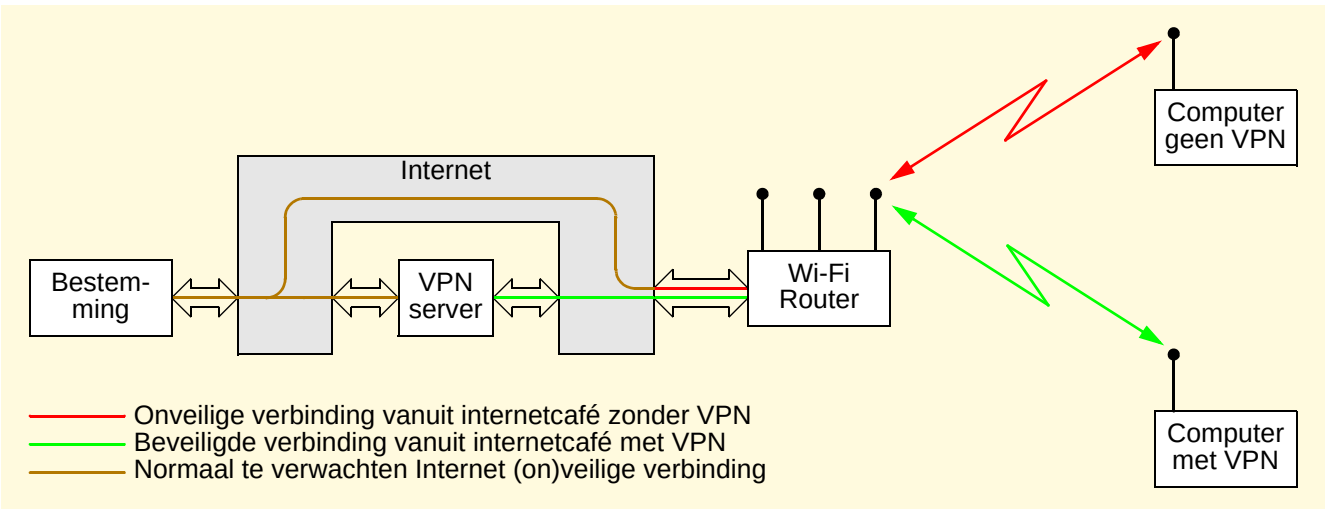
De VPN tunnel

Veilig een publiek Wi-Fi netwerk gebruiken



Voorwoord

Dit is een inleiding voor het gebruik van een VPN tunnel om de veiligheid van internetcommunicatie via een openbaar Wi-Fi netwerk te vergroten. VPN staat voor Virtual Private Network (Virtueel Privé Netwerk). Deze inleiding is bedoeld voor de voor de iets gevorderde computergebruiker. Standaard Windows handelingen, het downloaden van programma's en het aanmaken van accounts wordt bekend verondersteld. Beschreven wordt:

- Wat is een VPN en hoe vergroot het gebruik van een VPN de veiligheid van datacommunicatie over internet.
- Het kiezen van een VPN provider. Opgenomen is een beperkt overzicht van VPN providers die minimaal een gratis probeermogelijkheid bieden.
- Een eventueel handig hulpprogramma (WhatInStartup).

Gustaaf van Dijk
Technisch Auteur

Versie: S20150223

Inhoudsopgave

Versie: S20150223

Lijst van figuren

Inleiding

Hoe gebruikt u deze handleiding?

Vanuit de bron van deze handleiding worden – met behulp van twee verschillende opmaaksjablonen en voorwaardelijke teksten – twee verschillende versies van dezelfde handleiding gegenereerd:

- Een versie die bedoeld is om af te drukken op papier (A4 formaat): VPN_Handleiding_Print.pdf.
- Een versie die bedoeld is voor elektronisch interactief gebruik: VPN_Handleiding_Scherm.pdf.

Beide versies zijn beschikbaar als PDF. Om deze 'Portable Document Format' documenten te kunnen lezen en afdrukken moet een PDF-lezer geïnstalleerd zijn.

Bijvoorbeeld de gratis PDF-lezer van Adobe. Deze is te downloaden vanaf: http://get.adobe.com/nl/reader/.

Er bestaan meer PDF lezers van andere aanbieders. De nu volgende beschrijving is gebaseerd op de 'Adobe Reader'.

Met de PDF-lezer van Adobe werkt deze handleiding interactief zoals hieronder beschreven. Het kan zijn dat andere PDF-lezers één of meer mogelijkheden niet ondersteunen.

In de 'Adobe Reader' kan met de toetscombinatie 'Ctrl+L' heen en terug geschakeld worden naar vertoning op volledige schermgrootte. De 'terugbalk' werkt optimaal als de gehele bladzijde zichtbaar is op het scherm.

