# Korte uitleg: "Network Adress Translation" en "Port Forwarding" op je router

Deze *Korte uitleg* borduurt verder op de kennis van *Korte uitleg: IP adressen* en *Korte uitleg: TCP/IP poorten*.

We zagen daar dat in je thuisnetwerk (LAN) meestal privé adressen worden gebruikt, die niet op het Internet worden gerouteerd. Waarom kan je dan toch verbinding maken met systemen op het Internet? Dat doet je modem/router, het apparaat tussen je LAN en het Internet. Aan de Internet kant (dat gaat dus eerst naar je ISP, je Internet Service Provider, het bedrijf waarmee je een contract hebt) heeft die router wel een public IP adres. Alle adressen van pakketjes die van je computer naar de router gaan en die verder moeten naar het Internet, worden door de router gewijzigd. Het privé afzenderadres wordt vervangen door het public IP adres van de router. Nu kan het pakket over het Internet verstuurd worden. Een pakket dat terugkomt wordt dan uiteraard naar de router gestuurd. De router verandert het adres weer in het privé-adres van je computer en stuurt het verder over het LAN. De router zal ook een nieuw poortnummer gebruiken aan de zendende kant, omdat het oorspronkelijke poortnummer, gegeven door de Kernel van het systeem met het privé-adres, niet uniek hoeft te zijn bij de router.

De router weet wat hij doen moet omdat hij een lijst bijhoudt van de established sessions en welke partners/poortnummers daar bijhoren.

Dit omzetten van IP adressen door de router heet "Network Adress Translation" of NAT. Ook uitgebreider Netwerk and Port Translation. Tenslotte wordt er ook een poortnummer aangepast.

## Sessie opbouwen van het LAN naar het Internet

Dit werkt prima als het initiatief tot het maken van een established session bij de computer in het LAN ligt. Die computer will bevoorbeeld een sessie met de HTTP server van `forums.opensuse.org`. Het proces (een draaiende Firefox bijvoorbeeld), vraagt aan de Kernel om een verbinding naar `130.57.66.6:80`. De kernel hangt daar als afzender het IP adres van de gebruikte NIC aan en een willekeurig vrij poortnummer: `10.0.0.154:64547`. De router wijzigt de afzender in zijn IP adres `80.101.225.164` en past ook het poortnummer aan. Op het Internet is dus `80.101.225.164:54345-130.57.66.6:80` de identificatie van de sessie. Alles wat de router terugkrijgt voor die sessie stuurt hij naar de sessie op het LAN en dus naar `10.0.0.154:16547`, waar het weer bij het Firefox process terecht komt. Let op: voor het lokale systeem met het privé adres is de sessie dus `10.0.0.154:64574-130.57.66.6:80`.

Je ziet hierboven dus dat een tweede process (Firefox, SSH) dat naar het Internet gaat een ander vrij poortnummer krijgt, zelfs als het naar hetzelfde adres:poortnummer wil. En een andere computer in het LAN heeft zelfs een ander IP adres. Dus de router kan dat allemaal uit elkaar houden.

## Sessie opbouwen van het Internet naar het LAN

Maar nu omgekeerd. Een systeem op het Internet wil een verbinding met een computer op je LAN opbouwen. Het Internet systeem kan niet anders dan het adres van de router gebruiken, want het privé adres is onbereikbaar (het kan natuurlijk op zijn eigen LAN bestaan, maar daarheen was de bedoeling niet). Dat gaat dus niet zonder meer en dat is meteen een goede bescherming tegen allerlei aanvallen vanaf het Internet.

Stel je hebt op `10.0.0.154` een web-server (Apache) draaien en je wilt die vanaf het Internet laten gebruiken. De "well known" port voor HTTP is `80` en je lokale systeem gebruikt dus `10.0.0.154:80` om te luisteren. Vanaf het Internet vragen ze verbinding met het adres van je router `80.101.225.164:80`. Je moet de router dus zo configureren dat hij de doorverbinding verzorgt (hoe dat moet hangt af van je merk en type router). Dat heet "port forwarding". Uiteraard kun je niet op deze manier twee of meer web-servers op je LAN hebben. Er kan maar één doorverwijzing van `80.101.225.164:80` zijn. Wel kan je op je router een andere poort kiezen, bijv. `80.101.225.164:8080`, en dan die laten doorverbinden met `10.0.0.156:80`. Uiteraard moet dat in het client systeem wel aangegeven worden in bijv. Firefox met `http://www.korteuitleg.henm.xs4al.nl:8080`, want bij verstek vraagt Firefox (en alle HTTP browsers) om poort `80`.

Nu is `8080` al als alternative poort geregistreerd bij IANA en dus niet helemaal onbekend bij sommige Internet gebruikers. Maar als je een heel ander poortnummer gebruikt om te forwarden en dat geheim houdt, kun je van overal op het internet naar je eigen web-server en zeer waarschijnlijk probeert verder niemand dat. Dat lijkt een beetje een grapje, maar het wordt serieuzer als je niet HTTP, maar SSH gaat gebruiken. De geregistreerde well-known port voor SSH is `22`. Als je dat op je router forward naar één van je systemen, kun je duizenden inbraakpogingen per dag verwachten. Als je daarentegen poort `50483` forward zal er weinig aangeklopt worden. Wel dat nummer onthouden, als je tenminste vanuit het Internet op je systeem wilt inloggen met SSH.