Linux
Sendmail 8.12

INHOUDSOPGAVE

Hoofdstuk 1

1 Inleiding

Sendmail is een traditie. Sinds het ontstaan van het Internet vormt Sendmail de kern van het e-mail gebeuren. In de jaren '90 transporteerde Sendmail naar schatting 80% van alle e-mails over het Internet.

Sendmail is echter al lang niet meer de alleenheerser. Naast de opkomst van een aantal commerciële pakketten (zoals Microsoft Exchange), hebben ook andere open source pakketten hun intrede gedaan in dit segment van de Internetmarkt. Vooral Postfix en Qmail worden tegenwoordig veelvuldig gebruikt als mailsysteem. De belangrijkste reden hiervoor is dat Sendmail relatief moeilijk te configureren is.

Een gedreven systeembeheerder laat zich hierdoor echter niet afschrikken. Eens Sendmail op jouw netwerk draait, kan je rekenen op een betrouwbaar en degelijk mailsysteem.

Hoofdstuk 2

2 Voorbereiden van de server

2.1 Installatie van Linux

Linux Installeren

Er zijn veel verschillende distributies van Linux op de markt, allemaal met hun eigen specifieke eigenschappen en commando's. In deze cursus werd gekozen voor de distributie Fedora, waarvan de actuele versie Fedora Core 3 is. De commando's die vermeld staan in deze cursus zijn dan ook bestemd voor deze distributie. Uiteraard kan je Sendmail ook installeren op andere Linux- en Unixdistributies. De werkwijze en concepten zijn op elke distributie hetzelfde, enkel de commando's die vermeld staan in deze cursus, kunnen anders zijn op andere distributies.

We kiezen dus voor een standaardinstallatie van Fedora Core 3. Tijdens de installatie zal Fedora voorstellen zelf een firewall in te stellen. Voor een eerste kennismaking met Sendmail is het echter beter geen rekening te moeten houden met de beperkingen die een firewall oplegt aan het netwerkverkeer. Let er daarom tijdens de installatie op dat deze firewall niet geactiveerd wordt. Verderop in de cursus zal besproken worden hoe Sendmail en een firewall kunnen samenwerken om een veilig mailsysteem op te zetten.

2.2 Na de installatie

Na de installatie van Fedora moeten nog een paar instellingen gebeuren voordat we kunnen beginnen met Sendmail:

Netwerk-instellingen

Om vlot te kunnen werken met het mailsysteem, moeten de netwerkinstellingen van het systeem goed zijn ingesteld. Let er daarom op dat volgende instellingen zorgvuldig gekozen worden en goed geconfigureerd worden. Overleg eventueel met de netwerkbeheerder welke settings je kan kiezen.

- De computer- en domeinnaam van de server
- Het (vaste) IP-adres van de server
- Het subnet mask
- De default gateway
- De DNS-server. Dit is (voorlopig) de DNS-server van het netwerk waarop je je bevindt. Later zullen we zien dat Sendmail en DNS nauw samenwerken, en zullen we onze eigen DNS-server opzetten.

In Fedora kunnen de computernaam, domeinnaam en netwerkinstellingen gemakkelijk aangepast worden met het commando

```
system-config-network.
```

Netwerk herstarten

Nadat je de netwerkinstellingen aangepast hebt, moet je zowel de netwerkservice als de X-server herstarten. In Fedora kan je hiervoor volgende commando's gebruiken:

Om de netwerk service te herstarten:

```
service network restart
```

Ofwel:

```
/etc/init.d/network restart
```

X-server herstarten

Om de X-server te herstarten (let op: hierbij worden alle grafische programma's afgesloten en word je zelfs uitgelogd indien je in de grafische omgeving ingelogd was):

```
[ctrl] – [Alt] – [Backspace]
```

Om zeker te zijn dat alle instellingen geactiveerd worden, kan je het systeem natuurlijk ook herstarten. Hierbij zou het kunnen dat het heropstarten heel traag gaat en je systeem hapert bij het starten van de Sendmail Deamon. Dit komt omdat de naam van het systeem gewijzigd werd zonder dat DNS aangepast werd. Dit probleem wordt verderop in de cursus aangepakt. Gelukkig zal het opstarten (na een time-out van enkele minuten) toch lukken.

Voordat begonnen kan worden met de installatie van Sendmail, moeten alle systemen correct in het netwerk gebracht zijn. Test dit uit door te **pingen** naar de andere computers in het netwerk (op IP-adres, pingen op computernaam lukt pas als we DNS geconfigureerd hebben). Ook moeten alle systemen op het Internet kunnen surfen.

Verder is het ook wenselijk een gebruiker aan te maken, waarmee we later het mailsysteem kunnen testen.

2.3 Webmin

Webmin

In Linux worden zeer veel instellingen opgeslagen in tekstbestanden, die zich meestal in de folder /etc bevinden. Doorwinterde Linux-systeembeheerders configureren hun systeem dan ook meestal door deze tekstbestanden aan te passen. Voor minder ervaren Linux-gebruikers, is de grafische interface vaak eenvoudiger te gebruiken. Nadeel aan deze grafische interfaces (Gnome, KDE, ...) is dat ze minder mogelijkheden bieden dan de tekstcommando's en configuratiebestanden. De mogelijkheden van de grafische interface zijn bovendien sterk afhankelijk van de distributie waarmee gewerkt wordt (RedHat, SuSe, Mandrake, Slackware, ...). In deze cursus wordt ervoor gekozen een middenweg te zoeken tussen de commando's en de grafische hulpmiddelen.

Een zeer handig grafisch hulpmiddel, dat bovendien op alle gangbare Linux distributies beschikbaar is, is Webmin. Webmin is een service die je op de Linux server kan draaien, en die toelaat de server via een webinterface te configureren. Omdat in deze cursus vaak gebruik zal gemaakt worden van Webmin, is het best deze nu reeds te installeren.

Je kan Webmin downloaden van http://www.webmin.com/. Hier zijn gecompileerde pakketten beschikbaar voor verschillende distributies. We kiezen ervoor Webmin te installeren m.b.v. **rpm**. Ga daarom op de site van Webmin op zoek naar het bestand **webmin-1.160-1.noarch.rpm**. Download het bestand en bewaar het op je systeem.

Webmin installeren

Dit rpm-pakket installeer je m.b.v. van het volgende commando:

```
rpm -i webmin-1.160-1.noarch.rpm
```

Hierbij staat “-i” voor “install". Andere opties zijn “-e” voor het verwijderen van rpm's, “-u” voor het updaten van rpm's, en “-qa” om op te vragen welke rpm's geïnstalleerd zijn op het systeem. “webmin-1.160-1.noarch.rpm” verwijst naar het bestand dat je zonet gedownload hebt. Als je niet in de folder staat waar het bestand gedownload werd, moet je de bestandsnaam laten voorafgaan door het pad waar het bestand zich bevindt.

Eens Webmin geïnstalleerd, luistert het naar poort 10000. Je kan Webmin gebruiken door met een webclient te surfen naar http://localhost:10000.

Hoofdstuk 3

3 Inleiding op mailsystemen

Tegenwoordig is iedereen vertrouwd met het lezen en versturen van e-mail. Achter dit lezen en versturen, schuilen echter heel wat beginselen die voor de gewone gebruiker onzichtbaar en daardoor ook vaak onbekend zijn. Om Sendmail te kunnen beheren, is het echter nodig deze beginselen van e-mail te begrijpen.

3.1 Het e-mailmodel

Om Sendmail goed te kunnen configureren, is het belangrijk een goed beeld te hebben van het volledige e-mailmodel. Sendmail vormt op zich namelijk slechts één schakel in het e-mailmodel. Om een werkend mailsysteem op te zetten, dienen er meerdere dingen te gebeuren dan enkel Sendmail configureren.

E-mailsystemen bestaan uit de volgende componenten:

Mail User Agent

MUA (Mail User Agent): dit is een programma dat op het systeem van de eindgebruiker draait, en waarmee hij e-mails opstelt, verstuurt, afhaalt en leest. Vaak wordt dit ook de e-mail client genoemd. Enkele voorbeelden van MUA's op Microsoft Windows zijn Eudora (één van de eerste mailprogramma's op het Windows-besturingssysteem), Outlook en Outlook Express van Microsoft, ... Op Unix en Linux heb je o.a. /bin/mail (een zeer eenvoudige CLI of Command Line Interface), Mutt (één van de eerste mailprogramma's ooit, werkt met een TUI of Text User Interface), Emacs readmail, KMail (een component van KDE), Evolution (Outlook-kloon, gemaakt door Ximian), Mozilla Mail, enz.

Mail Transfer Agent

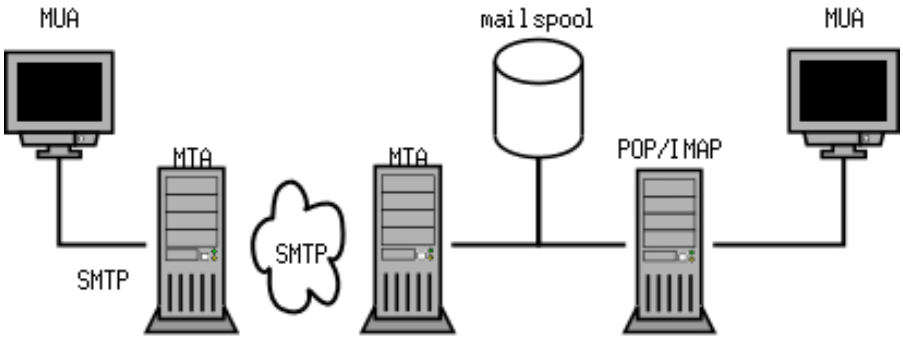
MTA (Mail Transfer Agent): Als een gebruiker een mail verstuurt (via zijn MUA), wordt het doorgegeven aan de MTA. De MTA zorgt ervoor dat de mail naar de MTA van de bestemmeling verstuurd wordt. De MTA van de bestemmeling slaat het bericht op in de e-mail spool directory, waar het wacht om opgehaald te worden. Sendmail is een MTA. Voor het doorsturen van berichten van een MUA naar een MTA, of tussen MTA's onderling, wordt het SMTP protocol gebruikt.

Mailbox protocols

Mailbox protocols: Als een gebruiker zijn e-mails wil lezen, kan dit op twee manieren. De oorspronkelijke manier is dat de gebruiker inlogt op de MTA, en zijn berichten rechtstreeks gaat lezen in de spool directory, waar ze door de MTA opgeslagen werden. MUA's die hiervoor geschikt zijn, zijn /bin/mail en Mutt. Tegenwoordig werken nog maar zeer weinig mensen op die manier. De meeste mensen lezen hun berichten niet rechtstreeks op de server, maar op hun client PC. Het doorgeven van berichten van de MTA naar de MUA op de client PC, gebeurt met de protocollen POP3 of IMAP4. Sendmail zelf kent geen POP3 of IMAP4, en kan dus ook geen berichten doorgeven aan MUA's op client computers. Voorbeelden

van servers die IMAP4 of POP3 ondersteunen zijn Courier, Uwash, Cyrus, Dovecot, Qpopper, enz.

In onderstaande figuur vind je een grafische voorstelling van deze principes.



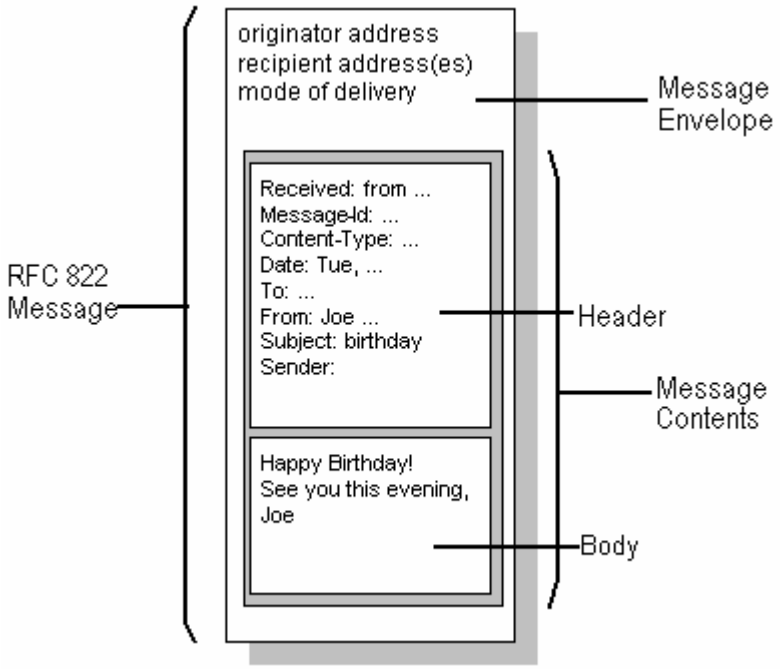
3.2 SMTP

Simple Mail Transfer Protocol

SMTP staat voor “Simple Mail Transfer Protocol” en is het protocol dat gebruikt wordt om e-mail te versturen van de MUA naar de MTA, en tussen MTA's onderling. Het wordt beschreven in 2 RFC's, namelijk RFC 821 en RFC 822.

