2014-2015

Portfolio: Internettechnologie & Systeembeheer

Een OSPF-netwerk met behulp van RouterOS

Voorbereiding

Om deze oefening te maken, maak ik gebruik van virtuele machines onder VMWare Workstation 10. Hierop draai ik als operating system RouterOS van Mikrotik.

Ik maak één virtuele machine met één netwerkinterface aan, die als basis dient om de andere virtuele machines te klonen. Dit doe ik voor mijzelf, om het overzicht te bewaren.

Dus mijn werkwijze is als volgt:

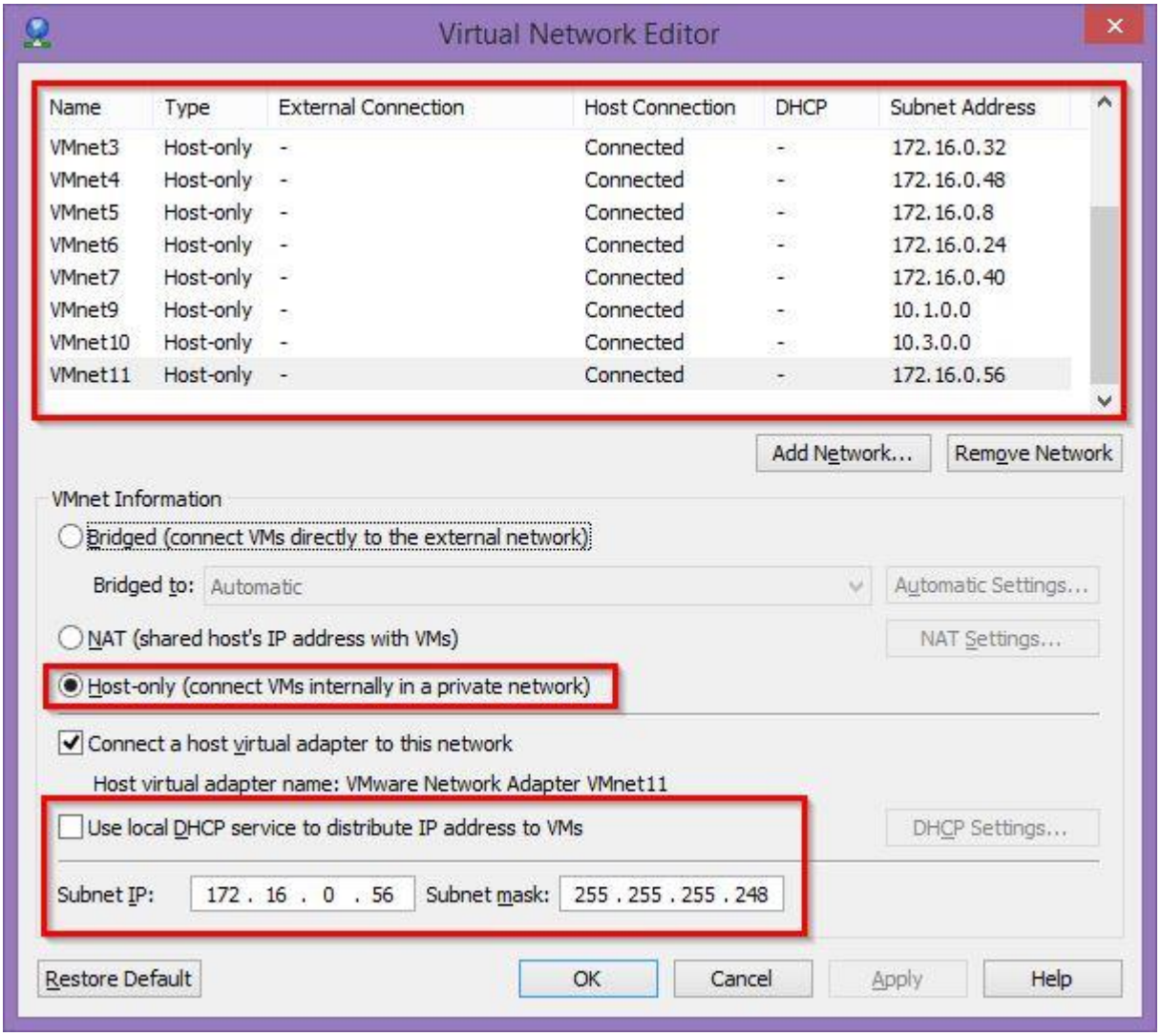
- Klonen van basismachine met één interface
- Router-identiteit opgeven in RouterOS
- De bestaande interface een naam en een IP geven in RouterOS
- De virtuele machine afsluiten
- Interface bijmaken in VMWare Workstation
- De bestaande interface een naam en een IP geven in RouterOS
- De virtuele machine afsluiten
- …

En dit zoveel maal als er interfaces bestaan. Dit kan misschien sneller, maar zo houd ik een goed overzicht.

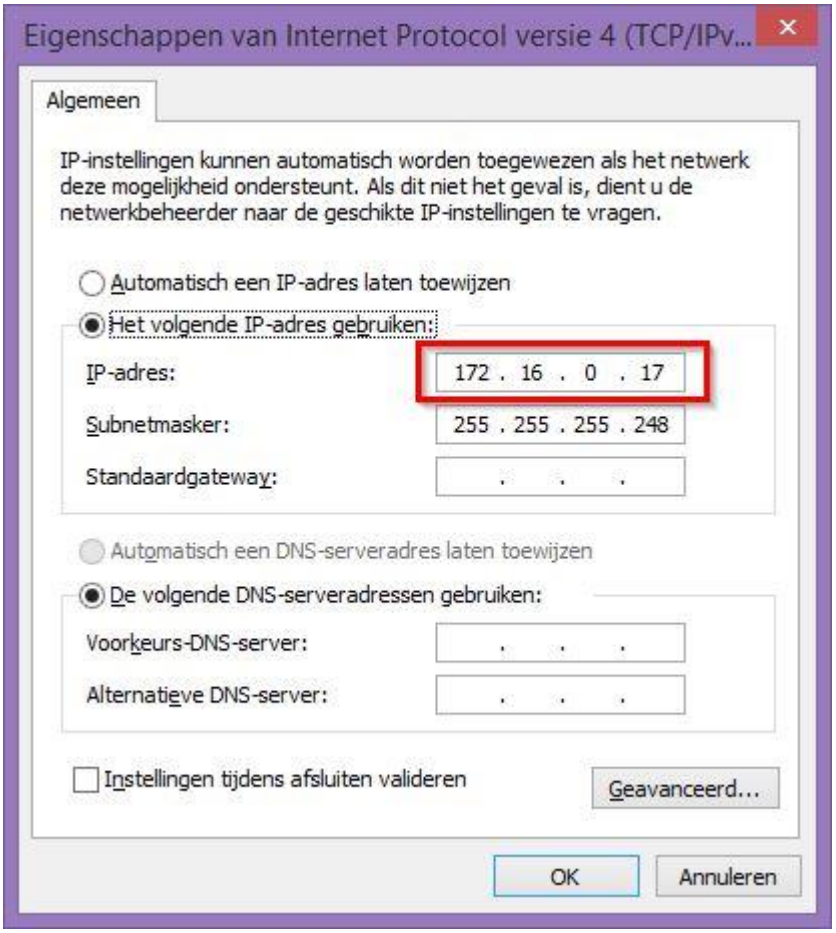
Voor men begint met de virtuele machines te maken, moeten we ook nog de virtuele netwerken maken.

Ik heb gebruik gemaakt van volgende netwerken:

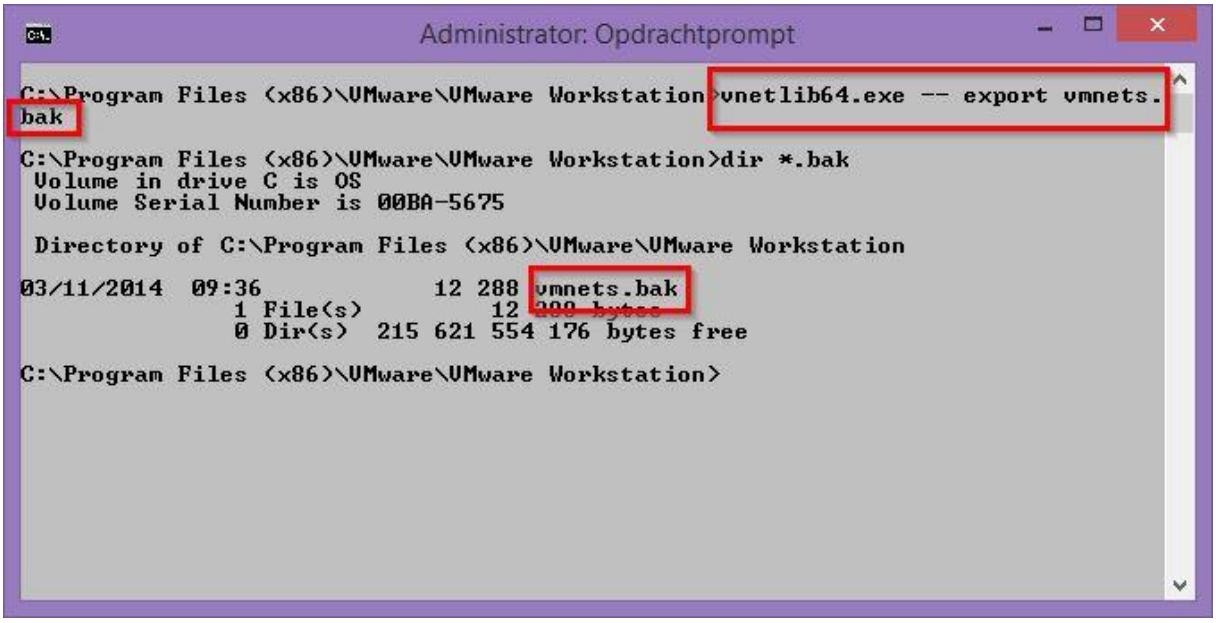
Vmnets			
Netwerk	Netwerknaam	Eerste adres	Laatste adres
172.16.0.16/29	vmnet2	172.16.0.17	172.16.0.22
172.16.0.32/29	vmnet3	172.16.0.33	172.16.0.38
172.16.0.48/29	vmnet4	172.16.0.49	172.16.0.54
172.16.0.8/29	vmnet5	172.16.0.9	172.16.0.14
172.16.0.24/29	vmnet6	172.16.0.25	172.16.0.30
172.16.0.40/29	vmnet7	172.16.0.41	172.16.0.46
10.1.0.0	vmnet9	10.1.0.1	10.1.0.254
10.3.0.0	vmnet10	10.3.0.1	10.3.0.254
172.16.0.56	vmnet11	172.16.0.57	172.16.0.62



Op deze virtuele netwerken krijgt onze host ook een IP-adres.



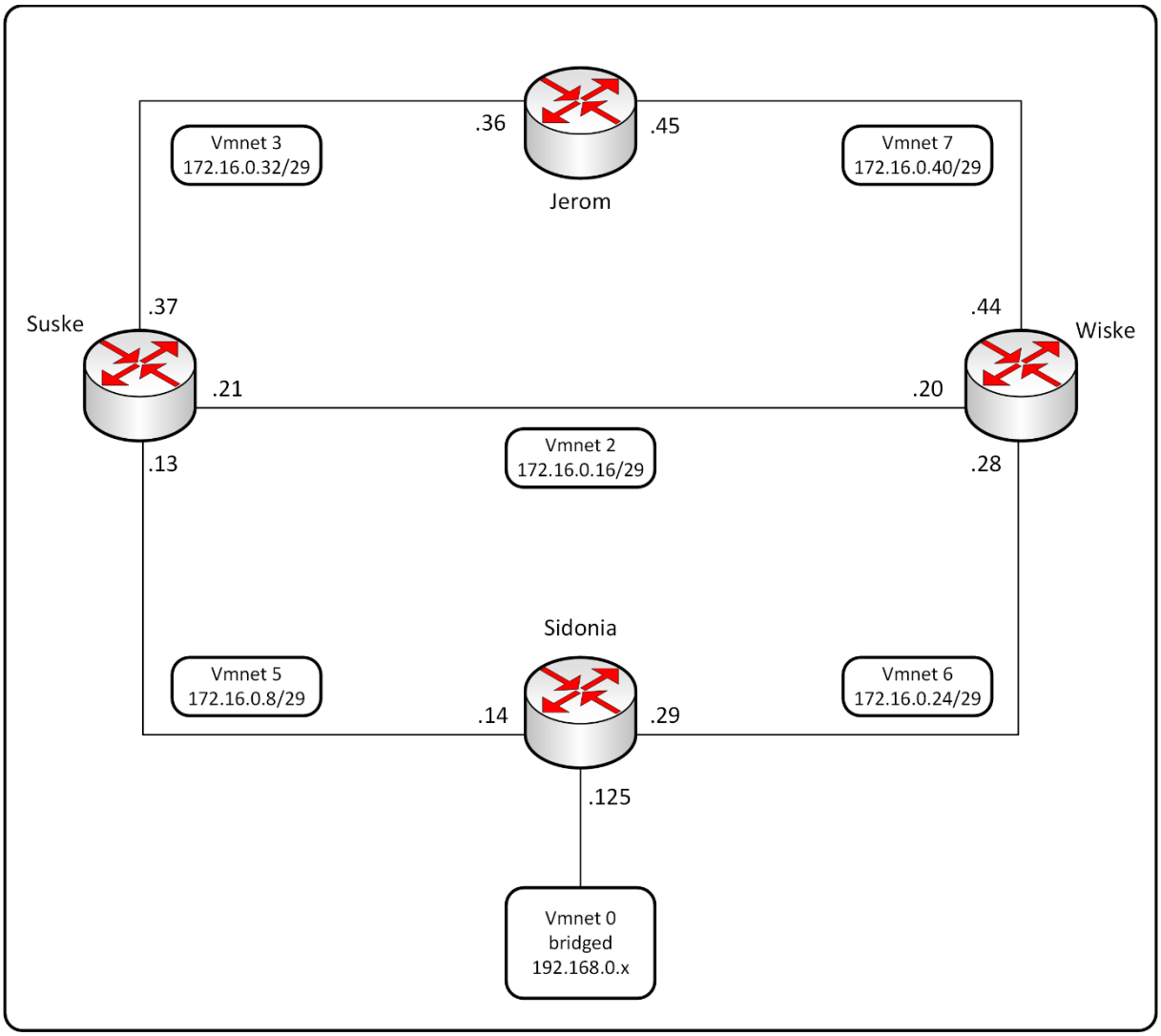
Om later, in geval van nood, tijd te besparen, maak ik van mijn virtuele netwerken een back-up:



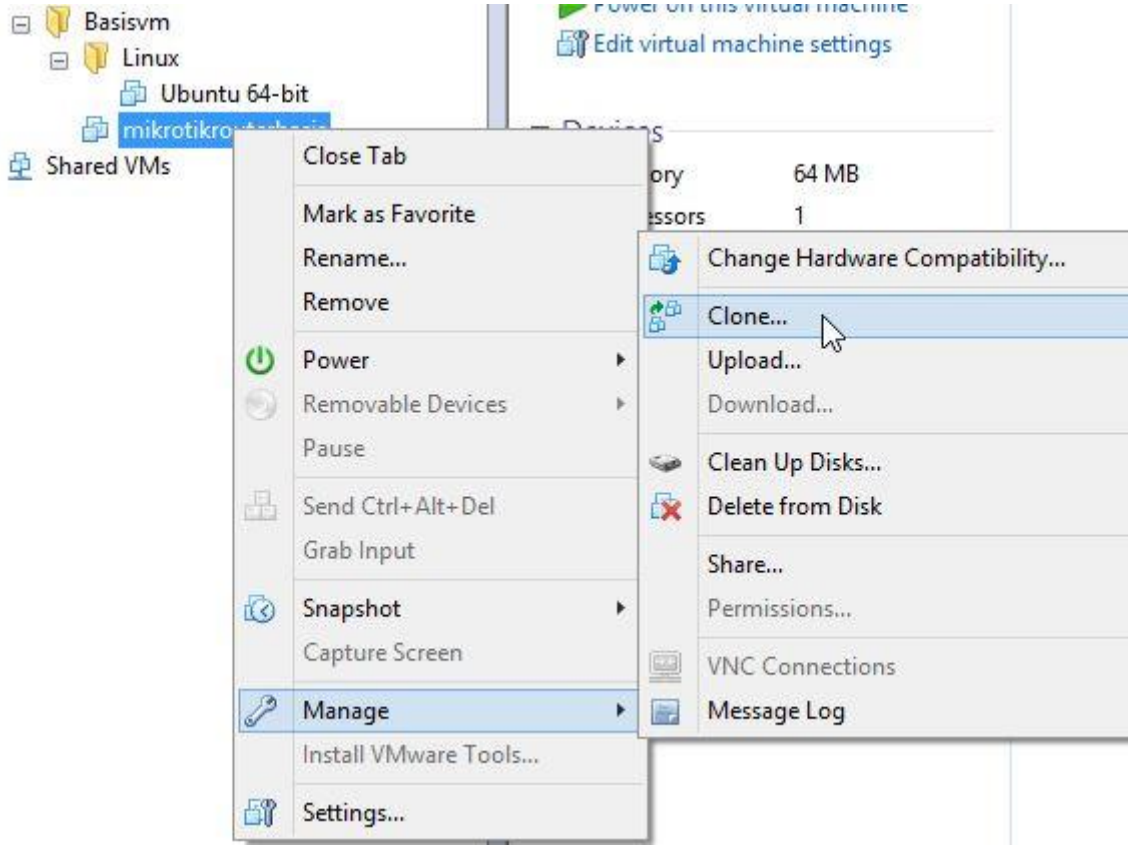
Het is zeer belangrijk om alle info (IP-adressen, namen van interface,…) op voorhand in een duidelijk schema te zetten.

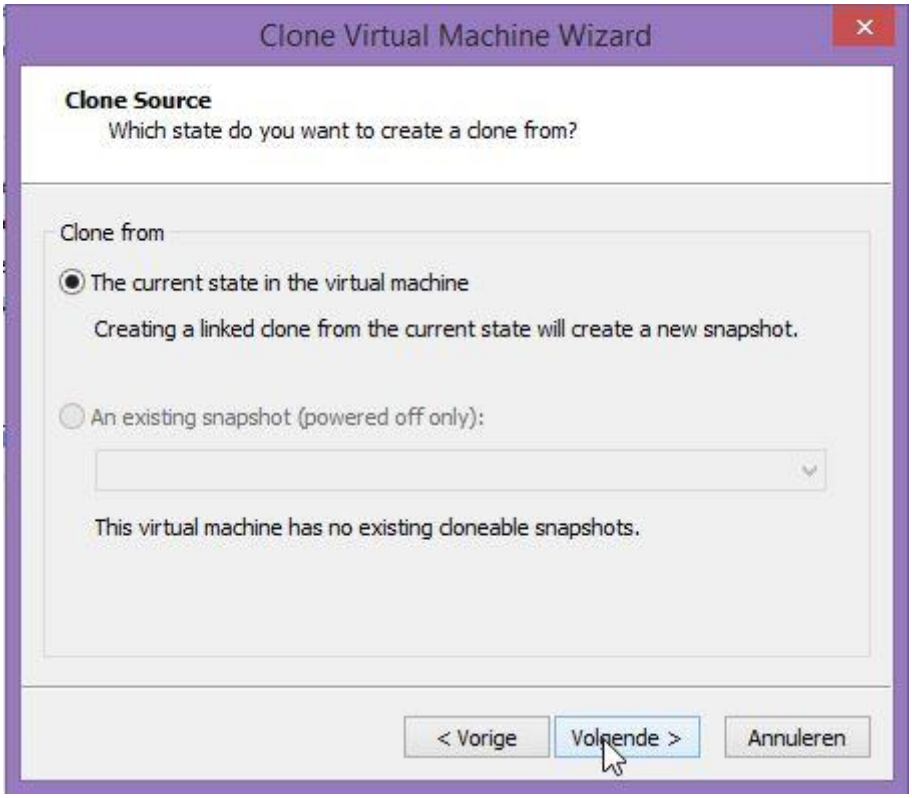
Backbone

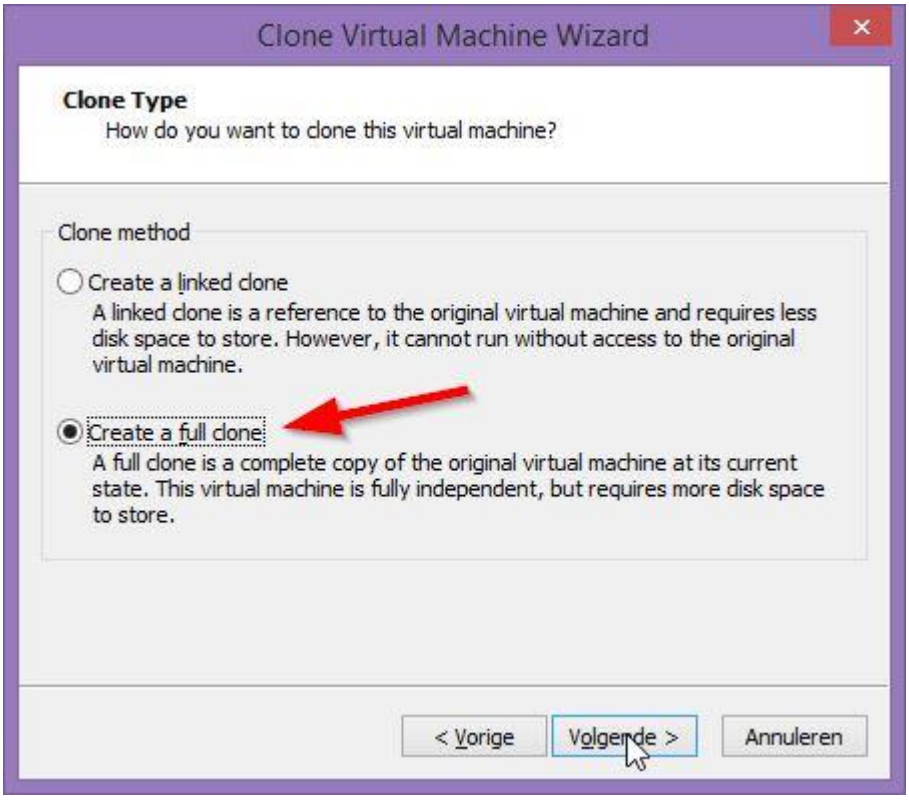
De backbone, het “hoofdgedeelte” van ons OSPF-netwerk bestaat uit 4 routers: sidonia, suske, wiske en jerom. We zetten ze als volgt op:

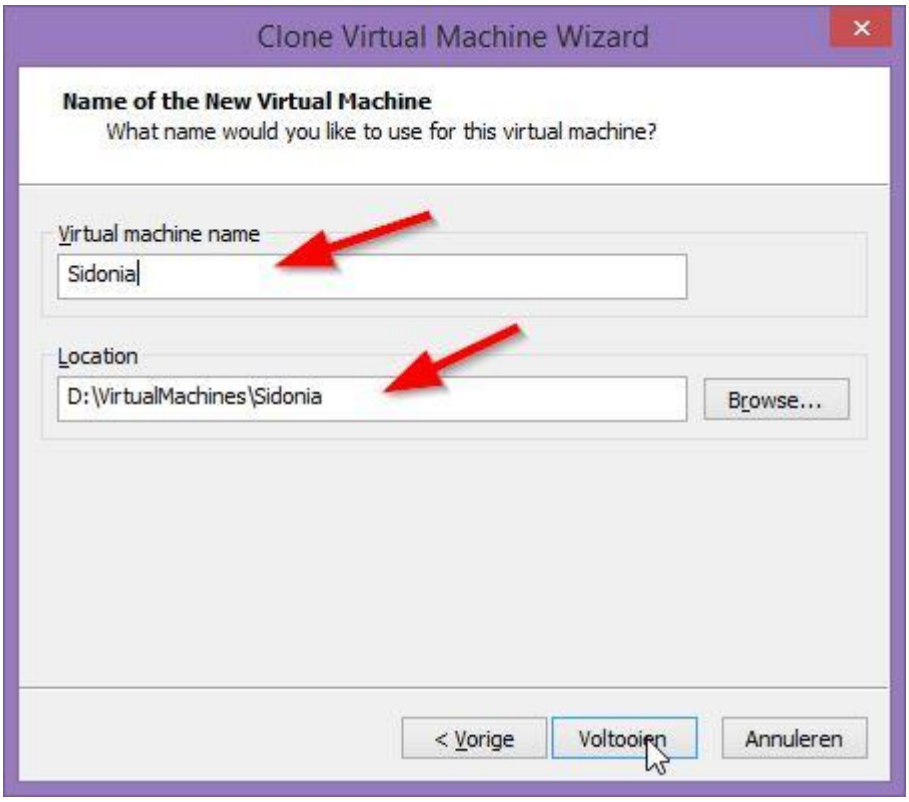


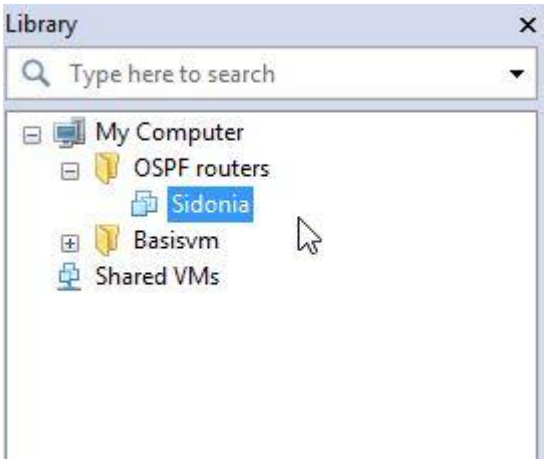
We beginnen met een nieuwe virtuele machine te klonen, dit zal de router “sidonia” zijn.


Basisvm
Linux
Ubuntu 64-bit
Shared VMs
Edit virtual machine settings
64 MB
1
Close Tab
Mark as Favorite
Rename...
Remove
Power
Removable Devices
Pause
Send Ctrl+Alt+Del
Grab Input
Snapshot
Capture Screen
Manage
Install VMware Tools...
Settings...
Change Hardware Compatibility...
Clone...
Upload...
Download...
Clean Up Disks...
Delete from Disk
Share...
Permissions...
VNC Connections
Message Log

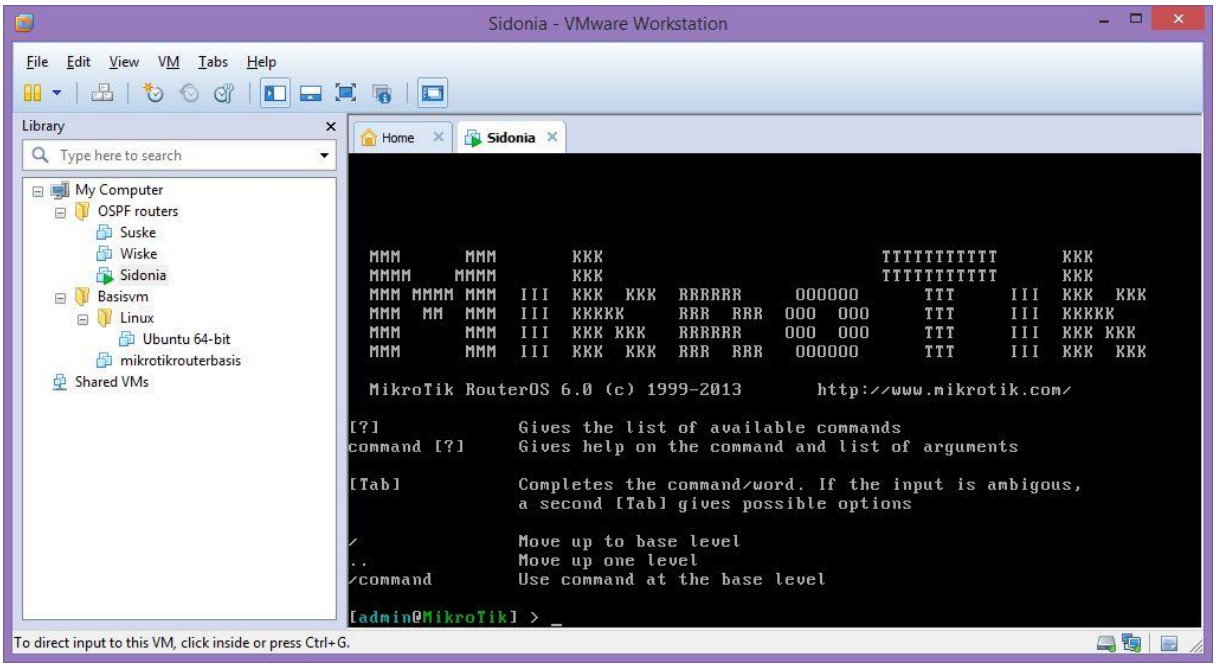

Clone Virtual Machine Wizard
Clone Source
Which state do you want to create a clone from?
Clone from
The current state in the virtual machine
Creating a linked clone from the current state will create a new snapshot.
An existing snapshot (powered off only):
This virtual machine has no existing cloneable snapshots.
< Vorige
Volgende >
Annuleren


Clone Virtual Machine Wizard
Clone Type
How do you want to clone this virtual machine?
Clone method
Create a linked clone
A linked clone is a reference to the original virtual machine and requires less disk space to store. However, it cannot run without access to the original virtual machine.
Create a full clone
A full clone is a complete copy of the original virtual machine at its current state. This virtual machine is fully independent, but requires more disk space to store.
< Vorige
Volgende >
Annuleren


Clone Virtual Machine Wizard
Name of the New Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name
Sidonia
Location
D:\VirtualMachines\Sidonia
Browse...
< Vorige
Voltooien
Annuleren



Daarna starten we de router sidonia op voor de eerste keer:

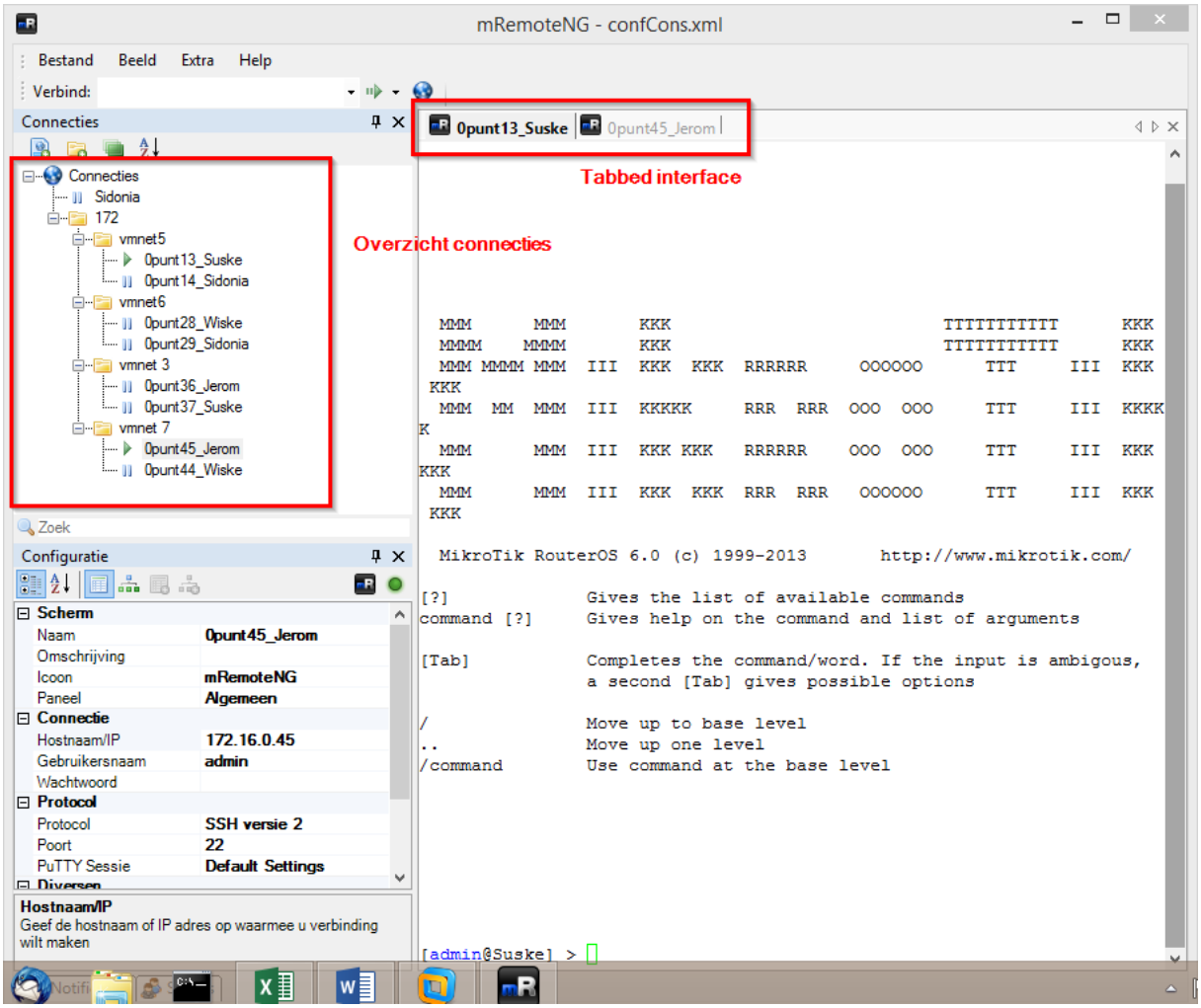


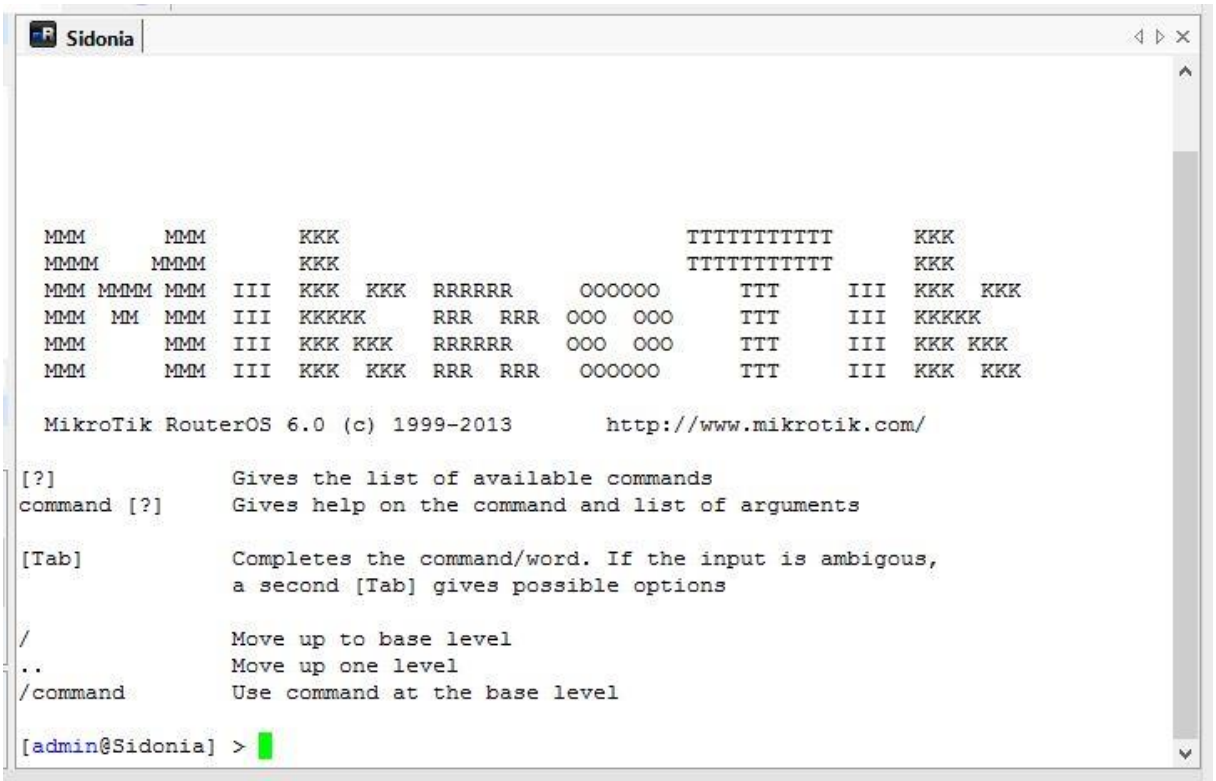
Nu moeten we de router een naam geven, de interface een naam geven en een IP-adres toewijzen aan de interface. Dit doe ik met volgende commando's:

```
/system identity set name=sidonia
/interface set "eth0" name="ToHost"
/ip address add address=192.168.0.125/24 interface=ToHost
```

Het hernoemen van de interface en het toewijzen van het IP-adres herhaal ik per interface. Als we de eerste interface hebben ingesteld kan ik met mRemoteNG verbinding maken met de router.

mRemoteNG is een programma zoals PUTTY, maar met uitgebreidere mogelijkheden, zoals een "tabbed interface".


mRemoteNG - confCons.xml
Bestand
Beeld
Extra
Help
Verbind:
Connecties
0punt13_Suske
0punt45_Jerom
Tabbed interface
Overzicht connecties
Connecties
Sidonia
172
vmnet5
0punt13_Suske
0punt14_Sidonia
vmnet6
0punt28_Wiske
0punt29_Sidonia
vmnet 3
0punt36_Jerom
0punt37_Suske
vmnet 7
0punt45_Jerom
0punt44_Wiske
Zoek
Configuratie
Scherm
Naam 0punt45_Jerom
Omschrijving
Icoon mRemoteNG
Paneel Algemeen
Connectie
Hostnaam/IP 172.16.0.45
Gebruikersnaam admin
Wachtwoord
Protocol
Protocol SSH versie 2
Poort 22
PuTTY Sessie Default Settings
Diversen
Hostnaam/IP
Geef de hostnaam of IP adres op waarmee u verbinding wilt maken
MMM MMM KKK TTTTTTTTTTT KKK
MMMM MMMM KKK TTTTTTTTTTT KKK
MMM MMMM MMM III KKK KKK RRRRRR OOOOOO TTT III KKK KKK
MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK
MMM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK
MikroTik RouterOS 6.0 (c) 1999-2013 http://www.mikrotik.com/
[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments
[Tab] Completes the command/word. If the input is ambigous,
a second [Tab] gives possible options
/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@Suske] >


Sidonia
MMM MMM KKK TTTTTTTTTTT KKK
MMMM MMMM KKK TTTTTTTTTTT KKK
MMM MMMM MMM III KKK KKK RRRRRR OOOOOO TTT III KKK KKK
MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK
MMM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK
MikroTik RouterOS 6.0 (c) 1999-2013 http://www.mikrotik.com/
[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments
[Tab] Completes the command/word. If the input is ambigous,
a second [Tab] gives possible options
/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@Sidonia] >

Als alle interfaces zijn ingesteld, voegen we nog een loopback-interface toe.

```
[admin@Sidonia] > /interface bridge add name=loopbackSidonia
[admin@Sidonia] > /ip address add address=10.4.255.1/32 interface=loopbackSidonia
```

Aangezien de router sidonia op de grens staat tussen ons virtueel OSPF-netwerk en mijn thuisnetwerk, voeg ik nog een default route toe:

```
[admin@Sidonia] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.0.125/24   192.168.0.0     ToHost
 1   172.16.0.14/29     172.16.0.8      ToSuske
 2   172.16.0.29/29     172.16.0.24     ToWiske
 3   10.4.255.1/32      10.4.255.1      loopbackSidonia
[admin@Sidonia] > /ip route add dst-address=0.0.0.0/0 gateway=ToHost

[admin@Sidonia] >
```

Voorlopig werken we met statische routers. Ik zet even de configuratie van de backbone-routers op een rijtje.

```
[admin@Sidonia] > /interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME                                                                MTU MAC-ADDRESS       ARP
 0 R  ToHost                                                             1500 00:0C:29:BE:E8:25 enabled
 1 R  ToSuske                                                            1500 00:0C:29:BE:E8:2F enabled
 2 R  ToWiske                                                            1500 00:50:56:34:67:D9 enabled
[admin@Sidonia] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.0.125/24   192.168.0.0     ToHost
 1   172.16.0.14/29     172.16.0.8      ToSuske
 2   172.16.0.29/29     172.16.0.24     ToWiske
 3   10.4.255.1/32      10.4.255.1      loopbackSidonia
[admin@Sidonia] > /ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          ToHost                    1
 1 ADC  10.4.255.1/32      10.4.255.1      loopbackSidonia           0
 2 ADC  172.16.0.8/29      172.16.0.14     ToSuske                   0
 3 ADC  172.16.0.24/29     172.16.0.29     ToWiske                   0
 4 ADC  192.168.0.0/24     192.168.0.125   ToHost                    0
```

```
[admin@Suske] > /interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME                                                    MTU MAC-ADDRESS       ARP
 0 R  ToJerom                                                1500 00:0C:29:10:38:23 enabled
 1 R  ToLambik                                               1500 00:0C:29:10:38:2D enabled
 2 R  ToSidonia                                              1500 00:0C:29:10:38:0F enabled
 3 R  ToWiske                                                1500 00:0C:29:10:38:19 enabled
[admin@Suske] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   172.16.0.13/29     172.16.0.8      ToSidonia
 1   172.16.0.21/29     172.16.0.16     ToWiske
 2   172.16.0.37/29     172.16.0.32     ToJerom
 3   172.16.0.53/29     172.16.0.48     ToLambik
 4   10.0.255.1/32      10.0.255.1      loopbackSuske
[admin@Suske] > /ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.0.255.1/32      10.0.255.1      loopbackSuske             0
 1 ADC  172.16.0.8/29      172.16.0.13     ToSidonia                 0
 2 ADC  172.16.0.16/29     172.16.0.21     ToWiske                   0
 3 ADC  172.16.0.32/29     172.16.0.37     ToJerom                   0
 4 ADC  172.16.0.48/29     172.16.0.53     ToLambik                  0
[admin@Suske] >
```

```
[admin@Wiske] > /interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME                                                    MTU MAC-ADDRESS       ARP
 0 R  ToBarabas                                              1500 00:0C:29:85:66:B5 enabled
 1 R  ToJerom                                                1500 00:0C:29:85:66:AB enabled
 2 R  ToSidonia                                              1500 00:0C:29:85:66:97 enabled
 3 R  ToSuske                                                1500 00:0C:29:85:66:A1 enabled
[admin@Wiske] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.2.255.1/32      10.2.255.1      loopbackWiske
 1   172.16.0.28/29     172.16.0.24     ToSidonia
 2   172.16.0.20/29     172.16.0.16     ToSuske
 3   172.16.0.44/29     172.16.0.40     ToJerom
 4   172.16.0.60/29     172.16.0.56     ToBarabas
[admin@Wiske] > /ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.2.255.1/32      10.2.255.1      loopbackWiske             0
 1 ADC  172.16.0.16/29     172.16.0.20     ToSuske                   0
 2 ADC  172.16.0.24/29     172.16.0.28     ToSidonia                 0
 3 ADC  172.16.0.40/29     172.16.0.44     ToJerom                   0
 4 ADC  172.16.0.56/29     172.16.0.60     ToBarabas                 0
```

```
[admin@Jerom] > /interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME                                                    MTU MAC-ADDRESS       ARP
 0 R  ToSuske                                                1500 00:50:56:35:00:65 enabled
 1 R  ToWiske                                                1500 00:0C:29:04:27:5D enabled
[admin@Jerom] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   172.16.0.36/29     172.16.0.32     ToSuske
 1   10.2.255.1/32      10.2.255.1      loopbackJerom
 2   172.16.0.45/29     172.16.0.40     ToWiske
[admin@Jerom] > /ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.2.255.1/32      10.2.255.1      loopbackJerom             0
 1 ADC  172.16.0.32/29     172.16.0.36     ToSuske                   0
 2 ADC  172.16.0.40/29     172.16.0.45     ToWiske                   0
```

Nu gaan we OSPF inschakelen op de backbone. Daarvoor voeren we volgende commando's uit (dit voorbeeld is van router Sidonia):

```
/routing ospf instance add name=default
/routing ospf instance set 0 router-id=10.4.255.1
/routing ospf network add network=172.16.0.24/29 area=backbone
/routing ospf network add network=172.16.0.8/29 area=backbone
```

Normaal gezien is de default instantie al gemaakt bij de installatie van RouterOS, dus krijgen we hier een foutmelding van.

```
[admin@Sidonia] > /routing ospf instance add name=default
failure: duplicated name
[admin@Sidonia] > /routing ospf instance set 0 router-id=10.4.255.1
[admin@Sidonia] > /routing ospf network add network=172.16.0.24/29 area
=backbone
[admin@Sidonia] > /routing ospf network add network=172.16.0.8/29 area=
backbone
[admin@Sidonia] > /routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
 #    INTERFACE         COST PRI NETWORK-TYPE   AUT... AUTHENTICATIO...
 0 D  ToWiske             10   1 broadcast      none
 1 D  ToSuske             10   1 broadcast      none
```

Hier zien we dat router Sidonia twee buren heeft:

```
[admin@Sidonia] > /routing ospf neighbor print
 0 instance=default router-id=10.0.255.1 address=172.16.0.13
   interface=ToSuske priority=1 dr-address=172.16.0.14
   backup-dr-address=172.16.0.13 state="Full" state-changes=4
   ls-retransmits=0 ls-requests=0 db-summaries=0 adjacency=20m31s

 1 instance=default router-id=10.2.255.1 address=172.16.0.28
   interface=ToWiske priority=1 dr-address=172.16.0.29
   backup-dr-address=172.16.0.28 state="Full" state-changes=4
   ls-retransmits=0 ls-requests=0 db-summaries=0 adjacency=20m57s
```

We leiden er ook vanaf dat tussen router Sidonia en Wiske de router Sidonia (172.16.0.29) de designated router (DR) is.

```
[admin@Suske] > /routing ospf instance add name=default
failure: duplicated name
[admin@Suske] > /routing ospf instance set 0 router-id=10.0.255.1
[admin@Suske] > /routing ospf network add network=172.16.0.8/29 area=ba
ckbone
[admin@Suske] > /routing ospf network add network=172.16.0.32/29 area=b
ackbone
[admin@Suske] > /routing ospf network add network=172.16.0.16/29 area=b
ackbone
[admin@Suske] > /routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
 #    INTERFACE         COST PRI NETWORK-TYPE   AUT... AUTHENTICATIO...
 0 D  ToSidonia           10   1 broadcast      none
 1 D  ToJerom             10   1 broadcast      none
 2 D  ToWiske             10   1 broadcast      none
[admin@Suske] >
```

Om router suske zijn router-ID te kennen kunnen we volgend commando uitvoeren:

`/routing ospf instance print status`

```
[admin@Suske] > /routing ospf instance print status
Flags: X - disabled, * - default
 0  * name="default" router-id=10.0.255.1 distribute-default=never
      redistribute-connected=no redistribute-static=no
      redistribute-rip=no redistribute-bgp=no
      redistribute-other-ospf=no metric-default=1
      metric-connected=20 metric-static=20 metric-rip=20
      metric-bgp=auto metric-other-ospf=auto in-filter=ospf-in
      out-filter=ospf-out state=running
      effective-router-id=10.0.255.1 dijkstras=7 db-exchanges=0
      external-imports=0
```

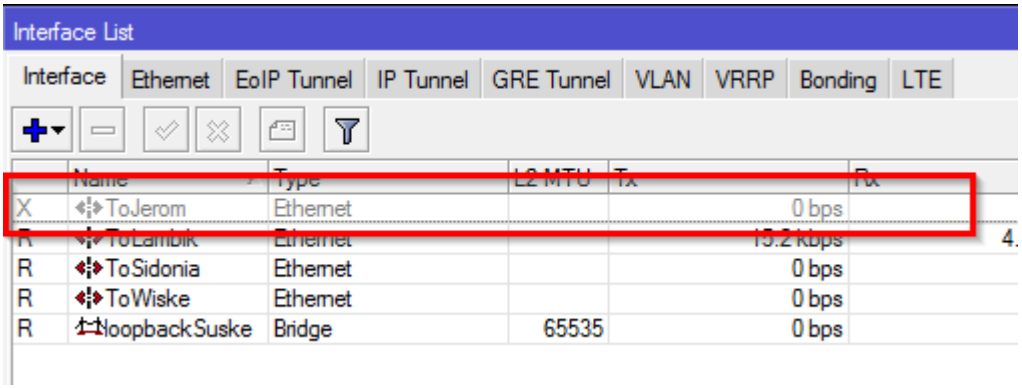
OSPF inschakelen op router Jerom:

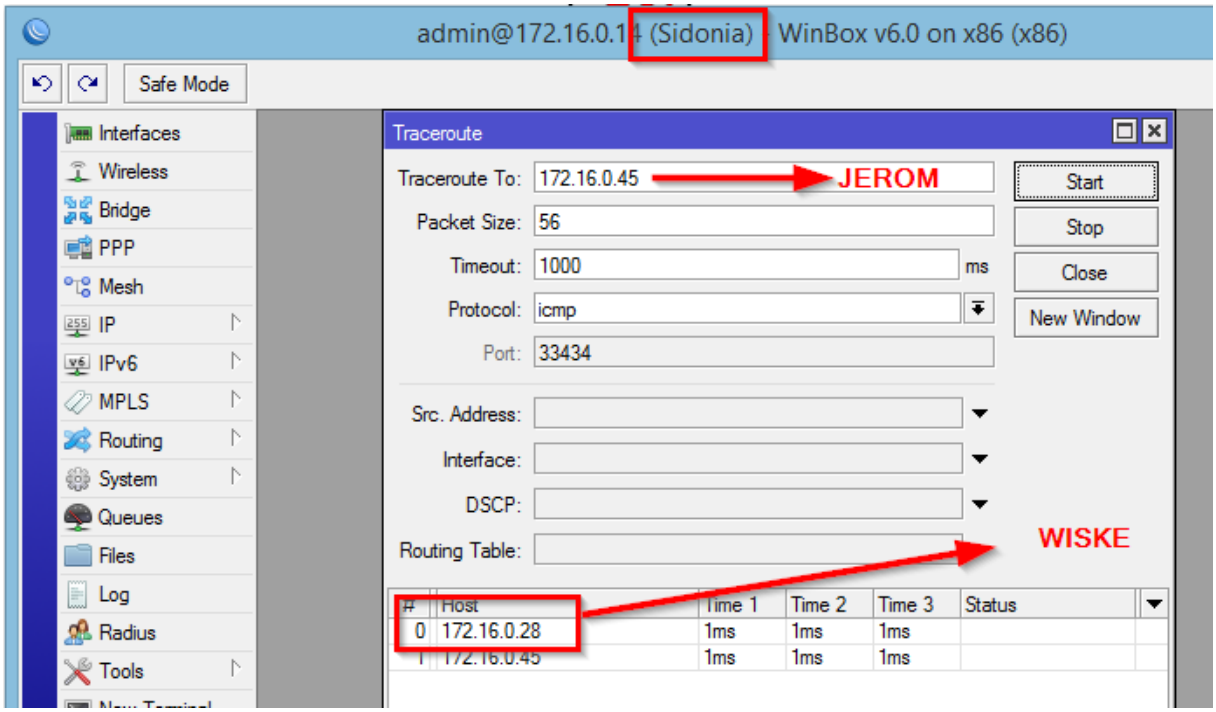
```
[admin@Jerom] > /routing ospf instance add name=default
failure: duplicated name
[admin@Jerom] > /routing ospf instance set 0 router-id=10.5.255.1
[admin@Jerom] > /routing ospf network add network=172.16.0.32/29 area=b
ackbone
[admin@Jerom] > /routing ospf network add network=172.16.0.40/29 area=b
ackbone
[admin@Jerom] > /routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
 #    INTERFACE         COST PRI NETWORK-TYPE   AUT... AUTHENTICATIO...
 0 D  ToSuske             10   1 broadcast      none
 1 D  ToWiske             10   1 broadcast      none
```

Als we van router Jerom naar router Sidonia “tracerouten”, zien we dat hij de route over router Suske neemt:

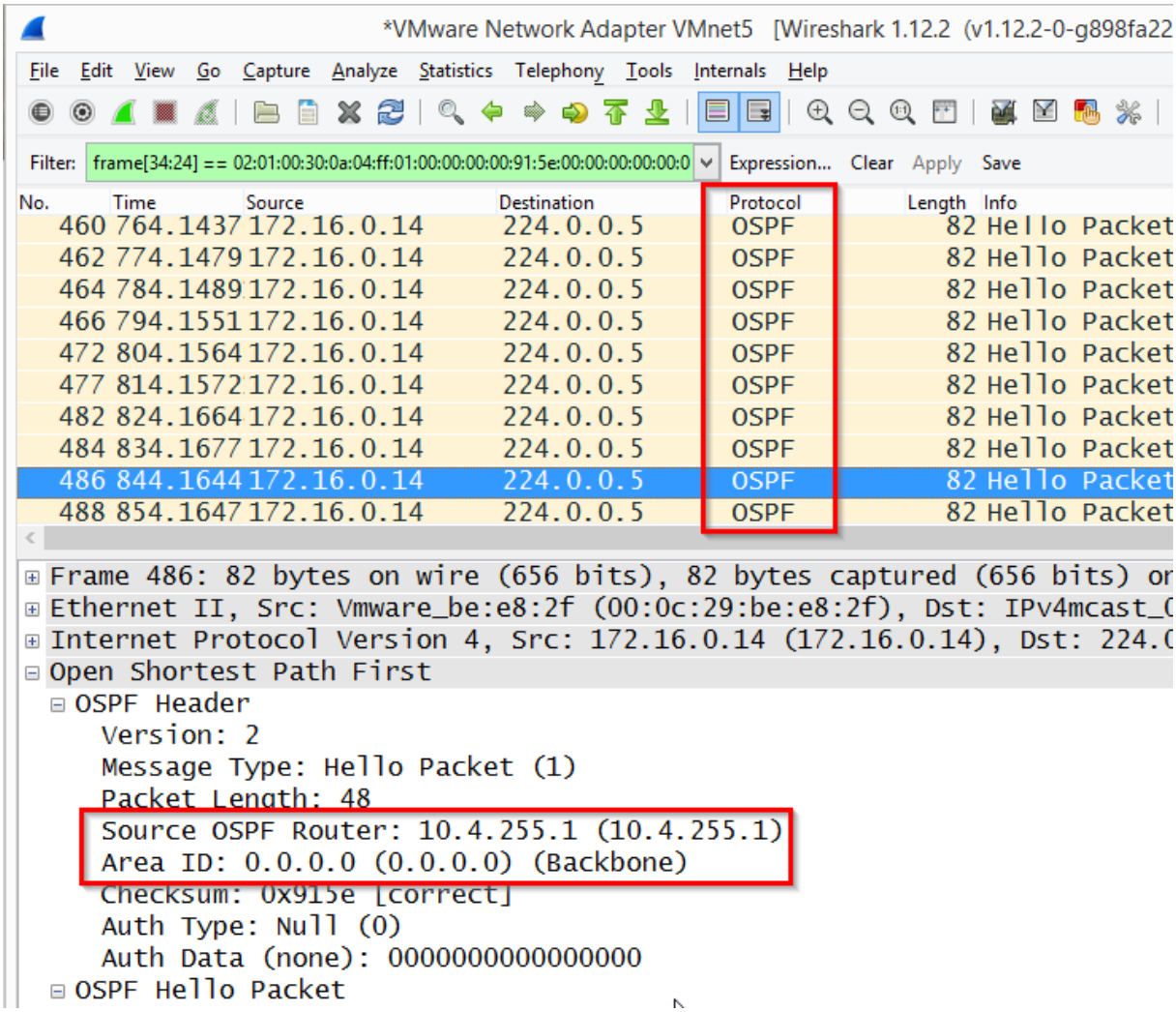
```
[admin@Sidonia] /tool> traceroute
address: 172.16.0.36
 # ADDRESS                                  RT1    RT2    RT3    STATUS
 1 172.16.0.13                              1ms    1ms    1ms
 2 172.16.0.36                              1ms    1ms    1ms
```

Als we nu een interface van router Suske uitschakelen, dan zullen we zien dat de route automatisch verandert, en over router Wiske zal gaan.

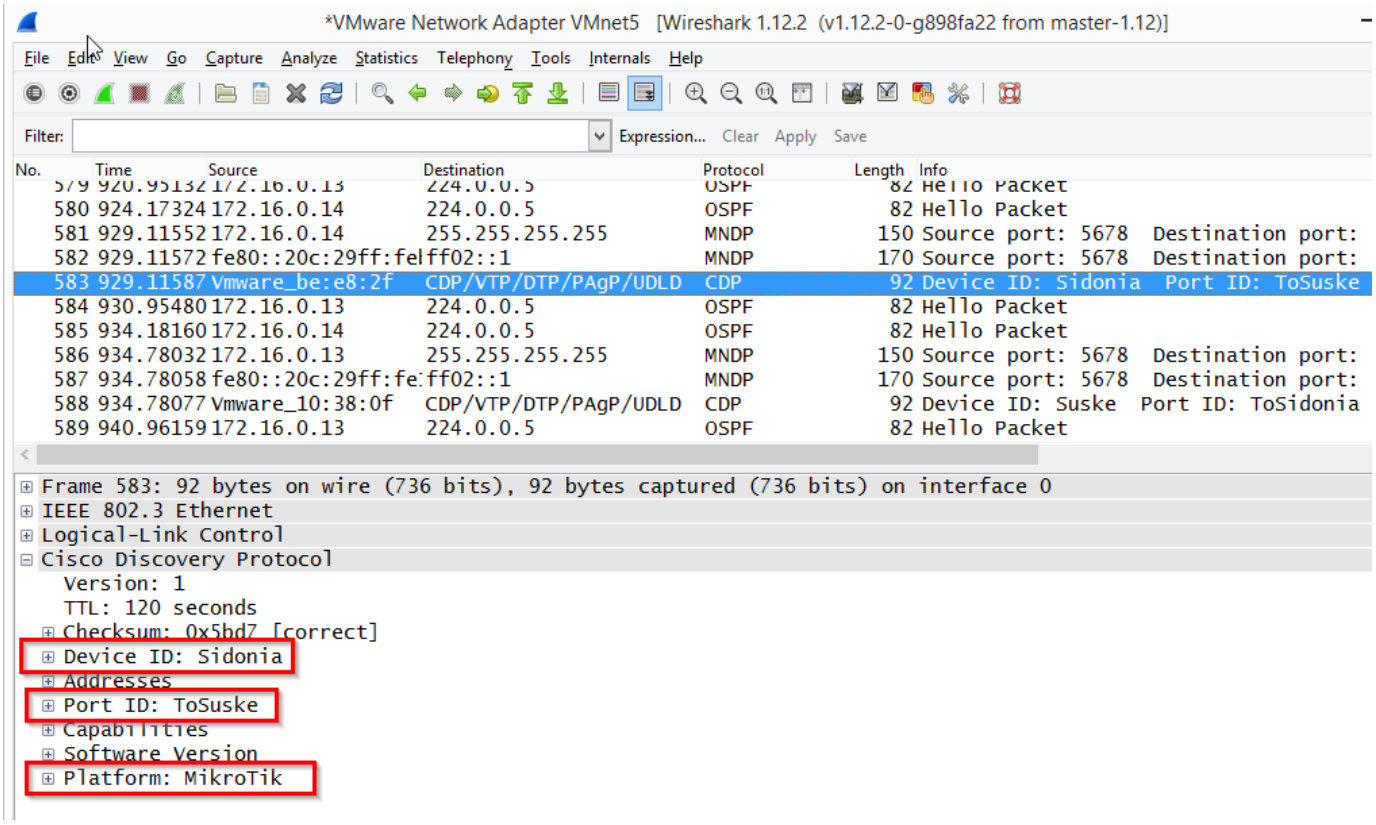


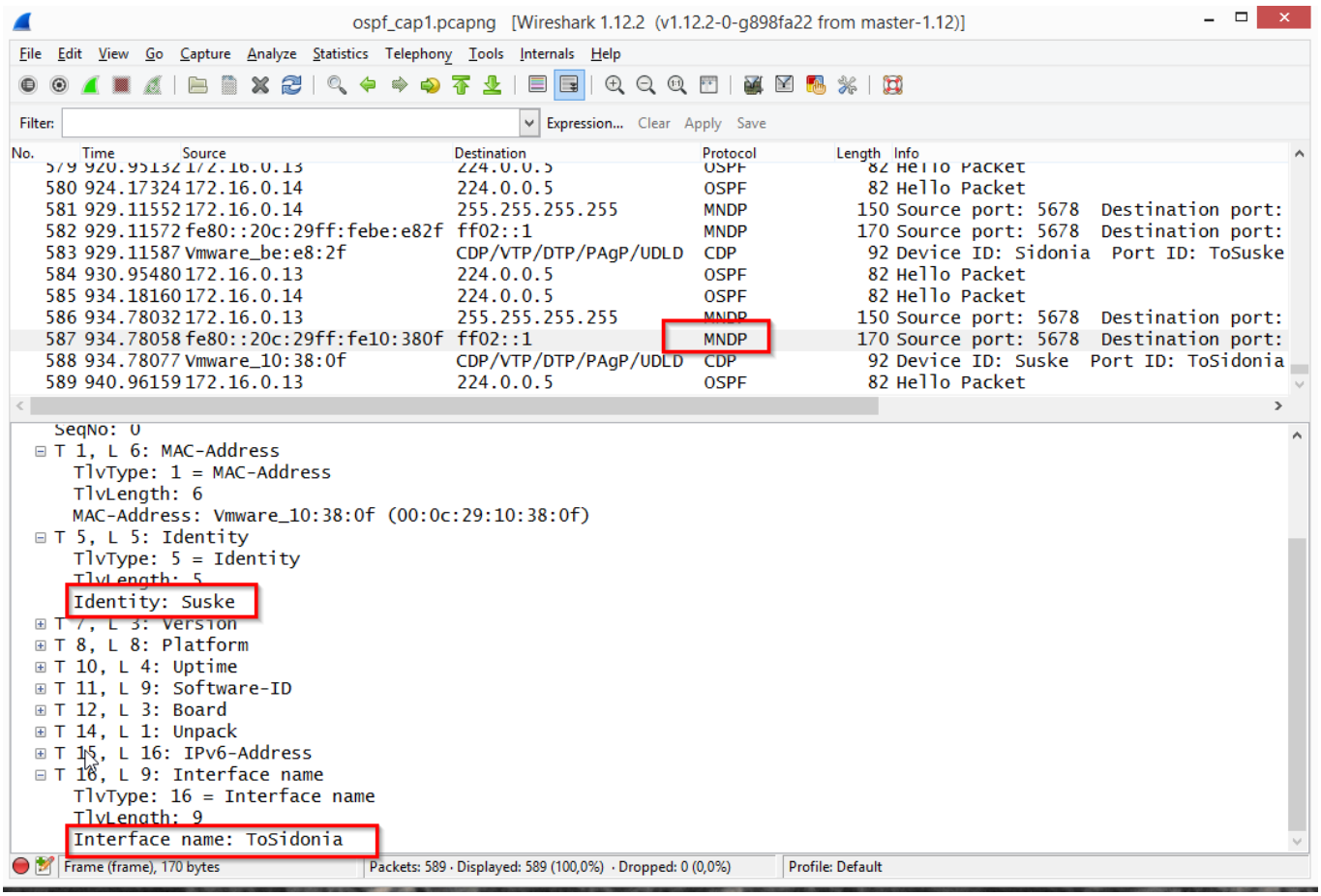


Tijdens deze handelingen liet ik op mijn host Wireshark draaien, en daar kon ik duidelijk het OSPF-verkeer onderscheiden.



Buiten het OSPF-protocol zien we op de Wireshark-capture ook het MNDP-protocol, wat staat voor “Mikrotik Network Discovery Protocol” en het CDP-protocol (Cisco Discovery Protocol). Aangezien we zelf geen Cisco-apparatuur in het netwerk hebben geplaatst, vermoed ik dat het hier gaat over de virtuele netwerk-infrastructuur van VMware Workstation.





