

Wat een VPN echt is

Het verandert wie je kan zien, niet of iemand het kan.

Eenvoudig gezegd: een VPN zorgt ervoor dat je internetprovider of de wifi op een vliegveld niet meer ziet waar je verbinding mee maakt. Die informatie verdwijnt niet: ze gaat naar het VPN-bedrijf, dat het nu wel ziet. Wat al versleuteld reisde, zoals je e-mail of bank, was dat daarvoor ook al. Het dient voor een paar concrete zaken en wordt vaak verkocht alsof het veel meer oplost.

Jarenlang hoorde ik over VPN's en besteedde ik er geen aandacht aan, net als bij antivirusprogramma's: ik gebruik geen antivirus, of bijna nooit. Ik heb realtime kopieën van alles op drie plekken en let goed op wat ik download, op welke links ik klik en welke websites ik bezoek. Het is geen honderd procent veiligheid, maar voor mij werkt het. Op een dag zag ik een VPN-aanbieding voor iets meer dan twee euro per maand en nam het uit nieuwsgierigheid. Het werkt goed, maar ik heb er weinig aan gehad: bijvoorbeeld om een dienst te testen die toen alleen in de Verenigde Staten beschikbaar was. Voel ik me veiliger? Nee. Als ze het me weer voor die prijs aanbieden, verleng ik misschien; zo niet, dan niet. Het is slechts mijn eigen ervaring, het bewijst niets. Dus vroeg ik me af wat een VPN precies doet. Dit is hoe ik het begrepen heb.

Stel je voor dat je een brief in de brievenbus gooi met het adres van de ontvanger duidelijk zichtbaar. De postbode ziet naar wie je hem stuurt, ook al kan hij hem niet lezen als hij dichtgeplakt is. Die postbode is je internetprovider. Een VPN stopt je brief in een andere envelop, geadresseerd aan een tussenpersoon die hem opent en doorstuurt. Je vaste postbode ziet het echte adres niet meer. Hij ziet alleen dat je naar die tussenpersoon schrijft.

Degene die het netwerk beheert vanwaar je verbinding maakt – bijvoorbeeld de wifi op een vliegveld –, ziet niet meer waar je naartoe gaat. Maar de tussenpersoon ziet nu wat je provider vroeger zag, en soms meer, omdat al je verkeer via hem loopt. Het toezicht verdwijnt niet: het wisselt van eigenaar. Vandaar de naam.

Bovendien reist bijna alles wat je vandaag doet – zoals je mail openen of inloggen bij de bank –, al versleuteld naar de bestemmingsserver dankzij het slotje in de browser. Dat gebeurt met en zonder VPN. Een VPN voegt alleen bescherming toe op het eerste traject, tot aan zijn eigen server. Vanaf daar is de weg dezelfde als altijd.

Daarom zijn er dingen die het je niet kan beloven, ook al wordt het soms zo verkocht. Als je bent ingelogd op je e-mail of bank, weet die dienst wie je bent, met of zonder VPN. Het garandeert ook niet dat niemand je verkeer bekijkt: het verandert alleen wie er kijkt. Dat het bedrijf zegt dat het «geen logs bijhoudt», is een belofte, net zoals wanneer een groot platform zegt «je berichten zijn versleuteld, we lezen ze niet». Een audit kan dat op een bepaald moment bevestigen, maar het blijft iets waarvan je vertrouwt dat het wordt nageleefd, niet iets wat door de architectuur zelf onmogelijk te schenden is.

En de inhoud van een gesprek blijft gelijk. Als je berichten-app al van begin tot eind versleutelt, voegt een VPN niets toe. Doet hij dat niet, dan lost een VPN dat ook niet op: het beschermt het traject van het bericht, niet wat de app of zijn server ermee doen zodra het aankomt.

Niets hiervan maakt het nutteloos. Verbergen waar je verbinding mee maakt voor openbare wifi, voor een provider die die geschiedenis wil verkopen of voor een land dat een dienst blokkeert, is echt werk en dat doet het goed. De marketing belooft echter meestal meer dan deze laag kan waarmaken.

De vraag die je jezelf moet stellen bij een VPN of elke dienst die belooft je te beschermen, is niet «is het versleuteld?». Waarschijnlijk wel, in elk geval op een deel van het traject. Het is deze andere: bij wie leg ik het vertrouwen neer dat ik een ander heb ontnomen? En wat houd ik over als dat ongegrond blijkt?

Een VPN verandert, als het zijn werk goed doet, alleen wie de tussenpersoon van je verbinding is. Een app zoals Solo2, waarvan de berichten via geen enkele server lopen, haalt de tussenpersoon volledig uit het gesprek. Ze concurreren niet: ze lossen verschillende problemen op.

Ze verwarren is een veelvoorkomende manier om te denken dat je beter beschermd bent dan je in werkelijkheid bent.

Noot van de redactie: wanneer deze Cuadernos bedrijven of producten noemen, is dat niet om te beschuldigen. Degenen die ze bouwen, leveren werk dat miljoenen mensen gebruiken en waarderen. Wat we aanstippen is structureel — het model, niet het merk. Merken verschijnen als voorbeeld omdat dit de merken zijn die de lezer herkent.

Bronnen und verdere lectuur

- Het HTTPS-protocol en transportversleuteling zijn open standaarden, publiek gedocumenteerd door de IETF.
- In deze reeks: «Wanneer er niemand in het midden is» en «Je bent niet anoniem» belichten vanuit andere invalshoeken hetzelfde onderscheid tussen structuur en belofte.

[← Vorige Je bent niet anoniem](#)

Recente artikelen

- [Reflectie · 29 juni 2026 Je bent niet anoniem](#)
- [Reflectie · 27 mei 2026 Wat een handtekening niet kan oplossen](#)
- [Analyse · 26 mei 2026 Echte vs. schijnbare privacy: de vragen die men zich moet stellen](#)

Neem dit artikel mee naar waar je het nodig hebt.

[↓ Markdown](#) [↓ Platte tekst](#) [↓ PDF](#)

Het bestand wordt gedownload naar je apparaat. Van daaruit kun je het opslaan, importeren in Solo2 of delen waar je maar wilt. Cuadernos beslist niet voor jou over de bestemming.

Lakzegel · SHA-256 6d12752b9159123ed271a7d8687833664e609803941206ac67b2bb45e62f157e

[Functies](#) [Prijzen](#) [Installeren](#) [Nieuws](#) [Blog](#) [Pro](#) [Hulp](#) [Over](#) [Contact](#)
[Transparantie](#) [Verificatie](#) [Privacy](#) [Voorwaarden](#) [Cookies](#)

Cuadernos Lacre · Een uitgave van [Menzuri Gestión S.L.](#) ·
geschreven door R.Eugenio · geredigeerd door het team van [Solo2](#).

Deze website gebruikt geen cookies. Alles wat je browser laadt, is door ons geschreven of onder ons toezicht en wordt gehost op onze Europese servers: de anonieme bezoeker (Umami, zelf gehost) en het minimale JavaScript dat nodig is voor de taalkeuze en je voorkeur voor een licht/donker thema, die op je eigen apparaat wordt opgeslagen. Geen bronnen van derden, geen trackers, geen profilering, geen delen van gegevens. Als je ons wilt volgen: [RSS](#).