RFC 821 beschrijft hoe een e-mail uitgewisseld wordt tussen twee systemen. Hoe dit gebeurt, bespreken we meer in detail als de SMTP-servers geconfigureerd zijn.

RFC 822, “Standard for the Format of ARPA Internet Messages” beschrijft hoe een e-mail opgebouwd moet zijn om via SMTP verstuurd te kunnen worden. Volgens dit protocol bestaat een e-mail bericht uit drie delen: de envelope, de header en de body. De header en de body worden van elkaar gescheiden door een lege lijn.



De envelope bevat het adres van de afzender, de adressen van de ontvangers en eventueel een “mode of delivery”, die echter meestal genegeerd wordt.

De header bestaat uit individuele lijnen, die allemaal beginnen met een header name. In de header vind je o.a. volgende informatie terug:

- Van wie het bericht komt
- Voor wie het bericht bestemd is
- Door welke MTA's het bericht doorgestuurd werd
- Het onderwerp van het bericht
- ...

Na de eerste lege lijn komt de message body. Hierin staat het eigenlijke bericht. Dit bericht bestaat uit lijnen van maximaal 1000 karakters. De karakters mogen uitsluitend uit 7 bits ASCII bestaan.

Een voorbeeld van een SMTP bericht volgens RCF 822 vind je hieronder:

```
From user1@dom1.edu  Wed Nov 10 15:57:28 2004
Return-Path: <user1@dom1.edu>
Received: from comp1.dom1.edu (comp1.dom1.edu
[192.168.123.137])by comp2.dom2.edu
(8.12.11/8.12.11) with SMTP id iA8AAt7v004420
for user2@dom2.edu; Mon, 8 Nov 2004 11:11:27
+0100
Date: Wed, 10 Nov 2004 15:57:27 +0100
From: user1@dom1.edu
To: user2@dom2.edu
Subject: Dit is een testmail


Gelieve deze mail te negeren.
```

3.3 MIME

Multipurpose Internet Mail Extensions

RFC 822 bevat vooral omschrijvingen over de message headers, maar is heel vaag over de specificaties van de message body. Quasi de enige beperking is dat de body uit 7 bits ASCII bestaat.

Dit wil zeggen dat je met deze standaard geen berichten kan versturen waarin speciale karakters staan, wat in sommige talen een zeer grote beperking betekent. Verder laat dit protocol ook geen binaire data toe.

Om voor deze beperkingen een oplossing te vinden, werd MIME (Multipurpose Internet Mail Extensions) ontwikkeld. MIME staat beschreven in RFC 2045 tot 2049. MIME herdefinieert het formaat van de ‘message body’ om meerdere tekst en niet-tekst (multimedia) objecten als ‘attachments’ te versturen.

In het geval gegevens verstuurd moeten worden die niet enkel uit 7 bits ASCII bestaan, doet MIME het volgende:

- De zender zal de data eerst omvormen tot 7 bits ASCII (uiteraard zonder dat hierbij gegevens verloren gaan). Technieken die hiervoor gebruikt worden zijn o.a. base64 en quoted-printable.
- Vervolgens wordt het bericht verstuurd. Omdat het nu enkel uit 7 bits ASCII bestaat, kan het gewoon met SMTP verstuurd worden.
- De ontvanger zet het bericht terug om van ASCII naar zijn oorspronkelijke vorm.

3.4 ESMTP

Enhanced SMTP

ESMTP("Enhanced SMTP") bevat een aantal uitbreidingen op SMTP die betrekking hebben op beveiliging, authenticatie, het versturen van binaire data en het reduceren van de gebruikte bandbreedte.

Als de zender van het bericht ESMTP ondersteunt, meldt hij dit aan de ontvanger. Als de ontvanger positief op deze mededeling reageert, wordt het bericht via ESMTP verstuurd. Als de ontvanger niet of met een foutmelding op mededeling reageert, betekent dit dat SMTP niet ondersteund wordt. De zender gebruikt dan SMTP om het bericht te versturen.

3.5 DNS

Domain Naming System

We zagen reeds dat we naast Sendmail ook een programma nodig hebben dat POP3 en/of IMAP4 ondersteunt. Dit is echter nog niet alles. Ook DNS speelt een zeer belangrijke rol bij het versturen van e-mails.

De hoofdtaak van DNS is het omzetten van computernamen in IP-adressen. Hiervoor gebruikt DNS de zogenaamde A-records. DNS kan ook IP-adressen omzetten in computernamen. Hiervoor gebruikt het de zogenaamde PTR records. DNS beschikt echter nog over een belangrijk soort records, namelijk de MX records of Mail Exchanger Records. MX records worden door MTA's gebruikt om te achterhalen op welke server de e-mails afgeleverd kunnen worden.

Stel dat een MTA van op het Internet mails moet bezorgen aan Bart.Mendez@xyz.be. Deze mails worden niet rechtstreeks naar Bart Mendez gestuurd, maar wel naar de mailserver van xyz.be, waar ze blijven wachten tot ze opgehaald worden door Bart Mendez. Maar hoe weet de zendende MTA nu wat de mailserver is van xyz.be? Tenslotte heeft xyz.be verschillende systemen verbonden met het Internet.

MX-records

De zendende MTA doet dit door de MX-record voor xyz.be op te vragen bij DNS. Het antwoord van DNS ziet er dan bijvoorbeeld als volgt uit:

```
xyz.be  mail exchanger = 10 mailhost.xyz.be.
```

```
xyz.be  mail exchanger = 100 mail.belnet.be.
```

Een MX record bestaat uit:

- een naam (in dit voorbeeld xyz**.be**);
- een prioriteit (in dit voorbeeld **10** en **100**);
- een bestemming (in dit voorbeeld **mailhost.xyz.be** en **mail.belnet.be).**

De MTA doet het volgende met deze data:

- Eerst probeert het de e-mail door te geven aan de bestemming met het laagste getal in de prioriteit (in dit geval **mailhost.xyz.be).**
- Lukt dit niet, dan probeert de MTA de mail af te leveren bij de bestemming met de tweede laagste prioriteit.
- En zo verder tot alle MX records uitgeprobeerd werden.
- Tenslotte probeert de MTA het bericht door te geven aan de host “xyz.be” zelf.

Om berichten van het Internet te kunnen ontvangen, is het van groot belang dat de MX records voor jouw domein juist ingesteld zijn en bekend zijn op het Internet. Ook hieraan zal een hoofdstuk in de cursus gewijd worden.

Hoofdstuk 4

4 Sendmail installeren

Op de meeste Linux-distributies is Sendmail reeds voorgeïnstalleerd. Zo ook op Fedora. We hoeven er dus enkel nog op te letten dat we de meest recente versie hebben.

4.1 Controle van de geïnstalleerde pakketten

Sendmail installeren

Voor de installatie van software maakt Fedora gebruik van rpm's. Met het commando **rpm -qa** kan je opvragen welke rpm's geïnstalleerd zijn. Voor Sendmail heb je volgende rpm's nodig:

- sendmail: het Sendmail programma zelf
- sendmail-cf: dit heb je nodig als je Sendmail wil configureren
- sendmail-devel: dit heb je nodig als je zelf programma's gaat schrijven om bepaalde Sendmail features te gebruiken
- sendmail-doc: de documentatie van Sendmail
- m4: dit heb je nodig als je Sendmail wil configureren m.b.v. macro's.

Controleer of deze pakketten geïnstalleerd zijn met volgende commando's:

```
rpm -qa | grep sendmail
rpm -qa | grep m4
```

4.2 Update naar de meest recente versie

Sendmail updaten

Omwille van beveiligingsrisico's is het belangrijk steeds de meest recente versie van deze rpm's te gebruiken.

Om dit te controleren, kan je op de site van Fedora gaan kijken wat de meest recente rpm's zijn van deze pakketten.

Surf hiervoor naar http://fedora.redhat.com en klik door op **download -> download server -> core -> 2 -> i386 -> os -> Fedora -> RPMS.**

Hier kan je controleren wat de meest recente versie is van de rpm's.

Het updaten van je systeem naar meer recente versies kan je doen met volgend commando:

```
rpm -U <de rpm die je net gedownload hebt>
```

Alternatief kan je je systeem ook updaten met yum. Het commando

```
yum update sendmail
```

onderzoekt zelf of er recentere versies op het Internet te vinden zijn, download ze en installeert ze.

4.3 Sendmail starten en stoppen

Sendmail starten en stoppen

Nu Sendmail geïnstalleerd is, moeten we er nog voor zorgen dat de server ook draait. Om services te beheren, beschikt Fedora over het commando **service**

```
service sendmail
{start|stop|restart|condrestart|status}
```

Hetzelfde kan je doen met volgend commando:

```
/etc/init.d/sendmail
{start|stop|restart|condrestart|status}
```

Als je wil dat Sendmail automatisch opstart bij het booten van je systeem, kan je hiervoor volgend commando gebruiken:

```
chkconfig sendmail on
```

Ervoor zorgen dat Sendmail niet meer automatisch opstart doe je door in het chkconfig commando “on” door “off” te vervangen.

4.4 Sendmail zelf compileren

Sendmail zelf compileren

Je kan er ook voor kiezen de source code van Sendmail te downloaden, en de software zelf te compileren en te installeren.

De Sendmail source code vind je op www.sendmail.org.

De source code uitpakken, doe je met het commando:

```
tar xvzf sendmail.versienummer.tar.gz
```

Het configureren en installeren doe je niet met de gebruikelijke commando's ./configure, make en make install, maar wel met

```
./Build
./Build install
```

Dit script bevindt zich in de hoofdfolder van de source code.

4.5 Controleren of Sendmail draait

Sendmail processen controleren

Controleren of Sendmail draait, doe je door na te gaan of het Sendmail proces actief is:

```
ps –ef | grep sendmail
```

Hoofdstuk 5

5 Mails versturen tussen gebruikers van hetzelfde systeem

Na een standaardinstallatie is Sendmail zo geconfigureerd dat het onmiddellijk gebruikt kan worden om mails te versturen tussen de gebruikers van het systeem zelf. Let wel op: de mails kunnen nog niet afgehaald worden met POP3 of IMAP4. De gebruikers moeten dus op het systeem inloggen om hun mails te kunnen lezen. Dit kan ofwel rechtstreeks, ofwel via telnet, ssh, rlogin, enz.

Lokale mailboxen

Als Sendmail een e-mail ontvangt die voor een lokale gebruiker bestemd is, dan slaat het dit bericht op in volgend bestand:

/var/spool/mail/<*gebruiker*>

Sommige Linux mail clients (MUA's) kunnen dit bestand raadplegen. Enkele voorbeelden hiervan zijn **/bin/mail** en **Mutt**.

Gebruik /bin/mail om berichten te versturen van de gebruiker **root** naar de gebruiker **user1** ga je als volgt te werk:

- Log in als **root**, en typ het commando **mail user1**
- Na het opgeven van de Subject, kan je de tekst van je bericht intypen. Als je hiermee klaar bent, sluit je het bericht af met ***ctrl-d*** (*ctrl-d* betekent in Linux hetzelfde als EOF, “End Of File”) of een punt op een lege regel.

Gebruik /bin/mail om de berichten op te vragen van **user1*:***

- Log in als gebruiker **user1** en type het commando **mail**.
- Gebruik het commando **help** om erachter te komen hoe je met **mail** je berichten kan lezen.

Merk op wat er gebeurt als je **mail** verlaat:

- Als je **mail** verlaat met het commando **x** (exit) worden er geen wijzigingen aan de mailbox opgeslagen.
- Als je **mail** verlaat met het commando **q** (quit), worden wijzigingen aan de mailbox opgeslagen. Eigenaardig hierbij is dat alle gelezen berichten verplaatst worden van /var/spool/mail/<*gebruiker*> naar het bestand ~/mbox (het bestand mbox in de home directory van de gebruiker). Als je opnieuw het programma **mail** oproept, is dit bericht dus niet meer zichtbaar. Berichten die opgeslagen zijn in het bestand **~/mbox** kan je raadplegen m.b.v. het commando

```
mail -f ~/mbox
```

Probeer ook eens uit wat er gebeurt als je mail probeert te versturen naar je eigen e-mail adres op het Internet. Komt dit bericht aan? Waarom (niet)?

De werkwijze van **Mutt** is gelijkaardig. Probeer dit eveneens uit.

Hoofdstuk 6

6 DNS

DNS speelt een belangrijke rol bij het doorsturen van e-mails tussen verschillende mailservers. Het is daarom van groot belang dat we DNS goed configureren.

