VPN uitgelegd: Wat is een VPN en waar gebruik je het voor?

VPN info https://www.vpngids.nl/vpn-info/

Wat is een VPN?

Een VPN is een Virtual Private Network. Dit 'virtuele privénetwerk' stelt gebruikers in staat om hun dataverkeer via een versleutelde, beveiligde verbinding naar een externe VPN-server te sturen. Van daaruit wordt het dataverkeer dan weer het internet op gestuurd. Een VPN-verbinding biedt een internetgebruiker drie zeer essentiële zaken: veiligheid, anonimiteit en vrijheid op het internet.

- **Veiligheid** wordt geboden doordat een VPN al het internetverkeer versleutelt en beveiligt tegen partijen die data proberen te onderscheppen, zoals hackers en overheden.
- **Anonimiteit** wordt geboden doordat jouw IP-adres wordt verborgen zodra je verbinding maakt met een VPN-server. Het IP-adres is als het ware de persoonlijke identificatiecode van jouw internetverbinding, waaraan je herkend kan worden online. Als VPN-gebruiker neem je het IP-adres van de VPN-server aan. Hierdoor kunnen andere partijen op het internet jouw locatie en identiteit niet langer achterhalen.
- **Vrijheid** wordt geboden doordat een VPN-provider je in staat stelt te verbinden met servers over de hele wereld. Door te verbinden met een VPN-server in een bepaald land, ga je het internet op alsof je zelf in dat land bent. Het internet is namelijk niet overal ter wereld vrij toegankelijk. Je kan daarbij denken aan online censuur, restricties op sociale media en beperkingen van online streamingdiensten. Ook als Nederlander heb je daarmee te maken. Veel Nederlandse websites en streamingdiensten werken niet buiten Nederland. Dit kan je oplossen met een VPN. Ook kan je vanuit Nederland toegang krijgen tot sites en diensten die normaal gesproken niet in Nederland beschikbaar zijn, zoals de Amerikaanse versie van Netflix.

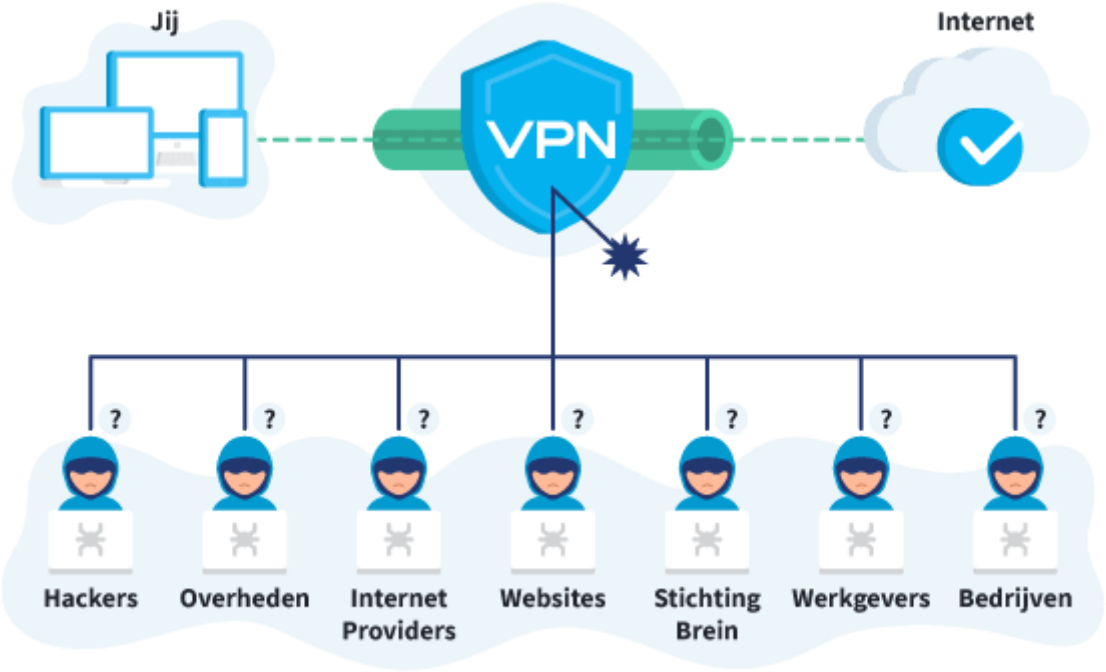
Veel mensen vinden het fenomeen VPN maar complex. Daarom leggen we op deze pagina precies uit wat VPN is, hoe je het gebruikt en welke handige toepassingen er allemaal mogelijk zijn!

Wil je graag zelf alvast gebruik gaan maken van een VPN, dan is ons overzicht van de beste VPN-aanbieders interessant voor jou:

Bekijk beste VPN's

Hoe maak je zelf makkelijk gebruik van een VPN?

