

# Privacy & Security Essentials

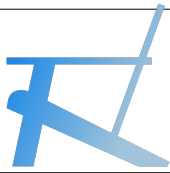
## VPN

—

Virtual Private Network

—

2019 v2



## VPN – IP adres privacy en security issue

Zo'n beetje elk technisch infrastructureel component dat functioneert met enige vorm van software en aangesloten op het internet of netwerk, heeft een IP adres waarmee het zichtbaar en uniek identificeerbaar is voor andere componenten op het internet. Ten tijde van opzet van het www-internet had men geen idee dat er zoveel apparaten zouden worden aangesloten en versie Ipv4 gebaseerd op 32 bits liep vol, en nu hebben we "erbij" Ipv6 gebaseerd op 128 bits.

Die IP adressen zijn te vergelijken met telefoonnummers: een IP-adres op het www-internet is gekoppeld aan een bedrijf, huis, mobiele telefoon, instantie, of apparaat zoals beveiligingscamera of auto boardcomputer etc (IoT). Zo is te achterhalen waar bewerkingen onder een bepaald IP-adres vandaan komen cq informatie naar toe moet worden teruggezonden.

Dus bezig vanuit kantoor, huis of op G3/G4/G5 netwerk: een internet service provider (ISP - zoals KPN, T-Mobile, Ziggo) weten de bron en doel van het internet verkeer. Het internet is hierdoor niet anoniem. Elke ISP houdt een logboek bij van hun dataverkeer tussen de IP-adressen van hun klanten en de IP-adressen die klanten bezoeken.

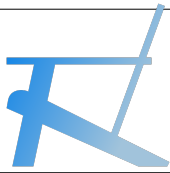
Zo weet de ISP exact met welk (huis-)adres of lokatie, met welk apparaat op welke dag en tijdstip welke www-website of www-server contact is geweest. In veel landen is het gebruikelijk dat deze ISP's hun logboek gegevens verkopen aan adverteerders die daarmee "op maat" reclame aan gebruiker zenden.

Niet alleen de ISP houdt een logboek bij, dat doen ook de meeste www-websites van bezoekers hun gegevens. En daarnaast houden de meeste (niet allen) DNS ook een logboek bij. En "overheid surveillance" houdt ook een logboek bij.

Naast hiervoor genoemde gebrek aan privacy is er ook een security issue. Want, alhoewel de 'data' meestal is encrypt, het IP-adres van de bron-naar-doel en vice versa zijn niet encrypted. Dus net zoals bij DNS kan ook tussen de ISP's en gebruikers door een "man in the middle attack" met behulp van search en replace het beoogde IP-adres worden vervangen door verwijzing naar een malafide website of server.

De kans op "aanvallen" is ook vele malen groter bij gratis wifi netwerk waarop iedereen kan inhaken en zodoende onverlaten binnen dat wifi netwerk andere gebruikers opsporen, en aldus in de gelegenheid zijn tot malafide handelingen.





# VPN – IP adres privacy en security issue

Zoals in vorige slide is uiteengezet weten ISP'ers in de vorm van logboek dus bijzonder veel over gebruikers. Dat “weten of logboek” komt bovenop wat DNS providers bijhouden van gebruikers. Kort samengevat ISP en DNS hebben het profiel van gebruiker en met zijn/haar woonadres, alle websides die zijn bezocht inclusief tijdstip en duur.

Bij profiel denk aan bezochte kranten alle(!) artikelen, bladen, datingsites, webshops, bank(en), leveranciers, vakanties inclusief transport, bestemming, werk, hobbies, etc etc etc. Metadata valt ook te extraheren zoals dag- en nachtritme.

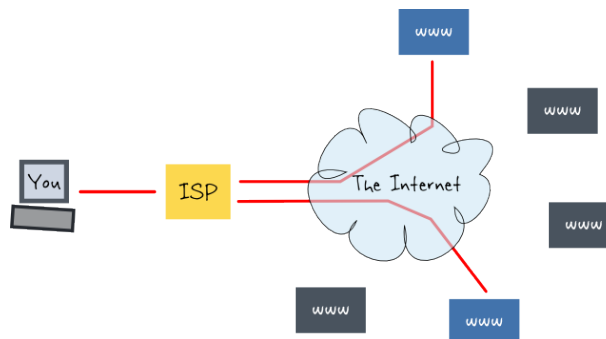
Het www-internet is ontworpen dat een bericht de kortste route neemt van bron-naar-doel. Tegelijkertijd als die kortste route om welke reden dan ook niet beschikbaar is (of te druk bezet), dan zal het bericht een alternatieve route nemen. Voor die routing zijn mondiaal Internet Exchange Point (IEP) opgezet, zoals bijvoorbeeld in NL: AMS-IX en in die regio weer ~12 sub-servers of Co-locations.