6.1 DNS installeren

DNS installeren

De meest gebruikte DNS-server op Linux is BIND, dat onderhouden wordt door het Internet Systems Consortium (www.isc.org). De eenvoudigste manier om BIND te installeren is de rpm's van de download server Fedora te halen, en deze te installeren m.b.v. **rpm -i <*bestandsnaam*>**

Volgende rpm's heb je nodig voor BIND:

- bind-utils-9.2.3-13
- bind-libs-9.2.3-13
- bind-9.2.3-13

Uiteraard kan je BIND configureren via tekstbestanden. Het voornaamste tekstbestand is **/etc/named/named.conf**. Hierin vind je de basisconfiguratie van BIND terug. In dit bestand staan verwijzingen naar andere bestanden. Voor elke zone waarvoor jouw server verantwoordelijk is, is er een verwijzing naar een bestand in de folder **/var/named**.

Het configureren van BIND gaat echter ook zeer goed via Webmin. Webmin hebben we in het begin van deze cursus geïnstalleerd. Je kan het gebruiken door te surfen naar http://localhost:10000.

6.2 DNS forward lookup zones aanmaken

Forward lookup zones aanmaken

Een forward lookup in DNS is het omzetten van een naam in een IP-adres. De records die nodig zijn om deze omzetting te kunnen doen, worden bijgehouden in een forward lookup zone.

In Webmin (http://localhost:1000) een forward lookup zone aanmaken, doe je op volgende manier:

- Ga in Webmin naar **Servers** en vervolgens naar **BIND DNS-server**.
- Doe voor elke zone die je wil aanmaken het volgende:
  - Klik op **Create master zone**
  - Zorg ervoor dat **Zone type Forward** ingesteld is
  - Vul de **domeinnaam** in van de zone die je wil aanmaken (bijvoorbeeld **dom1.edu)**
  - Vul jouw computer naam in bij **Master Server**

(bijvoorbeeld **comp1.dom*x*.edu)**

- Vul jouw e-mail adres in in het veld e-mail **address (**bijvoorbeeld **user1@dom1.edu**)
- Klik op **Create**.

6.3 DNS Reverse lookup zones aanmaken

Reverse lookup zones aanmaken

Naast forward lookup zones hebben we ook een reverse lookup zone nodig. In deze zone worden records bijgehouden waarmee IP-adressen naar namen omgezet worden. Reverse lookup zones zijn geordend volgens IP-subnetten. Daarom is het belangrijk evenveel reverse lookup zones aan te maken als er IP-subnetten zijn.

Om een Reverse lookup zone aan te maken, ga je als volgt te werk:

- Ga in **webmin** naar **Servers -> BIND DNS server**
- Klik op **Create master zone**
- Kies voor **Zone type Reverse (Addresses to names)**
- Vul bij **Domain name / Network** het **netwerk gedeelte van het IP adres** van je systeem in (bijvoorbeeld **192.168.1**).
- Klik op **Create**

6.4 DNS forward lookup zones vullen

Forward lookup zones vullen

Vervolgens moeten we de forward lookup zones opvullen met de juiste records. Naast de record die er automatisch aan toegevoegd werd (SOA), moeten we A-records toevoegen voor alle hosts in het domein, en een MX-records voor alle mailservers in het domein.

Een A-record toevoegen doe je als volgt:

- Ga in **webmin** naar **Servers -> BIND DNS Server**
- Klik op de **Forward Lookup zone** waaraan je de records wil toevoegen
- Klik op **Address (A)**
- In het veld **Name** vul je de **naam** van de computer in, zonder de DNS suffix (bijvoorbeeld **comp1**)
- In het veld **Address** vul je het bijhorende **IP-adres** van deze computer in.
- De andere parameters laat je op hun standaard waarde staan.
- Klik op **Create**

Dit herhaal je voor elke host uit je domein.

Een MX-record toevoegen, doe je als volgt:

- Ga in **webmin** naar **Servers -> BIND DNS Server**

- Klik op de **Forward Lookup zone** waaraan je de records wil toevoegen
- Klik op **Mail server (MX)**
- Laat het veld **Name** leeg
- In het veld **Mail** Server vul je de naam van de mailserver voor dit domein in, met DNS-suffix, en gevolgd door een punt. Bijvoorbeeld "**comp1.dom1.edu."** (vergeet het puntje niet op het einde van de DNS suffix)
- In het veld **Priority** vul je de prioriteit van de mailserver in. De waarde **10** is hiervoor een goede standaardwaarde.
- De andere parameters laat je op hun standaardwaarde staan.
- Klik op **Create**

Herhaal dit voor elke mailserver uit jouw domein. Let er wel op elke mailserver een andere prioriteit te geven. Hoe lager dit getal, hoe belangrijker de mailserver is.

6.5 DNS reverse lookup zones vullen

Reverse lookup zones vullen

Omdat we de optie Update **reverse** op **Yes** hebben laten staan, zou dit automatisch gebeurd moeten zijn. Controleer op de volgende manier of de PTR (Pointer) records aan de reverse lookup zone toegevoegd werden:

- Ga in **Webmin** naar **Servers -> BIND DNS server**
- Klik op de **Reverse Lookup zone** die je daarnet aangemaakt hebt
- Klik op **Reverse Addresses**
- Controleer of je hier de PTR-records van alle computers uit jouw domein kan terugvinden. Als dit niet het geval zou zijn, moet je ze manueel toevoegen m.b.v. **Create.**

6.6 Forwarders toevoegen voor het omzetten van namen in IP adressen

Forwarders voor Forward lookups

Als een DNS-server niet kan antwoorden op vragen van de client, zal het de vraag doorgeven aan één van de root DNS-servers van het Internet. Voor bepaalde zones kan het echt nuttig zijn dat de vraag van de client niet doorgegeven wordt aan een root DNS-server, maar rechtstreeks aan een DNS-server van het domein waarvoor de vraag bestemd is.

Bijvoorbeeld: jij werkt op client1.dom1.edu, en je wil het IP-adres van client2.dom2.edu weten. Je stuurt dus een DNS-aanvraag naar jouw DNS-server, namelijk comp1.dom1.edu. Normaal zal deze DNS-server niet kunnen antwoorden op jouw vraag, en de vraag

doorsturen naar een root DNS-server. Indien het domein dom2.edu niet geregistreerd is op het Internet, zal de root DNS-server hierop echter niet kunnen antwoorden, en krijg je dus geen antwoord op jouw vraag. Het zou dus beter zijn indien jouw DNS-server, comp1.edom1.edu, jouw vraag rechtstreeks doorgeeft aan de DNS-server van dom2.edu, namelijk comp2.dom2.edu.

Om dit te doen, gebruik je een zogenaamde **forward zone**.

Forward zones kan je zowel toevoegen voor forward lookups (namen omzetten in IP-adressen) als voor reverse lookups (IP-adressen omzetten in namen). In het volgende voorbeeld voegen we een **forward zone** toe voor een **forward lookup**.

Een forward zone voor forward lookups aanmaken, doe je als volgt:

- Ga in **Webmin** naar **Servers -> BIND DNS Server**
- Klik op de **Create forward zone**
- Bij **Zone type** kies je voor **Forward (names to Addresses)**
- In het veld **Domain name/Network** geef je de naam van het domein op waarnaar je aanvragen wil doorsturen (bijvoorbeeld **dom2.edu**)
- In het veld **Master servers** geef je het IP-adres op van de DNS-server van deze zone.
- Klik op **Create**

Herhaal dit voor elk domein waarnaar je aanvragen rechtstreeks wil doorsturen.

6.7 Forwarders toevoegen voor het omzetten van IP adressen in namen

Forwarders voor Reverse lookup

Daarstraks zagen we hoe we Forwarders kunnen toevoegen voor het omzetten van namen in IP-adressen. Hetzelfde kan je doen voor het omzetten van IP-adressen in namen. Stel dat jouw DNS-server enkel de reverse lookup zone 192.168.1 heeft, en je wil een naam opvragen uit de zone 192.168.2. In dit geval moet jouw DNS-server de vraag doorsturen naar een andere DNS-server. M.b.v. **forward zones** kan je ervoor zorgen dat jouw vraag rechtstreeks aan je juiste DNS-server doorgestuurd wordt in plaats van naar een root DNS-server.

Een forward zone voor reverse lookups aanmaken, doe je als volgt:

- Ga in **Webmin** naar **Servers -> BIND DNS Server**
- Klik op de **Create forward zone**
- Bij **Zone type** kies je voor **Reverse (Addresses to Names)**
- In het veld **Domain name/Network** geef je het netwerk IP-adres in van het subnet waarnaar je aanvragen wil doorsturen (bijvoorbeeld **192.168.2**)

- In het veld **Master servers** geef je het IP-adres op van de DNS-server van deze zone (bijvoorbeeld **192.168.2.1**).
- Klik op **Create.**

Herhaal dit voor elk domein waarnaar je aanvragen rechtstreeks wil doorsturen.

6.8 De DNS-clients aanpassen

DNS clients

Nu alle zones en records toegevoegd werden aan DNS, moeten we enkel nog aan onze computers vertellen dat ze zichzelf als DNS-server kunnen gebruiken.

Dit kan je eveneens in Webmin doen:

- Ga naar **Networking -> Network Configuration -> DNS client**
- In het veld **Hostname** moet je de naam van jouw computer zien staan. Als dat niet zo is, pas het aan.
- Bij **DNS servers** vul je als eerste server het **IP-adres van jouw server** in. Eventueel kan je de DNS-server van je buur als tweede DNS-server opgeven.
- M.b.v. **Resolution order** zorg je ervoor dat je systeem eerst DNS gaat raadplegen, en daarna pas gebruik maakt van hosts.
- Bij **Search domains** geef je de naam op van je eigen domein (bijvoorbeeld dom1.edu). Als er naar het IP-adres van een computer gevraagd wordt zonder de DNS-suffix op te geven (dus bijvoorbeeld comp1 en niet comp1.dom1.edu), wordt automatisch de DNS-suffix toegevoegd die opgegeven werd in **Search domains**. Hiermee zorg je er dus voor dat je systeem steeds zoekt naar **comp1.dom1.edu** telkens je **comp1** zou zoeken.

De instellingen voor de DNS-client worden opgeslagen in het bestand /etc/resolv.conf. Om te kijken of webmin de wijzigingen correct heeft doorgevoerd, kan je dit tekstbestand controleren.

6.9 DNS starten

DNS starten

Nadat alle wijzigingen aangebracht zijn, moet DNS gestart worden. Ook dit kan via Webmin:

- Ga naar **Servers -> BIND DNS Server.**
- Klik op **Start Name Server** (als de server nog niet opgestart is) of op **Apply Changes** (om de nieuwe configuratie te activeren als de server al gestart is).

Standaard start BIND niet op bij het opstarten van het systeem. Om ervoor te zorgen dat BIND automatisch opstart, geef je volgend commando op:

```
chkconfig named on
```

6.10 DNS testen

Testen of de DNS-instellingen correct zijn, kan je met **host** of **nslookup**.

host

Eerst bekijken we **host**:

```
host compx.domx.edu
```

host, gevolgd door de **FQDN** (Fully Qualified Domain Name, de volledige naam van een computer, inclusief het domein), controleert of de naam omgezet kan worden in een IP-adres. Het doet dus een **Forward DNS Lookup.**

```
host comp1
```

Als **host** gevolgd wordt door de **hostname** (zonder vermelding van het domein), voegt host de naam van het **Search domain** toe (deze naam heb je daarnet m.b.v. Webmin toegevoegd aan **/etc/resolv.conf**). Vervolgens controleert het of het de volledige naam (FQDN) kan omzetten in een IP-adres. Het doet dus eveneens een **Forward Lookup Query**.

```
host www.microsoft.com
```

Dit commando zal ook een **Forward Lookup Query** doen, en probeert het IP-adres van de webserver van Microsoft te vinden. Onze DNS-servers kunnen hierop echter geen antwoord geven. Onze DNS-server geeft de vraag daarom door aan één van de **root DNS-servers** op het Internet. Omdat deze root DNS-server zelf ook het IP-adres van www.microsoft.com niet kent, geeft het de vraag door aan de **Name Server** (DNS-server, gekend a.d.h.v. **NS-records** in de root DNS-zone) van het **.com** domein. Deze geeft de vraag op zijn beurt door aan de Name Server van het microsoft.com domein. Deze Name Server kent het IP-adres van www.microsoft.com wél, en geeft het door aan onze DNS-server. Onze DNS-server kan dan het antwoord doorgeven aan het host programma op onze client.

```
host domx.edu
```

Als het bij het host-commando enkel een domeinnaam opgegeven wordt, gaat host op zoek naar de **MX-records** voor dit domein. MX-records vertellen aan welke server e-mails voor dit domein doorgegeven moeten worden.

```
host ip-address
```

host, gevolgd door een **IP-adres**, doet een **reverse DNS lookup**. Het probeert dus de naam van het systeem op te zoeken dat dit IP-adres heeft.

nslookup

We bekijken ook nog **nslookup**:

nslookup werkt gelijkaardig aan host, maar biedt meer mogelijkheden. Gebruik de manual page van nslookup **(man**

nslookup) om uit te zoeken hoe je m.b.v. nslookup mx-records kan opvragen van een andere name server.

