Problemen met DNS-servers

Kees van der Vlies

De DDOS-aanval van enige maanden geleden op de server van Ziggo had tot gevolg dat gebruikers wel toegang hadden tot het internet, maar geen verbinding konden krijgen met de DNS-server van hun provider, en dus niet konden browsen. Resetten van router/modem en pc helpt dan niet. Toch moet je het altijd proberen!

De DNS-server is een 'verplicht' tussenstation om internetadressen te 'vertalen' in IP-adressen. DNS staat voor Domain Name System, dus een systeem van of voor domeinnamen.
Internetadressen zijn altijd cijferreeksen, en voor de 'leesbaarheid' worden aan de cijferreeks letters en 'woorden' toegekend. Dat zijn de websitenamen zoals wij die kennen: www.hcc.nl, enz. Typ je zo'n adres (een domeinnaam) in, dan gaat het naar de DNS-server van je internetprovider, die er een IP-adres van maakt. Van de HCC, bijvoorbeeld, heeft de server het IP-adres 212.72.227.82. Ook je eigen computer heeft in een (inter)netwerk altijd een IP-adres. Buienradar (van RTL) heeft het IP-adres 217.118.167.200, Google 74.125.195.102, en zo zijn er natuurlijk vele miljoenen IP-adressen op de wereld. Zo veel zelfs dat men een nieuw IP-adressensysteem heeft moeten ontwikkelen. Dat heet IPv6, en heeft een veel grotere capaciteit dan het huidige en (nog steeds) meest gebruikte IPv4.

Elke internetprovider heeft een eigen DNS-server, een computer die de aangevraagde 'naam' naar een IP-adres omzet of beter: in een tabel opzoekt. En ook het omgekeerde komt voor. Daarnaast zijn er vele min of meer 'onafhankelijke' DNS-servers, die hetzelfde werk doen, maar buiten je eigen provider om. Zie bijv. lijsten als: http://public-dns.tk/ of 'google' naar een lijst. Bij een DDOS-aanval worden er op één DNS-server zoveel verzoeken gedaan om IP-nummers/ internetadressen te vertalen, dat de server overbelast raakt en bonafide gebruikers niet meer goed van dienst kan zijn. Op zo'n moment zou je dus je 'eigen', overbelaste DNS-server – dus die van je provider – moeten kunnen omzeilen en van een algemene DNS-server gebruik kunnen maken. Het interne IP-adres van elke computer (localhost of loopback) is altijd: 127.0.0.1, om te testen. Voor de uitleg is onder meer gebruik gemaakt van het artikel van Menno Schoone. Zie: https://www.schoonepc.nl/tools/websites_blokkeren_met_opendns.html

Voor OpenDNS Home kan een extra filter worden ingesteld. Voordat het filter wordt geactiveerd, moet eerst nog via de website https://store.opendns.com/get/home-free een gratis account worden aangemaakt. Een filter (shield) blokkeert (voor kinderen) ongewenste websites.
Het is zinvol om een mix te maken van de twee blokken zodat, bij uitval/onbereikbaarheid van de DNS-servers van Google, de DNS-servers van OpenDNS kunnen worden gebruikt en andersom. Zo'n mix zou kunnen zijn: 8.8.8.8 en 208.67.222.123.
Denk erom dat de DNS-server u altijd een IP-adres (getallen met punten) laat invoeren, nooit een naam.
Trouwens, als u IP-adressen bij de hand hebt, die u wilt gebruiken in plaats van een naam, zou dat ook moeten werken zónder tussenkomst van uw 'eigen' DNS-server.

Enkele voorbeelden van goede algemeen toegankelijke DNS-servers

OpenDNS FamilyShield	208.67.222.123	208.67.220.123
OpenDNS Home	208.67.222.222	208.67.220.220
GoogleDNS	8.8.8.8	8.8.4.4
OpenNIC	31.220.43.191	151.236.29.92
Norton Connect Safe	199.85.126.10	199.85.127.10
Comodo	8.26.56.26	8.20.247.20
DNS Watch	84.200.69.80	84.200.70.40
Free DNS	37.235.1.174	37.235.1.177