Als we nu een interface van Suske uitschakelen, zien we het volgende:

```
⊞ Frame 128: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
⊞ Ethernet II, Src: Vmware_04:27:5d (00:0c:29:04:27:5d), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
⊞ Internet Protocol Version 4, Src: 172.16.0.45 (172.16.0.45), Dst: 224.0.0.5 (224.0.0.5)
⊟ Open Shortest Path First
  ⊟ OSPF Header
      Version: 2
      Message Type: LS Update (4)
      Packet Length: 108
      Source OSPF Router: 10.5.255.1 (10.5.255.1)
      Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
      Checksum: 0xdb80 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  ⊞ LS Update Packet
```

```
⊞ Frame 130: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 2
⊞ Ethernet II, Src: Vmware_85:66:a1 (00:0c:29:85:66:a1), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
⊞ Internet Protocol Version 4, Src: 172.16.0.20 (172.16.0.20), Dst: 224.0.0.5 (224.0.0.5)
⊟ Open Shortest Path First
  ⊟ OSPF Header
      Version: 2
      Message Type: LS Update (4)
      Packet Length: 108
      Source OSPF Router: 10.2.255.1 (10.2.255.1)
      Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
      Checksum: 0xdb82 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  ⊟ LS Update Packet
      Number of LSAs: 2
    ⊞ Router-LSA
    ⊞ Network-LSA
```

Dus kun je de verschillende LSA's zien. Als we dan de interface op router Suske terug aanschakelen, bekijk ik terug de details van een "LSA Acknowledge" pakket:

```
⊟ Open Shortest Path First
  ⊟ OSPF Header
      Version: 2
      Message Type: LS Acknowledge (5)
      Packet Length: 64
      Source OSPF Router: 10.0.255.1 (10.0.255.1)
      Area ID: 0.0.0.0 (0.0.0.0) (Backbone)
      Checksum: 0xf96d [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  ⊟ LSA Header
      .000 0000 0000 0011 = LS Age (seconds): 3
      0... .... .... .... = Do Not Age Flag: 0
    ⊞ Options: 0x02 (E)
      LS Type: Router-LSA (1)
      Link State ID: 10.5.255.1 (10.5.255.1)
      Advertising Router: 10.5.255.1 (10.5.255.1)
      Sequence Number: 0x80000007
      Checksum: 0x510d
      Length: 48
  ⊟ LSA Header
      .000 1110 0001 0000 = LS Age (seconds): 3600
      0... .... .... .... = Do Not Age Flag: 0
    ⊞ Options: 0x02 (E)
      LS Type: Network-LSA (2)
      Link State ID: 172.16.0.36 (172.16.0.36)
      Advertising Router: 10.5.255.1 (10.5.255.1)
      Sequence Number: 0x80000003
```

We kunnen ook de ingestelde loopback-adressen gebruiken om te pingen.

```
[admin@Wiske] > ping 10.0.255.1
HOST                                     SIZE TTL TIME  STATUS
10.0.255.1                                 56  64 0ms
10.0.255.1                                 56  64 0ms
10.0.255.1                                 56  64 0ms
10.0.255.1                                 56  64 0ms
10.0.255.1                                 56  64 0ms
10.0.255.1                                 56  64 0ms
10.0.255.1                                 56  64 0ms
    sent=7 received=7 packet-loss=0% min-rtt=0ms avg-rtt=0ms
   max-rtt=0ms
```

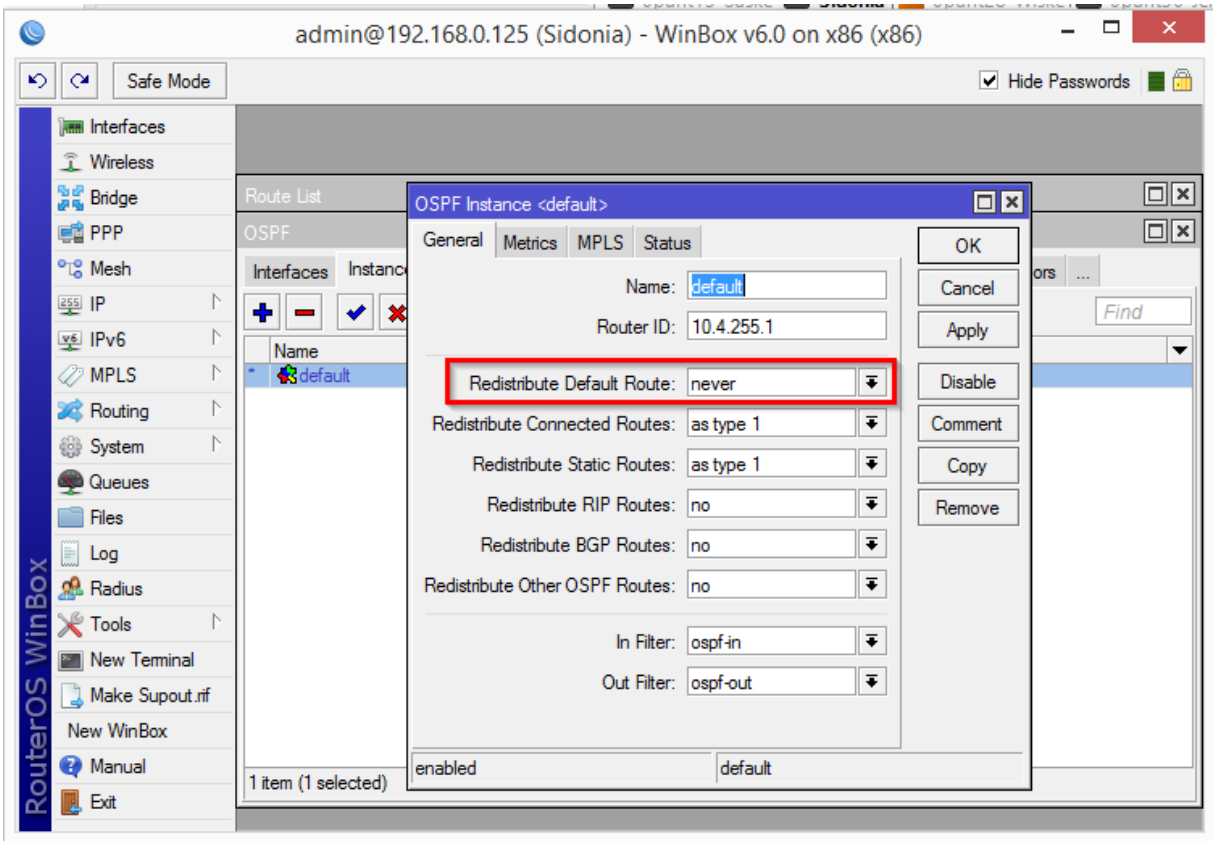
Ik wou er voor zorgen dat ook de niet-OSPF-routes werden verdeeld via OSPF:

```
[admin@Sidonia] /routing ospf instance> set 0 redistribute-connected=as
-type-1
[admin@Sidonia] /routing ospf instance> set 0 redistribute-static=as-ty
pe-1
[admin@Sidonia] /routing ospf instance>
```

Als ik dan op router Suske ging kijken naar de OSPF-routetabel, zag die er zo uit:

```
[admin@Suske] > /routing ospf route print
 #  DST-ADDRESS         STATE           COST       GATEWAY
 0  10.0.255.1/32       imported-ext-1  20
 1  10.2.255.1/32       ext-1           30         172.16.0.20
                                                   172.16.0.36
 2  10.4.255.1/32       ext-1           30         172.16.0.14
 3  172.16.0.8/29       intra-area      10         0.0.0.0
 4  172.16.0.16/29      intra-area      10         0.0.0.0
 5  172.16.0.24/29      intra-area      20         172.16.0.14
                                                   172.16.0.20
 6  172.16.0.32/29      intra-area      10         0.0.0.0
 7  172.16.0.40/29      intra-area      20         172.16.0.20
                                                   172.16.0.36
 8  172.16.0.48/29      imported-ext-1  20
 9  172.16.0.56/29      ext-1           30         172.16.0.20
10  192.168.0.0/24      ext-1           30         172.16.0.14
```

Ik merkte op dat de default route niet werd verdeeld. Eerst probeerde ik dit via de commandline, maar ook al gebruikte ik commando's uit de Mikrotik-wiki, ik kreeg syntax-errors. Daarom gebruikte ik Winbox:



Daarna werd de default-route van router Sidonia ook naar de andere routers verdeeld. Pingen naar mijn VM-host ging, maar pingen naar 8.8.8.8 ging niet. Daarom probeerde ik source natting te activeren:

```
[admin@Wiske] > ping 192.168.0.191
HOST                                     SIZE TTL TIME  STATUS
192.168.0.191                              56 127 0ms
192.168.0.191                              56 127 0ms
192.168.0.191                              56 127 0ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms
   max-rtt=0ms

[admin@Wiske] > ping 8.8.8.8
HOST                                     SIZE TTL TIME  STATUS
                                                      no route to
                                                      no route to
                                                      no route to
                                                      no route to
                                                      no route to
    sent=5 received=0 packet-loss=100%

[admin@Sidonia] > /ip firewall nat add chain=srcnat action=masquerade o
ut-interface=ToHost
```

Na deze source natting te activeren, kon ik nog niet pingen naar 8.8.8.8. Dit heb ik nog niet kunnen oplossen:

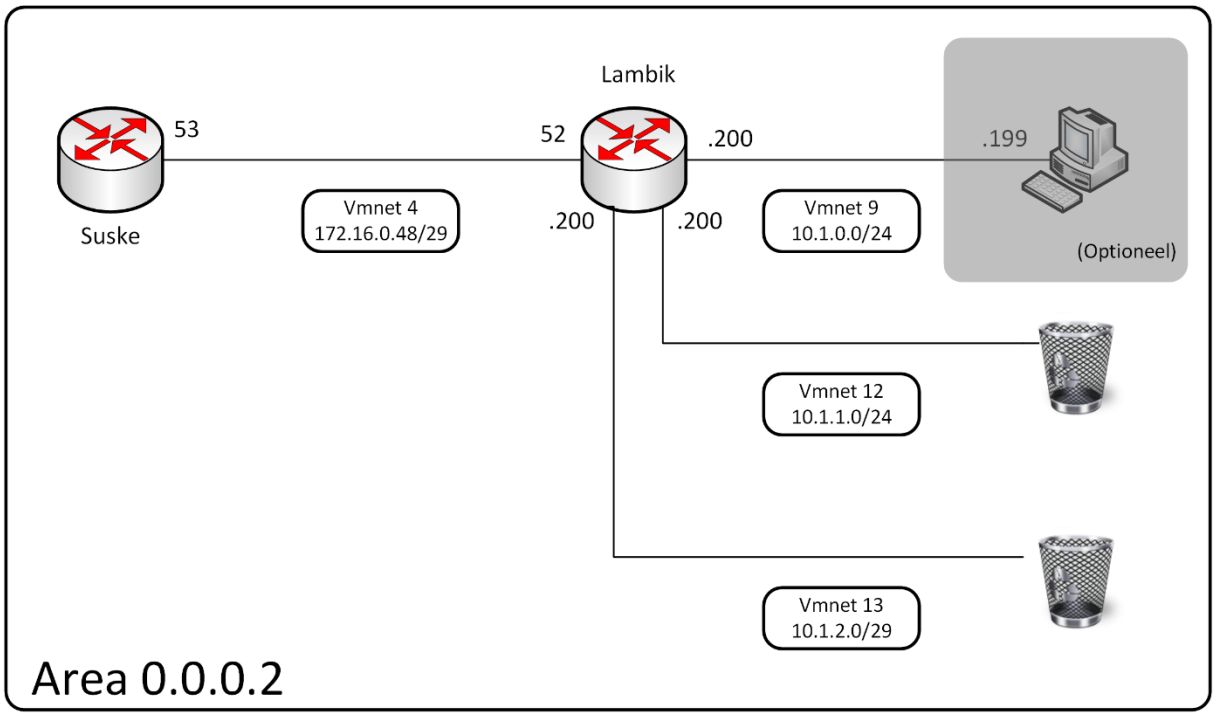
```
[admin@Wiske] > /tool traceroute 8.8.8.8
 # ADDRESS                                  RT1    RT2    RT3    STATUS
 1 172.16.0.29                              1ms    1ms    1ms
 2 192.168.0.125                            0ms    0ms    985ms host u...
 3 192.168.0.125                            0ms    0ms    992ms host u...
 4 192.168.0.125                            0ms    0ms    993ms host u...
 5 192.168.0.125                            0ms    0ms    993ms host u...
 6 192.168.0.125                            0ms    0ms    993ms host u...
 7 192.168.0.125                            0ms    0ms    992ms host u...

[admin@Wiske] > ping 192.168.0.125
HOST                                     SIZE TTL TIME  STATUS
192.168.0.125                              56  64 0ms
192.168.0.125                              56  64 0ms
192.168.0.125                              56  64 0ms
192.168.0.125                              56  64 0ms
192.168.0.125                              56  64 0ms
192.168.0.125                              56  64 0ms
    sent=6 received=6 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@Wiske] > ping 192.168.0.191
HOST                                     SIZE TTL TIME  STATUS
192.168.0.191                              56 127 0ms
192.168.0.191                              56 127 0ms
192.168.0.191                              56 127 0ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

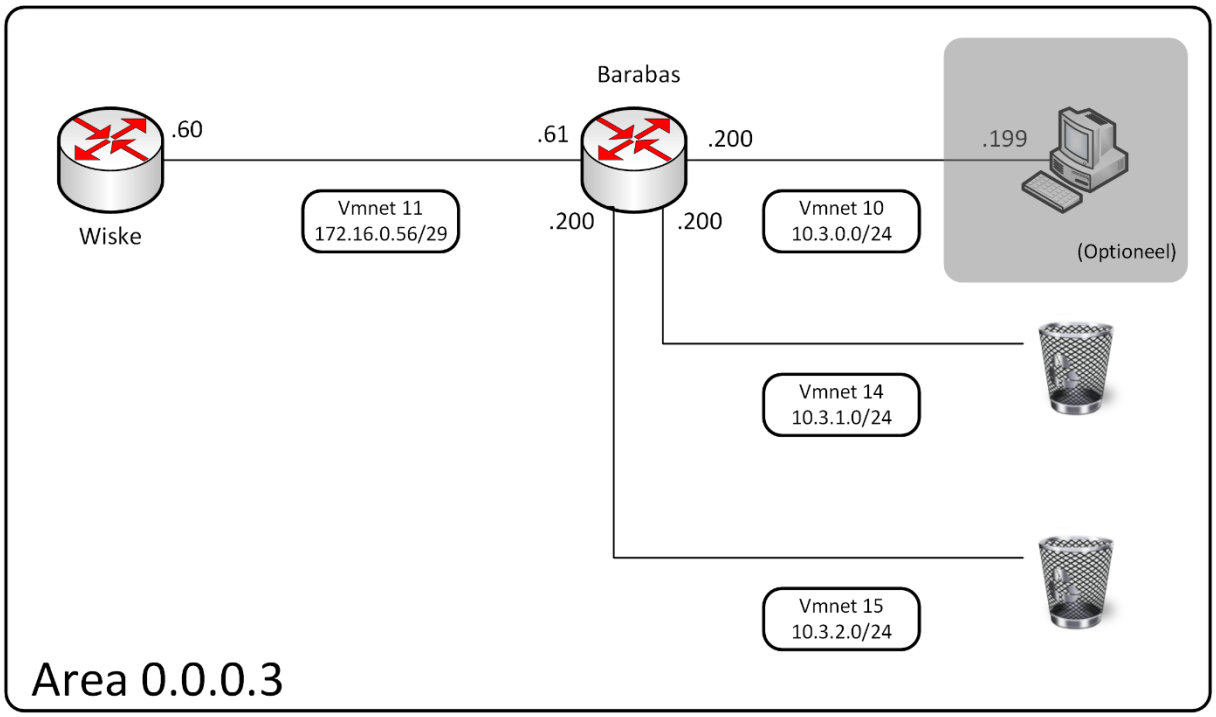
Uitbreiding naar meerdere area's

Nu we een backbone-infrastructuur hebben, gaan we deze uitbreiden naar een infrastructuur met twee extra area's. Zowel aan router Suske als router Wiske hangen we een nieuwe router. Deze vormt dan samen met de desbetreffende interface op Suske of Wiske de nieuwe area.

Indien de tijd het toelaat hang ik aan één van de extra area's een webserver, en aan de andere een cliënt voor test-doeleinden.

De extra area's zien er dan zo uit:





Verkeer op vmnets 12 tot en met 15 zal worden afgeleid naar “black hole interfaces”. Dit verkeer verdwijnt. Men kan dit vergelijken met het in Linux kopiëren van bestanden naar /dev/null. Onderstaande screenshot laat zien hoe men dit kan doen:

```
[admin@MikroTik] >  /ip route add dst-address=10.1.2.0/24 type=blackhole
[admin@MikroTik] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.1.0.0/24        10.1.0.200      ToAlpha                   0
 1 ADC  10.1.1.0/24        10.1.1.200      ToKilo                    0
 2   SB 10.1.1.0/24                                                  1
 3 A SB 10.1.2.0/24                                                  1
 4 ADC  10.1.2.200/29      10.1.2.200      ToLima                    0
 5 ADC  172.16.0.48/29     172.16.0.52     ToSuske                   0
```

De procedure om nieuwe “area’s” toe te voegen gaat als volgt:

- Eerst voegt men aan de bestaande grensrouter een area toe, en wijst men daar de juiste netwerken aan toe.
- Daarna voegt men de volgend router en de juiste netwerken aan die area toe:

Voor router Wiske deed ik bvb. volgende commando’s:

```
/routing ospf area add name=area3 area-id=0.0.0.3
/routing ospf network add network=172.16.0.56/29 area=area3
```

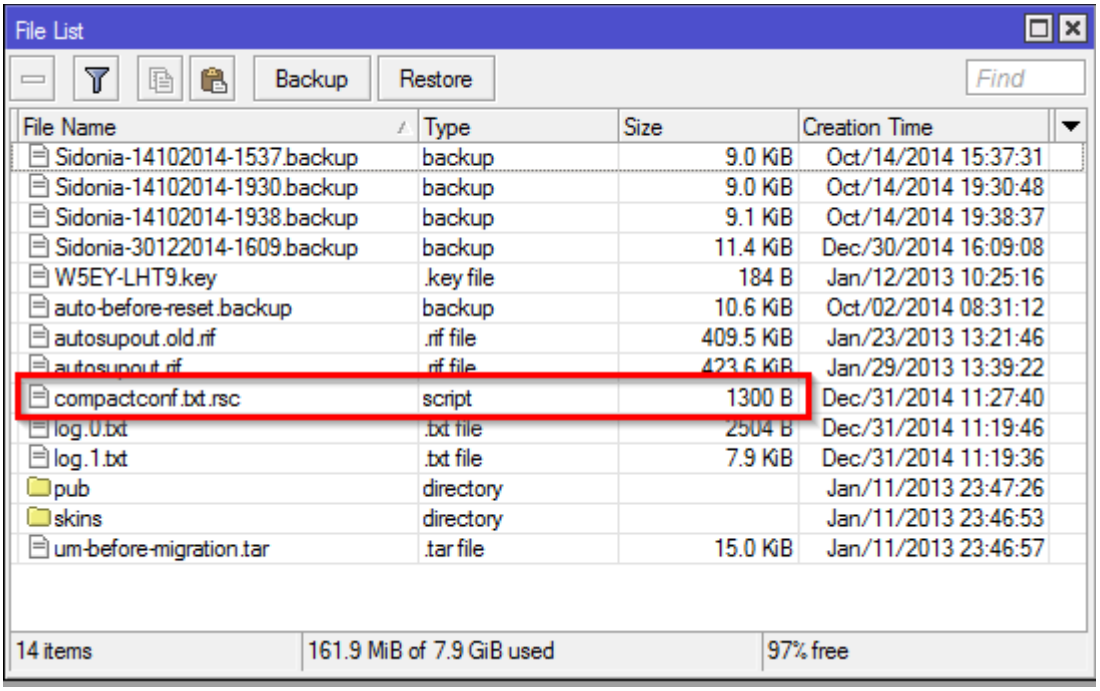
En dan voor de daarop volgende router Barabas deed ik:

```
/routing ospf area add name=area3 area-id=0.0.0.3
/routing ospf network add network=172.16.0.56/29 area=area3
/routing ospf network add network=10.3.0.0/29 area=area3
```

```
[admin@Suske] > /routing ospf area add name=area2 area-id=0.0.0.2
[admin@Suske] > /routing ospf network add network=172.16.0.48/29 area=area2
[admin@Suske] > /routing ospf route print
 # DST-ADDRESS        STATE          COST       GATEWAY
 0 0.0.0.0/0          ext-1          11         172.16.0.14
 1 10.0.255.1/32      imported-ext-1 20
 2 10.2.255.1/32      ext-1          30         172.16.0.20
                                                172.16.0.36
 3 10.4.255.1/32      ext-1          30         172.16.0.14
 4 172.16.0.8/29      intra-area     10         0.0.0.0
 5 172.16.0.16/29     intra-area     10         0.0.0.0
 6 172.16.0.24/29     intra-area     20         172.16.0.14
                                                172.16.0.20
 7 172.16.0.32/29     intra-area     10         0.0.0.0
 8 172.16.0.40/29     intra-area     20         172.16.0.20
                                                172.16.0.36
 9 172.16.0.48/29     intra-area     10         0.0.0.0
10 172.16.0.56/29     ext-1          30         172.16.0.20
11 192.168.0.0/24     ext-1          30         172.16.0.14
[admin@Suske] > /routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #    NAME                                AREA-ID         TYPE     DEFAULT-COST
 0  * backbone                            0.0.0.0         default
 1    area2                               0.0.0.2         default
```

```
[admin@Lambik] > /routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #    NAME                                AREA-ID         TYPE     DEFAULT-COST
 0  * backbone                            0.0.0.0         default
 1    area2                               0.0.0.2         default
[admin@Lambik] > /routing ospf network print
Flags: X - disabled, I - invalid
 #    NETWORK             AREA
 0    172.16.0.48/29      area2
 1    10.1.0.0/24         area2
[admin@Lambik] > /routing ospf route print
 # DST-ADDRESS         STATE           COST        GATEWAY
 0 0.0.0.0/0           ext-1           21          172.16.0.53
 1 10.0.255.1/32       ext-1           30          172.16.0.53
 2 10.1.0.0/24         intra-area      10          0.0.0.0
 3 10.2.255.1/32       ext-1           40          172.16.0.53
 4 10.4.255.1/32       ext-1           40          172.16.0.53
 5 172.16.0.8/29       inter-area      20          172.16.0.53
 6 172.16.0.16/29      inter-area      20          172.16.0.53
 7 172.16.0.24/29      inter-area      30          172.16.0.53
 8 172.16.0.32/29      inter-area      20          172.16.0.53
 9 172.16.0.40/29      inter-area      30          172.16.0.53
10 172.16.0.48/29      intra-area      10          0.0.0.0
11 172.16.0.56/29      ext-1           40          172.16.0.53
12 192.168.0.0/24      ext-1           40          172.16.0.53
```

Als men het commando “`export compact file=compactconf.txt`” uitvoert krijgt men een scriptfile waarin alle uitgevoerde veranderingen staan. Dit is handig als men vanaf nul moet herbeginnen.



```
# dec/31/2014 11:27:39 by RouterOS 6.0
# software id = V9JS-UDXR
#
/interface bridge
add name=loopbackSidonia
/interface ethernet
set 0 name=ToHost
set 1 name=ToSuske
set 2 name=ToWiske
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m \
    mac-cookie-timeout=3d
/port
set 0 name=serial0
set 1 name=serial1
/routing ospf instance
set [ find default=yes ] distribute-default=always-as-type-1 \
    redistribute-connected=as-type-1 redistribute-static=as-type-1 router-id=\
    10.4.255.1
/ip address
add address=192.168.0.125/24 interface=ToHost network=192.168.0.0
add address=172.16.0.14/29 interface=ToSuske network=172.16.0.8
add address=172.16.0.29/29 interface=ToWiske network=172.16.0.24
add address=10.4.255.1/32 interface=loopbackSidonia network=10.4.255.1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ToHost to-addresses=0.0.0.0
add action=masquerade chain=srcnat out-interface=ToHost to-addresses=0.0.0.0
/ip route
add check-gateway=ping distance=1 gateway=ToHost
/routing ospf network
add area=backbone network=172.16.0.24/29
add area=backbone network=172.16.0.8/29
```

Inter-area Route Summarization

De originele route-lijst van Lambik ziet er zo uit:

Route List

Routes | Nexthops | Rules | VRF

Find: all

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAo	10.0.255.1	172.16.0.53 reachable ToSuske	110		
DAC	10.1.0.0/24	ToAlpha reachable	0		10.1.0.200
SB	10.1.1.0/24		1		
DAC	10.1.1.0/24	ToIndia reachable	0		10.1.1.200
ASB	10.1.2.0/24		1		
DAC	10.1.2.200/29	ToJuliet reachable	0		10.1.2.200
DAC	10.1.255.1	loopbackLambik reachable	0		10.1.255.1
DAo	10.2.255.1	172.16.0.53 reachable ToSuske	110		
DAo	10.3.0.0/24	172.16.0.53 reachable ToSuske	110		
DAo	10.3.1.0/24	172.16.0.53 reachable ToSuske	110		
DAo	10.3.2.0/24	172.16.0.53 reachable ToSuske	110		
DAo	10.3.255.1	172.16.0.53 reachable ToSuske	110		
DAo	10.4.255.1	172.16.0.53 reachable ToSuske	110		
DAo	172.16.0.8/29	172.16.0.53 reachable ToSuske	110		
DAo	172.16.0.16/29	172.16.0.53 reachable ToSuske	110		
DAo	172.16.0.24/29	172.16.0.53 reachable ToSuske	110		
DAo	172.16.0.32/29	172.16.0.53 reachable ToSuske	110		
DAo	172.16.0.40/29	172.16.0.53 reachable ToSuske	110		
DAC	172.16.0.48/29	ToSuske reachable	0		172.16.0.52
DAo	172.16.0.56/29	172.16.0.53 reachable ToSuske	110		
DAo	192.168.0.0/24	172.16.0.53 reachable ToSuske	110		

Om deze lijst in te korten maken we van area 2 een stub-area.

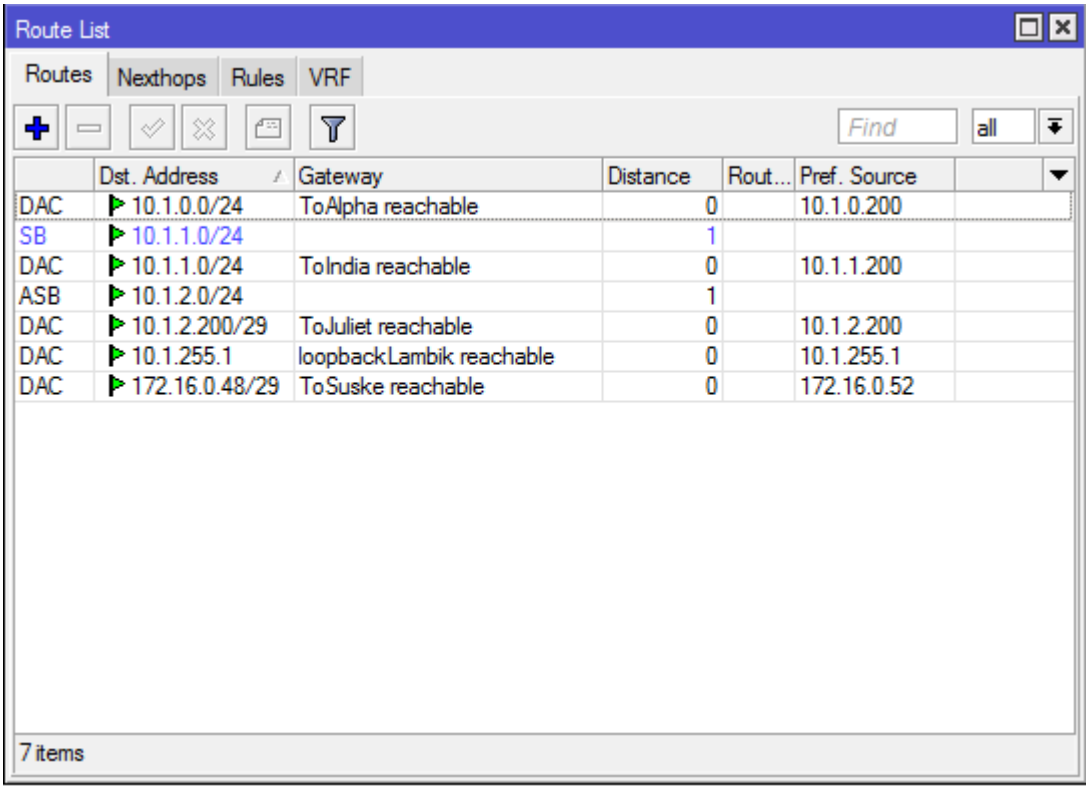
OSPF Area <area2>

Area Name: area2
Instance: default
Area ID: 0.0.0.2
Type: stub
Translator Role: translate never
Inject Summary LSAs
Default Cost: 1
Interfaces: 2
Active Interfaces: 2
Neighbors: 1
Adjacent Neighbors: 1

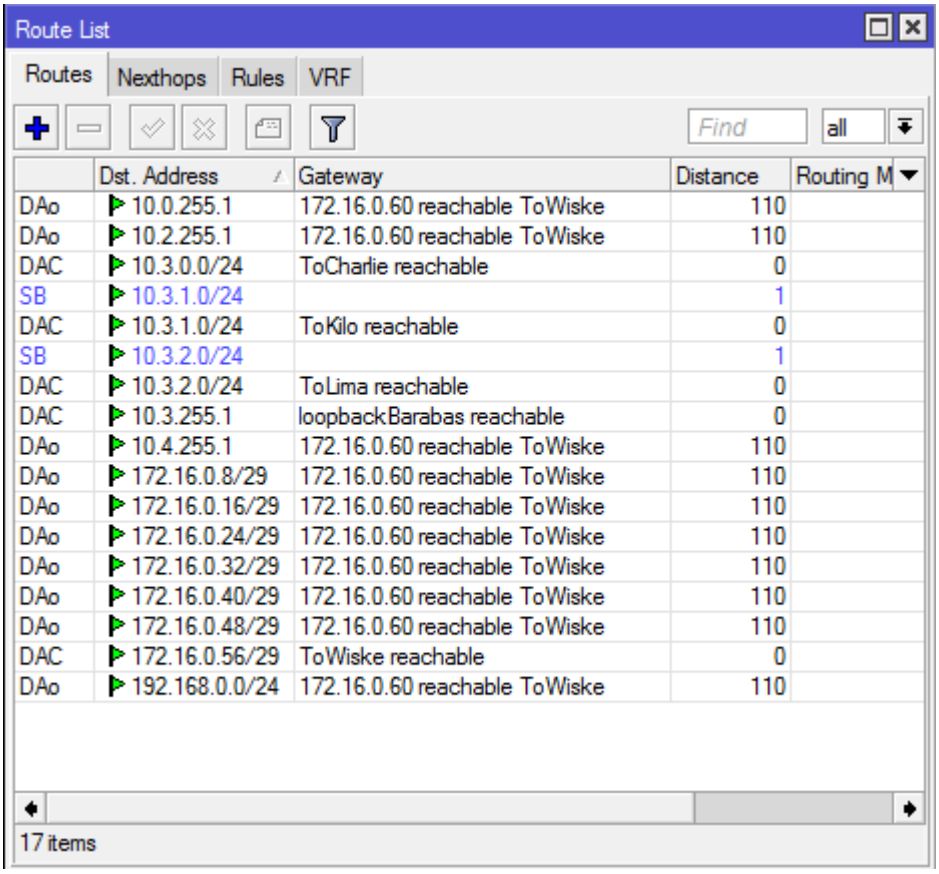
OK | Cancel | Apply | Disable | Comment | Copy | Remove

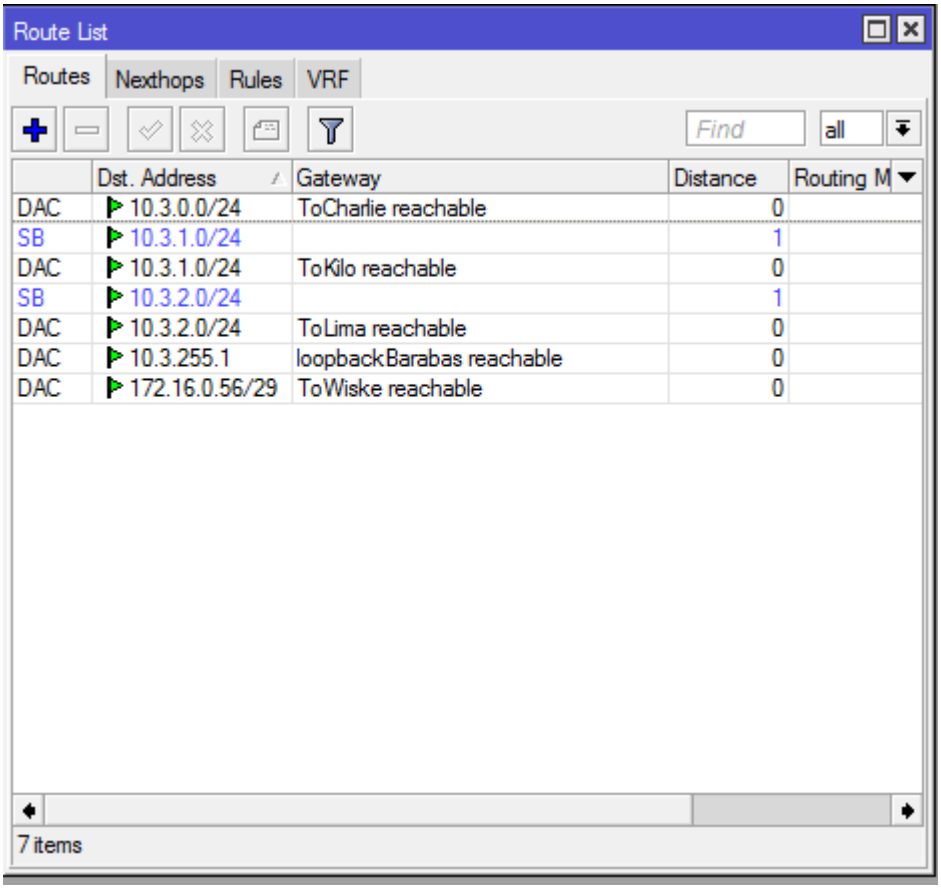
enabled

Met als resultaat:



En nu doen we hetzelfde voor Barabas:





OSPF Logging

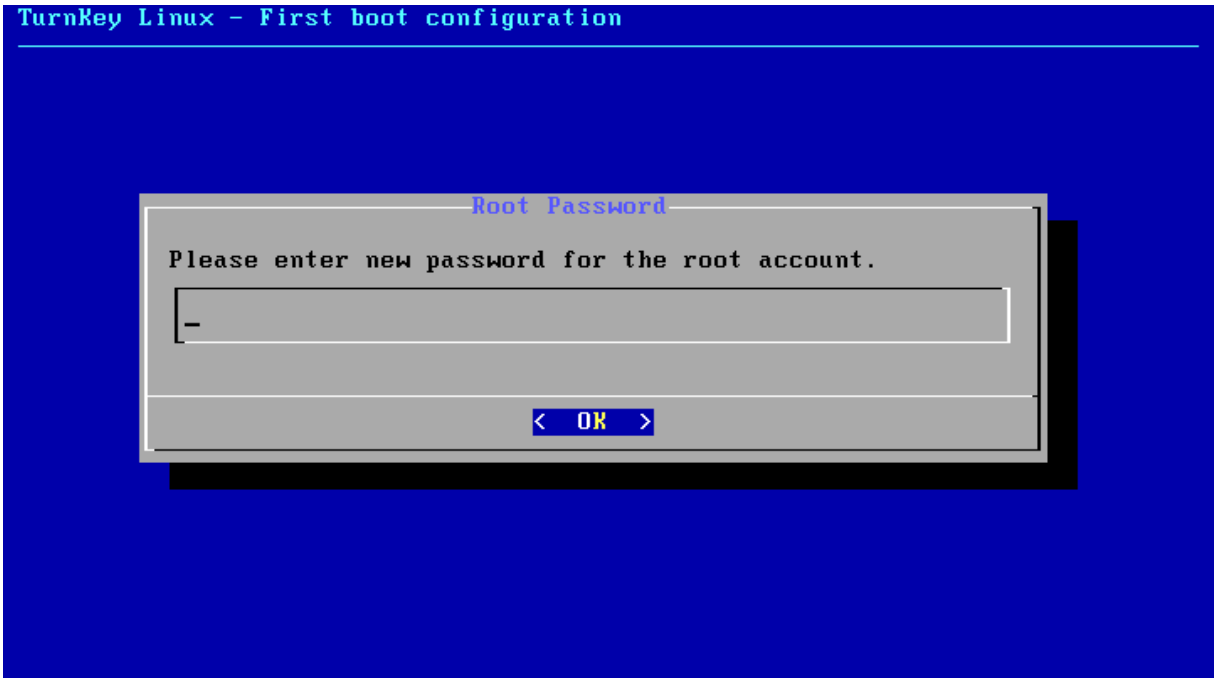
Met het onderstaande commando voegt men OSPF-events toe aan het logging-systeem. In het onderdeel "topics" specifieert men wat men wel wilt loggen, en wat niet. Hier wil ik dus wel ospf-events loggen, maar om het leesbaar te maken, wil ik geen raw-events loggen.

```
[admin@Sidonia] > /system logging add topics=ospf,!raw
[admin@Sidonia] >
```

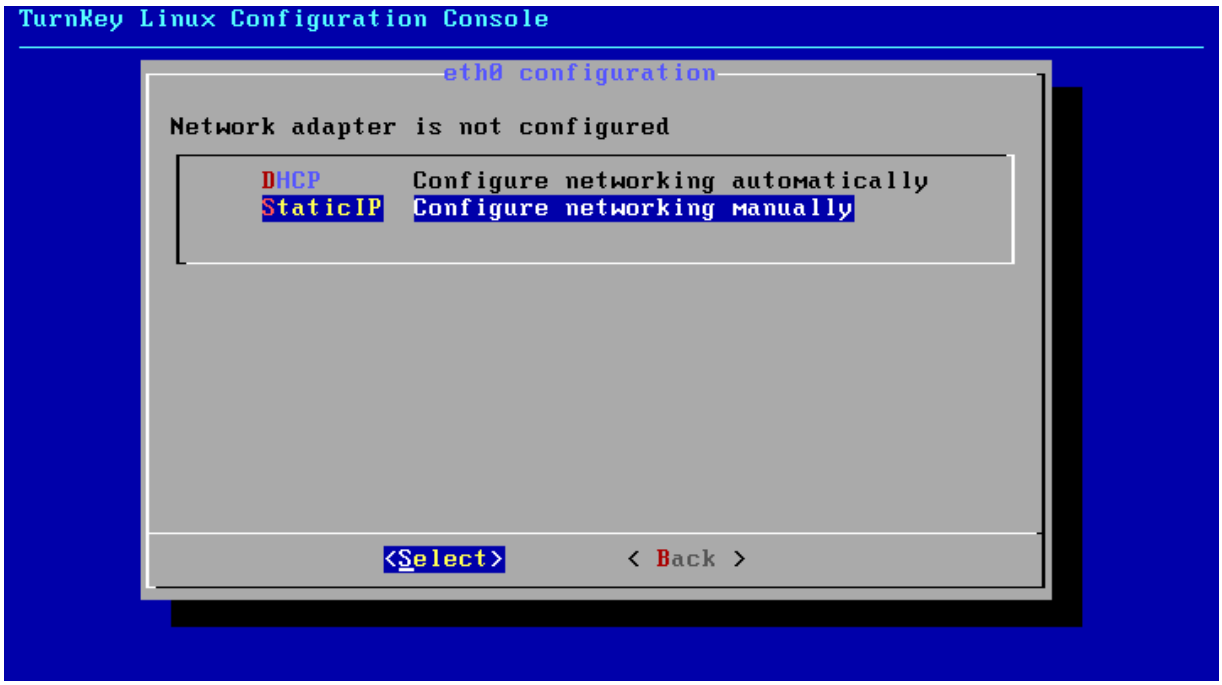
Dec/31/2014 12:10:21	memory	route, ospf, debug	SEND: Hello 172.16.0.14 -> 224.0.0.5 on ToSuske
Dec/31/2014 12:10:21	memory	route, ospf, debug	SEND: Hello 172.16.0.29 -> 224.0.0.5 on ToWiske
Dec/31/2014 12:10:22	memory	route, ospf, debug	RECV: Hello <- 172.16.0.28 on ToWiske (172.16.0.29)
Dec/31/2014 12:10:22	memory	route, ospf, debug	received options: E
Dec/31/2014 12:14:10	memory	route, ospf, info	OSPFv2 neighbor 10.0.255.1: state change from Full to Down

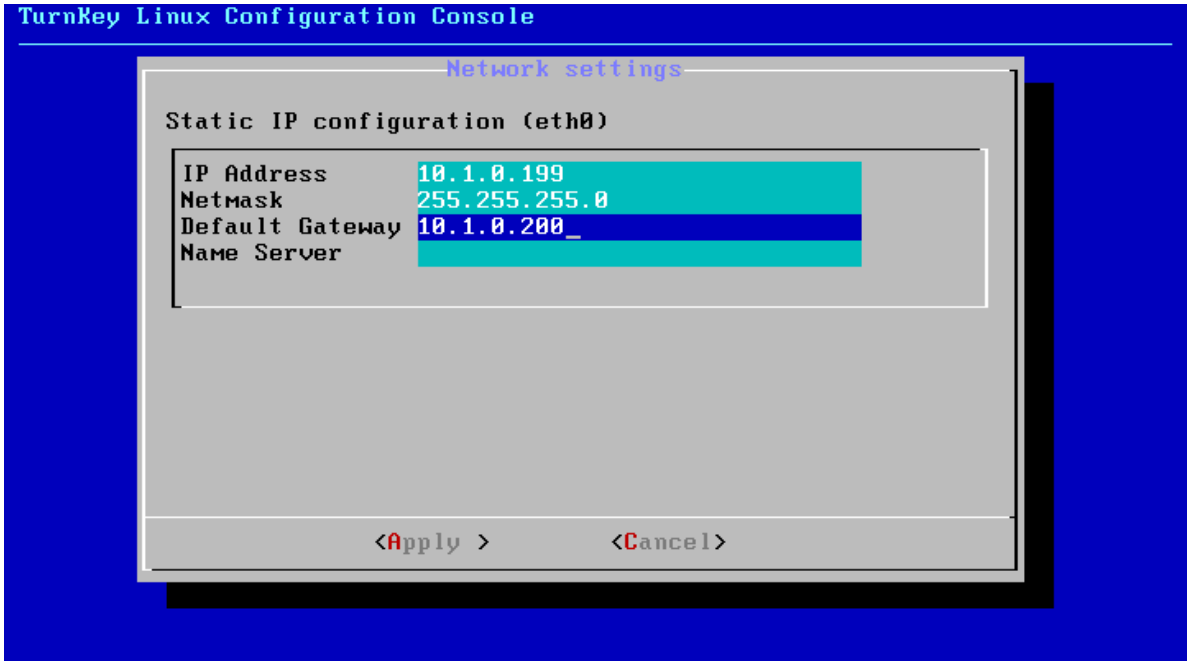
Op area 0.0.0.2 zal ik een webserver toevoegen, en op area 0.0.0.3 zal ik een linux-cliënt toevoegen.

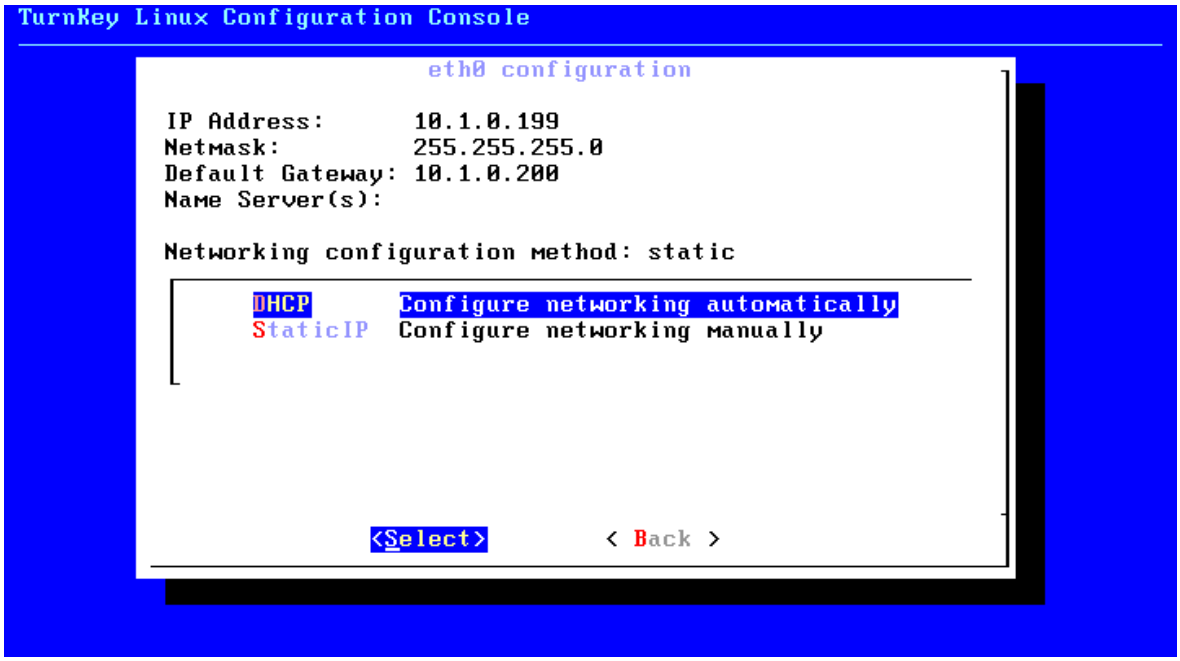
Als webserver gebruik ik de LAMP-appliance van Turnkey. Turnkey biedt kant-en-klare appliances/virtuele machines aan die men, mits enkele instellingen te wijzigen, gemakkelijk en snel kan uitrollen. De LAMP-appliance bevat bvb. al phpmyadmin en webmin voor geïnstalleerd.



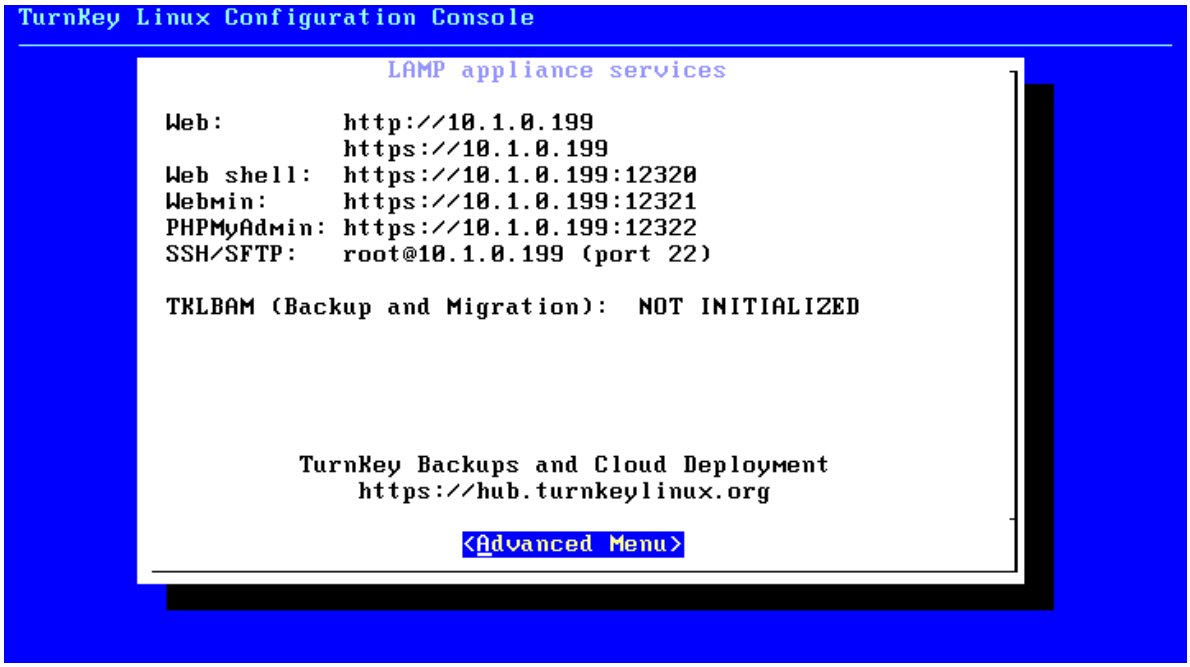
Aangezien we hier met een statisch IP-adres werken, moeten we de netwerkinstellingen nog wijzigen:



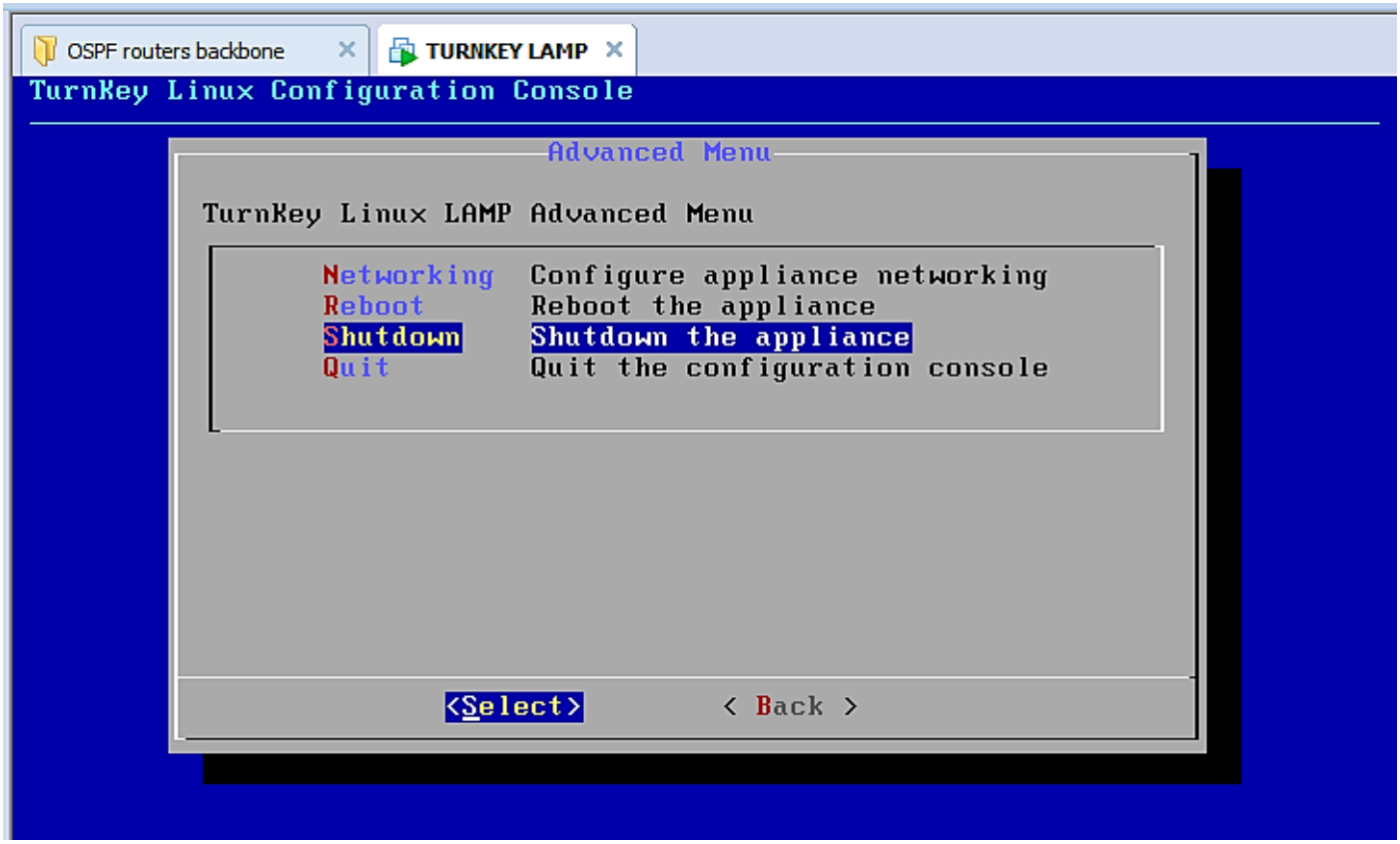

TurnKey Linux Configuration Console
Network settings
Static IP configuration (eth0)
IP Address 10.1.0.199
Netmask 255.255.255.0
Default Gateway 10.1.0.200
Name Server
<Apply >
<Cancel>


TurnKey Linux Configuration Console
eth0 configuration
IP Address: 10.1.0.199
Netmask: 255.255.255.0
Default Gateway: 10.1.0.200
Name Server(s):
Networking configuration method: static
DHCP Configure networking automatically
StaticIP Configure networking manually
<Select>
< Back >

En dit zijn enkele manieren om de webserver te bereiken, of om instellingen te wijzigen:



En als men het “advanced menu” oproept, kan men de netwerkinstellingen aanpassen, of de webserver herstarten of afsluiten.

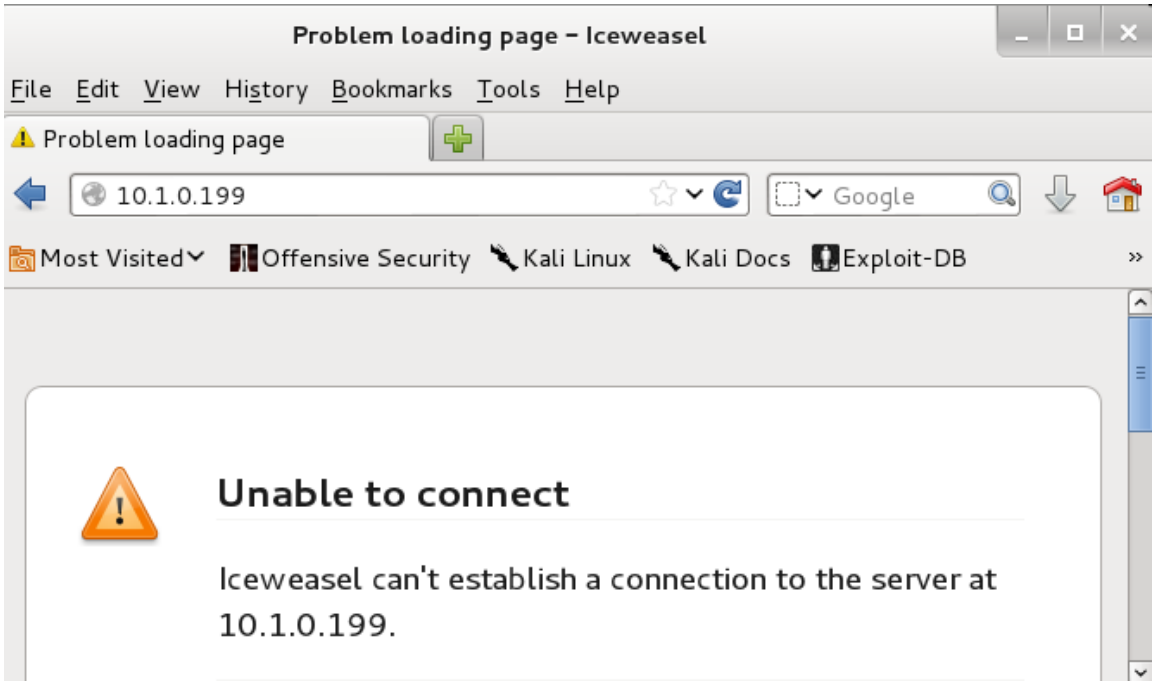


Voor de linux-cliënt maak ik gebruik van een op Debian gebaseerde distro, namelijk Kali Linux.

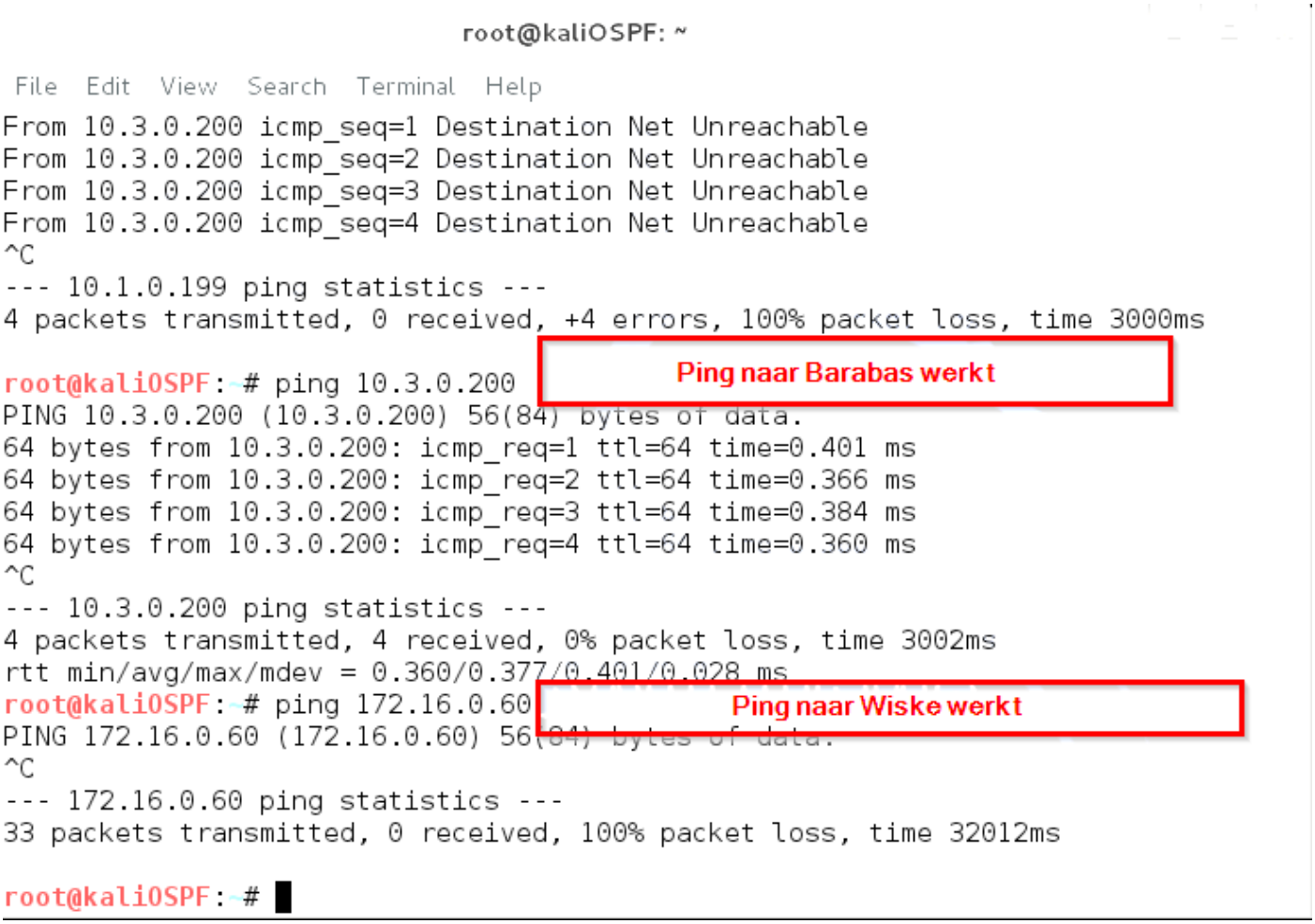
Bij de installatie van Kali op een virtuele machine stelde VMWare Workstation een harde schijf voor van 8 Gb, maar tijdens de installatie kreeg ik constant een foutmelding bij het kopiëren van bestanden van de Cd-rom naar de harde schijf. Bij onderzoek van dit probleem door het nalezen van officiële fora kwam ik te weten dat Kali toch wel 20 Gb nodig had om te werken, en 30 Gb werd zelfs aangeraden.

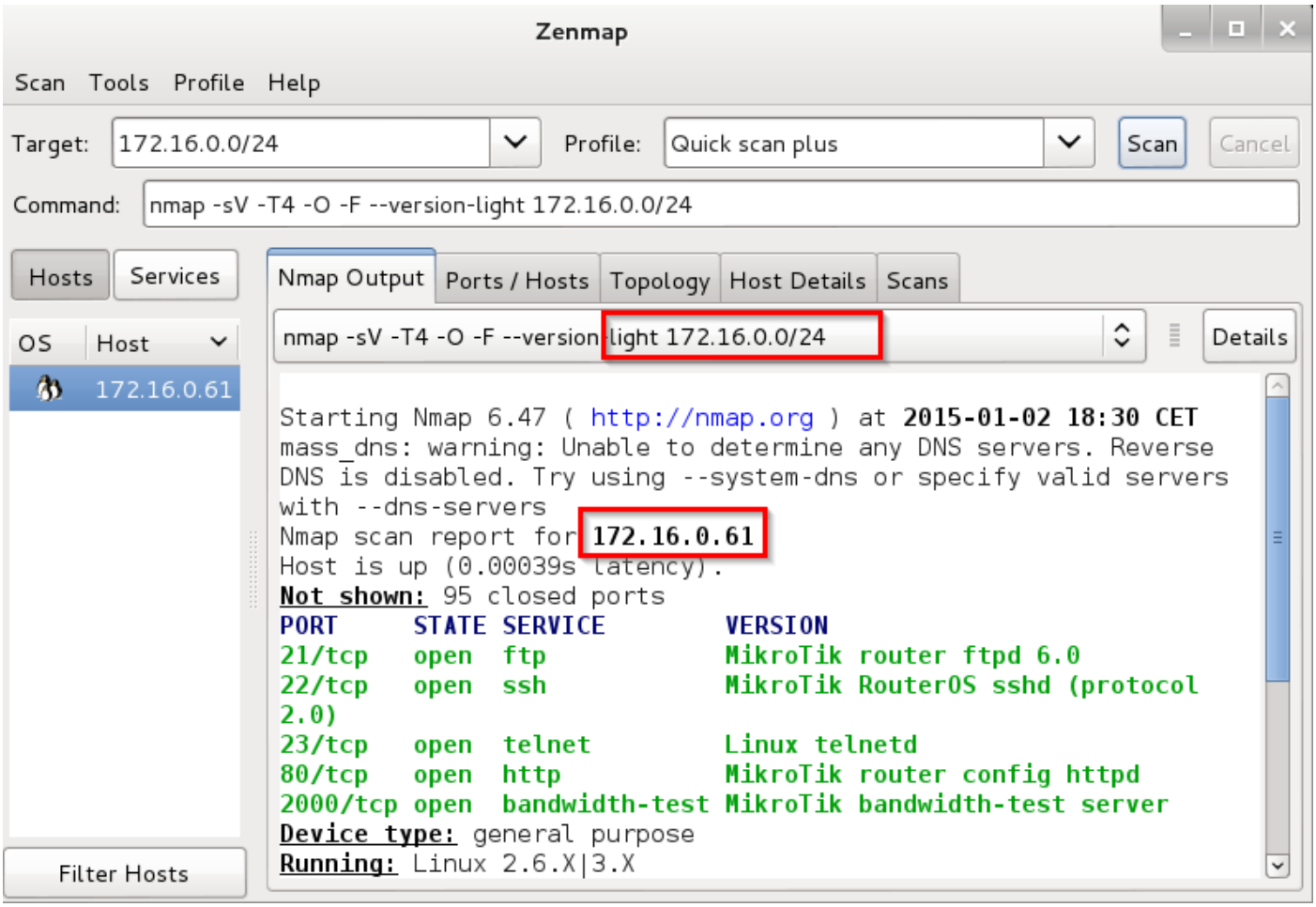
Ook hier moest ik de statische netwerk-info opgeven:

Na de installatie herstart ik de virtuele machine, en wil ik met een browser in Kali Linux naar onze webserver in de andere area surfen.



Onze webserver is niet bereikbaar, ook niet via een ping. Daarom begin ik vanaf onze cliënt naar de webserver toe te werken om te zien waar het probleem is. Aangezien ik Barabas kan pingen, en nmap Barabas ook ziet, probeer ik router Wiske te bereiken.


root@kaliOSPF: ~
File Edit View Search Terminal Help
From 10.3.0.200 icmp_seq=1 Destination Net Unreachable
From 10.3.0.200 icmp_seq=2 Destination Net Unreachable
From 10.3.0.200 icmp_seq=3 Destination Net Unreachable
From 10.3.0.200 icmp_seq=4 Destination Net Unreachable
^C
--- 10.1.0.199 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3000ms
root@kaliOSPF:~# ping 10.3.0.200
Ping naar Barabas werkt
PING 10.3.0.200 (10.3.0.200) 56(84) bytes of data.
64 bytes from 10.3.0.200: icmp_req=1 ttl=64 time=0.401 ms
64 bytes from 10.3.0.200: icmp_req=2 ttl=64 time=0.366 ms
64 bytes from 10.3.0.200: icmp_req=3 ttl=64 time=0.384 ms
64 bytes from 10.3.0.200: icmp_req=4 ttl=64 time=0.360 ms
^C
--- 10.3.0.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.360/0.377/0.401/0.028 ms
root@kaliOSPF:~# ping 172.16.0.60
Ping naar Wiske werkt
PING 172.16.0.60 (172.16.0.60) 56(84) bytes of data.
^C
--- 172.16.0.60 ping statistics ---
33 packets transmitted, 0 received, 100% packet loss, time 32012ms
root@kaliOSPF:~#


Zenmap
Scan Tools Profile Help
Target: 172.16.0.0/24
Profile: Quick scan plus
Scan
Cancel
Command: nmap -sV -T4 -O -F --version-light 172.16.0.0/24
Hosts
Services
OS
Host
172.16.0.61
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV -T4 -O -F --version-light 172.16.0.0/24
Details
Starting Nmap 6.47 (http://nmap.org) at 2015-01-02 18:30 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.0.61
Host is up (0.00039s latency).
Not shown: 95 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp MikroTik router ftpd 6.0
22/tcp open ssh MikroTik RouterOS sshd (protocol 2.0)
23/tcp open telnet Linux telnetd
80/tcp open http MikroTik router config httpd
2000/tcp open bandwidth-test MikroTik bandwidth-test server
Device type: general purpose
Running: Linux 2.6.X|3.X

Aangezien ik met nmap het volledige 172.16.0.0/24 netwerk scande en alleen de interface van router Wiske in de area 0.0.0.3 zichtbaar was, vermoedde ik een probleem met de instellingen van die area. Dit ook omdat ik van Wiske perfect de backbone kon bereiken.

```
[admin@Barabas] > ping 172.16.0.60
HOST                                     SIZE TTL TIME  STATUS
172.16.0.60                                56  64 0ms
172.16.0.60                                56  64 0ms
172.16.0.60                                56  64 0ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@Barabas] > ping 172.16.0.44
HOST                                     SIZE TTL TIME  STATUS
                                                       no route to host
                                                       no route to host
                                                       no route to host
                                                       no route to host
    sent=4 received=0 packet-loss=100%

[admin@Barabas] >
```

```
[admin@Wiske] > ping 172.16.0.60
HOST                                     SIZE TTL TIME  STATUS
172.16.0.60                                56  64 1ms
172.16.0.60                                56  64 7ms
    sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=4ms max-rtt=7ms

[admin@Wiske] > ping 172.16.0.53
HOST                                     SIZE TTL TIME  STATUS
172.16.0.53                                56  64 0ms
172.16.0.53                                56  64 0ms
    sent=2 received=2 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

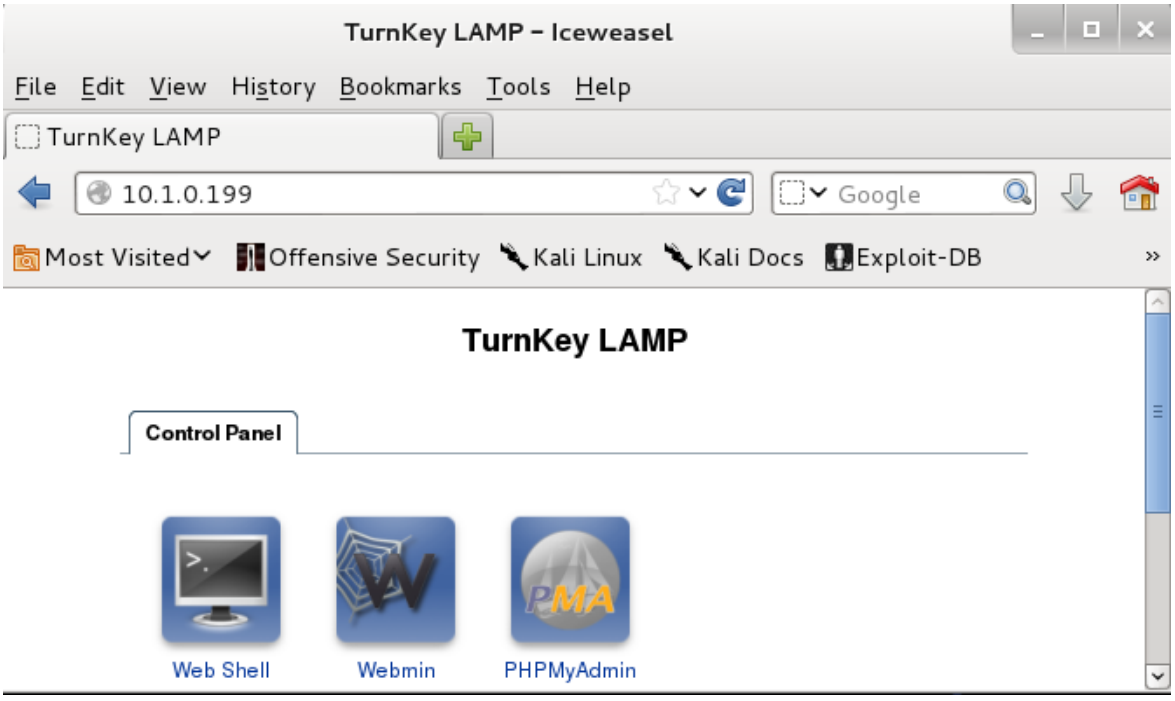
Ping naar Barabas

Ping naar Suske

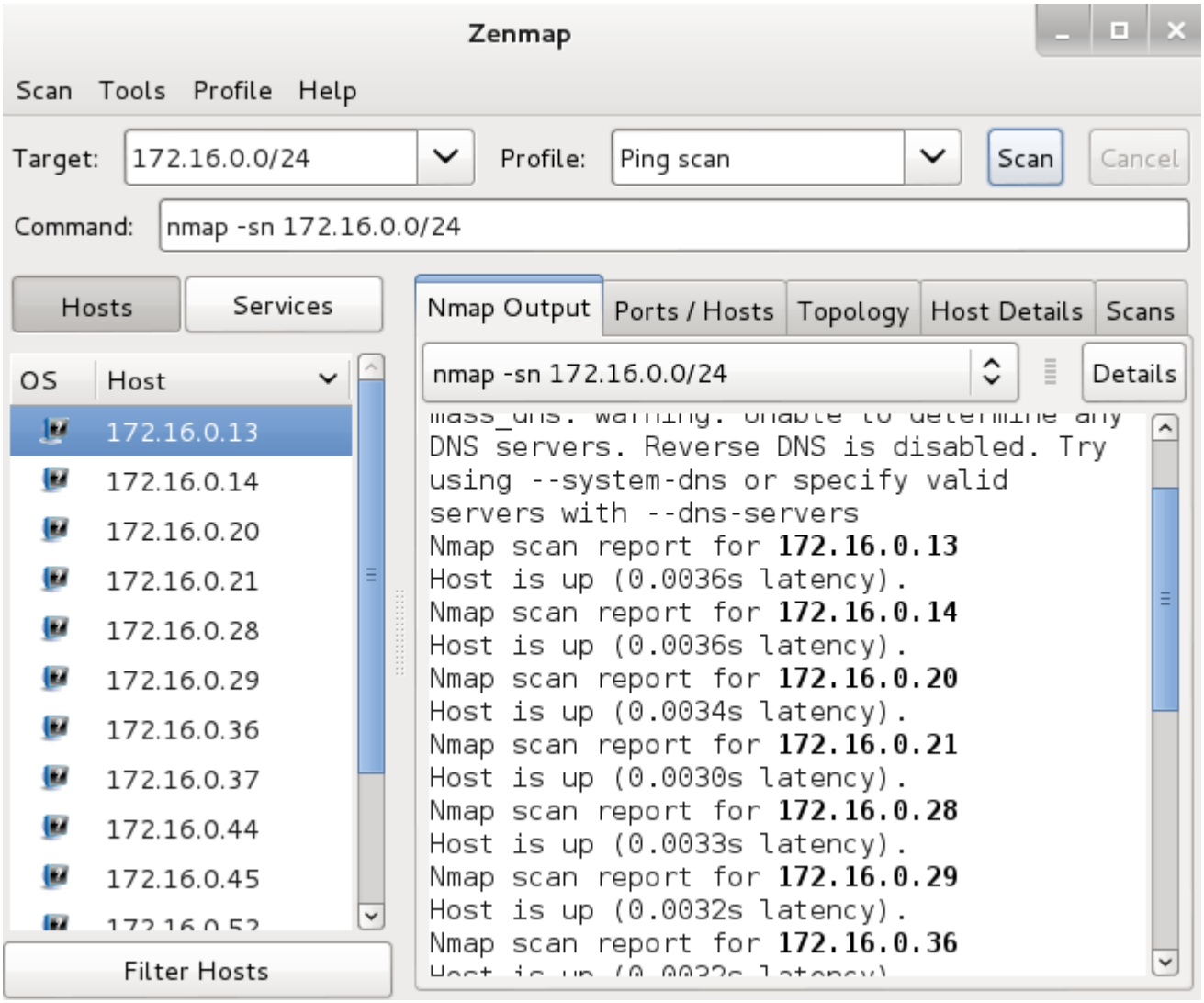
Dus veranderde ik op router Barabas en router Lambik de area van stub naar normaal. Na deze verandering kon router Wiske de webserver bereiken.

```
[admin@Wiske] > ping 10.1.0.199
HOST                                     SIZE TTL TIME  STATUS
10.1.0.199                                                timeout
10.1.0.199                                                timeout
10.1.0.199                                                timeout
10.1.0.199                                                timeout
10.1.0.199                                                timeout
10.1.0.199                                 56  62 1ms
10.1.0.199                                 56  62 1ms
10.1.0.199                                 56  62 1ms
10.1.0.199                                 56  62 1ms
    sent=9 received=4 packet-loss=55% min-rtt=1ms avg-rtt=1ms max-rtt=1ms
```

Ook van de Kali-cliënt kan ik de webserver bereiken:



Als we nu een nmap-scan doen van het 172.16.0.0/24 netwerk, zien we alle IP-adressen van ons backbone-netwerk.