De elementen van deze handleiding

Tekstconventies

Teksten die letterlijk voorkomen in een venster zijn *cursief*.

Gebruikte termen beginnen met een hoofdletter.

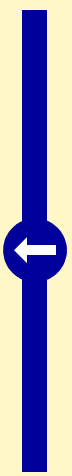
Andere termen staan 'tussen aanhalingstekens'.

Verwijzingen

Verwijzingen hebben deze kleur. Door erop te klikken wordt gesprongen naar de plaats waarnaar verwezen wordt. Als deze plaats reeds zichtbaar is op het scherm dan gebeurd er logischerwijze niets.

Als de verwijzing een URL is, dan wordt de betreffende webpagina geopend.

De 'terugbalk'



Door op deze balk te klikken keert u terug naar bovenaan de **bladzijde** waar u vandaan bent gekomen. Het kan dus zijn dat de **plaats** waar u vandaan bent gekomen net niet op het scherm staat.

Er wordt een geschiedenis van een aantal stappen opgeslagen in een buffer. Door meerder keren op de terugbalk te klikken kunt u dus evenzovele stappen terug. Als de buffer leeg raakt dan gebeurt er niets meer.

De tabbladen

De tabbladen (rechts op de pagina) verwijzen naar de hoofdstukken en andere onderdelen van deze beschrijving.

Versie: S20150223

Hfdstk 1 VPN wetenswaardigheden

1 WAAROM EEN VPN GEBRUIKEN?

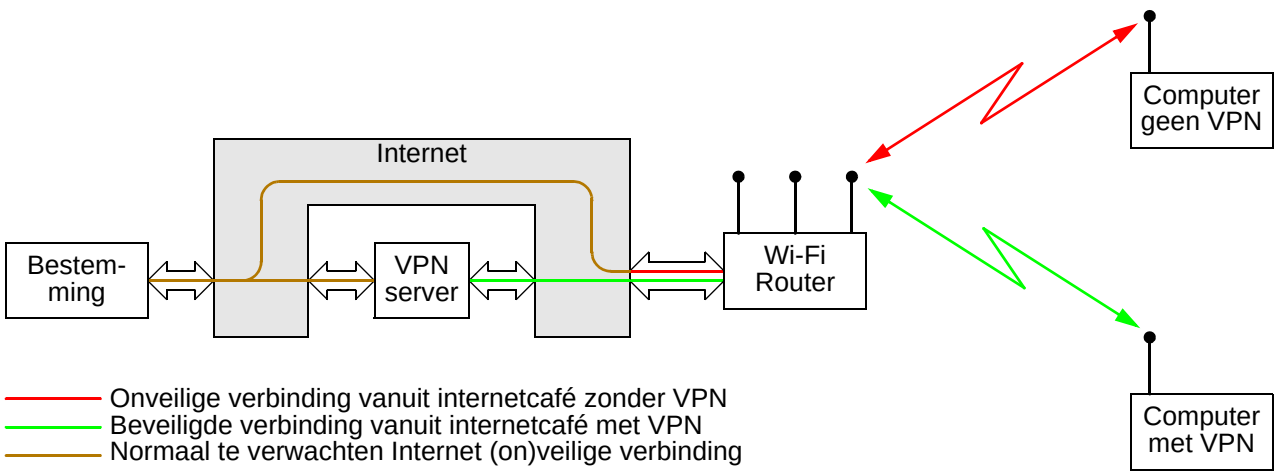
1.1 Wat is een VPN?

Een VPN[1)] is een manier om binnen een openbaar netwerk een privé netwerk te creëren.

Een voorbeeld van een onveilig openbaar netwerk is een netwerk – bijvoorbeeld in een internetcafé – waar iedereen met hetzelfde Wi-Fi[2)] wachtwoord toegang heeft. Dit geeft in principe alle deelnemers toegang tot alle apparatuur op dat netwerk. Met name gedeelde mappen zijn – afhankelijk van de beveiligingsinstellingen – voor iedereen toegankelijk. Bovendien kan alle dataverkeer op dat netwerk met daarvoor geschikte programma's afgetapt worden.

Tip: Maak bij voorkeur op een mobiele computer geen gedeelde mappen aan. Als u tussen uw mobiele computer en thuiscomputer bestanden wilt uitwisselen, deel dan mappen op de thuiscomputer met de mobiele computer en niet omgekeerd.

Figuur 1-1 Voorbeeld van de situatie in een internetcafé



Een VPN creëert als het ware een beveiligde 'tunnel' met tweerichtingsverkeer door dit onveilige netwerk. Deze is alleen voor geautoriseerde gebruiker(s) toegankelijk (zie Figuur 1-1 voor de situatie mèt en zonder VPN). De beveiliging gebeurt door het dataverkeer binnen het VPN in twee richtingen te versleutelen (encryptie). De gebruiker opent de 'tunnel' door in te loggen met de

1) VPN staat voor 'Virtual Private Network' (nederlands: Virtueel Privé Netwerk).
2) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/Wi-Fi.

