Index

RISICO'S

back to index

De veiligheidsrisico's

ALLES KAN GEKRAAKT WORDEN.

Hoezeer we ook ons best gaan doen om alle veiligheidsrisico's te vermijden, het zal altijd mogelijk zijn gehacked te worden.
Een voorbeeld daarvan was onlangs nog in het nieuws. Met de Pegasus software konden geheime diensten telefoons infecteren en helemaal besturen zonder dat de gebruiker het in de gaten had.

De bekende valkuilen

- telefoontjes (whaling)
- fake emails (met bijlage)
- phishing : fake websites
- hotspots
- open poorten op computer en andere apparatuur

Hoe moeten we ons beveiligen?

- Gedrag
- Software
- Hardware

GEDRAG

Alertheid en (gezond) wantrouwen

- let op websites (phishing)
- klik niet zomaar op een link
- open geen bijlagen die u niet vertrouwt
- wantrouw bellers (whaling)
- controleer https (slotje) (dat is geen waterdichte garantie)

Accounts

- steeds meer: email, winkels, google, ...
- gebruik verschillende email adressen
- gebruik verschillende sterke wachtwoorden
- geef geen/weinig/verkeerde informatie
- bij kritische zaken: gebruik 2FA (2 Factor Authorisation)

Tijdelijk email

Wachtwoorden

- wachtwoord
- DigiD
- 2FA

Internetbankieren

- ING : mijn ing
- Rabo

Online winkelen

betalen: ideal, creditcard, paypal, afterpay, ...

Software installeren

- free (gratis) : wees voorzichtig !!
- open source is altijd beter

SOFTWARE

Virusscanners e.a. bescherming

- PC-veilig etc
- virusscanner

Browser instellingen

- Instellingen aanpassen
- Addons: https-everyehwre, ghostery, ...

Alternatieve software

- Firefox ipv Edge / Chrome
- Duckduckgo ipv Google
- Openstreetmap ipv Google Maps
- Protonmail of tutanota ipv outlook of gmail

Apps op de smartphone

- betrouwbare bron (Google Play Store)
  maar: apps verzamelen allerlei onnodige data (voorbeelden)
- beperk onnodige permissies
- gebruik firewall: NoRoot Firewall (screenshot)

Online controle tools

- virustotal.com
- checkjelinkje.nl

Geavanceerde maatregelen

- VPN
- Tor-brouwser
- Linux

HARDWARE

De router

- WAP2(3) gebruiken (geen WEP)
- updates installeren (eerst backup maken)
- verander de SSID (de naam)
- verander de login naam en paswoord
- liever geen externe UPnP poorten open (Universal Plug and Play)
- liever geen andere open poorten
- disable inloggen via WAN
- 5GHz heeft korter bereik dan 2.4-GHz, dus veiliger
- maak een Guest-account voor IoT apparaten
- disable WPS (Wifi Protected Setup) (altijd dezelfde pincode!)
- test : shieldsup
- blokkeer onbekende MAC-adressen

De router is het belangrijkste apparaat in huis voor het 'internetten'. Vaak ook voor telefoneren en tv kijken.

Het internet

back to index

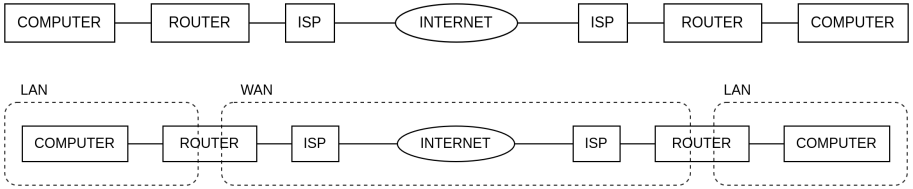
Client, server en protocols

- Client: programma op eigen computer bv. Email, Browser, ...
  - vraagt om informatie op internet
  - kan informatie weergeven en bewerken
- Server: programma op co puter elders bv. Webserver, Email server, ...
  - biedt informatie aan
- Protocol: afspraak over de vorm van communicatie
  - TCP/IP : Transmission Control Protocol over Internet Protocol
    UDP : User Datagram Protocol
    HTTPS : HyperText Transmission Protocol Secure
  - Protocols komen in 'lagen' (layers)

Het netwerk

- ISP = Internet Service Provider

Het netwerk

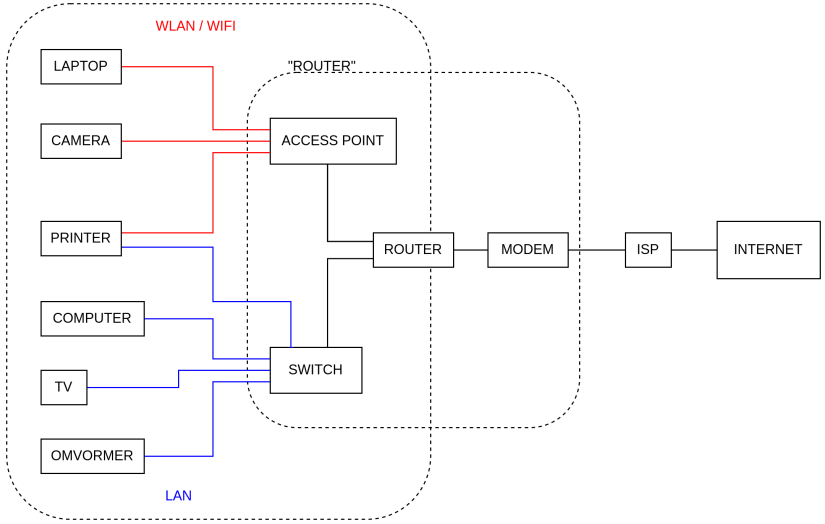


- ISP = Internet Service Provider
- LAN = Local Area Network
- WAN = Wide Area Network
- ISP's verbonden via TIER's

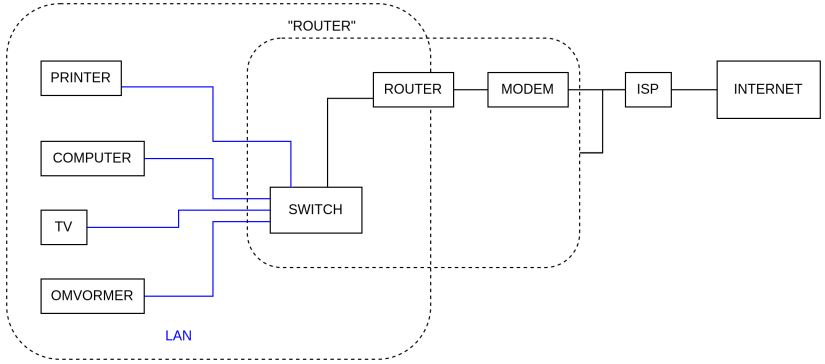
Internet communicatie

- lokaal netwerk →internet →ontvanger ; vice versa
- data wordt verstuurd in 'data-pakketjes'
- data-pakketje bevat: afzender(zender)adres, data, bestemmingsadress
- data-uitwisseling gebeurt volgens vast 'protocol'
  UDP, TCP/IP, etc
- datapakketjes geen kris-kras door het internet
  optimale route bepaald door BGP (Border Gateway Protocol)

Het lokale netwerk

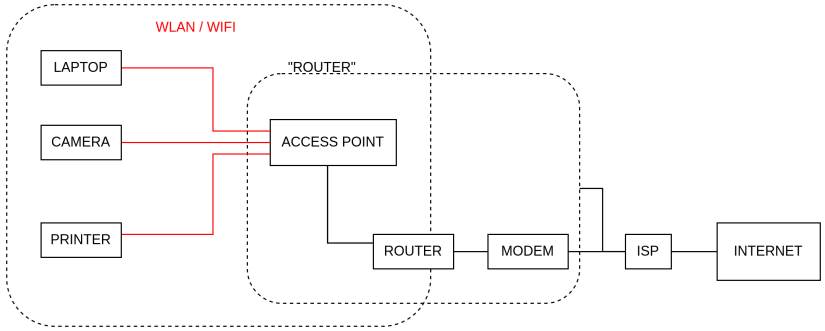


Bekabeld netwerk



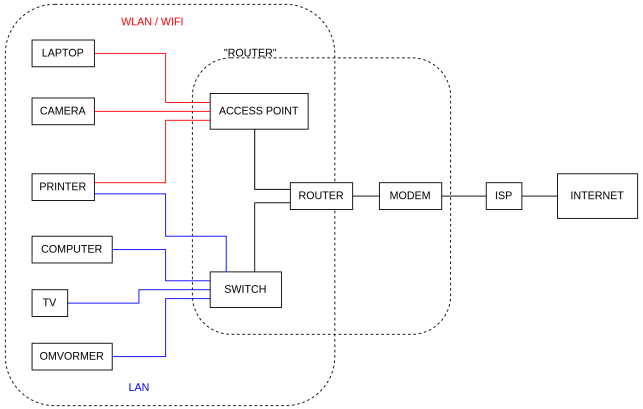
- Ethernet
- UTP-kabel
- veilig en snel

Wifi



- Inloggen met wachtwoord
- WEP, WPA1(2,3)
- onveilig

Adressen

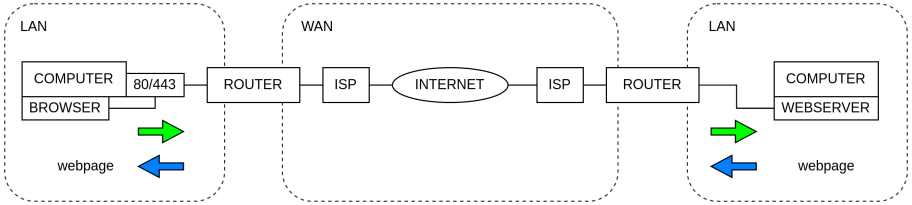


- Router (DHCP server) maakt lokaal netwerk
- LAN-adres van een computer : 192.168.0.41 vb
- WAN=adres van de router : 77.143.87.34
- LAN-adres van de router (meestal) : 192.168.0.1

Het MAC-adres

- MAC = Media Access Control = hardware adres
- MAC-adressen filter in router

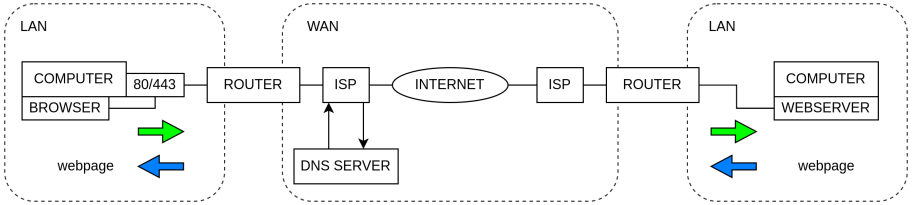
Browser - Webserver



- Communicatie via 'poort' van de computer
- Browser : 80 / 443 ; FTP : 21 ; SSH : 22
- Open poortsen scannen ('port sniffers')

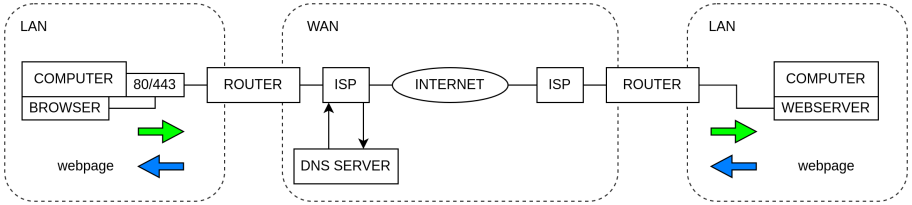
- browser stuurt verzoek om webpagina
- HTTP-websites : geen encryptie $\rightarrow$ onveilig
- HTTPS-websites : wel encryptie $\rightarrow$ veilig

Browser - Webserver



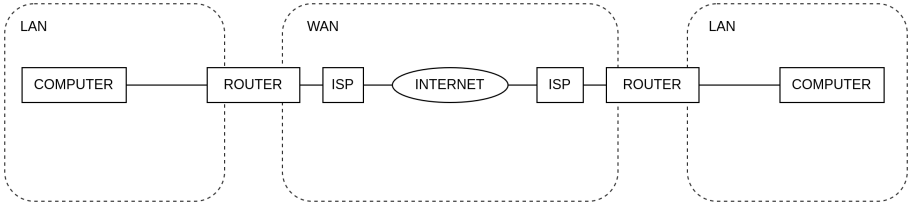
- DNS server

Browser - Webserver

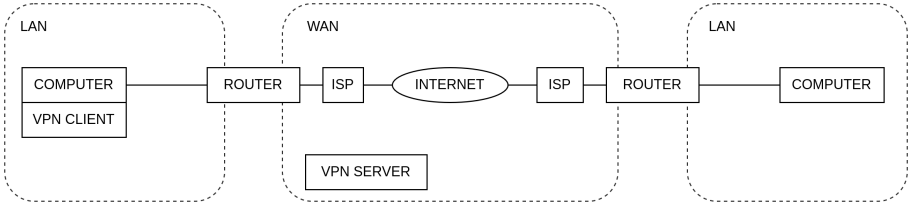


- webserver stuurt webpagina
- ... maar ook : cookies, third-party-cookies, trackers, malware, advertenties
- blokkeer dit in browser instellingen
- gebruik virusscanner of firewall
- gebruik browser addons (ook: adblocker)
- toch identificatie mogelijk door 'browser fingerprinting'

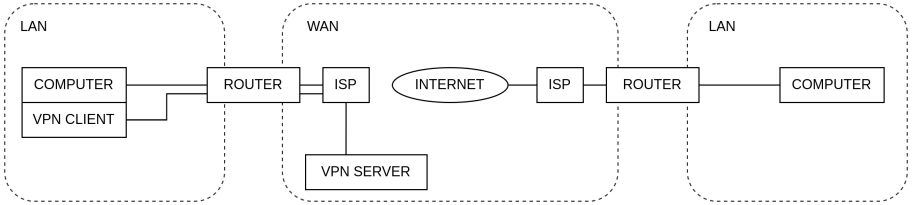
VPN



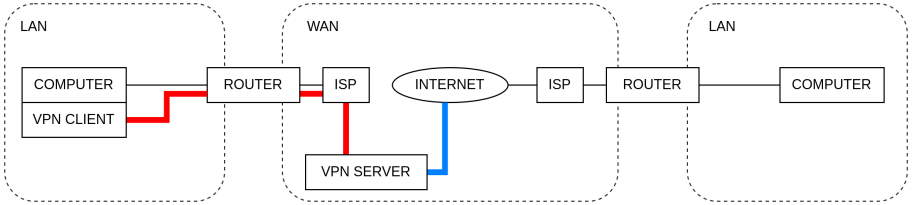
VPN


LAN
WAN
LAN
COMPUTER
VPN CLIENT
ROUTER
ISP
INTERNET
ISP
ROUTER
COMPUTER
VPN SERVER

VPN

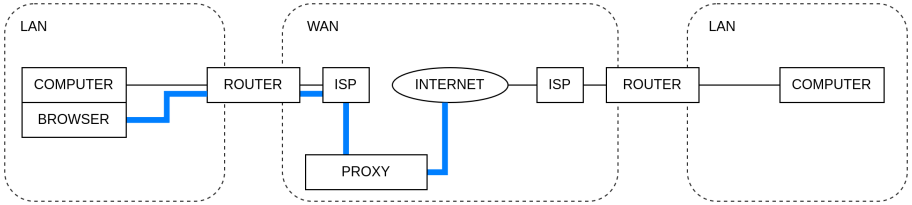

LAN
WAN
LAN
COMPUTER
VPN CLIENT
ROUTER
ISP
INTERNET
ISP
ROUTER
COMPUTER
VPN SERVER

VPN



- na VPN: geen encryptie
- computer based
- browser based
  altijd eerst computer verbinden dan pas browsen
- geen garantie voor privacy (browser fingerprinting, cookies)

PROXY



- computer based : SOCKS proxy
- browser based : HTTP proxy

De Tor-browser

Piet Schreurs (Bieb) 41 / 41