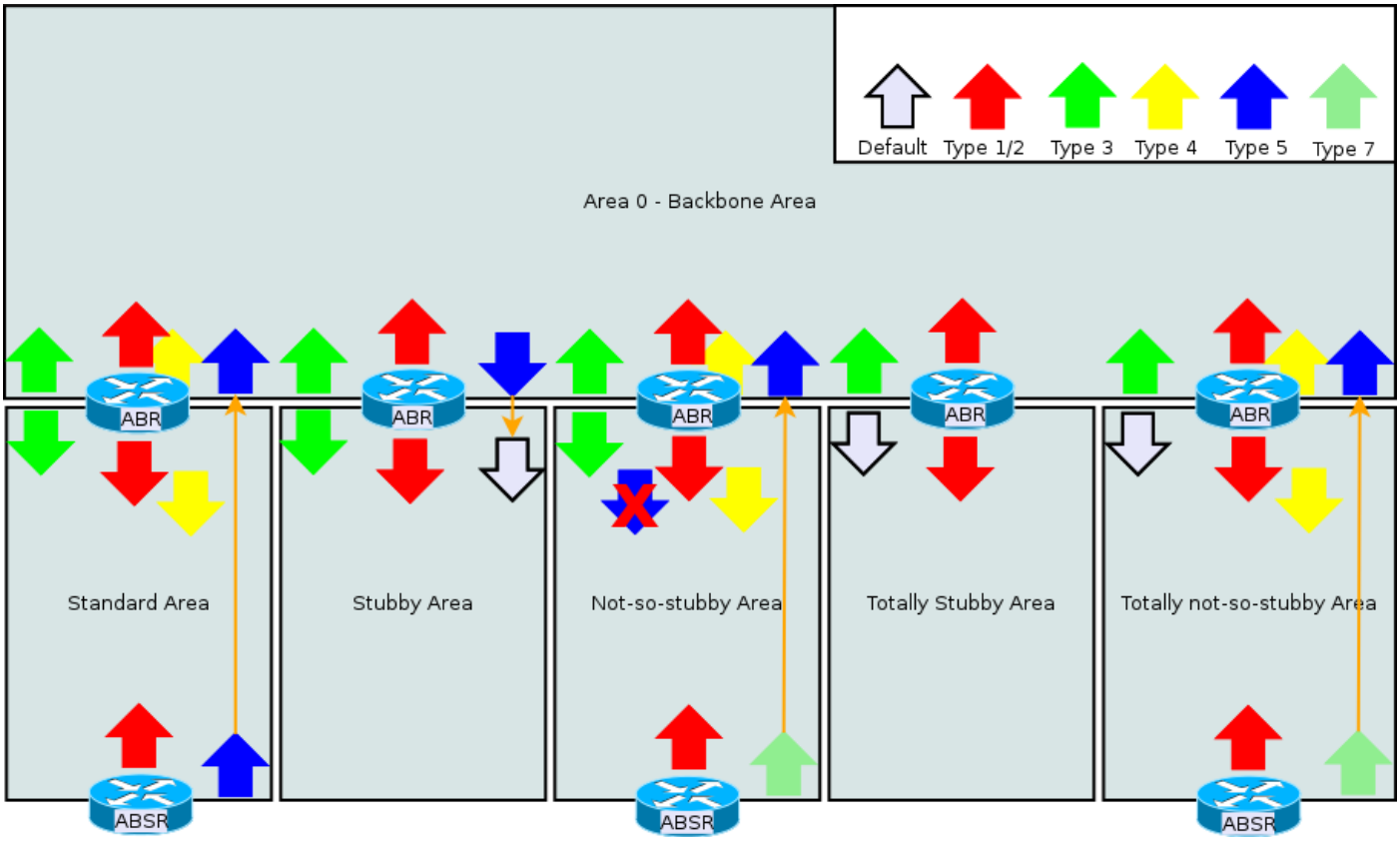


Dit probleem had ik kunnen voorzien aangezien bij een stub area bij OSPF de area border router alleen type 3 LSA's doorstuurt. Dit zijn "summary" link state advertisements.

Er worden bij standaard OSPF 8 types link state advertisements gebruikt. Er bestaan nog 3 andere LSA's, die door specifieke applicaties kunnen gebruikt worden als uitbreiding.

LSA	UITLEG
1	Dit is een "router"-LSA en wordt door alle routers gemaakt om directe buren te beschrijven. Het gaat hier om intra-area verkeer, dus dit type LSA verlaat de area niet.
2	Type 2-LSA's zijn netwerk-LSA's en worden door de designated router gemaakt om alle buren van dat segment op te noemen. Ook deze LSA's zijn intra-area.
3	Hier gaat het over een "summary"-LSA die door de area border router (ABR) gemaakt is om aan de zone te vertellen welke routes er grenzen aan die zone. Dit is een intra-area route.
4	Ook dit is een "summary"-LSA die de ABR gebruikt om aan routers buiten de area de route naar de ASBR (autonomous system border router) te vertellen.
5	Dit is een external LSA, gemaakt door de ASBR om in het OSPF-domein te melden welke routes er buiten het domein liggen.
6	Deze LSA is gebruikt voor multicast OSPF. Wordt niet door alle router-producenten ondersteund.
7	Type 7-LSA's zijn LSA's speciaal voor not so stubby area's. Als de ASBR in zo een area ligt, zal hij externe routes met zo'n LSA beschrijven. Van het moment dat deze LSA de not so stubby area verlaat, wordt deze "vertaald" naar type 5-LSA's
8	Een type 8-LSA is een LSA die gebruikt is bij OSPFv3 en geeft IPv6 info door. Oorspronkelijk bedoelt om een ander routing protocol, internal BGP, te vervangen. Routing info zou dan in een type 5 LSA komen, en de BGP info in een type 8 LSA

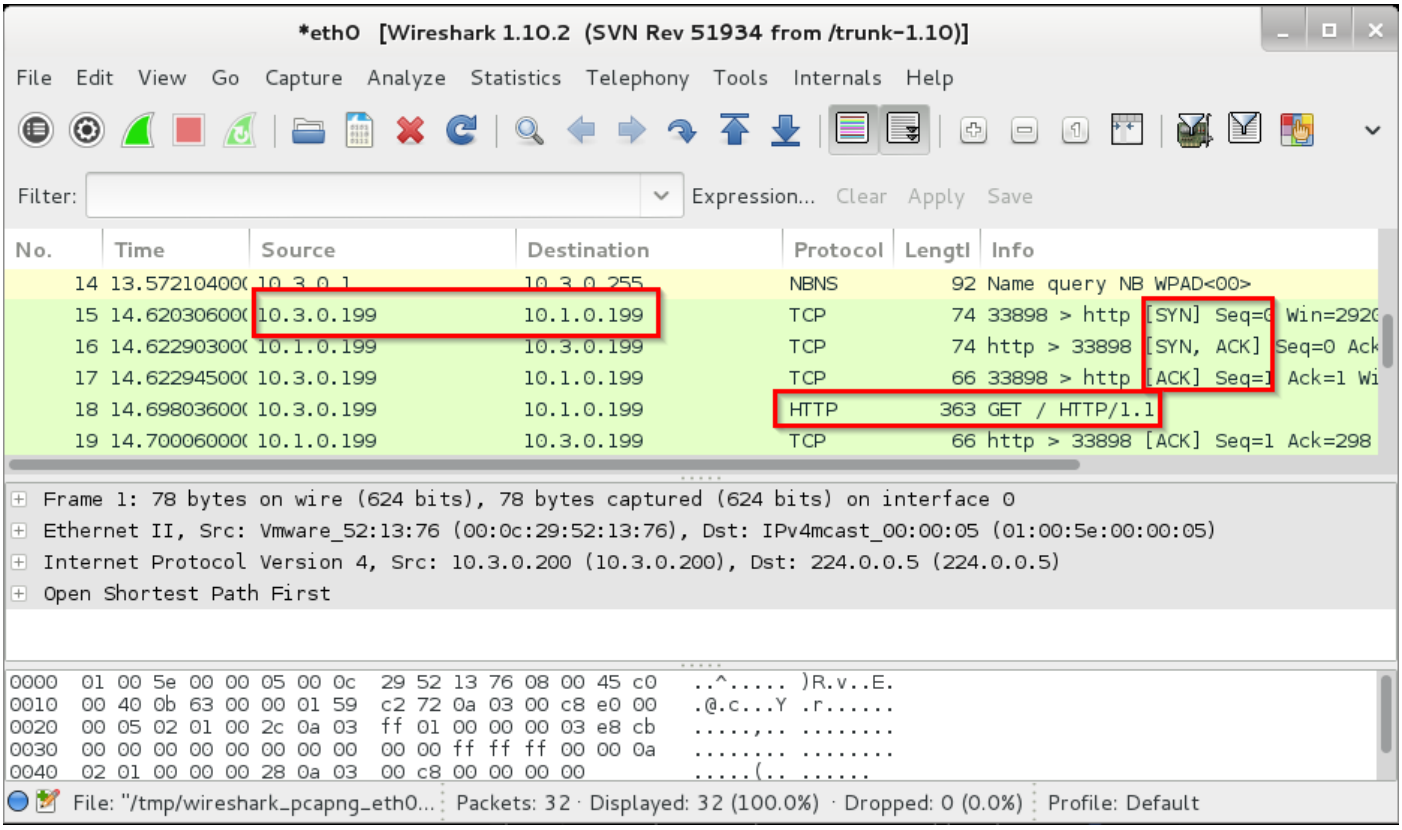
Naargelang het type router en het type area worden bepaalde LSA's wel of niet doorgegeven, en soms maar in één richting.



De oplossing die ik had gebruikt, het uitschakelen van de stub-functionaliteit is een mogelijkheid, maar ik merkte ook dat ik de instellingen voor stub op Lambik en Barabas had gedaan. Aangezien in deze oefening router Suske en Wiske de area border router zijn, denk ik dat op alle routers de desbetreffende area's op stub had moeten zetten. Dit heb ik nog niet kunnen testen.

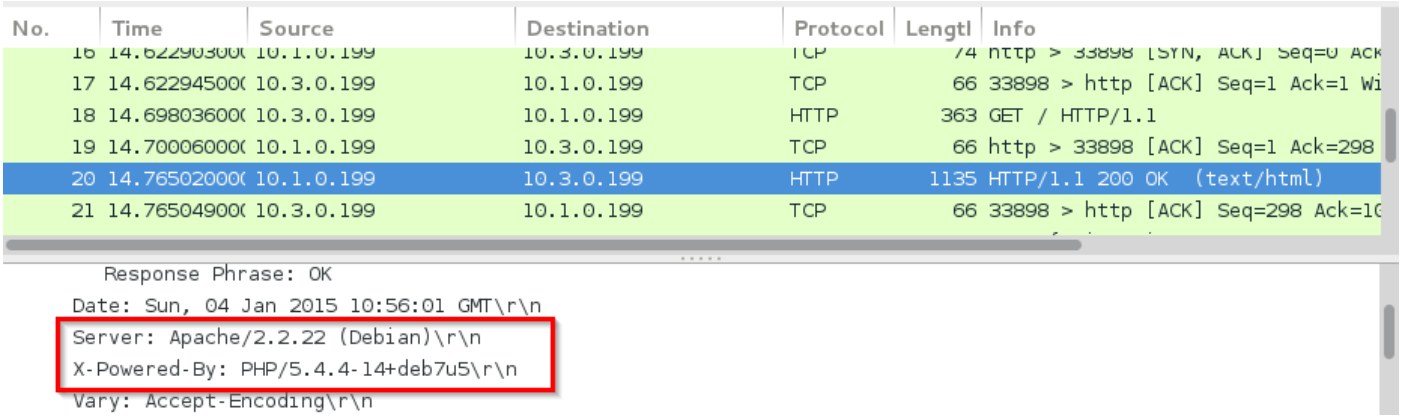
Analyse van het verkeer tussen webserver en cliënt

Aangezien Kali een distro is, gespecialiseerd in security, zijn er al heel wat tools voor geïnstalleerd. Een van deze tools is het ons bekende Wireshark. Ik analyseer het verkeer als ik vanaf de cliënt naar de webserver surf.

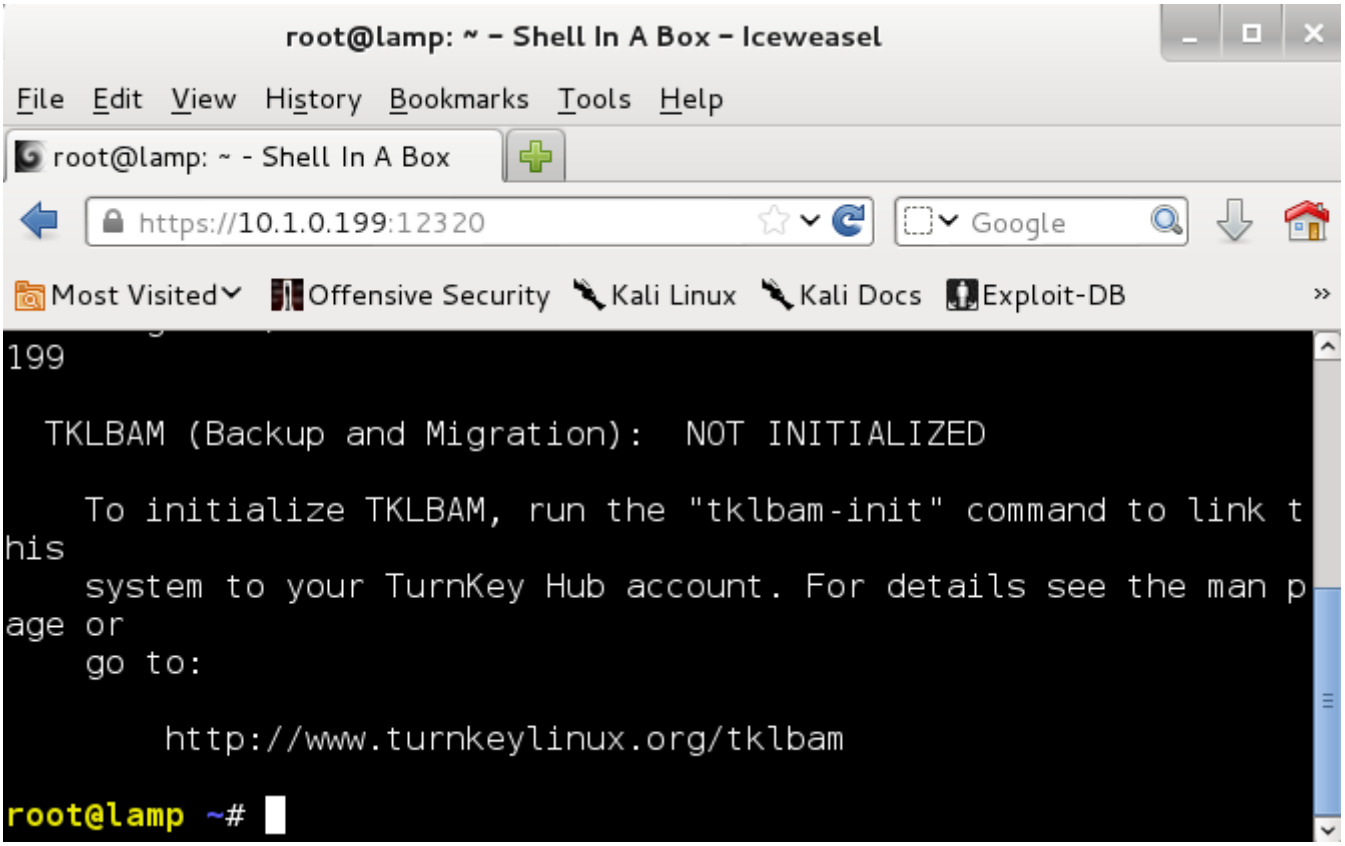


Op bovenstaande screenshot zie je het tot stand komen van een TCP-connectie tussen de cliënt en server, met daarna een http GET-methode.

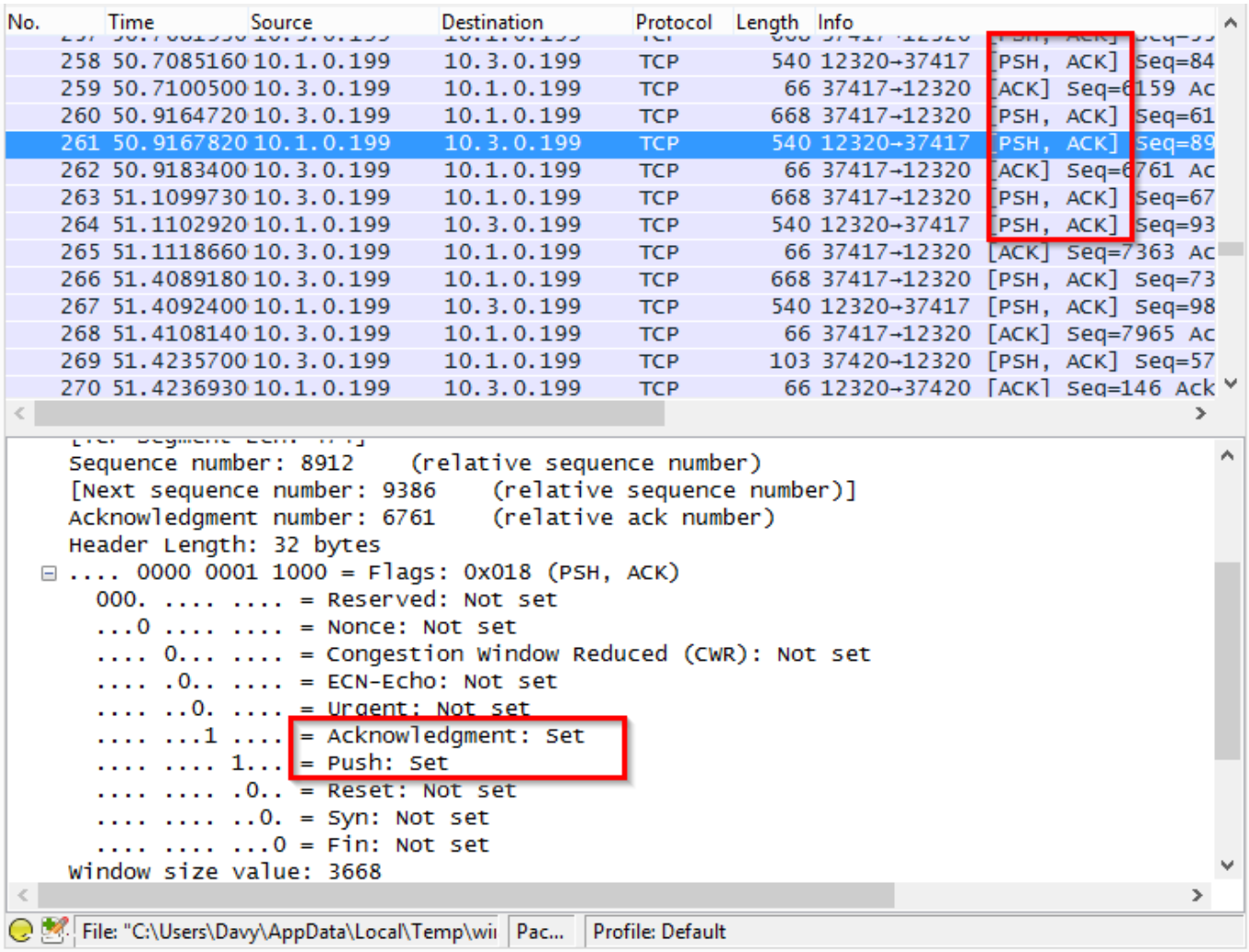
Ook leerde ik dat de appliance van Turnkey gebruik maakt van Apache 2.2 en PHP 5.4.4. Op het moment van schrijven is van Apache versie 2.4 uit, en van PHP versie 5.6, dus de Turnkey-appliances zijn iets verouderd.



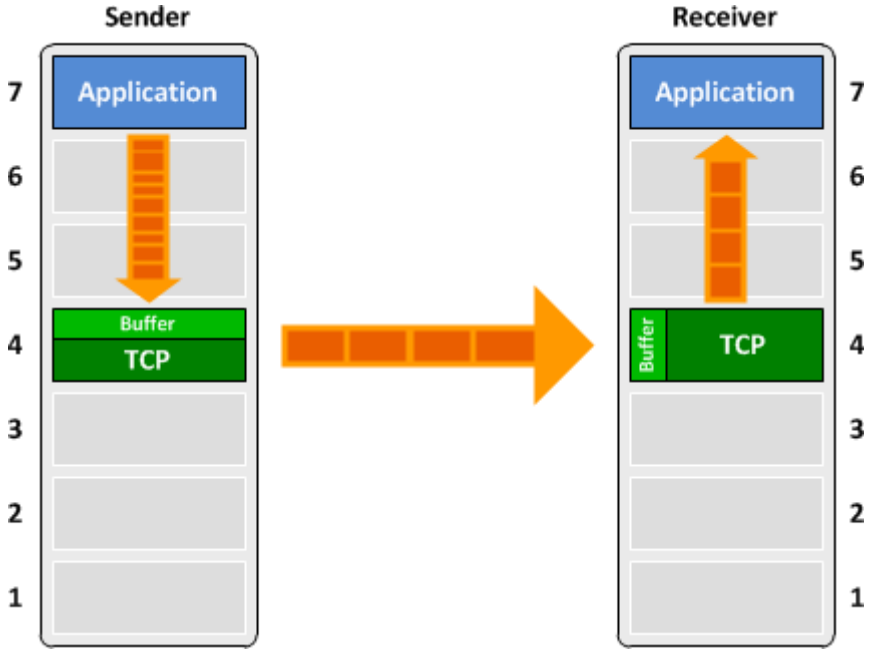
Vanaf de Kali-cliënt kan ik nu een command prompt openen, mits ik de juiste inloggegevens heb.



Tijdens het starten van deze “web shell” had ik op mijn host Wireshark aangeschakeld, en ik ving dit op:


No. Time Source Destination Protocol Length Info
258 50.7085160 10.1.0.199 10.3.0.199 TCP 540 12320→37417 [PSH, ACK] Seq=84
259 50.7100500 10.3.0.199 10.1.0.199 TCP 66 37417→12320 [ACK] Seq=6159 Ac
260 50.9164720 10.3.0.199 10.1.0.199 TCP 668 37417→12320 [PSH, ACK] Seq=61
261 50.9167820 10.1.0.199 10.3.0.199 TCP 540 12320→37417 [PSH, ACK] Seq=89
262 50.9183400 10.3.0.199 10.1.0.199 TCP 66 37417→12320 [ACK] Seq=6761 Ac
263 51.1099730 10.3.0.199 10.1.0.199 TCP 668 37417→12320 [PSH, ACK] Seq=67
264 51.1102920 10.1.0.199 10.3.0.199 TCP 540 12320→37417 [PSH, ACK] Seq=93
265 51.1118660 10.3.0.199 10.1.0.199 TCP 66 37417→12320 [ACK] Seq=7363 Ac
266 51.4089180 10.3.0.199 10.1.0.199 TCP 668 37417→12320 [PSH, ACK] Seq=73
267 51.4092400 10.1.0.199 10.3.0.199 TCP 540 12320→37417 [PSH, ACK] Seq=98
268 51.4108140 10.3.0.199 10.1.0.199 TCP 66 37417→12320 [ACK] Seq=7965 Ac
269 51.4235700 10.3.0.199 10.1.0.199 TCP 103 37420→12320 [PSH, ACK] Seq=57
270 51.4236930 10.1.0.199 10.3.0.199 TCP 66 12320→37420 [ACK] Seq=146 Ack
Sequence number: 8912 (relative sequence number)
[Next sequence number: 9386 (relative sequence number)]
Acknowledgment number: 6761 (relative ack number)
Header Length: 32 bytes
.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
Window size value: 3668
File: "C:\Users\Davy\AppData\Local\Temp\wi
Pac...
Profile: Default

De PSH TCP-flags vertellen mij dat deze toepassing werkt met een buffer. De flags dienen ervoor om ons communicatiesysteem te vertellen dat de gebufferde data mag doorgestuurd worden, ook al is de maximum grootte van het data-segment nog niet bereikt.



Ook de RST-flag zag ik in de Wireshark-capture, ofwel de “reset”-flag. Dit wil zeggen dat de verbinding op dat moment geherinitialiseerd werd omdat er een fout optrad.

Schema's

Virtuele netwerken

Vmnets			
172.16.0.16/29	vmnet2	172.16.0.17	172.16.0.22
172.16.0.32/29	vmnet3	172.16.0.33	172.16.0.38
172.16.0.48/29	vmnet4	172.16.0.49	172.16.0.54
172.16.0.8/29	vmnet5	172.16.0.9	172.16.0.14
172.16.0.24/29	vmnet6	172.16.0.25	172.16.0.30
172.16.0.40/29	vmnet7	172.16.0.41	172.16.0.46
10.1.0.0	vmnet9	10.1.0.1	10.1.0.254
10.3.0.0	vmnet10	10.3.0.1	10.3.0.254
172.16.0.56	vmnet11	172.16.0.57	172.16.0.62
10.1.1.0	vmnet12	10.1.1.1	10.1.1.254
10.1.2.0	vmnet13	10.1.2.1	10.1.2.254
10.3.1.0	vmnet14	10.3.1.1	10.3.1.254
10.3.2.0	vmnet15	10.3.2.1	10.3.2.254

Routers

Suske				
wiske	172.16.0.21	/29	ToWiske	vmnet2
jerom	172.16.0.37	/29	ToJerom	vmnet3
lambik	172.16.0.53	/29	ToLambik	vmnet4
sidonia	172.16.0.13	/29	ToSidonia	vmnet5
loopbackSuske	10.0.255.1	/32	loopbackSuske	

Wiske				
suske	172.16.0.20	/29	ToSuske	vmnet2
jerom	172.16.0.44	/29	ToJerom	vmnet7
barabas	172.16.0.60	/29	ToBarabas	vmnet11
sidonia	172.16.0.28	/29	ToSidonia	vmnet6
loopbackWiske	10.2.255.1	/32	loopbackWiske	

Sidonia				
suske	172.16.0.14	/29	ToSuske	vmnet5
wiske	172.16.0.29	/29	ToWiske	vmnet6
eigen pc	192.168.9.x	/24	ToHost	vmnet0(bridged)
loopbackSidonia	10.4.255.1	/32	loopbackSidonia	

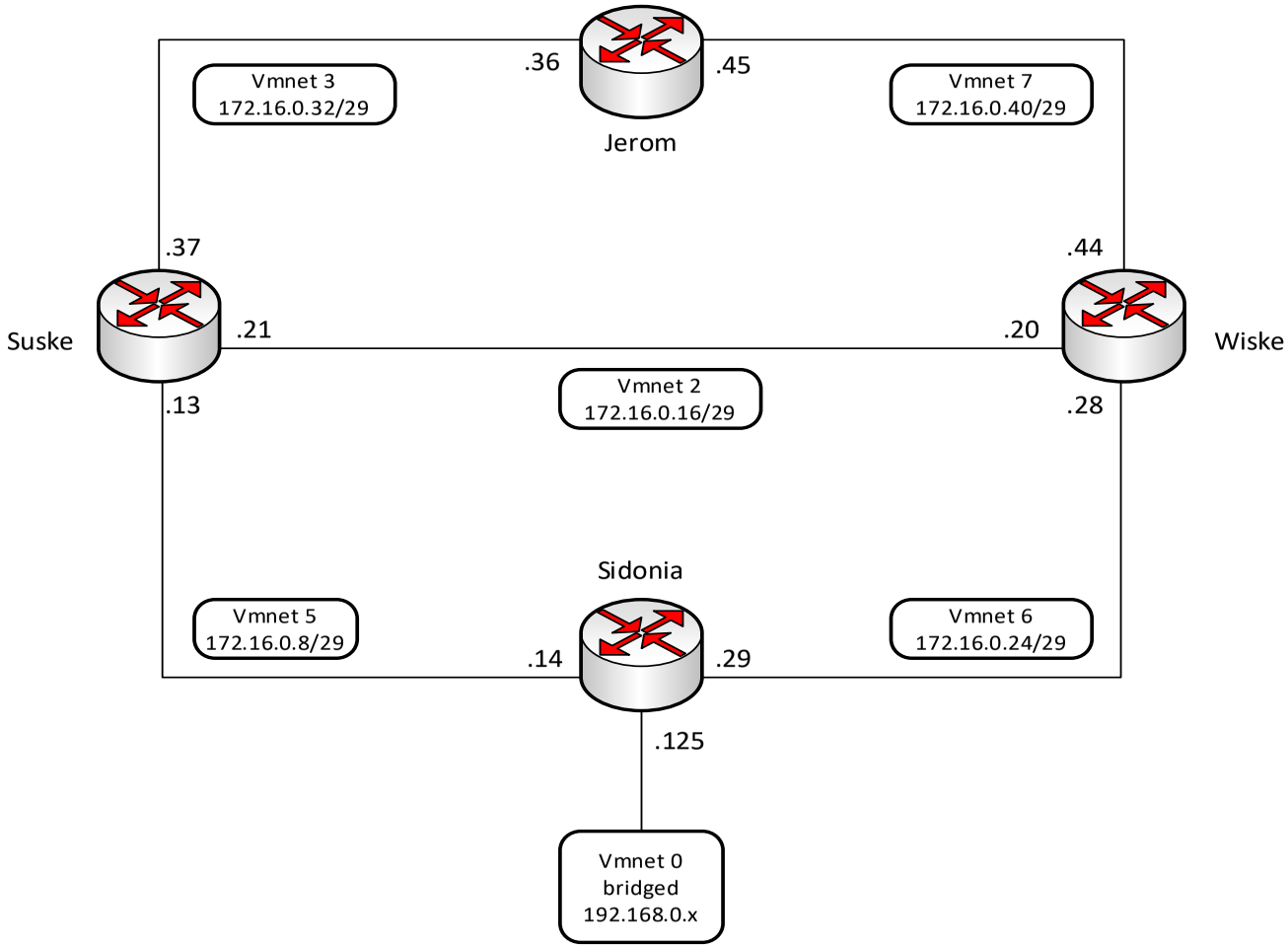
Jerom				
suske	172.16.0.36	/29	ToSuske	vmnet3
wiske	172.16.0.45	/29	ToWiske	vmnet7
loopbackJerom	10.5.255.1	/32	loopbackJerom	

Barabas				
wiske	172.16.0.61	/29	ToWiske	vmnet11
charlie	10.3.0.200	/24	ToCharlie	vmnet10
loopbackBarabas	10.3.255.1	/32	loopbackBarabas	

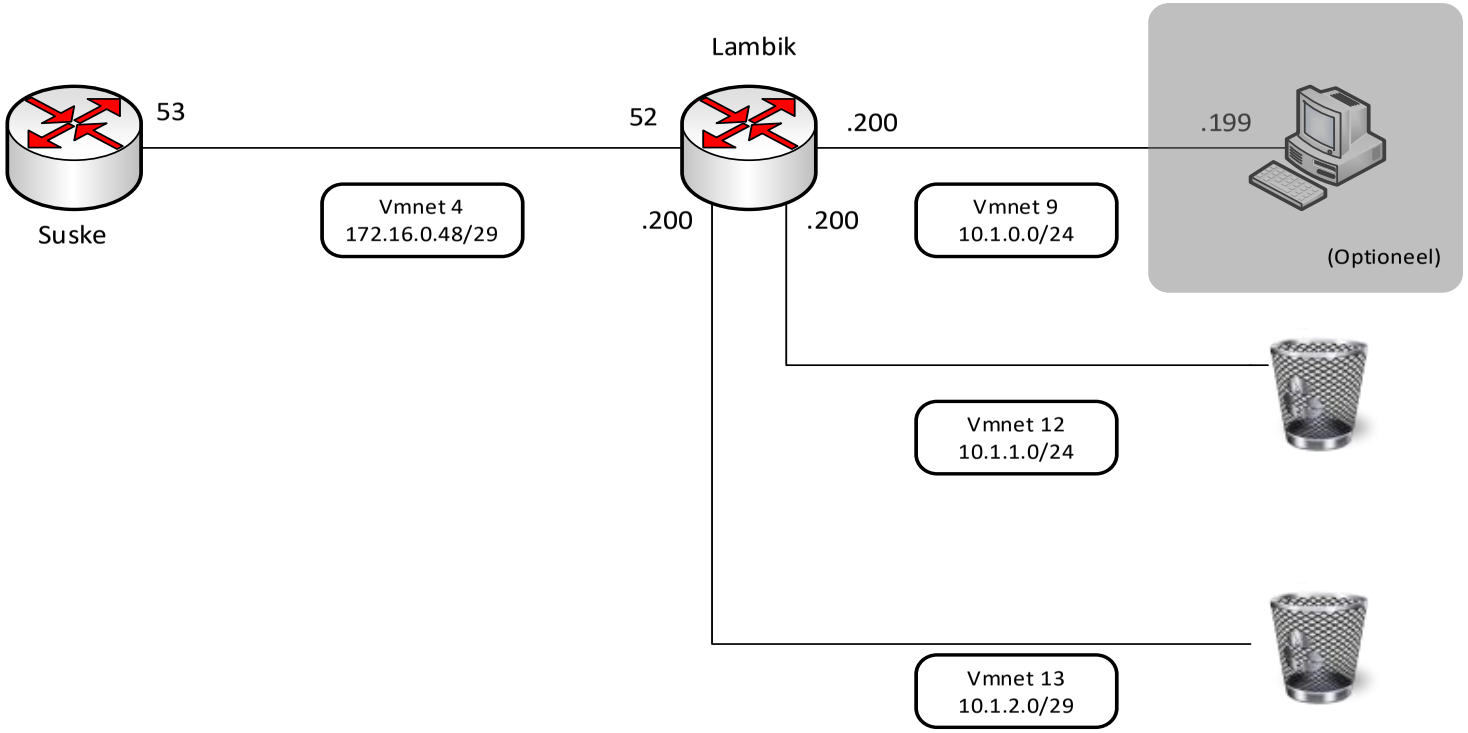
10.1.1.0 en 10.1.2.0/24 blackhole

Lambik				
suske	172.16.0.52	/29	ToSuske	vmnet4
alpha	10.1.0.200	/24	ToAlpha	vmnet9
loopbackLambik	10.1.255.1	/32	loopbackLambik	

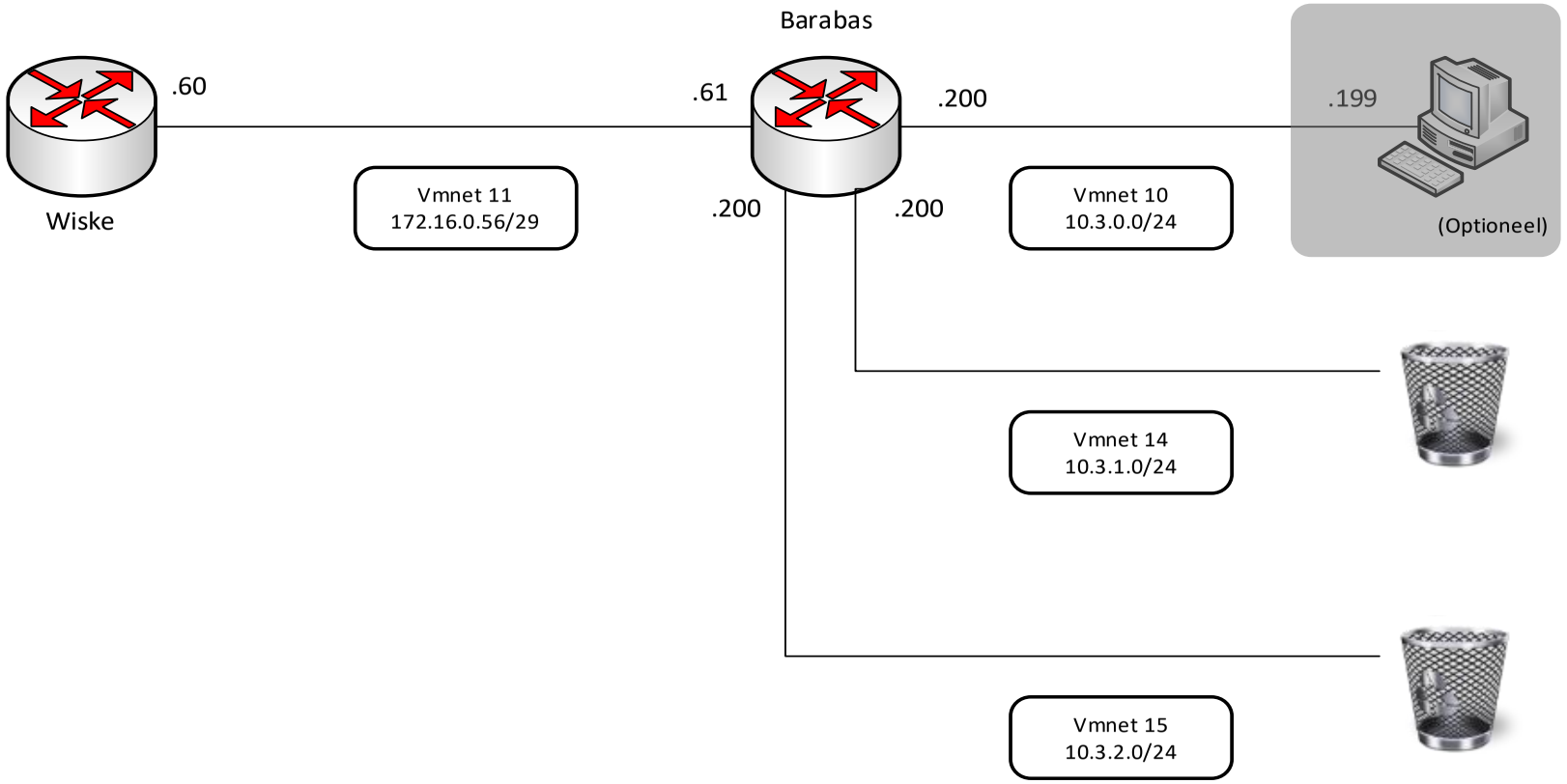
10.1.1.0 en 10.1.2.0/24 blackhole



TITLE			
Backbone OSPF			
DRAWN BY	DATE	REVISED	VERSION
Davy Van Eynde	15/10/2014	28/12/2014	2.0



TITLE			
Area 0.0.0.2			
DRAWN BY	DATE	REVISED	VERSION
Davy Van Eynde	28/12/2014	28/12/2014	1.0

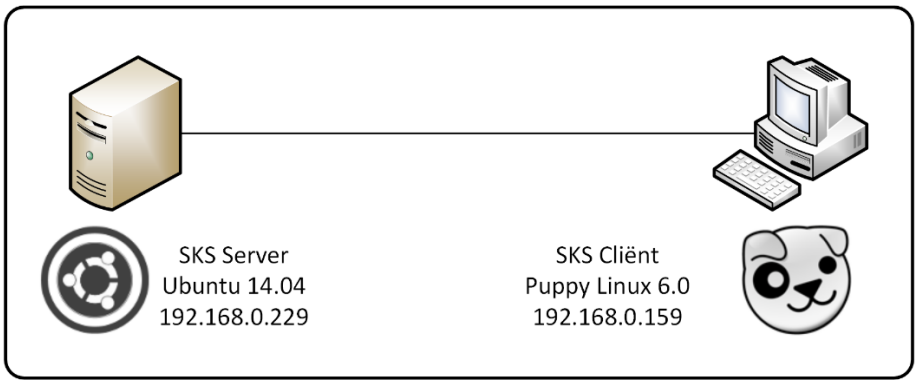


TITLE			
Area 0.0.0.3			
DRAWN BY	DATE	REVISED	VERSION
Davy Van Eynde	28/12/2014	28/12/2014	1.0

Een eigen keyserver opzetten

Voorbereiding

In deze oefening maak ik gebruik van twee virtuele machines, namelijk één Ubuntu-machine die als keyserver zal dienen en één cliënt die verbinding zal maken met de keyserver. Deze cliënt zal als OS Puppy Linux draaien.

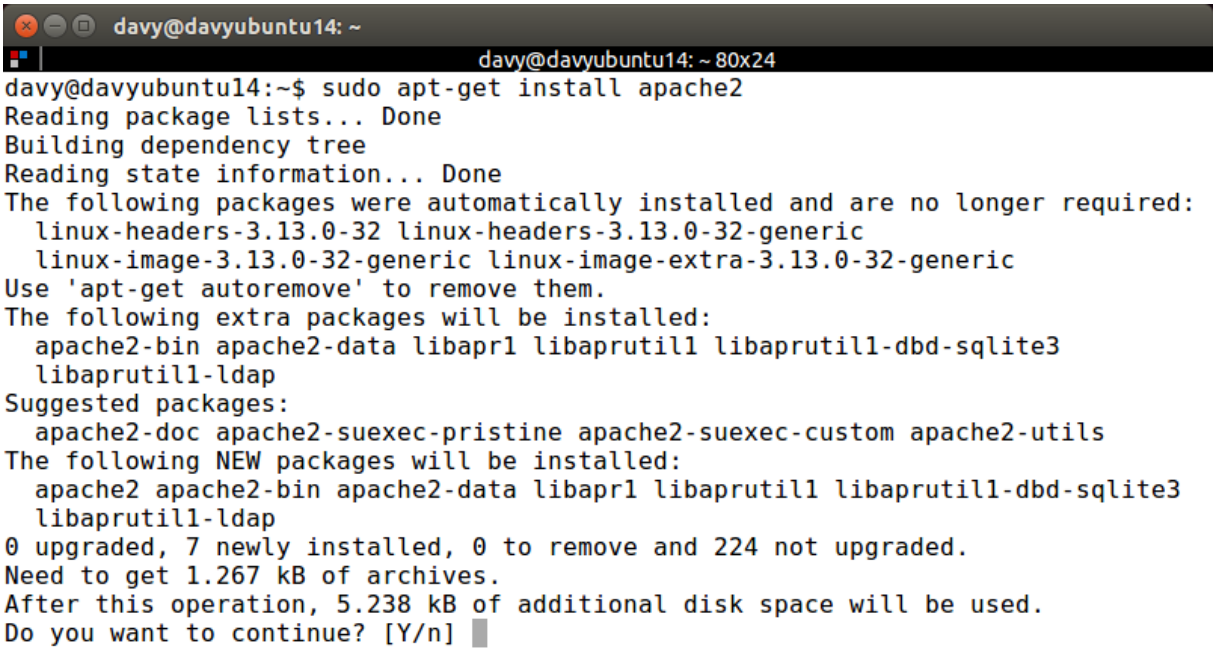


Server

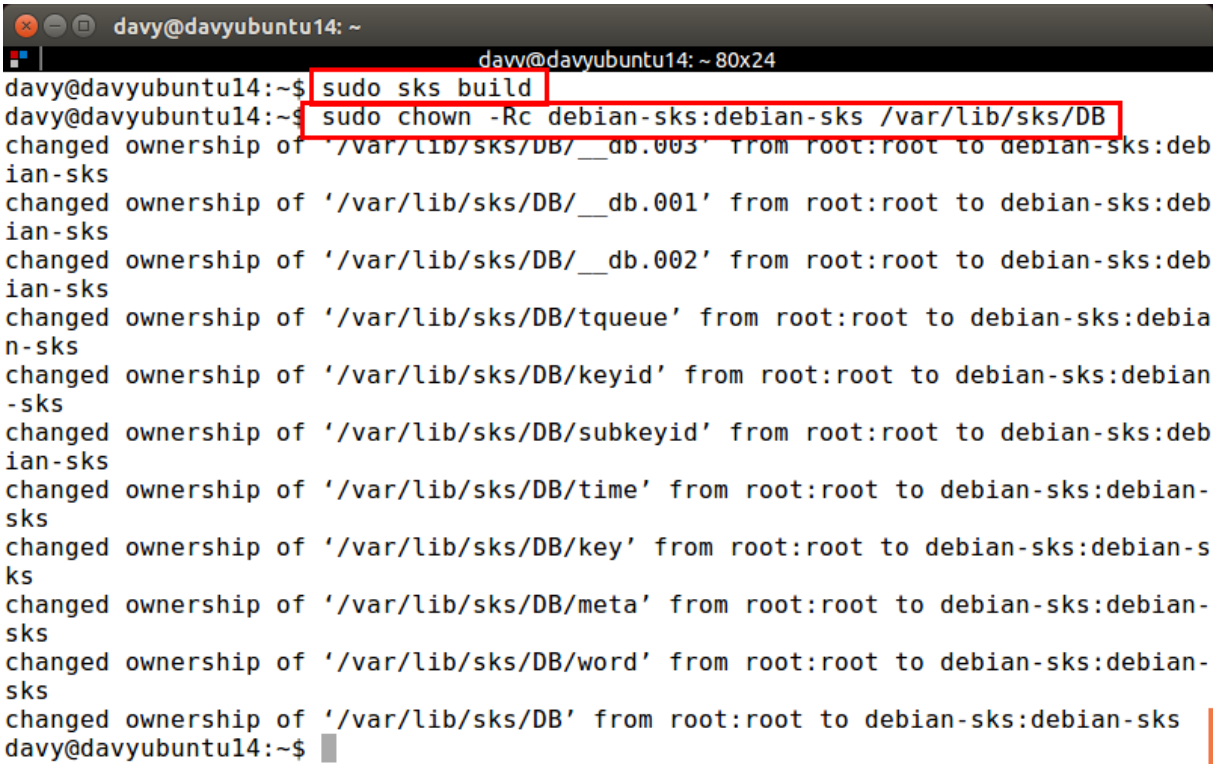
We installeren SKS:

```
davy@davyubuntu14: ~
davy@davyubuntu14: ~ 80x24
davy@davyubuntu14:~$ sudo apt-get install sks
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-3.13.0-32 linux-headers-3.13.0-32-generic
  linux-image-3.13.0-32-generic linux-image-extra-3.13.0-32-generic
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  db-util db5.3-util
Suggested packages:
  procmail
The following NEW packages will be installed:
  db-util db5.3-util sks
0 upgraded, 3 newly installed, 0 to remove and 224 not upgraded.
Need to get 687 kB of archives.
After this operation, 3.059 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

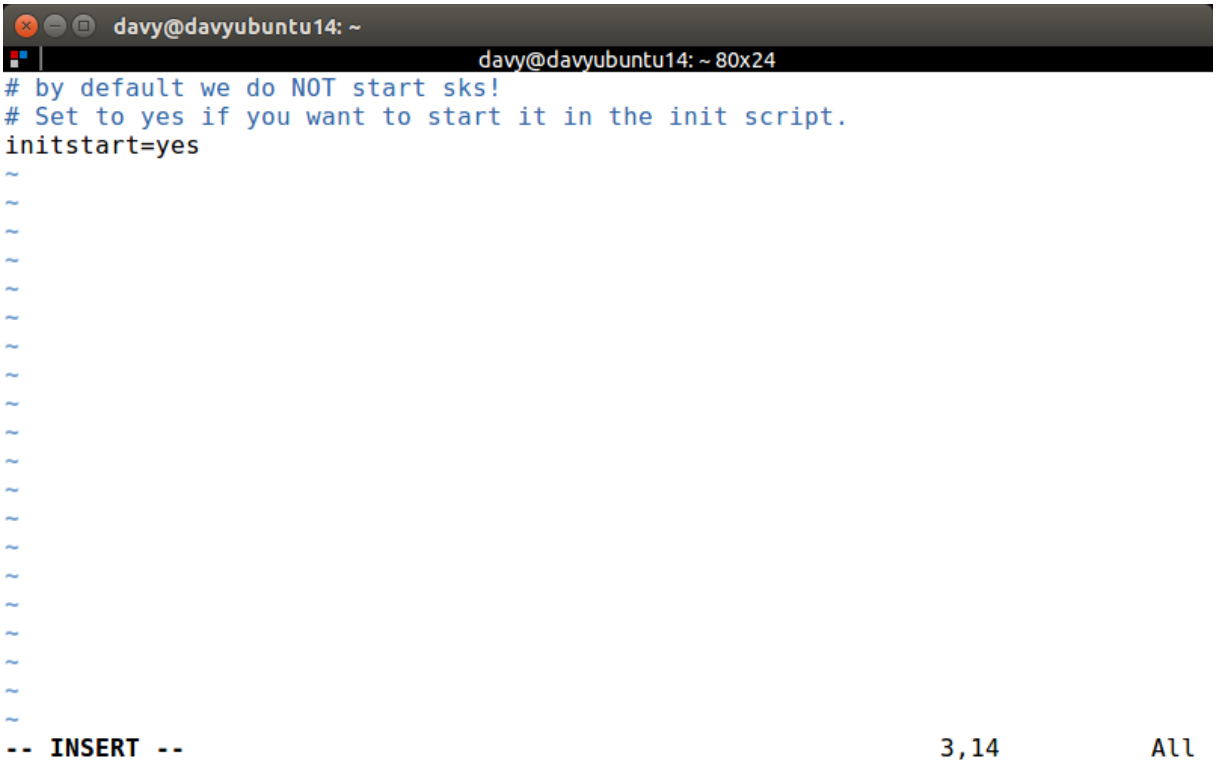
Daarna installeren we Apache:



Nu maken we met het commando “sudo sks build” de database aan die de sleutels zal bevatten. Daarna geven we met het chown-commando de eigendom van de databasefiles aan de gebruiker “debian-sks” uit de groep “debian-sks”. Deze zijn aangemaakt bij de installatie van sks.



Om sks automatisch te doen starten, zetten we in het bestand /etc/default/sks de optie initstart op “yes”.



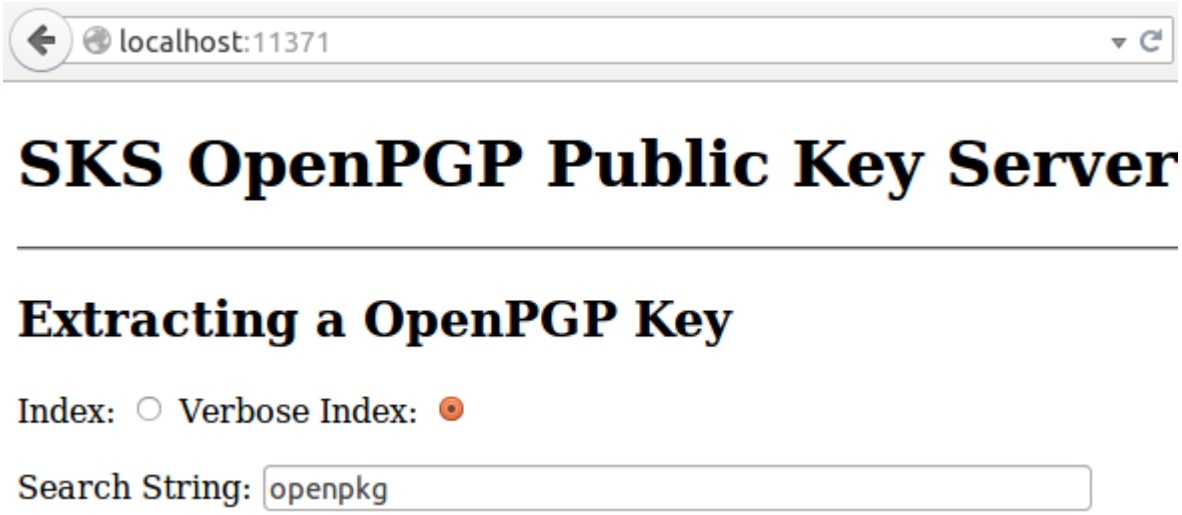
Daarna herstarten we sks.

```
davy@davyubuntu14:~$ sudo /etc/init.d/sks restart
Stopping sks daemons: sksrecon.. sksdb.. done.
Starting sks daemons: sksdb.. sksrecon.. done.
davy@davyubuntu14:~$
```

Vorig jaar moesten we nog de web interface van sks downloaden, en handmatig installeren. Bij deze vernieuwde versie van sks zit er al een web interface bij.

```
davy@davyubuntu14:~$ ls /var/lib/sks/www
ls: cannot access /var/lib/sks/www: Permission denied
davy@davyubuntu14:~$ sudo !!
sudo ls /var/lib/sks/www
index.html  README  robots.txt
davy@davyubuntu14:~$
```

Zoals je ziet, als ik in mijn browser naar localhost poort 11371 ga, kan ik de web interface zien:

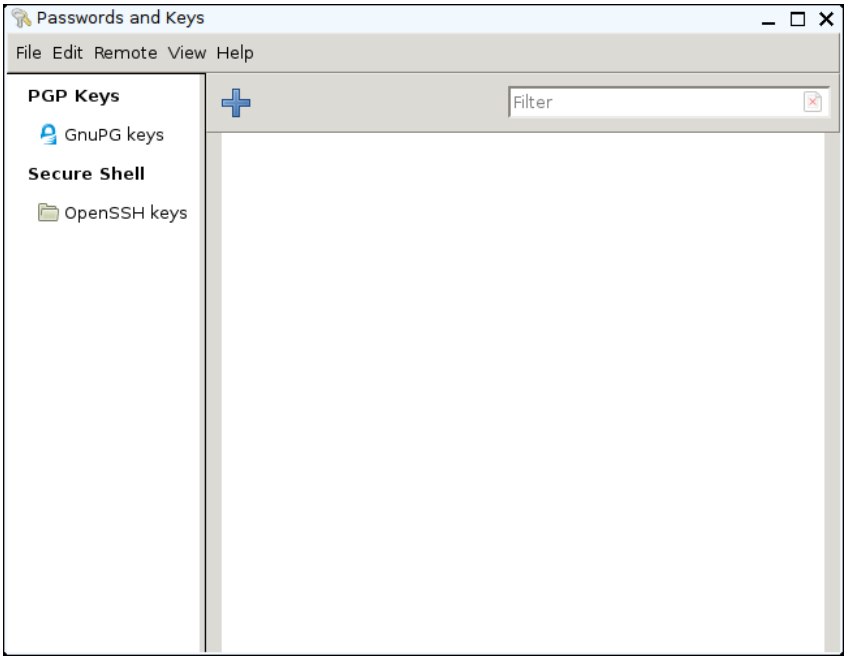


Via de commandline kunnen we ook zien of sks aan het draaien is. Dit doen we via het netstat-commando, waarna we filteren op poort 11371.

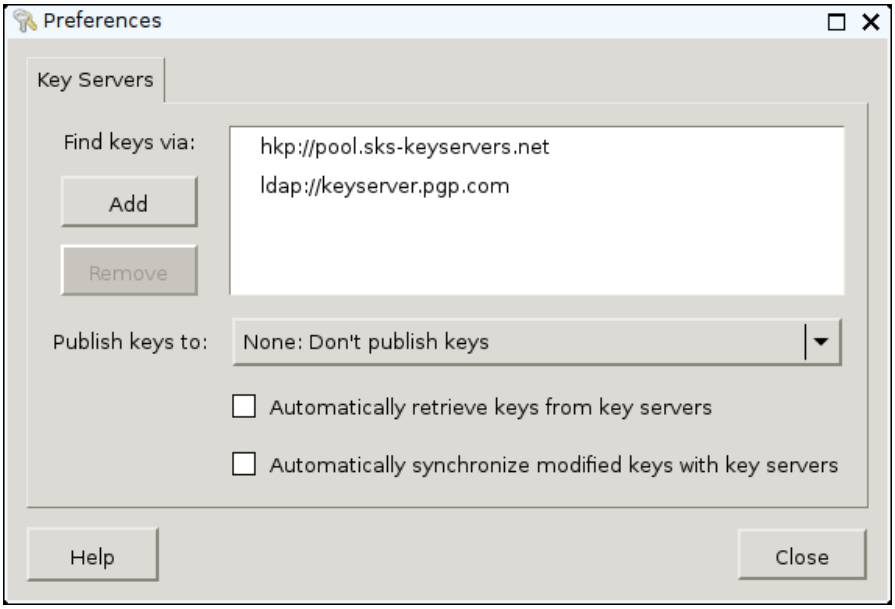
```
davy@davyubuntu14:~$ sudo netstat -anp | grep 11371
tcp        0      0 0.0.0.0:11371           0.0.0.0:*               LISTEN
5764/sks
davy@davyubuntu14:~$
```

Cliënt

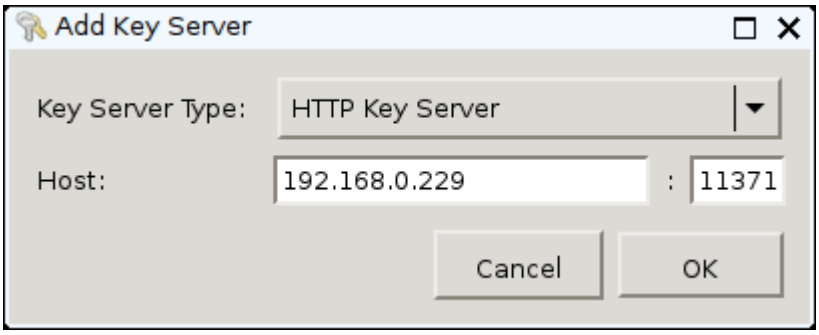
Op de cliënt, hier Puppy Linux starten we Seahorse, of een soortgelijk programma op:



Daarna halen we eerst bij de instellingen (Edit > Settings) de andere keyservers weg zodat we onze testgegevens lokaal houden.



Hierna voegen we onze keyserver toe.



Als we dat hebben gedaan, voegen we een sleutel toe aan onze sleutelring. Daarna gaan we synchroniseren met de keyserver.

Analyse van het netwerkverkeer

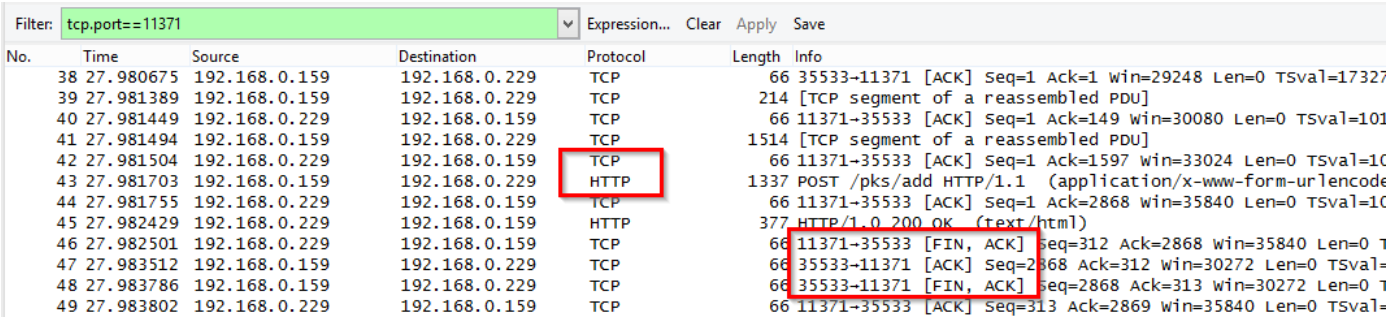
Tijdens het op de cliënt synchroniseren van de sleutelring met de keyserver had ik op de keyserver het tcpdump commando draaien, zodat ik het netwerkverkeer dat op de server binnenkwam of vertrok kon bekijken.

Dit was het commando:

```
davy@davyubuntu14:~$ tcpdump -vvv -n port 11371 -w capturing.cap -i eth0
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
davy@davyubuntu14:~$ sudo !!
sudo tcpdump -vvv -n port 11371 -w capturing.cap -i eth0
[sudo] password for davy:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
^C49 packets captured
49 packets received by filter
0 packets dropped by kernel
```

Het bestand “capturing.cap” exporteerde ik daarna naar mijn Windows-machine, zodat ik het met Wireshark kon analyseren.

Wat mij opviel is dat het synchroniseren gebeurde via TCP en HTTP.

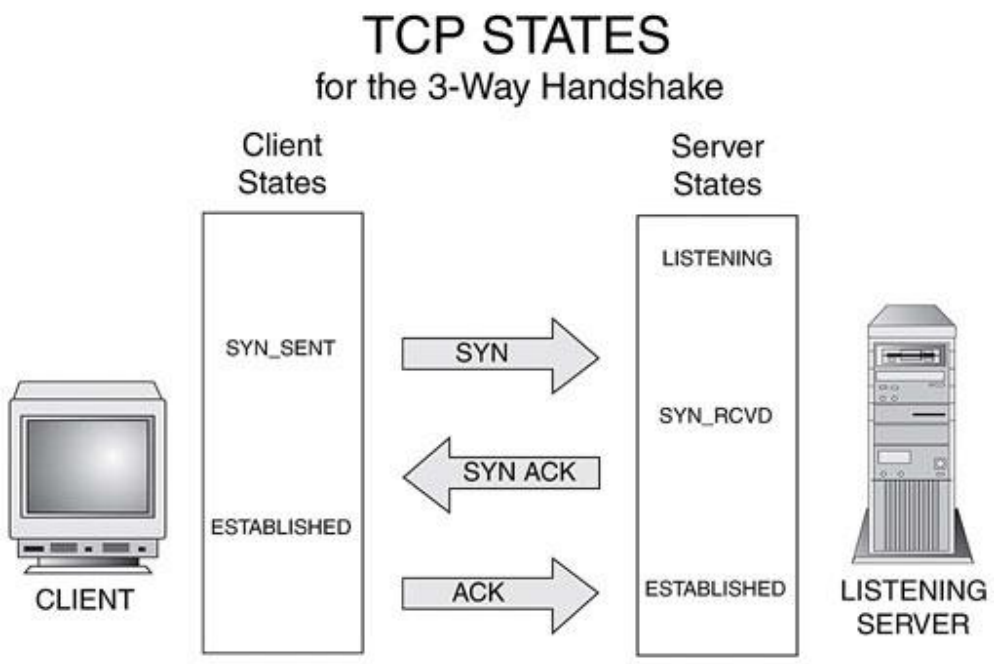


Op bovenstaande screenshot zie je ook dat niet alleen poort 11371, maar ook poort 35533 gebruikt wordt. Om volledig te zijn, eerder in de pakket-analyse zag ik dat er nog een derde poort, namelijk 35532 werd gebruikt.

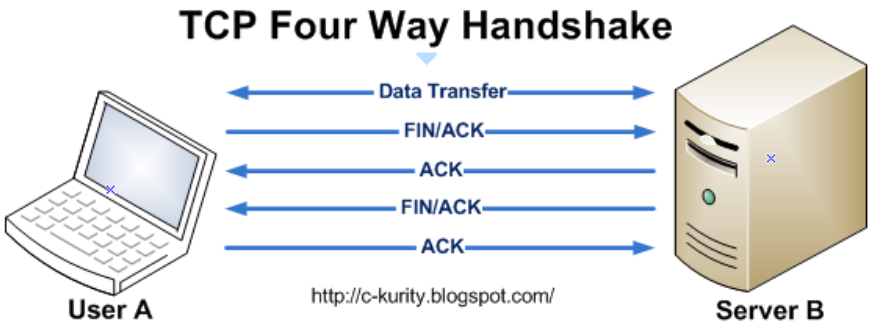
Ook zie je mooi de het einde van de TCP-connectie op de screenshot.

TCP is een communicatie-protocol op de 4de laag van het OSI-model, en is connectie-georiënteerd. Dit wil zeggen dat er foutcontrole gebeurt, en eventuele her verzenden van pakketten. Als data correct moet aankomen, zal men TCP gebruiken, als data snel moet zijn en her verzenden geen zit heeft, zal men vlugger UDP gebruiken. Dit laatste bvb. bij voice-over-IP.

Een TCP-connectie begint met een “handshake”, een “three-way handshake”.



Als de data is verstuurd zal er ook een “handshake” gebeuren om de connectie af te sluiten:



Als we daarna van zo’n pakket de TCP-stream gaan volgen, zien we dat de publieke sleutel leesbaar is doorgestuurd. Men kan zelfs de HTML-code zien die gebruikt is op de server.

Apache webserver

Een base64 encoder met behulp van bash en CGI

Eerst maak ik een cgi-script aan dat we in onze browser kunnen oproepen door de URL “localhost/cgi-bin/base64.cgi?stringie=test” in te typen.
Dit script staat in de directory /usr/lib/cgi-bin.