Versie: S20150223

eigen VPN gebruikersnaam en wachtwoord. Veelal vindt autorisatie met behulp van een certificaat[1] plaats. Andere bezoekers van het internetcafé worden effectief buitengesloten.

1.2 Hoe beveiligt een VPN tegen ‘meekijken’?

Een VPN creëert een beveiligde verbinding tussen twee computers (de computer van een gebruiker en de VPN server computer). Het dataverkeer wordt versleuteld op de computer van de gebruiker, via de onveilige internetverbinding (nu onleesbaar) verzonden en vervolgens gedecodeerd op de VPN server. De VPN server stuurt het dan onversleutelde dataverkeer naar de uiteindelijke bestemming. In de omgekeerde richting gebeurt het versleutelen op de VPN server en het decoderen op de ontvangende computer.

Tussen de computer van de gebruiker en de VPN server kan niemand de gegevens lezen of weten waar de gegevens uiteindelijk naar toe gaan, vandaan kwamen of wat voor soort dataverkeer plaats vindt.

Hoe kom ik aan een VPN?

Er zijn tientallen VPN providers die een VPN dienst aanbieden, zowel gratis als betaald. Door een account aan te maken bij zo’n VPN provider kunt u van de aangeboden dienst(en) gebruik maken.

Wordt al het dataverkeer over het internet beveiligd?

Dat hangt ervan af.

Zo heb ik een ‘laptop van de baas’ die via VPN toegang verschaft tot het bedrijfsnetwerk voor b.v. e-mail en RDP[2] werken op lokatie of bij een klant (zie paragraaf 1.4 – ‘Bedrijfstoepassingen’). Het bedrijf heeft er geen belang bij om hun VPN server te laten belasten met privé datastromen voor surfen of muziek/video streamen. De webbrowser loopt in dit geval dan ook buiten de VPN tunnel om.

In principe is voor een VPN verbinding in te stellen wat niet en wat wel via de VPN tunnel loopt. De VPN provider stelt de aangeboden diensten in. Het is heel lastig om er achter te komen wat wel beveiligd wordt en wat mogelijk niet. Websites van VPN providers blinken meestal niet uit in het zwart op wit specificeren van wat ze voor je doen.

Let Op: Denk niet dat alles meteen beveiligd verstuurd wordt als VPN gebruikt wordt. Controleer wat een VPN provider

1) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/Certificaat_(PKI).
2) Remote Desktop Protocol (NL: extern bureaublad of bureaublad op afstand), Wikipedia: http://nl.wikipedia.org/wiki/Remote_Desktop.

belooft te beveiligen en denk ook mèt VPN na over wat je via Wi-Fi doet!

Normaal gesproken heeft een VPN provider er wel baat bij om zoveel mogelijk via de VPN tunnel te leiden. Hij verdient aan dataverbruik, maar er zijn uitzonderingen (zie bijvoorbeeld hoofdstuk 2 – paragraaf 2.3 – 'SecurityKiss').

Tip: VPN providers beveiligen wel altijd het webbrowser dataverkeer. Wilt u maximale veiligheid? Gebruik dan bij voorkeur op een openbaar netwerk alleen de webbrowser en webmail in plaats van een mail client zoals bijvoorbeeld Outlook of Live Mail.

1.3 Wat kan een VPN nog meer doen?

In het bovenstaande voorbeeld is uitgegaan van een beruchte onveilige situatie, waarin het hoe dan ook verstandig is een VPN te gebruiken. Maar een VPN kan nog meer doen. Ook vanuit huis uit een VPN tunnel gebruiken kan voordelen bieden.

1.3.1 Het IP-adres van de gebruiker verbergen – anoniem surfen

Wat zien websites?

Klik hier

Zonder VPN weet elke website die bezocht wordt het IP-adres[1)] van de router[2)] van de bezoeker. Dit is het adres dat de provider aan de internetkant aan de router toekent, vergelijkbaar met een huisadres. Naar dit retouradres levert de website de gevraagde webpagina's en andere data terug. Via dit IP-adres kunnen veel gegevens van de gebruiker achterhaald worden.

