VPN: hoe werkt een VPN verbinding?

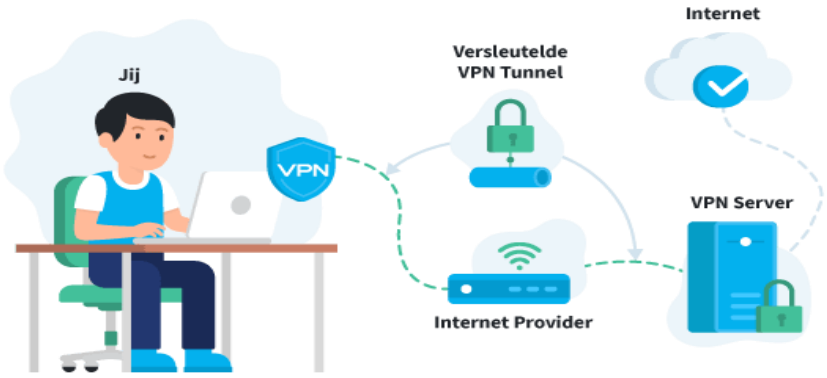
Een VPN-verbinding (wat staat voor Virtual Private Network), geeft een gebruiker **beveiligde (versleutelde)** en **anonieme (omgeleide)** toegang tot een netwerk en maakt daarmee de internetverbinding veiliger. Net zoals een firewall de gegevens op je computer beschermt, beschermt een VPN je gegevens online.
Een VPN-verbinding werkt op de achtergrond en verandert dus niks in het gebruik van de computer of smartphone. Al je internetverkeer wordt **versleuteld** waardoor andere partijen (zoals hackers, overheden, internetproviders, websites en je werkgever) niet meer kunnen zien waar jij mee bezig bent op het internet. Daarnaast wordt het internetverkeer via de VPN-server **omgeleid** waardoor je locatie wordt verborgen. Een VPN-verbinding kan om verschillende redenen worden gebruikt. Het gebruik van een VPN wordt op publieke wifi-netwerken bijvoorbeeld sterk aangeraden. Ook stelt een VPN je in staat om anoniem te downloaden.

Hoe werkt het internet?

Om een VPN te begrijpen is het eerst belangrijk om basaal te begrijpen hoe het internet werkt. Als je een website wil bezoeken dan doe je een aanvraag via je computer aan je router. Je router geeft deze aanvraag door aan je internetprovider. De internetprovider geeft deze aanvraag door aan de website die zich bevindt op een server ergens op de wereld. Deze server stuurt vervolgens een reactie op je aanvraag terug via dezelfde weg als waar de aanvraag vandaan komt. Deze aanvraag kan zijn het verzoek om een website te bezoeken door een webadres in te voeren, of bijvoorbeeld een muisklik om naar een nieuwe pagina te navigeren. Alles wat je online doet is dus in principe een reeks van verzoekjes en antwoorden. Zie het als het versturen en ontvangen van een brief. Je schrijft iets op en doet het in de brievenbus. Vervolgens zorgt PostNL dat je brief wordt bezorgd. De reactie wordt via PostNL weer terug bij jou bezorgd. Zo werkt het als het ware op internet ook. Een VPN is een extra laag beveiliging en privacy die als een soort van veilige en anonieme tunnel werkt zodat niemand jouw correspondentie kan onderscheppen.

Hoe werkt een VPN?

Een VPN werkt als een veilige en anonieme tunnel waar alle communicatie met het internet doorheen loopt. VPN-software op je computer of smartphone pakt elk verzoek wat je doet in en zet er een slot op. Dit slot is zo goed als niet te kraken. Vervolgens wordt je verzoek via je router en internetprovider verstuurd naar een VPN-server. Deze server pakt je verzoek uit en stuurt je verzoek door naar de website die je bezoekt. De reactie van de website wordt naar de VPN-server gestuurd waar de data weer wordt ingepakt. Deze versleutelde reactie wordt bezorgd aan jouw computer of device, waar de VPN-software de reactie weer uitpakt en toont. Dit is in de basis hoe een VPN werkt.



De versleuteling is natuurlijk niet een echt wachtwoord met een slot. Jouw verzoek wordt middels een complexe encryptiemethode omgevormd tot een soort onleesbare reeks van letters en cijfers. Omdat in dit verzoek ook verwerkt zit waar het verzoek vandaan komt en waar het naartoe gaat, wordt ook die data onleesbaar gemaakt. Hierdoor kan niemand die tussen jou en de VPN-server zit zien waar het verzoek vandaan komt, wie het verzoek heeft gedaan en waar het naartoe gaat. Het enige wat ze kunnen zien zijn de gegevens van de VPN-server. Zelfs het getoonde IP-adres en de locatie waar het verzoek vandaan komt wordt veranderd naar het IP-adres en de locatie van de VPN server.