```
#!/bin/sh

echo Content-type:text/plain
echo
omvorm=$(echo $QUERY_STRING | sed s/stringie=// | openssl enc -base64)
echo $omvorm
~
```

Daarna ga ik proberen om dezelfde functionaliteit te verkrijgen via een formulier, zodat ons script iets gebruiksvriendelijker is. Eerst plaats ik in /var/www/html het volgende html bestand:

```
<!doctype html>
<html>
<head>
        <meta charset="utf-8">
        <link href="table.css" rel="stylesheet">
        <title>Base 64 Encoding</title>
</head>
<body>
    <form action="/cgi-bin/base64e.cgi" method="get">
          <label for="stringie">Te encoderen string:</label>
          <input type="text" name="stringie" id="stringie"/>
          <input type="submit" value="Verzenden"/>
        </form>
        <br>
        <br>
        <table id="resultaat">
          <tr>
                <th>Om te vormen string</th>
                <th>Omgevormde string</th>
          </tr>
          <tr>
                <td></td>
                <td></td>
          </tr>
        </table>
</body>
</html>
```

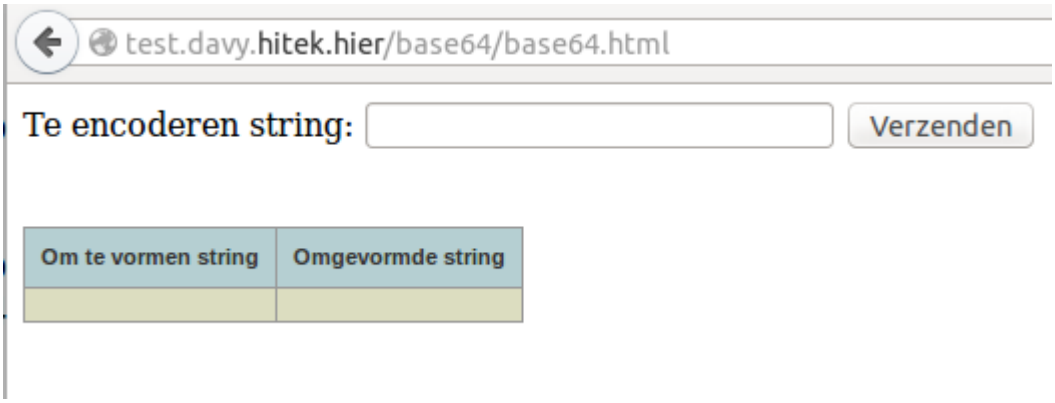
Het base64e.cgi script staat weer in de cgi-bin directory, en ziet er zo uit:

```
#!/bin/bash
echo "Content-type:text/html"
echo ""

omtevorm=$(echo $QUERY_STRING | sed s/stringie=//)
omvorm=$(echo $QUERY_STRING | sed s/stringie=// | openssl enc -base64)

echo "<!doctype html>"
echo "<html><head><meta charset="utf-8"><link href="/table.css" rel="stylesheet"><title>Base 64
Encoding</title></head>"
echo "<body>"
echo "<form action="/cgi-bin/base64e.cgi" method="get">"
echo "<label for="stringie">Te encoderen string:</label>"
echo "<input type="text" name="stringie" id="stringie">"
echo "<input type="submit" value="Verzenden">"
echo "</form>"
echo "<br><br>"
echo "<table id="resultaat">"
echo "<tr>"
echo "<th>Om te vormen string</th>"
echo "<th>Omgevormde string</th>"
echo "</tr>"
echo "<tr>"
echo "<td>$omtevorm</td>"
echo "<td>$omvorm</td>"
echo "</tr></table></body></html>"
```

Hier zie je de locatie van de bestanden:

```
davy@davyubuntu14:~$ ls -l /usr/lib/cgi-bin/
total 8
-rwxr-xr-x 1 davy davy 129 Nov 22 16:23 base64.cgi
-rwxr-xr-x 1 davy davy 805 Nov 22 16:04 base64e.cgi
davy@davyubuntu14:~$ ls -l /var/www/html/
total 24
-rwxr-xr-x 1 davy davy   573 Nov 24 18:06 base64.html
-rw-r--r-- 1 root root 11510 Nov 21 17:51 index.html
-rwxr-xr-x 1 davy davy   394 Dez  1  2013 table.css
-rwxrw-rw- 1 davy davy    24 Nov 23 12:59 test.php
davy@davyubuntu14:~$
```

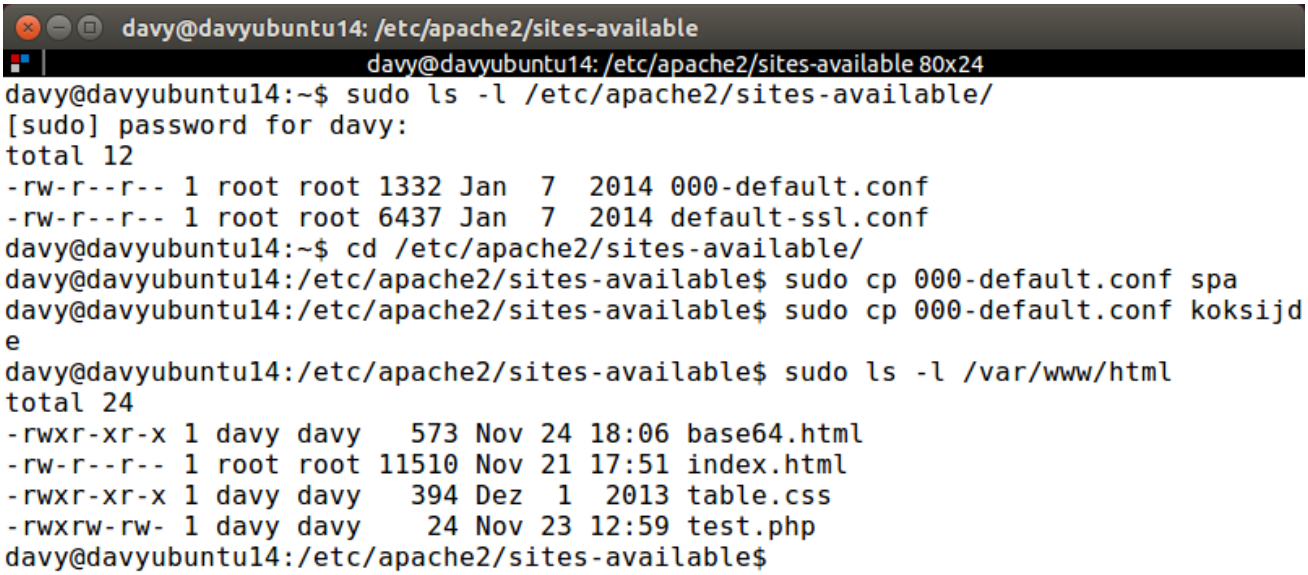
Als we de test doen:



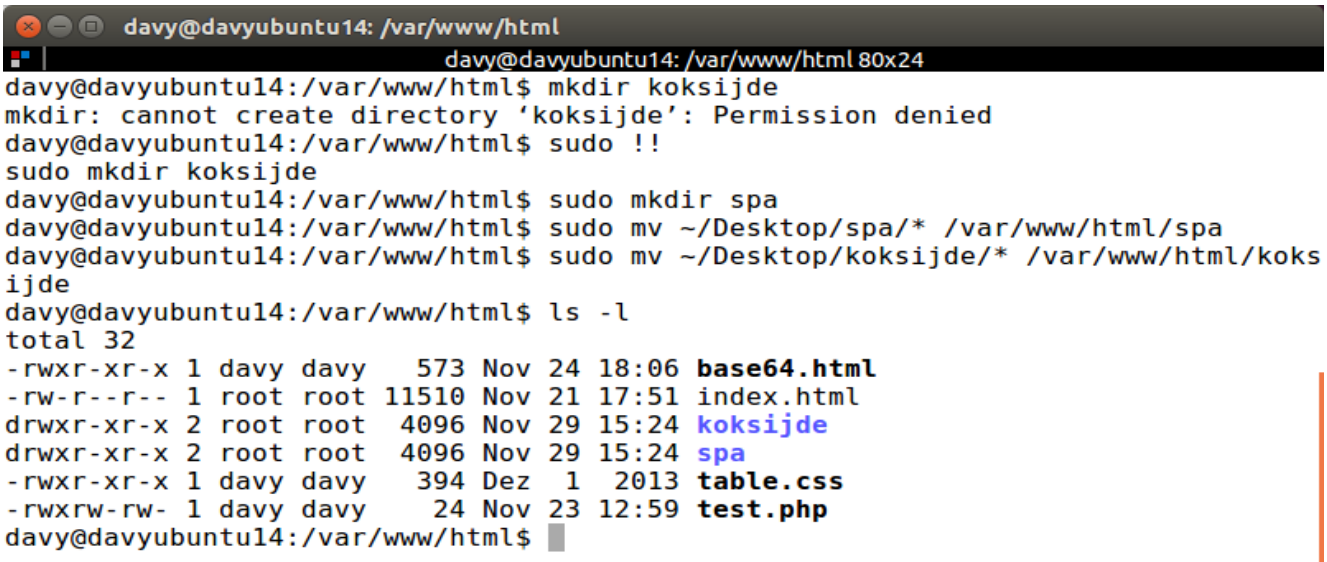
Zoals je ziet, is het CSS-bestand niet gebruikt bij het resultaat. Er is dus een fout in de link naar de CSS in mijn CGI-script. Eerst dacht ik, net zoals bij index.html, de css-file in de cgi-bin map te plaatsen, maar dit werkte niet.

Het opzetten van virtuele hosts

Ik begon eerst met het opzetten van twee virtual hosts, zonder extra configuratie zoals authenticatie. Om dit te doen, kopieerde ik het bestand 000-default.conf naar respectievelijk spa.conf en koksijde.conf. Vanaf Apache versie 2.4 moet men de extensie “conf” gebruiken.



Daarna maakte ik in /var/www/html twee directories aan, één voor iedere virtual host. Later, tijdens het troubleshooten van een probleem zou ik deze verplaatsen naar /var/www/



Daarna maakte ik de directories voor de custom log-bestanden aan.

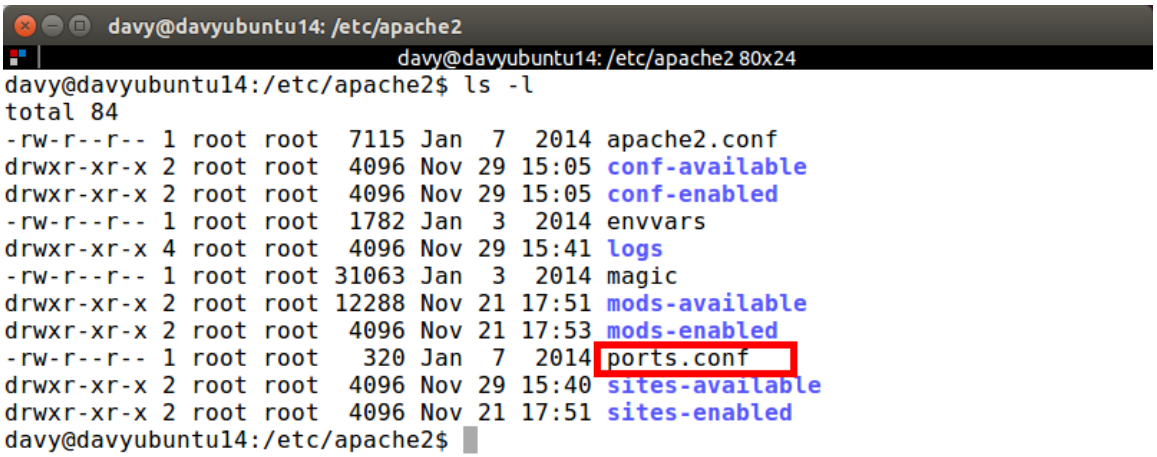
```
davy@davyubuntu14:/etc/apache2$ mkdir logs
mkdir: cannot create directory ‘logs’: Permission denied
davy@davyubuntu14:/etc/apache2$ sudo !!
sudo mkdir logs
davy@davyubuntu14:/etc/apache2$ cd logs
davy@davyubuntu14:/etc/apache2/logs$ sudo mkdir spa koksijde
davy@davyubuntu14:/etc/apache2/logs$ ls
koksijde  spa
davy@davyubuntu14:/etc/apache2/logs$ cd koksijde
davy@davyubuntu14:/etc/apache2/logs/koksijde$
```

Nu ging ik de configuratiebestanden van iedere virtual host aanpassen.

```
<VirtualHost *:8080>
    ServerName koksijde.davy.hitek.hier
    DocumentRoot /var/www/html/koksijde
    ErrorDocument 404 /var/www/html/koksijde/404.html
    ErrorLog /logs/koksijde/error.log
    CustomLog /logs/koksijde/access.log combined
</VirtualHost>
```

```
<VirtualHost *:80>
        ServerName spa.davy.hitek.hier
        DocumentRoot /var/www/html/spa
        ErrorDocument 404 /var/www/html/spa/404.html
        ErrorLog /logs/spa/error.log
        CustomLog /logs/spa/access.log combined
</VirtualHost>
```

Aangezien de virtual host “koksijde” op poort 8080 draait, moest ik ook het bestand ports.conf in /etc/apache2 aanpassen.

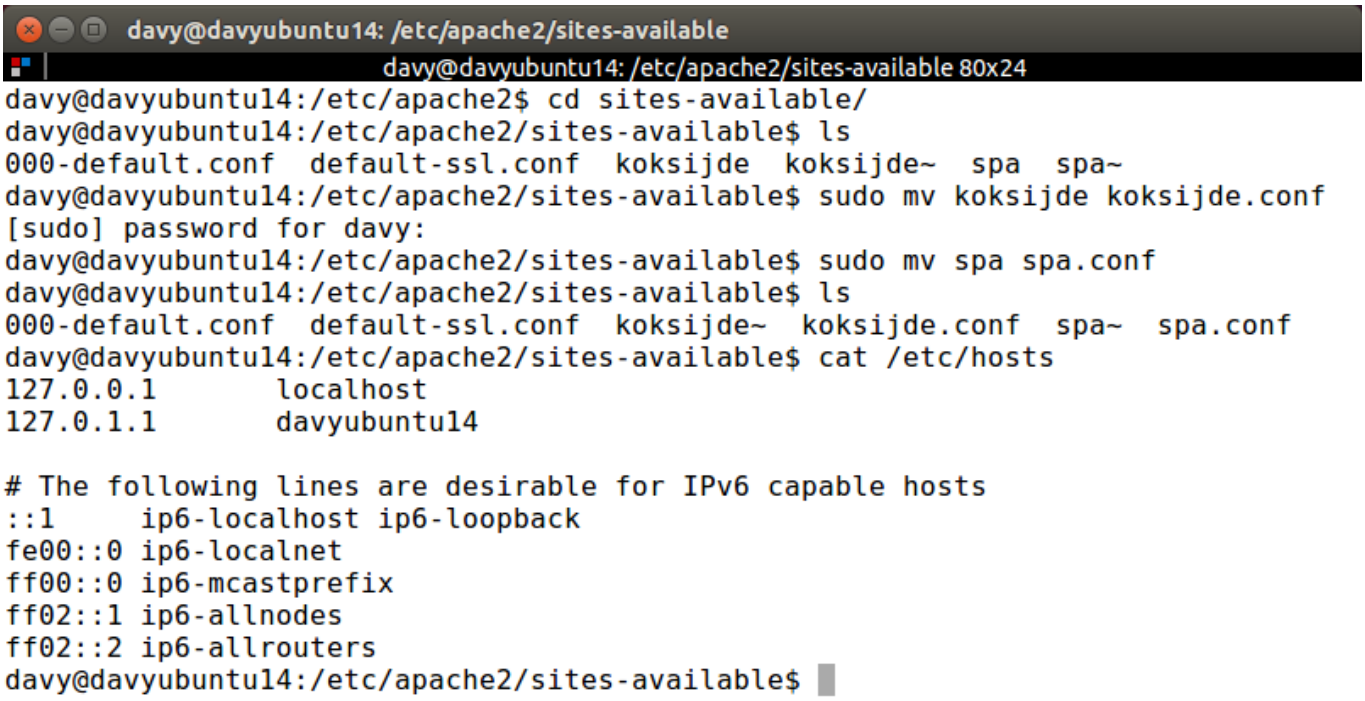



```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 8080

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

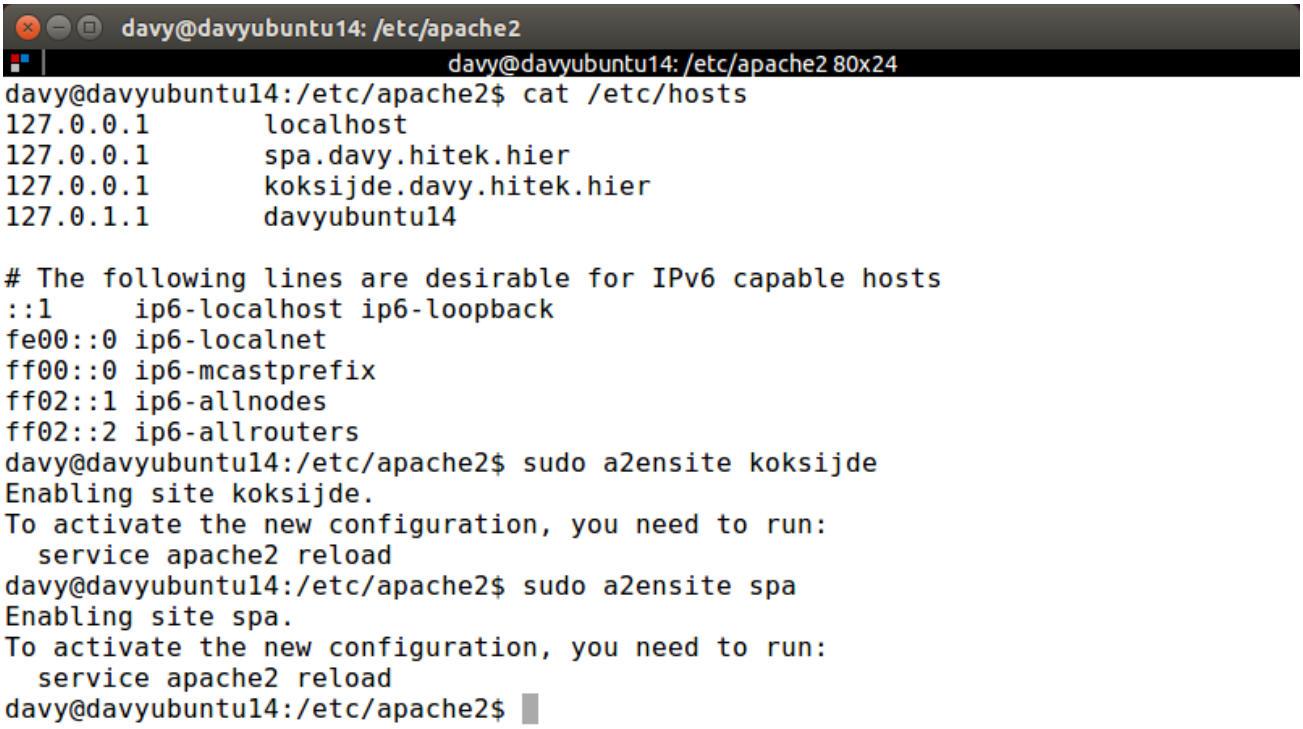
Nu plaats ik de eigen 404 foutpagina in de directories:

```
davy@davyubuntu14:/etc/apache2$ cd ~Desktop
bash: cd: ~Desktop: No such file or directory
davy@davyubuntu14:/etc/apache2$ sudo mv ~/Desktop/404.html /var/www/html/koksijd
e
davy@davyubuntu14:/etc/apache2$ sudo mv ~/Desktop/404.html /var/www/html/spa
mv: cannot stat ‘/home/davy/Desktop/404.html’: No such file or directory
davy@davyubuntu14:/etc/apache2$ sudo cp /var/www/html/koksijde/404.html /var/www
/html/spa
davy@davyubuntu14:/etc/apache2$
```

Als je de extensie “conf” vergeten bent, kan je dat verbeteren. Een mogelijkheid is het gebruik van het commando “mv”:



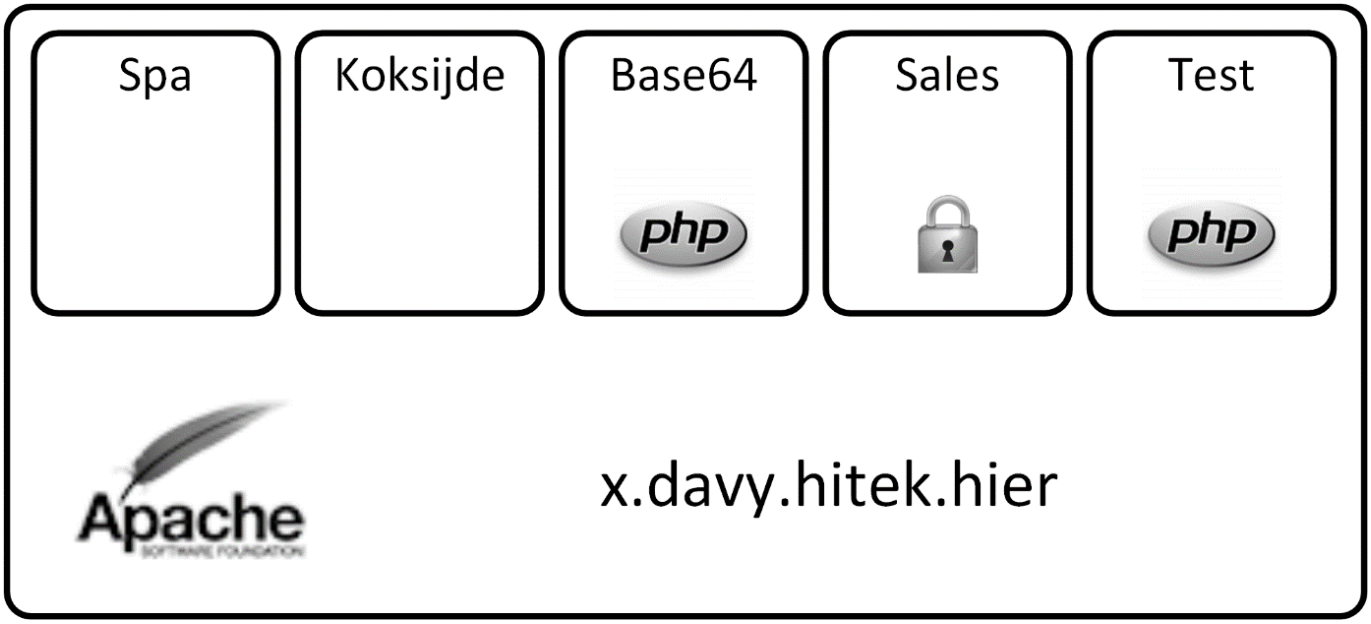
Zoals je hierboven ziet, vraag ik het bestand /etc/hosts/ op. Dit ga ik aanpassen zodat ik zonder DNS-server naar bvb. “spa.davy.hitek.hier” kan surfen.



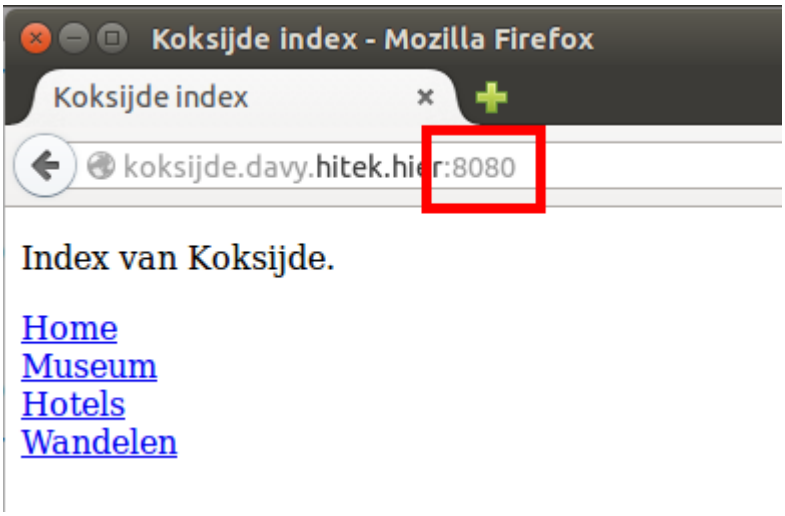
Hierna merkte ik dat ik alleen maar de standaard index-pagina van Apache te zien kreeg, ook al bezocht ik de virtual hosts. Daarom ben ik beginnen te zoeken, heb ik tevergeefs veranderingen aan configuratie-files, directory structuren, … uitgevoerd.

Uiteindelijk, na het disablen van de default virtual host 000-default.conf lukte het wel. Later in dit document volgen de uiteindelijke configuratiebestanden van de virtual hosts.

Omdat virtual hosts gemakkelijk zijn om een opdeling van mijn webserver te maken heb ik er nog twee bijgemaakt, één voor de base64-encoder en één om de kleine taken van PHP te testen. De webserver is dus als volgt opgebouwd:



Hier surf ik bijvoorbeeld naar koksijde.



Een base64 encoder in PHP

Net zoals we met bash en cgi een base64 encoder gemaakt hebben, kan dit ook met PHP. We beginnen met een index-pagina.

index.html

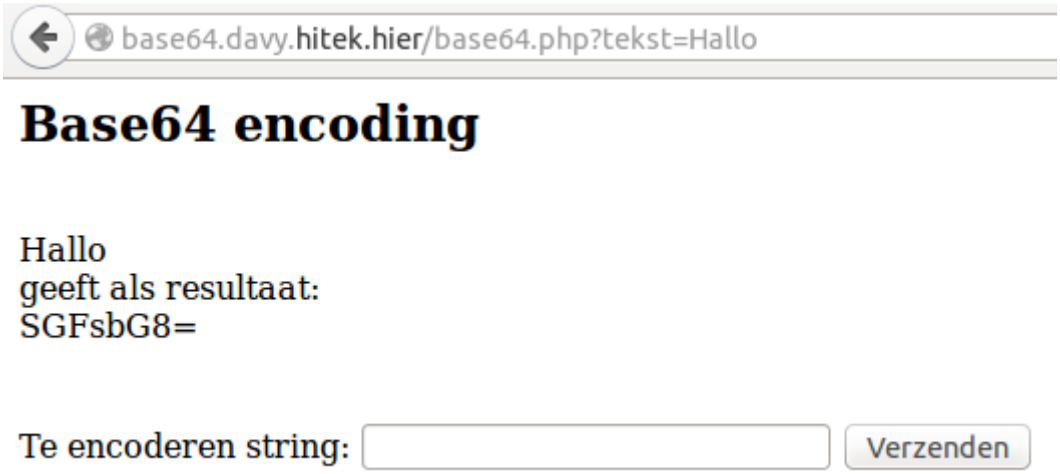
```
<html>
<head>
      <meta charset="utf-8">
      <title>Base 64 Encoding</title>
</head>
<body>
      <form action="base64.php" method="get">
        <label for="tekst">Te encoderen string:</label>
        <input type="text" name="tekst"/>
        <input type="submit" value="Verzenden"/>
      </form>
      <br>
</body>
</html>
```

Deze index-pagina roept volgend PHP-script aan:

base64.php

```
<html>
<head>
      <meta charset="utf-8">
      <title>Base 64 Encoding</title>
</head>
<body>
      <h2> Base64 encoding </h2><br>
      <?php
            echo $_GET["tekst"];
      ?>
      <br>
      geeft als resultaat:
      <br>
      <?php
            echo base64_encode($_GET["tekst"]);
      ?>
      <br>
      <br>
      <br>
      <form action="base64.php" method="get">
        <label for="tekst">Te encoderen string:</label>
        <input type="text" name="tekst"/>
        <input type="submit" value="Verzenden"/>
      </form>
      <br>
</body>
</html>
```


base64.davy.hitek.hier
Te encoderen string:
Verzenden


base64.davy.hitek.hier/base64.php?tekst=Hallo
Base64 encoding
Hallo
geeft als resultaat:
SGFsbG8=
Te encoderen string:
Verzenden

Een https-website opzetten

De virtuele host “sales” moet toegankelijk zijn via https.

De benodigde certificaat- en sleutelbestanden zijn gemaakt via een zelf-opgezette certificate authority (CA). Deze bestanden kopiëren we naar onze webserver, maar we gebruiken wel een directory die NIET in de documentroot ligt. Standaard is dit /etc/ssl/certs/.

Daarna moeten we in het configuratiebestand van de virtuele host, SSL aanzetten en ook verwijzen naar de bestanden die we zojuist gekopieerd hebben. Dit doen we door volgende regels toe te voegen:

```
SSLEngine on
SSLCertificateFile /etc/ssl/certs/admin@davy.hitek.hier-cert.pem
SSLCertificateKeyFile /etc/ssl/certs/admin@davy.hitek.hier-key.pem
```

Let er wel op dat de virtuele host poort 443 gebruikt!

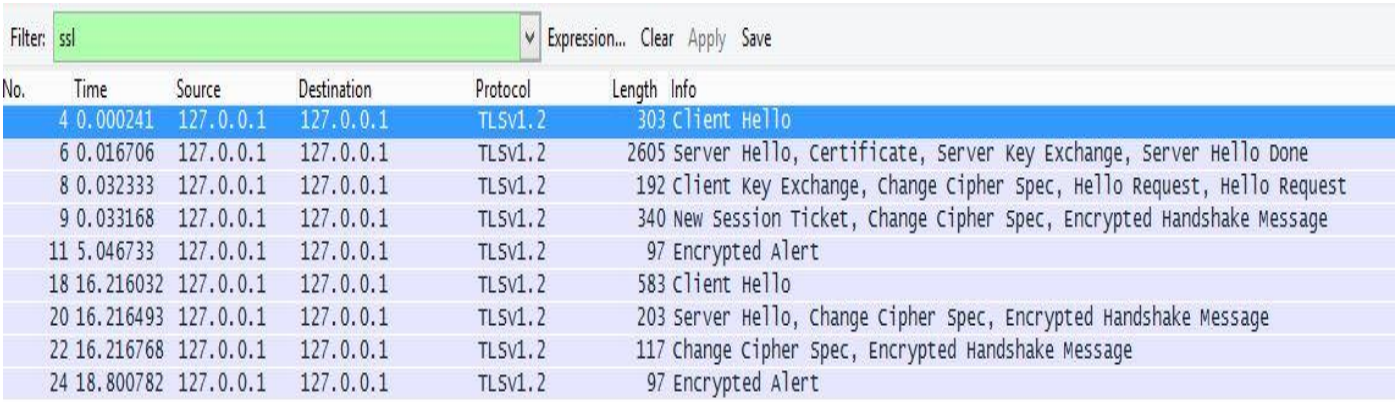
Als we dan surfen naar sales.davy.hitek.hier krijgen we eerst een melding dat het certificaat onbekend is. Aangezien het hier om ons certificaat gaat, kunnen we deze melding negeren.

We kunnen het verkeer op poort 443 bekijken met tcpdump-commando:

```
davy@davyubuntu14:~/Desktop$ sudo tcpdump -vvv -n port 443 -i lo -w capture.cap
```

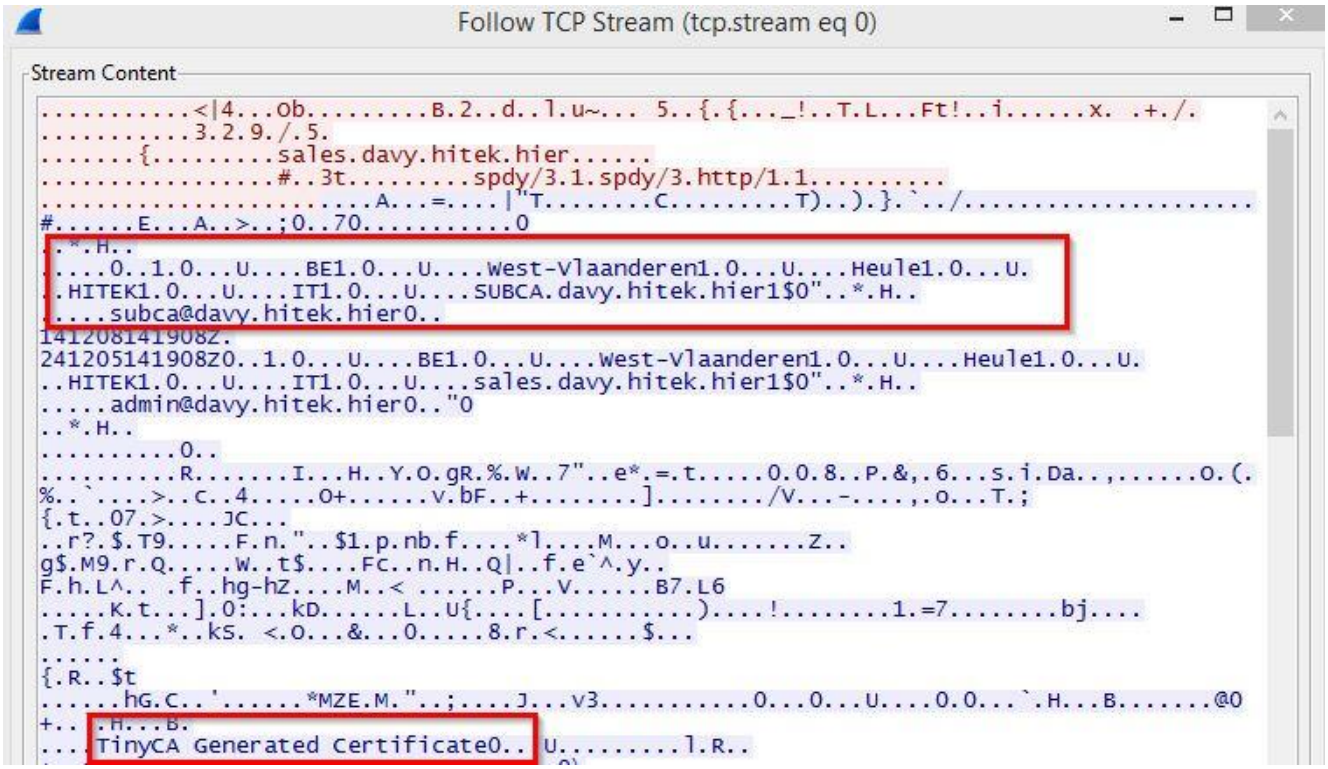
Dit commando luistert op de lokale interface naar verkeer op poort 443. Om dit te bekijken met Wireshark schrijf ik dit weg naar het bestand capture.cap. Aangezien ik het maximumniveau van verbositeit heb gebruikt, hebben we veel info in dit bestand staan.

Ik open Wireshark, en ik laat al het verkeer in verband met SSL zien:



No.	Time	Source	Destination	Protocol	Length	Info
4	0.000241	127.0.0.1	127.0.0.1	TLSv1.2	303	Client Hello
6	0.016706	127.0.0.1	127.0.0.1	TLSv1.2	2605	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8	0.032333	127.0.0.1	127.0.0.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
9	0.033168	127.0.0.1	127.0.0.1	TLSv1.2	340	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	5.046733	127.0.0.1	127.0.0.1	TLSv1.2	97	Encrypted Alert
18	16.216032	127.0.0.1	127.0.0.1	TLSv1.2	583	Client Hello
20	16.216493	127.0.0.1	127.0.0.1	TLSv1.2	203	Server Hello, Change Cipher Spec, Encrypted Handshake Message
22	16.216768	127.0.0.1	127.0.0.1	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
24	18.800782	127.0.0.1	127.0.0.1	TLSv1.2	97	Encrypted Alert

Als we de TCP-stream volgen, zien we dat er info leesbaar is. Het gaat hier over info over de certificate authority.



DBM autorisatie

We beginnen met de directory te maken:

```
davy@davyubuntu14:/var/www$ ls
base64  html  koksijde  spa
davy@davyubuntu14:/var/www$ cd spa
davy@davyubuntu14:/var/www/spa$ ls
404.html  hotels.html  index.html  museum.html  wandelen.html
davy@davyubuntu14:/var/www/spa$ mkdir secret
mkdir: cannot create directory ‘secret’: Permission denied
davy@davyubuntu14:/var/www/spa$ sudo !!
sudo mkdir secret
davy@davyubuntu14:/var/www/spa$ ls
404.html  hotels.html  index.html  museum.html  secret  wandelen.html
davy@davyubuntu14:/var/www/spa$
```

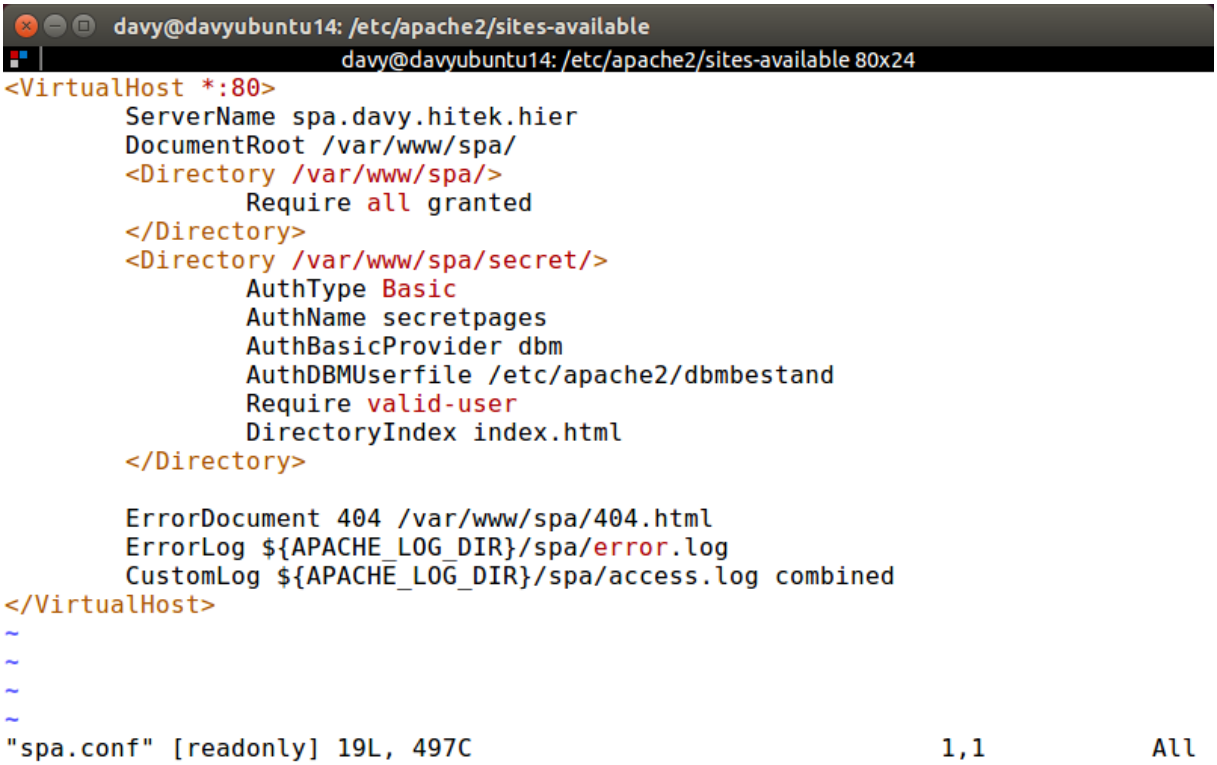
Daarna laadde ik twee modules, authn_dbm en auth_digest. Die laatste was, achteraf gezien, niet nodig.

```
davy@davyubuntu14: /etc/apache2
davy@davyubuntu14: /etc/apache2 80x24
davy@davyubuntu14:/etc/apache2$ ls mods-enabled/
access_compat.load  authz_user.load  env.load          php5.conf
alias.conf          autoindex.conf   filter.load       php5.load
alias.load          autoindex.load   mime.conf         setenvif.conf
auth_basic.load     cgi.load         mime.load         setenvif.load
authn_core.load     deflate.conf     mpm_prefork.conf  status.conf
authn_file.load     deflate.load     mpm_prefork.load  status.load
authz_core.load     dir.conf         negotiation.conf
authz_host.load     dir.load         negotiation.load
davy@davyubuntu14:/etc/apache2$ sudo a2enmod authn_dbm
Enabling module authn_dbm.
To activate the new configuration, you need to run:
  service apache2 restart
davy@davyubuntu14:/etc/apache2$ sudo a2enmod auth_digest
Considering dependency authn_core for auth_digest:
Module authn_core already enabled
Enabling module auth_digest.
To activate the new configuration, you need to run:
  service apache2 restart
davy@davyubuntu14:/etc/apache2$
```

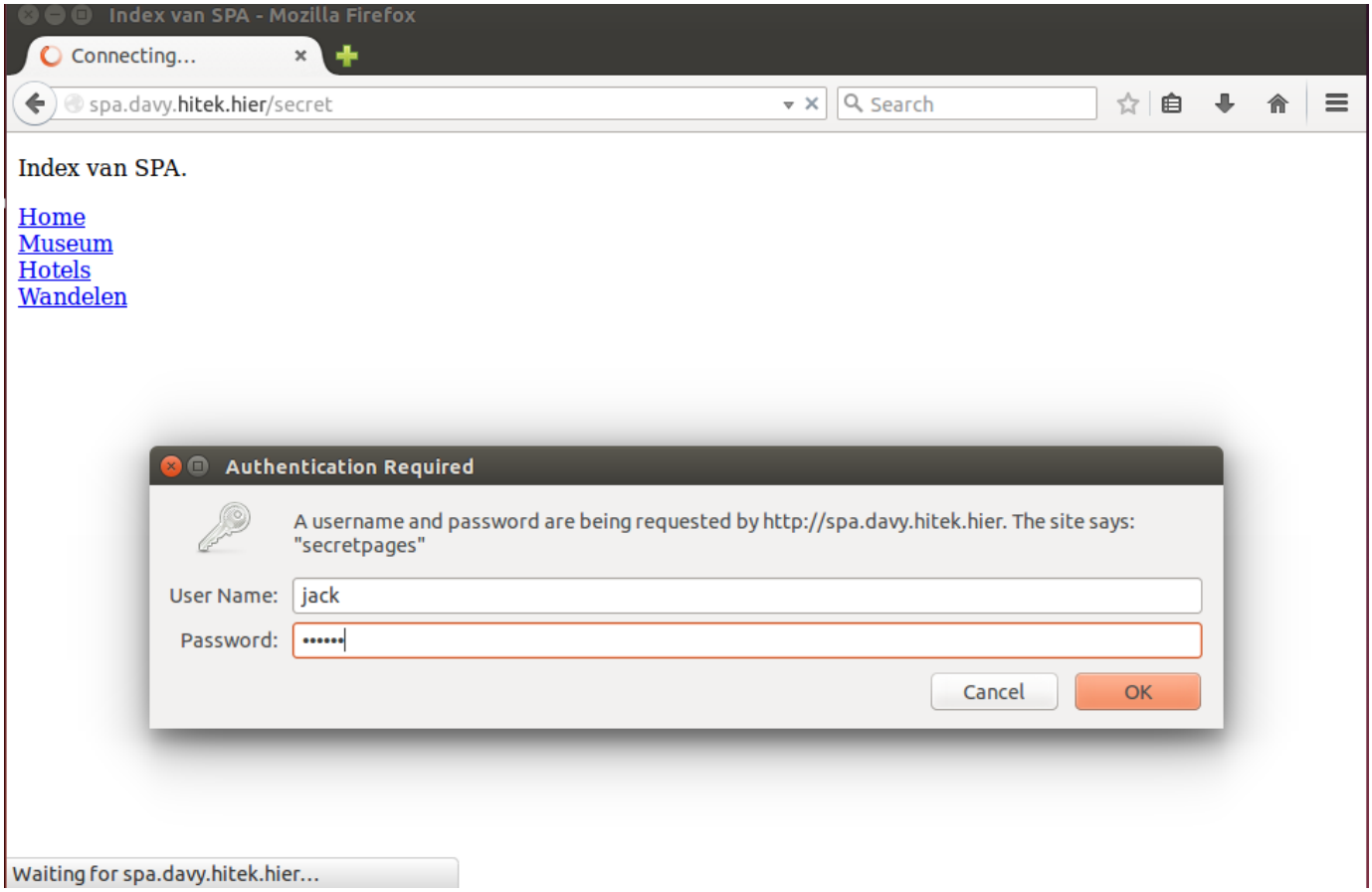
Nadat ik de modules had geladen, maakte ik een user aan, met bijhorend paswoord. Deze info is opgeslagen in een directory die niet publiek toegankelijk is.

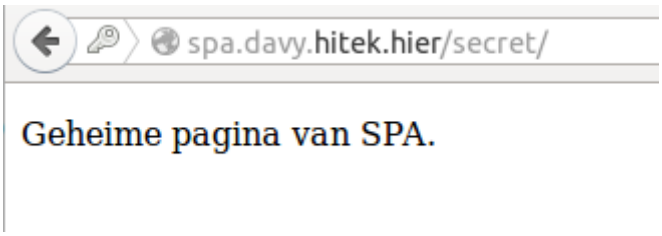
```
davy@davyubuntu14:/etc/apache2$ htdbm -c /etc/apache2/dbmbestand jack
Error opening database /etc/apache2/dbmbestand
APR does not understand this error code
davy@davyubuntu14:/etc/apache2$ sudo !!
sudo htdbm -c /etc/apache2/dbmbestand jack
[sudo] password for davy:
New password:
Re-type new password:
Database /etc/apache2/dbmbestand created.
davy@davyubuntu14:/etc/apache2$
```

Ook het configuratiebestand van de virtuele host in kwestie moet aangepast worden, zodat de autorisatie werkt.



Zoals je hierboven ziet, gebruik ik de autorisatie-methode “basic”. Eerst gebruikte ik de methode “digest”, om dat verschillende tutorials hierover spraken. Hierdoor kreeg ik wel de vraag om een gebruikersnaam en paswoord op te geven, maar, indien deze correct waren, ik kreeg de inhoud van het beveiligde gedeelte niet te zien.


Index van SPA - Mozilla Firefox
Connecting...
spa.davy.hitek.hier/secret
Search
Index van SPA.
Home
Museum
Hotels
Wandelen
Authentication Required
A username and password are being requested by http://spa.davy.hitek.hier. The site says: "secretpages"
User Name:
jack
Password:
Cancel
OK
Waiting for spa.davy.hitek.hier...


spa.davy.hitek.hier/secret/
Geheime pagina van SPA.

Na het uitvoeren van de oefening, bekom ik de volgende configuratiebestanden.

koksijde.conf

```
<VirtualHost *:8080>
      ServerName koksijde.davy.hitek.hier
      DocumentRoot /var/www/koksijde/
      <Directory /var/www/koksijde/>
            Require all granted
      </Directory>
      ErrorDocument 404 /var/www/koksijde/404.html
      ErrorLog ${APACHE_LOG_DIR}/koksijde/error.log
      CustomLog ${APACHE_LOG_DIR}/koksijde/access.log combined
</VirtualHost>
```

spa.conf

```
<VirtualHost *:80>
      ServerName spa.davy.hitek.hier
      DocumentRoot /var/www/spa/
      <Directory /var/www/spa/>
            <RequireAll>
                  Require all granted
                  Require not ip 192.168.9.55
            </RequireAll>
      </Directory>
      <Directory /var/www/spa/secret/>
            AuthType Basic
            AuthName secretpages
            AuthBasicProvider dbm
            AuthDBMUserfile /etc/apache2/dbmbestand
            Require valid-user
            DirectoryIndex index.html
      </Directory>

      ErrorDocument 404 /var/www/spa/404.html
      ErrorLog ${APACHE_LOG_DIR}/spa/error.log
      CustomLog ${APACHE_LOG_DIR}/spa/access.log combined
</VirtualHost>
```

sales.conf

```
<VirtualHost *:443>
            ServerName sales.davy.hitek.hier
            DocumentRoot /var/www/sales
            SSLEngine on
            SSLCertificateFile     /etc/ssl/certs/admin@davy.hitek.hier-
cert.pem
            SSLCertificateKeyFile /etc/ssl/certs/admin@davy.hitek.hier-
key.pem
</VirtualHost>
```

base64.conf

```
<VirtualHost *:80>
      ServerName base64.davy.hitek.hier
      DocumentRoot /var/www/base64/
      <Directory /var/www/base64/>
            Require all granted
      </Directory>
      ErrorLog ${APACHE_LOG_DIR}/base64/error.log
      CustomLog ${APACHE_LOG_DIR}/base64/access.log combined
</VirtualHost>
```

test.conf

```
<VirtualHost *:80>
      ServerName test.davy.hitek.hier
      ServerAdmin webmaster@localhost
      DocumentRoot /var/www/html
      ErrorLog ${APACHE_LOG_DIR}/test/error.log
      CustomLog ${APACHE_LOG_DIR}/test/access.log combined
</VirtualHost>
```

ports.conf

```
Listen 80
Listen 8080

<IfModule ssl_module>
      Listen 443
</IfModule>

<IfModule mod_gnutls.c>
      Listen 443
</IfModule>
```

/etc/hosts

```
127.0.0.1   localhost
127.0.0.1   spa.davy.hitek.hier
127.0.0.1   koksijde.davy.hitek.hier
127.0.0.1   base64.davy.hitek.hier
127.0.0.1   test.davy.hitek.hier
127.0.0.1   sales.davy.hitek.hier
127.0.1.1   davyubuntu14

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Directory-structuur

Met behulp van het commando “ls –R [directory] > [filename]” kan ik de directorystructuur laten zien.

Alle data (html, PHP, …) staan in de /var/www directory. Dit is een momentopname, als ik nieuwe scripts of websites maak, komen die hier ook terecht.

/var/www

```
/var/www/:
base64
html
koksijde
sales
spa

/var/www/base64:
base64.php
base64.php~
index.html
index.html~

/var/www/html:
base64
database
indax.html
post
sessioncounter
sessionvegetable
testphp

/var/www/html/base64:
base64.html
table.css

/var/www/html/database:
showdatabase.php
showdatabase.php~
showtable.php
showtable.php~

/var/www/html/post:
code_test_post.php
code_test_post.php~

/var/www/html/sessioncounter:
session.php
session.php~

/var/www/html/sessionvegetable:
change.php
change.php~
destroy.php
destroy.php~
show.php
show.php~
```

```
start.php
start.php~

/var/www/html/testphp:
test.php

/var/www/koksijde:
404.html
hotels.html
index.html
museum.html
wandelen.html

/var/www/sales:
index.html

/var/www/spa:
404.html
hotels.html
index.html
museum.html
secret
wandelen.html

/var/www/spa/secret:
index.html
```

In de map /var/log/apache2/ komen de log-files terecht, eventueel per virtuele host.

/var/log/apache2

```
/var/log/apache2/:
access.log
access.log.1
base64
error.log
error.log.1
error.log.2.gz
koksijde
other_vhosts_access.log
spa
test

/var/log/apache2/base64:
access.log
error.log

/var/log/apache2/koksijde:
access.log
error.log

/var/log/apache2/spa:
access.log
error.log

/var/log/apache2/test:
access.log
error.log
```

Als we de map /etc/apache2/sites-enabled bekijken, zien we welke virtual hosts er op dat moment actief waren.

/etc/apache2/sites-enabled
/etc/apache2/sites-enabled/: base64.conf koksijde.conf sales.conf spa.conf test.conf

En de geactiveerde modules zien we in volgende map:

/etc/apache2/mods-enabled
/etc/apache2/mods-enabled/: access_compat.load alias.conf alias.load auth_basic.load authn_core.load authn_dbm.load authn_file.load authz_core.load authz_host.load authz_user.load autoindex.conf autoindex.load cgi.load deflate.conf deflate.load dir.conf dir.load env.load filter.load mime.conf mime.load mpm_prefork.conf mpm_prefork.load negotiation.conf negotiation.load php5.conf php5.load setenvif.conf setenvif.load socache_shmcb.load ssl.conf ssl.load status.conf status.load

Observaties

Tijdens het opstellen van het logboek (januari 2015), heb ik voor mezelf al enkele conclusies gemaakt over het hele proces.

1. Een bepaalde kennis van de theorie is onmisbaar. Iedereen kan een commando overtypen, of ergens klikken, maar als het dan misgaat, is het zonder theoretische kennis moeilijker om een oorzaak te vinden. Dit zag ik toen ik bij de OSPF-opdracht de area's naar een stub-area moest omvormen.
2. Eenmaal men de juiste commando's kent, gaat het vlugger werken via de commandline interface als met een GUI.
3. Het is zeer belangrijk om alles op voorhand uit te werken op een manier die voor jou persoonlijk het overzichtelijkst is. Tabellen en schema's werden door mij dagelijks geraadpleegd.
4. Tijdens het raadplegen van handleidingen en fora moet men op de software-versie letten. Zo vond ik in verband met virtual hosts veel info in verband op fora die met Apache 2.2 werkten terwijl ik met Apache 2.4 werkte. Tussen deze twee versies zaten op het eerste zicht kleine verschillen, maar deze waren wel primair voor de goede werking.
5. Voordat men fora gaat raadplegen is het handig om de originele manuals te raadplegen.

In dit hoofdstuk beschrijf ik enkele zaken die ik opmerkte tijdens het maken van de oefeningen. Het gaat hier over mijn persoonlijke visie.

Ten eerste loont het de moeite om te letten op changelogs en versies. Tijdens de oefening over MikroTik-firewalls stootte ik op een probleem dat opgelost is door een functie te gebruiken in een nieuwere versie van de software.

Wel moet men nagaan, of de nieuwe versie alle nodige functionaliteit ondersteunt. Het zou jammer zijn om door een upgrade één probleem op te lossen, maar ook tien bijkomende problemen te veroorzaken.

Ik merkte over dit punt wel op dat een officiële verzameling van changelogs moeilijk of niet te vinden is (zie bronnen, punt 49).

Daarnaast, als tweede punt, is het belangrijk om eerst klein te beginnen. Als je dan een positief resultaat behaalt kan men daarop verder bouwen. Wanneer je bijvoorbeeld een simpele DNS-opstelling met 1 zone niet draaiend krijgt, heeft het geen nut om over verschillende zones, masters, slaves, … te beginnen.

Ook heb ik, als laatste weer de kracht van ***regelmatige back-ups en snapshots*** ontdekt. Indien je een project tot een bepaald punt werkend hebt, neem je best een back-up of een snapshot. Bij incidenten bij verdere stappen kan je dan sneller en gemakkelijker zaken ongedaan maken.

Kleine opdrachten

Linux one-liners

Oneliners

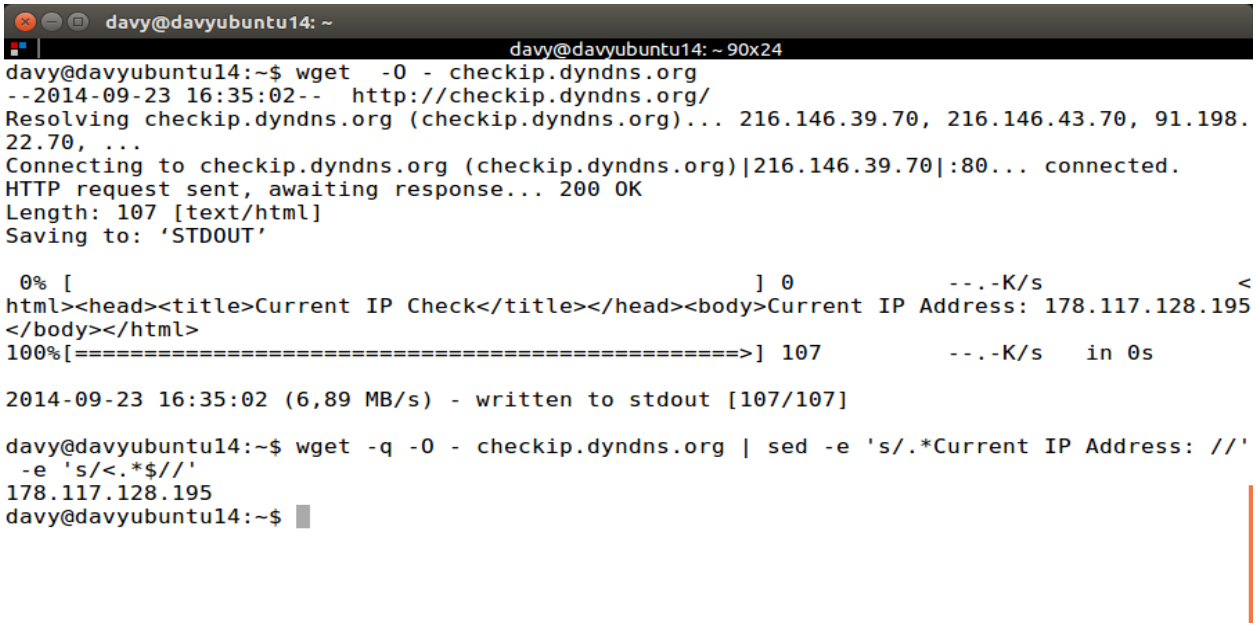
A. Controleer waar “blah” staat geïnstalleerd, en welke versie. Indien er foutmeldingen zijn, herinstalleer “blah”.
B. Creëer een file “random_file” van een megabyte groot, gevuld met random data. Door het getal bij optie “bs” te vermenigvuldigen met het getal achter “count” krijgt men de totale grootte van het bestand.
C. Maak 8 willekeurige bytes, en stuur eventuele fouten naar /dev/null. Encodeer deze bytes met base64, en verwijder daarna alle gelijkheidstekens op het einde van de regel.

```
davy@davyubuntu14:~$ dd if=/dev/random bs=8 count=1 2>/dev/null | base64
AmPwPo6BrS0=
davy@davyubuntu14:~$ dd if=/dev/random bs=8 count=1 2>/dev/null | base64 | sed -e 's/=*$//
'
s5oJlTVEMhI
```

D. Download het bestand winbox.exe, met als outputfile /dev/null. Door deze oneliner uit te voeren, gaat men de gewenste data wel downloaden, maar niet meer terugvinden. Indien men dit bestand wil gebruiken, moet een andere outputfile gekozen worden.

```
davy@davyubuntu14: ~ 90x24
davy@davyubuntu14:~$ wget -O /dev/null http://www.mikrotik.com/download/winbox.e
xe
--2014-09-23 16:26:45--  http://www.mikrotik.com/download/winbox.exe
Resolving www.mikrotik.com (www.mikrotik.com)... 159.148.147.196, 2a02:610:7501:
1000::2
Connecting to www.mikrotik.com (www.mikrotik.com)|159.148.147.196|:80... connect
ed.
HTTP request sent, awaiting response... 302 Found
Location: http://download2.mikrotik.com/winbox.exe [following]
--2014-09-23 16:26:48--  http://download2.mikrotik.com/winbox.exe
Resolving download2.mikrotik.com (download2.mikrotik.com)... 54.240.184.81, 54.2
40.184.234, 54.230.129.229, ...
Connecting to download2.mikrotik.com (download2.mikrotik.com)|54.240.184.81|:80.
.. connected.
HTTP request sent, awaiting response... 200 OK
Length: 114176 (112K) [application/x-msdownload]
Saving to: '/dev/null'

100%[======================================>] 114.176      656KB/s   in 0,2s

2014-09-23 16:26:48 (656 KB/s) - '/dev/null' saved [114176/114176]

davy@davyubuntu14:~$ ls -l /dev/null
crw-rw-rw- 1 root root 1, 3 Sep 23 15:38 /dev/null
```

E. Vraag in stille modus je eigen WAN IP-adres op, en stuur dit naar stdout. Filter daar alle ongewenste karakters uit (HTML-tags,…) zodat alleen het IP-adres overblijft.



F. Maak een rij van 6 willekeurige, hexadecimale getallen, en voeg daar na ieder getal een dubbel punt aan toe. Dit resulteert in een willekeurig MAC-adres.

```
davy@davyubuntu14:~$ openssl rand -hex 6
8e1ad967ef02
davy@davyubuntu14:~$ openssl rand -hex 6 | sed 's/\(..\)/\1:/g; s/.$//'
97:93:b2:8a:22:89
davy@davyubuntu14:~$
```

G. Vraag een lijst op van uitgevoerde commando's, haal de regelnummers weg, sorteer deze alfabetisch en tel hoeveel keer ieder uniek commando voorkomt. Sorteer deze lijst (aantal + commando) van groot aantal naar klein aantal. Deze lijst draait men om met het commando "tac", waarna men van dit resultaat de eerste 3 lijnen laat zien.

H. Vraag een lijst op van uitgevoerde commando's, maar alleen het commando, geen opties (dus ls ipv ls –l). Tel hoeveel keer ieder uniek commando voorkomt, en sorteer het resultaat van groot naar klein. Vraag van dit resultaat de eerste 3 lijnen op. Als eindresultaat krijg je de 3 meest gebruikte commando's samen met het aantal keer dat ze gebruikt zijn.

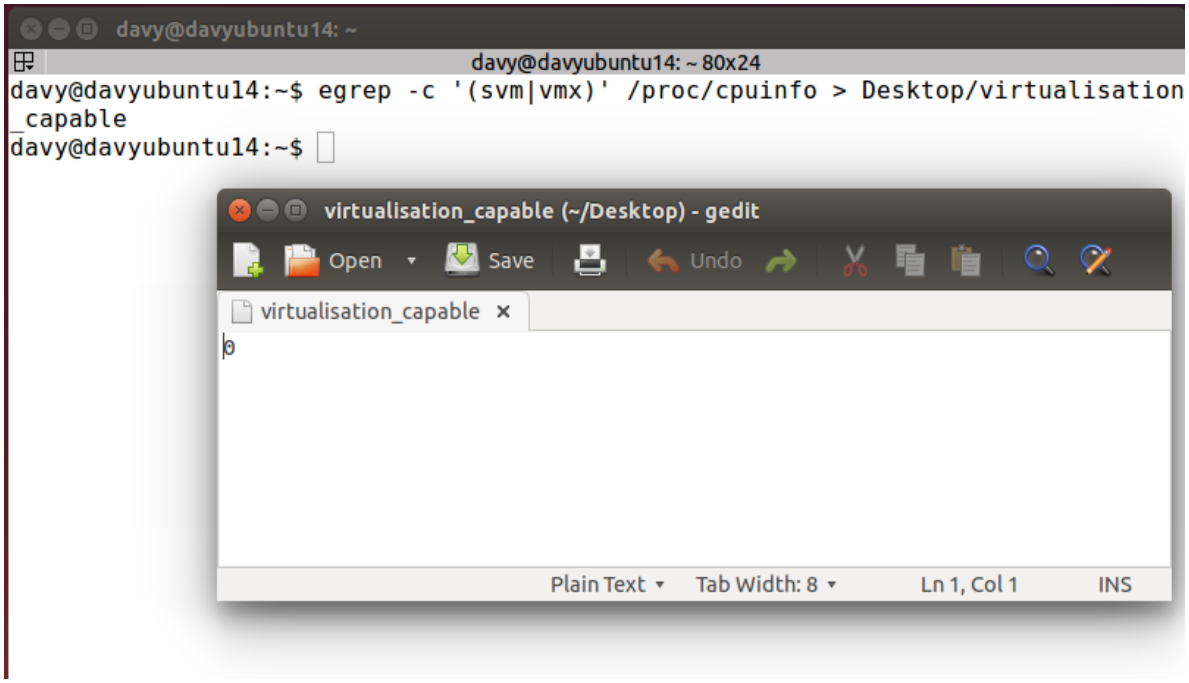
```
davy@davyubuntu14:~/Desktop$ history | awk {'print $2'} | sort | uniq -c | sort
-k1 -rn | head -n3
     10 history
      6 ls
      6 clear
davy@davyubuntu14:~/Desktop$
```

I. Maak een lijst van de locatie van alle geïnstalleerde packages die “apt” bevatten, als de locatie zich in de /usr/bin/ directory bevindt. Mail deze lijst door naar bruno.on.theroad@gmail.com, met als onderwerp “apt query RESULTS on <datum + tijd>.