Voordat we het mailsysteem kunnen gebruiken is het belangrijk dat DNS goed werkt. Controleer daarom grondig je eigen DNS-server m.b.v. host of nslookup. Via DNS moet je alle computernamen, IP-adressen en MX-records uit het klaslokaal kunnen opvragen. Ook MX records van het Internet moeten opgevraagd kunnen worden.

De informatie over DNS in deze cursus is voldoende om een testomgeving op te zetten waarin we met Sendmail kunnen werken. Over DNS valt echter nog heel wat meer te vertellen. Denk maar aan delegatie van subdomeinen, het opzetten van Secondary DNS servers, Zone overdrachten, forwarders, beveiligen van DNS-servers, enz. Als je DNS in een productie-omgeving wil inzetten, is een veel grondigere kennis van DNS noodzakelijk.

Hoofdstuk 7

7 Basisconfiguratie van Sendmail

Nu DNS naar behoren werkt (althans voor onze testomgeving), en Sendmail geïnstalleerd is, kunnen we de configuratie van Sendmail onder de loep nemen.

7.1 Sendmail cf-bestanden

Sendmail cf-bestanden

De configuratie van Sendmail gebeurt via een bestand **sendmail.cf**. Bij Fedora vind je dit bestand op volgende locatie:

/etc/mail/sendmail.cf

Telkens Sendmail opstart, leest het zijn configuratie uit dit bestand. Dit bestand is enkele honderden lijnen lang, en bestaat uit een zeer cryptische syntax, die door Sendmail zelf zeer eenvoudig te interpreteren is, maar door mensen slechts zeer moeizaam te verstaan valt. Als systeem administrator is het jouw job dit bestand te configureren.

Gelukkig hoef je niet met deze honderden lijnen cryptische code te werken, maar kan je werken met enkele lijnen macro-code die dit bestand zullen genereren.

7.2 De Sendmail m4 macro's

Sendmail.mc

Het bestand sendmail.cf wordt gemaakt m.b.v. het macro-configuratie bestand sendmail.mc. Bij Fedora vind je dit bestand onder

/etc/mail/sendmail.mc

De macro's die je in dit bestand opneemt, stammen van de macro definitie **m4**. Dit is een algemene macro-taal, die niet specifiek voor Sendmail geschreven is, maar wel vooral door Sendmail bekend geworden is. Je zal merken dat deze macrocommando's weliswaar eenvoudiger zijn dan de sendmail.cf configuraties, maar toch relatief cryptisch blijven. Dit is één van de redenen waarom Sendmail de naam heeft moeilijk te configureren te zijn.

Een eerste voorbeeld van /etc/mail/sendmail.mc vind je hieronder:

```
include(`/usr/share/sendmail-cf/m4/cf.m4')
OSTYPE(`linux')

define(`confMAX_HOP',`25')
```

```
define(`confSMTP_LOGIN_MSG',`$j mailer ready
at $b')
define(`confMIME_FORMAT_ERRORS',`False')


FEATURE(`promiscuous_relay')
FEATURE(`accept_unqualified_senders')
FEATURE(`use_cw_file')


MASQUERADE_AS(dom1.edu)
MAILER(smtp)
```

We gebruiken dit voorbeeld om vertrouwd te geraken met de m4-macro's voor Sendmail:

include

```
include(`/usr/share/sendmail-cf/m4/cf.m4')
```

Deze regel wordt gebruikt om een aantal standaard configuratiebestanden op te nemen in de configuratie van Sendmail. Deze regel dient steeds als eerste opgenomen te worden in /etc/mail/sendmail.mc. Merk op dat deze regel zeer eigenaardige accenten bevat: de “back quote” en de “gewone quote”. Het is belangrijk deze accenten juist in te typen, anders kan het bestand sendmail.mc niet correct omgezet worden naar het sendmail.cf bestand.

OSTYPE(`linux')

Op de tweede regel, `OSTYPE(`linux')`, wordt opgegeven dat Sendmail op een Linux-systeem draait. Het zorgt er op zijn beurt voor dat specifieke instellingen voor Linux geladen worden, door het bestand /usr/share/sendmail-cf/ostype/linux.m4 op te nemen in de configuratie. Deze regel dient steeds als tweede in sendmail.mc opgenomen te worden. Welke waarden OSTYPE nog kan aannemen, kan je te weten komen door een lijst op te vragen van alle bestanden in /usr/share/sendmail-cf/ostype/.

Vervolgens zien we een aantal regels die beginnen met het commando **define**. Define zorgt ervoor dat bepaalde parameters opgenomen worden in sendmail.cf. Er zijn honderden parameters in Sendmail, maar de meesten ervan worden in “normale” omstandigheden nooit gebruikt. Een volledig overzicht van deze variabelen vind je in elk van de boeken die vermeld staan in de literatuurlijst achteraan deze cursus. De belangrijkste van deze variabelen worden besproken in de voorbeelden in deze cursus.

confMAX_HOP

```
define(`confMAX_HOP',`25')
```

Om te vermijden dat e-mails eeuwig rondzwerven op het Internet, is het aan te raden ervoor te zorgen dat berichten na een aantal *hops* door Sendmail weggegooid worden. Standaard accepteert Sendmail berichten zonder beperking wat het aantal hops betreft. Met de optie **confMAX_HOP** wordt hieraan een beperking opgelegd. **25** is een redelijke instelling voor deze variabele.

```
define(`confSMTP_LOGIN_MSG',`$j mailer ready at
$b')
```

confSMTP_LOGIN_MSG

Standaard deelt Sendmail bij elke SMTP-connectie zijn naam en versie mee aan de zender. Dit is bijzonder interessant voor hackers,

want die kunnen a.d.h.v. deze informatie op zoek gaan naar bekende bugs om het systeem te misbruiken. Daarom is het beter een aangepaste boodschap in te stellen. Dit doe je m.b.v. de optie **confSMTP_LOGIN_MSG**. Hierin zijn **$j** en **$b** Sendmail variabelen. **$j** staat voor de FQDN van de mailserver, **$b** voor de actuele datum. Een lijst met alle Sendmail-variabelen vind je eveneens in de boeken in de literatuurlijst.

confMIME_ FORMAT_ERRORS

```
define(`confMIME_FORMAT_ERRORS',`False')
```

Standaard worden foutboodschappen van Sendmail verstuurd in **MIME** formaat. Als je dit niet wil (bijvoorbeeld omdat **root** zijn e-mails leest m.b.v. **/bin/mail**), dan kan je dit uitschakelen door **confMIME_FORMAT_ERRORS** op **False** te zetten.

Vervolgens zien we een regel die begint met het woord **FEATURE**. Hiermee kunnen we optionele Sendmail-features opnemen in de configuratie.

promiscuous_relay

```
FEATURE(`promiscuous_relay')
```

Door de toename van Spam op het Internet zijn een aantal standaardinstellingen van Sendmail aangepast. Vroeger stond **relaying** standaard open op elke Sendmail-mailserver. Tegenwoordig staat relaying standaard toe op elke mailserver. Hoewel het indruist tegen de huidige richtlijnen, is het voor ons op dit moment handiger relaying open te zetten. Later in de cursus zal relaying uitgebreid behandeld worden. Bovenvermelde regel zet relaying open.

accept_ unqualified_ senders

```
FEATURE(`accept_unqualified_senders')
```

Standaard zal Sendmail geen berichten ontvangen van afzenders die geen domeinnaam vermelden in het From adres. Ook dit is om spam aan banden te leggen. Als je Sendmail voor intern gebruik wil opzetten, kan het handig zijn toch afzenders toe te laten waarvan het domein niet bekend is. Dit kan je doen met de feature “accept_unqualified_senders”.

use_cw_file

```
FEATURE(`use_cw_file')
```

Na een standaardinstallatie weet Sendmail niet welke e-mails hij moet doorsturen naar andere mailservers, en welke hij lokaal moet afleveren. Met deze feature vertellen we aan Sendmail dat het in het bestand **/etc/mail/local-host-names** moet kijken om te weten voor welke domeinen het e-mails lokaal moet opslaan. In het bestand **/etc/mail/local-host-names** moet dan een lijst staan van alle domeinen waarvoor jouw mailserver verantwoordelijk is. Het bestand **/etc/mail/local-host-names** wordt verderop behandeld.

MASQUERADE_AS

```
MASQUERADE_AS(dom1.edu)
```

Als user1 uit dom1.edu vanuit **/bin/mail** een bericht verstuurt naar een ander domein, dan mag Sendmail dat bericht niet zomaar versturen alsof het van **user1** komt. Het moet een domeinnaam toevoegen aan de username. Standaard voegt Sendmail de computernaam toe als domeinnaam. Als we niets ondernemen, wordt het bericht dus verstuurd als **user1@comp1.dom1.edu**, en niet als **user1@dom1.edu**.

De lijn **MASQUARADE_AS(dom1.edu)** zorgt ervoor dat berichten van user1 verstuurd worden als **user1@dom1.edu** en niet als **user1@comp1.dom1.edu**.

MAILER(smtp)

```
MAILER(smtp)
```

Deze regel moet je steeds als laatste regel opnemen. Deze regel bepaalt dat Sendmail met SMPT dient te werken. Dit is in de meeste situaties het geval.

7.3 /etc/mail/local-host-names

/etc/mail/local-host-names

Sendmail weet niet automatisch welke mails het naar de buitenwereld dient verder te leiden, en welke mails het moet afleveren aan de lokale gebruikers. Dit moet je expliciet aan Sendmail vertellen. Met de macro `FEATURE(`use_cw_file')` in het bestand /etc/mail/sendmail.mc vertel je aan Sendmail dat het in het bestand /etc/mail/local-host-names moet kijken om te weten welke mails plaatselijk verwerkt moeten worden.

Alle mails bestemd voor jouw domein **dom1.edu** moeten door Sendmail plaatselijk verwerkt worden, alle andere mails moeten doorgestuurd worden naar andere mailservers. Dit vertel je aan Sendmail door de regel **dom1.edu** op te nemen in **/etc/mail/local-host-names**.

Als je in **/etc/mail/local-host-names** enkel **dom1.edu** opneemt, zal jouw mailserver e-mails die bestemd zijn voor **comp1.dom1.edu** niet als lokale mails beschouwen, en trachten ze door te sturen. Dit zal uiteraard niet lukken, omdat niemand e-mails voor **comp1.dom1.edu** als lokale mails zal beschouwen. Het is dus een goed idee ook de regel **compx.domx.edu** op te nemen in **/etc/mail/local-host-names**. Op die manier worden berichten die voor **compx.domx.edu** bestemd zijn, ook lokaal door de mailserver verwerkt.

/etc/hosts

Nog één belangrijke tip i.v.m. local-host-names: in het bestand **/etc/hosts** staat steeds een regel die begint met **127.0.0.1**, de local loopback:

```
127.0.0.1   localhost.localdomain   localhost
```

Sommige programma's vullen deze regel aan met de naam van de computer (comp1 en comp1.dom1.edu). Zorg ervoor dat de local loopback regel in /etc/hosts eruit ziet zoals hierboven, en dus de echte naam van je computer niet bevat. Uitleggen waarom dit nodig is, zou een hele uitwijding vragen over Sendmail-variabelen, wat buiten het bestek van deze cursus valt.

7.4 Van sendmail.mc naar sendmail.cf

m4

Sendmail kan het bestand /etc/mail/sendmail.mc niet lezen, het heeft het bestand /etc/mail/sendmail.cf nodig. De macro-taal m4 zet /etc/mail/sendmail.mc om in /etc/mail/sendmail.cf. Dit doe je met het volgende commando:

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Nu moeten we nog even Sendmail herstarten, en we kunnen het eindelijk gebruiken.

```
/etc/init.d/sendmail restart
```

7.5 Sendmail gebruiken

Sendmail gebruiken

Eindelijk zijn we klaar met de basisconfiguratie van Sendmail. Als je alles goed gedaan hebt, kan je nu Sendmail gebruiken om mails te versturen vanuit jouw domein naar andere domeinen.

Let wel op: we zijn nog steeds niet in staat e-mailclients te gebruiken die zich niet op de mailserver bevinden, want daarvoor hebben we nog POP3 of IMAP4 nodig.