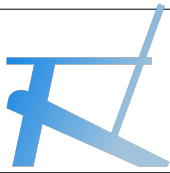
Mondiaal gezien zijn er honderden IEP's met ook weer Co-locations dus er zijn over de hele wereld duizenden IEP's en grotendeels allemaal met logboek en dus: de hele wereld kan privacy & security gegevens van gebruikers inzien.

Vervolgens, elke website kan een logboek hebben waaruit blijkt welk IP adres exact(!) welk artikel heeft bekeken, gekocht en dergelijke. En bijna alle commerciële websites verkopen bezoekers informatie aan geïnteresseerden (zie info Cookies Trackers). Kopers van gebruikers-informatie zijn advertentie makelaars die “op maat” gesneden reclame profielen aanbieden. De website zoekmachine Google kent de gebruiker heel goed inclusief zinneroerselen, ziektes, emoties, plaatjes etc etc etc.

Het issue is dus:

- Het hebben en gebruiken van eigen persoonlijke “door ISP geleverde IP adres” geeft de mogelijkheid door derden een persoonlijk profiel samen te stellen gesorteerd op dat persoonlijke IP adres
- Het hebben van een eigen IP adres is dus zeer gevoelig voor schending van persoonlijke privacy & security





# VPN – zoekmachines privacy en security

Het www-internet bestaat uit 2x onderdelen, namelijk:

- het internet, technisch faciliterende bedrijven / componenten die de technische infrastructuur vormen, en;
- het www, bedrijven, organisaties, personen die inhoud – content leveren

Beiden, dus het www-internet doen aan bijhouden van gegevens op basis van het IP adres

www en het issue van zoekmachines:

- bijna alle zoekmachines houden bij de gegevens van gebruikers op basis van IP adres (uitzondering is bijv. DuckDuckGo)
- plus die zoekmachines houden bij de computer gegevens van gebruikers

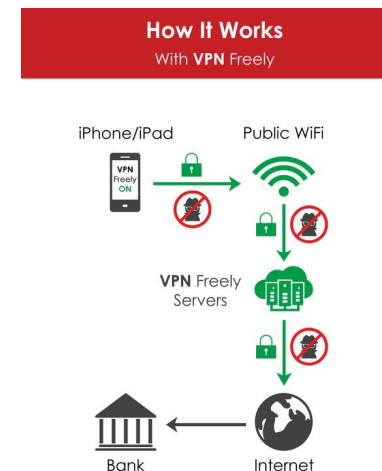
Het bijhouden EN combineren van deze gegevens zijn bedreigend voor privacy en security

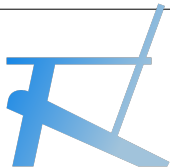
Zoekmachines maatregel:

- door altijd aanzetten van een VPN verdwijnt het IP adres van gebruiker in een grote vergaarbak van heel veel gebruikers
- gebruik alleen zoekmachines waarvan bekend is dat géén IP adres wordt bijgehouden, bijv.: DuckDuckGo

Volgende slides geven voorbeelden:

- volgende slide logboek gemaakt met netwerk monitor App Wireshark tijdens digitaal bezoek aan de Telegraaf
- daarna volgende slide voorbeeld overzicht van Internet Exchange Points
- daarna volgende slide voorbeeld zoekgeschiedenis logboek





# VPN – IP adres logboek

Capturing from tun0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

Name Resolution Preferences... Address: 217.196.36.12 Name: OK Cancel

No.	Time	Source	Destination	Protocol	Length	Info
1	2018-04-27 14:02:12.294239868	www.telegraaf.nl	10.8.0.48	TLSv1.2	83	Encrypted Alert
2	2018-04-27 14:02:12.294338628	10.8.0.48	www.telegraaf.nl	TCP	52	60828 → https(443) [ACK] Seq=...
3	2018-04-27 14:02:12.294530280	www.telegraaf.nl	10.8.0.48	TCP	52	https(443) → 60828 [FIN, ACK]...
4	2018-04-27 14:02:12.294569881	10.8.0.48	www.telegraaf.nl	TCP	52	60828 → https(443) [FIN, ACK]...
5	2018-04-27 14:02:12.294611439	10.8.0.48	www.telegraaf.nl	TCP	52	60828 → https(443) [ACK] Seq=...
6	2018-04-27 14:02:12.308132693	www.telegraaf.nl	10.8.0.48	TCP	52	https(443) → 60828 [ACK] Seq=...

