# Huiswerk Linux: DNS forwarding instellen

Je hebt nu een minimaal werkende DNS geïnstalleerd. Maar als je probeert vanuit school een ander domein dan de *localhost* op te zoeken, zul je merken dat het niet lukt. De oplossing is DNS-queries door te sturen naar de DNS server van schoolnetwerk of die van de VMWare interface. Dit noemen we *DNS forwarding*. De opdracht voor deze week is: stel je DNS server zodanig in dat hij queries doorstuurt.

## Over DNS forwarding

DNS is een over de hele wereld gedistribueerde database. Als wij bijvoorbeeld het IP-adres van *www.google.com* willen weten, dan zal onze machine rechtstreeks contact opnemen met de DNS van Google in Amerika. Op school, net als bij veel internet providers (KPN, Ziggo, Online.nl), is het niet toegestaan rechtstreeks contact op te nemen met andere DNS servers via poort 53 (zie ook: *Sendmail Smart Host*).

Gelukkig bieden de meeste providers ook gelijk de oplossing voor dit probleem. Zij hebben een interne DNS server klaarstaan die de queries voor jouw uitvoert. Dit doorsturen noemen we *DNS forwarding*.

## Het *sudo* mechanisme

Het configureren van Linux doen we namens de *super-user*. We moeten daarom tijdelijk inloggen als Administrator (root).

### Cygwin gebruikers

Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor **Als administrator uitvoeren**. Zorg er ook voor dat je DNS-server draait. Dit doe je met het *service* programma:

```
service bind start
```

### Andere Linux gebruikers

Sudo voor gebruikers van andere Linux-versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc): start een terminal met de toetsencombinatie **<Ctrl><Alt>-T**. We gebruiken het commando *sudo* om in te loggen met het *su* (become Super User) commando. Daardoor blijven we ingelogd:

```
sudo su
```

## DNS testen

DNS lookups worden via het *User Datagram Protocol* (UDP) op poort 53 uitgevoerd. Deze poort wordt geblokkeerd binnen het school-netwerk. Om te testen of het echt niet werkt, voeren we eerst een dns-query uit op een extern domein. Dit doen we met het programma *nslookup*:

```
nslookup www.xs4all.nl
```

Het kan zijn dat het gelijk lukt, maar je kunt zien dat de verkeerde server is geraadpleegd. Het *nslookup* programma kan *www.xs4all.nl* niet op je eigen DNS server (127.0.0.1) vinden en valt daarom terug op de DNS van school:

```
Server:         10.101.2.1
Address:        10.101.2.1#53

Non-authoritative answer:
Name:   www.xs4all.nl
Address: 194.109.6.92
```

Het kan ook zijn dat je de volgende foutmelding krijgt. Het *nslookup* programma valt terug op de DNS van het school-netwerk:

```
;; Got SERVFAIL reply from 127.0.0.1, trying next server
```

Of je krijgt:

```
;; connection timed out; no servers could be reached
```

Dit gaan we oplossen in de volgende stap.

# Forwarding DNS server opzoeken

Zoals eerder uitgelegd noemen we het mechanisme waarmee DNS informatie wordt opgezocht de *resolver*. De instellingen van de resolver worden bijgehouden in het bestand */etc/resolv.conf*. Op de meeste Linux versies wordt dit bestand bijgehouden door het programma *resolvconf*. Dit programma houdt alle DNS servers uit al jouw netwerken bij in aparte bestandjes. Je kunt de inhoud van deze bestandjes alsvolgt bekijken:

```
cat /var/run/resolvconf/interface/*
```

Ik krijg ongeveer het volgende te zien. De output is op iedere computer anders. We kunnen nu zien dat de DNS in mijn netwerk het IP-adres *10.0.0.200* heeft:

```
domain sassenheim.dmz
search sassenheim.dmz
nameserver 127.0.0.1
nameserver 10.0.0.200
```

**Let op**: *10.0.0.200* is de DNS server in mijn eigen netwerk. Die van het school-netwerk heeft een ander IP-adres. Onthoud dit adres, we hebben het in de volgende stap nodig.