Log in als een gewone gebruiker (bijvoorbeeld **user1**), en test uit of alles werkt met behulp van /bin/mail of Mutt. Je zou in staat moeten zijn:

- Berichten naar jezelf te sturen (zowel naar **user1** alsook naar **user1@dom1.edu**)
- Berichten naar andere gebruikers in jouw domein te versturen (**root** en **root@dom1.edu**)
- Berichten naar gebruikers in andere domeinen van ons klaslokaal te versturen (user1@domx.edu, waarbij x niet jouw domein is, maar een ander domein in het klaslokaal)
- Je kan ook berichten sturen naar domeinen die niet binnen ons klaslokaal liggen, al is het zeer de vraag of die andere domeinen jouw bericht zullen accepteren. We hebben immers een fictieve domeinnaam gebruikt. Als andere domeinen jouw e-mails accepteren, zijn ze onveilig geconfigureerd.

Als dit niet lukt, moet je op zoek gaan naar de oorzaak hiervan. Een goed hulpmiddel bij troubleshooting zijn de log files. Meer uitleg daarover vind je in volgende paragraaf.

7.6 Sendmail logfiles

/var/log/maillog

Sendmail maakt gebruik van syslog voor het loggen van alle activiteiten. Alle logging komt standaard terecht in /var/log/maillog.

In dit bestand staan niet enkel belangrijke gebeurtenissen zoals het herstarten van de server, of foutboodschappen, maar wordt ook voor elk bericht bijgehouden naar wie het werd doorgestuurd en of dit gelukt is.

confLOG_LEVEL

Het log level dat Sendmail gebruikt, kan je instellen d.m.v. volgende regel in sendmail.mc

```
define(`confLOG_LEVEL',10)
```

Log levels tussen 0 en 10 worden gebruikt om informatie te loggen die bruikbaar is voor Sendmail-administrators. De standaardwaarde 9 is een goed gemiddelde, dat slechts zelden gewijzigd moet worden. Log-levels tussen 10 en 64 geven heel wat meer informatie, terwijl log-levels boven 64 enkel gebruikt worden door de ontwikkelaars van Sendmail.

/var/log/maillog is een uitstekend hulpmiddel voor troubleshooting, maar ook voor het controleren van normale activiteiten op de mailserver.

7.7 Berichten versturen m.b.v. SMTP

SMTP

Na het toevoegen van de lijn mailer(smtp) aan sendmail.mc, wordt voor het versturen van berichten standaard ESMTP gebruikt. Enkel indien zender of ontvanger het ESMTP-protocol niet verstaat, wordt SMTP gebruikt.

Toch is het zeer interessant het SMTP-protocol even van dichterbij te bekijken, omdat het een heel handig hulpmiddel kan zijn bij troubleshooting.

De basis SMTP-commando's zijn:

`HELO`
Dit commando start de conversatie met de mailserver. Het wordt gevolgd door jouw domeinnaam, zodat de mailserver weet wie je bent. Bijvoorbeeld

HELO comp1.dom1.edu.

`MAIL`
Geeft aan door wie het bericht verstuurd wordt. Bijvoorbeeld

```
MAIL FROM: <user1@dom1.edu>.
```

`RCPT`
Geeft aan voor wie de mail bestemd is. Meerdere ontvangers worden opgegeven door het RCPT-commando meerdere keren te gebruiken. Bijvoorbeeld:

```
RCPT TO: <user2@dom2.edu>
RCPT TO: <user3@dom3.edu>
```

`DATA`
Dit commando geeft aan dat je klaar bent om het bericht zelf te versturen. Het bericht bestaat uit header lijnen (bijvoorbeeld: `Subject: testmail`) en de tekst zelf (maximaal 1000 karakters per lijn). De tekst eindigt met volgende vijf karakters (een punt op een lege regel):"\r\n.\r\n."

`QUIT`
Beëindigt de conversatie.

`EXPN`
Geeft aan dat je een mailinglist gebruikt. Dit commando wordt o.w.v. beveiligingsredenen niet door alle servers ondersteund.

HELP
Vraagt hulp aan de mailserver.

NOOP
No Operation: doet niets behalve een antwoord vragen van de mailserver.

RSET
Breekt een bericht af.

VRFY
Controleert of een bepaald e-mail adres op de server bestaat. Dit commando wordt vaak uitgeschakeld o.w.v. beveiligingsredenen.

De ontvangende server zal op elk commando een antwoord sturen. Bijvoorbeeld:

```
250 OK
```

of

```
500 Syntax error, command unrecognized.
```

Een volledige lijst van de antwoorden kan je terugvinden in RCF 821.

Je kan deze SMTP-commando's zelf gebruiken om berichten naar de mailserver te sturen. Dit is vaak zeer handig bij troubleshooting. De SMTP-server luistert meestal naar poort 25. Een verbinding opbouwen met deze poort kan je zeer eenvoudig m.b.v. telnet.

```
telnet comp1.dom1.edu 25
```

Een typische e-mailcommunicatie kan er als volgt uitzien (het teken “>” geeft aan dat het commando verstuurd wordt door de zender, “<” bevat de antwoorden van de ontvanger:

```
< 220 comp2.dom2.edu ESMTP mailer at Mon, 15 Nov
2004 10:07:18 +0100
> HELO dom1.edu
< 250 comp2.dom2.edu Hello comp1.dom1.edu
[192.168.123.137], pleased to meet you
> MAIL FROM: user1@dom1.edu
250 2.1.0 user1@dom1.edu... Sender ok
> RCPT TO: user2@dom2.edu
< 250 2.1.5 user1@dom1.edu... Recipient ok
> DATA
> 354 Enter mail, end with "." on a line by
itself
> Subject: Dit is een test
> Dit is een test
> .
< 250 2.0.0 iAF97I5B002344 Message accepted for
delivery
> QUIT
< 221 2.0.0 bastion.dom1.edu closing connection
```

7.8 Masquerading opties

MASQUERADE_AS

Stel dat een gebruiker user1 zijn mailbox heeft op de mailserver comp1.dom1.edu. Zonder masquerading zouden alle berichten van deze gebruiker verstuurd worden met als afzenderadres user1@comp1.dom1.edu. Dit is meestal niet wat we graag hebben. Liever hebben we dat de afzender user1@dom1.edu is. Hiervoor zorgt volgende regel:

```
MASQUERADE_AS(dom1.edu)
```

Masquerading heeft echter een aantal specifieke eigenschappen, waarvan de belangrijkste in deze paragraaf behandeld worden.

masquerade_ entire_domain

Standaard wordt masquerading enkel toegepast op adressen die voorkomen in het bestand /etc/mail/local-host-names. Dit wil zeggen dat bovenvermeld voorbeeld enkel werkt indien we niet enkel dom1.edu opnemen in /etc/mail/local-host-names, maar ook comp1.dom1.edu.

Dit is geen handige oplossing als in het domein dom1.edu meerdere mailservers gebruikt worden. In dat geval is het handiger als alle adressen uit het domein dom1.edu aangepast zouden worden. Dit kan je realiseren met volgende regel:

```
FEATURE (masquerade_entire_domain)
```

masquerade - envelope

Een e-mail heeft niet één afzender adres, maar twee: in de header en in de envelope. Standaard wordt masquerading enkel toegepast op het header afzenderadres. Dit maakt dat een bericht dat verstuurd wordt door user1 twee verschillende afzenderadressen heeft:

Het header afzenderadres: user1@dom1.edu

Het envelope afzenderadres: user1@comp1.dom1.edu

Meestal is dit geen probleem, omdat het envelope afzenderadres meestal niet gebruikt wordt. Toch is het uit beveiligingsoogpunt beter ook het envelope afzenderadres aan te passen. Dit doe je door volgende regel op te nemen in /etc/mail/sendmail.mc:

```
FEATURE (masquerade-envelope)
```

Er bestaan nog tal van andere opties i.v.m. masquerading. Hiervoor wordt echter doorverwezen naar de boeken die vermeld staan in de literatuurlijst.

Hoofdstuk 8

8 POP3 en IMAP4

Tot nu toe gebruikten we steeds mailclients die hun e-mails rechtstreeks in /var/spool/mail gingen lezen. In de praktijk wil een eindgebruiker zijn e-mails echter lokaal op zijn eigen PC kunnen lezen. We hebben dus nog een protocol nodig dat de berichten van de mailserver aan de eindgebruiker kan bezorgen. Hiervoor kan je POP3 (Post Office Protocol versie 3) gebruiken, of IMAP4 (Internet Message Access Protocol versie 4).

8.1 POP3 en IMAP4 servers

dovecot

Sendmail zelf biedt geen POP3- of IMAP4-protocol. We moeten dus een extra service installeren, die deze protocollen ondersteunt.

Er zijn verschillende producten beschikbaar die POP3 en/of IMAP4 ondersteunen: Cyrus, Uwash, Qpopper, Dovecot, enz. zijn maar een greep uit het aanbod.

Bij wijze van voorbeeld werken we in deze cursus met Dovecot.

Dovecot is standaard beschikbaar op Fedora, maar je kan het ook downloaden van www.dovecot.org.

Dovecot installeren kan je best doen door de rpm te downloaden van de Fedora download site. Nadat je de rpm gedownload hebt, installeer je Dovecot m.b.v. `rpm -i`

Dovecot starten en stoppen kan je met

```
/etc/init.d/dovecot { start|stop|restart}
```

Ervoor zorgen dat Dovecot automatisch opstart doe je m.b.v.

```
chkconfig dovecot on
```

Verder hoef je niets aan Dovecot te configureren.

Standaard biedt Dovecot een IMAP4-server en een beveiligde IMAP4-server aan. Indien je ook POP3 en beveiligde POP3 wil aanbieden, moet je het bestand /etc/dovecot.conf aanpassen.

TCP poorten

In volgende tabel vind je een overzicht van de TCP-poorten die gebruikt worden (en die dus niet afgeschermd mogen worden door een eventuele firewall).

Protocol	Poort (TCP)
SMTP	25
POP3	110
POP3 (secure)	995
IMAP4	143
IMAP4 (secure)	993

nmap

Je kan in Linux eenvoudig testen of een service draait, door te kijken of er een verbinding gemaakt kan worden met de poort waarop de service draait. Dit kan je doen met het tooltje nmap. Indien het niet op je server geïnstalleerd is, kan je het downloaden van de download site van Fedora (Fedora.redhat.com)

Het commando

```
nmap -p 25,110,143,993,995
```

controleert of er een service draait op de poorten 25 (SMTP), 110 (POP3), 143 IMAP4), 993 (Secure IMAP4) en 995 (Secure POP3)

8.2 POP3- en IMAP4-clients

POP3 en IMAP clients

Er zijn zeer veel POP3- en IMAP4-clients. Ook Microsoft Outlook en Outlook Express ondersteunen POP3 en IMAP4.

Voor deze cursus verkiezen we gebruik te maken van de LINUX mail client Mozilla Mail. Het ondersteunt POP3 en IMAP4 en dit zowel beveiligd als onbeveiligd.

- Installeer Mozilla Mail m.b.v. rpm.
- Configureer een POP3-account die gebruik maakt van jouw POP3-server en test deze uit.
- Configureer een IMAP4-account die gebruik maakt van jouw server en test deze uit.
- Configureer een beveiligde POP3-account die gebruik maakt van jouw server en test deze uit.
- Configureer een beveiligde IMAP4-account die gebruik maakt van jouw server en test deze uit.

8.3 POP3

POP3 protocol

POP3 (de opvolger van POP2) controleert de gebruikersnaam en het paswoord van de gebruiker, en verplaatst vervolgens de berichten voor de gebruiker van de mailserver naar de mailclient. POP3 gebruikt TCP poort 110. Het staat beschreven in RFC 1939.

De basis POP3-commando's zijn

`USER name`
Hiermee geef je de gebruikersnaam op waarmee ingelogd wordt.

`PASS string`
Hiermee geef je het paswoord op dat bij de gebruikersnaam hoort.

`STAT`
Hiermee vraag je het aantal ongelezen berichten/bytes op.

`LIST [msg]`

Hiermee vraag je de grootte van bericht *msg* of van alle berichten op.

`RETR msg`
Hiermee haal je bericht *msg* af van de server.

`DELE msg`
Hiermee verwijder je bericht *msg* van de server.

`NOOP`
Dit commando doet niets behalve een antwoord van de server vragen.

`RSET`
Hiermee maak je alle verwijderingen ongedaan en worden de berichten hernummerd vanaf 1.

`QUIT`
Hiermee beëindig je de sessie.

