Veilig surfen: hoe werkt een VPN?

Het gebruik van VPN's wordt steeds populairder, gaande van het versterken van de veiligheid van je internetverkeer, tot het bekijken van meer films op Netflix en helaas ook voor cyberaanvallen. Wat gebeurt er nu precies achter de schermen?

VPN's, oftewel Virtual Private Networks, bestaan nu al een tijdje en zijn steeds moeilijker weg te denken uit het digitale landschap. Sinds de eerste VPN's voor consumenten in 2005 zijn ze aan een flinke opmars bezig en de providers doen dan ook hun uiterste best om online zoveel mogelijk reclame te maken. VPN's werden eerst ontwikkeld voor en door bedrijven. Door een VPN in te schakelen konden hun werknemers op een veilige en discrete manier (zowel intern als extern) communiceren, zonder potentiële pottenkijkers.

Die voorlopers van VPN's hebben intussen een mooie evolutie doorgemaakt, en het is dan ook niet verwonderlijk dat bedrijven ze nog graag gebruiken om hun netwerken te beveiligen. Ze bestaan nu in allerlei vormen, gaande van een eenvoudige browserextensie, tot een applicatie op je desktop of laptop. Daarnaast zijn er nog meerdere protocollen, elk met zijn eigen mate van betrouwbaarheid, veiligheid en snelheid. VPN's hebben meerdere doeleinden, waaronder het beschermen van je data bij onbekende wifi-verbindingen, het deblokkeren van buitenlandse streamingdiensten of sportwedstrijden, het omzeilen van censuur of het algemeen beveiligen van je internetgebruik.

1. Wat is een VPN?

Ondanks al die voordelen is toch niet iedereen even goed op de hoogte van hoe een VPN echt werkt en wat de werking van de diensten allemaal kan betekenen voor je internetverkeer. Daar willen we dan graag even bij helpen. Wij zetten het hier voor jou even op een rijtje, zodat je bij het opstarten van je eigen VPN goed weet wat er nu precies met je data gebeurt.

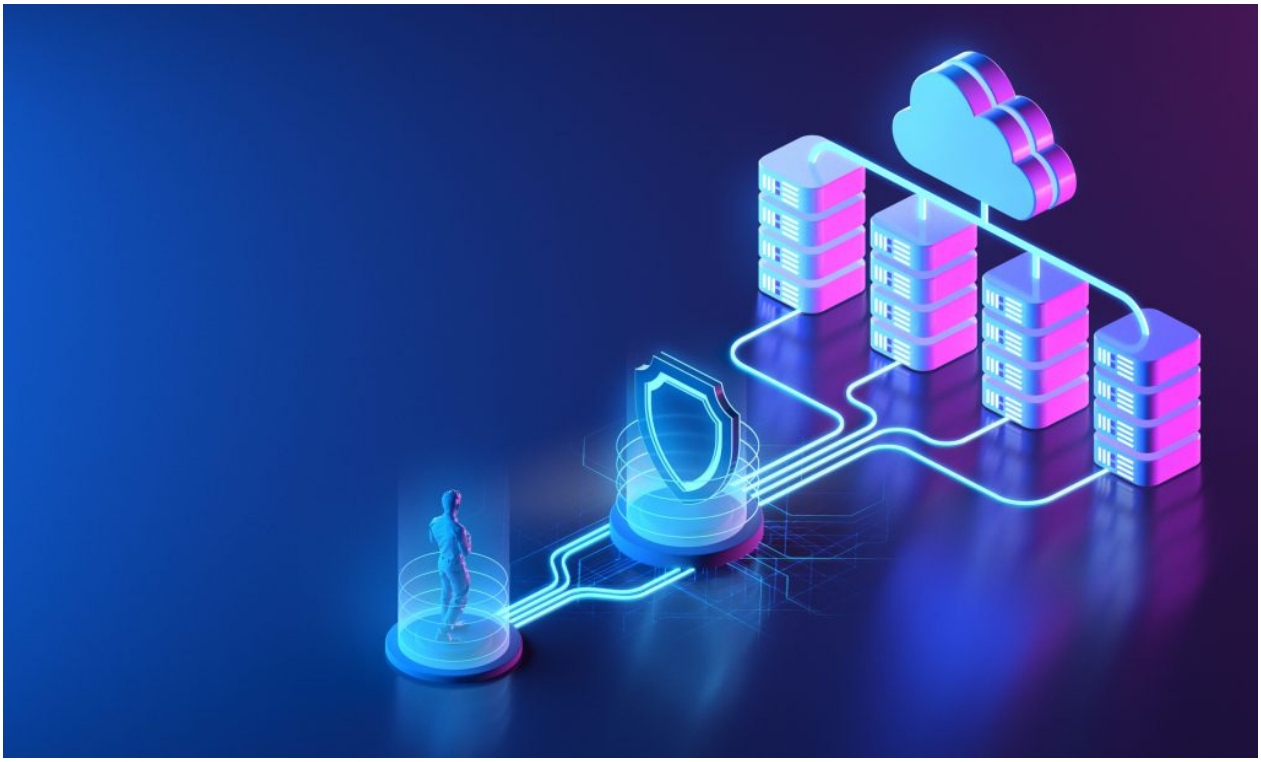
Dankzij een VPN heb je op een beschermde manier toegang tot de rest van het internet.