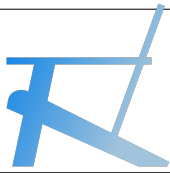
[Coloring Rule Name: TCP]  
[Coloring Rule String: tcp]

Raw packet data

Internet Protocol Version 4, Src: 10.8.0.48 (10.8.0.48), Dst: www.telegraaf.nl (217.196.36.12)

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 00.. = Differentiated Services Codepoint: Default (0)
- .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 52
- Identification: 0x8559 (34137)
- ▼ Flags: 0x02 (Don't Fragment)
- 0... .... = Reserved bit: Not set
- .1.. .... = Don't fragment: Set
- ..0. .... = More fragments: Not set
- Fragment offset: 0
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0xad62 [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.8.0.48 (10.8.0.48)

0000 45 00 00 34 85 59 40 00 40 06 ad 62 0a 08 00 30 E..4.Y@. @..b...0  
0010 d9 c4 24 0c ed 9c 01 bb 4a 2e 35 59 6b 91 b1 e6 ..S..... J.5Yk...  
0020 80 10 03 8d 0f d9 00 00 01 01 08 0a 18 90 fa e7 .....  
0030 73 49 48 36 sIH6



# VPN — list of internet exchange points

Privacy & Security Essentials x W List of Internet exchange points x +

https://en.wikipedia.org/wiki/List\_of\_Internet\_exchange\_points

manent link  
e information  
idata item  
e this page















it/export  
ate a book  
vnload as PDF  
itable version

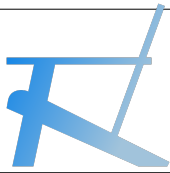
languages  
añol  
năă  
Edit links

- **Region:** The official [Regional Internet registry](#) (RIR) regions.
- **Country:** Uses [ISO 3166-1 alpha-3](#) to display the country flag.
- **City:** A reference to a city article within Wikipedia.
- **Name:** Longname (Shortname). Entries flagged with an asterisk (\*) do not appear in PeeringDB.
- **IX-F region:** IX-F region with which the IXP is associated.<sup>[1]</sup>

## Active internet exchanges [\[ edit \]](#)

The IXPs in the list that follows have a working webpage, are listed in [PeeringDB](#), or both.

Region ↕	Country, City/Region ↕	Name ↕	IX-F region ↕
Africa	 <a href="#">Angola, Luanda</a>	<a href="#">Angola Internet Exchange</a> (Angola-IXP, ANG-IX) <sup>[2]</sup>	Af-IX
Africa	 <a href="#">Angola, Luanda</a>	<a href="#">Angola Internet Exchange</a> (Angonix) <sup>[3]</sup>	Af-IX
Africa	 <a href="#">Benin, Cotonou</a>	<a href="#">Benin Internet Exchange Point</a> (BENIN-IX) <sup>[4]</sup>	Af-IX
Africa	 <a href="#">Botswana, Gaborone</a>	<a href="#">Botswana Internet Exchange</a> (BINX) *	Af-IX
Africa	 <a href="#">Republic of the Congo, Brazzaville</a>	<a href="#">Congo Internet eXchange</a> (CGIX) <sup>[5]</sup>	Af-IX
Africa	 <a href="#">Democratic Republic of the Congo, Kinshasa</a>	<a href="#">Kinshasa Internet Exchange</a> (RDC-IX/KINIX) <sup>[6]</sup>	Af-IX
Africa	 <a href="#">Djibouti, Djibouti</a>	<a href="#">The Djibouti Internet Exchange</a> (DjIX) <sup>[7]</sup>	Af-IX
Africa	 <a href="#">Gambia, Serekunda</a>	<a href="#">Serekunda Internet Exchange Point</a> (SIXP) <sup>[8]</sup>	Af-IX
Africa	 <a href="#">Ghana, Accra</a>	<a href="#">Ghana Internet Exchange</a> (GIX)	Af-IX
Africa	 <a href="#">Ivory Coast, Abidjan</a>	<a href="#">Côte d'Ivoire Internet Exchange Point</a> (CIVIX) <sup>[9]</sup>	Af-IX
Africa	 <a href="#">Kenya, Nairobi</a>	<a href="#">Kenya Internet Exchange</a> (KIXP)	Af-IX
Africa	 <a href="#">Lesotho, Maseru</a>	<a href="#">Lesotho Internet Exchange Point</a> (LIXP) <sup>[10]</sup>	Af-IX
Africa	 <a href="#">Madagascar, Antananarivo</a>	<a href="#">Madagascar Global Internet eXchange</a> (MGIX) <sup>[11]</sup>	Af-IX
Africa	 <a href="#">Malawi, Blantyre</a>	<a href="#">Malawi Internet Exchange</a> (MIX-BT) <sup>[12]</sup>	Af-IX