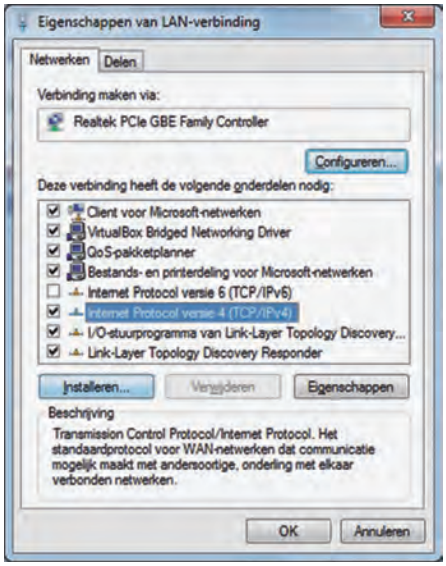
Het gaat in Windows dan als volgt:
1. Ga naar het Configuratiescherm. Dat kunt u eventueel vinden via een Windows-zoekopdracht.
   Klik op Netwerkcentrum (afbeelding 1) of Netwerk en Internet (afbeelding 2) en dan op Netwerkcentrum.
3. Klik in het venster aan de linkerkant op Adapterinstellingen wijzigen.
4. Roep de Eigenschappen van uw wifi- of LAN-verbinding op door met de rechtermuisknop te klikken op de naam van de verbinding die u gebruikt, meestal zijn dat er niet zo veel.
5. U ziet nu het venster als afgebeeld op de volgende pagina (afbeelding 3).

   Ga in de lijst naar Internet Protocol versie 4 (TCP/ IPv4). Als u daarop klikt, wordt de keuze blauw.
6. Klik dan op de knop Eigenschappen daar onder.

Afbeelding 1

Afhankelijk van uw instelling op 'Categorieën of 'Pictogrammen' ziet uw Configuratiescherm er uit als in afbeelding 1 of 2

Afbeelding 2



Afbeelding 3

7. Kies: De volgende DNS-serveradressen gebruiken.

8. Daar vult u een paar in uit de eerdergenoemde lijst (Open DNS, Google etc.)

Met een paar keer OK bevestigt u de nieuwe keuze. Als later de situatie weer 'normaal' is, kunt u terug naar standaard DNS van uw provider. Het is misschien verstandig die vooraf te noteren!
Niet alleen computers of servers hebben IP-adressen, ook uw router, webcam, printer en nog veel meer apparaten kunnen een IP-nummer hebben. Internet der dingen, apparatuur met een eigen taak.

Zijn er ook nadelen of gevaren aan het gebruik van vrij toegankelijke DNS-servers?

In theorie wel, de DNS-server staat niet onder controle van een provider en kan dus surfgedrag en IP-nummers (gebruikers) vastleggen en aan derden beschikbaar stellen. Dat kan (en moet soms) úw provider ook doen, dus of er echt een (groter) gevaar van uitgaat, is moeilijk vast te stellen. Ga ervan uit dat alles op internet min of meer openbaar is. Wie er met u meekijkt of wie in uw dataverkeer geïnteresseerd is? Joost mag 't weten. Als gebruiker heb je daar geen controle over. Criminelen pogen soms ingetypte internetadressen te veranderen om de gebruiker te misleiden.

DNS-servers over de hele wereld synchroniseren hun tabellen dagelijks, want er komen voortdurend sites bij en er verdwijnen ook sites of ze gaan over naar een andere host.
Misschien dat VPN, dat met zgn. tunneling werkt, iets veiliger is …
In ieder geval is de oplossing zoals hierboven geschetst, een bruikbaar (tijdelijk) alternatief.
Er is nog meer te vertellen over DNS(servers): propagatietijd, zones, A-record, SPF, CNAME, MX record (voor e-mail). Maar dat is echt iets voor de liefhebbers en de profs.

Volledige anonimiteit op het internet

Het is niet zozeer dat kwaadwillenden, hackers en overheden (die kunnen ook samengaan!) de inhoud van uw websitebezoek, zoekgedrag of e-mail zullen napluizen en u als persoon weten te traceren, maar wel erachter (willen) komen vanaf welk IP-adres welke handelingen gedaan en welke verbindingen gelegd worden. Daar wordt patroonherkenning op losgelaten en die analyse kan gebruikt/misbruikt of verkocht worden. Denk alleen maar aan op u gerichte reclame.
Wil je geen (IP-)sporen achterlaten op internet, dan is het gebruik van het TOR-netwerk daarvoor de aangewezen weg. Het verhusselt voortdurend alle IP-adressen van alle gebruikers en biedt zo een hoge mate van privacy. Wel zijn niet alle functionaliteiten via TOR operationeel, vooral die waarbij (Java) scripts, cookies of video vereist zijn; plug-ins worden namelijk geblokkeerd. Er is een TOR-browser: https://www.torproject.org/download/download.html.en.

De 'private mode' van sommige 'gewone' browsers is minder veilig; die slaat weliswaar uw browse-geschiedenis niet op en is soms kritischer met cookies, maar werkt meestal wel met uw eigen IP-adres!

Hoe kom ik IP-adressen te weten?