Net zoals SMTP kan je POP3 ook vanuit een telnetverbinding uitvoeren. Bijvoorbeeld op volgende manier:

```
telnet comp1.dom1.edu 110
```

Een voorbeeld van een POP3 sessie vind je hieronder:

```
USER user1
+OK
PASS p@ssw0rd
+OK Logged in.
LIST
+OK 12 messages:
1 1588
2 1584
3 722
4 1388
5 1899
6 2145
7 783
8 2167
9 2082
10 734
11 4613
12 731
.
RETR 1
+OK 1588 octets

>>>>> output omitted

subject: test

test
.
DELE 1
+OK Marked to be deleted.
QUIT
+OK Logging out, messages deleted.
```

```
Connection closed by foreign host.
```

8.4 IMAP4

IMAP4 protocol

IMAP4 is een alternatief voor POP3. In tegenstelling tot POP3 biedt het de mogelijkheid de mailbox op de client en op de server te synchroniseren. Hierbij worden de berichten zowel op de server als op de client bewaard, en worden de berichten op beide systemen up-to-date gehouden. Veranderingen aan de mailbox aan de client-kant worden automatisch doorgevoerd op de server en andersom.

IMAP4 werkt op TCP-poort 143 en wordt beschreven in RFC 2060

De werking van IMAP4 is complexer dan die van POP3. Daarom wordt het in deze cursus niet gedemonstreerd a.d.h.v. een telnet-verbinding.

Probeer echter wel de mogelijkheden van IMAP4 uit door gebruik te maken van een IMAP4-client.

Hoofdstuk 9

9 Aliases database

We zagen reeds dat we met het bestand **/etc/mail/local-host-names** kunnen regelen welke berichten door Sendmail aanvaard worden en welke niet. Eens het bericht aanvaard, moeten we nog bepalen wat er met het bericht moet gebeuren: moet het in de mailbox van een lokale gebruiker gestoken worden? Moet het verdeeld worden over de mailboxen van verschillende gebruikers? Of moet het doorgestuurd worden naar iemand anders? Zo zou het bijvoorbeeld kunnen dat een gebruiker de firma verlaten heeft, en zijn e-mails doorgestuurd moeten worden naar het nieuwe adres. Zulke beslissingen worden genomen op basis van de Aliases database.

Functies van de Aliases database

De Aliases database heeft drie functies:

- Specifiëren van nicknames voor individuele gebruikers
- Berichten doorsturen naar andere hosts
- Mailing lists aanmaken
- Berichten archiveren

Hoewel we spreken over de Aliases Database, gaat het hier om een gewoon tekstbestand. Later zullen we zien dat Sendmail voor sommige configuraties ook met binaire databases werkt.

De Aliases database bevindt zich in het bestand **/etc/aliases**. Het bestand bestaat uit regels van volgende vorm:

```
alias: recipient
```

Na elke wijziging in het bestand /etc/aliases, moet je volgend commando uit voeren:

```
newaliases
```

9.1 Nicknames

Nicknames

Nicknames worden gebruikt om berichten die bestemd zijn voor een bepaalde persoon, door te sturen naar een andere persoon. Volgende regel zorgt er bijvoorbeeld voor dat alle e-mails die bestemd zijn voor root, doorgestuurd worden naar user1:

```
root: user1
```

9.2 Berichten doorsturen naar andere hosts

Forwarding

De eerste situatie waarin je dit kan gebruiken, is het doorsturen van berichten naar een ander domein. Indien onze mailserver berichten aanvaardt voor het domein dom1.edu, dan kan je er bijvoorbeeld

voor zorgen dat berichten die bestemd zijn voor user1@dom1.edu doorgestuurd worden naar user2@dom2.edu. Dit kan je realiseren door volgende regel op te nemen in het bestand /etc/aliases van de mailserver van dom1.edu:

```
user1: user2@dom2.edu
```

Een tweede situatie waarin je dit kan gebruiken, is de volgende: je beschikt niet over één mailserver, maar over twee mailservers in hetzelfde domein: comp1.dom1.edu en mail1.dom1.edu. De helft van de gebruikers heeft een mailbox op comp1.dom1.edu, de andere helft op mail1.dom1.edu. De MX-records op het Internet zorgen ervoor dat alle mails voor dom1.edu aankomen op comp1.dom1.edu.

In dit geval moeten alle berichten voor gebruikers wiens mailbox zich op mail1.dom1.edu bevinden, doorgestuurd worden naar mail1.dom1.edu. Stel dat je de berichten van user1 wil doorsturen naar mail1.dom1.edu, dan kan je dit doen door volgende regel toe te voegen aan het bestand /etc/aliases van comp1.dom1.edu:

```
user1: user1@mail1.dom1.edu
```

Het bericht wordt dus binnen hetzelfde domein doorgestuurd naar een andere mailserver.

Indien het echter om een grote groep gebruikers gaat, kan je beter een apart bestand maken waarin deze gebruikers opgenomen worden.

In het bestand /etc/mail/sendmail.mc van comp1.dom1.edu neem je volgende regel op:

```
define(`ALIAS_FILE',`/etc/aliases, /etc/aliases_mail1')
```

In het bestand /etc/aliases_mail1 van comp1.dom1.edu neem je alle gebruikers op wiens mailbox zich op mail1.dom1.edu bevinden:

```
user1: user1@mail1.dom1.edu
```

Uiteraard moet je er, m.b.v. /etc/local-host-names, nog voor zorgen dat mail1.dom1.edu bereid is berichten voor het domein mail1.dom1.edu aan te nemen.

9.3 Mailing lists aanmaken

Mailing lists

Stel dat je een e-mailadres support@dom1.edu wil inrichten. Dit bericht moet echter aan alle leden van het support-team verdeeld worden. Hiervoor kan je volgende regel opnemen in /etc/aliases:

```
support: bram, bart, thierry, eric, luc
```

Elk bericht voor support@dom1.edu wordt nu doorgestuurd naar de gebruikers bram, bart, thierry, eric en luc op dezelfde mailserver.

9.4 Berichten archiveren

Archiveren

Het zou kunnen dat je alle berichten die aan support@dom1.edu verstuurd worden, wil archiveren in een bestand /var/archives/support. Hiervoor pas je /etc/aliases als volgt aan:

support: bram, bart, thierry, eric, luc, support-archive

support-archive: /var/archive/support

In dit geval wordt een kopie van elk bericht aan de groep support opgeslagen in het bestand /var/archive/support.

9.5 Personal Mail Aliases

.forward

Als een gebruiker wil dat zijn berichten doorgestuurd worden naar een ander e-mailadres, kan hij dit doen door aan de systeem administrator te vragen wijzigingen aan te brengen in het bestand /etc/aliases.

Hij kan dit echter zelf ook doen. Elk bericht dat toekomt in de mailbox van een gebruiker, kan doorgestuurd worden naar een ander e-mailadres door dit nieuwe e-mail adres op te nemen in het bestand **.forward** van de homedirectory van de gebruiker.

Zo zal de regel **user2@dom2.edu** in het bestand **/home/user1/.forward** van **comp1.dom1.edu** ervoor zorgen dat alle e-mails voor **user1@dom1.edu** doorgestuurd worden naar **user2@dom2.edu**. User1 kan deze regel zelf aanbrengen, er is geen tussenkomst van de systeem administrator nodig.

Hoofdstuk 10

10 Outgoing addresses (Generics)

De Generics database wordt gebruikt om uitgaande e-mailadressen om te vormen. Stel dat iemand een e-mail stuurt naar Bart.Mendez@dom1.edu, maar dat deze mail lokaal afgeleverd wordt aan user1@dom1.edu (o.w.v. een alias).

Omvormen van uitgaande e-mail adressen

Als user1 een reply doet op deze mail, dan wordt de mail verstuurd als user1@dom1.edu. Dit is niet fraai. Het zou beter zijn indien alle uitgaande mail van user1 verstuurd wordt als Bart.Mendez@dom1.edu.

Dit kan je doen via de Generics database.

Een Generics database opzetten doe je door volgende lijn toe te voegen aan sendmail.mc:

```
FEATURE(`genericstable')
```

Vervolgens kan je het bestand /etc/mail/genericstable aanvullen met de nodige records:

```
user1 Bart.Mendez@dom1.edu
```

Het bestand genericstable moet nog van een tekstbestand omgezet worden in een hash database:

```
makemap hash genericstable.db < genericstable
```

Verder is het ook nog nodig op te geven voor welke domeinen het omzetten van afzenderadressen dient te gebeuren. Dit doe je met volgende regel in sendmail.mc:

```
GENERIC_DOMAIN(`dom1.edu')
```

Dit zou er echter voor zorgen dat enkel die adressen aangepast worden, waarvan het gedeelte na het @-teken gelijk is aan “dom1.edu”. Het adres user1@dom1.edu wordt dus wél aangepast, terwijl het adres user1@comp1.dom1.edu niet aangepast wordt.

Om ervoor te zorgen dat ook dit laatste e-mail adres aangepast wordt, neem je best volgende regel op in /etc/mail/sendmail.mc:

```
FEATURE(`generics_entire_domain')
```

De Generics database heeft als nadeel dat het niet werkt op e-mails die lokaal afgeleverd worden.

In het geval de eindgebruikers gebruik maken van mailclients die SMTP gebruiken om berichten te verzenden, dan kan deze het uitgaande e-mailadres zelf instellen bij de configuratie van de account. Het is eenvoudiger de gebruikers zelf hun uitgaand e-mail adres te laten instellen dan het te definiëren via generics of de user database.

Hoofdstuk 11

11 User database

De User database verenigt de mogelijkheden van de Aliases database en van de User database: het laat toe zowel inkomende als uitgaande e-mailadressen te wijzigen.

User database

De User Database kan je enkel gebruiken als je volgende regel toevoegt aan /etc/mail/sendmail.mc:

```
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')
```

Nu kan je aan /etc/mail/userdb.db vergelijkbare regels toevoegen als aan /etc/aliases. Enkel de syntax is een beetje verschillend.

Om ervoor te zorgen dat berichten voor Bart.Mendez@dom1.edu afgeleverd worden aan gebruiker user1, kan je volgende regel toevoegen aan /etc/mail/userdb.db

```
Bart.Mendez:maildrop user1
```

Dit heeft hetzelfde effect als volgende regel toevoegen aan /etc/aliases:

```
Bart.Mendez: user1
```

Met de User database kan je er echter ook voor zorgen dat adressen van uitgaande mails herschreven worden. Als je wil dat alle berichten van user1 uitgestuurd worden als berichten van Bart.Mendez@dom1.edu, kan je hiervoor volgende regel toevoegen aan /etc/mail/userdb.db:

```
user1:mailname Bart.Mendez@dom1.edu
```

Samengevat komt het gebruik van de User database hierop neer:

- Gebruik het woord **maildrop** om het inkomende e-mailadres aan te passen.
- Gebruik het woord **mailname** om uitgaande e-mailadressen aan te passen.

De user database wordt toegepast na /etc/aliases, en voor de .forward bestanden.

Hoofdstuk 12

12 Address Mappings (Virtuser)

Address Mappings zijn gelijkaardig aan aliases in die zin dat ze ervoor zorgen dat berichten naar een andere bestemming doorgestuurd kunnen worden. Address Mappings zijn echter geschikter dan aliases als je berichten naar andere domeinen wil doorsturen.

Berichten doorsturen naar andere domeinen

Address Mappings worden gebruikt om

- Berichten bestemd voor een volledig domein door te sturen naar één e-mail adres;
- Berichten bestemd voor een gebruiker uit één domein door te sturen naar een gebruiker uit een ander domein;
- Alle berichten voor een volledig domein door te sturen naar een ander domein.

De voorwaarden waaronder Address Mappings kunnen werken:

- In DNS moet een MX-record naar jouw mailserver wijzen, zodat berichten voor een bepaald domein bij jou terecht komen
- Jouw mailserver moet de berichten voor het domein aanvaarden. Dit kan je doen door het domein toe te voegen aan /etc/mail/local-host-names.
- Jouw mailserver moet geconfigureerd zijn om met Address Mappings te werken. Dit kan je bereiken door volgende regel op te nemen in het bestand sendmail.mc:

```
FEATURE(`virtusertable')
```

De werking van virtusertable wordt uitgelegd a.d.h.v. een voorbeeld:

```
[root]#cat /etc/mail/local-host-names
dom1.edu
comp1.dom1.edu
bedrijf.com
firma.be
imaginary.com
outofbusiness.com
other.org

[root]#cat /etc/mail/virtusertable
sales@bedrijf.com          user1
info@firma.be              Bart.Mendez@xyz.be
@imaginary.com             user1
sales@outofbusinnes.com    error: address invalid
@other.org                 %1@local.org

[root]#makemap hash virtusertable.db \
< virtusertable
[root]#/etc/init.d sendmail restart
```

De eerste regel uit /etc/mail/virtusertable zorgt ervoor dat alle berichten die gericht zijn aan sales@bedrijf.com in de mailbox van user1 terechtkomen.

De tweede regel zorgt ervoor dat alle berichten die bestemd zijn voor info@firma.be doorgestuurd worden naar het externe e-mail adres Bart.Mendez@xyz.be.