# VPN – Google search logboek

Chrome Browser - Privacy Policy - Mozilla Firefox

Google Chrome [DOWNLOAD CHROME](#)

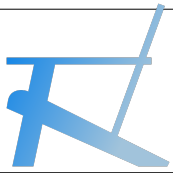
Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts:

`123.45.67.89 - 25/Mar/2003 10:15:32 - http://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969`

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
- `25/Mar/2003 10:15:32` is the date and time of the query;
- `http://www.google.com/search?q=cars` is the requested URL, including the search query;
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used; and
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to the user the next time s/he visits Google from that particular computer).

Menu Privacy Security... Chrome Browse... Donderdag 17 mei, 10:18



# VPN – Privacy & Security Maatregel

## DOEN:

- Vermijd het gebruik van eigen IP adres op alle apparaten die in contact staan met internet
- Wijzig eigen IP adres naar VPN algemene of neutrale locatie EN dat die VPN waarborgt geen logboek wordt bijgehouden

## Dus:

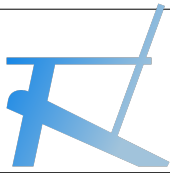
- maak bij een VPN provider een account aan, bij voorkeur waarvoor je moet betalen
- Telkenmale bij aanzetten van “op internet aangesloten” apparaat zet aan de: VPN

## Resultaat van gebruik VPN:

- gebruiker is onherkenbaar gemaskeerd puur door grote aantallen andere gebruikers van zelfde VPN server IP adres







# VPN — protonvpn.com homescreen

www-internet privacy & security techies zijn redelijk unaniem om protonvpn aan te bevelen voor gebruik. Ontstaangeschiedenis van bedrijf ligt in Zwitserland bij CERN alwaar tooling is ontwikkeld om gegarandeerd veilig te mailen (zie info Email) en prive & secure het internet te betreden cq gebruiken. Er wordt op gewezen dat Zwitserland een van de hoogste privacy wetgeving heeft en het land is niet aangesloten bij groep “Fourteen Eyes Government Serveillance”.

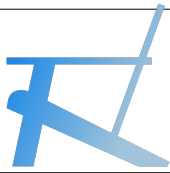
Te doen voor nieuw account:

→ druk rechtsboven op groene button “SIGNUP”

Na aanmaak van account kan gebruiker instellingen wijzigen door:

→ druk rechtsboven op groene letter button “LOGIN”





# VPN — protonvpn step 1 select a plan

Protonvpn kent vier verschillende “plannen” waarbij de 1<sup>e</sup> gratis is, en volgende drie zijn betaald met elk specifieke kenmerken.

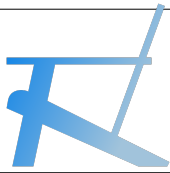
Gebruiker kan beginnen met plan FREE en elk moment daarna via LOGIN “upgrade” naar betaald plan.