```
davy@davyubuntu14:~$ dpkg -L apt | grep "^/usr/bin" | tee apt_query_results
/usr/bin
/usr/bin/apt-get
/usr/bin/apt-mark
/usr/bin/apt
/usr/bin/apt-key
/usr/bin/apt-cdrom
/usr/bin/apt-config
/usr/bin/apt-cache
davy@davyubuntu14:~$ ls -l
total 48
-rw-rw-r-- 1 davy davy  132 Sep 23 11:40 apt_query_results
drwxr-xr-x 2 davy davy 4096 Sep 14 12:42 Desktop
drwxr-xr-x 3 davy davy 4096 Sep 15 16:54 Documents
drwxr-xr-x 2 davy davy 4096 Sep 14 12:42 Downloads
-rw-r--r-- 1 davy davy 8980 Sep 14 12:13 examples.desktop
drwxr-xr-x 2 davy davy 4096 Sep 14 12:42 Music
drwxr-xr-x 2 davy davy 4096 Sep 23 11:25 Pictures
drwxr-xr-x 2 davy davy 4096 Sep 14 12:42 Public
drwxr-xr-x 2 davy davy 4096 Sep 14 12:42 Templates
drwxr-xr-x 2 davy davy 4096 Sep 14 12:42 Videos
davy@davyubuntu14:~$
```

J. Tel in /proc/cpuinfo het aantal lijnen waar svm of vmx in voorkomt, en sla het resultaat op in het bestand “virtualisation_capable” dat zich op ons bureaublad bevindt.

Zoals je hieronder ziet heeft mijn machine (laptop) geen lijnen met svm of vmx, en heeft dus geen virtualisatie-technologie.

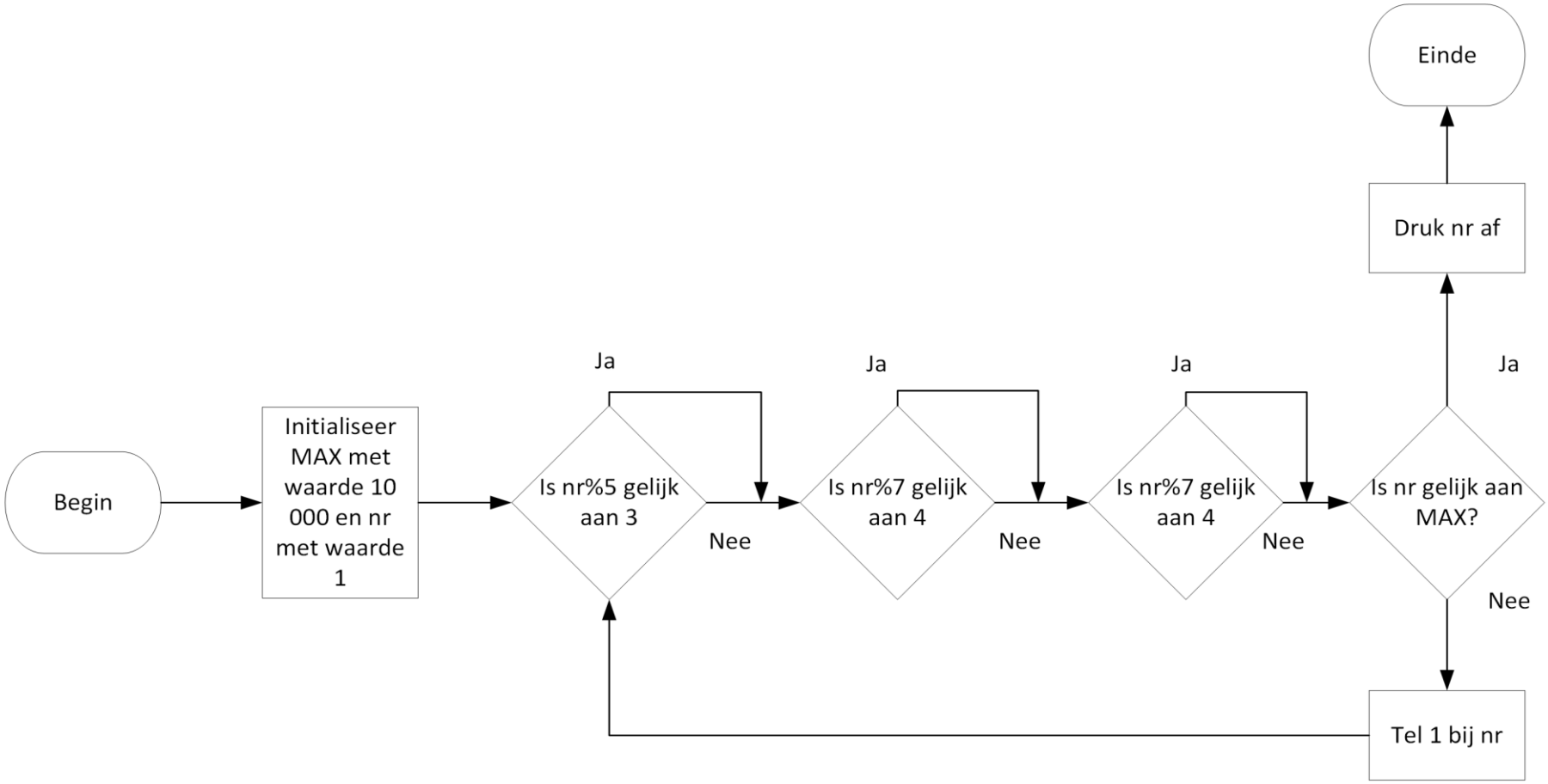


Script:

Het script telt van 1 tot MAX (hier 10 000) in stappen van 1. Tijdens dit tellen test het script of dat de deling van het huidige getal door 5,7 of 9 als rest respectievelijk niet gelijk is aan 3,4,5.

Op het einde van de loop laat het script de inhoud van de variabele “nr” zien, hier 10 000)

Als men de break in commentaar zet, blijkt er niets te gebeuren. Het script loopt zoals voorheen. Dit komt omdat het commando break er alleen voor zorgt dat we uit de loop gaan, niet uit het script. En aangezien “break” op het einde van de loop staat worden alle commando’s in de loop uitgevoerd. De werking van het script is te verklaren: in de if-statements gebruikt men geen else-statement, waardoor het script naar de volgende regel springt. Dit wordt duidelijk op de volgende pagina.



TITLE			
Flowchart: script Linux			
DRAWN BY	DATE	REVISED	VERSION
Davy Van Eynde	25/09/2014		1.0

Voorbeeld van herschreven script:

```
#!/bin/bash
MAX=10000
for ((nr=1; nr<MAX; nr++))
do
      t1= nr % 5
      t2= nr % 7
      t3= nr % 9

      if (( (t1 -ne 3) && (t2 -ne 4) && (t3 -ne 5) ))
      then
            Continue
      fi
      break
done
echo "Number = $nr"
exit 0
```

Subnetting door middel van VLSM

Om aan subnetting te beginnen moeten we eerst kijken hoeveel subnets we nodig hebben, en hoeveel hosts per subnet er nodig zijn:

	ROUTER OF CONNECTIE	AANTAL HOSTS
1	suske	126
2	jerom	62
3	lambik	30
4	wiske	14
5	sidonia-suske	2
6	sidonia-jerom	2
7	sidonia-lambik	2
8	sidonia-wiske	2

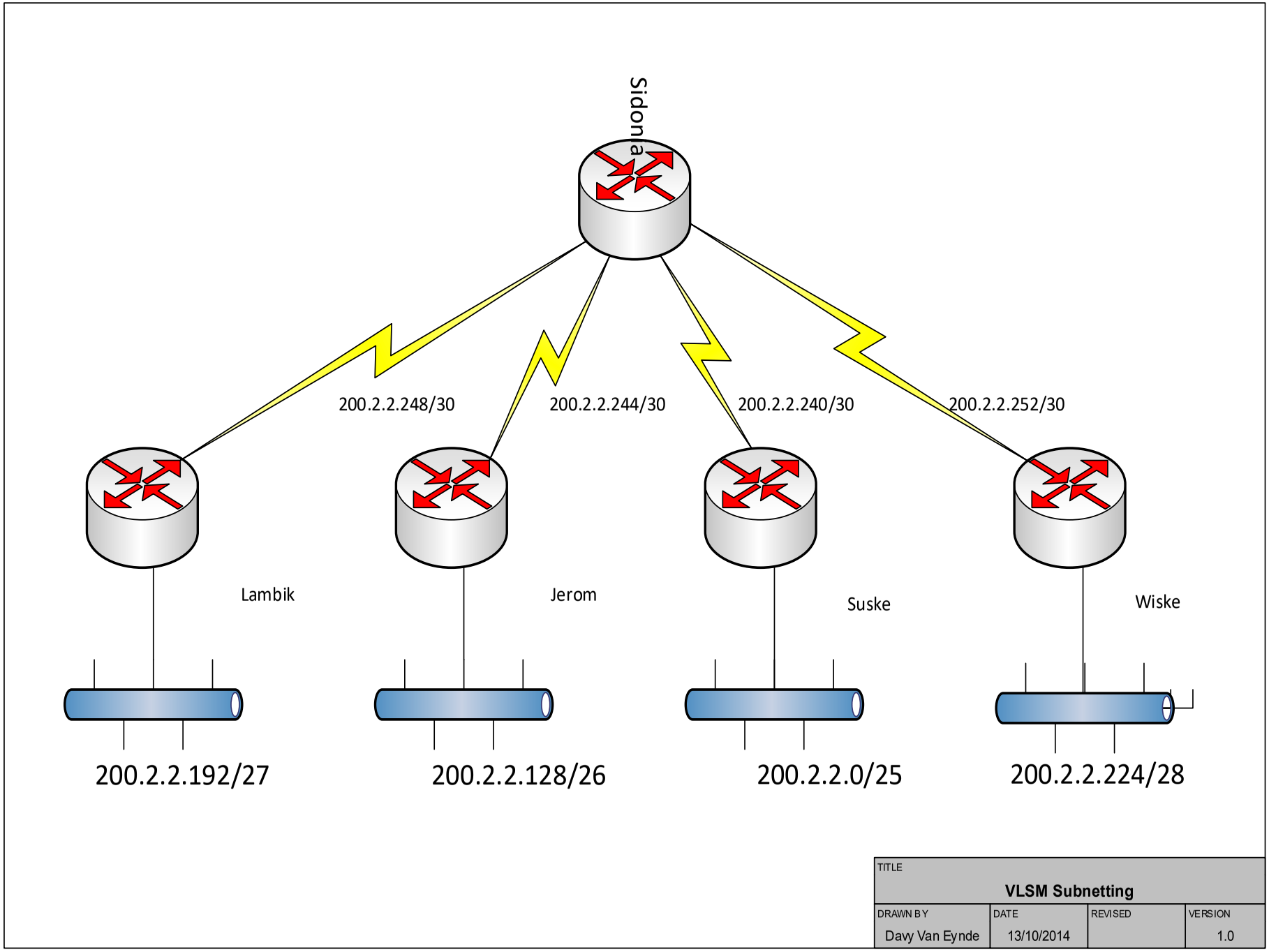
Nu ga ik een hulptabel maken:

Aantal hosts	256	128	64	32	16	8	4	2
Binair	128	64	32	16	8	4	2	1
/x	/25	/26	/27	/28	/29	/30		

We kunnen er aan beginnen. Voor subnet 1, bij router suske, heb ik 126 hosts nodig. Dit subnet begint bij 200.2.2.0. Dus kijk ik in mijn hulptabel, en het best passende aantal hosts is 128. Het volgende subnet is dus 200.2.2.128. Daaruit leid ik af dat het broadcast-adres van het eerste subnet 200.2.2.127 is, en de bruikbare IP-adressen 200.2.2.1 tot 200.2.2.126 zijn. De CIDR-notatie van dit eerste subnet is 200.2.2.0/25.

Op deze manier werkte ik verder voor alle subnets, en kreeg ik volgend resultaat:

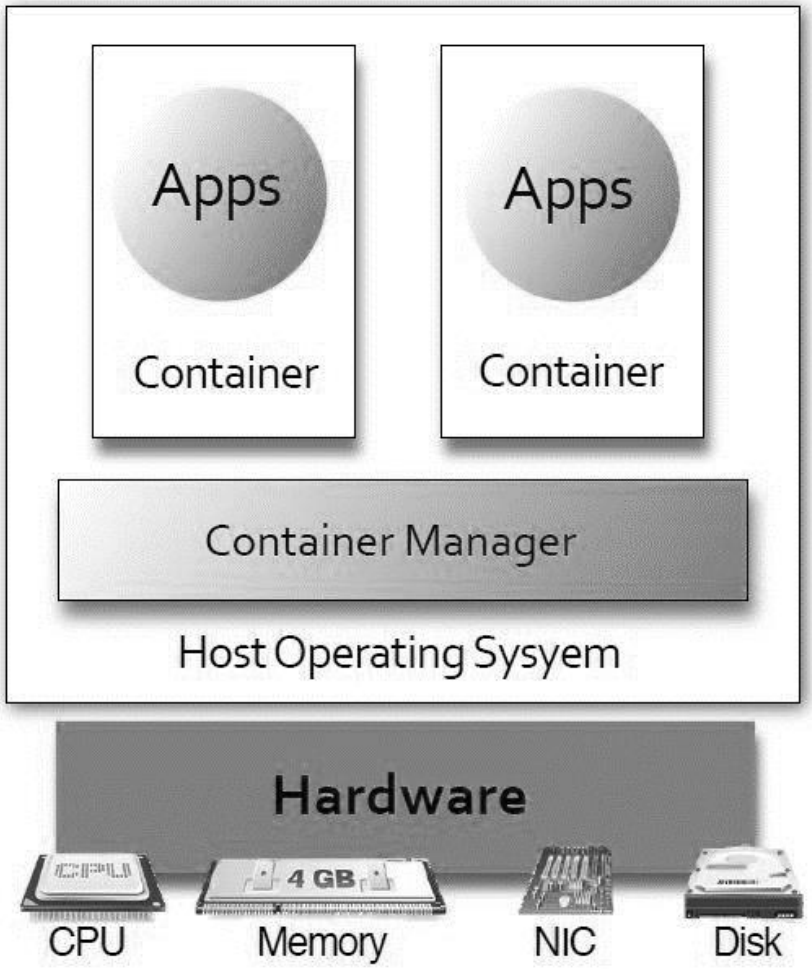
Subnet	CIDR-notatie	Broadcast-adres	Te gebruiken IP-range
1	200.2.2.0/25	200.2.2.127	200.2.2.1 - 200.2.2.126
2	200.2.2.128/26	200.2.2.191	200.2.2.129 - 200.2.2.190
3	200.2.2.192/27	200.2.2.223	200.2.2.193 - 200.2.2.223
4	200.2.2.224/28	200.2.2.239	200.2.2.225 - 200.2.2.238
5	200.2.2.240/30	200.2.2.243	200.2.2.241 - 200.2.2.242
6	200.2.2.244/30	200.2.2.247	200.2.2.245 - 200.2.2.246
7	200.2.2.248/30	200.2.2.251	200.2.2.249 - 200.2.2.250
8	200.2.2.252/30	200.2.2.255	200.2.2.253 - 200.2.2.254


Sidonia
200.2.2.248/30
200.2.2.244/30
200.2.2.240/30
200.2.2.252/30
Lambik
Jerom
Suske
Wiske
200.2.2.192/27
200.2.2.128/26
200.2.2.0/25
200.2.2.224/28
TITLE
VLSM Subnetting
DRAWN BY
Davy Van Eynde
DATE
13/10/2014
REVISED
VERSION
1.0

Virtualisatie door middel van containers

Bij virtualisatie door middel van containers wordt er gebruik gemaakt van “user spaces”. Op de hardware-laag draait een host-OS, waarop dan weer die user spaces of “containers” draaien. In deze containers kunnen dan applicaties draaien. Het komt er op neer dat alle virtuele machines op dezelfde hardware en kernel draaien, maar dat ze ieder hun eigen filesystem, processen en virtuele apparaten/geheugen hebben.

Een grafische voorstelling van container-based virtualisatie:



De voordelen van container-based virtualisatie zijn te vinden op vlak van schaalbaarheid en performance. Bij dit systeem kunnen er evenveel CPU’s en geheugen gebruikt worden als dat er beschikbaar gesteld worden door de host-hardware.

Door de goede schaalbaarheid zijn containers populair op systemen waar er bvb. 100 Linux-guests moeten draaien, zoals bij hosting firma’s.

Voorbeelden van container-based virtualisatiesystemen zijn Docker en LXZ onder Linux. HP en Solaris hebben hiervoor proprietary software, namelijk HP-UX en Solaris Containers. Soortgelijke systemen bestonden vroeger al, namelijk chroot (1982) voor UNIX-varianten en FreeBSD jails (1998) voor FreeBSD.

Docker wordt onder andere gebruikt in bedrijven zoals E-Bay en Spotify.

CISSP Domeinen

CISSP staat voor Certified Information Systems Security Professional. Dit certificaat, dat onafhankelijk en wereldwijd behaalbaar is, behandelt de veiligheid van datasystemen en bedrijfsprocessen.

Om de vele onderwerpen die hiermee te maken hebben, heeft men ze ingedeeld in 10 categorieën, de 10 “domeinen”. Ik ga nu de domeinen kort bespreken:

1. **Access Control:**
   In dit domein worden de mechanismes besproken die ervoor zorgen dat een persoon alleen toegang heeft tot de data/systemen waar hij recht toe heeft. Voorbeelden hiervan zijn een paswoord, maar ook bvb. een single sign-on device voor two-factor authenticatie. Dit single sign-on device is een apparaat dat codes genereert, en om in te loggen heeft men een paswoord nodig **EN** de gegenereerde code.

   Voorbeeld uit de schoolomgeving: gebruikersnamen en paswoorden per leerling

2. **Telecommunicatie en netwerkveiligheid:**
   Hier spreekt men vooral over “het netwerk” dat men gebruikt om onze data te bereiken. Bij dit domein vraagt men zich af welke apparaten, protocollen en netwerk services zullen gebruikt worden. Welke firewall gaat men bvb. installeren, of hoe kunnen we twee van onze gebouwen verbinden?

   Voorbeeld uit de schoolomgeving: de door de school gebruikte gateway en de aanwezigheid van een eigen DNS-server.

3. **Business continuity planning en disaster recovery:**
   Dit domein bespreekt hoe men, indien er toch iets misloopt, ervoor kan zorgen dat men zo snel mogelijk de systemen terug draaiende heeft, en zo veel mogelijk data terug beschikbaar heeft. Back-ups van de data en redundante hardware (eventueel op een andere site) zijn mogelijke onderwerpen, maar ook bvb. de vraag of er iemand de nodige kennis heeft om het bedrijf draaiende te houden als de systeembeheerder ziek is.

   Voorbeeld uit de schoolomgeving: Ik ben niet zeker of dit aanwezig is, maar de school kan mits imaging (of zelfs met de Microsoft Deployment Kit) snel werkstations herinstalleren indien er iets misgaat met de OS-installatie.

4. **Security management:**
   Op het niveau van management gaat men bij dit domein kijken of de juiste procedures en info is verschaft aan alle medewerkers. Als men iemand niet uitlegt hoe hij/zij veilig omgaat met onze data kunnen we nooit verwachten dat die persoon dat effectief doet. Ook risk assessment is een deel van dit domein: als men niet weet dat er nieuwe risico's zijn, kan men voor deze risico's geen nieuwe procedures maken.

   Voorbeeld uit de schoolomgeving: opleiding/opfrissing in de veiligheidsprocedures voor de leerkrachten.

5. **Applications/System Development Security:**
   Hier gaat het vooral over de gebruikte en gemaakte software waarmee we onze data behandelen. Hoe is die software ontwikkeld? Hoe gaat die software onze data benaderen? Zorgt die niet voor veiligheidslekken, zoals bvb. SQL injectie? Zijn er backdoors die er voor zorgen dat derden aan onze data kunnen?

   Voorbeeld uit de schoolomgeving: analyse en testing van de software om aanwezigheden in te voeren.

6. **Cryptografie:**
   De methodes en procedures om onze data te versleutelen worden hier besproken, zowel welke algoritmes er gebruikt zullen worden, als hoe we al die sleutels gaan managen. Als iedereen namelijk onze sleutels kan gebruiken en zo de sleutels verspreid worden, heeft encryptie niet veel zin.

   Voorbeeld uit de schoolomgeving: versleuteling van de leerling gegevens in de schooldatabase.

7. **Security Architecture en modellen:**
   Als men dit domein bekijkt gaat het vooral over richtlijnen om veilig te werken: antivirus-richtlijnen, welke back-ups worden wanneer en hoe genomen, patch-policy,…

   Voorbeeld uit de schoolomgeving: procedure omtrent patchen van het OS en de software

8. **Operations security:**
   Dit gaat over de dagdagelijkse “systeem”-bezigheden, en kan gaan over het personeel, de hardware, en het controleren/monitoring van je systeem. Niet alleen de methodes worden hier besproken, maar ook wie wat mag doen, en wanneer…

   Voorbeeld uit de schoolomgeving: de dames van het secretariaat die geen documenten meer van USB-stick mogen afdrukken voor leerlingen.

9. **Fysieke veiligheid:**
   Bij fysieke veiligheid bespreekt men alle fysieke risico’s en maatregelen om deze risico’s te beperken. Het gaat hier over risico’s voor data, systemen/hardware, gebouwen en personeel. Inbraak en diefstal zijn natuurlijk een bekend risico, en dan kan men zich afvragen of onze servers achter slot en grendel staan? Kan men nagaan wie wanneer in de serverroom kan? Is er een goedwerkend badge-systeem? Maar in domein zal men ook risico’s zoals overstroming, oververhitting in de serverroom,… bespreken.

   Voorbeeld uit de schoolomgeving: men kan bvb. de switch die zich in sommige lokalen bevindt achter slot en grendel zetten, zodat niemand per ongeluk kabels kan verwisselen.

10. **Law, Investigation & Ethics:**
    In het laatste domein bespreekt men de wetgeving en de ethische regels waaraan men moet voldoen, maar ook hoe men gaat reageren wanneer er iemand in of buiten onze organisatie die regels overtreedt. Ook de gebruikte methodes om aan wetgeving/ethiek te voldoen worden hier besproken. De bekendste regelgevingen zijn natuurlijk strafrecht en copyright, maar men heeft ook bvb. handelsrecht en privacy.
    Stel bvb. dat er iemand in ons netwerk inbreekt, en data steelt. Dan moeten we dit natuurlijk detecteren, we moeten weten welke instanties er verwittigd moeten worden, maar ook hoe men deze data-diefstal kan bewijzen.

    Voorbeeld uit de schoolomgeving: de school die meedoet aan het MA3D-project, zodat leerlingen bepaalde software legaal kunnen gebruiken tegen een lage kost. Dit vermindert de kans op inbreuken tegen de copyright-wetgeving.

Eigen opmerking:
na mijn onderzoek ben ik van mening dat de onderverdeling in de verschillende domeinen vrij vaag is, en dat als men bvb. een specifiek voorbeeld zou bespreken men al vlug een overlapping heeft tussen de verschillende domeinen.
Zo zal bvb. een secretaresse die een illegale versie van Office installeert op haar workstation al snel in “Law”, “Security management” en “Access control” vallen.

Diffie-Hellman

Het Diffie-Hellman sleuteluitwisselingsprotocol is een methode waardoor twee partijen, die elkaar nog niet kennen, een gedeelde geheime sleutel kunnen uitwisselen over een onbeveiligde lijn.

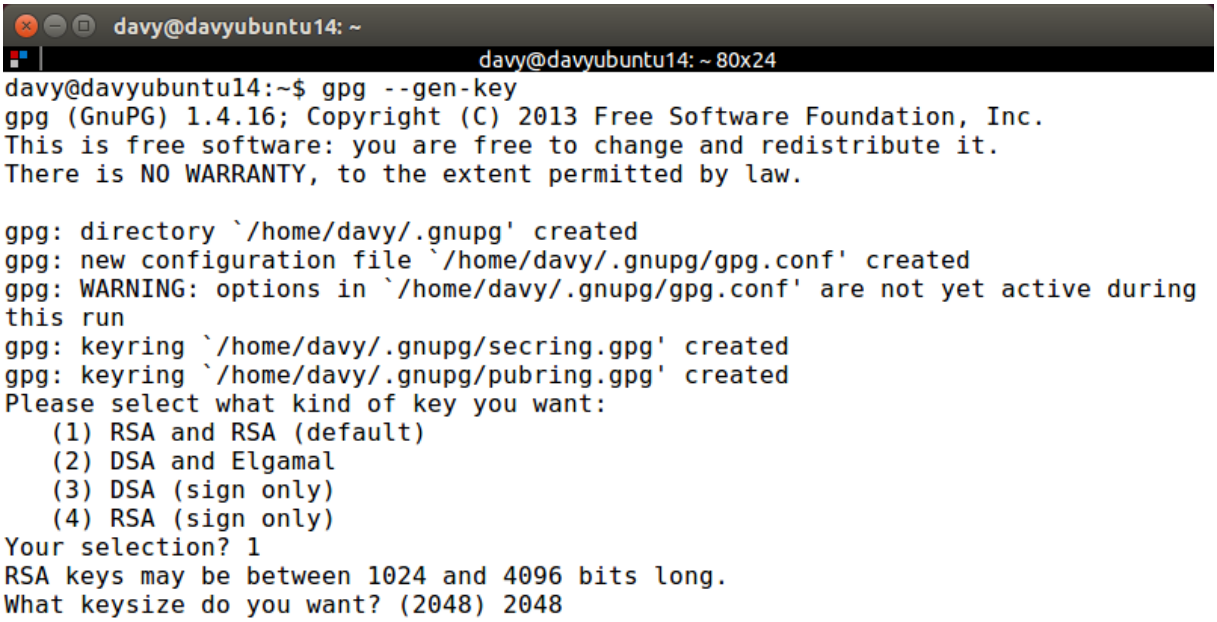
Deze geheime sleutel kan dan gebruikt worden om door beide partijen data te encrypteren of te decrypteren: symmetrische versleuteling.

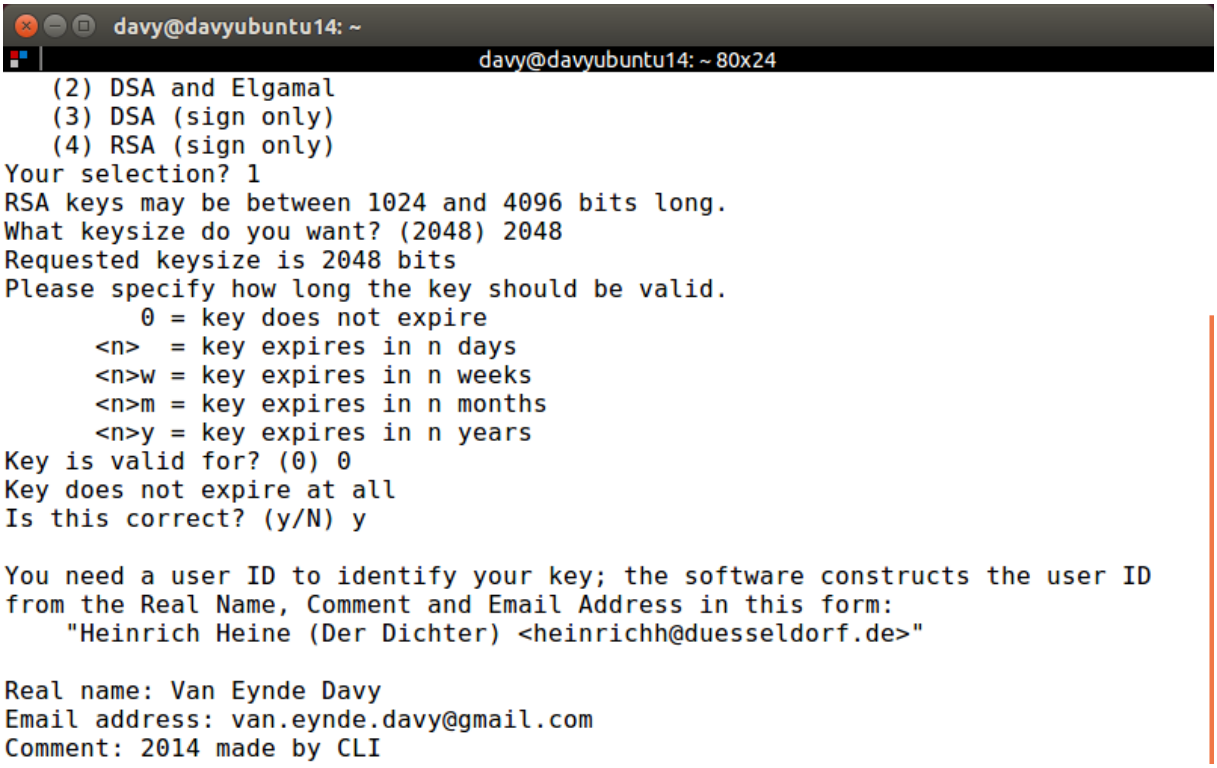
Het basisidee achter het Diffie-Hellman protocol:

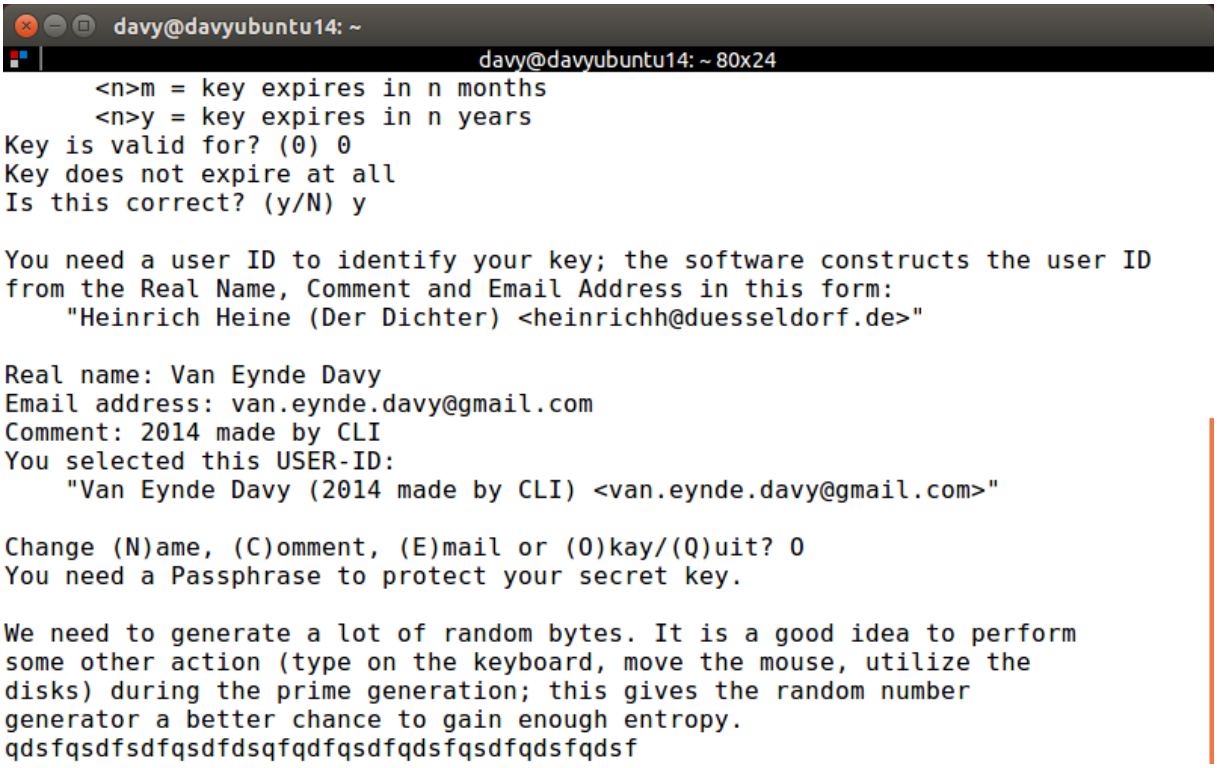
1. Ik kies twee priemgetallen en laat jou weten welke (bvb. 11 en 37)
2. Jij kiest een getal, en houdt dit geheim. (bvb. 4) Daarmee doe je een berekening (11 tot de 4^{de} mod 37, 14641 mod 37, of 26). Deze uitkomst stuur je door naar mij.
3. Ik doe hetzelfde (bvb. 7). Weer gebeurt er een berekening (11 tot de 9de mod 37, of 36), en ik stuur de uitkomst door naar jou
4. Met die uitkomst die jij kreeg in stap 3, doe je dezelfde berekening van stap 2 (36 tot de 4^{de} mod 37=1)
5. Met de uitkomst die ik kreeg in stap 2, doe ik dezelfde berekening als in stap 3 (26 tot de 9^{de} mod 37=1)

In ons voorbeeld is “1” de gedeelde geheime sleutel.

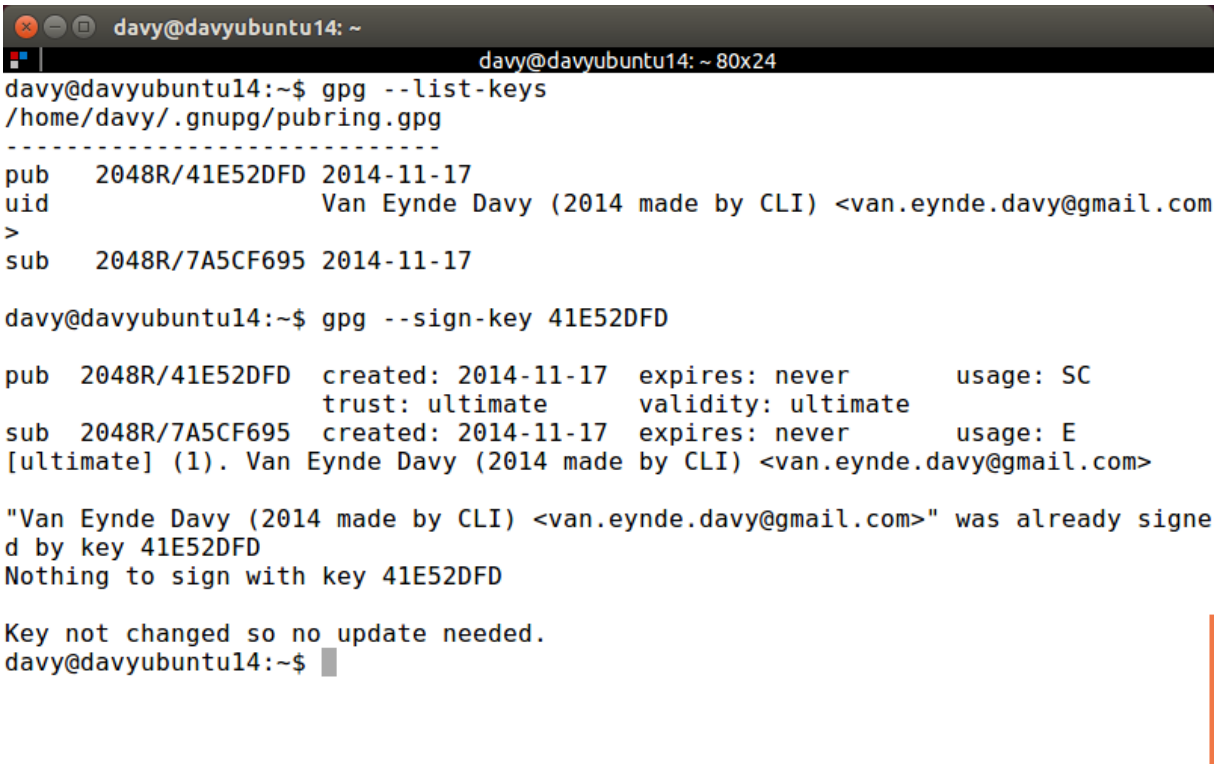
Eerst moet ik het sleutelpaar (privaat/publiek) aanmaken. Aangezien ik bij een vorige poging problemen had toen ik Seahorse gebruikte, gebruik ik nu de commandline.



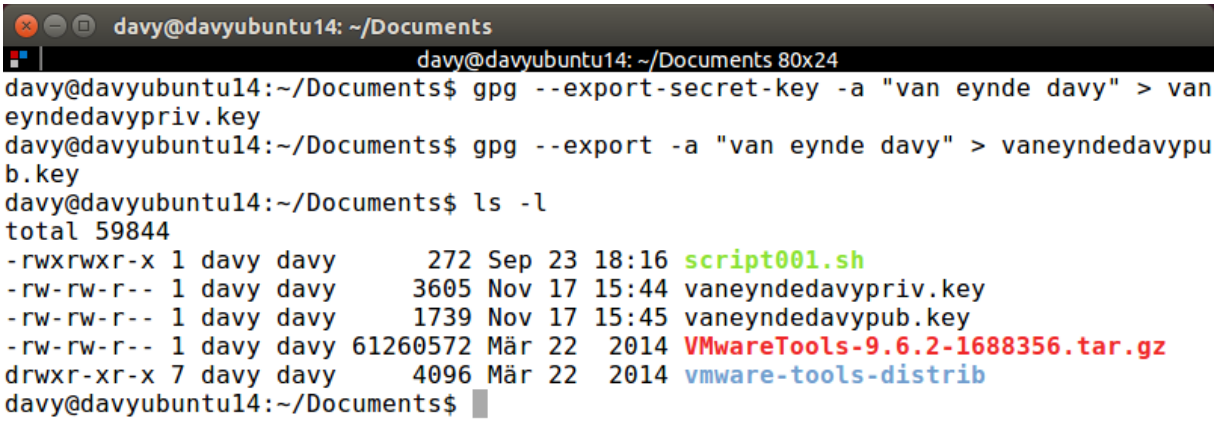




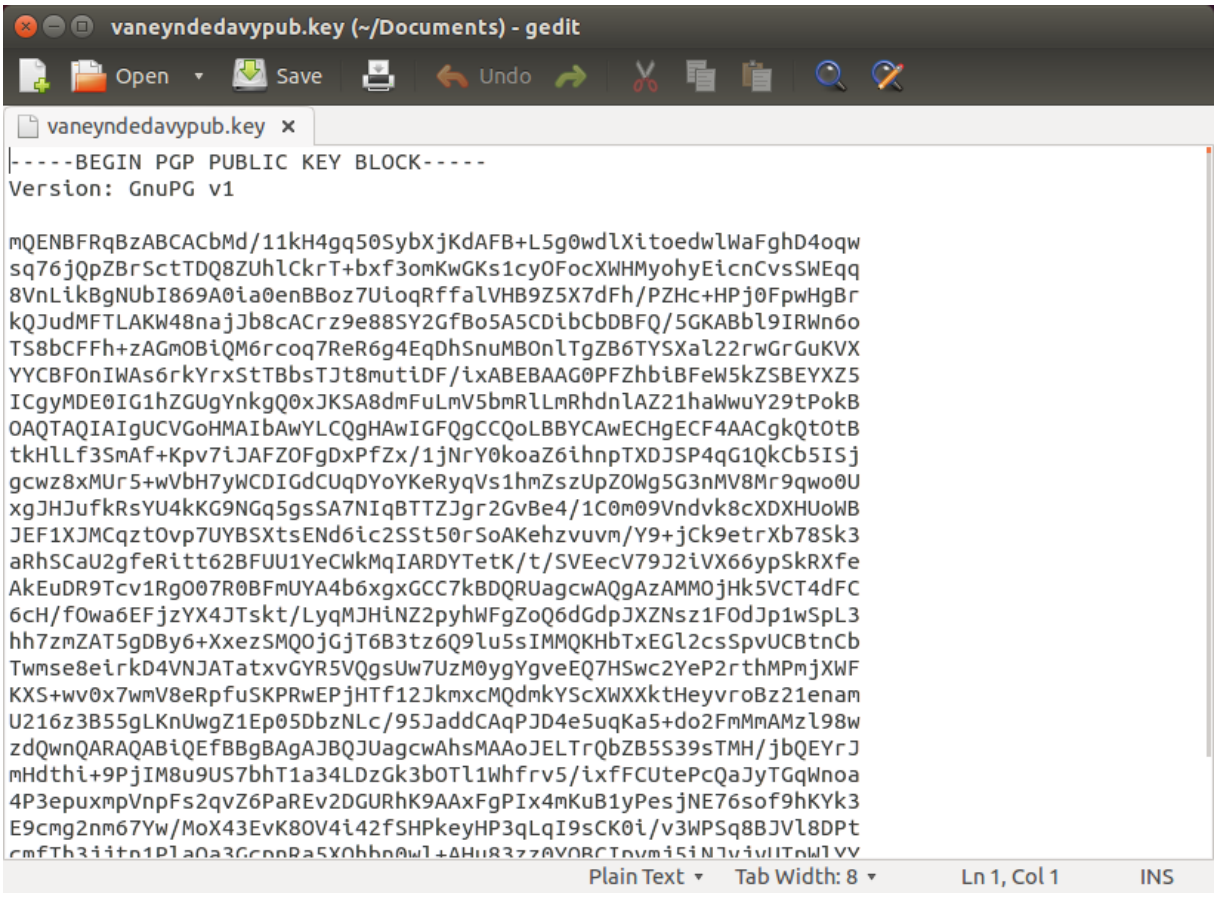
Als het sleutelpaar is aangemaakt, dan tekenen we onze eigen sleutel:



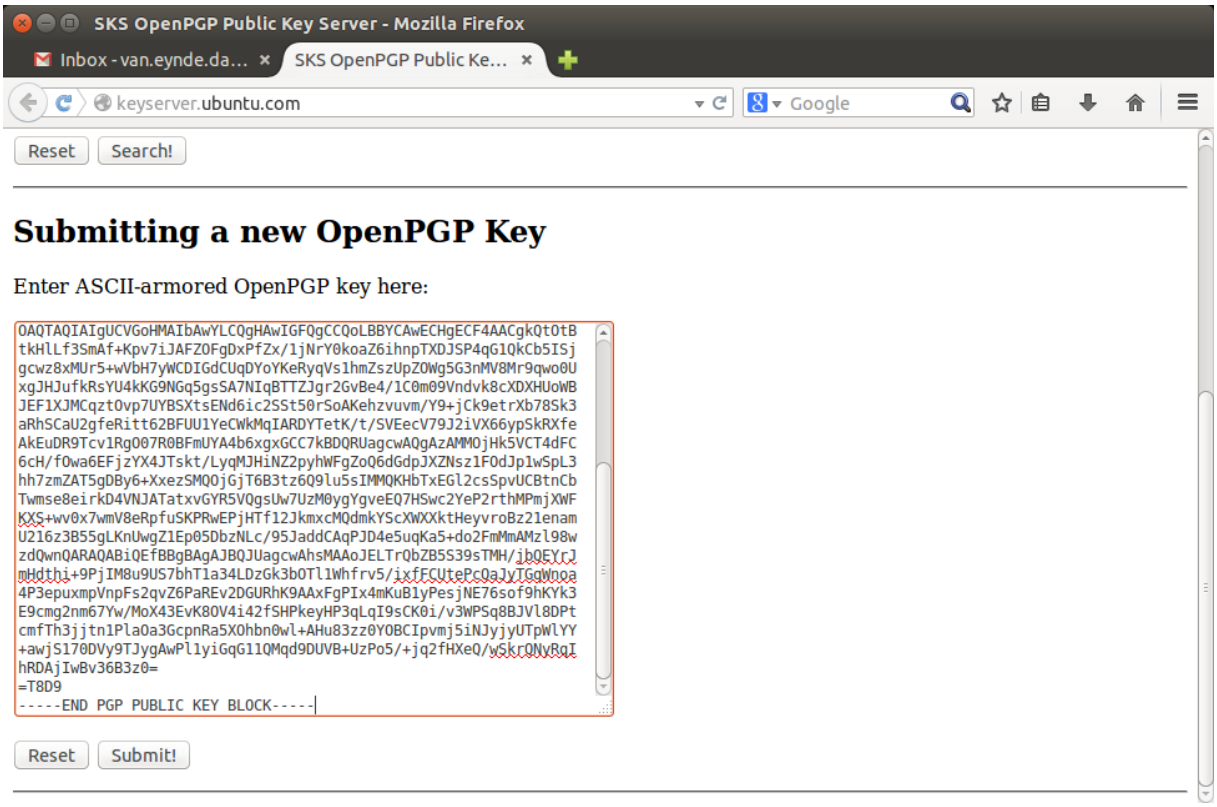
Daarna exporteer ik deze sleutel naar een bestand:



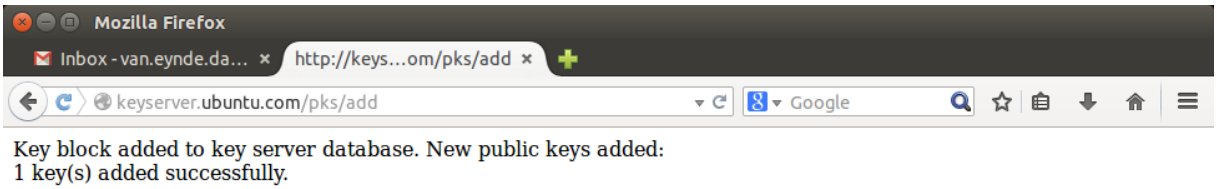
Een mogelijkheid om onze publieke sleutel bekend te maken aan derden is via een keyserver. Eerst open ik het bestand waar de sleutel instaat:



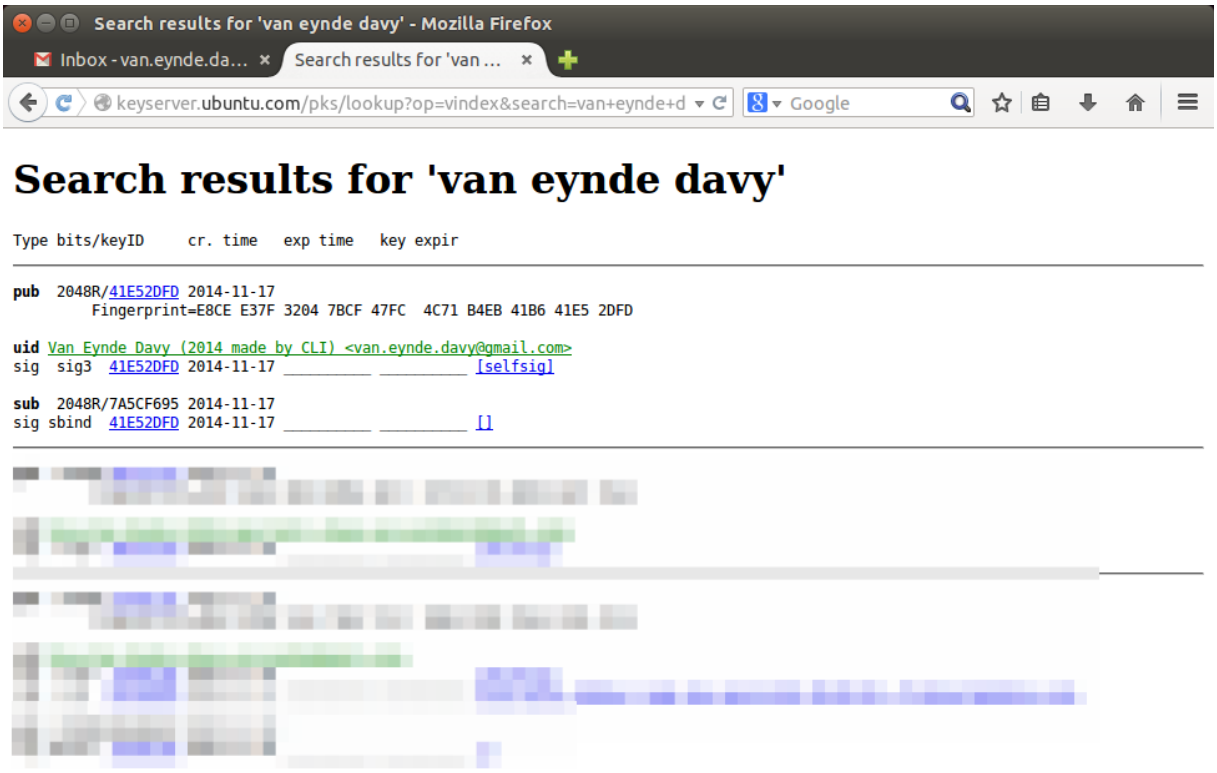
Daarna ga ik met mijn browser naar een keyserver, en plak ik mijn publieke sleutel in het juiste veld:



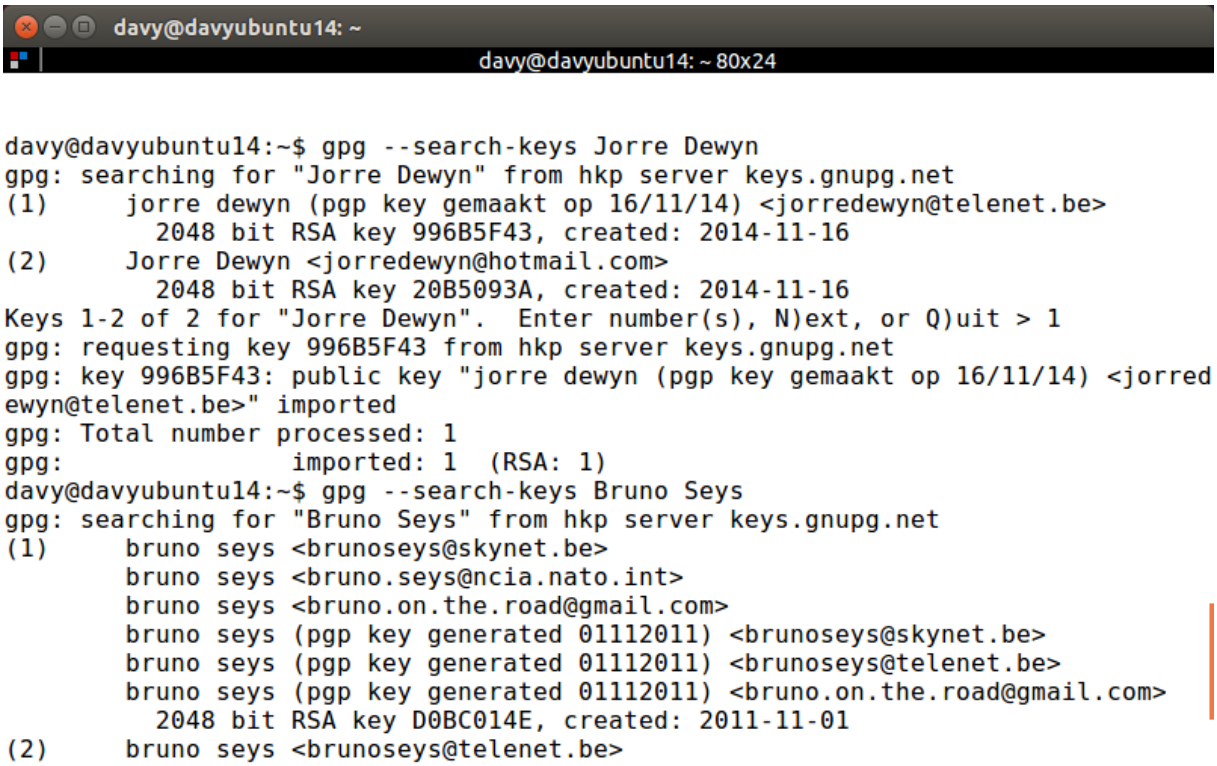
Als ik dan op “Submit!” klik, en alles verloopt correct, krijg ik volgend scherm:



Nu is mijn publieke sleutel openbaar gemaakt. Als controle zoek ik mijn naam op:

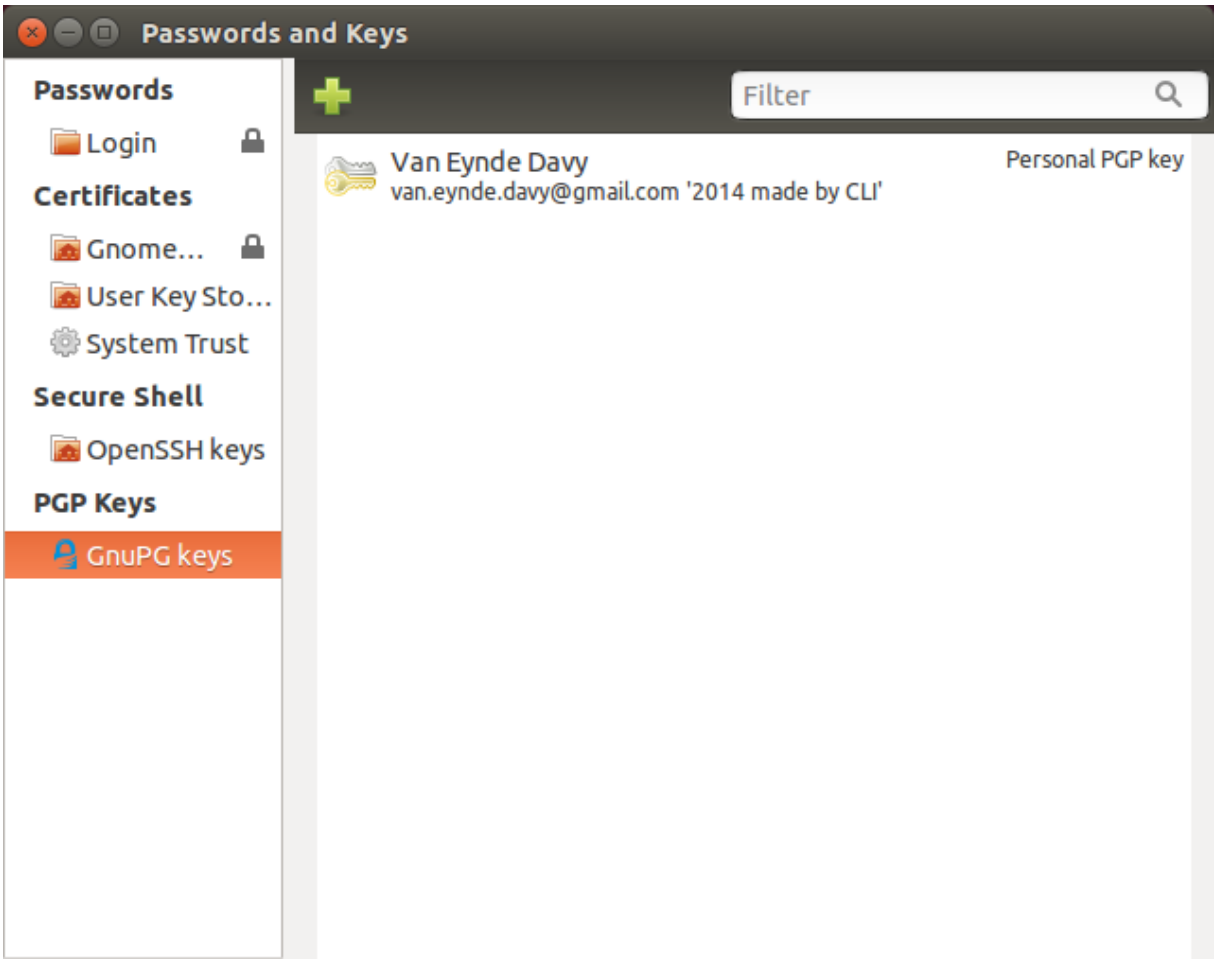


Sleutels van anderen kan men niet alleen opzoeken via onze browser, maar ook via de CLI:



En dan kan men ook de gevonden sleutels tekenen via de CLI:

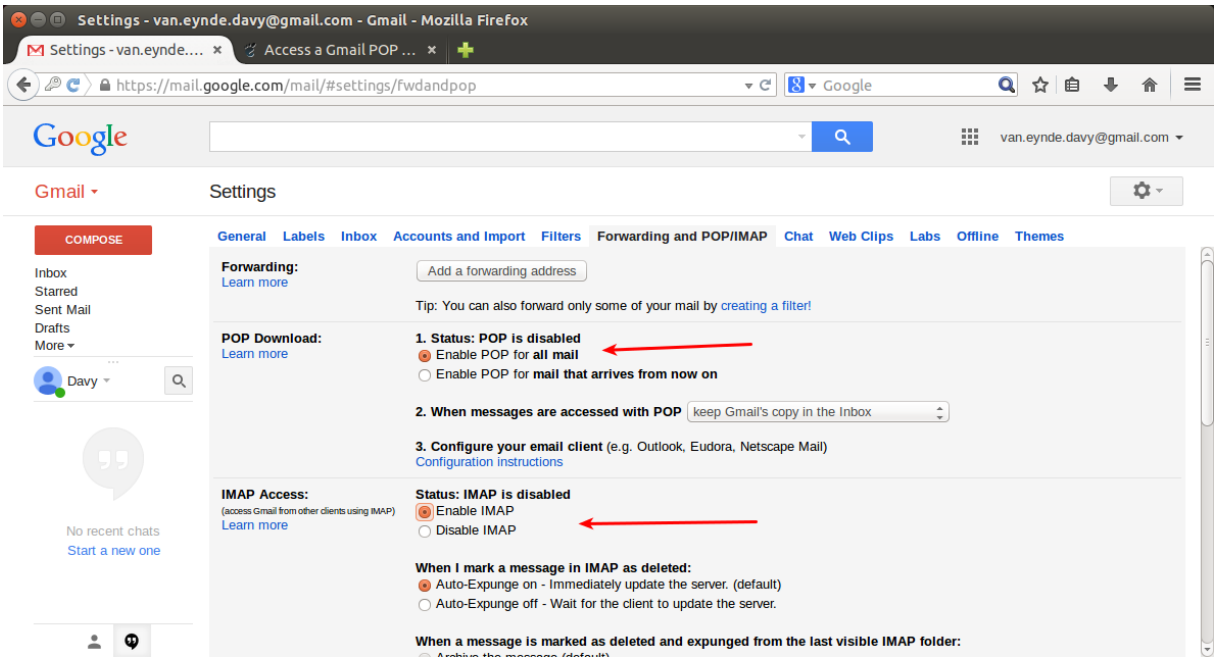
Als ik nu Seahorse open, en alleen de eigen sleutels tonen, zien we dat de sleutel op de lijst staat.



Hierna wil ik via Thunderbird/Enigmail een versleutelde en ondertekende mail sturen, maar ik krijg de foutmelding dat het paswoord van mijn e-mail account (Gmail) fout zou zijn. Als ik via de web-interface inlog met hetzelfde paswoord werkt alles perfect, maar via Thunderbird kan ik mijn Gmail-account niet toevoegen.

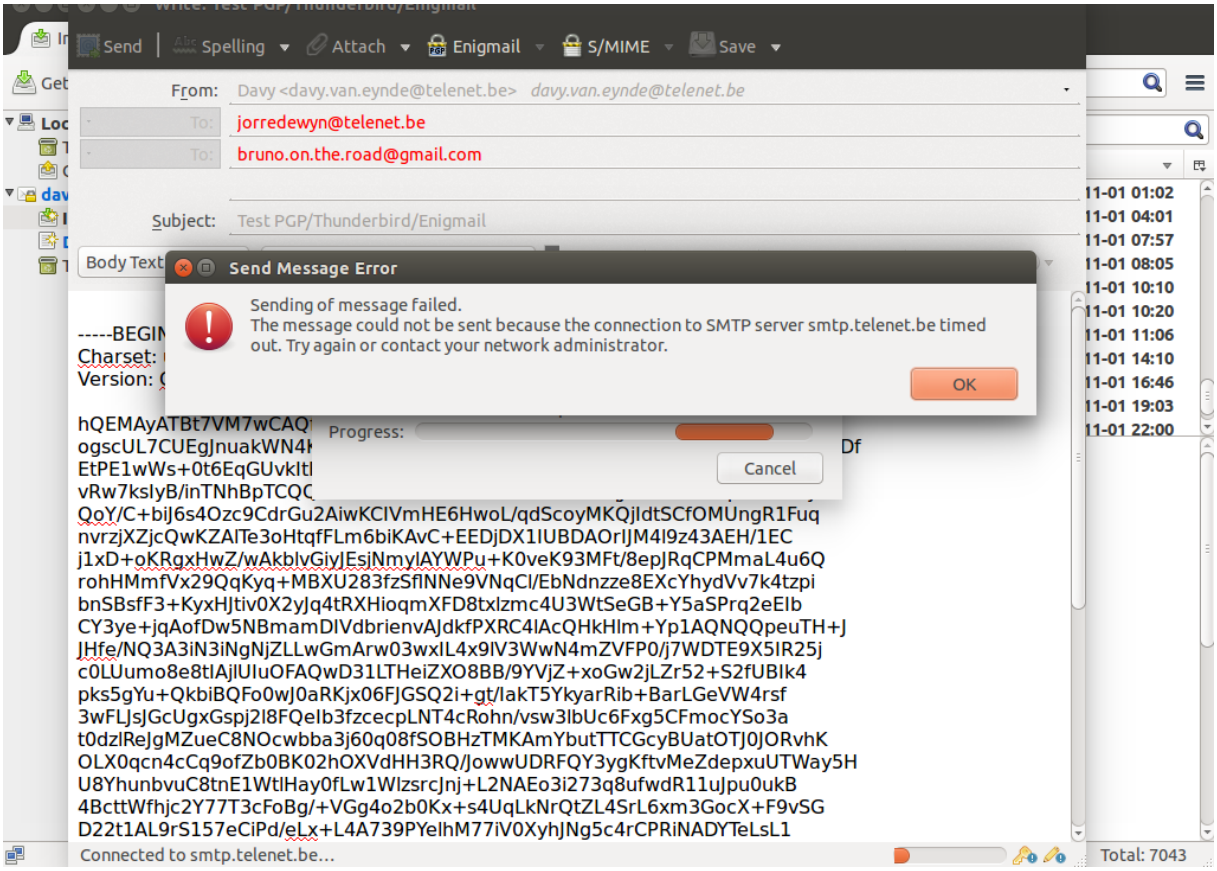
Bij nazicht op diverse fora en websites blijkt er in de communicatie tussen Thunderbird en Gmail iets mis te lopen, en er worden enkele oplossingen voorgesteld.

Deze spreken bvb. over het activeren van POP en IMAP in de Gmail-account

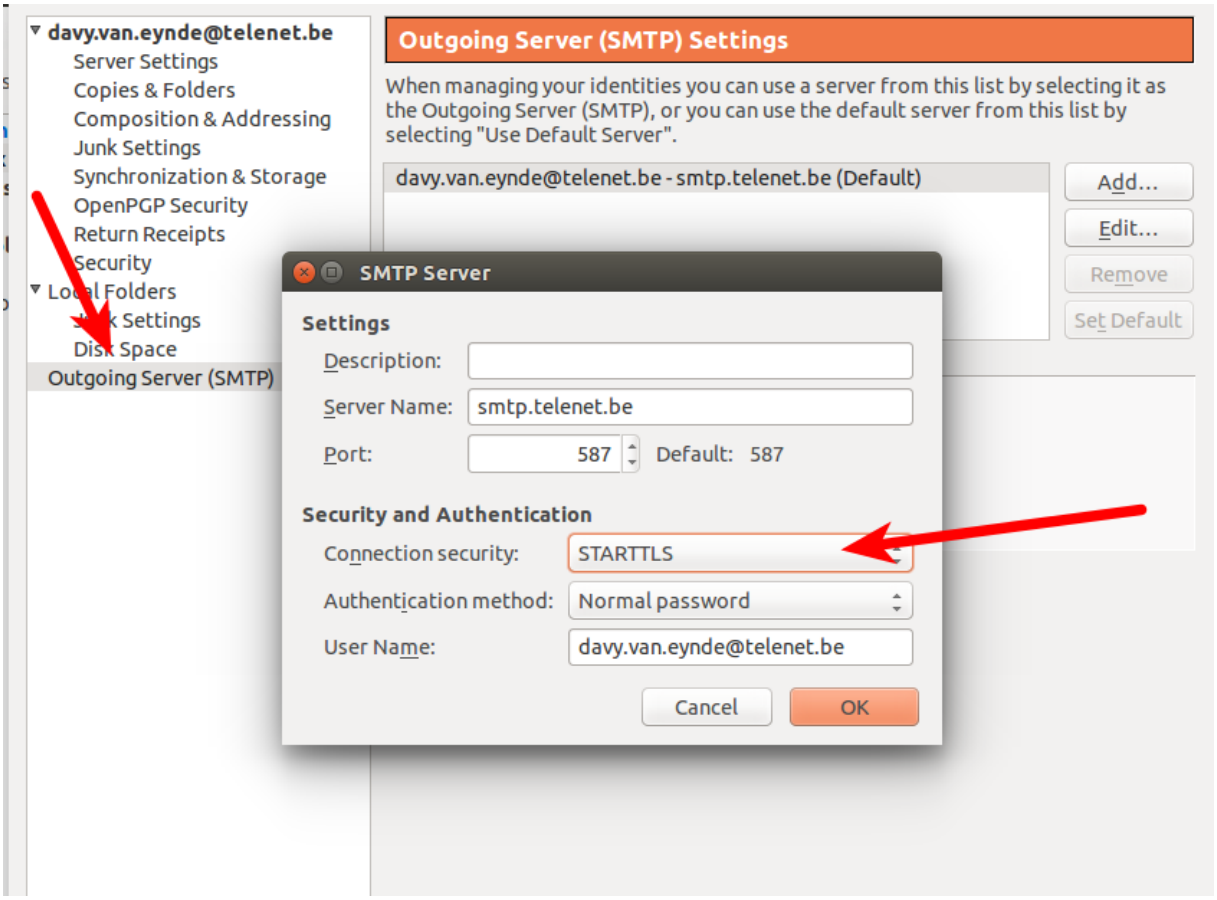


Géén van deze oplossingen hielpen voor mij. Daarom ben ik terug vanaf nul begonnen, maar ditmaal met mijn Telenet mailaccount.

Nadat ik alles herhaald had, kreeg ik bij het versturen van mail een SMTP-fout:



Dit heb ik kunnen verhelpen door bij Thunderbird de SMTP-instellingen van TLS/SSL te veranderen naar STARTTLS. Hierna lukte het mij om mail te versturen.


davy.van.eynde@telenet.be
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Synchronization & Storage
OpenPGP Security
Return Receipts
Security
Local Folders
Disk Space
Outgoing Server (SMTP)
Outgoing Server (SMTP) Settings
When managing your identities you can use a server from this list by selecting it as the Outgoing Server (SMTP), or you can use the default server from this list by selecting "Use Default Server".
davy.van.eynde@telenet.be - smtp.telenet.be (Default)
Add...
Edit...
Remove
Set Default
SMTP Server
Settings
Description:
Server Name: smtp.telenet.be
Port: 587 Default: 587
Security and Authentication
Connection security: STARTTLS
Authentication method: Normal password
User Name: davy.van.eynde@telenet.be
Cancel
OK

HTTP headers

Onderverdeling in request/response

Er werden enkele voorbeelden van header-velden gegeven in de cursus. Aan ons om deze op te delen in twee categorieën: de request en de response.

Request
If-Modified-Since
Content-Type
Authorization
From
Content-Length
User-Agent
Response
Content-Length
Last-Modified
WWW-Authenticate

HTTP headers analyseren bij gebruik van een eigen webserver

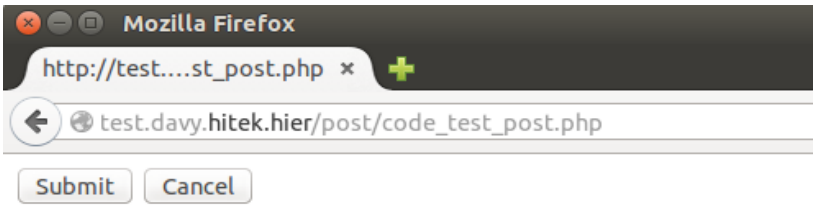
Als testomgeving heb ik een virtuele machine met Ubuntu 14.04 en de LAMP-stack gebruikt. Op deze webserver staat het bestand test.php, met de phpinfo()-functie.
Om de HTTP headers te bekijken open ik het bestand test.php met mijn browser vanuit de host-machine. Terwijl ik dit doe is Wireshark actief op de host-machine, waardoor ik de headers kan bekijken.

Request
GET /test.php HTTP/1.1
Host: 192.168.0.113
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.65 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4
Response
HTTP/1.1 200 OK
Date: Sun, 23 Nov 2014 16:36:13 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.5
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 18082
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Formulier gebruikmakend van de POST-methode

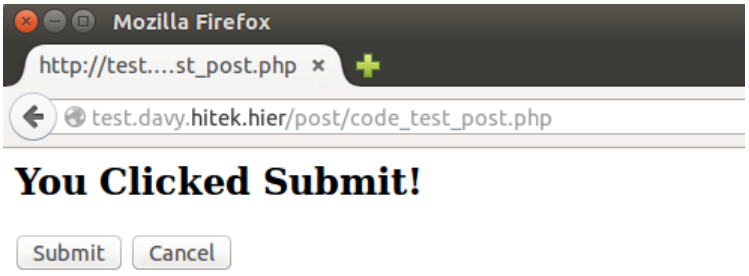
```
davy@davyubuntu14: /var/www/html/post
davy@davyubuntu14: /var/www/html/post 80x24
<html>
        <body>
                <?php
                        if(isset($_POST["submit"])){
                                echo "<h2>You Clicked Submit!</h2>";
                        } else if(isset($_POST["cancel"])){
                                echo "<h2>You Clicked Cancel!</h2>";
                        }
                ?>

                <form action="<?php echo $_SERVER['PHP_SELF']; ?>" method="post"
>
                <input type="submit" name="submit" value="Submit">
                <input type="submit" name="cancel" value="Cancel">
                </form>
                <br><br><br>
                <?php
                        echo date("l, F d, Y h:i", time());
                ?>
        </body>
</html>
~
~
"code_test_post.php" [dos] 20L, 475C                          1,1           All
```

Als men dan voor de eerste keer de pagina opent, krijgt men dit resultaat:



Wednesday, December 10, 2014 07:23

Als je dan op één van de twee knoppen klikt:



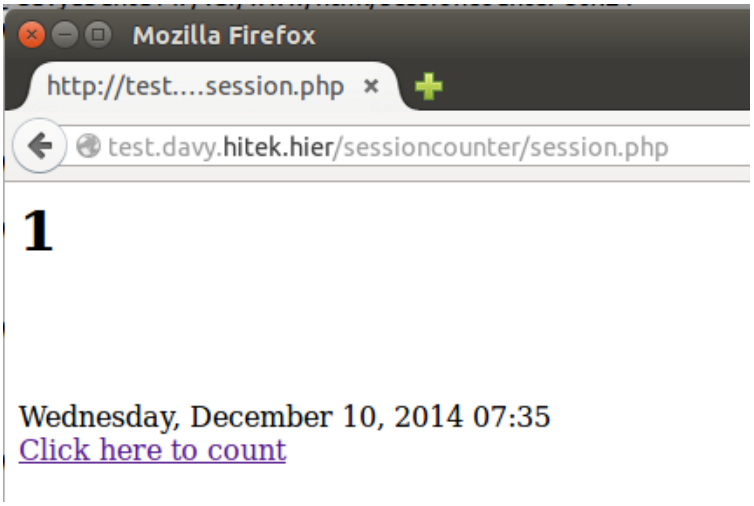
Wednesday, December 10, 2014 07:25

Hier maak ik een sessie aan die bijhoudt hoeveel keer men op de link klikt.

davy@davyubuntu14: /var/www/html/sessioncounter

davy@davyubuntu14: /var/www/html/sessioncounter 80x24

```
<html>

<body>

<?php
session_start();

if (!$_SESSION["count"]){
$_SESSION["count"] = 0;
}
if ($_GET["count"] == "yes"){
$_SESSION["count"] = $_SESSION["count"] + 1;
}
echo "<h1>".$_SESSION["count"]."</h1>";
echo "<br><br><br>";
echo date("l, F d, Y h:i", time());
?>
<br>
<a href="session.php?count=yes">Click here to count</a>

</body>
</html>
~
"session.php" [dos] 22L, 369C                                 1,1           All
```



PHP en sessies, deel 2

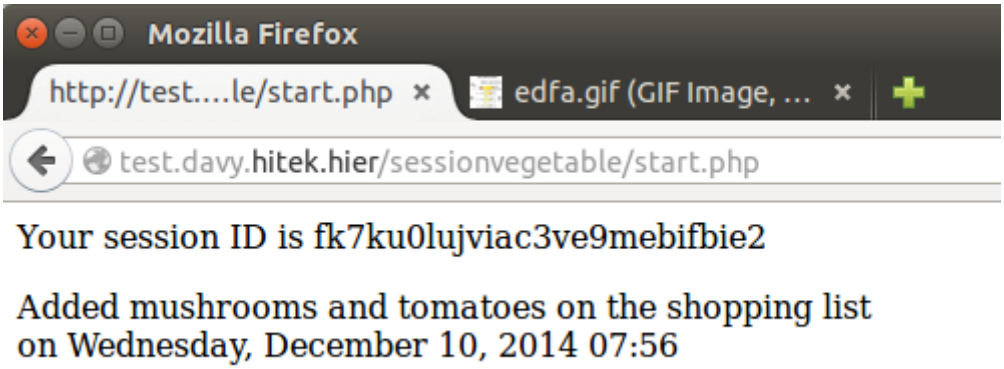
In deze oefening maak ik gebruik van sessies om data te op te slaan. Deze data is beschikbaar voor verschillende pagina's, zolang de sessie niet gesloten wordt.

Het eerste script maakt de sessie aan, en slaat de data op.

davy@davyubuntu14: /var/www/html/sessionvegetable

davy@davyubuntu14: /var/www/html/sessionvegetable 80x24

```
<html>
<body>
<?php
session_start();
$_SESSION["vegetable1"] = "mushrooms";
$_SESSION["vegetable2"] = "tomatoes";
echo "<p>Your session ID is ".session_id()."</p>";
echo "Added mushrooms and tomatoes on the shopping list ";
echo "<br>";
echo "on ".date("l, F d, Y h:i",time());
?>
</body>
</html>
~
~
~
~
~
~
~
~
~
~
"start.php" [dos] 13L, 310C                                   1,1           All
```

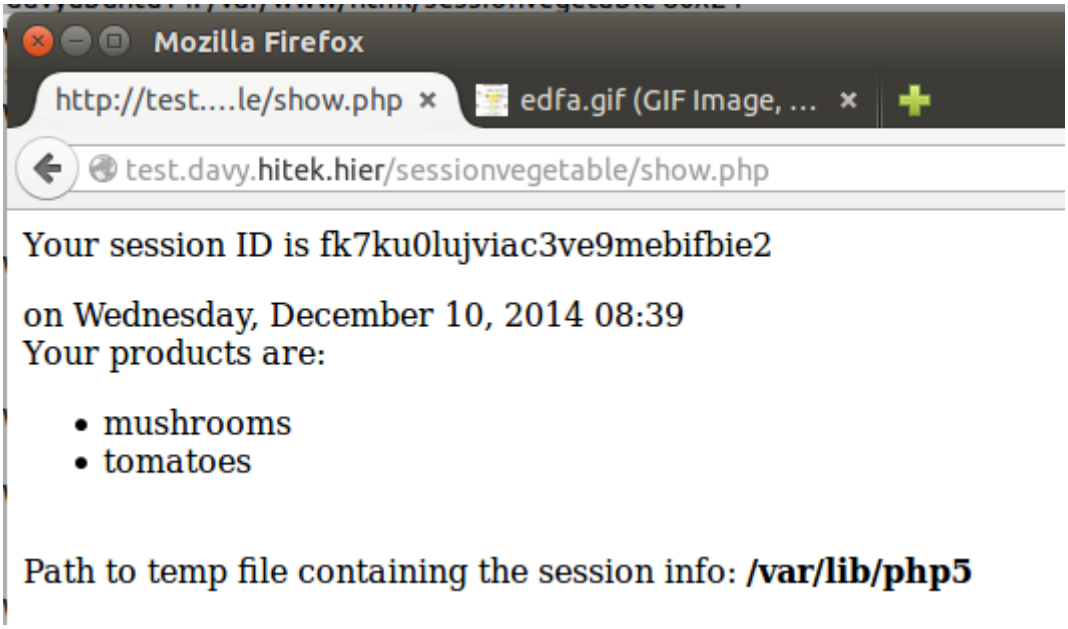


Nu laat ik zien hoe je de opgeslagen data kunt tonen:

davy@davyubuntu14: /var/www/html/sessionvegetable

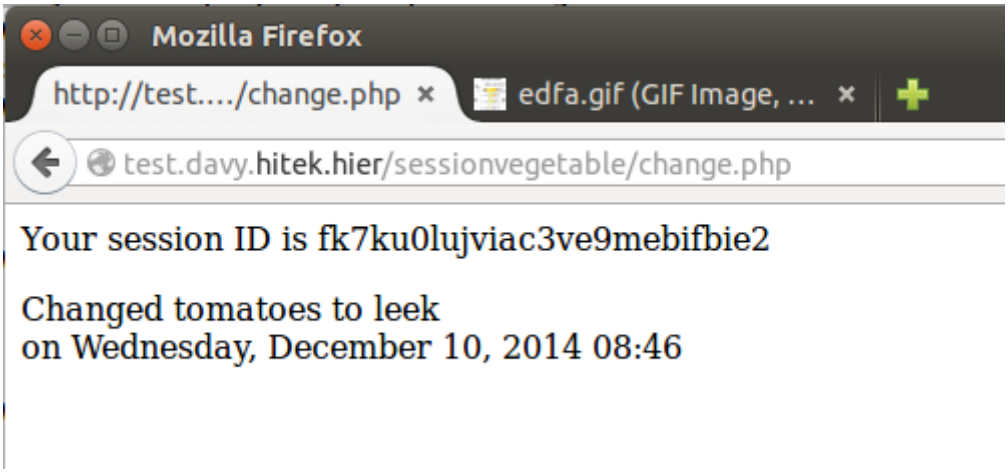
davy@davyubuntu14: /var/www/html/sessionvegetable 80x24