Het is heel eenvoudig om zelf gebruik te maken van een VPN. Om te beginnen sluit je een abonnement bij een betrouwbare VPN-aanbieder af. Dit kan je heel gemakkelijk en snel online doen, waarna je direct de benodigde VPN-software (apps) kan downloaden en installeren. Nu heb je toegang tot het servernetwerk van de VPN-provider. Met enkele klikken maak je vervolgens verbinding met een VPN-server. Dit kunnen servers over de hele wereld zijn. Vanaf dat moment loopt al je internetverkeer via de beveiligde VPN-verbinding en kan je veilig, vrij en anoniem gebruikmaken van het internet.

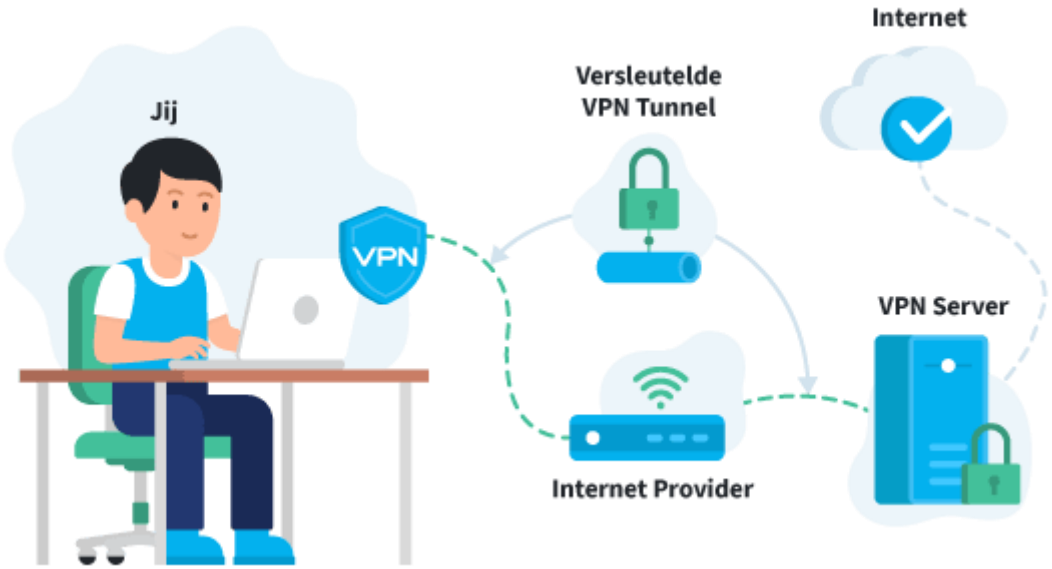


De meeste VPN-aanbieders bieden software aan voor al je apparaten en besturingssystemen (Windows, Mac, iPhone, Android). Ook is het in sommige gevallen mogelijk de VPN op de router te installeren. Hierdoor worden automatisch alle apparaten die op het netwerk zijn aangesloten beveiligd.

Hoe werkt een VPN

Als je een betrouwbare VPN-aanbieder gevonden hebt en de software hebt geïnstalleerd, kun je de gewenste veiligheidsinstellingen selecteren en verbinding maken met de gewenste VPN-server. Als de VPN-verbinding tot stand is gekomen, gebeurt er het volgende met je dataverkeer:

1. De VPN-software versleutelt het internetverkeer en stuurt jouw data over een beveiligde verbinding naar de VPN-server.
2. De VPN-server ontvangt het versleutelde internetverkeer van jouw apparaat en onstleutelt het internetverkeer.
3. De VPN-server stuurt vervolgens het ontsleutelde internetverkeer het internet op. Ook ontvangt de VPN-server eventueel teruggestuurd internetverkeer dat bedoeld is voor jou als gebruiker.
4. Het internetverkeer dat de VPN-server ontvangt wordt vervolgens versleuteld en via de beveiligde verbinding terug naar jou als gebruiker gestuurd.



De VPN-verbinding beveiligt je internetverkeer, zodat hackers je data niet meer zomaar kunnen onderscheppen. Daarnaast biedt een VPN-verbinding anonimiteit, doordat je internetverkeer wordt omgeleid via een externe VPN-server. Hierdoor registreert de rest van het internet het IP-adres van de VPN-server, terwijl jouw echte IP-adres verborgen blijft. Normaal gesproken wordt je middels dit IP-adres herkend online, maar dit kan dus niet meer. Je bent anoniem geworden.

Het komt erop neer dat de VPN-applicatie op de achtergrond van je computer, tablet of smartphone draait. Hier merk je zelf eigenlijk weinig van, en je kan gewoon gebruikmaken van het internet. Voor meer informatie over de precieze werking van een VPN verwijzen wij naar het artikel: Hoe werkt een VPN verbinding.