Het fijne hieraan is, is dat alles wat je op je computer doet waar het internet bij wordt gebruikt, versleuteld kan worden. Denk aan e-mail, het bezoeken van websites, videogames of zelfs het streamen van online video's. Deze encryptie zorgt er ook voor dat je volledig anoniem bent op het internet. Het enige wat anderen kunnen achterhalen zijn de gegevens van de VPN-server, waarbij niets nog te herleiden valt tot jou als gebruiker.

Hoe maak je gebruik van een VPN verbinding?

Om daadwerkelijk verbinding te maken met een VPN netwerk moet je een VPN abonnement hebben. Tegenwoordig zijn er tientallen VPN aanbieders. Om zeker te zijn dat je privacy goed wordt beschermd én je internetverbinding niet traag wordt is het belangrijk een abonnement af te nemen bij een **goede VPN aanbieder**. Een goede plek om te beginnen is ons overzicht met VPN-reviews.
Momenteel is ExpressVPN onze eerste keus aanbieder vanwege de bewezen betrouwbaarheid. Je kan deze VPN uitproberen met een 30 dagen geld-terug-garantie . Lees hier de gehele ExpressVPN review.

Hoe werken VPN's op je computer?

Hierboven kun je lezen hoe VPN's basaal werken en hoe je deze kunt installeren en gebruiken. Er zit echter een verschil tussen VPN's op verschillende besturingssystemen. Niet elke VPN werkt op elk besturingssysteem en soms kan het installatieproces verschillen. Hieronder bespreken we kort enkele bijzonderheden van VPN's per besturingssysteem.

Windows

Windows is het meest gebruikte besturingssysteem voor VPN's. Zo'n beetje elke serieuze VPN heeft software voor Windows. Windows wordt dan ook vaak gezien als de 'standaard' vanuit VPN's. Bij het installeren van een VPN op een Windows computer kan het zijn dat je de VPN software toestemming moet geven om aanpassingen te maken aan je netwerkinstellingen. Dit is nodig zodat de VPN kan worden opgezet. De standaardinstellingen van je netwerk zijn namelijk niet altijd geschikt voor VPN verkeer.

MacOS

Naast Windows is MacOS het meest gebruikte besturingssysteem voor desktop PC's en laptops. Het is dan ook niet verbazend dat de meeste VPN's ook werken op MacOS. Het verschil tussen de werking van VPN's op MacOS en Windows zijn minimaal. Bekijk ook ons artikel: VPN instellen op Mac.

Linux

Een VPN gebruiken op Linux is een ander verhaal. Omdat Linux vanuit zichzelf al redelijk veilig is, en omdat de gebruikers van Linux meestal enige technische kennis hebben, hebben de meeste VPN's geen speciale VPN-software voor het Linux besturingssysteem. Toch bieden de grote VPN-providers wel aan dat je hun VPN op Linux kunt gebruiken. De installatie hiervan vereist iets meer technische kennis omdat je zelf het een en ander moet instellen. Zo moet je bij de VPN-provider eerst nieuwe credentials aanmaken. Hierbij selecteer je het protocol en eventueel het land waarmee je wil verbinden. Je krijgt vervolgens een server, speciale username en een wachtwoord die je kunt gebruiken om verbinding te maken met het internet middels die VPN-server.

Hoe werkt een VPN op je tablet of smartphone?

VPN's op tablet en smartphone installeren is vrij simpel. De meeste VPN's zijn namelijk gewoon beschikbaar als app. Dit betekent dat je de VPN kunt downloaden uit de app store. Je hoeft dan alleen je accountgegevens in te voeren als je de VPN hebt opgestart en je zou hem moeten kunnen gebruiken. Wel vraagt de VPN-app toestemming om aanpassingen te maken aan je netwerkinstellingen. Dit is nodig om de VPN-verbinding werkend te krijgen op je smartphone. Op Android, iOS en Windows zal de VPN je ook beveiligen als je gebruikmaakt van andere apps die internet nodig hebben. Zo beveiligen ze al je mobiele gegevens online. Tevens zorgt een VPN voor een sterk verbeterde veiligheid als je verbinding maakt met onbeschermde of publieke wif-netwerken. Omdat je vaker met dit soort netwerken zal verbinden op je smartphone en tablet dan op je desktop PC, is een VPN op tablet of smartphone geen overbodige luxe.

Hoe werkt een VPN op je router?

VPN-providers hebben een limiet ingesteld op hoeveel devices je tegelijkertijd gebruik kunt maken van een VPN. Mocht je dit willen omzeilen, of mocht je gemakshalve alle devices in huis willen laten verbinden middels VPN, dan kun je er voor kiezen om een VPN te installeren op je router. Je hoeft de VPN dan niet meer individueel op elk apparaat te installeren. Elk apparaat wat gebruik maakt van jouw router zal beveiligd zijn.