De derde regel zorgt ervoor dat alle berichten die bestemd zijn voor het domein imaginary.com in de mailbox van user1 terechtkomen.

De vierde regel zorgt ervoor dat de afzender van een bericht aan sales@outofbusiness.com een foutboodschap krijgt en dat het bericht verwijderd wordt.

De laatste regel zorgt ervoor dat alle berichten voor het domein other.org doorgestuurd worden naar local.org. Hierin stelt %1 de naam van de ontvanger van het bericht voor.

Dit laatste is zeer handig als je over twee domeinnamen beschikt, en je wil alle e-mails die naar het eerste domein gestuurd worden, doorsturen naar het tweede domein.

Hoofdstuk 13

13 Relay domains

In het begin van deze cursus hebben we volgende regel toegevoegd aan Sendmail:

```
FEATURE(`promiscuous_relay')
```

Relaying

Hiermee zorgen we ervoor dat Sendmail alle berichten die het niet lokaal kan afleveren, doorstuurt naar een andere MTA. Dit was vroeger het standaardgedrag van Sendmail. Aangezien dit echter een openstaande deur vormt voor het versturen van Spam via iemand anders' MTA, werd dit standaardgedrag aangepast in versie 8.9. Sinds deze versie stuurt Sendmail geen enkel bericht meer door, tenzij het hiervoor geconfigureerd is.

We verwijderen de regel

```
FEATURE(`promiscuous_relay')
```

uit het bestand /etc/mail/sendmail.mc, maken een nieuw sendmail.cf bestand (m.b.v. het commando **m4**) en herstarten Sendmail (m.b.v. **/etc/init.d/sendmail restart**). Test nu of Sendmail nog berichten accepteert die binnen komen via SMTP. Dit mag niet meer werken, tenzij de SMTP-verbinding vanop de server zelf gestart wordt. Sendmail laat namelijk standaard enkel relaying toe vanaf localhost. Test dit dus uit door een SMTP-verbinding te starten vanaf een andere PC.

/etc/mail/relay-domains

Je kan het relay gedrag van Sendmail beïnvloeden door het bestand **/etc/mail/relay-domains** aan te passen.

Elke host die in dit bestand voorkomt, mag de server gebruiken voor relaying. Berichten van deze hosts worden dus doorgestuurd naar andere mailservers. Je kan in dit bestand dus alle hosts van je eigen domein opnemen, om ervoor te zorgen dat jouw eindgebruikers mails naar buiten mogen sturen:

```
dom1.edu
```

Het toevoegen van dom1.edu aan /etc/mail/relay-domains zorgt ervoor dat alle berichten van of naar dom1.edu toegelaten worden.

Merk op dat je Sendmail opnieuw moet starten na elke wijziging aan dit bestand.

Hoofdstuk 14

14 Access database

De access database wordt gebruikt voor volgende zaken:

- Configureren van relay servers
- Spam control

Access database

Je kan er m.b.v. de access database voor zorgen dat bepaalde berichten

- verworpen worden;
- doorgelaten worden om lokaal verwerkt te worden;
- doorgelaten worden om te worden gerelayed naar andere mailservers.

In Fedora is de access database standaard ingeschakeld, en laat ze relaying toe van en naar localhost (de mailserver zelf). Op andere distributies kan het zijn dat je de access database nog moet activeren. Dit doe je m.b.v. volgende regel in sendmail.mc:

```
FEATURE(`access-db')
```

Nadat je dit gedaan hebt, kan je de access database het eenvoudigst bekijken m.b.v. webmin:

- Surf naar http://localhost:10000.
- Log in als root.
- Ga naar Servers -> Sendmail Configuration -> Spam Control (access).

Veranderingen die je via webmin aanbrengt, worden eerst weggeschreven naar het bestand **/etc/mail/access**.

Vervolgens wordt het programma **makemap hash /etc/mail/access.db < /etc/mail/access** uitgevoerd. Hiermee wordt de access database van een tekstbestand omgezet in een hash database die leesbaar is voor Sendmail.

Alle records in /etc/mail/access bestaan uit twee velden: het adres veld en het actie veld

14.1 Adres veld

Het adres veld

Het adres veld kan volgende zaken bevatten:

- een gebruiker
- een e-mailadres
- een source IP-adres
- een netwerkadres
- een naam van een domein

14.2 Actieveld

Het actieveld

In het actieveld staat wat er met e-mails moet gebeuren die verzonden werden vanaf het adres dat in het adres veld vermeld staat.

- OK: het bericht wordt aanvaard als het bestemd is om lokaal verwerkt te worden. Het wordt niet gerelayed.
- RELAY: relay het bericht van het opgegeven adres of naar het opgegeven adres. Relay betekent ook dat berichten aanvaard worden om lokaal verwerkt te worden.
- REJECT: het bericht wordt niet aanvaard. De afzender krijgt een standaard foutboodschap.
- DISCARD: het bericht wordt verworpen, de zender krijgt hiervan geen verwittiging.
- ERROR: *code text*: Het bericht wordt verworpen, de afzender krijgt een bericht dat een RFC 821 response code bevat, samen met de tekst die gespecifieerd is in het adresveld

14.3 De access database inschakelen

makemap

Als je het bestand /**etc/mail/access** manueel aanpast (i.e. zonder gebruik te maken van webmin), dan moet je eraan denken zelf het tekstbestand om te zetten in het hash bestand. Dit doe je met volgend commando:

makemap hash /etc/mail/access.db < /etc/mail/access

14.4 Enkele voorbeelden

```
cyberspammer.com          ERROR:"550 rejected"
okay.cyberspammer.com     OK
sendmail.org              RELAY
128.32                    RELAY
IPv6:1:2:3:4:5:6:7        RELAY
```

Hoofdstuk 15

15 Domain mappings (domaintable)

Domaintable wordt gebruikt om de overgang van een oude domeinnaam naar een nieuwe te vereenvoudigen.

Domain mapping past het `To:` adres aan van alle berichten die verstuurd worden vanuit jouw server. Ook het `To:` adres van berichten die gerelayed worden door jouw server of afgeleverd worden op jouw server, worden aangepast.

Het `From:` adres van gerelayede berichten en berichten van lokale gebruikers wordt ook aangepast.

domaintable

Om domain mappings te gebruiken, moet je volgende regel toevoegen aan sendmail.mc:

```
FEATURE(`domaintable')
```

Vervolgens moet opgegeven worden welke domeinen op elkaar afgestemd moeten worden. Stel bijvoorbeeld dat je je oude domeinnaam **ouddomein.be** wil vervangen door **nieuwdomein.be**. Je kan dan volgende regel opnemen in het bestand /etc/mail/domaintable:

```
ouddomein.be          nieuwdomein.be
```

Dit bestand moet met het commando makemap omgezet worden van een tekstbestand naar een hash database (één regel):

```
makemap hash /etc/mail/domaintable
/etc/mail/domaintable.db
```

Verder moet je erop te letten dat het MX-record van beide domeinen naar jouw mailserver verwijzen. Hoe je dit doet, werd in hoofdstuk 6 behandeld.

Tenslotte moet jouw mailserver ook bereid zijn berichten voor beide domeinen te accepteren. Dit doe je door de feature “**use_cw_file**” op te nemen in **/etc/mail/sendmail.mc**, en beide domeinen op te nemen in het bestand **/etc/mail/local-host-names**.

Hoofdstuk 16

16 Spam filtering

Naar schatting 80 procent van alle e-mails is Spam. De mailboxen van de gebruikers hiervan vrijwaren, is geen evidente opgave. Gelukkig biedt Sendmail een aantal mogelijkheden om dit probleem aan te pakken.

16.1 Access database tags

Access database tags

De werking van de access database werd hogerop reeds besproken. Door deze database in te schakelen, is het mogelijk een groot deel van de spamberichten tegen te houden. Om de database op een doeltreffende manier te kunnen configureren, gaan we hier nog even verder in op de mogelijkheden ervan.

Standaard gebeurt de controle van de access database enkel op het adres van de afzender. Dit kan je aanpassen m.b.v. **tags**.

Enkele voorbeelden:

```
From:spammer@some.dom    REJECT
To:friend.domain         RELAY
Connect:friend.domain    OK
Connect:from.domain      RELAY
From:good@another.dom    OK
From:another.dom         REJECT
```

Het adresveld van de access database entries wordt nu voorafgegaan door het woord *From:*, *To:* of *Connect:*.

De betekenis hiervan is de volgende:

- From: enkel het afzender adres wordt gecontroleerd. Dit is het standaard gedrag, tenzij de FEATURE *blacklist_recipients* aan staat.
- To: enkel het adres van de ontvanger wordt gecontroleerd.
- Connect: het opgegeven adres is het adres van het systeem aan de andere kant van de SMTP verbinding.

Het voorbeeld van hierboven heeft volgend effect:

- E-mails van *spammer@some.dom* worden tegengehouden, maar je kan er zelf nog wel berichten naartoe sturen, zelfs al staat de FEATURE(`blacklist_recipients') aan.
- Relaying naar *friend.domain* wordt toegestaan, maar niet van *friend.domain.*
- Een verbinding vanaf datzelfde domein is toegestaan, zelfs al komt het voor in een DNS blacklist.

- Relaying is toegestaan vanaf *from.domain*, maar niet naar dat domein. (*Connect* controleert enkel uitgaande relaying, inkomende relaying wordt gecontroleerd d.m.v. de *To* tag.)
- De laatste twee regels zorgen ervoor dat e-mails van *good@another.dom*, toegelaten worden, maar alle andere afzenders van dit adres worden geweigerd.

Vergeet niet het bestand /etc/mail/access om te vormen naar het hash bestand /etc/mail/access.db m.b.v. het commando **makemap**.

16.2 FEATURE blacklist_recipients

Blacklist_ recipients

Als je gebruik maakt van volgende regel in sendmail.mc

```
FEATURE(`blacklist_recipients')
```

dan kan je ervoor zorgen dat bepaalde gebruikers of computers in jouw domein geen e-mails meer ontvangen.

Enkele voorbeelden uit /etc/mail/access:

```
badlocaluser@           ERROR:550 Mailbox disabled for
this username
host.mydomain.com       ERROR:550 That host does not
accept mail
user@otherhost.mydomain.com     ERROR:550 Mailbox
disabled
```

Hiermee zorg je ervoor dat volgende gebruikers geen e-mail meer kunnen ontvangen:

- *badlocaluser@mydomain.com*
- elke gebruiker uit *host.mydomain.com*
- de gebruiker *user@otherhost.mydomain.com*

Merk op dat een lokale gebruiker in deze lijst gevolgd wordt door een @. Dit zorgt ervoor dat er een onderscheid gemaakt kan worden tussen gebruikers en computers of domeinen. Zo zorgt onderstaand voorbeeld ervoor dat geen e-mail meer afgeleverd wordt aan de gebruiker *spammer@aol.com* en aan geen enkele gebruiker uit het domein *cyberspammer.com.*

```
spammer@aol.com          REJECT

cyberspammer.com         REJECT
```

16.3 DNS blacklists

DNS blacklists

Een DNS-blacklist is een database van spammers die in DNS beschikbaar is. Er bestaan meerdere DNS-blacklists, de eerste was RBL ("*Realtime Blackhole List*") van het MAPS (Mail Abuse Prevention System) project (http://mail-abuse.org).

Om e-mails tegen te houden die afkomstig is van een DNS-blacklist, kan je volgende regel toevoegen aan sendmail.mc:

```
FEATURE(`dnsbl')
```

Hiermee zorg je ervoor dat Sendmail alle mails tegenhoudt die vermeld staat in de oorspronkelijke *Realtime Blackhole List database*.

Sinds enkele jaren moet je je laten registreren voor deze service. Zie hiervoor http://mail-abuse.org.

Je kan ook andere blacklists gebruiken door een extra argument toe te voegen aan de dnsbl FEATURE. Bijvoorbeeld:

```
FEATURE(`dnsbl', `dnsbl.example.com')
```

Om te vermijden dat jouw eigen domein gecheckt wordt door de blacklist, kan je het toevoegen aan de access database:

```
Connect:10.1            OK
Connect:127.0.0.1       RELAY
```

Deze twee voorbeelden betekenen dat alle verbindingen vanaf het 10.1 netwerk naar de server toegelaten worden als het bericht lokaal afgeleverd wordt. Als de verbinding vanaf de localhost gemaakt wordt (127.0.0.1), wordt ook relaying toegelaten. De betekenis van het woord *connect* wordt hieronder verder uitgelegd.

16.4 Spamassassin

Spamassassin

Sendmail zelf plaatst geen berichten in de mailboxen van de gebruikers, dit gebeurt door het programma procmail, dat standaard mee geïnstalleerd wordt met Sendmail. M.b.v. procmail is het mogelijk e-mails eerst aan externe programma's door te geven voordat de berichten in de mailboxen van de gebruikers afgeleverd worden. Een typische toepassing hiervan is **spamassassin**.