Er zijn veel sites die IP-adressen kunnen tonen of omgekeerd de naam van de server kunnen vinden die bij een IP-adres hoort.
http://www.mijn-ip.net/ip-adres-zoeken/ geeft eerst uw eigen IP-adres en biedt op het scherm de mogelijkheid een IP-adres in te vullen, waarbij dan de naam van de server gevonden wordt.

http://whois.domaintools.com. Als je daar bijv. zoekt naar microsoft.nl, komt het IP-adres van de server tevoorschijn: 94.245.126.102 en die blijkt in Dublin te staan. Er worden nog meer details getoond.

https://www.iplocation.net/ geeft de locatiegegevens van uw IP-adres, gevonden volgens een aantal diensten. Die diensten zijn het niet allemaal met elkaar eens. Zo kan één adres in Nederland zowel gelokaliseerd zijn in Amsterdam, als in Breda, Hague (dat zal Den Haag zijn), of Netterden (nog nét in Gelderland?). Het eerder gevonden IP-adres van Microsoft Nederland blijkt daar niet alleen in Dublin te huizen, maar eveneens in UK, Londen en Unstone.

Zoekmachines kunnen een IP-adres (helpen) thuisbrengen.
Zoek maar eens op: 67.138.108.201 en zie welke website daarachter zit. Of 54.246.215.9, maar wat doen Dublin (alweer) en Amazon daarbij? Het is meteen duidelijk dat het www écht wereldwijd is, zonder dat we dat steeds merken.

http://www.hcidata.info/host2ip.htm en http://whoismachine.com/ werken naar beide kanten:
IP-adres <-> Host name.
http://ipaddress.com/ip-lookup/ ook, plus extra's.
http://www.ipsglider.com/ en http://www.clearwebstats.com/ zijn kort en overzichtelijk; ook weer tweezijdig zoeken.
http://www.speedguide.net/ip/ is de IP-keuzesectie van een grote website, geheel gewijd aan communicatie, internet, nieuws, besprekingen, e.d. In het Engels, zoals veel van deze services.

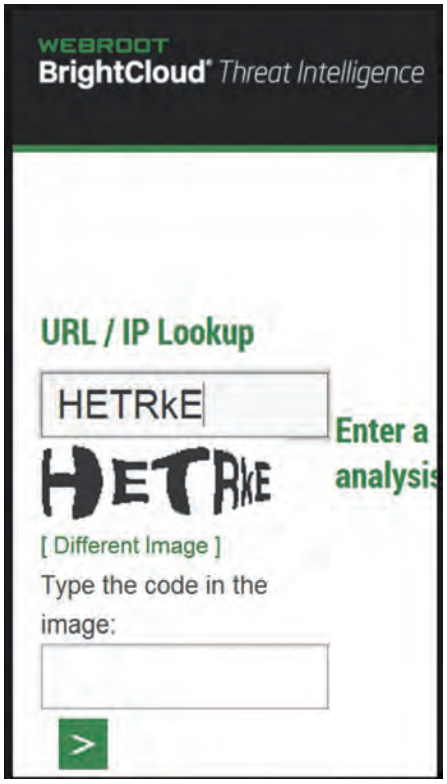
Een IP-adres zoeken in één commandoregel gaat met http://www.[naam].basicwebreport.net/. Voor [naam] vult u de website-URL in, bijv. http://www.limmerick.nl.basicwebreport.net/
Bedenk wel dat heel vaak de (host)-server gevonden wordt, maar niet altijd de website die u zocht.

Servers bieden dikwijls onderdak aan tientallen of honderden websites, die pas bij het zoeken van verdere details (misschien) gevonden worden. Veel zoeksites gaan niet zover in het vermelden van details als de hierboven genoemde. Zie bijv. http://www.natlo.nl/ip/31.186.169.20/.

Voor sommigen schijnt de informatie over de locatie ook de hoogte boven de zeespiegel te moeten omvatten. Zo meldt www.iplocationtools.com/ bijv.: Tilburg, 16 m. http://whatismyipaddress.com/ip-lookup vindt de naam bij een IP-adres. Eénrichting. http://everindex.nl/ geeft verschillende soorten informatie, zoals 'ranking' van de gevonden sites. De URL http://www.ipdatabase.com biedt meervoudige services. Maak je keuze in de linkerbalk.

nslookup

En dan hebben we in Microsoft ook nog het commando **nslookup**. Dat voert u uit in het commandovenster, oftewel de opdrachtprompt. Het werkt - maar niet altijd goed - in twee richtingen en maakt gebruik van uw DNS-server. Typ maar eens in:
nslookup hcc.nl
of
nslookup 145.58.28.39 .