Het installeren van een VPN op je router is lastiger dan op de meeste andere devices. Je moet namelijk een speciale router hebben of je router 'flashen'. Dit betekent het aanpassen van de firmware van je router zodat je er en VPN op kunt installeren. Hoe dit precies werkt kun je hier vinden: VPN instellen op je router. Ook is het mogelijk om een router te kopen die al eerder geflashed is. Je hoeft dan zelf alleen nog maar de VPN te installeren op deze pre-flashed routers.

VPN en veiligheid: hoe werken VPN protocollen?

De meeste VPN's geven de optie om te kiezen uit verschillende beveiligingsprotocollen. Deze protocollen hebben allemaal hun eigen voor- en nadelen. Vaak is dit een technisch verhaal waarbij het ene protocol wel een bepaalde toepassing toestaat en de ander niet. De meeste VPN-gebruikers kunnen uit de voeten met OpenVPN. Dit is een open-source VPN protocol dat gebruikmaakt van verschillende algoritmes voor encryptie. Dit protocol kent dan ook weinig veiligheidsproblemen. Hieronder kun je kort een uitwerking lezen van enkele andere veel voorkomende VPN-protocollen en hoe die werken.

VPN beveiligingsprotocollen

Veel verschillende securityprotocollen zijn ontwikkeld voor VPN's, elk met verschillende niveaus van beveiliging en functies. De meest voorkomende zijn:

IP-beveiliging (IPSec):

IPSec wordt vaak gebruikt om internetcommunicatie te beveiligen en kent twee versies (modi). Transportmodus versleutelt alleen het datapakket zelf terwijl de Tunneling modus het gehele datapakket versleutelt. Dit protocol kan ook gebruikt worden in combinatie met andere protocollen om gezamenlijk het veiligheidsniveau te verhogen.

Layer 2 Tunneling Protocol (L2TP) / IPsec:

De L2TP en IPsec-protocollen combineren hun beste individuele eigenschappen om een zeer veilige VPN-verbinding te creëren. Aangezien L2TP niet kan coderen genereert deze de tunnel en wordt het IPSec protocol gebruikt voor de codering.

Secure Sockets Layer (SSL) en Transport Layer Security (TLS):

SSL en TLS worden veel gebruikt in de beveiliging van online retailers en dienstverleners. Deze protocollen werken door middel van een handshake-methode. IBM legt uit: "*Een HTTP-SSL-verbinding wordt altijd geïnitieerd door de klant via een URL beginnend met https:// in plaats van http://. Aan het begin van een SSL-sessie, is een SSL-handshake uitgevoerd. Deze handdruk produceert de cryptografische parameters van de sessie.*" Deze parameters, meestal digitale certificaten, zijn de middelen waarmee de twee systemen encryptiesleutels uitwisselen, de sessie autoriseren en de beveiligde verbinding creëren.

Point-to-Point Tunneling Protocol (PPTP):

PPTP is een zeer veel gebruikt VPN-protocol en kan op een enorme verscheidenheid aan besturingssystemen worden geïnstalleerd. Net als L2TP, encrypt PPTP zelf geen data, maar legt het een tunnel en kapselt het daarbij het datapakket in.
Daarbij wordt een tweede protocol (bv TCP of GRE) gebruikt voor de codering. PPTP is overschaduwd door nieuwere methoden; het protocol blijft sterk, maar is niet meer de veiligste.

Secure Shell (SSH):

SSH legt de VPN-tunnel en zorgt voor de encryptie. De data zelf is niet versleuteld, maar het kanaal wel. SSH-verbindingen worden gemaakt door een SSH-client, die het verkeer doorstuurt van een lokale poort naar een externe server. Alle gegevens tussen de twee kanten van de tunnel stromen door deze gespecificeerde poorten.

Om daadwerkelijk gebruik te maken van de VPN-tunnel, moet de lokale machine een VPN-client (programma) draaien. Open-VPN is een populaire (én gratis) multi-platform applicatie, maar de meeste goede VPN providers leveren hun eigen software mee.

Wat is een goede VPN provider?

De keuze voor een VPN provider kan moeilijk zijn. Het aantal providers waaruit je kunt kiezen neemt bijna dagelijks toe. Helaas zit er een heleboel “rommel” tussen de beschikbare providers en is het soms lastig om een goed onderscheid te maken tussen goede providers en slechte VPN providers.

Een goede VPN provider moet voldoen aan verschillende voorwaarden. Allereerst moet de aanbieder een **goed server netwerk** hebben. Het server netwerk moet verspreid zijn over verschillende landen, omdat elk land weer zijn eigen voor- en nadelen heeft. Daarnaast moeten de servers zélf snel zijn én hun verbinding met de rest van het internet moet snel zijn.

Daarnaast moet de provider een goede omgang met jouw gegevens garanderen. Er moeten zo min mogelijk logs bijgehouden worden en de beste protocollen (zoals OpenVPN) moeten beschikbaar zijn. Hier zit bij veel providers een groot probleem. Het kan ook lastig zijn voor consumenten om goed na te gaan welke providers het beste met hun privacy omgaan.