De website van Spamassassin is http://spamassassin.apache.org. Hier vind je o.a. de source code van deze spam-filter. Fedora biedt echter ook rpm's aan om Spamassassin te installeren. Let wel op: om Spamassassin te installeren heb je ook de **perl** rpm's nodig.

Spamassassin installeren

De eenvoudigste manier om Spamassassin te installeren op Fedora, is met volgend commando:

```
yum install spamassassin
```

Yum controleert namelijk zelf welke pakketten er nodig zijn, de zogenaamde **dependencies**, en installeert deze automatisch mee.

Spamassassin starten doe je met

```
/etc/init.d/spamassassin start
```

Spamass-milter

Spamassassin is geen onderdeel van Sendmail, het is een extern programma. Daarom hebben we een interface nodig tussen Spamassassin en Sendmail. Sinds versie 8.11 biedt Sendmail een interface om via API's te communiceren met andere programma's. Deze interface wordt **Milter** (Mail Filter) genoemd. Voor Spamassassin bestaat er een extra pakket dat de verbinding tussen Spamassassin en Milter verzorgt, namelijk **spamass-milter**.

De officiële website van Spamass-milter is http://savannah.nongnu.org/projects/spamass-milt/. Hier kan je wel de source code downloaden, maar niet de rpm's. Voor de rpm's kan je o.a. terecht op http://dag.wieers.com/packages/spamass-milter/.

Eens Spamass-milter geïnstalleerd, kan je het starten met volgend commando:

```
/etc/init.d/spamass-milter start
```

Spamassassin koppelen aan Sendmail

Nu moeten we nog aan Sendmail vertellen dat het alle berichten eerst door Spamassassin moet laten controleren, voordat het in de mailbox van de gebruiker afgeleverd wordt. Dit doe je door volgende regel toe te voegen aan /etc/mail/sendmail.mc (op één regel):

```
INPUT_MAIL_FILTER(`spamassassin',
`S=local:/var/run/sendmail/spamass.sock,
F=,T=C:15m;S:4m;R:4m;E:10m')
```

Spamassassin testen

Spamassassin checkt of binnenkomende berichten als spam beschouwd kunnen worden. Het verwijdert echter geen spamberichten. Wat het wel doet is een header-lijn toevoegen aan het bericht, en het onderwerp laten voorafgaan door het woord [SPAM]. Het verwijderen van de berichten gebeurt meestal door filterregels in te stellen op de client computer.

Om te testen of dit werkt, worden volgende mails meegeleverd met Spamassassin:

`/usr/share/doc/spamassassin-x.x/sample-spam.txt`

`/usr/share/doc/spamassassin-x.x/sample-nonspam.txt`

Deze uitleg laat een heel aantal vragen over Spamassassin onbeantwoord. De website

http://savannah.nongnu.org/projects/spamass-milt/ is echter een uitstekend startpunt om meer te leren over dit product.

Hoofdstuk 17

17 Antivirus software

De Milter-interface van Sendmail wordt ook gebruikt door antivirussoftware. Verschillende firma's hebben antivirussoftware geschreven die kan ingeplugd worden in Sendmail m.b.v. Milter. Een goede oplossing die eenvoudig te implementeren is, is **AntiVir Milter for Sendmail**.

Antivir Milter

Een trial-versie van deze software kan je vinden op de website van Antivir: http://www.antivir.de. Een duidelijke installatie- en configuratie handleiding is eveneens beschikbaar op deze website: http://www.antivir.de/fileadmin/user_files/downloads/handbuecher/english/milter-engl.pdf.

Let wel op: voor een versie met up-to-date virusdefinitiebestanden, dient wel betaald te worden.

Hoofdstuk 18

18 Sendmail en firewalls

Je mailsysteem wordt nooit rechtstreeks met het Internet verbonden. Meestal zal je werken met een Demilitarized Zone (DMZ) waarin een relay server staat, en staat de mailserver met de mailboxen binnen het beveiligde netwerk.

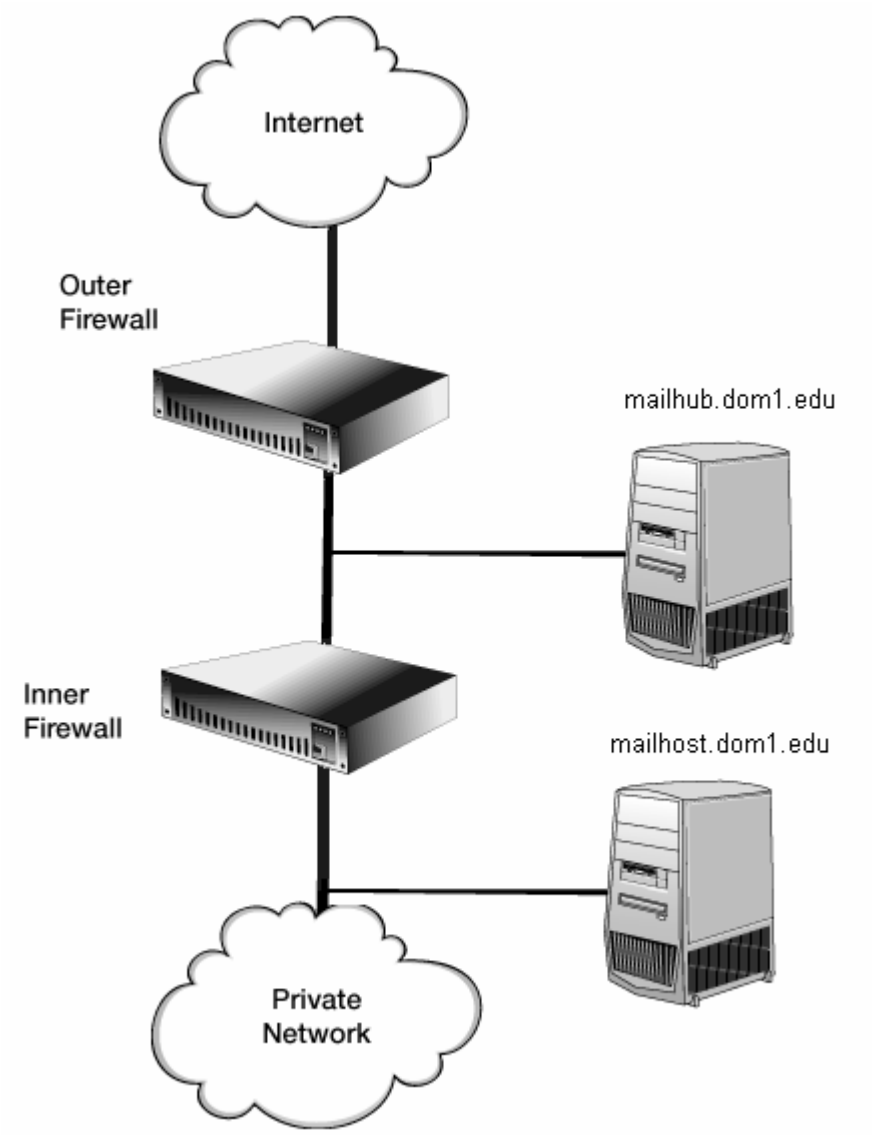
DMZ

Inkomende berichten komen steeds toe op de mailserver in de DMZ. Deze geeft ze door aan de interne mailserver, waar de gebruiker ze kan afhalen.

Uitgaande berichten worden steeds afgeleverd aan de interne mailserver. Deze geeft de berichten door aan de mailserver in de DMZ, die ze op zijn beurt doorgeeft aan de mailserver van de bestemming.

Om dit te verduidelijken bekijken we volgend voorbeeld:

- Stel dat de interne mailserver **mailhost.dom1.edu** noemt.
- De externe mailserver noemt **mailhub.dom1.edu**
- Alle interne gebruikers gebruiken **mailhub.dom1.edu** voor het afhalen én verzenden van hun berichten
- De MX records wijzen naar **mailhub.dom1.edu** zodat alle inkomende berichten op de mailserver in de DMZ terecht komen.



SMARTHOST

Om ervoor te zorgen dat mailhost zijn uitgaande berichten doorgeeft aan mailhub, voegen we volgende regel toe aan het bestand sendmail.mc van mailhost:

```
define(`SMART_HOST',`mailhub.dom1.edu')
```

MAIL_HUB

Om ervoor te zorgen dat mailhub de inkomende berichten doorgeeft aan mailhost, voegen we volgende regel toe aan het bestand sendmail.mc van mailhub:

```
define(`MAIL_HUB', `mailhost.dom1.edu')
```

Dit werkt enkel indien je mailhub.dom1.edu en mailhost.dom1.edu zodanig configureert dat ze berichten mogen relayen voor het domein dom1.edu (via **/etc/mail/relay-domains**).

Hoofdstuk 19

19 Mail Queue

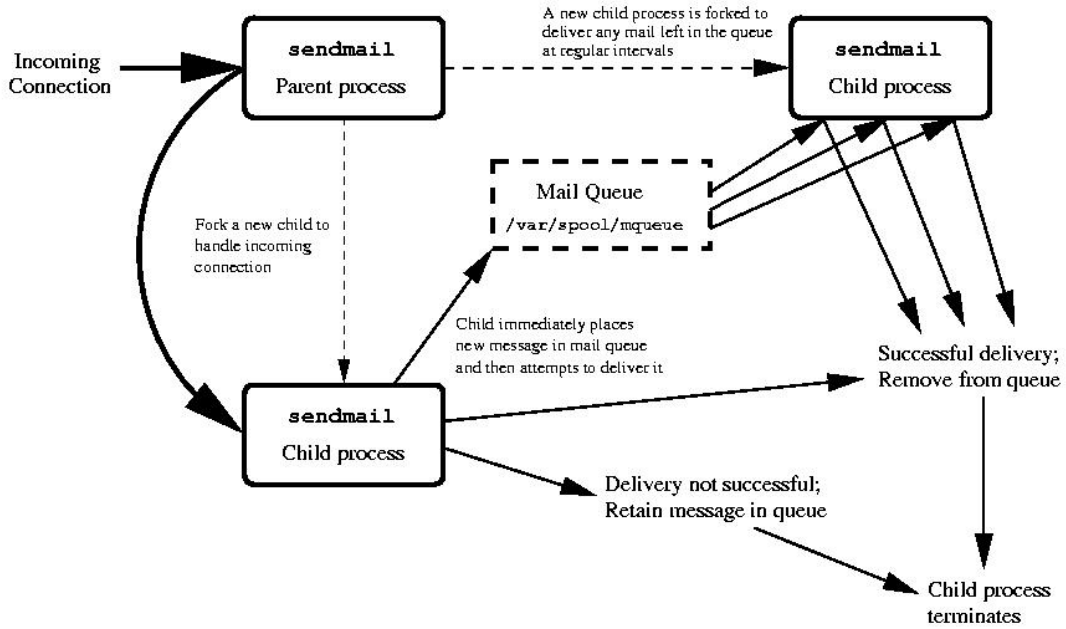
In een normale configuratie draait Sendmail op de achtergrond, waar het wacht op nieuwe berichten. Als een nieuw bericht toekomt, wordt een Sendmail **child** process opgestart om het bericht te verwerken. De **parent** wacht verder op inkomende verbindingen.

/var/spool/mqueue

Als een bericht binnen komt, plaatst het child process dit bericht in de mail queue. Standaard is dit /var/spool/mqueue.

Als het bericht onmiddellijk afgeleverd kan worden, wordt het afgeleverd en uit de queue verwijderd. Als het niet onmiddellijk afgeleverd kan worden, blijft het in de queue zitten en stopt het child process.

Berichten die in de queue achter blijven, blijven daar totdat de queue opnieuw geprocessed wordt. Standaard zal het parent Sendmail process op regelmatige tijdstippen een child process opstarten om de queue te processen.



Als een bericht gedurende vier uren niet afgeleverd kan worden, zal de afzender hiervan verwittigd worden. Na vijf dagen staakt Sendmail zijn pogingen om het bericht te versturen, verwijdert het uit de queue en verwittigt het de afzender hiervan.

De queue bekijken kan je op drie manieren:

- Bekijk de folder **/var/spool/mqueue.**
- Gebruik Webmin -> Servers -> Sendmail Configuration -> Mail Queue.
- Gebruik het commando **mailq.**

Hoofdstuk 18

20 Literatuurlijst

sendmail, 3th edition, Bryan Costales with Eric Allman, ISBN 1-56592-839-3

sendmail Desktop Reference, Bryan Costales & Eric Allman, ISBN 1-56592-278-6

Linux Sendmail Administration, Craig Hunt, ISBN 0-7821-2737-1

sendmail Cookbook, Craig Hunt, ISBN 0-596-00471-0