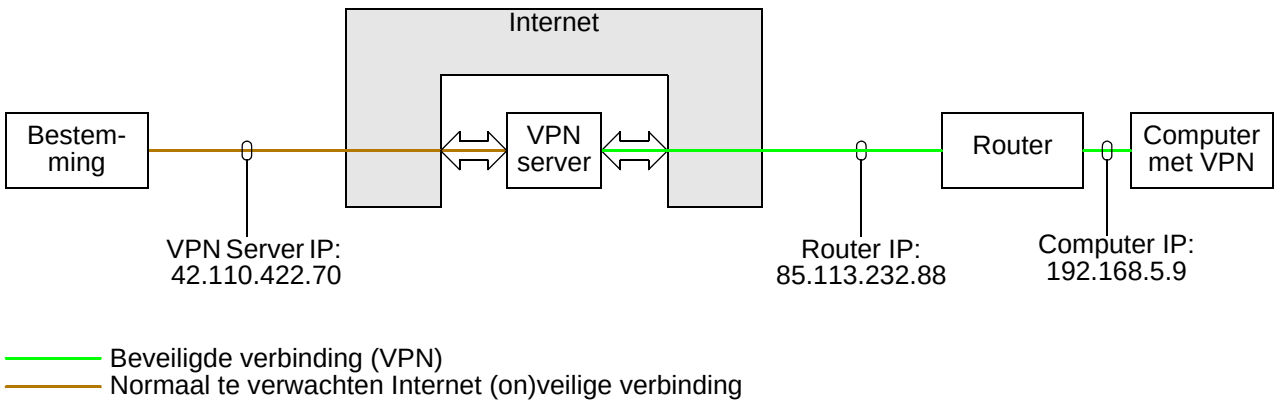
Hiermee kan een bedrijf als Google of Facebook met behulp van 'datamining[3)]' een aan de gebruiker gekoppeld profiel opbouwen en heel veel over een gebruiker te weten komen. Via eerder thuis op de computer geplaatste cookies kan deze ook weer geïdentificeerd worden als deze tijdelijk met een ander netwerk is verbonden (en omgekeerd!).
Met behulp van de betreffende Internet provider kunnen (in ieder geval door opsporingsautoriteiten) ook naam en adres van de gebruiker achterhaald worden.
Erger is dat hackers gemakkelijker gericht aanvallen kunnen lanceren naar een IP-adres, als dat bekend is. Wordt een 'verkeerde' website[4)] bezocht, dan kan een gebruiker zich hieraan blootstellen.

1) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/IP-adres.
2) Voor het begrip 'router' zie Wikipedia (NL): http://nl.wikipedia.org/wiki/Router.
3) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/Datamining.
4) Met 'verkeerde' website wordt bijvoorbeeld een website bedoeld die door hackers gekraakt is en van kwaadaardige software voorzien is.

Een VPN server kan het IP-adres van de gebruiker anonimiseren. Via VPN kan anoniem gesurfd worden (zie Figuur 1-2).

Op de VPN verbinding wordt tussen de router van de gebruiker en de VPN server gewerkt met het IP-adres van de router. De VPN server geeft dat IP-adres niet door. De door u gebruikte bestemming ziet alleen het IP-adres van de VPN server. De VPN server stuurt ontvangen data weer versleuteld naar het IP-adres van de router door; de router stuurt dit door naar het lokale IP-adres dat hij aan de computer van de gebruiker heeft toegekend.
Via VPN kan anoniem van diensten als bijvoorbeeld Google en Facebook gebruik gemaakt worden.

Figuur 1-2 Anoniem surfen



1.3.2 Toegang bieden tot geografisch begrensde websites

Er zijn websites die geografisch beperk zijn, bijvoorbeeld tot één land of een beperkt aantal landen. Zo is bijvoorbeeld de BBC iPlayer website beperkt tot het Verenigd Koninkrijk. VPN service providers kunnen in meerdere landen VPN servers aanbieden. Met een account bij een provider met keuzemogelijkheid voor een in één van de betreffende landen geplaatste VPN server, kan toegang tot zo'n website verkregen worden vanuit een geblokkeerd land. Volgens het IP-adres (van deze server) lijkt de gebruiker immers in een niet geblokkeerd land te zijn.

Het omgekeerde kan natuurlijk ook gebeuren. Zit de gebruiker op een VPN server buiten Nederland, dan zijn tot Nederland begrensde websites ontoegankelijk als VPN geactiveerd is.

Versie: S20150223

1.3.3 Toegang bieden tot geblokkeerde diensten

Beheerders van openbare Wi-Fi netwerken kunnen bepaalde diensten die voortdurend veel datatransport vergen – bijvoorbeeld VoIP[1)] of Skype[2)] – blokkeren om zo een te zware belasting (traagheid) van hun netwerk te voorkomen. Door de encryptie binnen de VPN tunnel kan niet langer gedetecteerd worden welke diensten hier doorheen gebruikt worden. Zo kan de betreffende dienst mogelijk via VPN toch gebruikt worden.