Te doen voor aanmaak protonvpn account:

→ druk op kolom FREE

Dan LET OP: scroll naar beneden voor step 2 – verdere ingaven; zie volgende slide

FREE	BASIC	PLUS	VISIONARY
<b>FREE</b>	4 € /month Billed as 48 €/year	8 € /month Billed as 96 €/year	24 € /month Billed as 288 €/year
3 countries	All countries	All countries	All countries
1 devices	2 devices	5 devices	10 devices
Speed: Low (No P2P)	Speed: High	Speed: Highest	Speed: Highest



# VPN — protonvpn step 2 create account

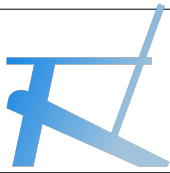
Aanmaak van een protonvpn account kan op twee manieren, te weten:

- 1) via reeds eerder aangemaakt protonmail account (zie schermafdruck groene ovale button), of;
- 2) zonder eerder aangemaakt protonmail account, met gebruik van reeds bestaand emailadres van gmail of dergelijke.

Te doen voor nieuw vpn account zonder protonmail – optie 2 van hierboven:

- geef in uniek voorkomend username (het systeem controleert realtime of gekozen naam nog vrij is)
- geef in eigen gekozen password (en onthouden!!)
- geef in ter bevestiging nogmaals eigen gekozen password
- geef in eigen reeds bestaand emailadres

Dan LET OP: scroll naar beneden voor step 3 verdere ingaven; zie volgende slide



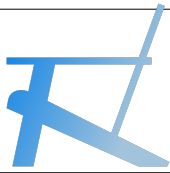
# VPN — protonvpn verificatie create account

In vervolg op vorige slide: gebruiker wordt gevraagd gegevens te verifiëren en tegelijkertijd controleert het systeem om ingegeven nieuwe account niet is gedaan door een geautomatiseerd proces. Dit laatste ter voorkoming dat hun servers dichtslibben door computer ondersteund geautomatiseerde processen – hackers verstoren diensten.

Ter verificatie:

- druk op vlag in groene kader en er verschijnt een pull-down menu en kies Netherlands
- geef eigen 06nummer in (dus zonder +31) en druk op groene button “SEND”
- een sms komt binnen met 6 cijferig verificatienummer en geef dat nummer in
- druk onderaan scherm op groene ovale button “Get ProtonVPN”

Hiermee is het protonvpn account aangemaakt.



# VPN — protonvpn aanzetten en gebruik

Er zijn twee manieren om protonvpn te gebruiken, namelijk:

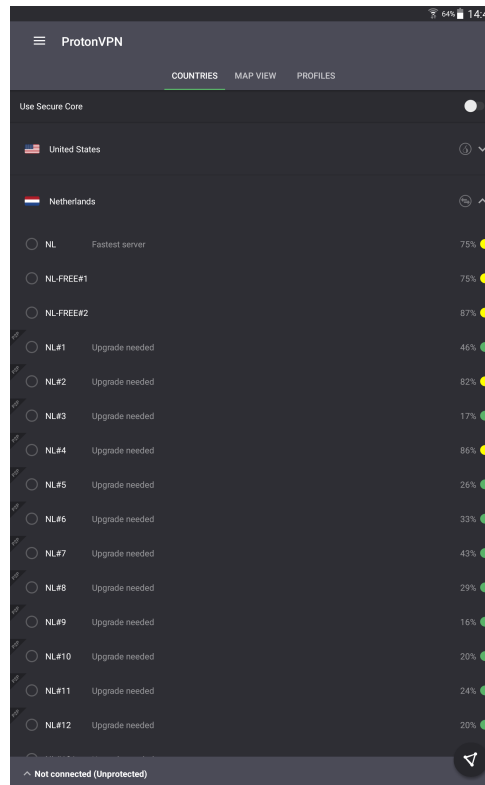
- 1) gebruik op PC, MAC, laptop, notebook, chromebook, of;
- 2) gebruik op mobiel apparaat met behulp van app uit PlayStore of AppStore

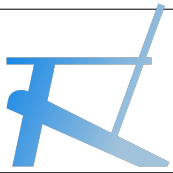
Bij gebruik optie 1:

- ga naar protonvpn website en “login”; ga naar instellingen en volg instructie voor installeren
- ga na installatie op eigen computer “NetwerkCentrum”; druk op “activeren vpn”; en klaar.