Waar wordt een VPN voor gebruikt

Er zijn diverse redenen waarom mensen een VPN gebruiken. De meest voorkomende redenen zijn:

- **Anonimiteit op het internet**: Een VPN-verbinding verbergt je IP-adres en locatie. Als gebruiker neem je namelijk het IP-adres van de VPN-server aan. Het lijkt nu alsof jij je bevindt op de locatie van de VPN-server. Hierdoor kunnen websites en anderen je echte locatie niet achterhalen. Ook kunnen andere partijen op het internet je niet langer identificeren middels je IP-adres, want ze zien slechts het nietszeggende IP-adres van de VPN-server.
- **Beveiliging tegen hacker en overheden**: In toenemende mate wordt bekend hoeveel er op het internet afgeluisterd wordt. Zonder VPN-verbinding stuur je al je gegevens onbeveiligd het internet op. Je internetverbinding is hierdoor erg makkelijk af te luisteren. Een VPN versleutelt je internetverkeer waardoor afluisteren geen zin heeft.
- **Veilig internetten op publieke netwerken**: Het gebruik van publieke netwerken is erg riskant. Andere gebruikers van publieke netwerken (bijvoorbeeld hackers) kunnen namelijk al je internetverkeer makkelijk afluisteren of omleiden. De kans dat je bijvoorbeeld de inloggegevens van je email of je creditcardgegevens op deze manier kwijtraakt is erg groot. Door een VPN te gebruiken versleutel je alle gegevens die je het netwerk op stuurt. Hierdoor heeft een hacker niks aan de afgeluisterde internetgegevens. In plaats van jouw belangrijke gegevens en wachtwoorden ziet de hacker slechts een gecodeerde wirwar van tekens (versleutelde data).
- **Censuur en geografische blokkades omzeilen:** Het internet kent vele restricties. Zo kun je normaal gesproken geen Nederlandse tv in het buitenland kijken en kun je met Netflix in Nederland beduidend minder films en series kijken dan met Netflix in Amerika. Daarnaast zijn er vele landen (bv China, Turkije en Arabische landen) die toegang tot bepaalde internetdiensten (bv Whatsapp, Skype of Facebook) blokkeren. Zelfs in Nederland wordt The Pirate Bay geblokkeerd. Een VPN verandert je geografische locatie waardoor dergelijke blokkades omzeild kunnen worden.
- **Anoniem downloaden (en uploaden)**: Downloaders (bv via Torrents of Usenet / nieuwsgroepen) worden steeds meer gevolgd. Veel mensen willen liever niet dat anderen weten wat ze gedownload hebben en kiezen er dus voor om anoniem te gaan downloaden. Een VPN verbinding is hier bij uitstek geschikt voor.
- **Een digitaal persoonsdossier voorkomen**: Advertentienetwerken zoals Facebook, Google en Twitter proberen een zo goed mogelijk privédossier over iedereen op te bouwen. Deze informatie kan vervolgens verkocht worden aan adverteerders of overheden. Het gebruik van een anonieme VPN verbinding gaat het opbouwen van een dergelijk dossier tegen.
- **Toegang tot bedrijfsnetwerken**: Steeds meer bedrijven bieden hun werknemers de mogelijkheid om van thuis op hun netwerk in te loggen en op deze manier van thuis uit te kunnen werken. Hiervoor worden ook VPN verbindingen gebruikt.

Voor een uitgebreider artikel over de redenen waarom mensen VPN netwerken gebruiken verwijzen wij je naar: Waarom mensen een VPN gebruiken.

Een VPN verbinding gebruiken

Om gebruik te maken van een VPN-netwerk heb je een **VPN-account** nodig. Een goed account kun je vaak al voor enkele euro's per maand afsluiten. Na het registeren geeft de aanbieder je inloggegevens voor hun VPN-servers. Deze inloggegevens kun je vervolgens gebruiken om verbinding te maken met de servers van de aanbieder. De meeste (grote) aanbieders bieden speciale (gratis) VPN-programma's of VPN-Apps waarmee je erg makkelijk een verbinding kunt opzetten. In deze programma's kun je vaak kiezen welk protocol je wil gebruiken en met welke servers in welk land / stad je wilt verbinden.

Twee goede VPN-providers

Wij hebben alle grote VPN aanbieders van dit moment getest. Een uitgebreidere beschrijving van goede aanbieders vind je in ons overzicht van de beste VPN providers. Mocht u aan de slag willen met een makkelijke, gebruiksvriendelijke en betrouwbare VPN, dan kunnen wij GOOSE VPN en ExpressVPN aanbevelen.