Er zijn landen met minder democratische regimes waar de autoriteiten pogen hun burgers de toegang tot bepaalde diensten te ontzeggen. China en sommige landen in het Midden-Oosten blokkeren met name de toegang tot sociale netwerken, zoals bijvoorbeeld Facebook en Twitter.
Met een VPN tunnel naar een server buiten zo'n land kan mogelijk vanuit zo'n land toegang verkregen worden tot websites/diensten die anders geblokkeerd zijn. In zo'n land is dit mogelijk strafbaar.

Websites/diensten kunnen gebruikers wegens misbruik afsluiten. Vanwege de anonimiteit van een VPN tunnel kan zo'n gebruiker via VPN mogelijk toch weer toegang krijgen tot die website en onder een aangenomen identiteit een account aanmaken.

VPN providers zullen er het mogelijke aan (blijven) doen om blokkade van de verbindingen van/naar hun VPN servers te omzeilen door geavanceerde technieken hiervoor in te zetten. Welke VPN provider dit het beste doet en of het blijft lukken? Ook hier geldt: „In het verleden behaalde resultaten geven geen garantie voor de toekomst".

1.4 Bedrijfstoepassingen

Een bedrijf dat commerciële belangen wil beschermen en hacken en aantasten van het functioneren van het bedrijfsnetwerk wil voorkomen zal eigen VPN servers op lokatie inzetten.

Met eigen VPN verbindingen kunnen de verbindingen van het bedrijfsnetwerk tussen geografisch verschillende locaties toch volledig beschermd via het onveilige internet lopen. De VPN tunnel loopt zonder onderbreking van lokatie tot lokatie; iets wat met een externe VPN server niet helemaal het geval is.

Thuiswerkers kunnen eveneens via een tunnel werken die zonder onderbreking van huis tot bedrijf beschermd is, of deze nu gedeeltelijk over een openbaar Wi-Fi netwerk loopt of niet.

1) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/IP-telefonie.
2) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/Skype.

1.5 VPN protocollen

VPN werkt met een bepaald protocol. Dit kan PPTP[1] zijn of OpenVPN[2]. VPN providers kunnen één of beide aanbieden.

1.5.1 PPTP (Point to Point Tunneling Protocol)

Dit is een standaard ontwikkeld door Microsoft die zich ontwikkeld heeft tot wereldstandaard. Het is aanwezig op zeer veel apparaten. In principe is het dan niet nodig om een VPN applicatie te installeren om VPN te gebruiken met PPTP. Echter, voor het aanpassen van de benodigde instellingen is veel informatie nodig. Het installeren van een applicatie van de gekozen VPN provider neemt u dit werk uit handen.

Tip: De VPN provider Your-Freedom[3] geeft (in het engels) veel achtergrondinformatie en gebruiksaanwijzingen; onder andere ook hoe PPTP (naar hen toe) handmatig is in te stellen.

PPTP is echter in zekere zin verouderd. De encryptie is al gekraakt. Het is alleen nog wel redelijk veilig als een zeer sterk wachtwoord gebruikt wordt (bestaande uit veel tekens). Met een wachtwoordkluisprogramma als bijvoorbeeld KeePass kan dit toch gebruikersvriendelijk.

1.5.2 OpenVPN

OpenVPN is, zoals de naam al suggereert, een ‘Open Source’ protocol. Het is moderner en veiliger dan PPTP. Tot 1024 bits sterke encryptie wordt aangeboden. Er zijn echter veel providers die vanwege de snelheid minder sterke 256 of 128 bits encryptie gebruiken (voor de datastroom; certificaten worden doorgaans wel met 1024 bits versleuteld). Voor de meeste privé toepassingen zal 128 bits encryptie wel voldoende zijn.

Tip: De VPN provider SecurityKiss[4] geeft veel achtergrondinformatie over het toepassen van OpenVPN (veel in het nederlands, sommige onderwerpen in het engels).

1) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol.
2) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/OpenVPN.
3) Your-Freedom (EN): https://www.your-freedom.net.
4) SecurityKiss (NL; deels EN voor achtergrondinformatie): http://www.securitykiss.com/.

2 WAT IS ER NODIG VOOR EEN VPN?

Om VPN te kunnen gebruiken is allereerst een account nodig bij een VPN service provider.

Vervolgens kan/moet doorgaans de applicatie die de VPN provider aanbiedt geïnstalleerd worden. Als deze wordt opstart en u inlogt, dan gaat het internetverkeer via het VPN. Vaak kan dit uitgeschakeld worden; dan gaat het internetverkeer weer (onversleuteld) direct via het internet. Dit kan handig zijn om dataverbruik te besparen tijdens internetactiviteiten waarbij u veiligheid van minder belang acht.
Er zijn tientallen VPN service providers, met zowel gratis als betaalde accounts.