```
<html>
<body>
<?php
session_start();
echo "<p>Your session ID is " .session_id() . "</p>";
echo "on ".date("l, F d, Y h:i", time());
echo "<br>";
echo "Your products are: ";
echo "<ul><li>$_SESSION[vegetable1]</li><li>$_SESSION[vegetable2]</li></ul>";
echo "<br>";
echo "Path to temp file containing the session info: ";
echo "<b>".session_save_path()."</b>";
?>
</body>
</html>
~
~
~
~
~
~
~
~
"show.php" [dos] 15L, 394C                                    1,1           All
```



Men kan de data ook gaan wijzigen:

```
davy@davyubuntu14: /var/www/html/sessionvegetable
davy@davyubuntu14: /var/www/html/sessionvegetable 80x24
<html>
<body>
<?php
session_start();
$_SESSION['vegetable2'] = "leek";
echo "<p>Your session ID is ".session_id()."</p>";
echo "Changed tomatoes to leek";
echo "<br>";
echo "on ".date("l, F d, Y h:i", time());
?>
</body>
</html>
~
~
~
~
~
~
~
~
~
~
~
"change.php" [dos] 12L, 241C                                  1,1           All
```

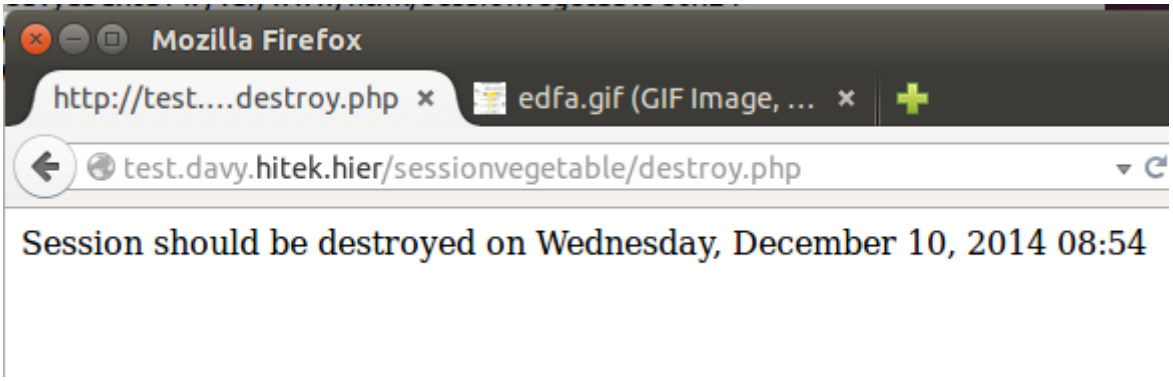


Als laatste sluiten we de sessie, en verwijderen we de data:

davy@davyubuntu14: /var/www/html/sessionvegetable

davy@davyubuntu14: /var/www/html/sessionvegetable 80x24

```
<html>
<body>
<?php
session_start();
unset($_SESSION["vegetable1"]);
unset($_SESSION["vegetable2"]);
echo $_SESSION["vegetable1"];
echo $_SESSION["vegetable2"];
session_destroy();
echo "Session should be destroyed ";
echo "on ".date("l, F d, Y h:i", time());
?>
</body>
</html>
~
~
~
~
~
~
~
~
~
"destroy.php" [dos] 14L, 292C                                  1,1           All
```



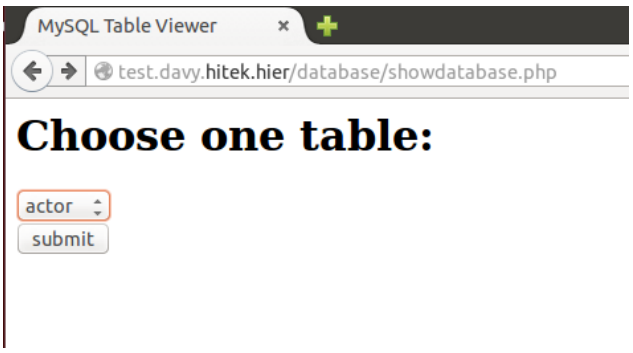
In het eerste script connecteer ik met de database en vraag ik alle tabellen op, zodat ik er één van kan kiezen. In het tweede script vraag ik de records op van deze tabel. Ik ga er van uit dat iedere tabel uit 3 kolommen bestaat.

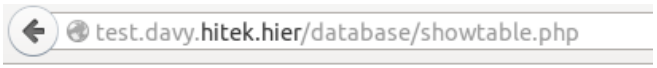
davy@davyubuntu14: /var/www/html/database

davy@davyubuntu14: /var/www/html/database 72x35

```
<html>
<head>
<title>MySQL Table Viewer</title>
</head>
<body>
<?php
$dbhost = 'localhost';
$dbuser = 'dennis';
$dbpass = 'menace';
$dbname = 'movies';
$table = 'movie';

/* connect to the db */
$connection = mysqli_connect($dbhost,$dbuser,$dbpass,$dbname);

/* show tables */
$sql="SHOW TABLES";
echo "<h1>Choose one table:</h1>";
echo "<form action=\"showtable.php\" method=\"POST\">";
echo "<select name=\"table\" size=\"1\" Font size=\"+2\">";
if ($result=mysqli_query($connection,$sql)){
        while ($row=mysqli_fetch_row($result)){
                echo "<option value=\"table\" >$row[0]</option>";
        }
        mysqli_free_result($result);
}
echo "</select>";
echo "<div><input type=\"submit\" value=\"submit\"></div>";
echo "</form>";


?>
</body>
</html>
                                                        1,1           All
```

```
davy@davyubuntu14: /var/www/html/database
davy@davyubuntu14: /var/www/html/database 73x30
<html><head>
<title>MySQL Table Viewer</title>
</head>
<body>
<?php
$dbhost = 'localhost';
$dbuser = 'dennis';
$dbpass = 'menace';
$dbname = 'movies';
$table = $_POST['table'];

$connection = mysqli_connect($dbhost,$dbuser,$dbpass,$dbname);
$sql="SELECT * FROM $table";


echo "<table border=\"1\">";
if ($result=mysqli_query($connection,$sql)){
        while ($row=mysqli_fetch_row($result)){
                echo "<tr>";
                echo "<td>".$row[0].'</td>';
                echo "<td>".$row[1].'</td>';
                echo "<td>".$row[2].'</td>';
                echo "</tr>";
        }
        mysqli_free_result($result);
}
echo "</table>";
?>
</body></html>
                                                                1,1           All
```





1	The Great Race	1965
2	Frankenstein	1935
3	Appolo 13	1995
4	The 12 Commands	1957
5	North by NorthWest	1964
6	Star Wars	1977

Cookie-based login-formulier

In deze oefening maak ik een formulier om op een website in te loggen. De gebruikersinfo sla ik op in een mySQL database.

Eerst begin ik met de startpagina:

login.html

```
<html>
<head>
<title>User Login Form</title>
</head>
<body>
<H1>Login Form</H1>
<FORM METHOD="POST" ACTION="userlogin.php">
<P><STRONG>Username:</STRONG><BR>
<INPUT TYPE="text" NAME="username"></p>
<P><STRONG>Password:</STRONG><BR>
<INPUT TYPE="password" NAME="password"></p>
<P><INPUT TYPE="SUBMIT" NAME="submit" VALUE="Login"></P>
</FORM>
</body>
</html>
```

Daarna komt “userlogin.php”:

userlogin.php

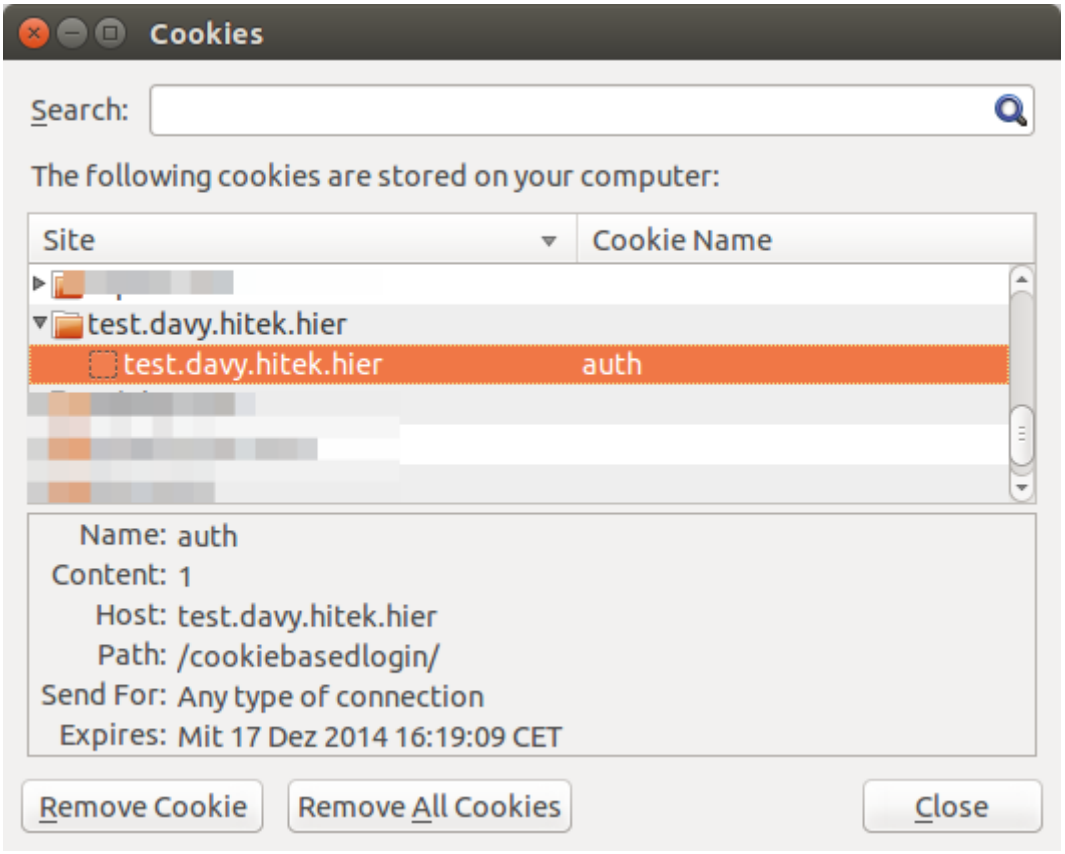
```
<?php
//check for required fields from the form
if (!isset($_POST['username']) || !isset($_POST['password'])) {
  header("Location: login.html");
  exit;
}

$dbhost = 'localhost';
$dbuser = 'dennis';
$dbpass = 'menace';
$dbname = 'apache';

$display_block = '';
/*bovenstaande was niet persé nodig, dit om error message "unset/undefined
variables"
te voorkomen*/

$connection = mysqli_connect($dbhost,$dbuser,$dbpass,$dbname);

$lguser = mysqli_real_escape_string ( $connection, $_POST['username']);
$lgpassword = mysqli_real_escape_string ( $connection, $_POST['password']);
/*mysqli_real_escape_string is om sql injectie te verhinderen*/

$sql="select `f_name`, `l_name` from `auth_users` where `username` = '{$lguser}'
AND `password` = password('{$lgpassword}')";
```

```
if ($result=mysqli_query($connection,$sql)){
  if (mysqli_num_rows($result) == 1){
    while ($row=mysqli_fetch_array($result)){
      /* eerst gebruikte ik hierboven fetch_row in plaats van fetch_array,
         waardoor mijn script niet werkte*/
         $f_name = $row['f_name'];
      $l_name = $row['l_name'];
      setcookie("auth","1", time()+60);
      $display_block = "<P>$f_name $l_name is authorized!</p>
        <P>Authorized Users' Menu:
        <ul>
          <li><a href=\"secretpage.php\">secret page</a>
        </ul>";
    }
  } else {
    header("Location: login.html");
    exit;
  }
  mysqli_free_result($result);
 }
?>
<HTML>
<HEAD>
<TITLE>User Login</TITLE>
</HEAD>
<BODY>
<?php echo "$display_block"; ?>
</BODY>
</HTML>
```

secretpage.php

```
<?php
if ($_COOKIE[auth] == "1") {
       $display_block = "<p>You are an authorized user.</p>";
} else {
       //redirect back to login form if not authorized
       header("Location: login.html");
       exit;
}
?>
<html>
<head>
<title>Secret Page</title>
</head>
<body>
<?php echo "$display_block";
print_r($_COOKIE);
?>
</body>
</html>
```

Als we inloggen met een correcte user, kunnen we via de browser de cookie controleren.



Custom logging met behulp van Apache, PHP en mySQL

We gaan in deze oefening registreren hoeveel keer een bepaalde pagina bezocht wordt, en met welke user agent/browser. Ook het aantal page-views van onze hele website zal gelogd worden.

Eerst begin ik met “snippet.php”. Dit bestand zal via een include in iedere pagina van onze site terechtkomen:

login.html

```
<?php
$dbhost = 'localhost';
$dbuser = 'dennis';
$dbpass = 'menace';
$dbname = 'apache';

$connection = mysqli_connect($dbhost,$dbuser,$dbpass,$dbname);
$sql="insert into access_tracker values ('', '$page_title', '$user_agent',
now())";
mysqli_query($connection,$sql);
?>
```

Nu laat ik een voorbeeld zien van zo'n pagina die gebruikers kunnen bezoeken:

sample1.php

```
<?php
$page_title = "sample page A";
$user_agent = getenv("HTTP_USER_AGENT");
include 'snippet.php';
?>
<HTML>
<HEAD>
<TITLE>Sample Page A</TITLE>
</HEAD>
<BODY>
<h1>Sample Page A</h1>
<P>Blah blah blah.</p>
</BODY>
</HTML>
```

Er moet natuurlijk een methode zijn om de opgeslagen data te bekijken als beheerder. Dit gebeurt zo:

rapport.php

```
<?php
error_reporting(E_ALL);
//connect to server and select database
$dbhost = 'localhost';
$dbuser = 'dennis';
$dbpass = 'menace';
$dbname = 'apache';
$connection = mysqli_connect($dbhost,$dbuser,$dbpass,$dbname) or
die(mysqli_error());

//Count total
$count_sql = "select page_title from access_tracker where page_title IS NOT NULL
AND TRIM(page_title) <> '' ";
$count_res = mysqli_query( $connection,$count_sql) or
die(mysqli_error($connection));
$all_count = mysqli_num_rows($count_res);



//results for each user agents
$user_agent_sql = "select distinct user_agent,count(user_agent) as count from
access_tracker group by user_agent order by count desc";
$user_agent_res = mysqli_query($connection,$user_agent_sql) or
die(mysqli_error($connection));

$user_agent_block = "<ul>";
while ($row=mysqli_fetch_row($user_agent_res)){
       $user_agent = $row[0];
       $user_agent_count = $row[1];
       $user_agent_block .= "<li>$user_agent<ul><li><em>accesses per browser:
$user_agent_count</em></ul>";
}
```

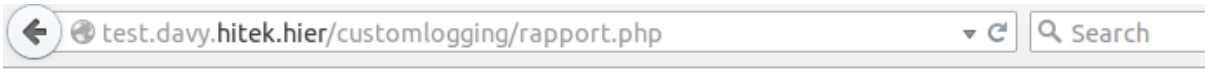
```
$user_agent_block .= "</ul>";
//results for each page
$page_title_sql = "select distinct page_title, count(page_title) as count from
access_tracker group by page_title order by count desc";
$page_title_res = mysqli_query($connection,$page_title_sql) or
die(mysqli_error("$connection"));

$page_title_block = "<ul>";
while ($row=mysqli_fetch_row($page_title_res)){
       $page_title = $row[0];
       $page_count = $row[1];
    $page_title_block .= "<li>$page_title<ul><li><em>accesses per page:
$page_count</em></ul>";
}
$page_title_block .= "</ul>";
?>
<HTML>
<HEAD>
<TITLE>Access Report</TITLE>
</HEAD>
<BODY>
<h1>Access Report</h1>
<P><strong>Total Accesses Tracked:</strong>
<?php echo "$all_count"; ?></p>
<P><strong>Web Browsers Used:</strong>
<?php print "$user_agent_block"; ?>
<P><strong>Individual Pages:</strong>
<?php print "$page_title_block"; ?>
</BODY>
</HTML>
```

In mijn code heb ik “error_reporting(E_ALL)” gebruikt, aangezien mijn script eerst niet werkte en ik de fout wou opsporen. Deze fout bleek uiteindelijk te zijn dat ik ergens nog “mysql” gebruikte in plaats van “mysqli”.

Index of /customlogging

Name	Last modified	Size	Description
Parent Directory		-	
rapport.php	2014-12-17 15:59	1.9K	
sample1.php	2014-12-17 16:07	236	
sample2.php	2014-12-17 16:11	236	
sample3.php	2014-12-17 16:12	236	
snippet.php	2014-12-15 17:11	280	

Apache/2.4.7 (Ubuntu) Server at test.davy.hitek.hier Port 80



Access Report

Total Accesses Tracked: 13

Web Browsers Used:

- Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:34.0) Gecko/20100101 Firefox/34.0
  - *accesses per browser: 13*

Individual Pages:

- sample page A
  - *accesses per page: 8*
- sample page B
  - *accesses per page: 4*
- sample page C
  - *accesses per page: 1*

Een eigen certificate authority maken

Een certificate authority is diegene die, in de cryptografie, certificaten uitdeelt. Met deze certificaten kan iemand z'n identiteit bewijzen en z'n publieke sleutel doorgeven. De certificate authority, of CA, is een soort van tussenpersoon die vertrouwd wordt door beide partijen. Er zijn commerciële CA's, gratis CA's, en bedrijven en instanties kunnen hun eigen certificate authority maken.

De mogelijkheid bestaat om, in Ubuntu, een eigen certificate authority op te zetten. Deze hebben we bvb. nodig in de Apache-oefening om een SSL-website op te zetten. Dit gebeurt via het programma "TinyCA".

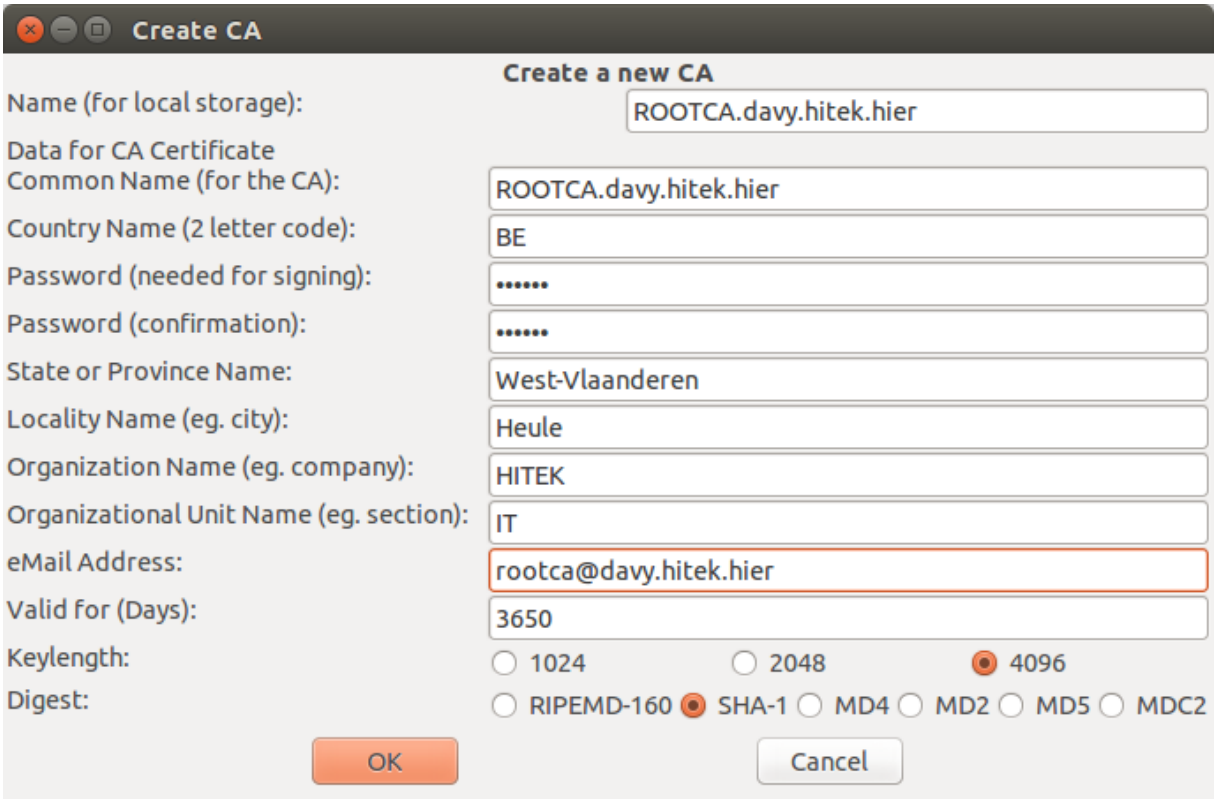
De installatie doen we met het apt-get install commando:

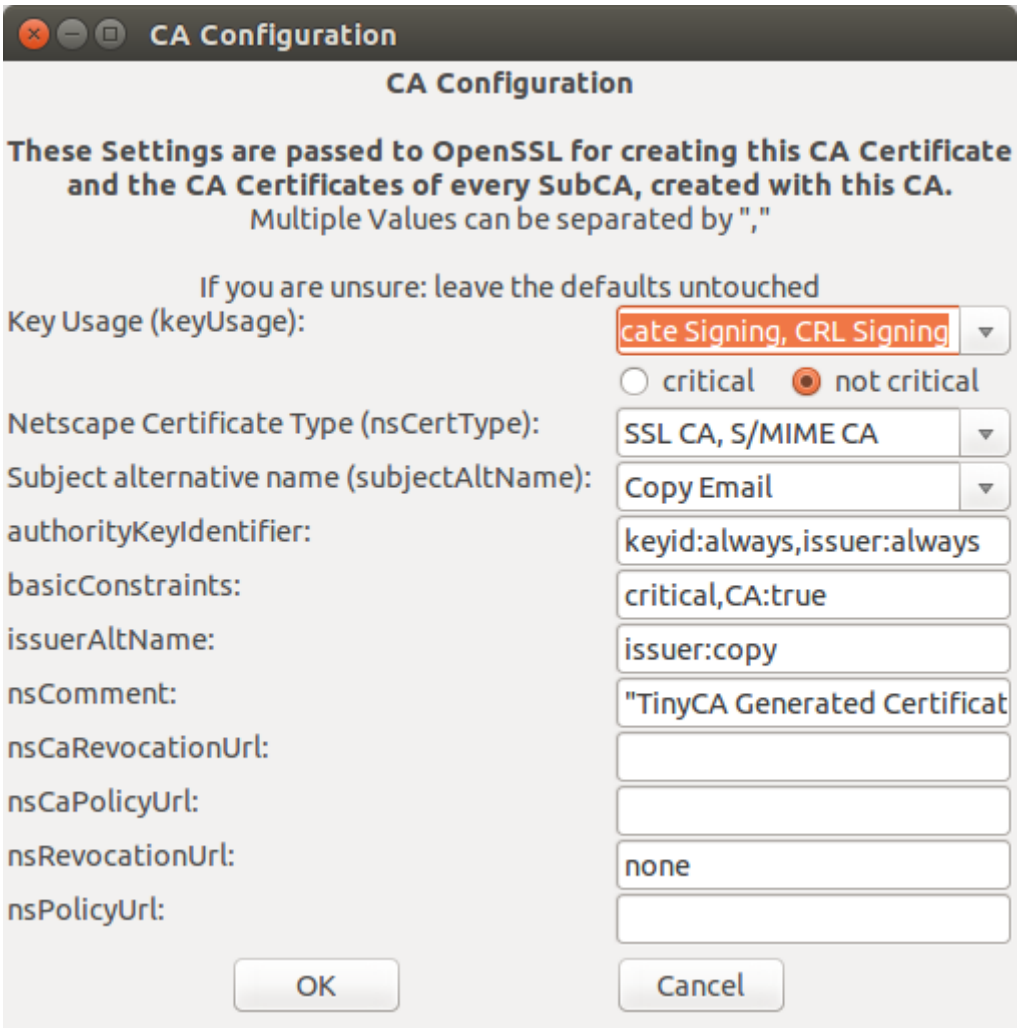
```
sudo apt-get install tinyca
```

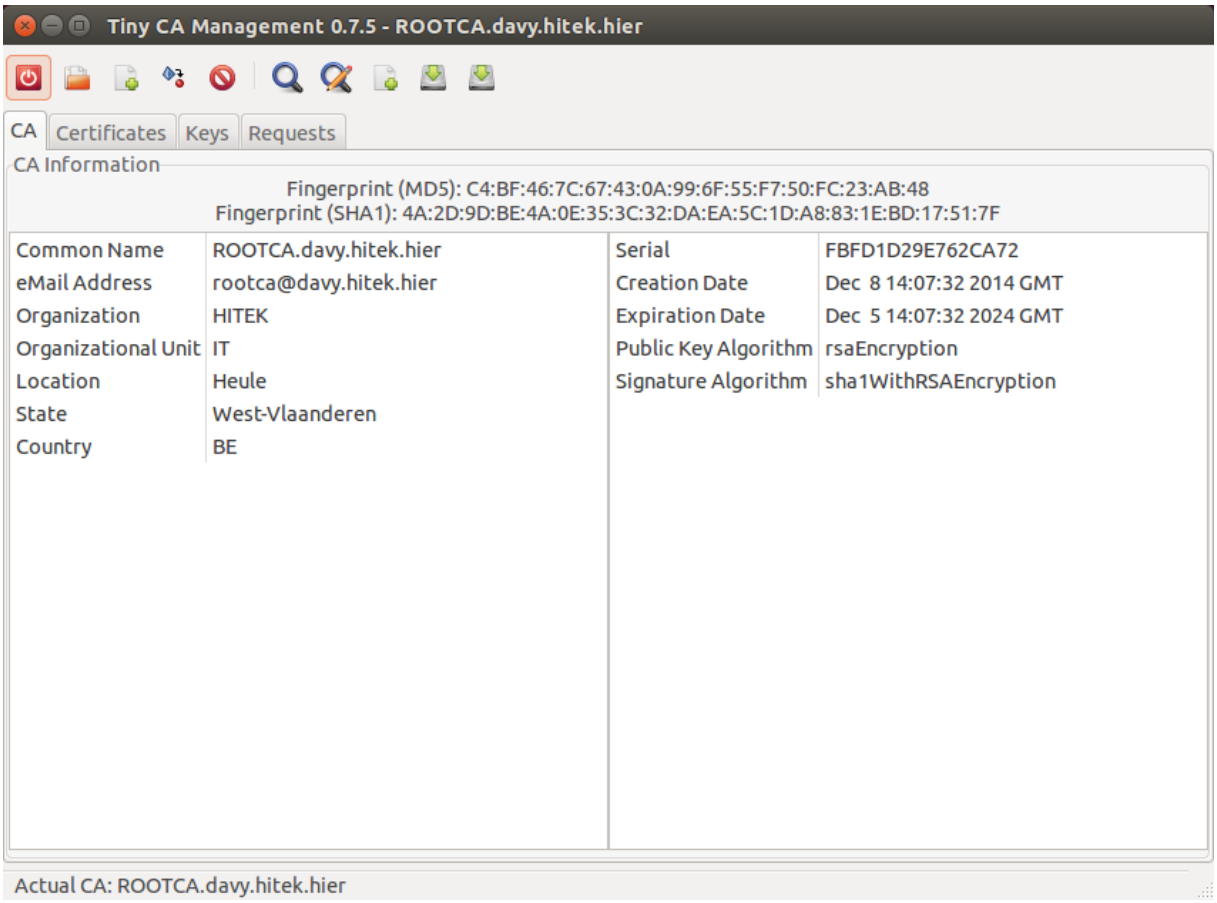
Daarna starten we het programma op met volgend commando:

```
tinyca2
```

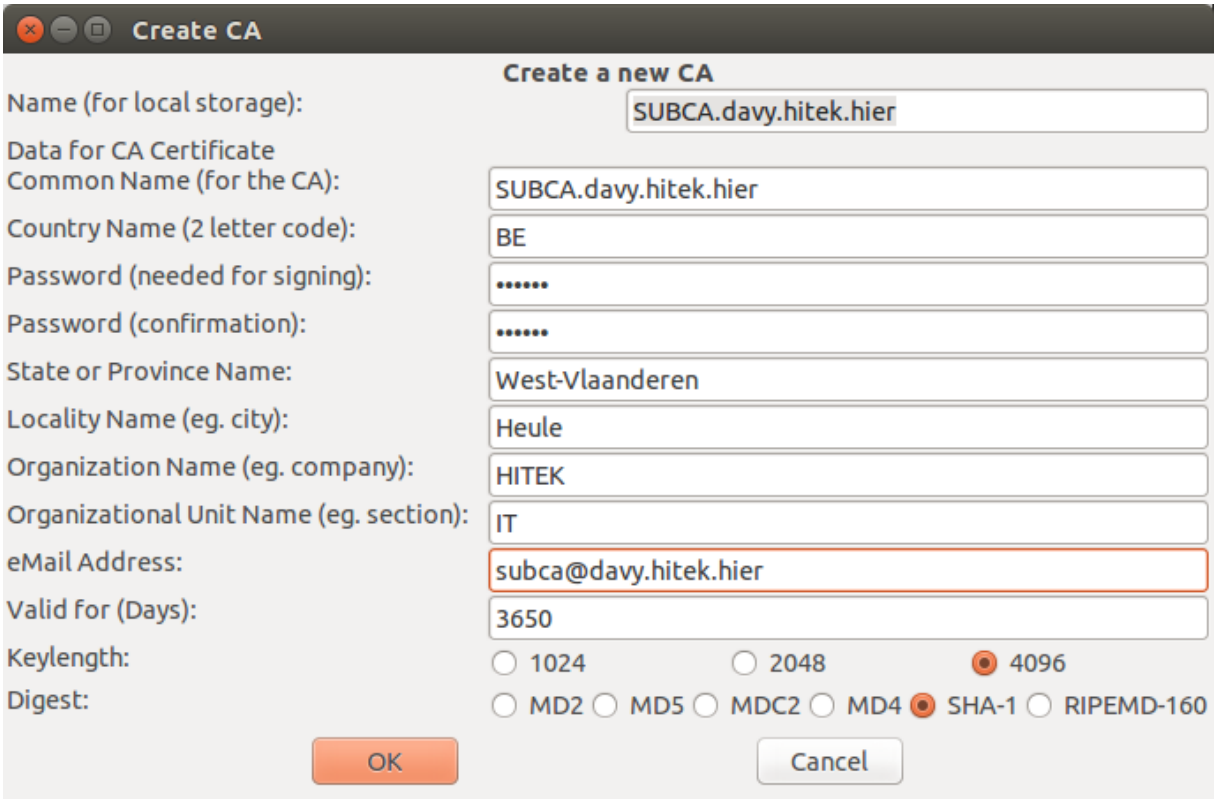
Als we TinyCA voor de eerste maal opstarten moeten we een rootCA aanmaken:



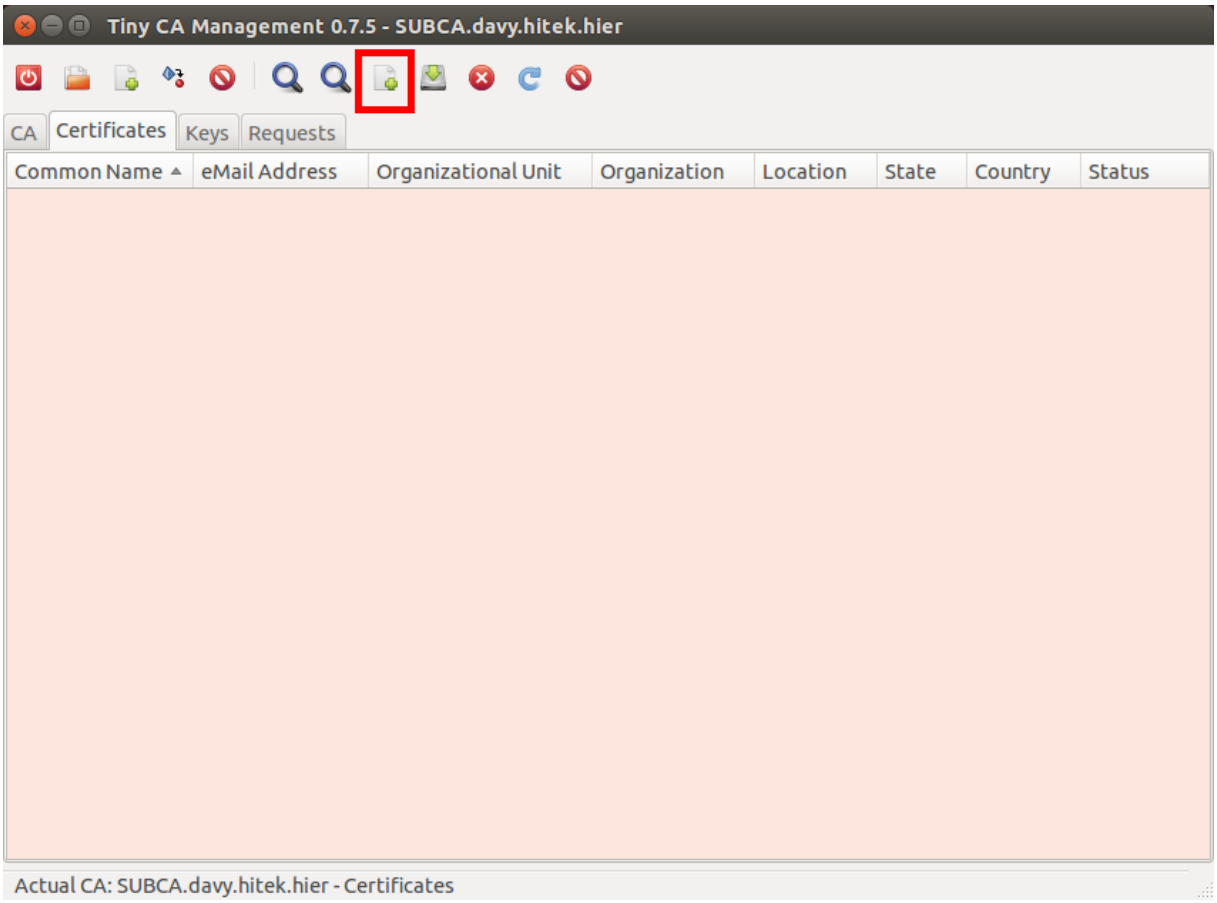

CA Configuration
CA Configuration
These Settings are passed to OpenSSL for creating this CA Certificate and the CA Certificates of every SubCA, created with this CA.
Multiple Values can be separated by ","
If you are unsure: leave the defaults untouched
Key Usage (keyUsage):
cate Signing, CRL Signing
critical
not critical
Netscape Certificate Type (nsCertType):
SSL CA, S/MIME CA
Subject alternative name (subjectAltName):
Copy Email
authorityKeyIdentifier:
keyid:always,issuer:always
basicConstraints:
critical,CA:true
issuerAltName:
issuer:copy
nsComment:
"TinyCA Generated Certificat
nsCaRevocationUrl:
nsCaPolicyUrl:
nsRevocationUrl:
none
nsPolicyUrl:
OK
Cancel

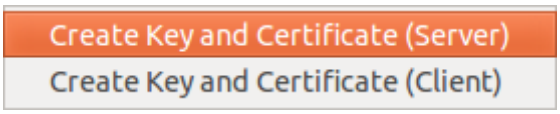


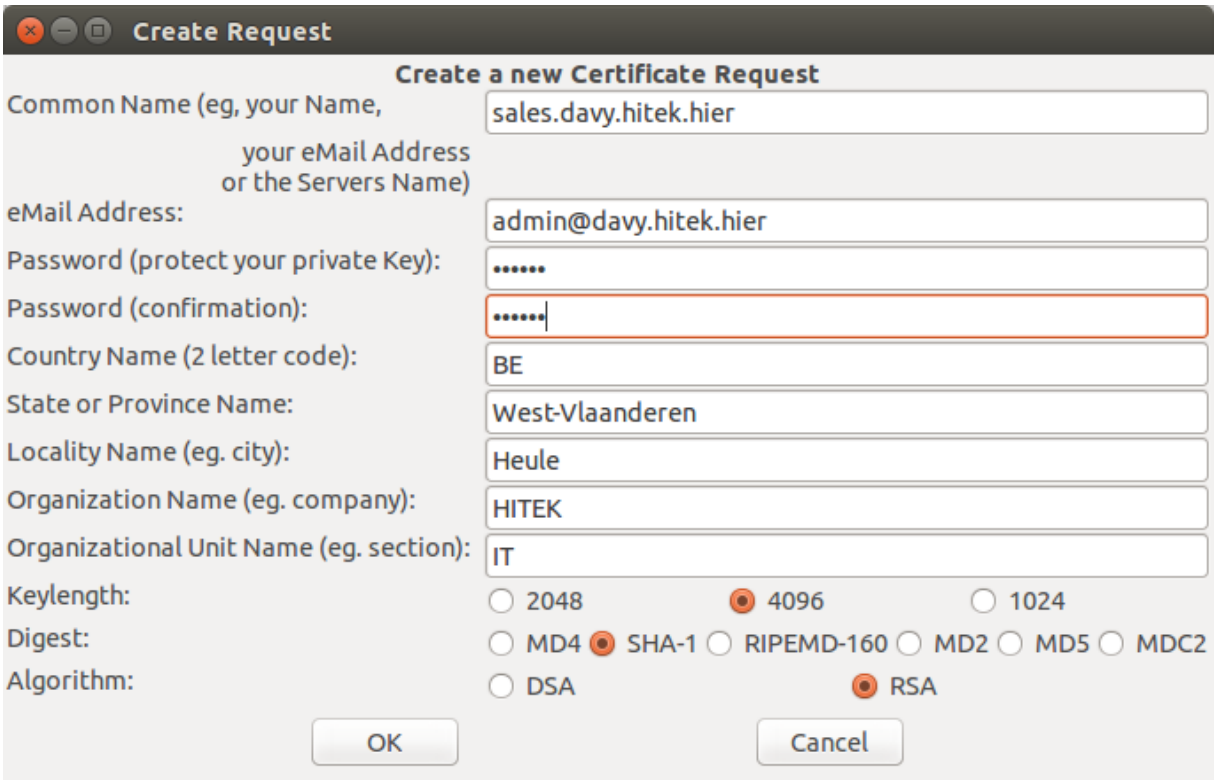
Als we dit root-certificaat aangemaakt hebben, maken we op dezelfde wijze een sub certificaat aan:



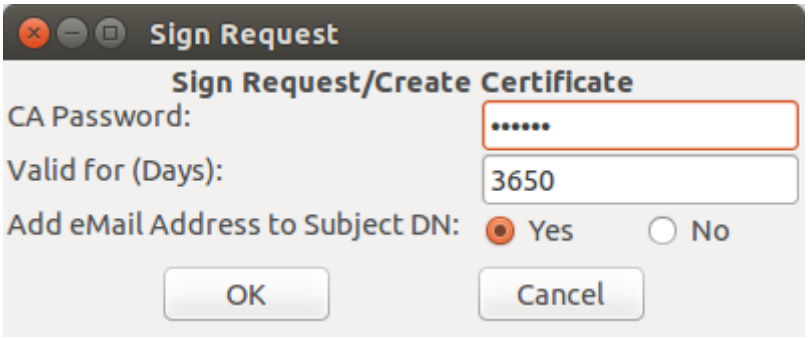
Daarna maken we een aanvraag voor het gewenste certificaat aan:



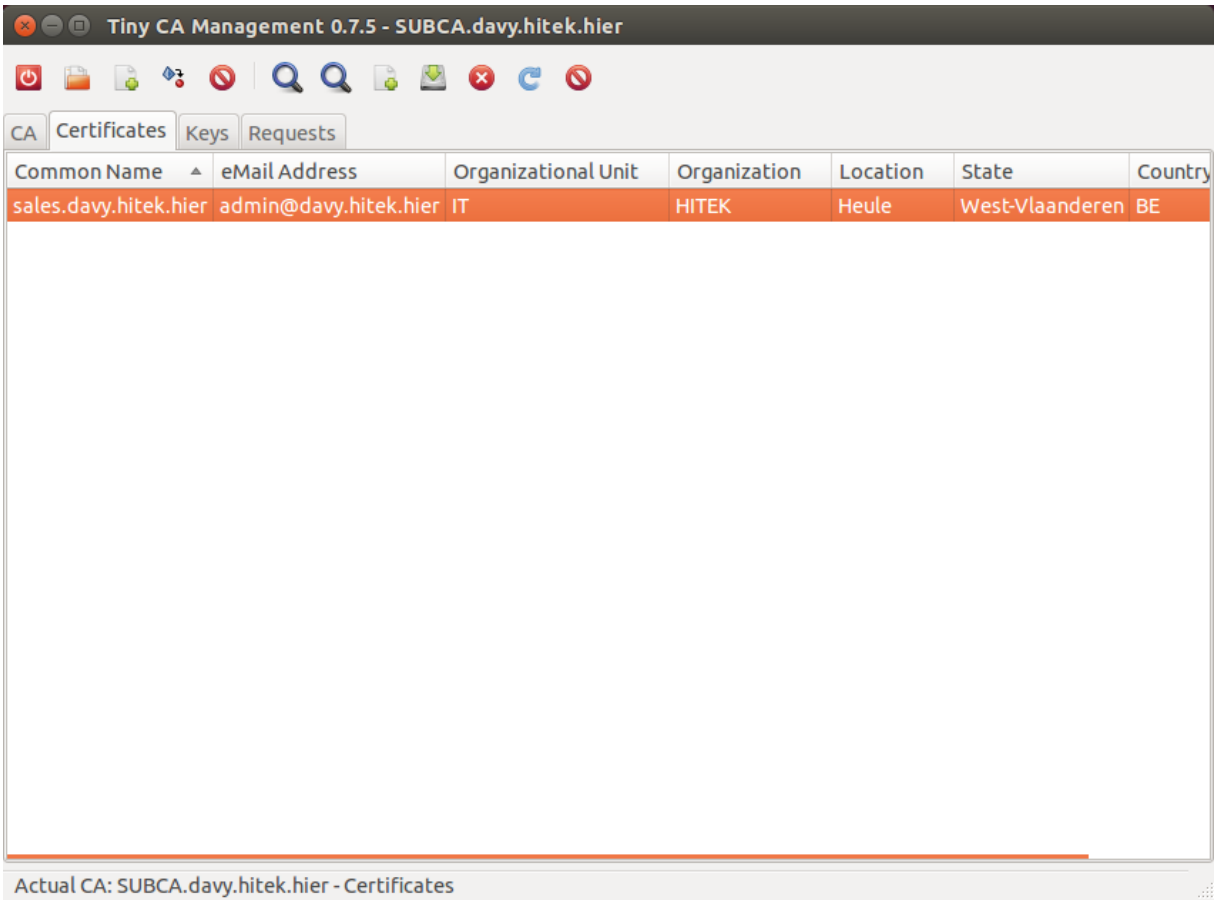


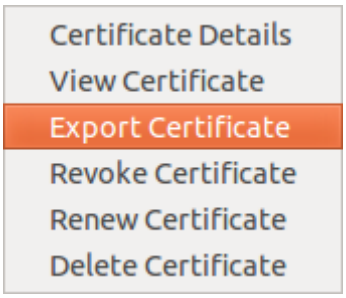


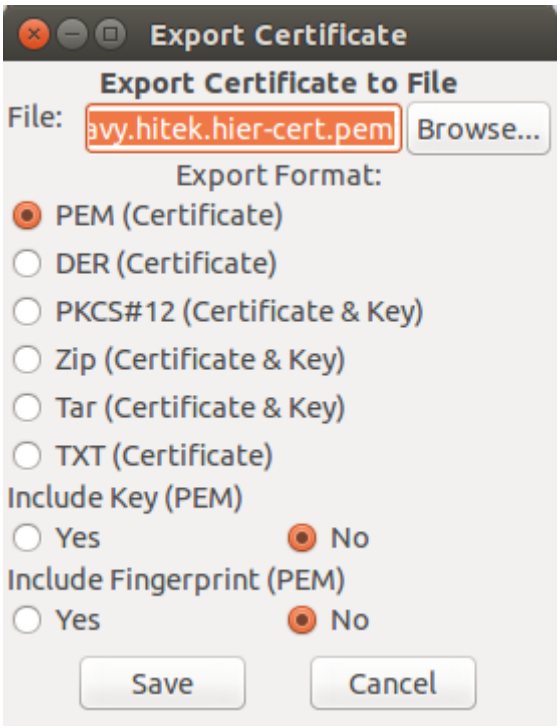
Dit zal ook getekend moeten worden:



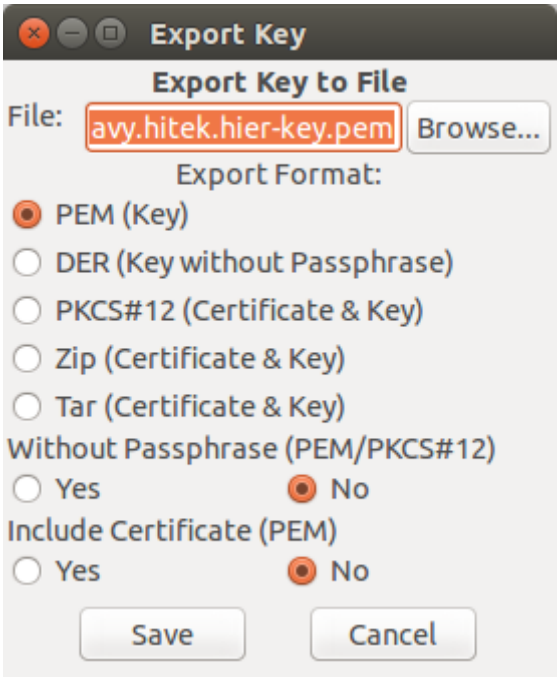
Het certificaat voor onze SSL-website is nu gemaakt. We gaan de nodige bestanden exporteren, zodat we die op de webserver kunnen plaatsen.


Tiny CA Management 0.7.5 - SUBCA.davy.hitek.hier
CA
Certificates
Keys
Requests
Common Name
eMail Address
Organizational Unit
Organization
Location
State
Country
sales.davy.hitek.hier
admin@davy.hitek.hier
IT
HITEK
Heule
West-Vlaanderen
BE
Actual CA: SUBCA.davy.hitek.hier - Certificates


Certificate Details
View Certificate
Export Certificate
Revoke Certificate
Renew Certificate
Delete Certificate



Na het certificaat, exporteren we ook de sleutel:

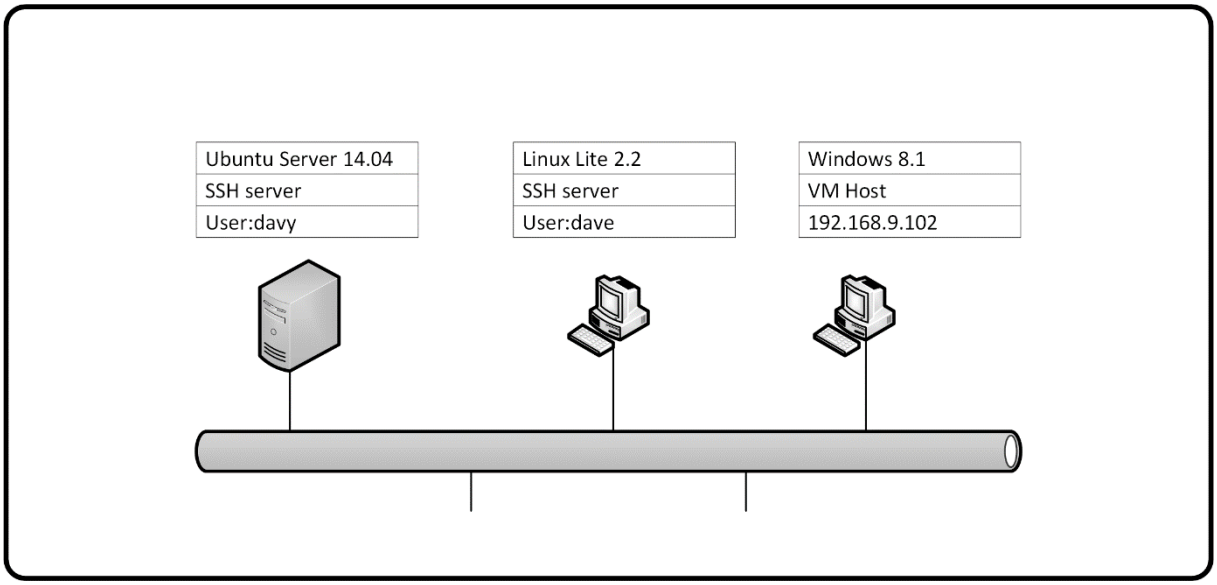


SSH & Unison

In deze oefening maken we kennis met verschillende mogelijkheden van OpenSSH, om als laatste een grove versie van een back-up systeem te maken met behulp van Unison.

Omgeving

De omgeving bestaat uit drie machines: één Windows 8.1 machine, één Ubuntu 14.04 Server en één Litelinux cliënt. Op deze laatste twee zal er een OpenSSH server draaien.

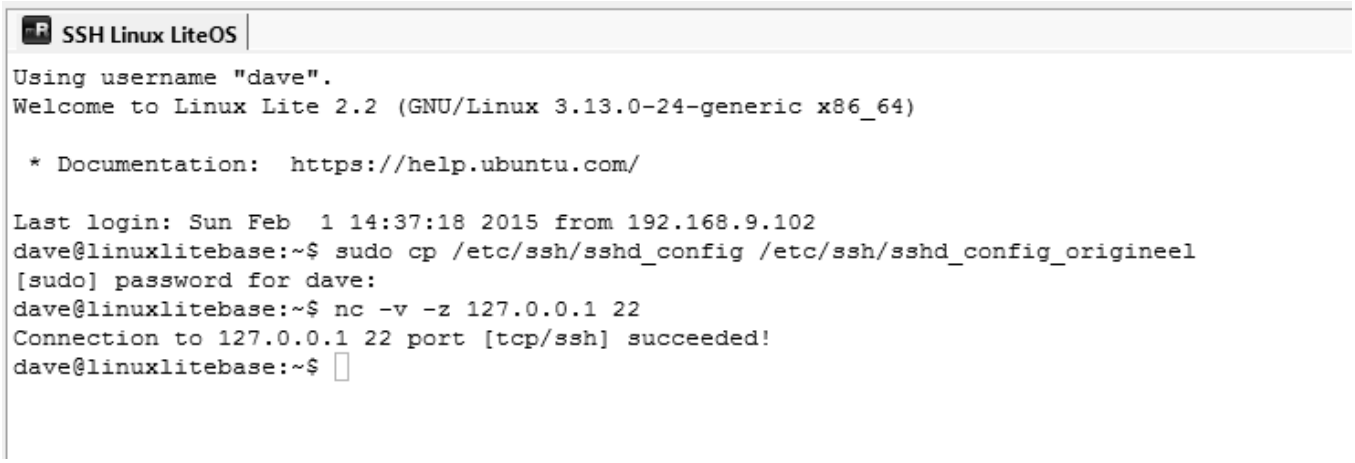


Installatie OpenSSH

Om op de Ubuntu server of de Litelinux cliënt een OpenSSH server te installeren, gebruikt men het volgende commando:

```
Apt-get install openssh-server
```

Om daarna te controleren of de server draait, zijn er verschillende methodes. Met het programma netcat kan men bijvoorbeeld een verbinding proberen te maken. De parameter –v zorgt voor een duidelijkere output, de parameter –z zorgt ervoor dat netcat scant naar draaiende daemons zonder data te versturen naar deze daemons.



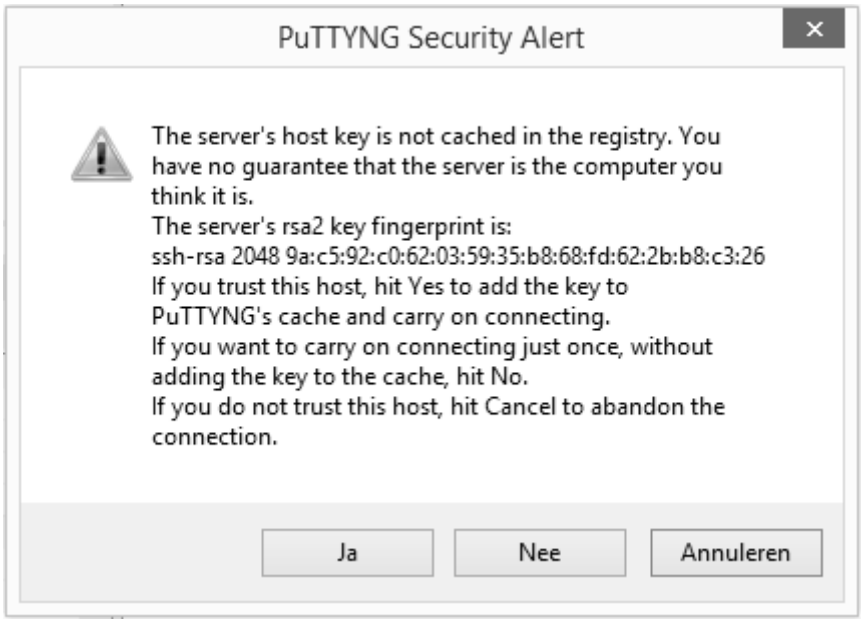
Een tweede mogelijkheid is gaan kijken met het commando netstat welke verbindingen er zijn op poort 22. Dit is de standaardpoort voor SSH.

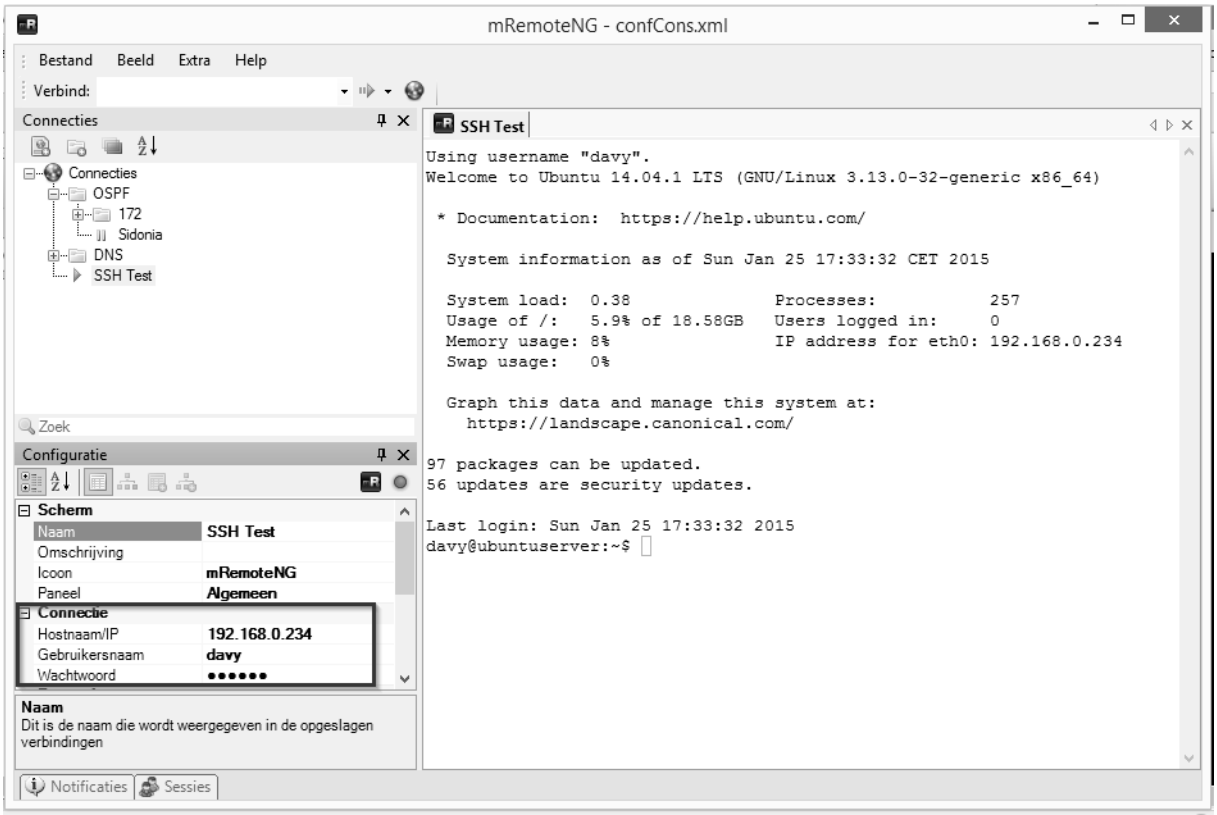
```
davy@ubuntuserver:~$ netstat -antp | grep ":22"
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.0.234:22        192.168.0.206:62791     ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -

davy@ubuntuserver:~$
```

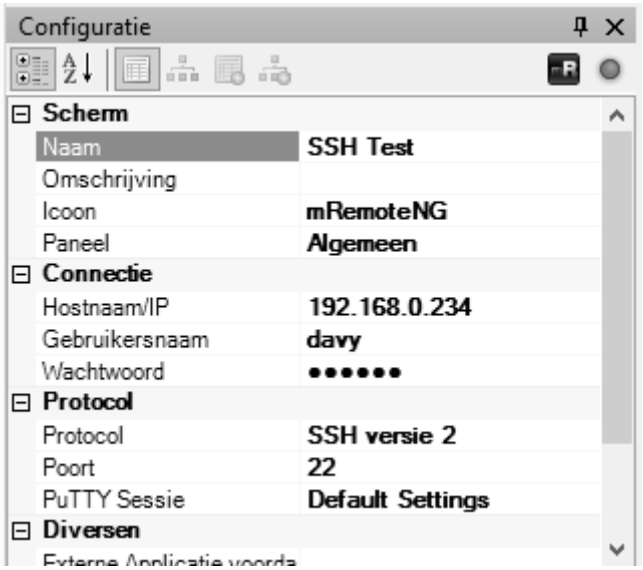
Best practice: ik raad aan om een kopie te nemen van het configuratiebestand (sshd_config) vooraleer men wijzigingen aan de configuratie toebrengt.

Test connectie met mRemoteNG

In de volgende screenshots log ik van de Windows 8.1-machine in op één van de twee SSH-servers. Als ik de eerste maal inlog op de server krijg ik de vraag of ik de SSH-server vertrouw. Aangezien het gaat om onze server, vertrouw ik hem.


PuTTYNG Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 9a:c5:92:c0:62:03:59:35:b8:68:fd:62:2b:b8:c3:26
If you trust this host, hit Yes to add the key to PuTTYNG's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Ja
Nee
Annuleren


mRemoteNG - confCons.xml
Bestand
Beeld
Extra
Help
Verbind:
Connecties
Connecties
OSPF
172
Sidonia
DNS
SSH Test
Zoek
Configuratie
Scherm
Naam
SSH Test
Omschrijving
Icoon
mRemoteNG
Paneel
Algemeen
Connectie
Hostnaam/IP
192.168.0.234
Gebruikersnaam
davy
Wachtwoord
Naam
Dit is de naam die wordt weergegeven in de opgeslagen verbindingen
Notificaties
Sessies
SSH Test
Using username "davy".
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)
* Documentation: https://help.ubuntu.com/
System information as of Sun Jan 25 17:33:32 CET 2015
System load: 0.38
Usage of /: 5.9% of 18.58GB
Memory usage: 8%
Swap usage: 0%
Processes: 257
Users logged in: 0
IP address for eth0: 192.168.0.234
Graph this data and manage this system at:
https://landscape.canonical.com/
97 packages can be updated.
56 updates are security updates.
Last login: Sun Jan 25 17:33:32 2015
davy@ubuntuserver:~$



Zoals je ziet moet ik bij de instellingen van mRemoteNG de gebruikersnaam en het paswoord instellen.

Paswoordloos inloggen

Om zonder paswoord connecties te kunnen maken, moeten we per server een sleutelpaar aanmaken, een publieke en een private sleutel. De publieke sleutel kopiëren we dan naar de tweede machine.

De sleutels aanmaken doen we met het commando:

```
ssh-keygen –t rsa
```

Vervolgens moeten we enkele gegevens meegeven. We gebruiken geen passphrase, en de sleutel moet in de voorgestelde map opgeslaan worden (meestal **~/.ssh/id_rsa**)

```
davy@ubuntuserver:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/davy/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/davy/.ssh/id_rsa.
Your public key has been saved in /home/davy/.ssh/id_rsa.pub.
The key fingerprint is:
60:c9:b0:d6:8c:66:29:e1:a5:11:67:87:53:08:11:f5 davy@ubuntuserver
The key's randomart image is:
+--[ RSA 2048]----+
|  B**+o          |
| . B+@ .         |
|  + B.E          |
|   = . .         |
|        S        |
|                 |
|                 |
|                 |
|                 |
+-----------------+
```

Daarna maken we op de andere machine een verborgen directory aan. Hierin zullen we de gegenereerde sleutel plaatsen.

```
davy@ubuntuserver:~$ ssh dave@192.168.9.106 mkdir -p .ssh
The authenticity of host '192.168.9.106 (192.168.9.106)' can't be established.
ECDSA key fingerprint is 6a:0b:01:09:14:0e:da:45:98:ae:e4:aa:6f:67:5e:82.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.9.106' (ECDSA) to the list of known hosts.
dave@192.168.9.106's password:
davy@ubuntuserver:~$
```

Daarna kopiëren we de publieke sleutel van de eerste machine naar de tweede machine met het commando:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub 192.168.100.4
```

Nu doen we hetzelfde, maar in de omgekeerde richting (van machine 2 naar machine 1).

```
dave@linuxlitebase:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/dave/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/dave/.ssh/id_rsa.
Your public key has been saved in /home/dave/.ssh/id_rsa.pub.
The key fingerprint is:
24:a0:47:a2:7b:45:57:a6:0e:a9:ee:b9:e3:ff:d8:1e dave@linuxlitebase
The key's randomart image is:
+--[ RSA 2048]----+
|  . + ..o        |
| . = + o         |
|. . = o .        |
| . + o o         |
|. o   . S        |
| o               |
|  .   E          |
| ... o .         |
| .=+oo+          |
+-----------------+
dave@linuxlitebase:~$
```

```
dave@linuxlitebase:~$ ssh davy@192.168.9.104 mkdir -p .ssh
The authenticity of host '192.168.9.104 (192.168.9.104)' can't be established.
ECDSA key fingerprint is ab:0b:0b:dd:f7:df:be:50:1c:36:77:ef:5a:c1:e7:f2.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.9.104' (ECDSA) to the list of known hosts.
davy@192.168.9.104's password:
```

```
dave@linuxlitebase:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub davy@192.168.9.104
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that ar
e already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
 install the new keys
davy@192.168.9.104's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'davy@192.168.9.104'"
and check to make sure that only the key(s) you wanted were added.

dave@linuxlitebase:~$
```

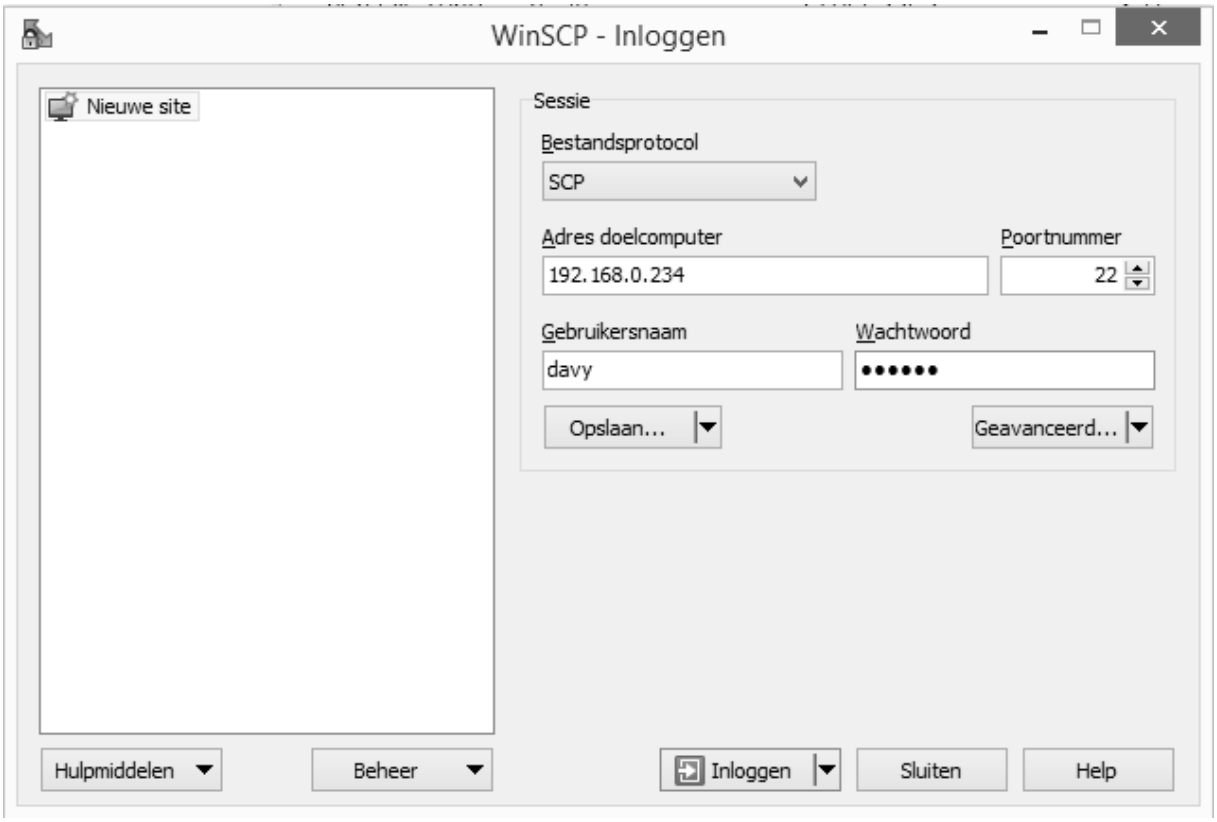
Als we dan voor de eerste maal een verbinding maken, zal er niet om het paswoord gevraagd worden.