Bij gebruik optie 2:

- download app “protonvpn”; geef in 1x malig accountname & password
- kies uit pulldown menu naar “land”; en kies binnen land naar “server” (igv plan FREE dan zijn er 2x servers beschikbaar)



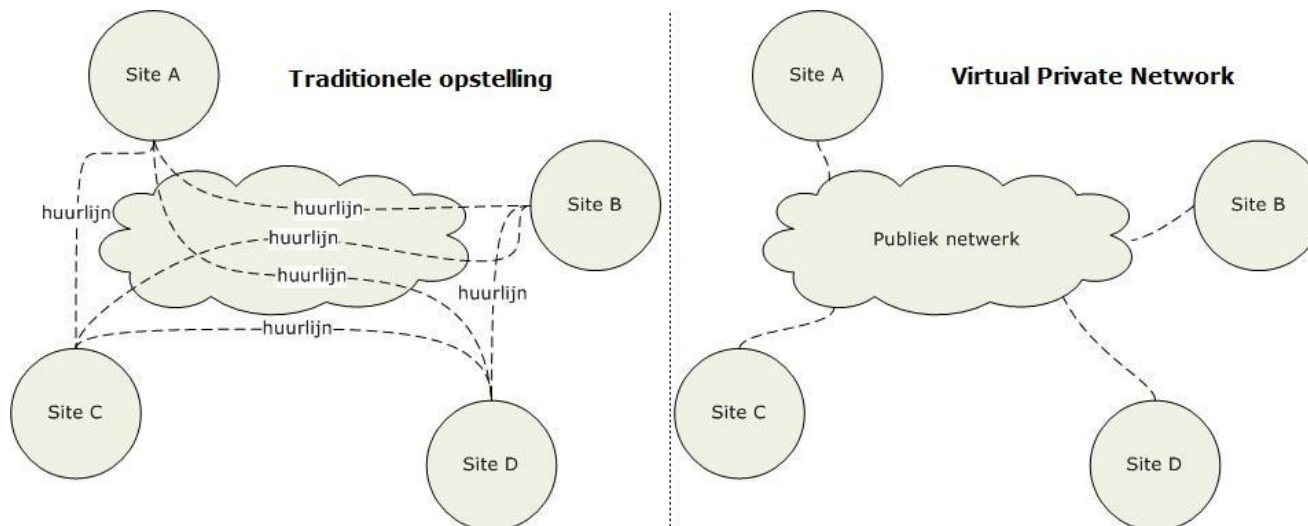


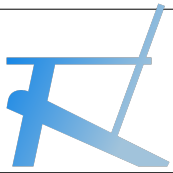
# VPN – werking

Een Virtueel Particulier Netwerk of Virtueel Privénetwerk (Engels: Virtual Private Network, VPN) is een goedkope manier om een Local Area Network (LAN) over een bestaande verbinding, een Wide Area Network (WAN), zoals het internet, uit te bouwen met behoud van vertrouwelijkheid.

Deze dienst maakt gebruik van een reeds bestaand netwerk, doorgaans het internet, om informatiedeling tussen geografisch gescheiden netwerken mogelijk te maken alsof er een dedicated network was. De verzonden data kunnen het best beveiligd worden zodat de integriteit, autorisatie en authenticiteit van de data over dit onderliggende netwerk gewaarborgd blijven. De eindgebruikers zullen in principe niet merken dat er een VPN gebruikt wordt

Door tunneling wordt een pakket voor het eigen cq private netwerk geëncapsuleerd binnen een nieuw pakket om over het publieke netwerk verzonden te worden. Een eerste reden hiervoor is om het originele pakket compatibel te maken met het publieke netwerk. Deze stap kan met de werking van een bridge vergeleken worden. Een andere reden is de beveiliging van het originele pakket. Het originele pakket kan namelijk volledig versleuteld worden, waarna het geëncapsuleerd zal worden binnen een nieuw pakket. Het geëncapsuleerde pakket zal dan verzonden worden via het onderliggende netwerk en na aankomst uitgepakt worden, zodat met het originele pakket verder gewerkt kan worden. Tunneling is een veelgebruikte techniek bij tal van VPN-implementaties.





# VPN – verantwoording

Bronvermelding staat meestal in de screenshots en verder Wikipedia en YouTube

Het www-internet is constant in beweging en feiten en situaties zijn aan wijzigingen onderhevig, daarom:

→ Informatie is van ten tijde van vervaardigen van deze info als vermeld op voorblad – slide 1

## TOOLING

Laptop	Acer – Linux Mint
VPN	protonvpn.com
Browser	Mozilla Firefox
Opmaak	LibreOffice
Website	www.summertime.tech