- Gratis heeft gebruiksbeperkingen en/of reclameboodschappen; een datalimiet, tijdslimiet of snelheidslimiet is er vrijwel altijd. Gratis (‘free’) is handig voor incidenteel gebruik.
- Betaald kan prepaid (handig voor incidenteel VPN’nen, bijvoorbeeld op vakantie) of als abonnement (voor regelmatig gebruik). Betalen of tegoed opwaarderen kan met Paypal[1)], creditcard of zelfs met Bitcoins[2)].

Ook zijn er verschillen met betrekking tot de ondersteuning van verschillende platforms. Eén Windows computer tegelijk wordt altijd wel ondersteund in de gratis versie. Ook meerdere computers en computers met andere operating systemen, tablets en smart phones en combinaties hiervan kunnen ondersteund worden, maar dan veelal wel betaald. Ook kunnen providers aanvullende diensten aanbieden, zoals een virusscanner en detectie van aanvallen door hackers.

Uitzoeken welke VPN service provider het beste bij u past is nog een hele klus. Eerst uitzoeken wat de voorwaarden en beperkingen van de ‘free’ versie en betaalde versies zijn vergt vaak aardig wat volharding. Wel bieden ze veelal gratis de mogelijkheid van een beperkt starttegoed aan data, een beperkt maandelijks datategoed of een beperkt aantal uren per dag. Het is dus vaak wel mogelijk een VPN provider gratis uit te proberen en later te gaan betalen. Soms is het ook mogelijk een provider gratis onbeperkt lang te blijven gebruiken, maar dan wel met andere beperking(en), zoals bijvoorbeeld (gebrek aan) snelheid.
En als het niet bevalt (of de limiet bereikt is), gewoon òp naar de volgende. In principe kunt u bij meerdere providers een gratis account aanmaken en de eventueel bijbehorende applicatie installeren (maar dan bij voorkeur wel altijd maar één applicatie tegelijk opstarten).

1) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/PayPal.
2) Zie Wikipedia (NL): http://nl.wikipedia.org/wiki/Bitcoin.

Hfdstk 2 Zomaar een aantal VPN providers

1 INLEIDING

De titel geeft het al aan; het hier noemen van een provider houdt geen enkel oordeel in. Dit is alleen maar een (hopelijk) handige – maar zeker geen volledige – 'startpagina'. Veruit het beste is om zelf op zoek te gaan om de beste keus voor uw situatie te bepalen. Googelen (met bijvoorbeeld trefwoorden 'VPN' **en** 'tunnel' **en** 'free') levert er nog veel meer op.
De opgenomen specificaties zijn alleen maar een indicatie voor een eerste indruk/overzicht en allesbehalve compleet. Zoeken op de aangegeven website levert meer op.

Let Op: Het kan zijn dat bij een provider niet alle dataverkeer via internet beveiligd wordt. Dit is niet altijd duidelijk op de website te vinden.

Net als bij virusscanners is het niet raadzaam om de VPN applicaties van meerdere providers tegelijk te laten 'draaien' op uw computer; mogelijk kunnen ze elkaar hinderen – met traagheid of slecht functioneren tot gevolg.

Om verschillende providers uit te kunnen proberen, om op dataverbruik te besparen of om afwisselend verschillende providers te gebruiken om uw datalimiet 'op te rekken' is het nodig om de VPN applicatie handmatig te kunnen starten en ook weer te kunnen stoppen. Maar met name het stoppen van een gestarte VPN applicatie is niet bij elke provider zomaar mogelijk. En als een VPN applicatie automatisch opstart bij inschakelen van de computer en inloggen, helpt opnieuw opstarten ook niet om de applicatie 'kwijt te raken'.

De oplossing is het toepassen van een programma om automatisch opstarten te beheren. Een voorbeeld van een programma hiervoor is WhatInStartup (zie hoofdstuk 3 – paragraaf 1.1 – 'WhatInStartup'). Hiermee kan automatisch opstarten van een programma uitgeschakeld worden. Dan helpt de computer opnieuw opstarten wel om een applicatie 'kwijt te raken'. Een andere mogelijkheid is om de applicatie via Windows taakbeheer (task manager) te stoppen.

Let Op: Dat het uitschakelen van de VPN tunnel, zoals b.v. bij SurfEasy heel gemakkelijk is, wil niet zeggen dat de betreffende VPN applicatie gestopt is. Bij SurfEasy kan deze alleen gestopt worden met Windows taakbeheer (task manager) of door middel van het herstarten van de computer (mits automatisch opstarten is uitgeschakeld).

2 VPN PROVIDERS

2.1 Niet verder opgenomen om diverse redenen

- Avast SecureLine: alleen beschikbaar voor gebruikers van het Avast anti-viruspakket. Daarom niet uitgeprobeerd.
- Cloak VPN: Rammelende website (FAQ pagina link werkt niet) met zeer weinig informatie; Niet gratis uit te proberen.
- Cyberghost: Met gratis versie nauwelijks vrije serververbinding te krijgen (´s avonds) en hinderlijke 'upgrade' pop-ups.
- Free Website VPN. Geheel gratis. Biedt geen applicatie aan; instellen via het configuratiescherm met behulp van hun handleiding. Het is mij niet gelukt om contact te krijgen met hun server met de in hun handleiding opgenomen gegevens.