2. Werking

Om de werking van een VPN te verduidelijken moeten we misschien even kijken hoe ons normale internetverkeer eruitziet bij bijvoorbeeld het bezoeken van een website. Als je een verbinding wil maken met een bepaalde website, zoals bijvoorbeeld facebook.com, dan leg je een connectie tussen je IP-adres, je internetprovider en het IP-adres van die website. Die internetprovider is nodig, omdat je anders gewoonweg geen toegang krijgt tot het wereldwijde web. Providers hebben een volledig overzicht van de diensten en webpagina's die je allemaal bezoekt. Dat houden ze dan allemaal bij en ze kunnen het ook te allen tijde lezen. Willen ze bijvoorbeeld niet dat je allerlei illegale pagina's, zoals torrent sites, bezoekt? Dan zullen ze je de toegang hiertoe ontzeggen. Wil de overheid je ook om een of andere reden in je zoekactiviteiten fnuiken?

Dan zullen zij de internetproviders van hun land allerlei regels opleggen, met de nodige censuur als gevolg. Bij een VPN worden er enkele extra stappen tussen geplaatst, om je data en identiteit te beschermen. Om te beginnen zal de VPN-provider met zijn software ervoor zorgen dat de data die je computer verlaat voorzien is van een encryptie. Die wordt door de VPN-dienst uitgevoerd, en zal ook enkel door hen gelezen kunnen worden. Daarna komt deze data terecht bij je internetprovider.

Die geëncrypteerde gegevens verlaten de servers van je provider en komen dan via het web bij servers van je VPN-provider terecht. Je internetprovider zal wel weten dat er een verbinding wordt gelegd tussen jouw toestel en de provider, maar verder zal die geen informatie hebben over de exacte inhoud van je verzoek.



Als laatste stap zal je VPN-provider je informatie van zijn servers doorsturen naar de gevraagde website. Die geeft je dan toegang tot zijn diensten, of stuurt de benodigde informatie terug naar de server van de VPN, en zo opnieuw geëncrypteerd naar jou. De VPN speelt dus zowat de rol van tussenpersoon als je een bepaalde website bezoekt. Je IP-adres stuitert via je toestel naar de internetprovider en zo naar de VPN-dienst. Wanneer het deze servers verlaat, wordt het omgezet naar een ander IP-adres, zijnde eentje van de locatie waar de servers zich bevinden.

Er wordt dus als het ware een datatunnel voorzien tussen je computer en de servers van de VPN-provider, waarin data zorgeloos kan stromen en je er zeker van kan zijn dan niemand meekijkt naar wat je juist doorstuurt of opvraagt, en van waar. Zo werkt het dan bijvoorbeeld ook bij het deblokkeren van streamingdiensten. Je laat de servers van het Amerikaanse Netflix geloven dat je je in de Verenigde Staten bevindt, waardoor zij je toegang geven tot alles van Netflix dat je daar kan bekijken.