# Forwarding instellen

De instellingen voor de BIND DNS server worden bijgehouden in het *named.conf* bestand.

### Cygwin gebruikers

Open het configuratiebestand met de *vi* editor:

```
vi /etc/named.conf
```

### Andere Linux gebruikers

In andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) staat het bestand in de */etc/bind* directory. Open het configuratiebestand met de *vi* editor:

```
vi /etc/bind/named.conf.options
```

Ongeveer bovenin het bestand zie je de *options* sectie staan. Deze verschilt per Linux systeem. Toets *i* (insert) om naar de *INSERT* modus te gaan en voeg de vetgedrukte regels in:

```
options {
      version "";     // remove this to allow version queries
      directory "/var/named";
      listen-on    { 127.0.0.1; };
      dnssec-enable no;
      listen-on-v6 { none; };
      allow-recursion { clients; };
      dnssec-validation no;
      forwarders { 10.0.0.200; };
      forward only;
};
```

**Let op**: het onderstreepte IP-adres *10.0.0.200* hoort bij mijn netwerk. Gebruik hier het IP-adres dat je in de vorige stap hebt gevonden.

Via de optie *forwarders* geven we aan naar welke DNS-servers we queries willen doorsturen. Met de optie *forward only* geven we aan dat alle queries moeten worden doorgestuurd.

Toets **<Esc>** om de *INSERT* modus te verlaten en geef de *vi* commando's *w* (write) en *q* (quit):

```
:wq
```

Het configuratiebestand wordt opgeslagen en we zijn terug op de Linux command-line.

# Het hoera-moment

Tot slot moeten we ervoor zorgen dat de BIND name daemon de gewijzigde instellingen opnieuw inleest. Dit doen we door BIND te herstarten met het *service* programma:

### Cygwin gebruikers

Herstart de BIND nameserver:

```
service bind --full-restart
```

### Andere Linux gebruikers

In andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) heet de service *bind9*:

```
service bind9 --full-restart
```

Bij een normale aanpassing in de BIND name-server hadden we het *restart* commando kunnen geven. De server ontvangt dan het *HUP* (hangup) signaal en leest de instellingen opnieuw in. Echter, na het wijzigen van opties heeft de BIND name-server een *full restart* nodig. De server wordt dan eerst gestopt en dan weer opgestart.

Nu kunnen we de configuratie testen. Dit doen we door het IP-adres van de web-server van XS4ALL op te zoeken met het progamma *nslookup*:

```
nslookup www.xs4all.nl
```

De output moet er alsvolgt uitzien. Als het goed is staat achter de veldnaam *Server* het IP-adres van de localhost (127.0.0.1). Dit betekent dat de query via je eigen DNS is uitgevoerd:

```
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   www.xs4all.nl
Address: 194.109.6.92
```

## Huiswerk opsturen

Je kunt de opdracht aftekenen door mij een e-mail met de output van het bovenstaande *nslookup* commando te sturen. Zorg dat het onderwerp van de e-mail tussen aanhalingstekens staat:

```
nslookup www.xs4all.nl | email -s "Configuratie forwarding" docent@localhost
```

Als je geen foutmelding ziet is de e-mail succesvol verstuurd.

## Administrator uitloggen

We hebben een *reverse lookup zone* aan de BIND DNS server toegevoegd en getest, maar we zijn nog steeds ingelogd als Administrator (*root*).

Geef tot slot **<Ctrl>-D** om de Administrator uit te loggen.

## Problemen oplossen

Als je in bovenstaande output een foutmelding krijgt, kijk dan in het algemene logbestand van Linux. Hier worden eventuele foutmeldingen bijgeschreven:

```
tail /var/log/daemon
```

**Let op**: in sommige Linux systemen heet het algemene logbestand **/var/log/daemon.log**. De output van een correct geïnstalleerde DNS server ziet er ongeveer alsvolgt uit:

```
Apr 17 20:20:12 optiplex named: PID 2644: command channel listening on 127.0.0.1#953
Apr 17 20:20:12 optiplex named: PID 2644: all zones loaded
Apr 17 20:20:12 optiplex named: PID 2644: running
```