2.2 Private Tunnel

OpenVPN (EN) (http://openvpn.net/).
Verwijst naar "Private Tunnel" downloadpagina:
https://www.privatetunnel.com/.
Uitgeprobeerd. Gemakkelijk installeren en gebruiken, maar bij gratis uitprobeerversie: „op-is-op". Interessant als 'prepaid' gewenst wordt.

- VPN tunnel is eenvoudig aan/uit te schakelen. Programma is eenvoudig af te sluiten. Automatisch opstarten kan in-/uitgeschakeld worden met WhatInStartup.
- Prepaid; betaald per hoeveelheid datatransport; tegoed onbeperkt houdbaar.
- Gratis éénmalig starttegoed van 100 MB om uit te proberen.
- Daarna databundels prepaid kopen (in US$) per 50 GB, 100 GB of 500 GB.

Kosten: https://www.privatetunnel.com/index.php/price.html.

2.3 SecurityKiss

SecurityKiss (NL/EN) (http://www.securitykiss.com/).
Uitgeprobeerd. Gemakkelijk installeren en gebruiken.

- Nederlandstalig met technische beschrijvingen soms in het engels.
- OpenVPN protocol met 128 bits Blowfish encryptie en L2TP.
- Gratis met beperking tot 300 MB per dag.

- Protocollen SSH[1], **FTP, RDP, Telnet niet ondersteund in de gratis versie** (dus dan is eigenlijk alleen het webbrowser data verkeer beveiligd)!
- Abonnementen (vooruitbetaald met automatische stop; betalen in €): 20 GB of 30 GB of 50 GB per maand of onbeperkte datahoeveelheid.

Kosten: http://www.securitykiss.com/pricing/.

2.4 SurfEasy

SurfEasy (EN) (http://www.surfeasy.com/).
Uitgeprobeerd. Gemakkelijk installeren en gebruiken; zie ook PC-Active, editie 280.

- Eenmaal opgestart is de VPN tunnel eenvoudig aan/uit te schakelen, maar programma afsluiten kan alleen via taakbeheer of opnieuw opstarten. Automatisch opstarten kan in-/uitgeschakeld worden met WhatInStartup.
- Gratis 500 MB per maand voor 5 apparaten.
- Twee verschillende abonnementen voor onbeperkt datagebruik. Een abonnement voor één mobiel apparaat en een duurder abonnement voor 5 apparaten.
- Betalen in US$ per creditcard of Paypal.

Kosten en aanmelden: https://www.surfeasy.com/register/#register.

2.5 TunnelBear

TunnelBear (EN) (https://www.tunnelbear.com).
Uitgeprobeerd. Gemakkelijk installeren en gebruiken.

- De VPN tunnel is eenvoudig aan/uit te schakelen. Het programma kan eenvoudig afgesloten worden.
- Gratis 500 MB per maand (voor één apparaat?).
- Maand en jaarabonnement onbeperkt dataverbruik voor 3 apparaten).
- Ondersteunt o.a. IRC[2], chatten, FTP, Skype, SSH (on port 22).
- Minpunt: **Automatisch opstarten is niet uit te schakelen met WhatInStartup**.

Kosten: https://www.tunnelbear.com/pricing/.

1) Secure SHell; Wikipedia: http://nl.wikipedia.org/wiki/Secure_Shell.
2) Internet Relay Chat; Wikipedia: http://nl.wikipedia.org/wiki/Internet_Relay_Chat.

2.6 Your-Freedom

Your-Freedom (EN) (https://www.your-freedom.net).
(Nog) niet uitgeprobeerd wegens te veel begrenzingen in de gratis versie. Mogelijk interessant als een abonnement gewenst wordt.

- OpenVPN en PPTP protocols.
- Gratis gebruik:
  - Snelheidslimiet: maximaal 64 kb/s (toch nog iets sneller dan historisch erfgoed 'De Telefoonmodem').
  - Tijdslimiet: maximaal 1 uur continu, maximaal 2 uur per etmaal, maximaal 5 uur per week.
- Abonnementen (vooruitbetaald met automatische stop; betalen in €: 256 kbits/s of 4 Mbits/s of ongelimiteerd. Geen tijdslimiet of datalimiet.

Kosten en **lijst van beveiligde datastromen** (waar RDP niet bij staat): https://www.your-freedom.net/index.php?id=account.

