diguin)
*¿El client he de fer servir per connectar-me (des del meu PC o dispositiu mòbil) al servidor VPN triat és lliure? ¿Quins són els termes d'ús d'aquest? ¿És multiplataforma?
*¿Quin tipus de criptografia i protocols VPN utilitzen els servidors oferits? ¿Han sigut auditat de forma externa?
*El servidor VPN triat ens permet "sortir a Internet" des d´un país diferent del meu? ¿Permet "P2P"?
*¿Quina és la velocitat de connexió màxima disponible? ¿Quants clients connectats a la vegada es permeten com a màxim? ¿Quin és el preu del servei?

NOTA: Teniu descrits més aspectes a considerar en els següents articles: https://www.cactusvpn.com/es/vpn/como-elegir-la-mejor-ubicacion-del-servidor-vpn , https://www.le-vpn.com/es/10-criterios-mejor-servicio-vpn i sobre tot, https://www.privacytools.io/providers/vpn/#criteria

Un llistat d´empreses que ofereixen aquest tipus de serveis el teniu a continuació:

AirVPN: https://airvpn.org
Mullvad: https://mullvad.net
ExpressVPN: https://www.expressvpn.com
NordVPN: https://nordvpn.com
IVPN: https://www.ivpn.net
Cyberghost: https://www.cyberghostvpn.com
ProtonVPN: https://protonvpn.com
Surfshark: https://surfshark.com
StrongVPN: https://strongvpn.com
Hideme: https://hide.me
Windscribe: https://windscribe.com
Tunnelbear: https://www.tunnelbear.com
Vyprvpn: https://www.vyprvpn.com
IPVanish: https://www.ipvanish.com
PrivateVPN: https://privatevpn.com

PIA: https://www.privateinternetaccess.com
PureVPN: https://www.purevpn.com
VPNArea: https://vpnarea.com
VPNht: https://vpn.ht
CactusVPN: https://www.cactusvpn.com
CCryptoVPN: https://vpn.ccrypto.org
CryptoStorm: https://cryptostorm.is
Ivacy: https://www.ivacy.com
FastestVPN: https://fastestvpn.com
Encrypt.me: https://encrypt.me
VikingVPN: https://vikingvpn.com
Aeroshield: https://aeroshield.me
SurfEasy: https://www.surfeasy.com
IronSocket: https://ironsocket.com
Whoer: https://whoer.net

NOTA: A https://www.vpn.com s´ofereixen articles comparatiu mensuals de serveis com els anteriors i a https://thatoneprivacysite.net s´ofereixen igualment taules comparatives confiables
NOTA: A més dels serveis anteriors també existeixen aplicacions client que es connecten a múltiples servidors VPN, fent servir connexions P2P o fins i tot Tor, enfortint així (en teoria) la privacitat de les comunicacions. Exemples són: **Lantern** (https://lantern.io), **Outline** (https://getoutline.org ; permet incorporar un servidor VPN propi a la xarxa), **Hola** (https://hola.org) o **Psiphon** (https://psiphon.ca)
NOTA: En relació a les VPN comercials de tipus OpenVPN (les més habituals encara avui dia), a continuació es llisten els enllaços concrets per descarregar-se la configuració particular que caldria introduir al nostre client OpenVPN per tal de poder-nos connectar a algun servidor VPN oferit per l´empresa en qüestió (un cop, òbviament, ens haguem registrat -i pagat- com a usuaris vàlids...si no els servidors VPN ens rebutjaran), o bé un client "modificat" però basat en el client OpenVPN estàndard: https://airvpn.org/linux; https://protonvpn.com/support/linux-vpn-tool; https://www.expressvpn.com/vpn-software/vpn-linux; https://www.cyberghostvpn.com/en_US/apps/linux-vpn; https://nordvpn.com/download; https://www.ivpn.net/setup/gnu-linux.html; https://mullvad.net/en/download; https://pritunl.com/platforms; https://torguard.net/downloads.php; https://www.purevpn.com/download/linux-vpn; https://www.privateinternetaccess.com/pages/download?platform=Linux o https://surfshark.com/download/linux. Si la descàrrega consisteix en simples fitxers de configuració, només caldrà incorporar-lo directament al client OpenVPN de terminal o bé, es poden integrar en el plugin OpenVPN que incorpora NetworkManager (disponible al paquet "NetworkManager-openvpn") i la seva versió gràfica, més còmoda i amigable (disponible al paquet "NetworkManager-openvpn-gnome").
NOTA: NetworkManager disposa d´un munt d´altres "plugins" que permeten connectar amb altres tipus de servidors VPN (IPSec, etc). Concretament, es poden trobar llistats a https://wiki.gnome.org/Projects/NetworkManager/VPN , d´entre els quals podem destacar "NetworkManager-libreswan-gnome", "NetworkManager-strongswan-gnome", "NetworkManager-fortisslvpn-gnome", "NetworkManager-openconnect-gnome", "NetworkManager-iodine-gnome", "NetworkManager-l2tp-gnome", "NetworkManager-vpnc-gnome", "NetworkManager-sstp-gnome", "NetworkManager-pptp-gnome" o "NetworkManager-ssh-gnome". En el cas concret de voler connectar a una VPN Wireguard, NetworkManager no disposa de "plugin" específic perquè ja incorpora aquesta funcionalitat en el seu "core" de forma nativa

Actualment no hi ha gaires serveis compatibles amb Wireguard, però poc a poc n´hi va havent més (com ara AzireVPN - https://www.azirevpn.com- entre d´altres; hi ha un llistat actualitzat a https://www.vpnmentor.com/blog/best-vpns-wireguard o a https://greycoder.com/a-list-of-wireguard-supporting-vpns)

Tor vs VPN

Recordem com funcionava la xarxa Tor:

* La nostra connexió a Internet s'encamina a través de com a mínim 3 nodes aleatoris
* Aquests nodes es poden ubicar a qualsevol part del món
* Les dades es xifren diverses vegades (cada vegada que passen per un node)
* Cada node només coneix les adreces IP que hi ha "davant" i l'adreça IP del node "darrere". Això hauria de significar que ningú en cap moment pot conèixer el camí complet entre l'ordinador i el lloc web al qual intentem connectar-nos (fins i tot si alguns nodes al llarg dels nodes del camí puguin estar controlats per entitats malicioses)

La gràcia de la xarxa Tor és que no cal confiar en ningú: està dissenyat perquè ningú pugui descobrir la nostra veritable identitat i (si ens connectem a un lloc web segur) ningú no pugui accedir a les nostres dades. No obstant, és lent: l´encaminament per tres nodes (que poden estar a qualsevol lloc del món i es reestableixen cada 10 minuts) i el xifratge que s´hi fa en cadascun d´ells (el qual requereix energia de processament de cada node) són les principals causes. A més, la llista de nodes de sortida és coneguda (està disponible públicament aquí: https://www.torproject.org/projects/tordnsel.html.en, amb la qual cosa és molt fàcil per determinats ISP o governs bloquejar els usuaris d´aquesta xarxa.

En canvi, el servei que pot oferir un servidor VPN és molt més ràpid per definició (només és un "node") i pot no estar censurat com poden estar els nodes de sortida de Tor. En canvi, el servidor que fem servir sap qui som (coneix quina adreça IP tenim, i, a partir d´ella, ens podrà geolocalitzar, a més de saber altres metadades del nostre sistema sovint publicades en les nostres connexions com ara el nostre sistema operatiu, el nostre navegador, etc) i sap què transferim (perquè té accés a tot el tràfic que enviem i rebem): tot això ho podrà guardar per tenir un registre de nosaltres. A més, és més senzill realitzar un atac DoS contra un sol servidor VPN que no pas contra tota la xarxa Tor. I per últim, els serveis VPN comercials són de pagament mentre que la xarxa Tor és gratuïta i col·laborativa.