Streamingdiensten deblokkeren is slechts een van de vele handige functies van een VPN.

3. Werkt een VPN dan ook echt?

Om de veiligheid van je VPN te bepalen is het zeker belangrijk dat je weet wat een VPN écht doet. Deze virtuele netwerken voorzien een beschermde laag rond je informatie en zorgen ervoor dat ze veilig op de bestemming aankomt. Dit geeft je echter geen vrijgeleide om zomaar op het internet te doen wat je wil. Als je bijvoorbeeld een verbinding maakt met een onbeschermde website of eentje die je computer met malware wil besmetten, dan zal een VPN weinig redding bieden.

Daarnaast hebben sommige hackers en inlichtingendiensten nog andere trucjes om te kijken wat je allemaal met een VPN doet. Door bijvoorbeeld de punten voor en na de VPN-servers te monitoren, kunnen ze zien wanneer je internetverbinding bij de VPN-servers binnenkomt, en wanneer er bij hen ook iets vertrekt. Door deze twee gegevens naast elkaar te leggen, zullen ze dan een inschatting kunnen maken qua tijden van binnenkomst en vertrek om zo te zien wat je allemaal uitspookt. Dit is zeker geen enorm betrouwbare methode om je op te volgen, maar echt onmogelijk is het zeker niet.

Ook VPN’s kunnen het slachtoffer worden van een hack en zijn dus niet onkwetsbaar.

Het is dan ook niet zo dat VPN-providers zelf volledig waterdicht zijn. Ook zij kunnen het slachtoffer zijn van een hack, waarbij hun data gestolen wordt. In maart van 2018 werd een Finse server van NordVPN nog getroffen door een cyberaanval. Het bedrijf kreeg ook pas een jaar later te horen dat een van zijn servers gehackt was, wat ook niet bepaald goede reclame is. Bovendien houden sommige VPN-diensten nog logs bij van al het verkeer op hun servers. Bij een hack of opvraging door ordediensten kan dit door externen gelezen worden en ze weten dan ongeveer alles.

De markt van VPN’s is zeer groot, en ze doen ook steeds hun uiterste best om uit te pakken met allerlei speciale functies, in de hoop je overtuigd te krijgen voor hun specifieke product. Ook hier moet je altijd wat scepsis aan de dag leggen, omdat die functies niet altijd zo goed werken als beloofd. Zo pakken veel diensten al dan niet groots uit met de mogelijkheid om buitenlandse streamingdiensten te deblokkeren. Gezien de wijzigende catalogi van bijvoorbeeld Netflix en Amazon Prime Video is dit voor velen dan ook een aantrekkelijke optie. De streamingdiensten worden echter steeds beter in het herkennen van de IP-adressen van VPN-diensten, waarna ze de toegang tot hun mediaservers zouden kunnen blokkeren.

Een VPN biedt wel wat bescherming, maar maakt je niet immuun voor cyberaanvallen.

Net als bij elk ander soort product speelt ook de kwaliteit van de VPN een grote rol. De meeste betaalde diensten voorzien naast de veilige en soms zelfontworpen protocollen ook nog allerlei andere functies, waaronder bijvoorbeeld een kill switch en een no-logging-beleid, zodat je er zeker van kan zijn dat zelfs in het geval van een hack bij je VPN-provider al je data ongeschonden blijft. Naast betaalde diensten zijn er ook gratis versies, maar ook hier is het belangrijk om te weten dat gratis zaken nooit ‘echt gratis’ zijn. De kans dat je dus op een bepaalde manier data zal moeten afstaan is groot, dus als je graag met een gratis VPN aan de slag wilt, raden we je toch aan om altijd de kleine lettertjes te lezen.

Daarom is het dan ook belangrijk om bij het beschermen van je netwerken niet enkel te willen vertrouwen op de werking van je VPN. Wil je steeds zoveel mogelijk zekerheid? Dan is het ook belangrijk om te investeren in een goed antiviruspakket, het instellen van de nodige tweestapsverificatie en je wachtwoorden regelmatig te veranderen.

Bron: TechPulse van 25 april 2022