Hfdstk 3 Hulpprogramma's en diversen

1 AUTOMATISCH OPSTARTEN BEHEREN

Er zijn twee gebruikelijke manieren waarop programma's bij het opstarten van de computer en inloggen automatisch opgestart kunnen worden:

- Via de map Opstarten (Startup) in het Windows startmenu. (Hier kunt u een programma zelf verwijderen).
- Via het Windows register (registry). (Zelf verwijderen van programma's alleen door experts of met behulp van een hulpprogramma).

Bij installatie kun je bij veel programma's aangeven of ze automatisch opgestart moeten worden.

Met het programma WhatInStartup.exe kan achteraf alsnog automatisch opstarten uitgeschakeld (en zo nodig later weer ingeschakeld) worden. Het maakt niet uit of dit via het register of het startmenu gebeurt.

Tip: Als u WhatInStartup gebruikt is het handig om bij installatie van elk programma automatisch opstarten in te stellen. U kunt dan later uit- en inschakelen naar wens.

Tip: Het beheren van automatisch opstarten lukt niet voor elk programma. Zo heeft de VPN provider TunnelBear kans gezien om onzichtbaar te blijven in WhatInStartup. TunnelBear start dus altijd automatisch op, maar heeft wel een mogelijkheid (Exit) om handmatig te stoppen.

1.1 WhatInStartup

WhatInStartup is een programma om automatisch opstarten van programma's bij het opstarten van de computer te beheren. Het is een Freeware 'portable' programma, dat niet geïnstalleerd hoeft te worden en dus ook vanaf een USB-stick gebruikt kan worden.

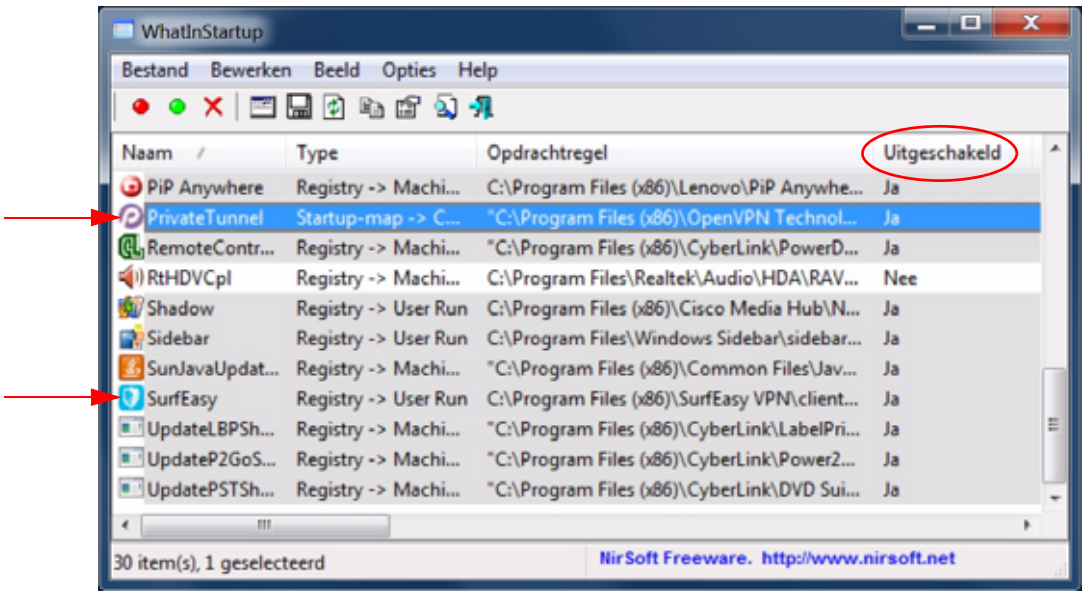
Er is een versie voor 64 bits Windows en 32 bits Windows. Bij twijfel de 32 bits versie kiezen, die draait altijd. En bij een klein programma dat incidenteel gebruikt wordt geeft 64 bits nauwelijks meerwaarde.

Het engelstalige WhatInStartup programma en het nederlandse taalbestand zijn (elk afzonderlijk) te downloaden vanaf: http://www.nirsoft.net/utils/what_run_in_startup.html.

Ga dan als volgt te werk:

1. Unzip beide zipbestanden en zet alles in één map bij elkaar.
2. Na het starten van WhatInStartup.exe verschijnt het hoofdscherm van Figuur 3-1.
3. Selecteer het betreffende programma om automatisch opstarten in of uit te schakelen (of selecteer meerdere programma's).
4. Kies uit het Bestandsmenu (zie Figuur 3-2) 'Geselecteerde items uitschakelen'.
5. Bij opnieuw opstarten van de computer zullen de 'Uitgeschakelde' programma's niet automatisch gestart worden.

Figuur 3-1 WhatInStartup startscherm



Figuur 3-2 whatInStartup bestandsmenu