Afbeelding 4 captcha

Een captcha is een controlemiddel dat (automatische) uitlezing door hackers-computerprogramma's moet tegengaan. Alleen menselijke ogen en interpretatie kunnen de vervormde letters en cijfers herkennen, zo is de redenering.

Betrouwbaarheid of reputatie

Een website die mogelijke malware op een site onderzoekt en u daarvan een rapport aanbiedt, is: https://urlquery.net/.

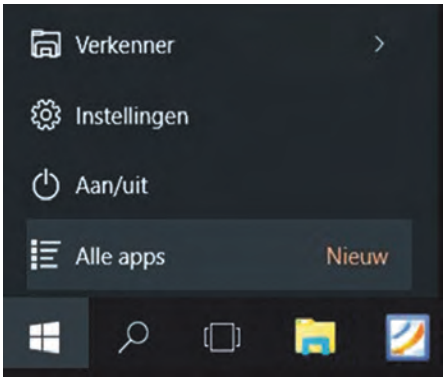
Nu we toch over de (on)betrouwbaarheid van websites hebben, daarvoor biedt McAfee (van Intel) de prima Engelstalige site: https://trustedsource.org/

Een ook kan : http://www.brightcloud.com/tools/url-ip-lookup.php u voor mogelijk onbetrouwbare IP-adressen of URL's waarschuwen. Wel elke keer een captcha invullen, zie afbeelding.

En ten slotte mag de site http://global.sitesafety.trendmicro.com/ in deze opsomming zeker niet onvermeld blijven.

Windows 10, alternatieve methode om van DNS-server te veranderen

Klik op Start of op de Windows-toets en kies **Instellingen** uit het lijstje links beneden (afbeelding 5).



Afbeelding 5

Kies in het vervolgvenster Ethernet. Dat ziet er dan zó uit als in afbeelding 6:

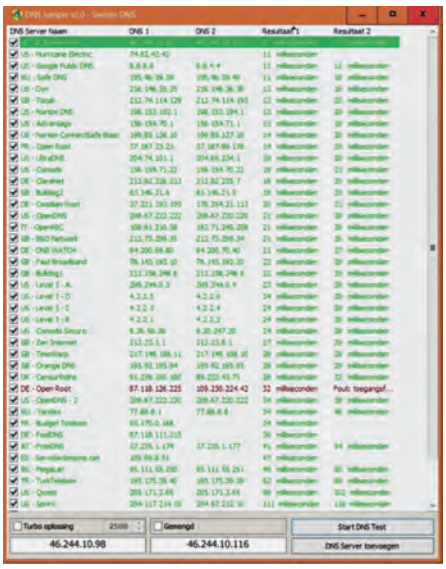
Afbeelding 6

Kies daarin Adapteropties wijzigen. De verdere procedure met rechtsklikken op uw netwerkverbinding is (in dit artikel) eerder beschreven.

DNS Jumper

De taak van het instellen van een andere DNS-server, zoals hiervoor beschreven, kan overgenomen worden door een klein (gratis) programmaatje: DNS Jumper v2.0. (zie afbeelding onder).
Het programma kan de snelste DNS-server zoeken, die op het moment van starten beschikbaar is.
Vaak zal dat de 'eigen' DNS-server van je provider zijn. Maar er verschijnen ook andere in het lijstje, die genoemd zijn in het begin: Norton, Google, Open DNS, Comodo, Open NIC.

DNS Jumper 2 is te downloaden van www.sordum.org. De Nederlandse (of eigenlijk Vlaamse) taal is te kiezen via het knopje Options. Het testresultaat kan gesorteerd worden naar naam (in feite landcode), DNS 1, DNS 2 en gemeten snelheid.

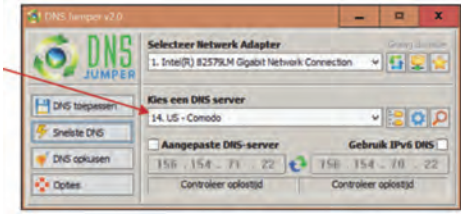


Afbeelding 7

Bedenk wel dat de snelheid een momentopname is. Een test, enkele seconden erna, geeft al een heel ander resultaat. Ook blijkt uit het lijstje dat niet alle DNS-servers (meer) 'in de lucht' zijn. (Zie afbeelding 7).

Wel duidelijk worden de verschillen in responstijden. In de hier afgebeelde lijst is de snelste 8 ms en de traagste 182 ms (naar beneden gescrold).

De gebruiker kan zelf DNS-serveradressen toevoegen. Door weg te vinken kan men een keuze maken voor de te gebruiken DNS-server(s). Zie het voorbeeld in afbeelding 8. Gekozen is voor Comodo.



Afbeelding 8