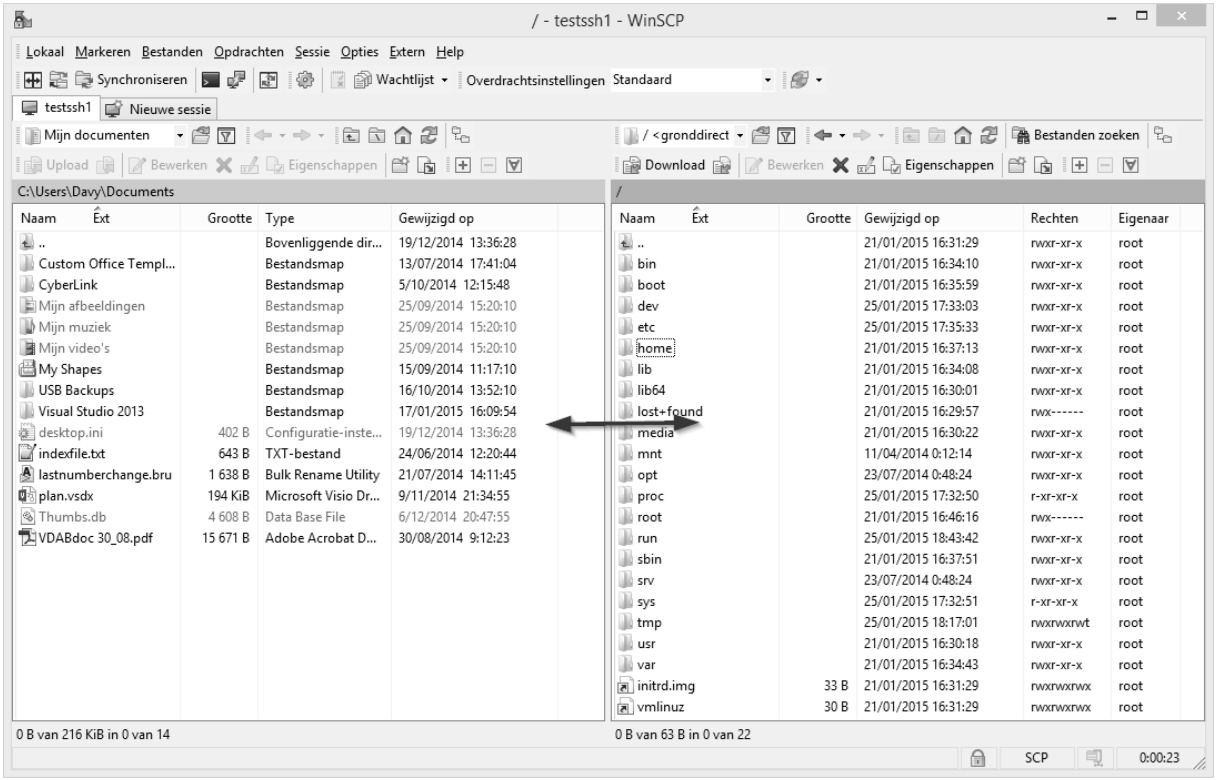
```
dave@linuxlitebase:~$ ssh davy@192.168.9.104
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sun Feb  1 16:53:07 CET 2015

  System load:  0.0               Processes:           227
  Usage of /:   6.0% of 18.58GB   Users logged in:     1
  Memory usage: 9%                IP address for eth0: 192.168.9.104
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Sun Feb  1 16:53:07 2015 from 192.168.9.106
davy@ubuntuserver:~$
```

SFTP en SCP

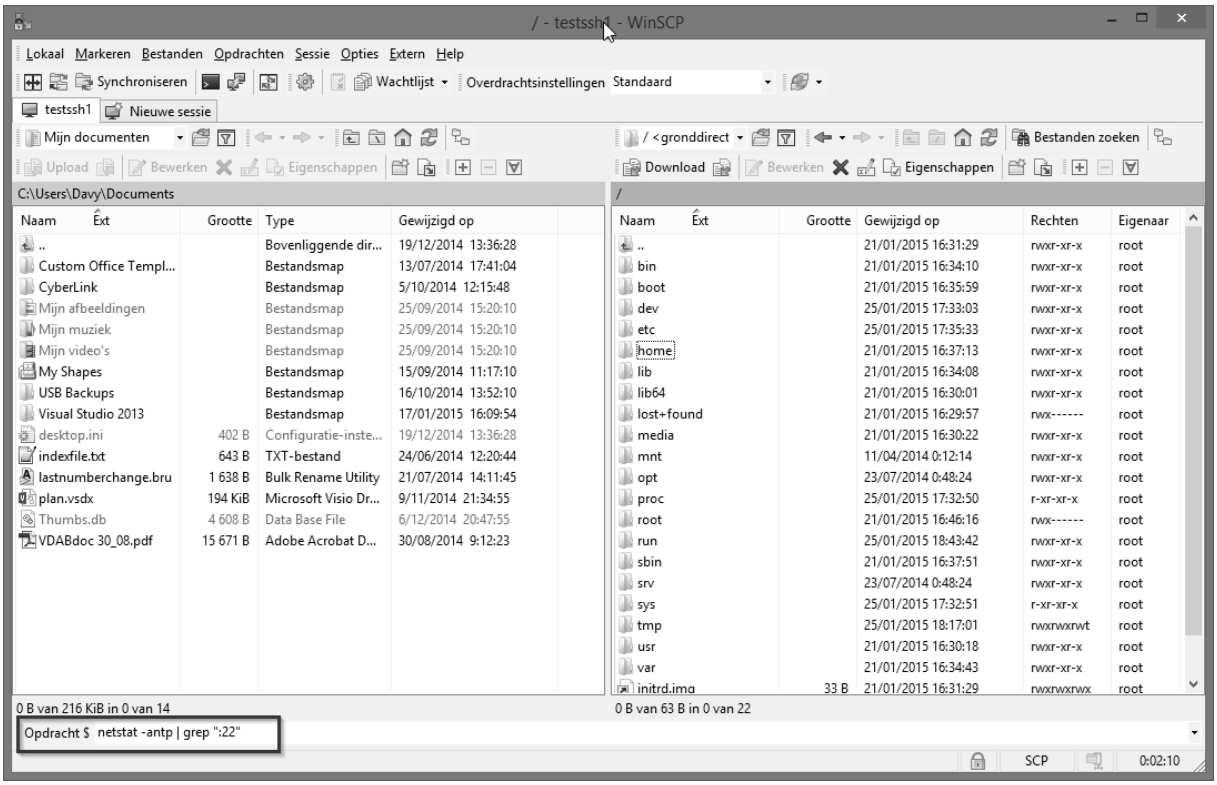
SSH biedt mogelijkheden om aan bestandsoverdracht te doen, namelijk secure copy of SCP en SFTP.

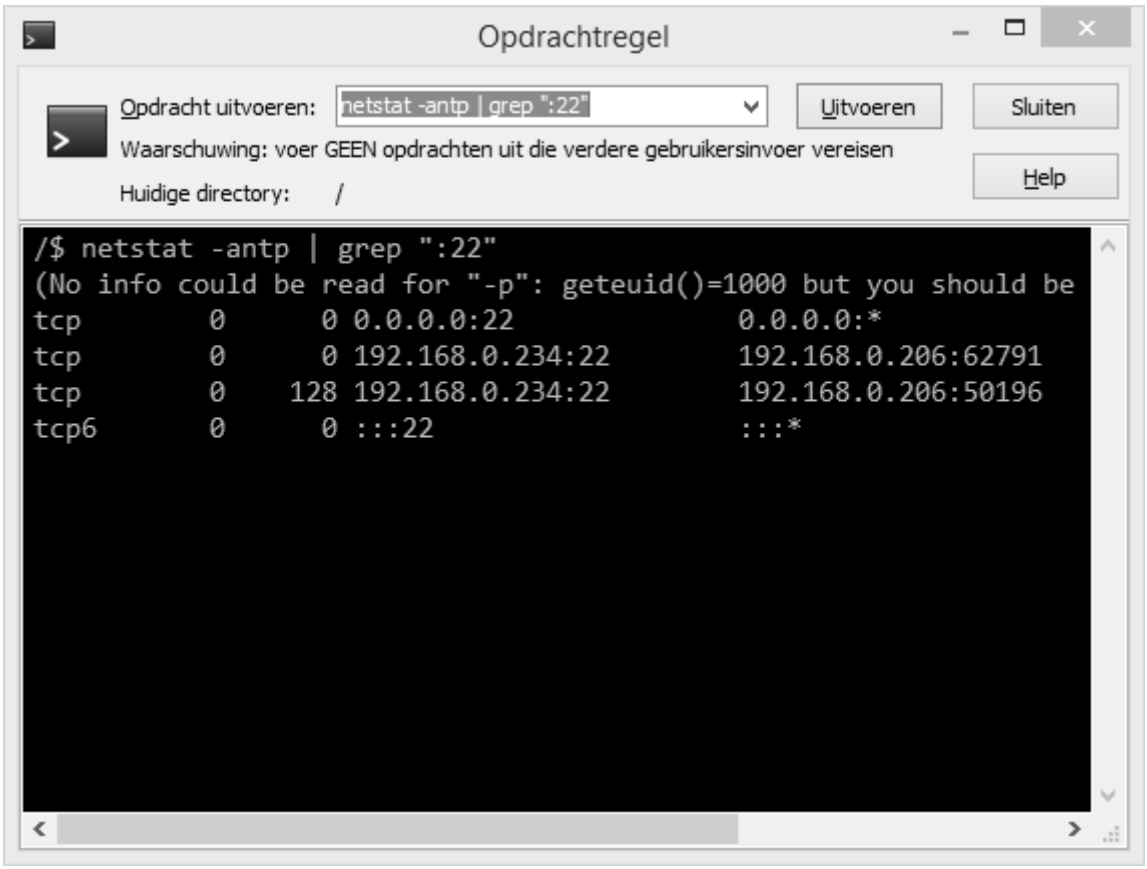
SCP test ik hier met behulp van mijn Windows-machine waar het programma WinSCP geïnstalleerd is.





Men kan ook via WinSCP commando's uitvoeren op de SSH-server

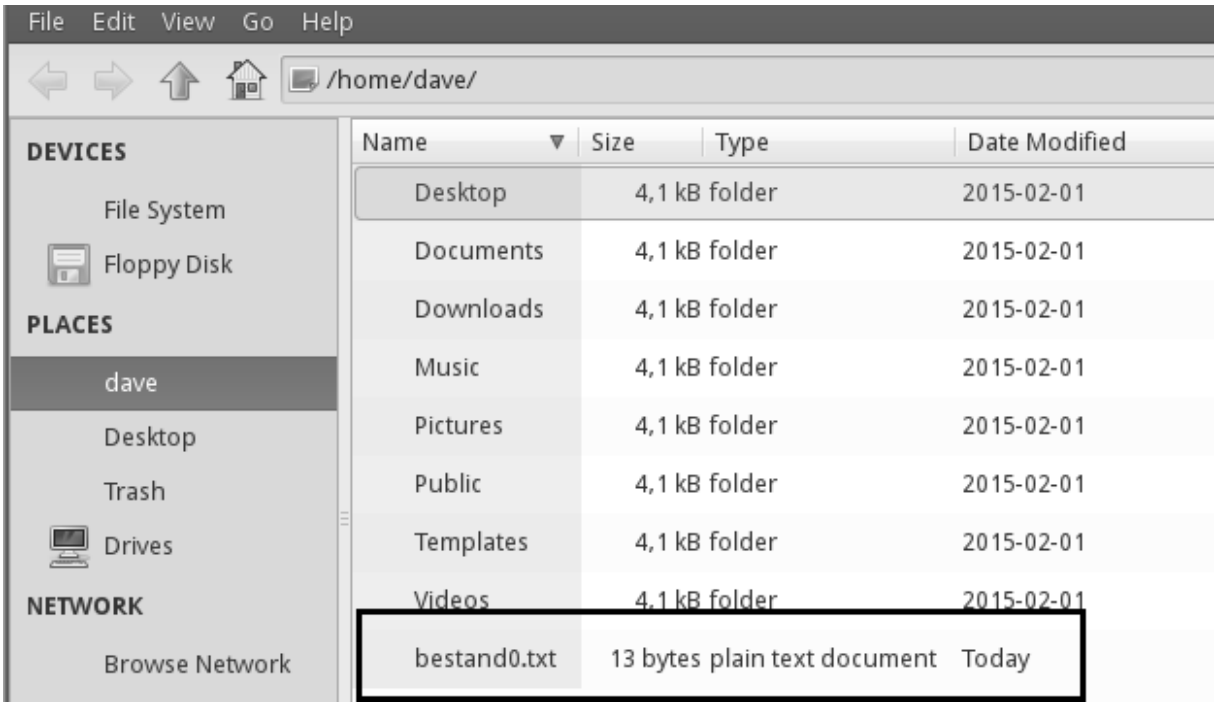




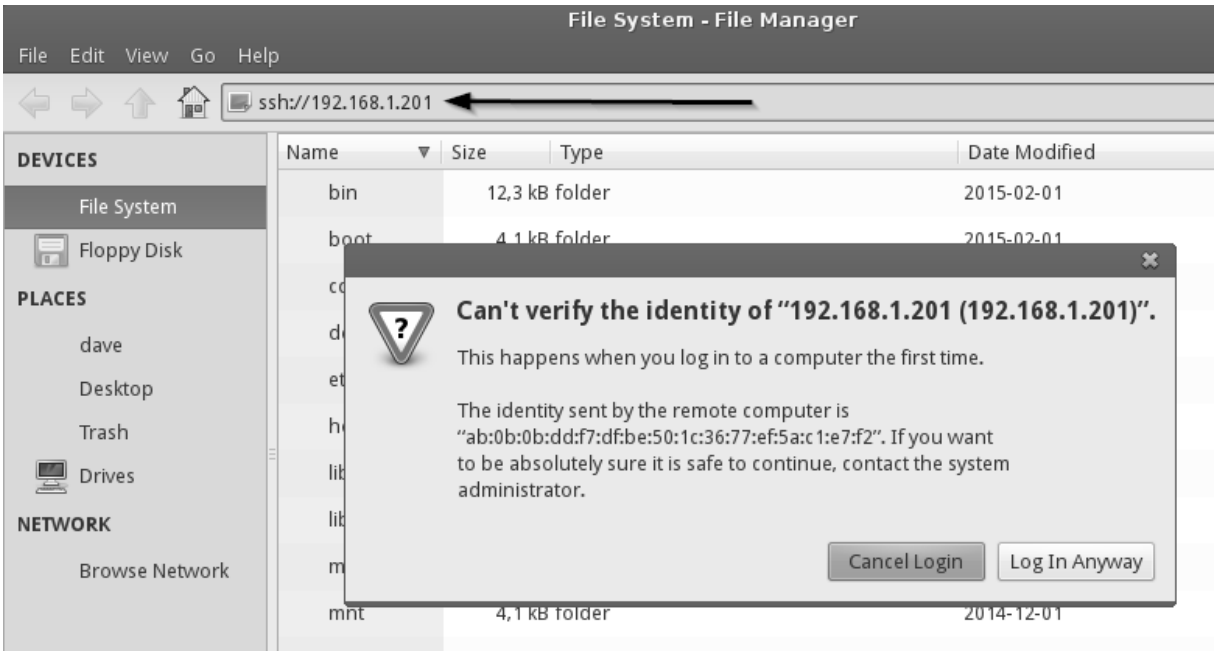
Nu ga ik SCP testen met een Linux-cliënt die onze SSH-server aanspreekt. Met het commando “scp” stuur ik bestand0.txt van de server naar de cliënt.

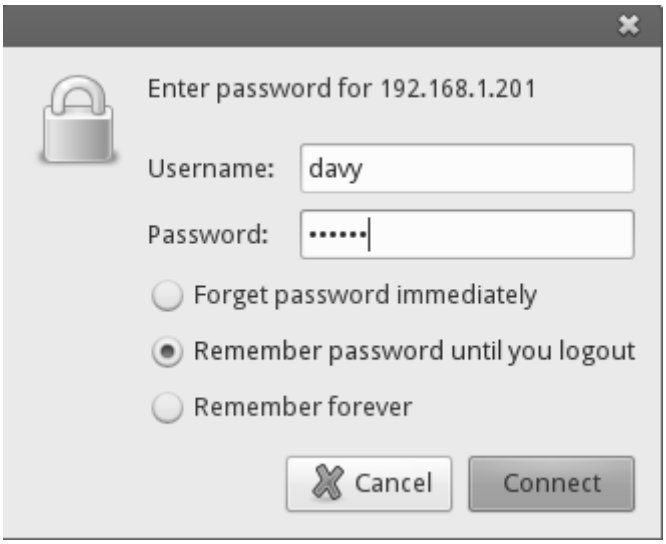
```
davy@ubuntuserver:~/mydocs$ ls
bestand0.txt  bestand1.txt  bestand2.txt  bestand3.txt  dave@192.168.1.200
davy@ubuntuserver:~/mydocs$ cat bestand0.txt
ubuntuserver
davy@ubuntuserver:~/mydocs$ scp bestand0.txt dave@192.168.1.200:~/
The authenticity of host '192.168.1.200 (192.168.1.200)' can't be established.
ECDSA key fingerprint is 6a:0b:01:09:14:0e:da:45:98:ae:e4:aa:6f:67:5e:82.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.1.200' (ECDSA) to the list of known hosts.
dave@192.168.1.200's password:
bestand0.txt                                                  100%   13     0.0KB/s   00:00
davy@ubuntuserver:~/mydocs$
```

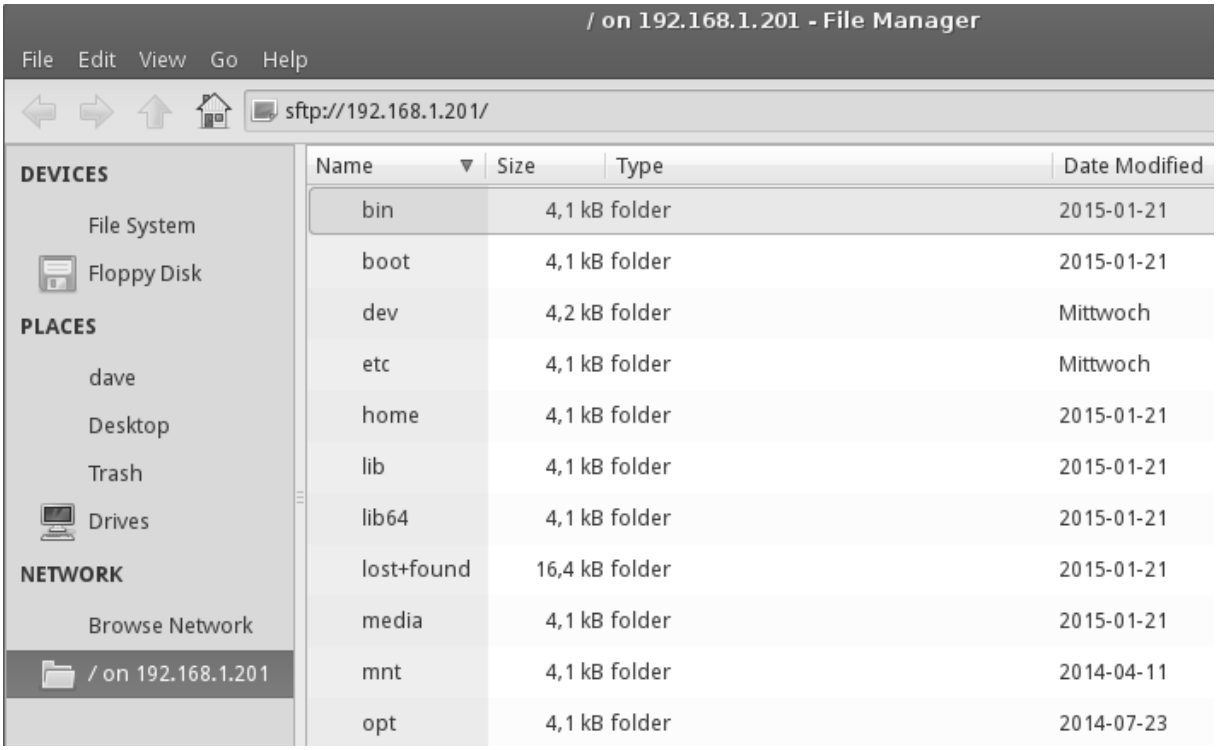
Op de cliënt zien we dan dat het bestand is gearriveerd:



Daarnaast kunnen we via SFTP ook bestanden overbrengen. Dit doet men gewoon door in de file-browser een “ssh-link” te typen. Daarna kunnen we de bestanden bekijken, alsof het een gewone map of schijf is.




Enter password for 192.168.1.201
Username:
davy
Password:
Forget password immediately
Remember password until you logout
Remember forever
Cancel
Connect


/ on 192.168.1.201 - File Manager
File Edit View Go Help
sftp://192.168.1.201/
DEVICES
File System
Floppy Disk
PLACES
dave
Desktop
Trash
Drives
NETWORK
Browse Network
/ on 192.168.1.201
Name
Size
Type
Date Modified
bin 4,1 kB folder 2015-01-21
boot 4,1 kB folder 2015-01-21
dev 4,2 kB folder Mittwoch
etc 4,1 kB folder Mittwoch
home 4,1 kB folder 2015-01-21
lib 4,1 kB folder 2015-01-21
lib64 4,1 kB folder 2015-01-21
lost+found 16,4 kB folder 2015-01-21
media 4,1 kB folder 2015-01-21
mnt 4,1 kB folder 2014-04-11
opt 4,1 kB folder 2014-07-23

SSH als SOCKS-proxy

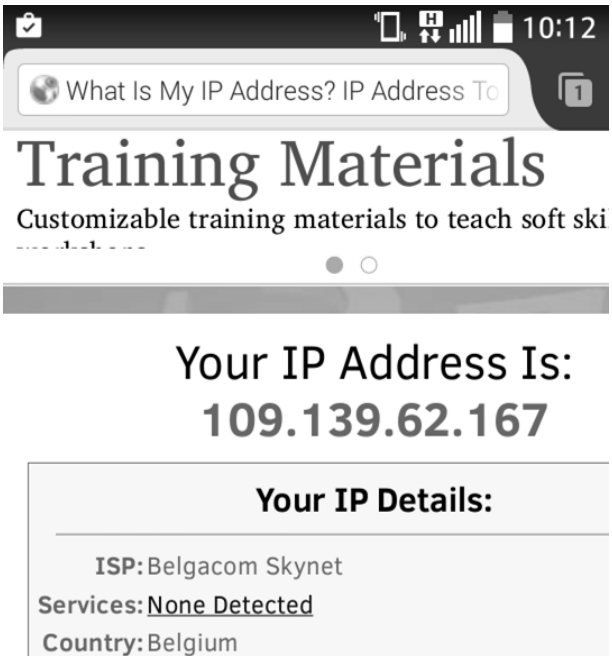
De SSH-server kan ook dienen als een soort van proxyserver. Hierdoor kan men bvb. veilig surfen op een publiek Wi-Fi netwerk, aangezien we gebruik maken van een geëncrypteerde “tunnel”.

Om dit te testen maak ik gebruik van de Ubuntu Server-machine, en over een LG L90 smartphone, met Android 4.4.

Aan de server uit vorige oefeningen moeten we niets veranderen, hij moet gewoon klaar staan om SSH-verbindingen aan te nemen.

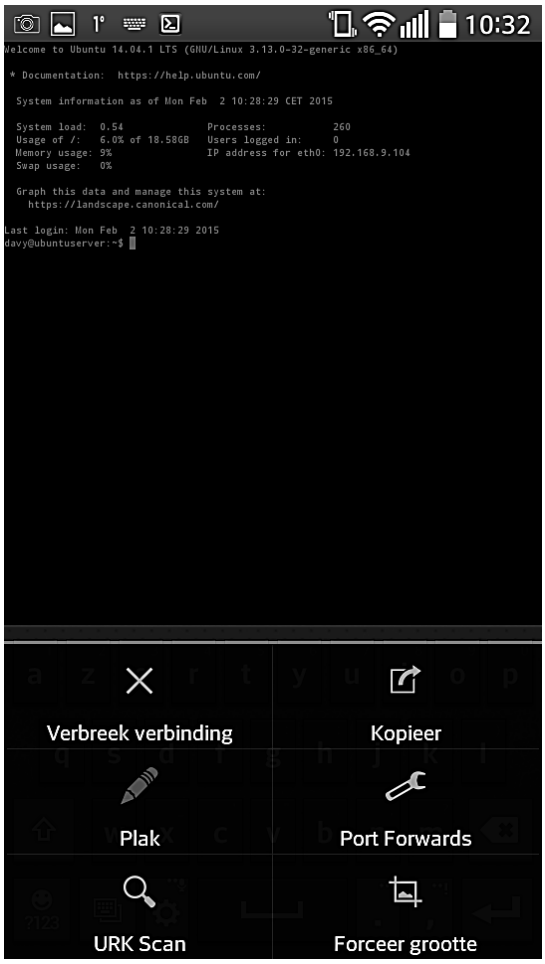
Op de smartphone installeer ik Firefox en Connectbot. Ik schakel mijn dataverbruik aan, zodat ik zeker niet op het lokale LAN zit.

Dan zoek ik via Firefox mijn huidig IP op:



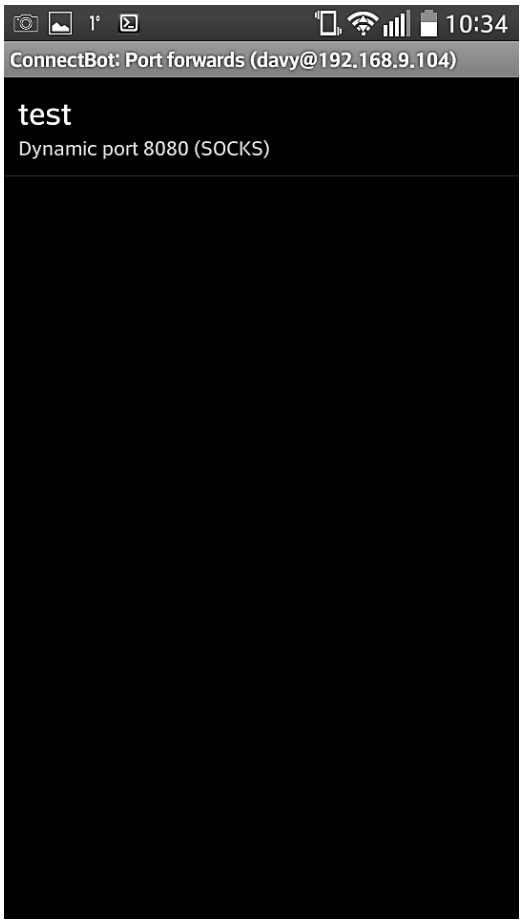
Zoals je ziet zit ik op het netwerk van Belgacom, via mijn mobiel abonnement.

Daarna maak ik via Connectbot een verbinding met mijn SSH-server.



Als de verbinding gemaakt is, druk je op de menu-toets van de smartphone. In het menu dat je dan krijgt, kies je voor “port forwards”.

Als men een nieuwe port forward maakt, kiest men voor het type dynamisch, en kiest men een poort.

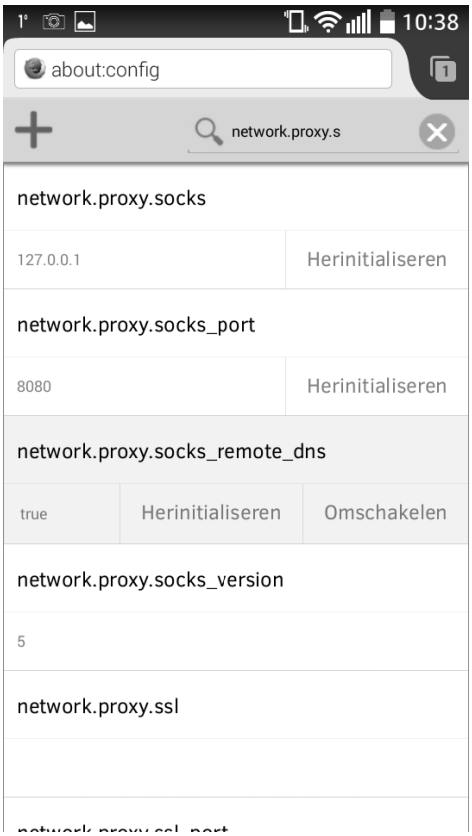


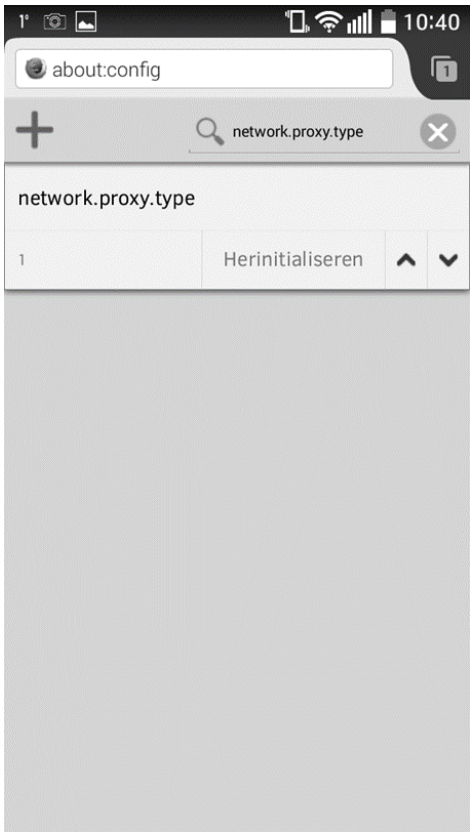
Het kan zijn dat na het aanmaken van de port forward, we onze SSH-connectie moeten heractiveren. Nu dat alles ingesteld is bij Connectbot, stellen we Firefox in.

De instellingen van Firefox vinden we door “about:config” in te geven in de URL-bar. Daarna zoeken we naar de instellingen door als sleutelwoord “network.proxy.socks” in te geven.

Hier geven we volgende gegevens in:

network.proxy.socks	127.0.0.1
network.proxy.socks_port	8080 (zelf gekozen in Connectbot)
network.proxy.socks_remote_dns	true
network.proxy.socks_version	5





Zoals je hierboven ziet, moeten we ook “network.proxy.type” op 1 zetten. Zo weet Firefox dat er handmatige proxy-instellingen gebruikt worden.

Als test surfen we nu nogmaals naar dezelfde website, en nu zien we dat we een ander IP hebben:

Unison

Eerst installeren we Unison

```
davy@ubuntuserver:~$ sudo apt-get install unison
[sudo] password for davy:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  unison-all
The following NEW packages will be installed:
  unison
0 upgraded, 1 newly installed, 0 to remove and 98 not upgraded.
Need to get 728 kB of archives.
After this operation, 2,028 kB of additional disk space will be used.
Get:1 http://be.archive.ubuntu.com/ubuntu/ trusty/universe unison amd64 2.40
.102-2ubuntu1 [728 kB]
Fetched 728 kB in 1s (522 kB/s)
Selecting previously unselected package unison.
(Reading database ... 95%
```

Ik heb enkele bestanden aangemaakt waarvan we een back-up gaan maken. Deze zet ik in een aparte directory om alles overzichtelijk te houden.

```
davy@ubuntuserver:~$ ls
bestand1.txt  bestand2.txt  bestand3.txt
davy@ubuntuserver:~$ cat bestand2.txt
ubuntuserver
1 2 3 4 5
davy@ubuntuserver:~$
```

```
davy@ubuntuserver:~$ mkdir mydocs
davy@ubuntuserver:~$ mv *.txt mydocs
davy@ubuntuserver:~$ ls mydocs
bestand1.txt  bestand2.txt  bestand3.txt
davy@ubuntuserver:~$
```

We controleren de versie van Unison op beide machines. Deze moeten gelijk zijn.

```
davy@ubuntuserver:~$ unison -version
unison version 2.40.102
davy@ubuntuserver:~$
```

```
dave@linuxlitebase:~$ unison -version
unison version 2.40.102
dave@linuxlitebase:~$
```

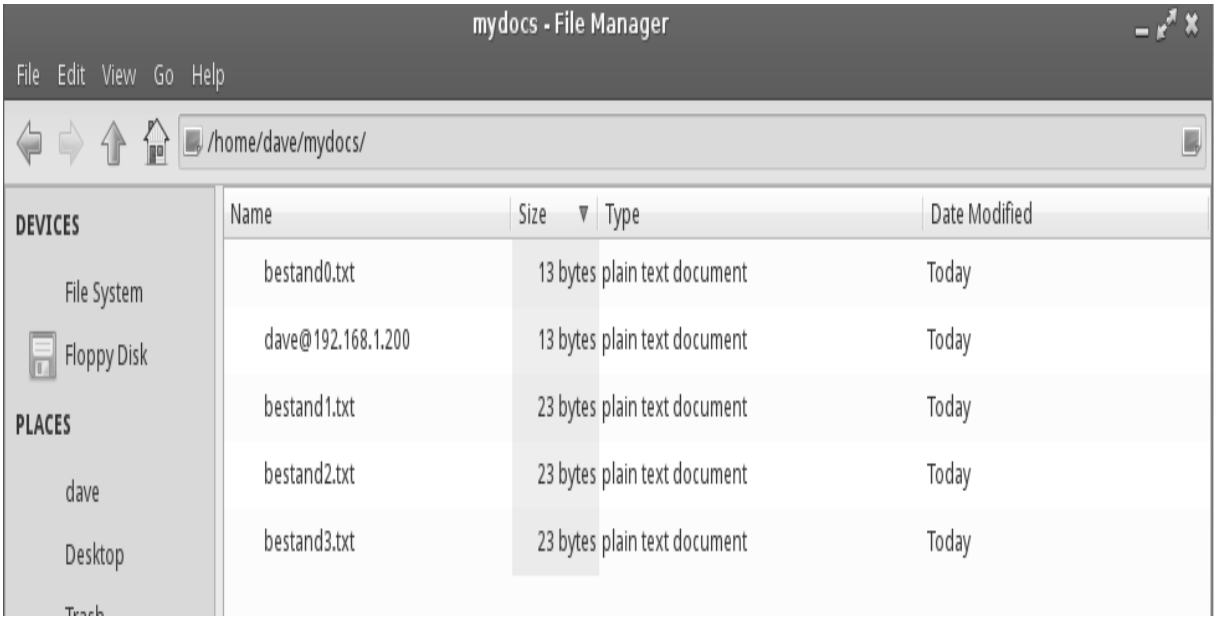
Nu Unison geïnstalleerd is, gaan we de test doen. De eerste maal dat we Unison gebruiken, worden de mappen gesynchroniseerd.

```
davy@ubuntuserver:~$ unison mydocs/ ssh://dave@192.168.1.200/mydocs
Contacting server...
dave@192.168.1.200's password:
Connected [//linuxlitebase//home/dave/mydocs -> //ubuntuserver//home/davy/mydocs]
Looking for changes
Warning: No archive files were found for these roots, whose canonical names are:
        /home/davy/mydocs
        //linuxlitebase//home/dave/mydocs
This can happen either
because this is the first time you have synchronized these roots,
or because you have upgraded Unison to a new version with a different
archive format.

Update detection may take a while on this run if the replicas are
large.

Unison will assume that the 'last synchronized state' of both replicas
was completely empty.  This means that any files that are different
will be reported as conflicts, and any files that exist only on one
replica will be judged as new and propagated to the other replica.
If the two replicas are identical, then no changes will be reported.

If you see this message repeatedly, it may be because one of your machines
is getting its address from DHCP, which is causing its host name to change
between synchronizations.  See the documentation for the UNISONLOCALHOSTNAME
environment variable for advice on how to correct this.

Donations to the Unison project are gratefully accepted:
http://www.cis.upenn.edu/~bcpierce/unison

Press return to continue.[<spc>] _
```

```
Press return to continue.[<spc>]   Waiting for changes from server
Reconciling changes

local          linuxlite...
dir      ---->            /  [f]

Proceed with propagating updates? [] y
Propagating updates


UNISON 2.40.102 started propagating changes at 21:52:09.87 on 04 Mar 2015
[BGN] Copying  from /home/davy/mydocs to //linuxlitebase//home/dave/mydocs
Shortcut: copied /home/dave/mydocs/dave@192.168.1.200 from local file /home/dave/.unison.mydocs.4657
cad2eaca3689d9644cfdf435e01a.unison.tmp/bestand0.txt
Shortcut: copied /home/dave/mydocs/bestand3.txt from local file /home/dave/.unison.mydocs.4657cad2ea
ca3689d9644cfdf435e01a.unison.tmp/bestand2.txt
Shortcut: copied /home/dave/mydocs/bestand2.txt from local file /home/dave/.unison.mydocs.4657cad2ea
ca3689d9644cfdf435e01a.unison.tmp/bestand1.txt
[END] Copying
UNISON 2.40.102 finished propagating changes at 21:52:09.88 on 04 Mar 2015


Saving synchronizer state
Synchronization complete at 21:52:09  (1 item transferred, 0 skipped, 0 failed)
davy@ubuntuserver:~$
```

Na de synchronisatie doen we de controle.

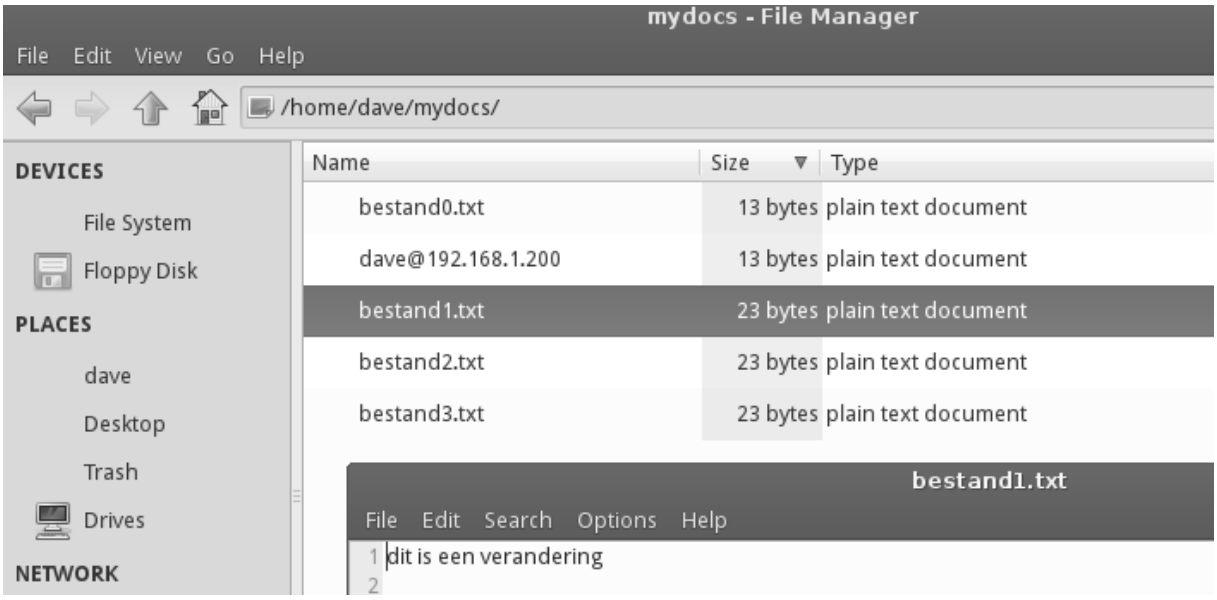
```
davy@ubuntuserver:~$ cd mydocs/
davy@ubuntuserver:~/mydocs$ ls
bestand0.txt  bestand1.txt  bestand2.txt  bestand3.txt  dave@192.168.1.200
davy@ubuntuserver:~/mydocs$
```



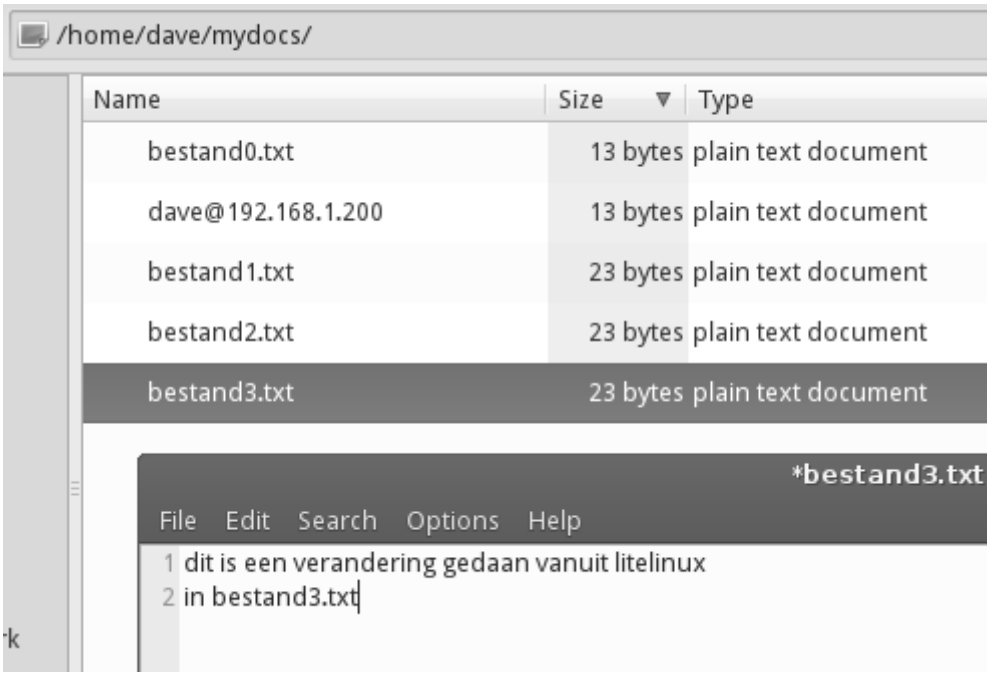
Nu de mappen op de server en cliënt zijn gesynchroniseerd, maak ik een verandering. Deze verandering zou dan met Unison van de ene naar de andere machine gekopieerd worden.

```
davy@ubuntuserver:~/mydocs$ echo "dit is een verandering" > bestand1.txt
davy@ubuntuserver:~/mydocs$ cd ..
davy@ubuntuserver:~$ unison mydocs/ ssh://dave@192.168.1.200/mydocs_
```

```
davy@ubuntuserver:~$ unison mydocs/ ssh://dave@192.168.1.200/mydocs
Contacting server...
dave@192.168.1.200's password:
Connected [//linuxlitebase//home/dave/mydocs -> //ubuntuserver//home/davy/mydocs]
Looking for changes
  Waiting for changes from server
Reconciling changes

local          linuxlite...
changed  ----->            bestand1.txt  [f]

Proceed with propagating updates? [] y
Propagating updates


UNISON 2.40.102 started propagating changes at 21:59:14.51 on 04 Mar 2015
[BGN] Updating file bestand1.txt from /home/davy/mydocs to //linuxlitebase//home/dave/mydocs
[END] Updating file bestand1.txt
UNISON 2.40.102 finished propagating changes at 21:59:14.52 on 04 Mar 2015


Saving synchronizer state
Synchronization complete at 21:59:14  (1 item transferred, 0 skipped, 0 failed)
davy@ubuntuserver:~$ _
```



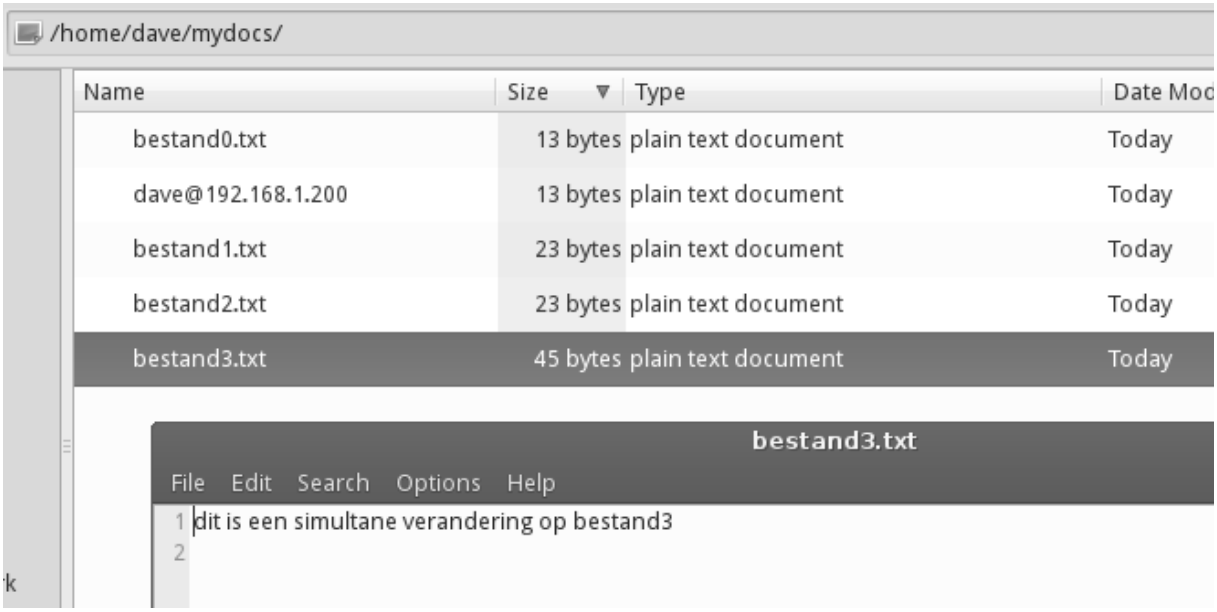
Als er aan beide zijden een verandering gebeurt, geven we via een keuzemenu door aan Unison welk bestand we willen behouden.




```
davy@ubuntuserver:~$ echo "dit is een simultane verandering op bestand3" > mydocs/bestand3.txt
davy@ubuntuserver:~$ unison mydocs/ ssh://dave@192.168.1.200/mydocs
Contacting server...
dave@192.168.1.200's password:
```

```
Connected [//linuxlitebase//home/dave/mydocs -> //ubuntuserver//home/davy/mydocs]
Looking for changes
  Waiting for changes from server
Reconciling changes

local          linuxlite...
changed  <-?-> changed    bestand3.txt  [] d

diff -u '/home/davy/mydocs/bestand3.txt.unison.diff-' '/home/davy/mydocs/bestand3.txt'

--- /home/davy/mydocs/bestand3.txt.unison.diff- 2015-03-04 22:07:03.306074963 +0100
+++ /home/davy/mydocs/bestand3.txt      2015-03-04 22:04:02.406077896 +0100
@@ -1,2 +1 @@
-dit is een verandering gedaan vanuit litelinux
-in bestand3.txt
\ No newline at end of file
+dit is een simultane verandering op bestand3

changed  <-?-> changed    bestand3.txt  [] _


local          linuxlite...
changed  <-?-> changed    bestand3.txt  [] d

diff -u '/home/davy/mydocs/bestand3.txt.unison.diff-' '/home/davy/mydocs/bestand3.txt'

--- /home/davy/mydocs/bestand3.txt.unison.diff- 2015-03-04 22:07:03.306074963 +0100
+++ /home/davy/mydocs/bestand3.txt      2015-03-04 22:04:02.406077896 +0100
@@ -1,2 +1 @@
-dit is een verandering gedaan vanuit litelinux
-in bestand3.txt
\ No newline at end of file
+dit is een simultane verandering op bestand3

changed  <-?-> changed    bestand3.txt  [] ?
Commands:
  f                    follow unison's recommendation (if any)
  I                    ignore this path permanently
  E                    permanently ignore files with this extension
  N                    permanently ignore paths ending with this name
  m                    merge the versions
  d                    show differences
  x                    show details
  L                    list all suggested changes tersely
  l                    list all suggested changes with details
  p or b               go back to previous item
  g                    proceed immediately to propagating changes
  q                    exit unison without propagating any changes
  /                    skip
  > or .               propagate from from local to linuxlitebase
  < or ,               propagate from from linuxlitebase to local
changed  ====> changed    bestand3.txt  [] >

Proceed with propagating updates? []
```

Ik kies hier om de wijziging op de server te propageren naar de lokale machine, met de keuze ">".



Unison in een cronjob

Om tot een geautomatiseerde back-up-oplossing te komen met Unison, kunnen we het Unison-commando in het crontab-bestand zetten.

Eerst maken we een profiel aan in de –verborgen- Unison-map. Hierin plaatsen we de benodigde gegevens en opties. Door de gebruikte opties bekom ik dat Unison loopt zonder gebruikersinvoer, en dat de nieuwste files gebruikt worden in de bestandsvergelijking.

```
davy@ubuntuserver:~/.unison$ cat default.prf
# Unison preferences file

# Roots to sync
root = /home/davy/
root = ssh://dave@192.168.1.200/

# Path to sync folder
path = mydocs/

# User questions off
auto=true
batch=true
silent=true

# Which files to take
prefer=newer
davy@ubuntuserver:~/.unison$
```

Nu kunnen we de back-up maken zonder parameters mee te geven aan Unison.

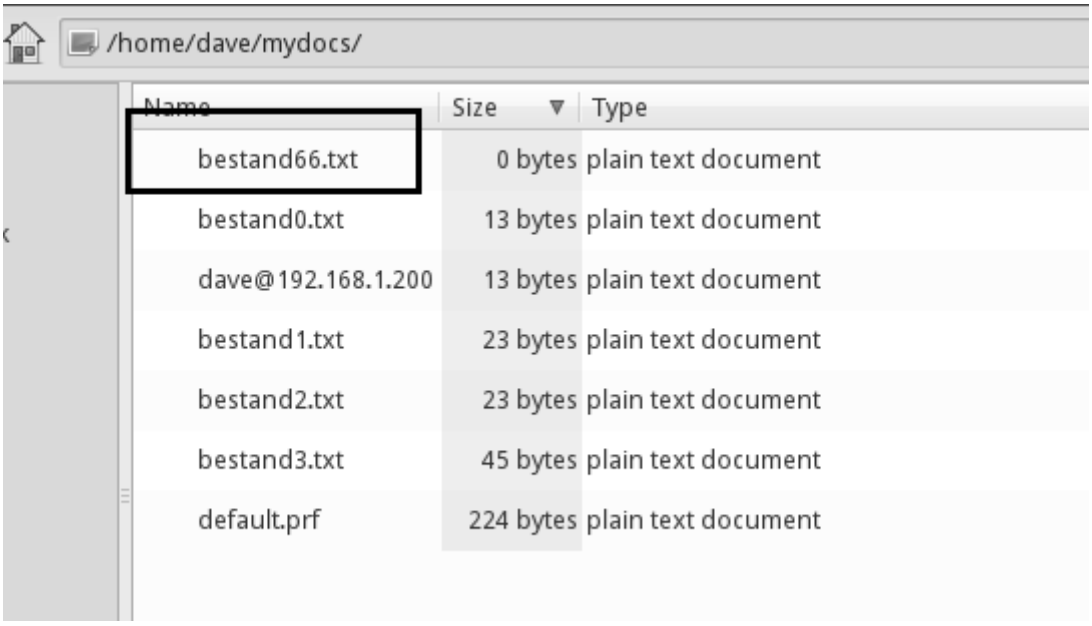
Ik heb een crontab aangemaakt die om de vijf minuten Unison draait in de background, zonder enige output

```
davy@ubuntuserver:~$ crontab -l > mycron.txt
davy@ubuntuserver:~$ cat mycron.txt
*/5 * * * * /usr/bin/unison &> /dev/null
davy@ubuntuserver:~$
```

We doen een verandering:

```
davy@ubuntuserver:/home$ cd davy/
davy@ubuntuserver:~$ cd mydocs/
davy@ubuntuserver:~/mydocs$ touch bestand66.txt
davy@ubuntuserver:~/mydocs$ _
```

En vijf minuten later zien we dit weer op de cliënt:



Unison en Incron

We kunnen Unison ook een back-up laten maken van zodra er veranderingen in de map gebeuren. Dit doen we met behulp van Incron.

We installeren Incron met behulp van “apt-get install incron”. Na de installatie controleren we of de Incron-service draait.

```
davy@ubuntuserver:~$ sudo /etc/init.d/incron status
 * incron is running
davy@ubuntuserver:~$ sudo cat /etc/incron.allow
davy@ubuntuserver:~$ sudo vim /etc/incron.allow
```

In het bestand “incron.allow” moeten we zetten welke gebruikers incron mogen gebruiken.

```
davy@ubuntuserver:~$ sudo cat /etc/incron.allow
root
davy
davy@ubuntuserver:~$
```

Daarna maken we, net zoals bij een cronjob, een incronjob aan. Dit doen we met “incrontab –e”.

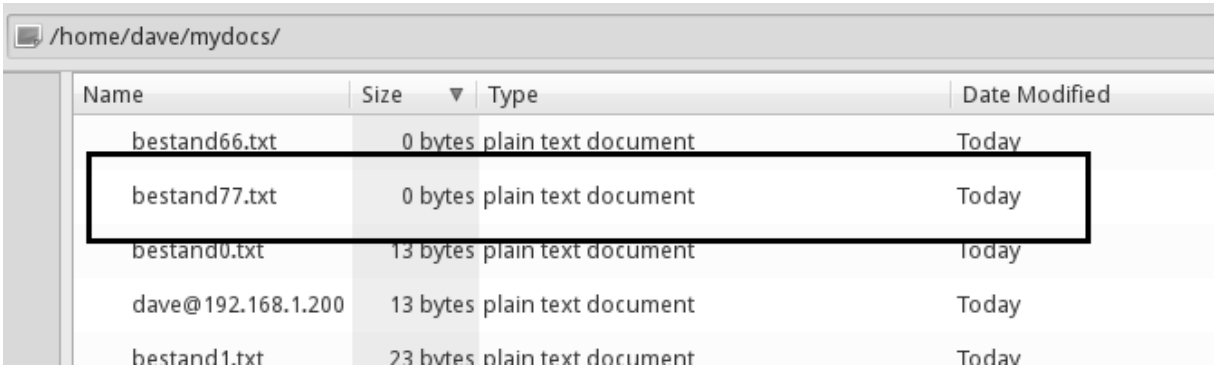
```
 GNU nano 2.2.6                File: /tmp/incron.table-84eivv

/home/davy/mydocs/ IN_MODIFY,IN_CREATE,IN_DELETE unison
```

In dit bestand staat welke map er moet “beheerd” worden, bij welke acties er iets moet ondernomen worden, en wat er ondernomen moet worden.

We maken een nieuw bestand aan in de map:

```
davy@ubuntuserver:~$ cd mydocs/
davy@ubuntuserver:~/mydocs$ touch bestand77.txt
davy@ubuntuserver:~/mydocs$ _
```

En nu gaan we onmiddellijk in de overeenstemmende map kijken op de cliënt.


/home/dave/mydocs/
Name
Size
Type
Date Modified
bestand66.txt
0 bytes
plain text document
Today
bestand77.txt
0 bytes
plain text document
Today
bestand0.txt
13 bytes
plain text document
Today
dave@192.168.1.200
13 bytes
plain text document
Today
bestand1.txt
23 bytes
plain text document
Today

DNS met behulp van BIND9

Intro

In deze oefening maken we twee DNS-zones aan, die ieder een DNS-server en een cliënt bevatten. We zorgen er voor dat ze onderling master en slave zijn, en dat ze DNS-requests buiten onze zone ook kunnen doorsturen en “cachen”.

Het netwerk-diagram ziet u op de volgende pagina.

Het is vanzelfsprekend nodig dat de router correct werkt, en verkeer van de ene naar de andere zone toelaat, en ook naar buiten toe.

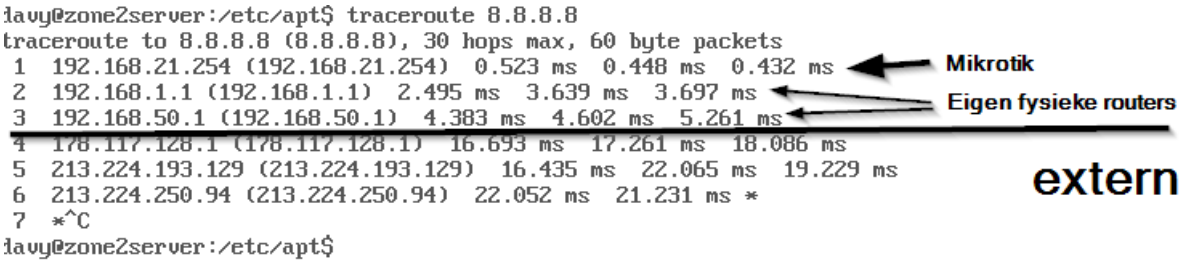
We pingen van zone 1 naar buiten:

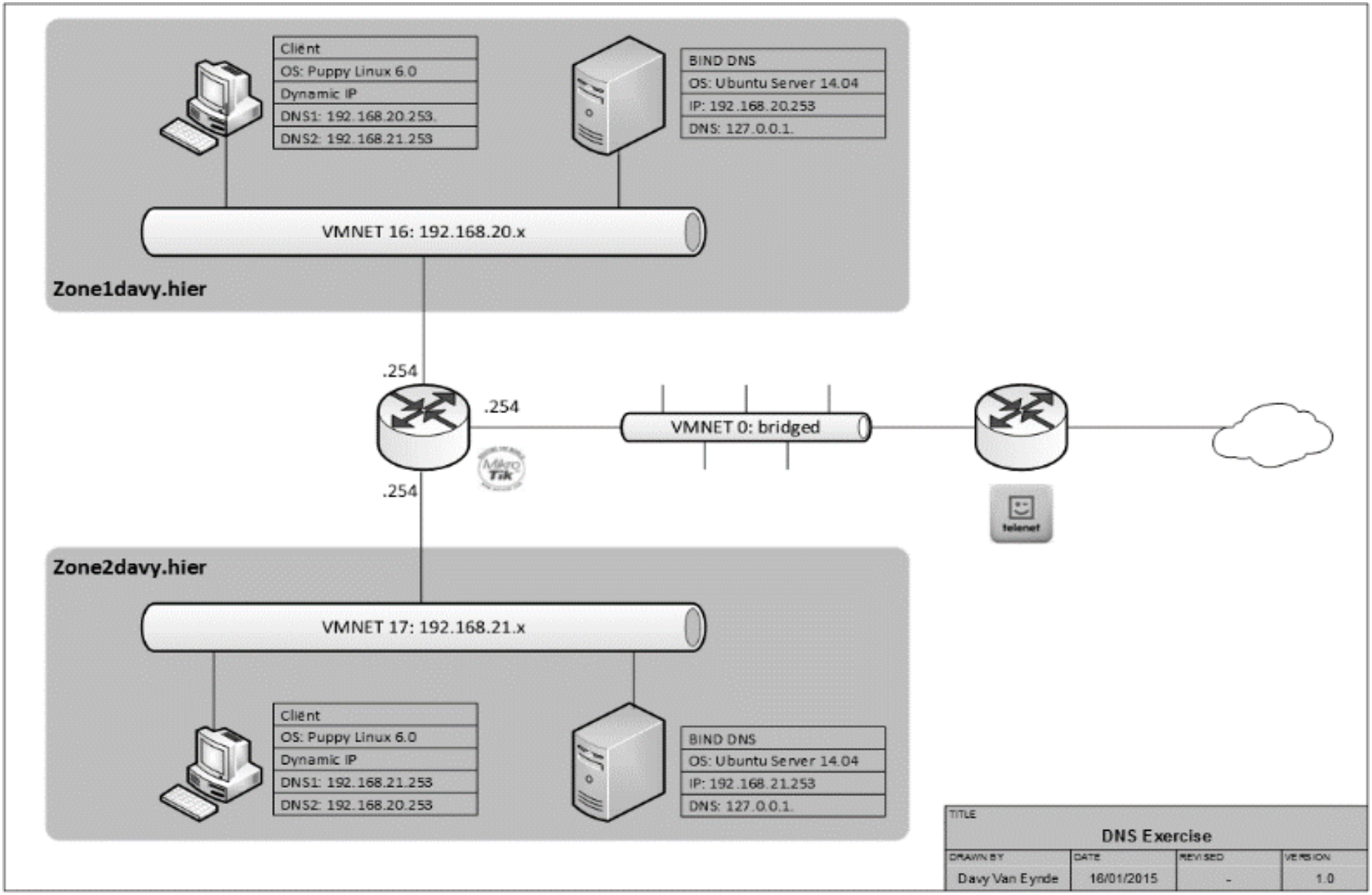
```
davy@zone1server:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=17.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=17.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=17.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=16.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=16.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=16.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=53 time=16.7 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6060ms
rtt min/avg/max/mdev = 16.016/16.732/17.220/0.434 ms
davy@zone1server:~$ _
```

En nu van zone 1 naar 2:

```
davy@zone1server:~$ ping 192.168.21.253
PING 192.168.21.253 (192.168.21.253) 56(84) bytes of data.
64 bytes from 192.168.21.253: icmp_seq=1 ttl=63 time=7.11 ms
64 bytes from 192.168.21.253: icmp_seq=2 ttl=63 time=0.622 ms
64 bytes from 192.168.21.253: icmp_seq=3 ttl=63 time=0.602 ms
64 bytes from 192.168.21.253: icmp_seq=4 ttl=63 time=0.652 ms
64 bytes from 192.168.21.253: icmp_seq=5 ttl=63 time=0.626 ms
64 bytes from 192.168.21.253: icmp_seq=6 ttl=63 time=0.529 ms
```

Waarna we een traceroute van zone 2 naar buiten doen:




Client
OS: Puppy Linux 6.0
Dynamic IP
DNS1: 192.168.20.253
DNS2: 192.168.21.253
BIND DNS
OS: Ubuntu Server 14.04
IP: 192.168.20.253
DNS: 127.0.0.1.
VMNET 16: 192.168.20.x
Zone1davy.hier
.254
.254
VMNET 0: bridged
.254
telenet
Zone2davy.hier
VMNET 17: 192.168.21.x
Client
OS: Puppy Linux 6.0
Dynamic IP
DNS1: 192.168.21.253
DNS2: 192.168.20.253
BIND DNS
OS: Ubuntu Server 14.04
IP: 192.168.21.253
DNS: 127.0.0.1.
TITLE
DNS Exercise
DRAWN BY
Davy Van Eynde
DATE
16/01/2015
REVISED
-
VERSION
1.0

Cachen van DNS-requests

DNS-requests die naar info vragen van domeinen buiten ons domein worden doorgestuurd naar andere DNS-servers. Ze worden dan lokaal “gecached” worden zodat in de toekomst deze requests sneller gaan

In het bestand “named.conf.options” zetten we de forwarders-clausule

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                8.8.8.8;
                8.8.4.4;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
~
~
~
~
~
~
~
~
"/etc/bind/named.conf.options" 27L, 894C                              1,1
```

Daarna restarten we onze DNS-service:

```
davy@ubuntuserver:~$ sudo service bind9 restart
 * Stopping domain name service... bind9
waiting for pid 3058 to die
                                                                      [ OK ]
 * Starting domain name service... bind9                             [ OK ]
davy@ubuntuserver:~$ _
```

```
; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> www.hln.be
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16389
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 13, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.hln.be.                    IN      A

;; ANSWER SECTION:
www.hln.be.             23      IN      CNAME   ssl-be.persgroep.edgekey.net.
ssl-be.persgroep.edgekey.net. 17839 IN  CNAME   e8838.ksd.akamaiedge.net.
e8838.ksd.akamaiedge.net. 19    IN      A       2.21.0.173

;; AUTHORITY SECTION:
.                       9109    IN      NS      c.root-servers.net.
.                       9109    IN      NS      d.root-servers.net.
.                       9109    IN      NS      f.root-servers.net.
.                       9109    IN      NS      e.root-servers.net.
.                       9109    IN      NS      a.root-servers.net.
.                       9109    IN      NS      i.root-servers.net.
.                       9109    IN      NS      h.root-servers.net.
.                       9109    IN      NS      l.root-servers.net.
.                       9109    IN      NS      k.root-servers.net.
.                       9109    IN      NS      g.root-servers.net.
.                       9109    IN      NS      j.root-servers.net.
.                       9109    IN      NS      m.root-servers.net.
.                       9109    IN      NS      b.root-servers.net.

;; Query time: 302 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 10 11:19:53 CET 2015
;; MSG SIZE  rcvd: 340

davy@ubuntuserver:~$ _
```

```
; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> www.hln.be
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58559
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 13, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.hln.be.                    IN      A

;; ANSWER SECTION:
www.hln.be.             34      IN      CNAME   ssl-be.persgroep.edgekey.net.
ssl-be.persgroep.edgekey.net. 17738 IN  CNAME   e8838.ksd.akamaiedge.net.
e8838.ksd.akamaiedge.net. 19    IN      A       2.21.0.173

;; AUTHORITY SECTION:
.                       9008    IN      NS      k.root-servers.net.
.                       9008    IN      NS      d.root-servers.net.
.                       9008    IN      NS      e.root-servers.net.
.                       9008    IN      NS      m.root-servers.net.
.                       9008    IN      NS      g.root-servers.net.
.                       9008    IN      NS      h.root-servers.net.
.                       9008    IN      NS      f.root-servers.net.
.                       9008    IN      NS      c.root-servers.net.
.                       9008    IN      NS      l.root-servers.net.
.                       9008    IN      NS      j.root-servers.net.
.                       9008    IN      NS      b.root-servers.net.
.                       9008    IN      NS      i.root-servers.net.
.                       9008    IN      NS      a.root-servers.net.

;; Query time: 80 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 10 11:21:34 CET 2015
;; MSG SIZE  rcvd: 340
```

Zoals je ziet is in bovenstaand voorbeeld de querytime van 300 naar 80 gezakt.

Opbouw zone 1

Eerst stellen we de server in.

In de map /etc/bind/ maken we de benodigde bestanden aan, door bestaande bestanden als sjabloon te maken. Ik heb hier “db.zone1davy.hier” aangemaakt, en “db.192” voor de reverse DNS.

```
davy@zone1server:/etc/bind$ ls
bind.keys  db.192    db.local          named.conf                named.conf
db.0       db.255    db.root           named.conf.default-zones  rndc.key
db.127     db.empty  db.zone1davy.hier  named.conf.local          zones.rfc1
davy@zone1server:/etc/bind$
```

Het bestand “db.zone1davy.hier” ziet er zo uit:

```
$TTL    604800
@       IN      SOA     ns.zone1davy.hier. admin.zone1davy.hier. (
                         2015021902             ; Serial
                          604800                ; Refresh
                           86400                ; Retry
                         2419200                ; Expire
                          604800 )              ; Negative Cache TTL
;
@       IN      NS      ns.zone1davy.hier.
;
@       IN      A       192.168.20.253
ns      IN      A       192.168.20.253
```

Als serial gebruik ik hier de datum in omgekeerde volgorde plus nog een volgnummer. Bij research kwam ik dit tegen als een soort stelregel.

De inhoud van mijn “db.192” bestand ziet er zo uit:

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.zone1davy.hier. admin.zone1davy.hier. (
                         2015021903     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                         2419200        ; Expire
                          604800 )      ; Negative Cache TTL
;
@       IN      NS      ns.
;
253     IN      PTR     ns.zone1davy.hier.

~
```

Nu moeten we alleen onze DNS-server nog vertellen dat deze bestanden bestaan. Dit doen we door het bestand “named.conf.local” aan te passen, en de DNS service te herstarten. “named.conf.local” ziet er zo uit:

```
zone "zone1davy.hier" {
        type master;
        file "/etc/bind/db.zone1davy.hier";
};

// reverse

zone "20.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
```

Nu gaan we testen of het werkt, eerst op de server:

```
davy@zone1server:/etc/bind$ ping ns.zone1davy.hier
PING ns.zone1davy.hier (192.168.20.253) 56(84) bytes of data.
64 bytes from ns.zone1davy.hier (192.168.20.253): icmp_seq=1 ttl=64 time=0.016 m
s
64 bytes from ns.zone1davy.hier (192.168.20.253): icmp_seq=2 ttl=64 time=0.030 m
s
64 bytes from ns.zone1davy.hier (192.168.20.253): icmp_seq=3 ttl=64 time=0.028 m
s

davy@zone1server:/etc/bind$ nslookup zone1davy.hier
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   zone1davy.hier
Address: 192.168.20.253
```

```
davy@zone1server:/etc/bind$ dig zone1davy.hier

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> zone1davy.hier
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65067
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;zone1davy.hier.                        IN      A

;; ANSWER SECTION:
zone1davy.hier.         604800  IN      A       192.168.20.253

;; AUTHORITY SECTION:
zone1davy.hier.         604800  IN      NS      ns.zone1davy.hier.

;; ADDITIONAL SECTION:
ns.zone1davy.hier.      604800  IN      A       192.168.20.253

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Feb 19 16:38:13 CET 2015
;; MSG SIZE  rcvd: 92
```

Nu dat we via de server getest hebben, ga ik testen via een cliënt:

```
# ping ns.zoneldavy.hier
PING ns.zoneldavy.hier (192.168.20.253): 56 data bytes
64 bytes from 192.168.20.253: seq=0 ttl=64 time=0.270 ms
64 bytes from 192.168.20.253: seq=1 ttl=64 time=0.355 ms
64 bytes from 192.168.20.253: seq=2 ttl=64 time=0.535 ms
64 bytes from 192.168.20.253: seq=3 ttl=64 time=0.311 ms
^C
--- ns.zoneldavy.hier ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.270/0.367/0.535 ms
```

```
# nslookup zoneldavy.hier
Server:     192.168.20.253
Address 1: 192.168.20.253 ns.zoneldavy.hier

Name:       zoneldavy.hier
Address 1: 192.168.20.253 ns.zoneldavy.hier
```

Opbouw zone 2

Dit verloopt identiek met de opbouw van zone 1, met de juiste zonenaam en IP-adressen.

```
davy@zone2server:/etc/bind$ ls
bind.keys  db.192    db.local           named.conf                named.conf.local    zones.rfc1918
db.0       db.255    db.root            named.conf.balocal        named.conf.options
db.127     db.empty  db.zone2davy.hier  named.conf.default-zones  rndc.key
davy@zone2server:/etc/bind$ cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "zone2davy.hier" {
        type master;
        file "/etc/bind/db.zone2davy.hier";
};

// reverse

zone "21.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
davy@zone2server:/etc/bind$
```

```
davy@zone2server:/etc/bind$ cat db.192
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.zone2davy.hier. admin.zone2davy.hier. (
                         2015022801     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
davy@zone2server:/etc/bind$
```

```
davy@zone2server:/etc/bind$ cat db.zone2davy.hier
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.zone2davy.hier. admin.zone2davy.hier. (
                         2015022801     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.zone2davy.hier.
;
@       IN      A       192.168.21.253
ns      IN      A       192.168.21.253
```

```
davy@zone2server:/etc/bind$ dig zone2davy.hier

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> zone2davy.hier
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18778
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;zone2davy.hier.                        IN      A

;; ANSWER SECTION:
zone2davy.hier.         604800  IN      A       192.168.21.253

;; AUTHORITY SECTION:
zone2davy.hier.         604800  IN      NS      ns.zone2davy.hier.

;; ADDITIONAL SECTION:
ns.zone2davy.hier.      604800  IN      A       192.168.21.253

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Feb 28 14:01:07 CET 2015
;; MSG SIZE  rcvd: 92

davy@zone2server:/etc/bind$ nslookup ns.zone2davy.hier
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   ns.zone2davy.hier
Address: 192.168.21.253
```

Master versus slave

Om een master-slave systeem te verkrijgen, moeten we het bestand “named.conf.local” aanpassen, en aan het bestand op de master twee “slave zones” aanmaken. Er zijn er twee, één voor forward en één voor reverse DNS.