GOOSE VPN

GOOSE is een VPN van Nederlandse bodem. Zo is er een Nederlandse klantenservice, wat heel fijn is als je ergens hulp bij nodig hebt. Ook de apps van GOOSE VPN zijn in te stellen op de Nederlandse taal. GOOSE VPN houdt je internetverbinding veilig en biedt je anonimiteit online. Er zijn makkelijke apps voor Windows, Mac, Android en iOS.

GOOSE VPN is uitermate geschikt voor het omzeilen van geografische blokkades en het veilig downloaden van torrents. En GOOSE VPN is erg goed geprijsd; voor slechts €2,99 per maand kan je de dienst al gebruiken. Dan heb je een datalimiet van 50GB per maand. Wil je zonder datalimiet al je internetverkeer beveiligen met GOOSE VPN, dan kan dat al voor €4,99 per maand. Met de kortingscode PRIVACY krijg je bij het afsluiten van je abonnement bovendien nog 30% korting.

Bezoek GOOSE VPN

Prima Nederlandse VPN. Betrouwbaar en 30 dagen geld-terug-garantie.
Actie: Krijg **30% korting** op de Unlimited Pakketten door bij het aanmelden de promotiecode '**Privacy**' te gebruiken.

ExpressVPN

ExpressVPN is een van de beste VPN-aanbieders die wij dusver hebben getest. Ze bieden snelle en stabiele servers, fijne apps voor alle devices en goede klantondersteuning. Wel is het zo dat ExpressVPN niet de goedkoopste VPN-aanbieder is. Ze zetten heel sterk in op kwaliteit, en dat komt met een prijskaartje. Via een speciale kortingsactie beginnen abonnementen nu bij $6,67 per maand. Dan heb je een abonnement waarmee je 3 apparaten tegelijkertijd kunt beveiligen met ExpressVPN.

Bezoek ExpressVPN

ExpressVPN

Beste Premium VPN. Snel, veilig en 30 dagen geld-terug-garantie.
Actie: **3 maanden gratis** bij een jaarabonnement. (Klik hier)*Werkt alleen via de links op onze website.

Extra tip: om in één keer alle apparaten thuis gebruik te laten maken van de VPN-verbinding kun je in sommige routers de VPN-verbinding instellen. Hierdoor gebruiken alle apparaten die met die router verbonden zijn automatisch de VPN-verbinding. Dit instellen kan technisch uitdagend zijn. Indien mogelijk adviseren wij DD-WRT routersoftware te gebruiken: zie dit artikel VPN op Router instellen (DD-WRT stappenplan)

Welke VPN protocollen zijn er?

VPN verbindingen maken gebruik van een versleutelde verbinding (tunnel). Er zijn verschillende manieren (protocollen) waarmee een dergelijke VPN verbinding kan worden opgezet. De meest gebruikte zijn:

- **OpenVPN**: OpenVPN is momenteel een van de meest gebruikte protocollen. OpenVPN is een open-source protocol met versleuteling op basis van OpenSSL en het SSLv3/TLSv1 protocol. OpenVPN wordt door de meeste VPN providers ondersteund e is beschikbaar voor vele diverse platformen (o.a. Windows, Mac (OSx), Android, iOS, Linux, DD-WRT routers). OpenVPN wordt over het algemeen als beste keuze gezien.
- **IPSec/L2TP:** in dit gecombineerde protocol zorgt IPsec voor de versleuteling (encryptie) en L2TP voor de verbinding (tunnel). IPsec/L2TP zit standaard gebouwd in de meeste besturingssystemen en is een goede keuze indien OpenVPN niet beschikbaar is.
- **PPTP**: PPTP (Point to Point Tunneling Protocol) is een van de eerste protocollen die beschikbaar kwam. Het protocol kent een aantal (potentiële) veiligheidslekken. Hierdoor is het gebruik van PPTP is veel gevallen af te raden tenzij snelheid belangrijker is dan veiligheid (bijvoorbeeld in het omzeilen van blokkades van streamingdiensten).
- **Softether**: Softether is geen stand-alone protocol maar een open-source applicatie die cross platform werkt en ondersteuning biedt voor VPN-protocollen zoals SSL VPN, L2TP / IPsec, OpenVPN en Microsoft Secure Socket Tunneling **Protocol.** Ondersteuning wordt door SoftEther geleverd in de vorm van één enkele VPN-server.

Een VPN verbinding opzetten: zelf aan de slag

Er zijn verschillende manieren om een VPN verbinding op te zetten. Thuisgebruikers kunnen het beste kiezen voor een abonnement bij een VPN-provider.
Er zijn een aantal zeer grote providers met zeer snelle VPN-servers over de hele wereld. Deze providers zorgen ervoor dat de beveiliging en snelheid van hun servers op orde is. Wij hebben de beste VPN providers op een rij gezet: