Noud van Kruysbergen, Urs Marsmann

Tunnel via internet

Mobiele apparaten veilig op internet via een VPN

Het gebruik van vreemde netwerken en open wifi's brengt de nodige risico's met zich mee. Met een VPN-tunnel naar je thuisnetwerk, het bedrijfsnetwerk of een commerciële dienst kun je de verbinding echter versleutelen en beveiligen tegen pottenkijkers. Bij sommige routers en NAS-systemen kun je vrij makkelijk een eigen VPN-dienst opzetten – geheel gratis.

Met VPN veilig op internet

Een mobiel apparaat verkeert vaak in veel vreemde netwerken. Zolang je het mobiele netwerk gebruikt (3G of 4G), ben je relatief veilig. Dat netwerk wordt beheerd door een betrouwbare provider wiens imago om zeep kan worden geholpen als hij zich daar niet aan houdt. Die provider houdt de beveiliging van het netwerk normaal gesproken helemaal up-to-date. Gebruik je echter wifi, dan weet je niet hoe het plaatje er beveiligingstechnisch uitziet.

In een onbeveiligd draadloos netwerk kunnen alle verbonden deelnemers de content van alle datapakketten volgen en analyseren. Ook bij een wifi met een wachtwoordbeveiliging kan de verbinding worden afgeluisterd als een aanvaller erin slaagt de eerste vier pakketten, waarbij de sleutel wordt uitgewisseld, te achterhalen en hij het wachtwoord van het wifi weet – alle gasten in een hotel of café gebruiken immers hetzelfde wachtwoord.

Een ramp zijn onbeveiligde wifi's overigens ook weer niet: de echt gevoelige inhoud als de overdracht van wachtwoorden, het gebruik van een bank-app of het ophalen van e-mails is sowieso via SSL versleuteld, maar alleen in de browser of bij mailclients is het gebruik van dergelijke versleutelingsmethoden echt transparant. Bij andere apps voor mobiele apparaten moeten gebruikers erop vertrouwen dat de dienst gevoelige informatie versleutelt – en dan ook nog goed.

Maar ook verbindingen bevatten gevoelige data die niet kan worden versleuteld, bijvoorbeeld de IP-doeladressen van de communicatie. Ook die wil je niet onnodig prijsgeven. Een VPN-tunnel versleutelt dat soort gegevens ook. Aanvallers kunnen dan alleen nog zien hoeveel data er wordt verstuurd en wat het IP-adres van de VPN-gateway is.

Virtuele locatie

Een VPN heeft nog een ander voordeel: ook de tegenpool ziet alleen het openbare IP-adres van de betreffende VPN-gateway en niet dat van de echte locatie. Het VPN is dan meteen een verlengstuk van je eigen interne netwerk met de betreffende locatie van dat moment. Je krijgt daarmee een privé IP-adres uit je thuisnetwerk, waarmee je dus alle apparaten en servers in je eigen netwerk direct kunt benaderen. Port-forwarding op je router instellen is niet nodig.

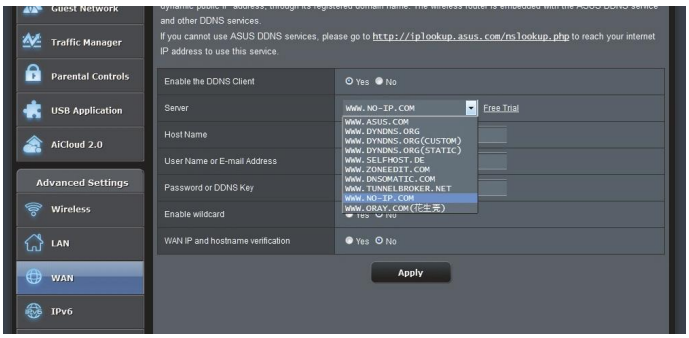
Vaak maken videoportals gebruik van geoblocking, waardoor content van een Nederlandse dienst ook alleen in Nederland te bekijken is – en het Amerikaanse aanbod alleen in de VS. Dat heeft vaak met licenties te maken die alleen voor het betreffende land gelden. Ook binnen de EU is het niet altijd en overal mogelijk om een uitzending van de NPO terug te kijken.

Een VPN-verbinding zorgt in dat geval in beide richtingen voor een oplossing. Enerzijds kun je in het buitenland dan verbinding maken met je eigen internetverbinding en daarmee content opvragen die alleen voor Nederland toegankelijk is (bijvoorbeeld een voetbalwedstrijd uit de Eredivisie via Foxsports), anderzijds kun je als Nederlander een internationaal commerciële VPN-dienst gebruiken en jezelf een IP-adres uit de VS, Australië, Japan of waar dan ook ter wereld bezorgen (zie pagina 138) om op die manier de content te bekijken die aan regionale beperkingen onderworpen is – zover daar althans geen maatregelen tegen worden genomen, zoals Netflix in januari aankondigde. Als een bedrijf een VPN beheert, kunnen medewerkers overal veilig op het bedrijfsnetwerk komen en de interne resources in het intranet gebruiken, zoals databases (zie pagina 137).

Zelfs de Great Firewall in China vormt met een VPN-tunnel geen obstakel meer. Aangezien nieuwspagina's en mailservers uit het westen en messagingdiensten als Facebook Messenger en Whatsapp in Chinese netwerken niet beschikbaar zijn – of hooguit in zeer beperkte mate – is het gebruik van een VPN een must voor iedereen die naar China reist en het niet helemaal zonder zijn normale informatiekanalen wil stellen.

Adres van buitenaf

Bij veel moderne routers kun je vrij snel zelf een VPN configureren en onderweg met je mobiele apparaat via die verbinding internetten, zoals we hier laten zien met de RT-AC66U van Asus. Dan moet wel aan een aantal voorwaarden voldaan zijn: de internetaansluiting van de router moet een eigen openbaar IPv4-adres hebben waarmee hij van buitenaf bereikbaar is. Het komt bij ons eigenlijk niet voor, maar als je router alleen een IPv6-adres van je provider krijgt en er voor IPv4 met DS-Lite, oftewel een NAT-methode (Network Address Translation) wordt gewerkt, dan lukt dat niet. Hetzelfde geldt wanneer je router bij een mobiel netwerk is aangemeld met bijvoorbeeld een 3G- of 4G-dongle. In veel gevallen is hij dan niet van buitenaf te bereiken. Mobiele providers gebruiken voor IPv4 door de schaarste aan adressen steeds vaker Carrier Grade NAT.



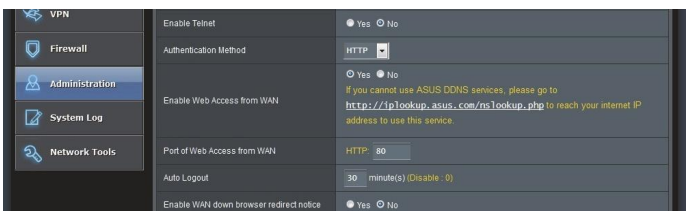
Heb je geen vast IP-adres of geen zin het IP-adres te onthouden, gebruik dan een van de DDNS-diensten.

Omgekeerd kun je wel een verbinding maken met dergelijke aansluitingen. Als je op een DS-Lite-aansluiting een LAN-LAN-koppeling via VPN wilt maken, moet je die vanuit de DS-Lite-aansluiting initialiseren. Dan kan de NAT-router van de carrier ook een verbinding maken. Routerfabrikanten hopen dat providers spoedig het Port Control Protocol implementeren waarmee je een IPv4-verbinding van buitenaf naar een apparaat achter een NAT-router kunt maken.

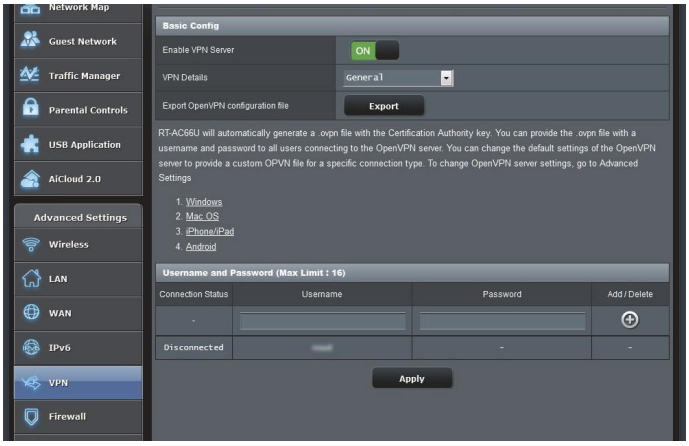
Het is eerst van belang dat je router van buitenaf bereikbaar is met een permanent adres. Heb je een dynamisch IP-adres dat om de zoveel tijd kan wijzigen, dan kun je overwegen een DDNS-dienst te gebruiken. Daarmee wordt je router van buitenaf bereikbaar via een makkelijk te onthouden url.

Veel routers en NAS-systemen hebben daar standaard een functie voor ingebouwd. Vaak zijn er al een paar veelgebruikte DDNS-diensten ingeprogrammeerd en hoef je alleen nog maar je gebruikersnaam en wachtwoord op te geven. Bereikbaarheid van buitenaf gaat wel gepaard met een bepaald risico. Gebruik daarom een sterk wachtwoord voor alle diensten waar je van buitenaf bij kunt. Omdat je de wachtwoorden voor een VPN bij mobiele apparaten kunt opslaan en die dus maar één keer hoeft op te geven, kun je het beste een lang wachtwoord gebruiken van minstens zestien tekens. Gebruik daarbij cijfers en hoofd- en kleine letters. Speciale tekens zijn niet aan te bevelen, want dat kan problemen opleveren. In de meeste gevallen verandert je IP-adres niet zo vaak of heb je zelfs een vast IP-adres. Dat laatste zal zeker bij een glasvezelverbinding vaak aan de orde zijn. Toch kun je er ook dan voor kiezen een DDNS-service te gebruiken, omdat de link die je dan moet intypen vaak beter te onthouden is dan een IP-adres van allemaal cijfers.

Bij de Asus RT-AC66U kun je via het menu-item WAN op het tabblad DDNS de DDNS-service van Asus zelf instellen, maar ook uit een aantal andere standaard DDNS-servers kiezen. Selecteer de service die je wilt gebruiken en vul de inloggegevens in. Vanaf dat moment kun je met bijvoorbeeld ctmagazine@no-ip.com bij je router komen omdat de router regelmatig bij no-ip.com controleert of zijn externe IP-adres nog hetzelfde is. Als dat niet zo is, wordt dat IP-adres bijgewerkt. Daar merk je zelf



Als je niet wilt dat je router zelf vanuit internet bereikbaar is, moet je die optie uitzetten. Wil je dat wel, verander dan in ieder geval het poortnummer van 80 in zoiets als 8088.



Het installeren van de VPN-server vergt op deze Asus-router niet meer dan het aanzetten van die optie. Onderaan kun je nieuwe VPN-gebruikers aanmaken.

Als iemand via VPN contact heeft gemaakt, zie je in de webinterface van de router dat hij verbonden is en wat zijn lokale IP-adres is geworden.

helemaal niets van, dus daar hoef je je niet meer druk over te maken.

Vanaf dat moment is je router toegankelijk van buitenaf, maar daar heb je dan nog niets aan. Controleer bij het menu-item Administration op het tabblad System onderaan of 'Enable Web Access from WAN' uit staat, want anders kun je via het DDNS-adres ook bij de webinterface van de router. Als je dat toch handig vindt, zorg er dan in ieder geval voor dat de 'Port of Web Access from WAN' op een andere poort staat dan de standaard 80.

OpenVPN

Nu wordt het tijd de VPN-server in te schakelen. We gaan in eerste instantie kijken naar het opzetten van een VPN met behulp van OpenVPN. Dat is een opensource VPN-service met een grote community. Het grote voordeel is dat er clients zijn voor zowel Windows en Mac OS X als Android en iOS. Ook voor Linux zijn er clients, die je bij bijvoorbeeld Debian en Ubuntu makkelijk installeert met `apt-get install openvpn`.

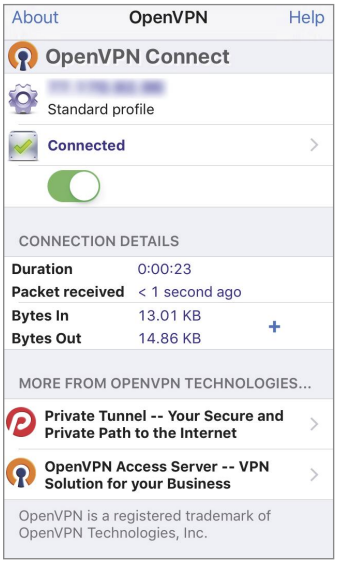
Bij de Asus gaat het installeren van een OpenVPN-server heel simpel omdat die al in de firmware van de router zit: selecteer bij het menu-item VPN op het tabblad 'VPN Server' de optie OpenVPN in plaats van PPTP en zet 'Enable VPN Server' op ON. Je hoeft verder niets in te stellen. Als je klikt op 'Apply', zul je zien dat er automatisch een account wordt aangemaakt. Dat account is het administrator-account dat je gebruikt om de router te beheren. Het is niet aan te raden dat te gebruiken om een VPN-verbinding mee te maken, vandaar dat je de mogelijkheid hebt om meerdere gebruikers aan te maken, die allemaal afzonderlijk (en tegelijk) contact met de VPN-server op de router kunnen maken. Bij de Asus RT-AC66U kun je maximaal 16 gebruikers toegang geven.

Vul een naam en wachtwoord in bij Username en Password en klik op de plusknop rechts ervan. Klik daarna op Apply, de gegevens worden niet meteen toegevoegd door de Add/Delete-knop. Een wachtwoord is achteraf niet te wijzigen, dan moet je het hele account verwijderen en een nieuw aanmaken met dezelfde naam en het nieuwe wachtwoord.

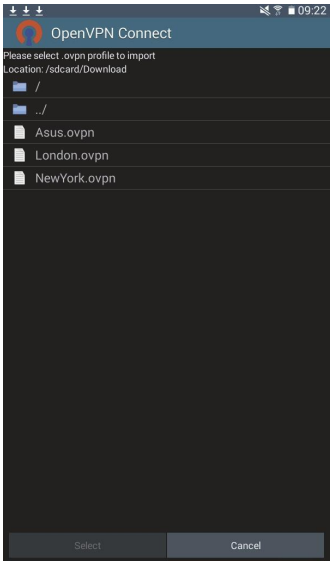
Voor een VPN met OpenVPN zit het grootste deel van het werk er dan al op. Als je contact wilt maken via een iOS-apparaat, klik je op de knop 'Export' voor het bestand client.ovpn. De certificaten en sleutels zitten meteen in dat bestand, zodat je je daar niet afzonderlijk druk over hoeft te maken. Stuur het bestand client.ovpn naar je iPhone of iPad. Zorg ervoor dat je de gratis OpenVPN-app geïnstalleerd hebt. Als je dan op het ovpn-bestand in de mail tikt, wordt dat automatisch geopend in de OpenVPN-app. Accepteer de gegevens door op het groene plusje te tikken en vul je inloggegevens in zoals die in de router zijn aangemaakt. Daarna is het een kwestie van de knop bij Disconnected naar rechts schuiven en dan zou er verbinding gemaakt moeten worden. Bij de interface van de Asus-router verandert het witte woord Disconnected in een groen Connected. Als je daar op klikt, krijg je het IP-adres van de remote verbinding te zien.

Op een apparaat met Android werkt het net zo eenvoudig. Daar gebruik je de officiële app OpenVPN Connect. Zorg er weer voor dat het bestand client.ovpn beschikbaar is door dat bijvoorbeeld naar je Gmail-account te sturen. Selecteer in de OpenVPN Connect-app de optie 'Import / Import Profile from SD card' en zoek in de bestandsmanager vervolgens je ovpn-bestand op – meestal staat hij dan in de map Download. Vervolgens geef je nog je Username en Password op en tik je op 'Connect'.

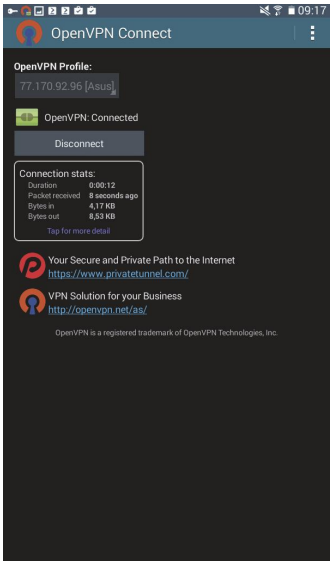
Op een notebook met Windows moet je de OpenVPN-software installeren (zie de link onderaan dit artikel). Daar waar het bij iOS en Android zo soepel gaat, werkt het bij Windows wat spartaanser. De software installeert een TAP-adapter waarlangs al het netwerkverkeer moet gaan lopen. Als je de OpenVPN GUI opent gebeurt er nog weinig, er komt op de systeembalk alleen een pictogrammetje waarmee je de proxy-instellingen kunt aanpassen of het programma kunt afsluiten. Het echte werk gebeurt pas als je rechtsklikt op een ovpn-bestand en dan de optie 'Start OpenVPN



In de OpenVPN-app van iOS kun je zien hoe lang je verbonden bent en hoeveel data er heen en weer gegaan is.

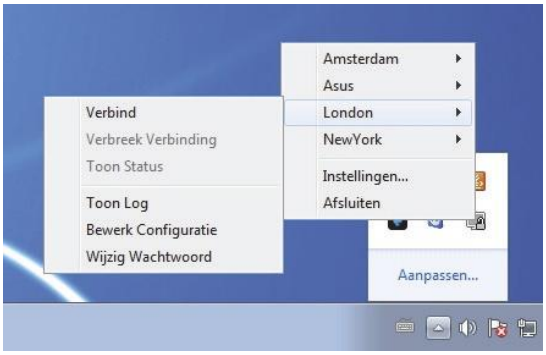


Bij de app OpenVPN Connect bij Android moet je de configuratiebestanden zelf importeren.



Bij OpenVPN Connect kun je net als bij iOS zien hoe lang je verbonden bent en hoe groot het dataverkeer is.

Het pictogrammetje van de OpenVPN GUI wordt groen als je verbinding hebt. Je kunt dan ook het toegekende IP-adres zien.



Als je meerdere VPN-servers geconfigureerd hebt, kun je met een rechtsklik op het pictogram van OpenVPN GUI makkelijk kiezen met welke je verbinding wilt hebben.

on this config file' aanklikt. Er verschijnt een Opdrachtprompt die naar je inloggegevens vraagt, waarna de verbinding wordt opgebouwd.

In de praktijk is het handiger om het ovpn-bestand naar de config-map van OpenVPN te kopieren (C:\Program Files\OpenVPN\config). Als je de OpenVPN GUI dan start, kun je meteen verbinden of de configuratie bewerken en het wachtwoord wijzigen. Dan verschijnt de uitvoer netjes in een venster zoals het Windows betaamt. Het voordeel daarbij is tevens dat het opstellen van de VPN-verbinding als Administrator gedaan wordt, wat tot foutmeldingen kan leiden als dat niet zo is.

Als je meerdere VPN-servers gebruikt, kun je de configuratiebestanden daarvan allemaal in de genoemde map zetten. Bij het pictogram van OpenVPN GUI worden ze dan netjes onder elkaar getoond en kun je selecteren met welke je verbinding wilt maken.

Voor al deze oplossingen geldt: als je via OpenVPN eenmaal contact hebt gemaakt met je thuisnetwerk, moet je aan het openbare IP-adres van je apparaat kunnen zien of dat werkt. Als je bijvoorbeeld naar whatismyip.com gaat, moet je daar een IP-adres zien dat hetzelfde is voor je apparaten thuis.

NAS-VPN

Een aantal NAS-systemen is uit te breiden met extra functies, en vaak zit daar standaard al een VPN-server bij. Bij een VPN via een NAS komen er nog wat extra problemen om de hoek kijken omdat je daar vaak wat meer bij moet instellen. Zo moet de router bijvoorbeeld weten dat al het VPN-verkeer naar je NAS moet. Bij OpenVPN wordt standaard poort 1194 gebruikt, dus als je al het (UDP-)verkeer dat bij die poort op de router binnenkomt doorstuurt naar dezelfde poort van je router, is de eerste hobbel genomen.

Bij de Asus ga je naar het menu-item WAN en dan naar het tabblad 'Virtual Server / Port Forwarding'. Als 'Enable Port Forwarding' nog niet op 'Yes' staat, moet je dat eerst nog doen. Vervolgens typ je bij 'Service Name' een omschrijving van deze portforwarding in, bijvoorbeeld 'NAS-VPN'. Bij 'Port Range' typ je 1194 in en bij 'Local IP' het IP-adres van je NAS. 'Local port' zet je ook op 1194. Het protocol zet je op 'UDP'. Klik vervolgens op het plusteken en daarna op 'Apply'. Let op: als je net hebt zitten experimenteren met de OpenVPN-server van de router, moet je die nu wel uitzetten anders gaan er dingen door elkaar lopen.

Synology heeft voor een VPN-server drie mogelijkheden, waaronder OpenVPN. Selecteer bij het item OpenVPN 'OpenVPN-server inschakelen'. De andere instellingen kun je laten voor wat ze zijn. Het maximum aantal verbindingen is 20, maar dat kun je in stappen van vijf lager instellen. Klik op 'Toepassen' om de VPN-server aan te zetten. Klik vervolgens op 'Configuratie exporteren' voor een zip-bestand met daarin een ovpn-bestand en een certificaat (ca.crt). Daarna moet je met een editor het bestand openvpn.ovpn openen. Bij de regel `remote YOUR_SERVER_IP 1194` verander je `YOUR_SERVER_IP` in het openbare IP-adres of het DDNS-adres van je netwerk. De regel `#redirect-gateway def1` verander je in `redirect-gateway`. Bij de regel `#dhcp-option DNS DNS_IP_ADDRESS` moet je het commentaarteken weghalen en `DNS_IP_ADDRESS` vervangen door het IP-adres van je router (bijvoorbeeld 192.168.0.1).

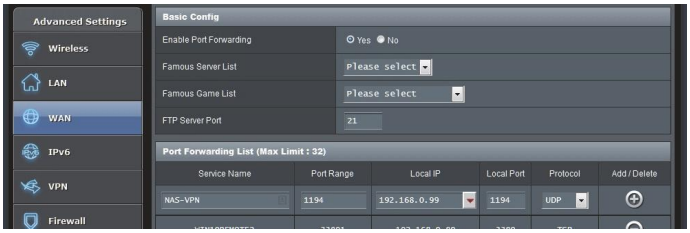
Daar waar `ca ca.crt` staat moet het certificaat komen. Verander die regel door de regels

```
<ca>
</ca>
```

en voeg daartussen de inhoud van het crt-bestand in, inclusief `-----BEGIN CERTIFICATE-----` en `-----END CERTIFICATE-----`.

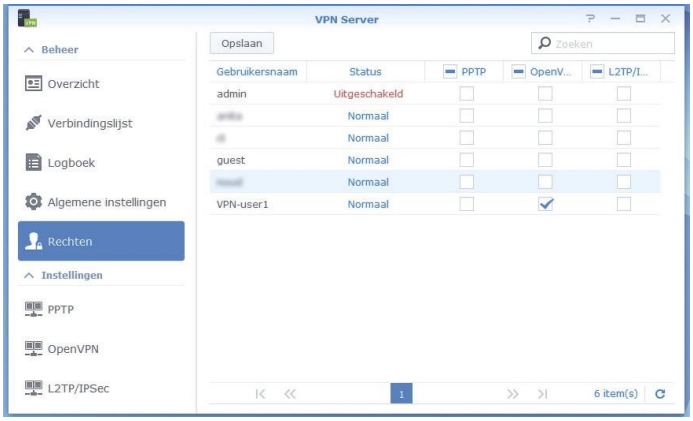
Voor de VPN-server van Synology wordt niet met aparte gebruikers gewerkt, maar met de accounts op de NAS. In principe hebben VPN-gebruikers niet automatisch iets op je NAS zelf te zoeken, die NAS wordt alleen gebruikt als intermediair. Het is het veiligst om voor de externe VPN-verbinding een of meerdere aparte accounts aan te maken. Maak in het Configuratiescherm bij Groep ook een nieuwe groep aan en geef die bijvoorbeeld de naam Synology-VPN. Bij de gedeelde mapmachtigingen hou je alles uitgevinkt, een VPN-gebruiker heeft standaard niets op de NAS te zoeken. Ook toegang tot de toepassingen moet je uitlaten, zoals je bij gewone netwerkapparaten ook zou doen. Na 'Toepassen' is de groep aangemaakt en kun je gebruikers gaan toevoegen.

Bij 'Gebruiker' voeg je via 'Maken' een nieuwe gebruiker toe. Bij het venster met 'Toevoegen aan groepen' vink je de net aangemaakte groep 'Synology-VPN' aan. Vink de optie 'De gebruiker niet toestaan om het wachtwoord van de account te wijzigen' aan om alles zelf onder controle te kunnen houden als je

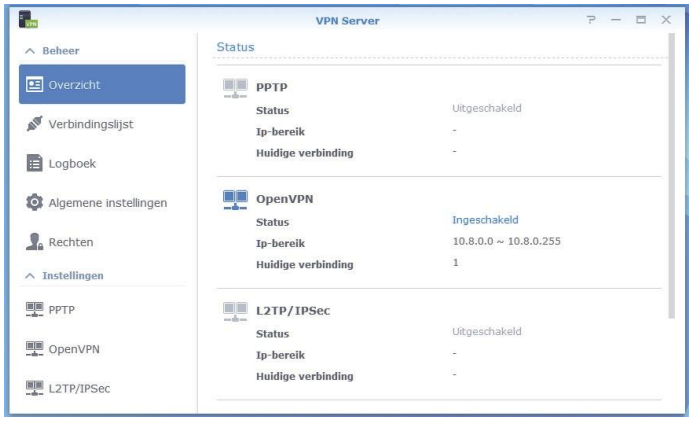


OpenVPN gebruikt standaard poort 1194, dus die poort moet je expliciet doorsluizen naar het NAS-apparaat waar de VPN-server op draait.

Maak voor je VPN aparte gebruikers aan die niet hetzelfde zijn als de gebruikers van je NAS.



Maak voor de VPN-server een aparte groep met specifieke VPN-gebruikers aan. Geef hen alleen toegang tot het protocol dat je gaat gebruiken.



In de DSM-interface van Synology kun je zien dat er op dit moment een iemand verbinding via VPN heeft gemaakt.

dat wilt. Ga vervolgens naar de instellingen van de VPN-server. Bij de instellingen van 'Rechten' kun je aangeven welke gebruikers toegang tot welke VPN-methoden mogen hebben. Daar zet je de optie voor OpenVPN voor de net aangemaakte gebruiker aan en alle andere uit.

Contact met de NAS

Het veranderde bestand openvpn.ovpn met het certificaat erin stuur je nu naar het apparaat waarmee je een VPN-verbinding met thuis wilt maken. Met de OpenVPN-app(licatie) open je dat bestand, typ je je inloggegevens in en wordt de VPN-verbinding met je NAS opgebouwd. Dat principe geldt op dezelfde manier voor alle platforms zoals hierboven beschreven.

Mocht je kunnen kiezen tussen een VPN-server op je router of op je NAS, dan heeft een router in principe de voorkeur. Bedenk bijvoorbeeld dat al het dataverkeer van de websites die je met je remote verbinding bezoekt eerst via je VPN-server thuis gaat. Als dat je router is, gaat dat dataverkeer vanuit internet meteen weer door naar jouw mobiele apparaat. Als de VPN-server op je NAS staat, moet het dataverkeer vanuit internet eerst via je router naar je NAS en vandaar weer terug naar de router en je mobiele apparaat. Die extra route levert een vertraging op, die in de praktijk mee kan vallen omdat de bottleneck in de verbinding waarschijnlijk in het dataverkeer tussen je router en het mobiele apparaat zit. Maar toch, alle kleine beetjes helpen.

Andere protocollen

Er zijn meerder mogelijkheden om een VPN-verbinding te maken. In principe zijn daar drie protocollen voor beschikbaar: PPTP, L2TP/IPSec en OpenVPN. Het Point-to-Point Tunneling Protocol moet je niet meer gebruiken, dat is te oud en simpel te kraken. Het Layer 2 Tunneling Protocol (L2TP) is een uitbreiding van PPTP en gebruikt IPSec voor het versleutelen van het dataverkeer. De data worden daarbij twee keer ingekapseld, wat meer tijd en/of performance van de VPN-server vraagt. OpenVPN werkt met de OpenSSL-versleutelingsbibliotheek en werkt met certificaten, waardoor minder resources nodig zijn. L2TP werkt met een paar vast ingestelde poorten (UDP-poorten 1701, 500 en 4500) en die willen nog wel eens geblokkeerd worden door een firewall. OpenVPN werkt daarentegen met maar één poort: die staat standaard op 1194, maar is vrij in te stellen. OpenVPN heeft qua veiligheid en snelheid dan ook de voorkeur, met L2TP/IPSec als goede tweede.

Wat ondersteuning van OpenVPN en L2TP/IPSec betreft zijn er wel wat verschillen. In de meeste besturingssystemen zit standaard ondersteuning voor L2TP/IPSec, terwijl je voor OpenVPN altijd een app of programma moet ondersteunen. Dat laatste heeft dan weer als voordeel dat het vrijwel meteen werkt.

Haken en ogen

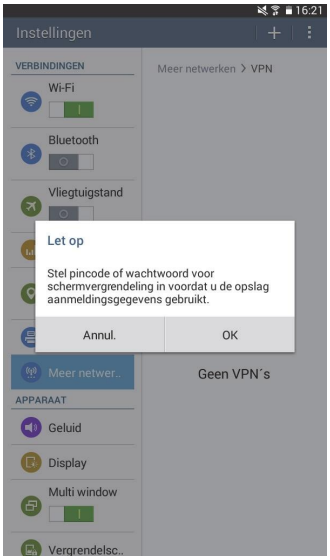
Een VPN heeft voordelen, zoals veilig internetten en geen meekijkers. Maar er zijn ook nadelen, waaronder een langzamere verbinding door versleuteling. Een nog niet genoemd nadeel is dat je internetverbinding wel goed moet zijn – en blijven. Telkens als je wifiverbinding even wegvalt (wat bij mobiele apparaten nog wel eens het geval wil zijn), wordt je VPN-verbinding afgebroken en moet je hem opnieuw opbouwen, al dan niet met het opnieuw intypen van je inloggegevens.

Je moet ook beseffen dat bij een VPN-verbinding via je thuisrouter of NAS al het dataverkeer langs je eigen netwerk komt en het mobiele apparaat ook als netwerkapparaat in je netwerk te zien zal zijn. En omgekeerd: alle in het netwerk aanwezige apparaten zijn op je mobiele apparaat te zien, inclusief allerlei shares. Je wilt natuurlijk niet dat iedereen daar zomaar bij kan komen, dus moet je het mobiele apparaat goed beveiligen. Bij Android staat het Apparaatbeheer standaard aan, als je OpenVPN Connect daar gaat gebruiken wordt standaard de pincodebeveiliging op het vergrendelingsscherm geactiveerd en moet je eerst een pincode opgeven voordat je met OpenVPN verder mag. Bij andere apparaten is dat niet zo, dus als je geen wachtwoord of andere vorm van identificatie ingesteld hebt, kan iedereen die bij je apparaat kan ook de VPN-verbinding inschakelen en op die manier bij alle bestanden in je netwerk komen. Dat moet je wel goed beseffen.

Als de wifiverbinding van je mobiele apparaat even wegvalt, is dus ook de VPN-verbinding weg. Als je op dat moment bestanden in het lokale netwerk geopend hebt, kun je daar dus niet meer bij. Dat merk je meteen, maar de openstaande websites werken nog gewoon door omdat je een link die je daar aanklikt dan via het draadloze netwerk waarop je aangesloten bent wordt geladen – en dat is dus niet meer veilig. Het is dan ook zaak de icoontjes voor de VPN-verbinding goed in te gaten te houden.

Een aantal van de haken en ogen die we hier noemen kun je oplossen met een commerciële VPN-aanbieder. Vanaf pagina 137 hebben we daar een aantal van getest. Dan heb je de eventuele beveiligingsproblemen met je eigen netwerk meteen getackeld. (nkr)

www.ct.nl/softlink/1604132



Als je via de instellingen van Android een VPN wilt instellen, moet je verplicht een pincode of wachtwoord instellen voor de veiligheid van je eigen data en netwerkomgeving. c't