Bij het “master”-gedeelte zeggen we dat we transfers kunnen ontvangen van de slave. In het “slave”-gedeelte verwijzen we naar de te gebruiken zone-database, en we vermelden wie de masters zijn.

```
davy@zone1server:~$ cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "zone1davy.hier" {
        type master;
        file "/etc/bind/db.zone1davy.hier";
        allow-transfer { 192.168.21.253; };
};

zone "zone2davy.hier" {
        type slave;
        file "/var/cache/bind/db.server2.hier";
        masters { 192.168.21.253; };
};
// reverse

zone "20.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
davy@zone1server:~$
```

```
davy@zone2server:~$ cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "zone2davy.hier" {
        type master;
        file "/etc/bind/db.zone2davy.hier";
        allow-transfer { 192.168.20.253; };
};

zone "zone1davy.hier" {
        type slave;
        file "/var/cache/bind/db.zone1davy.hier";
        masters { 192.168.20.253; };
};

// reverse

zone "21.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
davy@zone2server:~$
```

We verwijzen naar de map “/var/cache/bind/”, die moeten we nog aanmaken:

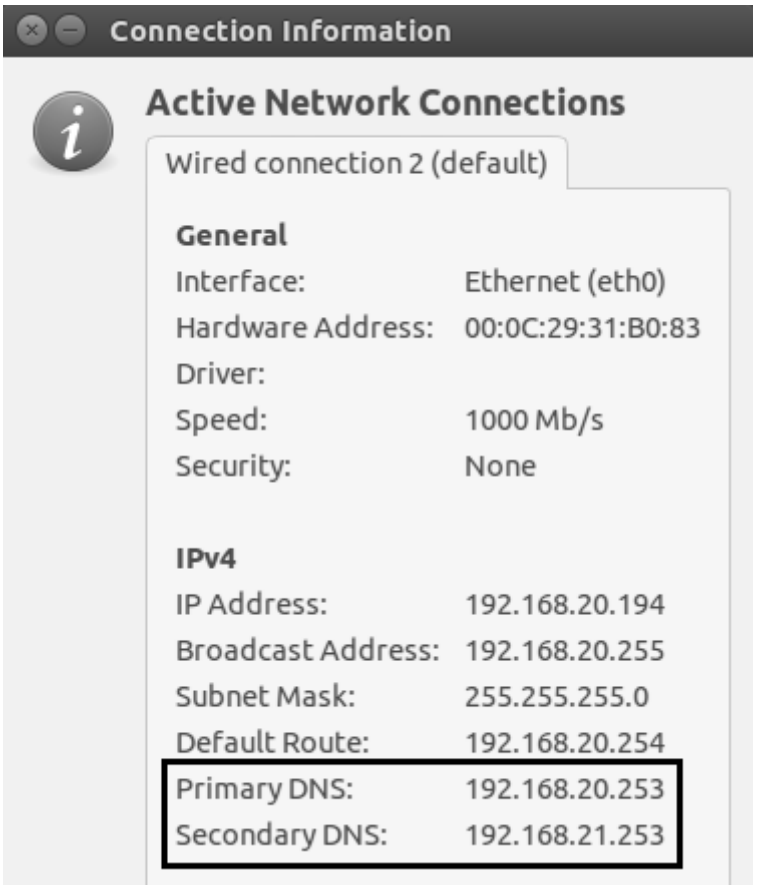
```
davy@zone1server:/var/log$ cd ..
davy@zone1server:/var$ cd cache/
davy@zone1server:/var/cache$ cd bind/
davy@zone1server:/var/cache/bind$ ls
db.server2.hier  managed-keys.bind
davy@zone1server:/var/cache/bind$
```

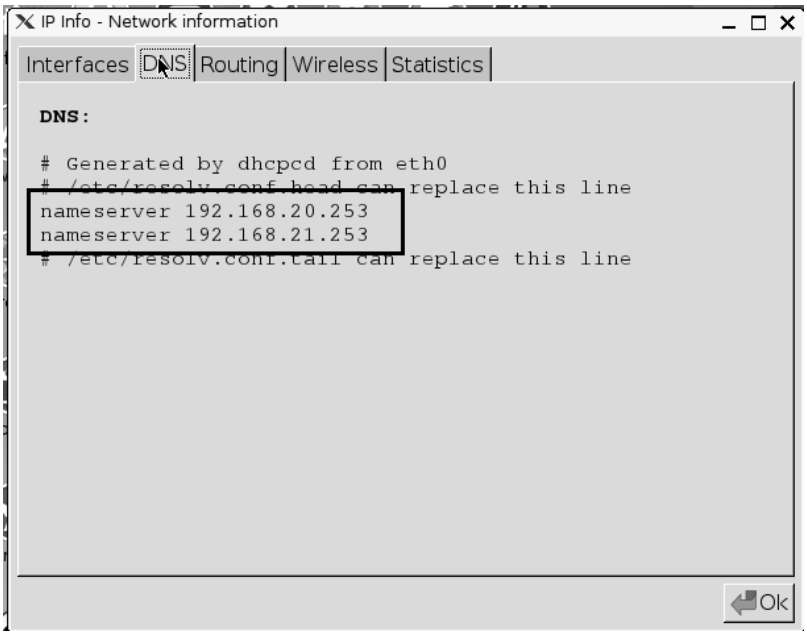
```
davy@zone2server:~$ ls /var/cache/bind/
db.zone1davy.hier  managed-keys.bind
davy@zone2server:~$
```

Als we dan de DNS-service op beide herstarten, kunnen we in het bestand “/var/log/syslog/” zien dat de zone-transfer gebeurd:

```
Feb 28 16:11:15 zone2server named[1277]: zone 21.168.192.in-addr.arpa/IN: sending notifies (serial 20150
22801)
Feb 28 16:11:15 zone2server named[1277]: zone zone1davy.hier/IN: Transfer started.
Feb 28 16:11:15 zone2server named[1277]: transfer of 'zone1davy.hier/IN' from 192.168.20.253#53: connect
ed using 192.168.21.253#48278
Feb 28 16:11:15 zone2server named[1277]: zone zone1davy.hier/IN: transferred serial 2015021903
Feb 28 16:11:15 zone2server named[1277]: transfer of 'zone1davy.hier/IN' from 192.168.20.253#53: Transfe
r completed: 1 messages, 6 records, 180 bytes, 0.001 secs (180000 bytes/sec)
Feb 28 16:16:53 zone2server named[1277]: client 192.168.20.253#39582 (zone2davy.hier): transfer of 'zone
2davy.hier/IN': AXFR started
Feb 28 16:16:53 zone2server named[1277]: client 192.168.20.253#39582 (zone2davy.hier): transfer of 'zone
2davy.hier/IN': AXFR ended
```

Op de cliënts van beide zones verwijzen we in de netwerk-instellingen naar beide DNS-servers.





Van cliënt 1 kan ik naar de nameserver van zone 2 pingen, met gebruik van de hostname.

```
davy@davyubuntu14:~$ ping ns.zone2davy.hier
PING ns.zone2davy.hier (192.168.21.253) 56(84) bytes of data.
64 bytes from 192.168.21.253: icmp_seq=1 ttl=63 time=0.755 ms
64 bytes from 192.168.21.253: icmp_seq=2 ttl=63 time=0.542 ms
64 bytes from 192.168.21.253: icmp_seq=3 ttl=63 time=0.613 ms
64 bytes from 192.168.21.253: icmp_seq=4 ttl=63 time=0.653 ms
64 bytes from 192.168.21.253: icmp_seq=5 ttl=63 time=0.614 ms
^C
--- ns.zone2davy.hier ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.542/0.635/0.755/0.073 ms
```

Van de cliënt in zone 2 kan ik pingen naar de nameserver van zone 1.

```
urxvt
# ping ns.zoneldavy.hier
PING ns.zoneldavy.hier (192.168.20.253): 56 data bytes
64 bytes from 192.168.20.253: seq=0 ttl=64 time=0.570 ms
64 bytes from 192.168.20.253: seq=1 ttl=64 time=0.334 ms
64 bytes from 192.168.20.253: seq=2 ttl=64 time=1.749 ms
64 bytes from 192.168.20.253: seq=3 ttl=64 time=0.276 ms
64 bytes from 192.168.20.253: seq=4 ttl=64 time=0.341 ms
^C
--- ns.zoneldavy.hier ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.276/0.654/1.749 ms
# _
```

Nu schakel ik de DNS-service van de zone1 server uit.

```
davy@zone1server:~$ sudo service bind9 stop
 * Stopping domain name service... bind9
waiting for pid 1538 to die

davy@zone1server:~$ sudo service bind9 status
 * bind9 is not running
davy@zone1server:~$
```

En probeer ik te pingen van cliënt 1 naar ns.zone2davy.hier.

```
davy@davyubuntu14:~$ ping ns.zone2davy.hier
PING ns.zone2davy.hier (192.168.21.253) 56(84) bytes of data.
64 bytes from 192.168.21.253: icmp_seq=1 ttl=63 time=0.460 ms
64 bytes from 192.168.21.253: icmp_seq=2 ttl=63 time=0.562 ms
64 bytes from 192.168.21.253: icmp_seq=3 ttl=63 time=0.574 ms
64 bytes from 192.168.21.253: icmp_seq=4 ttl=63 time=0.569 ms
64 bytes from 192.168.21.253: icmp_seq=5 ttl=63 time=0.581 ms
64 bytes from 192.168.21.253: icmp_seq=6 ttl=63 time=0.571 ms
^C
--- ns.zone2davy.hier ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 0.460/0.552/0.581/0.051 ms
davy@davyubuntu14:~$
```

Aangezien Ubuntu geen DNS-info cached weet ik dat er een nieuwe DNS-request is gebeurd.

Query log

We wensen de DNS-query's op onze server te loggen in het bestand "query.log". Hiervoor passen we het bestand "named.conf.options aan, en voegen we het logging-statement toe.

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                8.8.8.8;
                8.8.4.4;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};

logging {
channel simple_log {
        file "/var/log/query.log";
        severity debug 3;
        print-time yes;
};
category "queries" {
        simple_log;
};
```

Dit logging statement staat naast het options statement, en niet IN het options statement.

We moeten het bestand nog in de juiste directory aanmaken, en er voor zorgen dat dit bestand van de systeemuser "bind" is.

```
davy@zone1server:/etc/bind$ touch /var/log/query.log
touch: cannot touch '/var/log/query.log': Permission denied
davy@zone1server:/etc/bind$ sudo !!
sudo touch /var/log/query.log

davy@zone1server:/etc/bind$ sudo chown bind /var/log/query.log
davy@zone1server:/etc/bind$ cd /var/log/
davy@zone1server:/var/log$ ls -l q*
-rw-r--r-- 1 bind root 0 Mar  4 18:47 query.log
davy@zone1server:/var/log$
```

Ook moeten we het bestand “usr.sbin.named” aanmaken, zodat Apparmor geen fouten geeft. Dit bestand is een nieuw profiel in Apparmor.

```
davy@zone1server:/var/log$ cd /etc/apparmor.d/
davy@zone1server:/etc/apparmor.d$ ls
abstractions  disable        local          tunables       usr.sbin.rsyslogd
cache         force-complain sbin.dhclient  usr.sbin.named usr.sbin.tcpdump
davy@zone1server:/etc/apparmor.d$ cd local/
davy@zone1server:/etc/apparmor.d/local$ ls
README  sbin.dhclient  usr.sbin.named  usr.sbin.rsyslogd  usr.sbin.tcpdump
davy@zone1server:/etc/apparmor.d/local$ sudo vim usr.sbin.named
```

```
# Site-specific additions and overrides for usr.sbin.named.
# For more details, please see /etc/apparmor.d/local/README.
/var/log/query.log rw,
~
```

We laden het nieuwe Apparmor-profiel:

```
davy@zone1server:/etc/apparmor.d/local$ sudo apparmor_parser -r /etc/apparmor.d/usr.sbin.named
davy@zone1server:/etc/apparmor.d/local$
```

Apparmor is een beveiligingssysteem van de Linux-kernel, dat de rechten van programma’s regelt.

Nu doen we enkele DNS-request, en bekijken we daarna het log-bestand.

```
davy@zone1server:/etc/bind$ ping ns.zone1davy.hier
PING ns.zone1davy.hier (192.168.20.253) 56(84) bytes of data.
64 bytes from ns.zone1davy.hier (192.168.20.253): icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from ns.zone1davy.hier (192.168.20.253): icmp_seq=2 ttl=64 time=0.031 ms
64 bytes from ns.zone1davy.hier (192.168.20.253): icmp_seq=3 ttl=64 time=0.032 ms
64 bytes from ns.zone1davy.hier (192.168.20.253): icmp_seq=4 ttl=64 time=0.029 ms
^C
--- ns.zone1davy.hier ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.028/0.030/0.032/0.001 ms
davy@zone1server:/etc/bind$ cat /var/log/query.log
04-Mar-2015 19:43:23.125 client 127.0.0.1#40187 (ns.zone1davy.hier): query: ns.zone1davy.hier IN A + (127.0.0.1)
04-Mar-2015 19:43:23.126 client 127.0.0.1#57143 (253.20.168.192.in-addr.arpa): query: 253.20.168.192.in-addr.arp
a IN PTR + (127.0.0.1)
davy@zone1server:/etc/bind$
```

Mail-infrastructuur

Installatie Postfix

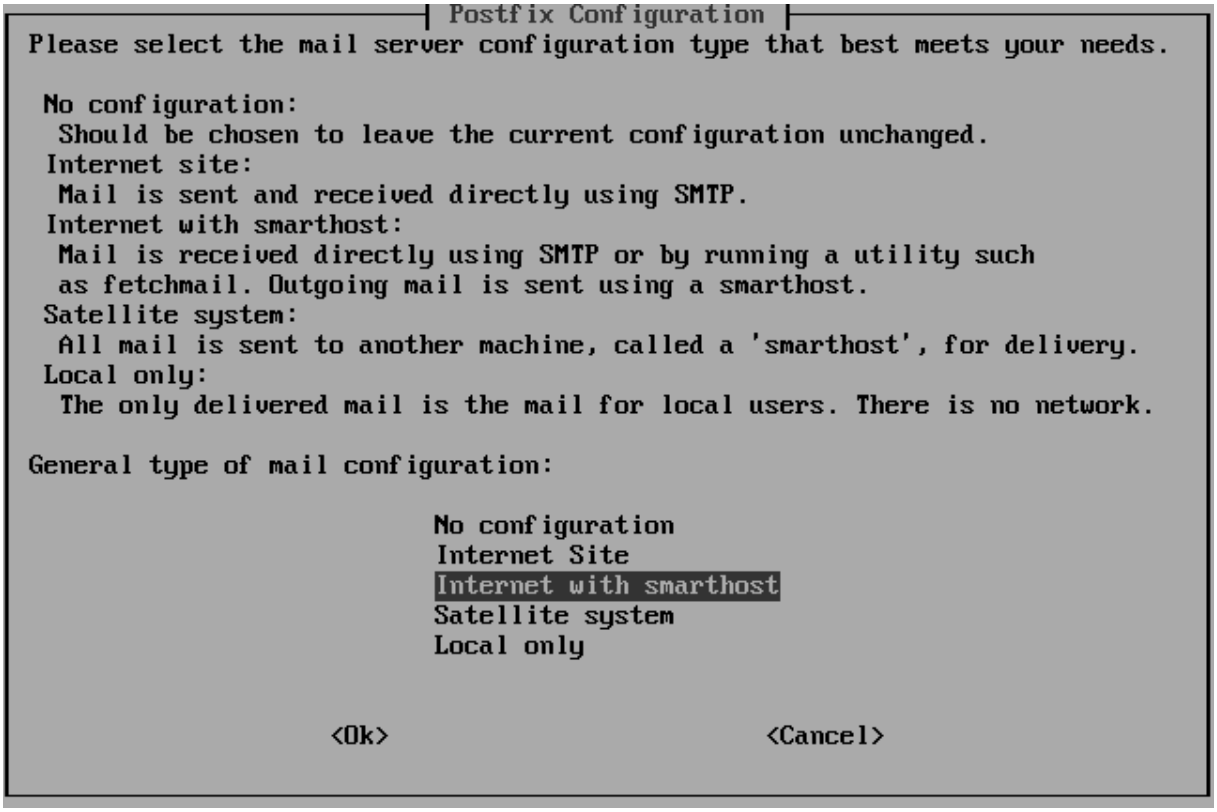
Om het gedeelte Postfix/Courrier/Squirrelmail op te lossen, hergebruik ik de zone 1-DNS server uit het hoofdstuk DNS.

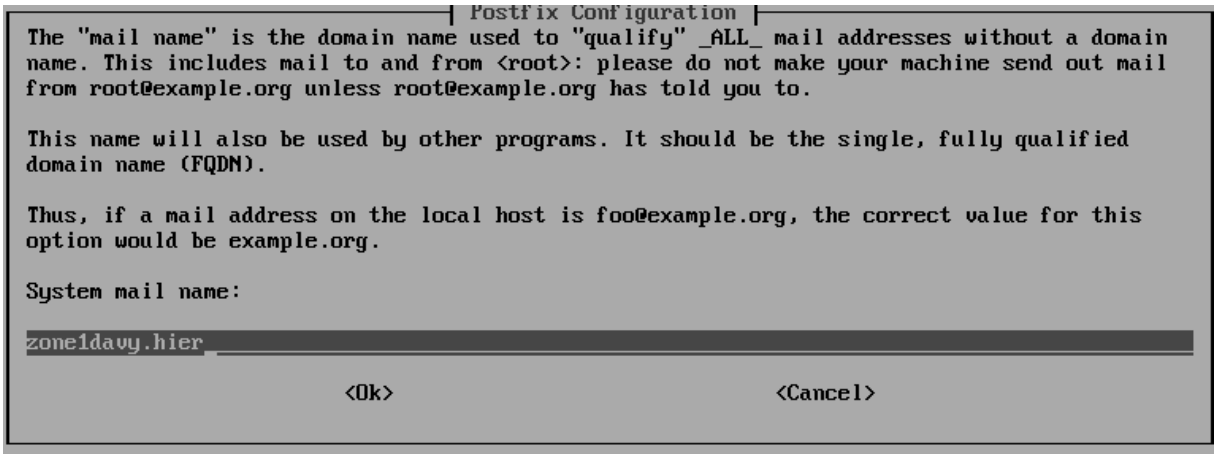
Eerst passen we onze DNS-records aan, we voegen een MX-record toe.

```
$TTL    604800
@       IN      SOA     ns.zone1davy.hier. admin.zone1davy.hier. (
                 2015021903             ; Serial
                  604800                ; Refresh
                   86400                ; Retry
                 2419200                ; Expire
                  604800 )              ; Negative Cache TTL
;
        IN      NS      ns
        IN      MX      10      mail
;
ns      IN      A       192.168.20.253
mail    IN      A       192.168.20.253
```

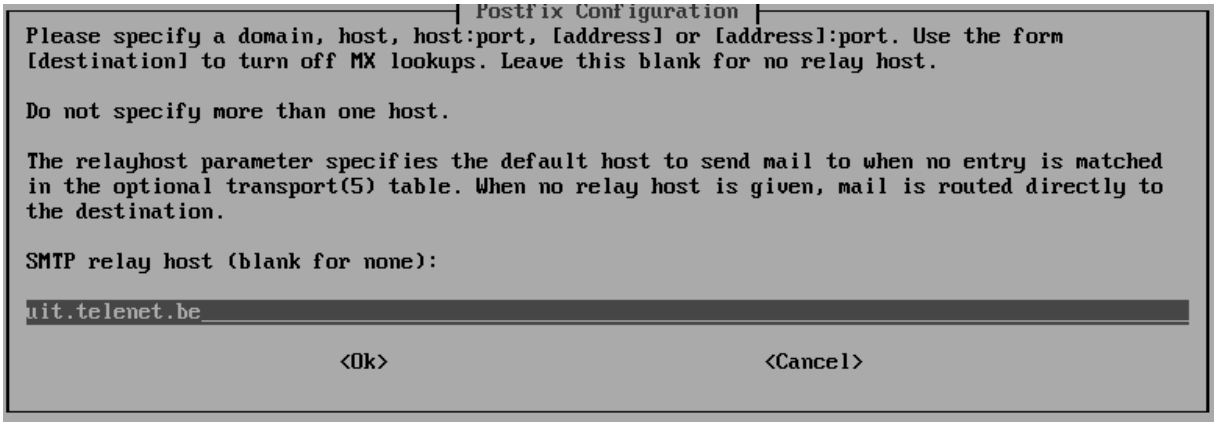
```
davy@zone1server:/etc/bind$ dig mx zone1davy.hier +short
10 mail.zone1davy.hier.
davy@zone1server:/etc/bind$
```

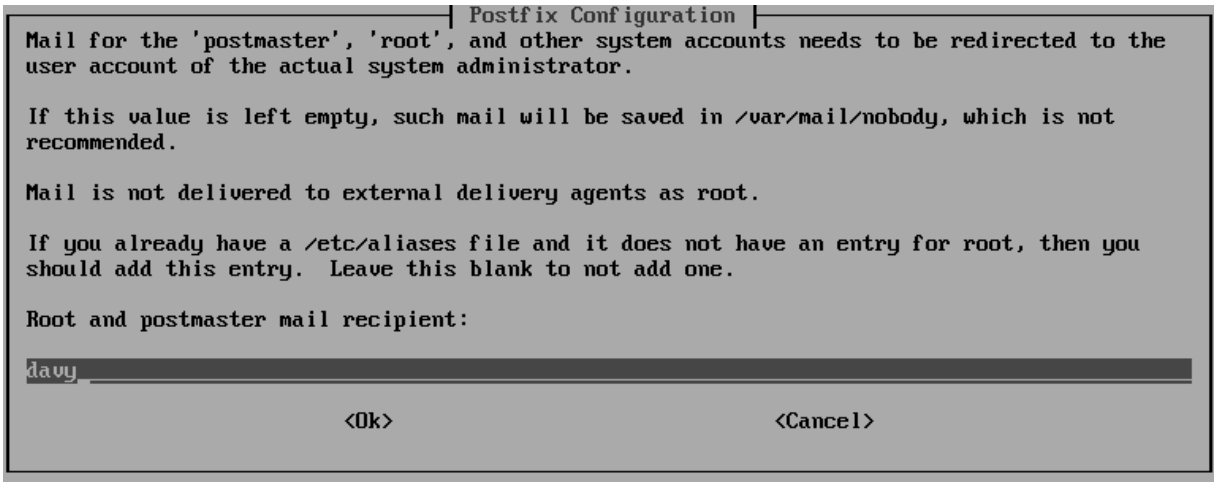
Daarna gaan we Postfix installeren (sudo apt-get install postfix postfix-docs)

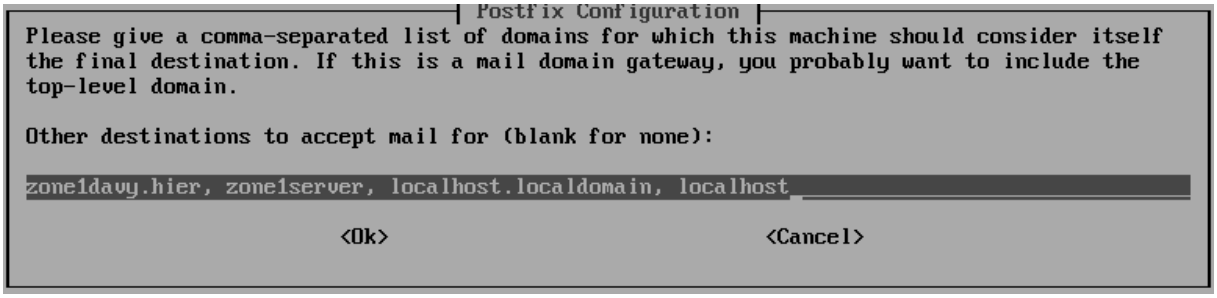


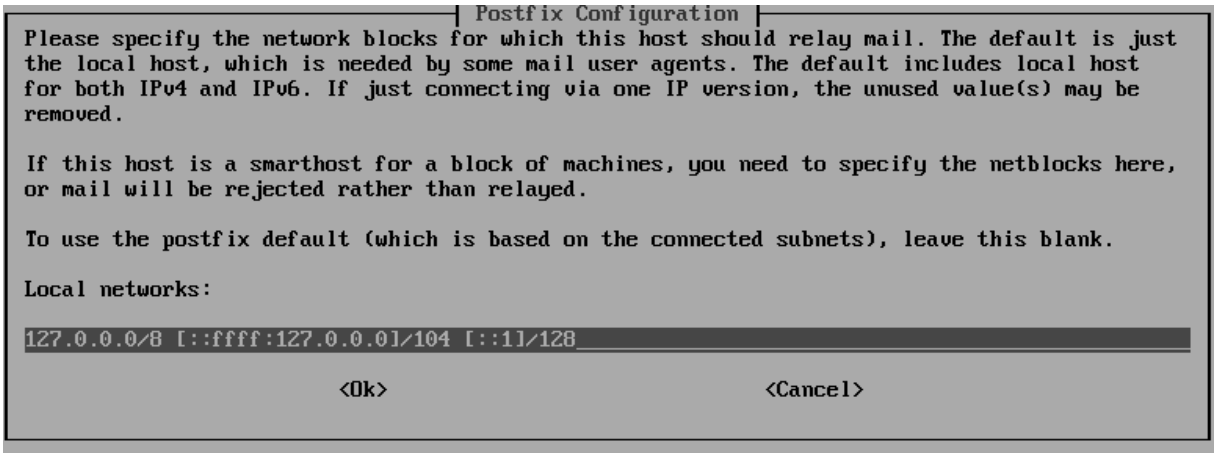


Hier geef ik de relay host van mijn ISP in, zodat het mogelijk zou moeten zijn om mail buiten onze virtuele omgeving te versturen.









Na de installatie voeren we een test uit. Op onderstaande screenshot zorg ik er eerst voor dat Postfix maildir gebruikt. Daarna maak ik een gebruiker “fmaster”.

```
davy@zone1server:~$ sudo postconf -e 'home_mailbox = Maildir/'
[sudo] password for davy:
davy@zone1server:~$ sudo useradd -m -s /bin/bash fmaster
davy@zone1server:~$ sudo passwd fmaster
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
davy@zone1server:~$
```

Nu ga ik verbinding maken met de mailserver via telnet, en een mail versturen naar fmaster.

```
davy@zone1server:~$ telnet mail.zone1davy.hier 25
Trying 192.168.20.253...
Connected to mail.zone1davy.hier.
Escape character is '^]'.
220 zone1server ESMTP Postfix (Ubuntu)
ehlo mail.zone1davy.hier
250-zone1server
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: admin@zone1davy.hier
250 2.1.0 Ok
rcpt to: fmaster@zone1davy.hier
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Testmail

Dit is een test
.
250 2.0.0 Ok: queued as 371F980A24
quit
221 2.0.0 Bye
Connection closed by foreign host.
davy@zone1server:~$ _
```

Nu de mail verzonden is, schakel ik met “su” over naar de account van fmaster, en controleer ik de mail. Dit doe ik door de inhoud van de map “new” in maildir te kijken. Mails staan daar opgeslagen in bestanden die je met “cat” kan bekijken.

```
davy@zone1server:~$ su - fmaster
Password:
fmaster@zone1server:~$ ls Maildir/new/
1424426887.V801I6066eM968226.zone1server
fmaster@zone1server:~$ cat Maildir/new/1424426887.V801I6066eM968226.zone1server
Return-Path: <admin@zone1davy.hier>
X-Original-To: fmaster@zone1davy.hier
Delivered-To: fmaster@zone1davy.hier
Received: from mail.zone1davy.hier (ns.zone1davy.hier [192.168.20.253])
        by zone1server (Postfix) with ESMTP id 371F980A24
        for <fmaster@zone1davy.hier>; Fri, 20 Feb 2015 11:07:14 +0100 (CET)
Subject: Testmail
Message-Id: <20150220100735.371F980A24@zone1server>
Date: Fri, 20 Feb 2015 11:07:14 +0100 (CET)
From: admin@zone1davy.hier

Dit is een test
fmaster@zone1server:~$ _
```

Mail versturen via de CLI

Intro

Om mails via commandline te versturen, heb ik een “Ubuntu Server” virtuele machine gebruikt. Op deze machine had ik Bind9 (domein zone1davy.hier) en Postfix geïnstalleerd.

Daarnaast had ik ook de packages mailutils en heirloom-mailx geïnstalleerd. Aangezien ik deze twee packages installeerde in het begin van de oefening, maakt het OS automatisch gebruik van mailx.

Bij de installatie van Postfix heb ik gekozen om mail op te slagen in de “Maildir”.

Met het commando “mail” verstuur ik een mail van mijn account (davy) naar een account die ik aan had gemaakt bij de installatie van postfix (fmaster).

De parameter **–s “Eerste mailtest”** stelt het onderwerp in van de mail, waarna de ontvanger volgt. Als we dan return drukken kunnen we het eigenlijke bericht typen. Om te eindigen en de mail te versturen, gebruiken we Ctrl-D

We kunnen ook de output van een commando als bericht gebruiken, door het pipe-teken te gebruiken.

```
davy@zone1server:~$ mail -s "Eerste mailtest" fmaster@zone1davy.hier
Dit is een eerste test van het mailcommando
EOT
davy@zone1server:~$ echo "Dit is het bericht van de tweede test" | mail -s "Tweede mailtest" fmaster
@zone1davy.hier
```

Om mails te lezen verander ik eerst van gebruiker met het commando “sudo su – fmaster” , waarna ik de inhoud van ~/Maildir/new/ bekijk.

Bestanden die daar in staan zijn mails, en die kunnen we met het “cat”-commando bekijken.

```
fmaster@zone1server:~/Maildir/new$ cat 1424445400.V801I60672M279980.zone1server
Return-Path: <davy@zone1davy.hier>
X-Original-To: fmaster@zone1davy.hier
Delivered-To: fmaster@zone1davy.hier
Received: by zone1server (Postfix, from userid 1000)
        id 41F3A80A3B; Fri, 20 Feb 2015 16:16:40 +0100 (CET)
Date: Fri, 20 Feb 2015 16:16:40 +0100
To: fmaster@zone1davy.hier
Subject: Eerste mailtest
User-Agent: Heirloom mailx 12.5 6/20/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20150220151640.41F3A80A3B@zone1server>
From: davy@zone1davy.hier (davy)

Dit is een eerste test van het mailcommando


fmaster@zone1server:~/Maildir/new$ ls
1424426887.V801I6066eM968226.zone1server  1424445486.V801I60673M32910.zone1server
1424445400.V801I60672M279980.zone1server
fmaster@zone1server:~/Maildir/new$ cat 1424445486.V801I60673M32910.zone1server
Return-Path: <davy@zone1davy.hier>
X-Original-To: fmaster@zone1davy.hier
Delivered-To: fmaster@zone1davy.hier
Received: by zone1server (Postfix, from userid 1000)
        id 0739780A3B; Fri, 20 Feb 2015 16:18:05 +0100 (CET)
Date: Fri, 20 Feb 2015 16:18:05 +0100
To: fmaster@zone1davy.hier
Subject: Tweede mailtest
User-Agent: Heirloom mailx 12.5 6/20/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20150220151806.0739780A3B@zone1server>
From: davy@zone1davy.hier (davy)

Dit is het bericht van de tweede test
fmaster@zone1server:~/Maildir/new$ _
```

Zoals we hierboven zien, is hier heirloom mailx gebruikt.

Carbon Copy

Als men als parameter –c of –b opgeeft, gevolgd door een bestemmeling, stuurt men een “carbon copy” of een “blind carbon copy” mail.

```
davy@zone1server:~$ mail -s "Vierde test" fmaster@zone1davy.hier -c davy@zone1server
Dit is een cc test
EOT
davy@zone1server:~$ ls
dead.letter  Maildir
davy@zone1server:~$ ls Maildir/new
1424446541.V801I60677M861082.zone1server
davy@zone1server:~$ cat Maildir/new/1424446541.V801I60677M861082.zone1server
Return-Path: <davy@zone1davy.hier>
X-Original-To: davy@zone1server
Delivered-To: davy@zone1server
Received: by zone1server (Postfix, from userid 1000)
        id CFD2180A3B; Fri, 20 Feb 2015 16:35:41 +0100 (CET)
Date: Fri, 20 Feb 2015 16:35:41 +0100
To: davy@zone1server, -c@zone1davy.hier, fmaster@zone1davy.hier
Subject: Vierde test
User-Agent: Heirloom mailx 12.5 6/20/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20150220153541.CFD2180A3B@zone1server>
From: davy@zone1davy.hier (davy)

Dit is een cc test
davy@zone1server:~$
```

Lokale mail

Het mail-commando laat ons ook toe om een mail te sturen naar lokale gebruiker, door in plaats van een mailadres een gebruikersnaam op te geven als bestemmeling.

```
davy@zone1server:~$ echo "Dit is een bericht voor jan" | mail -s "Hallo jan" jan
davy@zone1server:~$ sudo su - jan
[sudo] password for davy:
jan@zone1server:~$ cat Maildir/new/1424447636.V801I6067eM72724.zone1server
Return-Path: <davy@zone1davy.hier>
X-Original-To: jan
Delivered-To: jan@zone1davy.hier
Received: by zone1server (Postfix, from userid 1000)
        id 0C72980A3B; Fri, 20 Feb 2015 16:53:56 +0100 (CET)
Date: Fri, 20 Feb 2015 16:53:55 +0100
To: jan@zone1davy.hier
Subject: Hallo jan
User-Agent: Heirloom mailx 12.5 6/20/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20150220155356.0C72980A3B@zone1server>
From: davy@zone1davy.hier (davy)

Dit is een bericht voor jan
jan@zone1server:~$
```

Header-info

Het is mogelijk om header-informatie aan te passen door de parameter –r te gebruiken. In onderstaand voorbeeld pas ik de zender aan van de mail.

```
davy@zone1server:~$ echo "Help me with Ukraine" | mail -s "Hilfe" -r "Angela<angela.merkel@deutschla
nd.de>" fmaster@zone1davy.hier
davy@zone1server:~$ sudo su - fmaster
fmaster@zone1server:~$ ls Maildir/new/
1424426887.V801I6066eM968226.zone1server  1424446541.V801I6067aM864145.zone1server
1424445400.V801I60672M279980.zone1server  1424447352.V801I6067bM264397.zone1server
1424445486.V801I60673M32910.zone1server   1424448167.V801I60681M464945.zone1server
fmaster@zone1server:~$ ls -l Maildir/new/
total 24
-rw------- 1 fmaster fmaster 461 Feb 20 11:08 1424426887.V801I6066eM968226.zone1server
-rw------- 1 fmaster fmaster 570 Feb 20 16:16 1424445400.V801I60672M279980.zone1server
-rw------- 1 fmaster fmaster 564 Feb 20 16:18 1424445486.V801I60673M32910.zone1server
-rw------- 1 fmaster fmaster 578 Feb 20 16:35 1424446541.V801I6067aM864145.zone1server
-rw------- 1 fmaster fmaster 541 Feb 20 16:49 1424447352.V801I6067bM264397.zone1server
-rw------- 1 fmaster fmaster 573 Feb 20 17:02 1424448167.V801I60681M464945.zone1server
fmaster@zone1server:~$ cat Maildir/new/1424448167.V801I60681M464945.zone1server
Return-Path: <angela.merkel@deutschland.de>
X-Original-To: fmaster@zone1davy.hier
Delivered-To: fmaster@zone1davy.hier
Received: by zone1server (Postfix, from userid 1000)
        id 6F4A080A3B; Fri, 20 Feb 2015 17:02:47 +0100 (CET)
Date: Fri, 20 Feb 2015 17:02:47 +0100
From: Angela<angela.merkel@deutschland.de>
To: fmaster@zone1davy.hier
Subject: Hilfe
Message-ID: <54e75aa7.WYubyesrvXBfEGFi%angela.merkel@deutschland.de>
User-Agent: Heirloom mailx 12.5 6/20/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

Help me with Ukraine
fmaster@zone1server:~$
```

Attachments

Met mailx kan men ook bestanden als attachments versturen. Dit kan met de –a parameter.

```
davy@zone1server:~$ echo "Dit is een mail met attachment" | mail -s "mail met attachment" -a ~/besta
nd.txt fmaster@zone1davy.hier
davy@zone1server:~$
```

```
fmaster@zone1server:~$ cat Maildir/new/1424449956.V801I60683M546379.zone1server
Return-Path: <davy@zone1davy.hier>
X-Original-To: fmaster@zone1davy.hier
Delivered-To: fmaster@zone1davy.hier
Received: by zone1server (Postfix, from userid 1000)
        id 82F9180A3B; Fri, 20 Feb 2015 17:32:36 +0100 (CET)
Date: Fri, 20 Feb 2015 17:32:36 +0100
To: fmaster@zone1davy.hier
Subject: mail met attachment
User-Agent: Heirloom mailx 12.5 6/20/10
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="=_54e761a4.u5IQ8r2WHcsJ4BuV4+GqE8RIJrjz0tjhlequWpuvPER8hV65"
Message-Id: <20150220163236.82F9180A3B@zone1server>
From: davy@zone1davy.hier (davy)

This is a multi-part message in MIME format.

--=_54e761a4.u5IQ8r2WHcsJ4BuV4+GqE8RIJrjz0tjhlequWpuvPER8hV65
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Content-Disposition: inline

Dit is een mail met attachment

--=_54e761a4.u5IQ8r2WHcsJ4BuV4+GqE8RIJrjz0tjhlequWpuvPER8hV65
Content-Type: text/plain;
 charset=us-ascii
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
 filename="bestand.txt"
```

Courier

De installatie van Courier gaat zeer gemakkelijk: men voert gewoon "`apt-get install courier-imap courier-doc courier_authdaemon`". Daarmee is de installatie gebeurd.

Via telnet kunnen we controleren of onze installatie gelukt is.

```
davy@zone1server:~$ telnet localhost imap
Trying ::1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THRE
AD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION] Courier-IMAP ready. Copyright 1998
-2011 Double Precision, Inc.  See COPYING for distribution information.
1 login fmaster geheim
1 OK LOGIN Ok.
2 select "Inbox"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS (\* \Draft \Answered \Flagged \Deleted \Seen)] Limited
* 8 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 428838831] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
2 OK [READ-WRITE] Ok
3 logout
* BYE Courier-IMAP server shutting down
3 OK LOGOUT completed
Connection closed by foreign host.
davy@zone1server:~$
```

Let wel op, het cijfer voor de gegeven commando's moet men zelf ingeven, bijvoorbeeld "1 login fmaster geheim".

Aliassen

We gaan ook een alias toevoegen aan onze mailserver. We voegen eerst een gebruiker toe aan ons systeem, waarna we deze als alias vermelden in het bestand /etc/aliases.

```
davy@zone1server:~$ sudo useradd -m -s /bin/bash mailadmin
davy@zone1server:~$ sudo passwd mailadmin
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
davy@zone1server:~$ sudo vim /etc/aliases
davy@zone1server:~$ sudo newaliases
davy@zone1server:~$ sudo postfix reload
[sudo] password for davy:
postfix/postfix-script: refreshing the Postfix mail system
davy@zone1server:~$
```

Het commando "newaliases" en "postfix reload" is daarna nodig om de wijzigingen toe te passen.

```
davy@zone1server:~$ sudo cat /etc/aliases
# See man 5 aliases for format
postmaster:    root
davy: mailadmin
davy@zone1server:~$
```

Hierna merkte ik dat de alias niet werkte: mails kwamen terecht in de maildirectory van de gebruiker “mailadmin”, maar ze waren niet te zien in de map van “davy”.

Ik verstuurde via telnet een mail:

```
Escape character is '^]'.
220 zone1server ESMTP Postfix (Ubuntu)
ehlo localhost
250-zone1server
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: fmaster@zone1davy.hier
250 2.1.0 Ok
rcpt to: mailadmin@zone1davy.hier
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: final alias test
```

Maar deze was niet te zien in de maildirectory van “davy”. In de maildirectory van “mailadmin” daarentegen kwamen wel mails aan:

```
mailadmin@zone1server:~/Maildir/new$ cat 1428896837.V801I60691M345909.zone1server
Return-Path: <fmaster@zone1davy.hier>
X-Original-To: mailadmin
Delivered-To: mailadmin@zone1davy.hier
Received: from localhost (localhost [IPv6:::1])
        by zone1server (Postfix) with ESMTP id 1AEBC809AA
        for <mailadmin>; Mon, 13 Apr 2015 05:46:51 +0200 (CEST)
Subject: laatste test
Message-Id: <20150413034700.1AEBC809AA@zone1server>
Date: Mon, 13 Apr 2015 05:46:51 +0200 (CEST)
From: fmaster@zone1davy.hier

test van alias

mailadmin@zone1server:~/Maildir/new$
```

Uiteindelijk bleek dit te wijten aan een vergissing van mezelf. In het bestand /etc/aliases had ik eerst “davy: mailadmin” geschreven, terwijl dit omgekeerd moest zijn:

```
davy@zone1server:~$ sudo cat /etc/aliases
# See man 5 aliases for format
postmaster:    root
mailadmin: davy
davy@zone1server:~$
```

Daarna kon ik wel mails, bestemd voor mailadmin, in de directory van davy vinden:

```
davy@zone1server:~$ cd Maildir/
davy@zone1server:~/Maildir$ cd new/
davy@zone1server:~/Maildir/new$ ls
1424446541.V801I60677M861082.zone1server  1428904854.V801I6068bM168493.zone1server
davy@zone1server:~/Maildir/new$ ls -l
total 8
-rw------- 1 davy davy 566 Feb 20 16:35 1424446541.V801I60677M861082.zone1server
-rw------- 1 davy davy 422 Apr 13 08:00 1428904854.V801I6068bM168493.zone1server
davy@zone1server:~/Maildir/new$ cat 1428904854.V801I6068bM168493.zone1server
Return-Path: <fmaster@zone1davy.hier>
X-Original-To: mailadmin
Delivered-To: mailadmin@zone1davy.hier
Received: from localhost (localhost [IPv6:::1])
        by zone1server (Postfix) with ESMTP id D6DF380B20
        for <mailadmin>; Mon, 13 Apr 2015 08:00:23 +0200 (CEST)
Subject: allerlaatste test
Message-Id: <20150413060032.D6DF380B20@zone1server>
Date: Mon, 13 Apr 2015 08:00:23 +0200 (CEST)
From: fmaster@zone1davy.hier
```

Fetchmail

Na de installatie van fetchmail moeten we in het bestand /etc/default/fetchmail de optie voor het automatisch opstarten aanzetten:

```
# This file will be used to declare some vars for fetchmail
#
# Uncomment the following if you don't want localized log messages
# export LC_ALL=C

# If you want to specify any additional OPTION to the start
# scripts specify them here
# OPTIONS=...

# Declare here if we want to start fetchmail. 'yes' or 'no'
START_DAEMON=yes
~
```

Daarna moeten we het bestand /etc/.fetchmailrc aanmaken. Hierin komt de configuratie van fetchmail:

```
davy@zone1server:~$ sudo cat /etc/.fetchmailrc
set daemon 180 set postmaster "davy"
set syslog
poll imap.telenet.be protocol imap: username "davy.van.eynde@telenet.be" password "[redacted]" is davy
 here
davy@zone1server:~$
```

In dit configuratiebestand stel ik in dat er om de 180 seconden gepolld moet worden, dat de postmaster hier systeemaccount “davy” is, en dat de syslog gebruikt moet worden om te loggen.

Daarna geef ik de gegevens mee van mijn telenet-imap account, en verbindt die aan de systeemaccount “davy”.

Als men daarna het commando “`newaliases`” uitvoert, en postfix herstart, zou alles moeten werken.

Volgens documentatie die ik terugvond, kan men daarna met het commando “`fetchmail`” mail ophalen, maar dit leek niet te werken

```
davy@zone1server:/etc$ fetchmail
fetchmail: no mailservers have been specified.
davy@zone1server:/etc$
```

Squirrelmail

Na de installatie met apt-get, voeren we het commando "`squirrelmail-configure`" uit

```
Installing default squirrelmail config.
Run /usr/sbin/squirrelmail-configure as root to configure/
Setting up squirrelmail-locales (1.4.18-20090526-1) ...
Setting up squirrelmail-viewashtml (3.8-3) ...
Removing plugin view_as_html
Data saved in config.php
Activating plugin view_as_html
Data saved in config.php
Processing triggers for libc-bin (2.19-0ubuntu6) ...
davy@zone1server:~$ sudo squirrelmail-configure
```

Met dit commando kunnen we Squirrelmail configureren. Hier doe ik momenteel gewoon een kleine personalisatie.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> 1
```

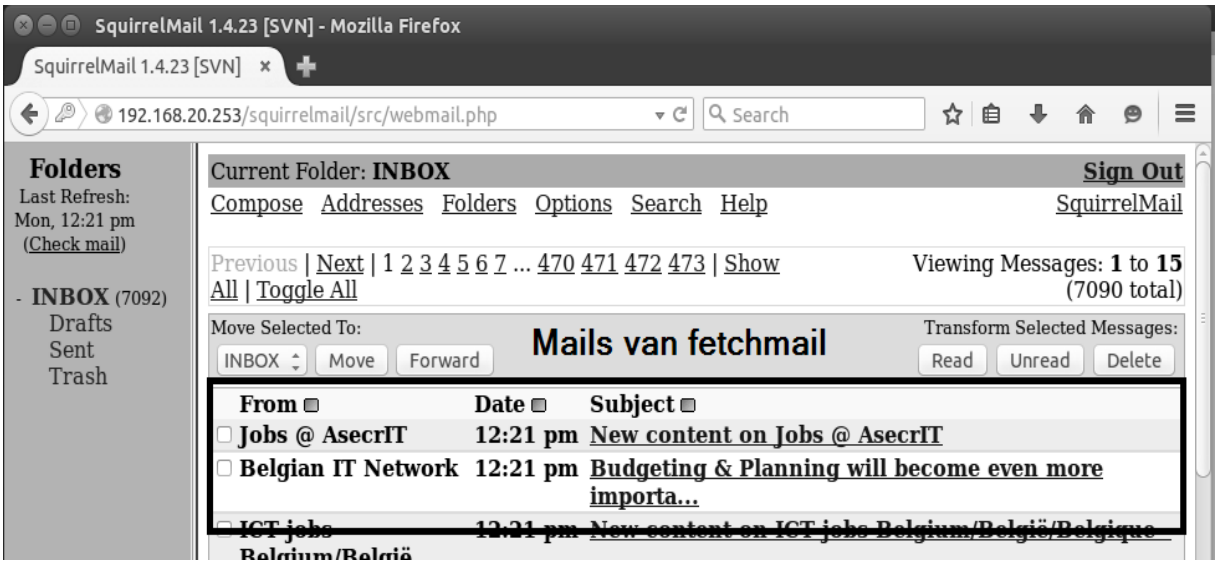
```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Organization Preferences
1.  Organization Name      : SquirrelMail
2.  Organization Logo      : ../images/sm_logo.png
3.  Org. Logo Width/Height : (308/111)
4.  Organization Title     : SquirrelMail $version
5.  Signout Page           :
6.  Top Frame              : _top
7.  Provider link          : http://squirrelmail.org/
8.  Provider name          : SquirrelMail

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> 1
```

Na de configuratie moeten we Squirrelmail nog toevoegen aan Apache als virtual host. Na onderstaande screenshot werkte Squirrelmail nog niet, omdat ik vergeten was de site actief te zetten met a2ensite.

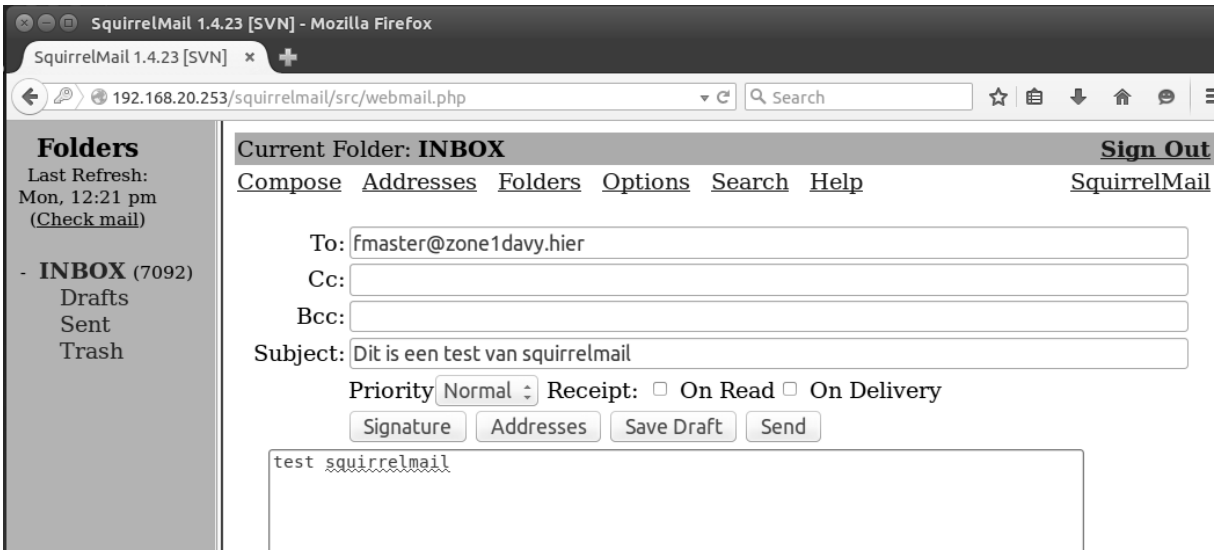
```
davy@zone1server:~$ sudo cp /etc/squirrelmail/apache.conf /etc/apache2/sites-available/squirrelmail
.conf
[sudo] password for davy:
davy@zone1server:~$ sudo service apache2 restart
 * Restarting web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.
0.1.1. Set the 'ServerName' directive globally to suppress this message
                                                                                          [ OK ]
davy@zone1server:~$
```

Nu kunnen we gaan testen. Ik log in met de systeemaccount “davy”:

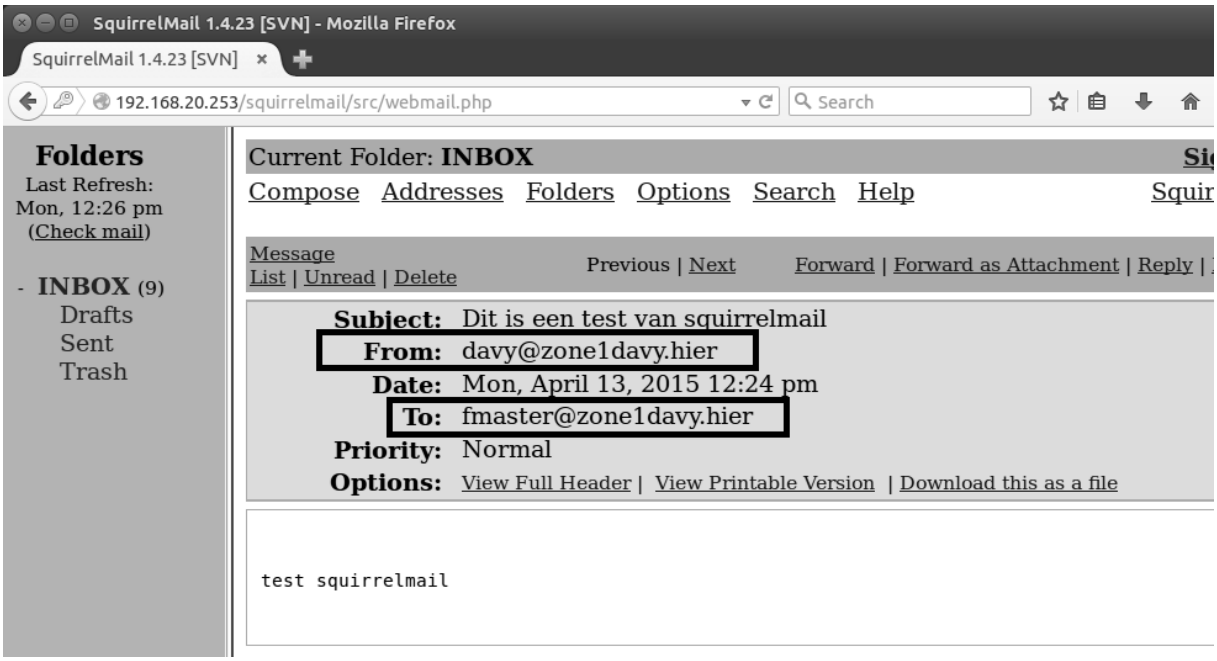
Als we ingelogd zijn, blijkt dat fetchmail wel zijn werk doet:



We gaan ook een mail versturen naar iemand anders:



Waarna we controleren of de mail is aangekomen.


SquirrelMail 1.4.23 [SVN] - Mozilla Firefox
SquirrelMail 1.4.23 [SVN]
192.168.20.253/squirrelmail/src/webmail.php
Search
Folders
Last Refresh:
Mon, 12:26 pm
(Check mail)
- INBOX (9)
Drafts
Sent
Trash
Current Folder: INBOX
Compose Addresses Folders Options Search Help
Message
List | Unread | Delete
Previous | Next
Forward | Forward as Attachment | Reply |
Subject: Dit is een test van squirrelmail
From: davy@zone1davy.hier
Date: Mon, April 13, 2015 12:24 pm
To: fmaster@zone1davy.hier
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file
test squirrelmail

Axigen

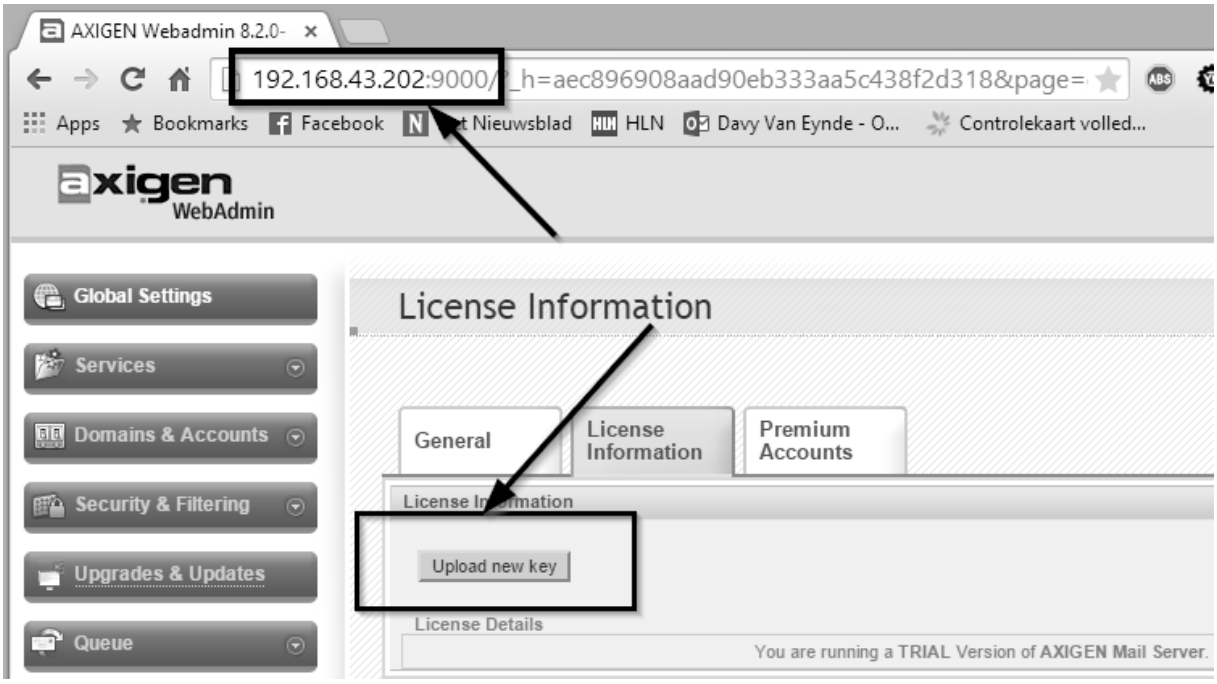
Intro

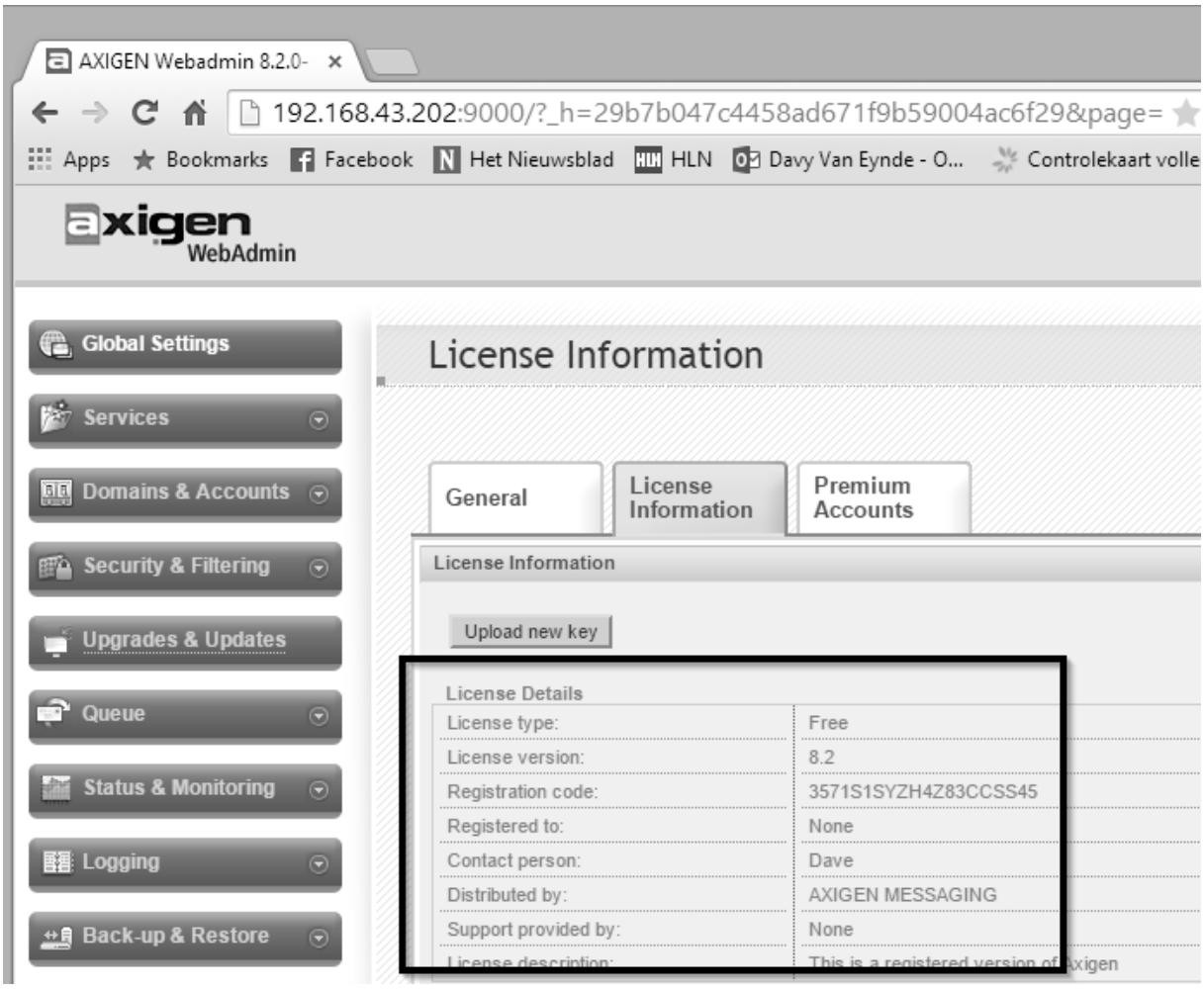
Axigen is een mailserver met webmail, webmin-paneel,… ingebouwd. In plaats van apart Postfix, Courier en Squirrelmail te installeren kan men één pakket installeren, namelijk Axigen.

Als men de gratis versie van Axigen wilt downloaden moet men zich inschrijven. Na het inschrijven kan men het installatiepakket downloaden en krijgt men een licentie-sleutel.

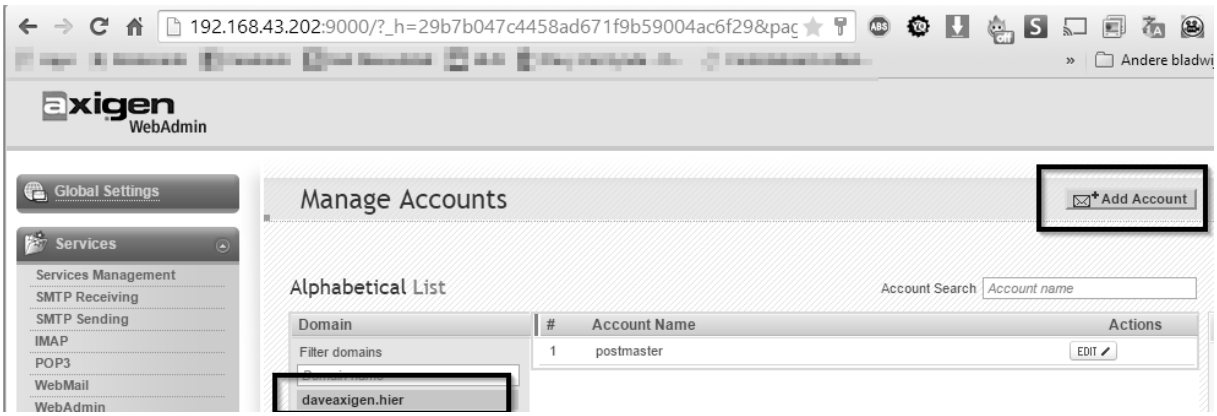
Tijdens het testen merkte ik dat er enkele zaken niet meer mogelijk waren met de huidige versie (8.2). Onder andere gedeelde mappen en gedeelde kalenders leken niet mogelijk.

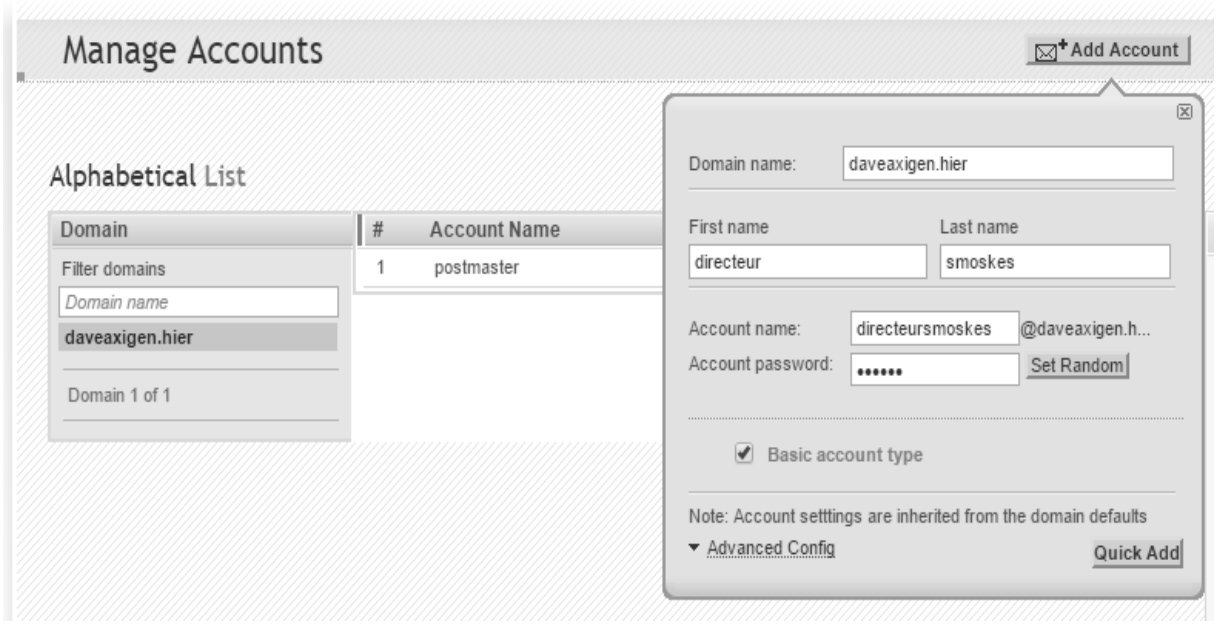
Na de installatie van Axigen kan men de licentie-sleutel uploaden.



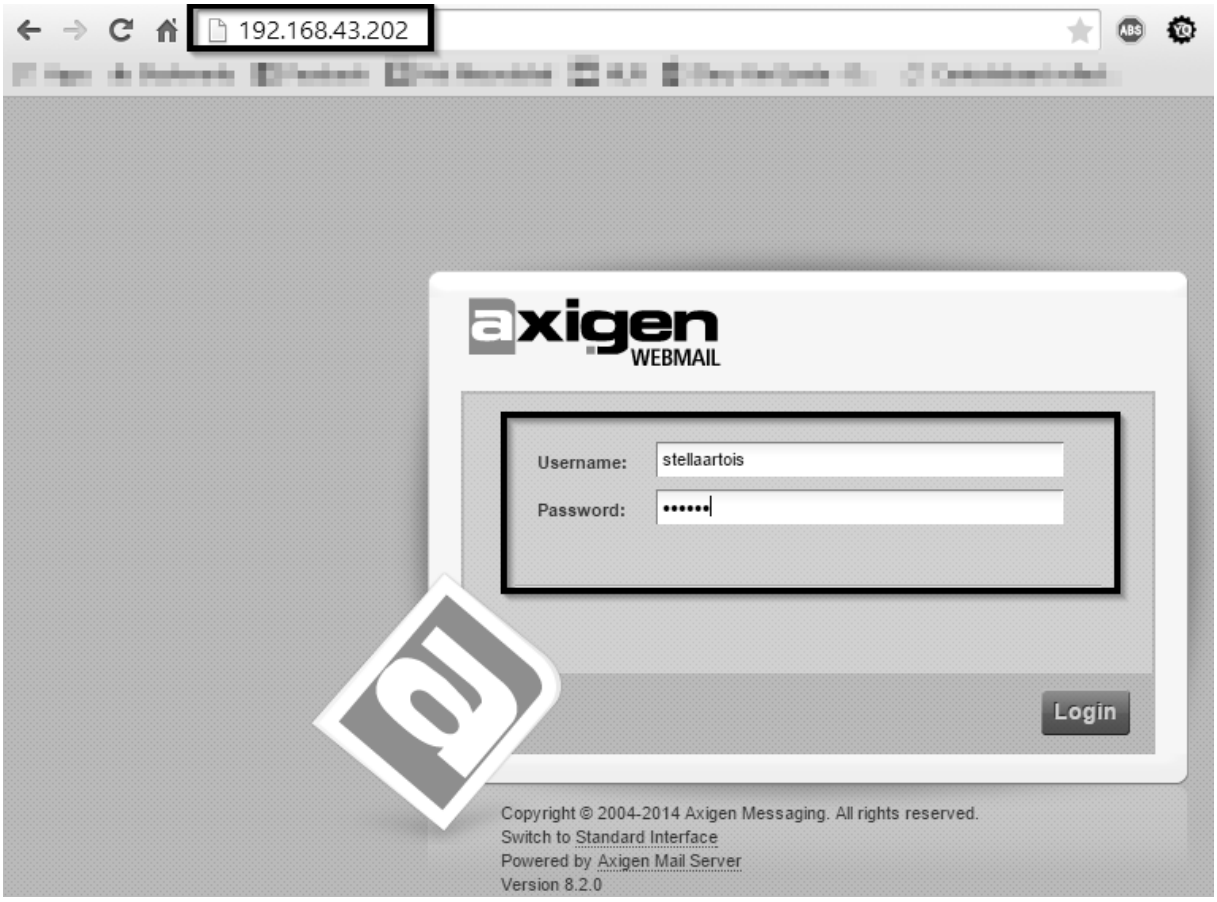

AXIGEN Webadmin 8.2.0-
192.168.43.202:9000/?_h=29b7b047c4458ad671f9b59004ac6f29&page=
Apps
Bookmarks
Facebook
Het Nieuwsblad
HLN
Davy Van Eynde - O...
Controlekaart volle
axigen
WebAdmin
Global Settings
Services
Domains & Accounts
Security & Filtering
Upgrades & Updates
Queue
Status & Monitoring
Logging
Back-up & Restore
License Information
General
License Information
Premium Accounts
License Information
Upload new key
License Details
License type: Free
License version: 8.2
Registration code: 3571S1SYZH4Z83CCSS45
Registered to: None
Contact person: Dave
Distributed by: AXIGEN MESSAGING
Support provided by: None
License description: This is a registered version of Axigen

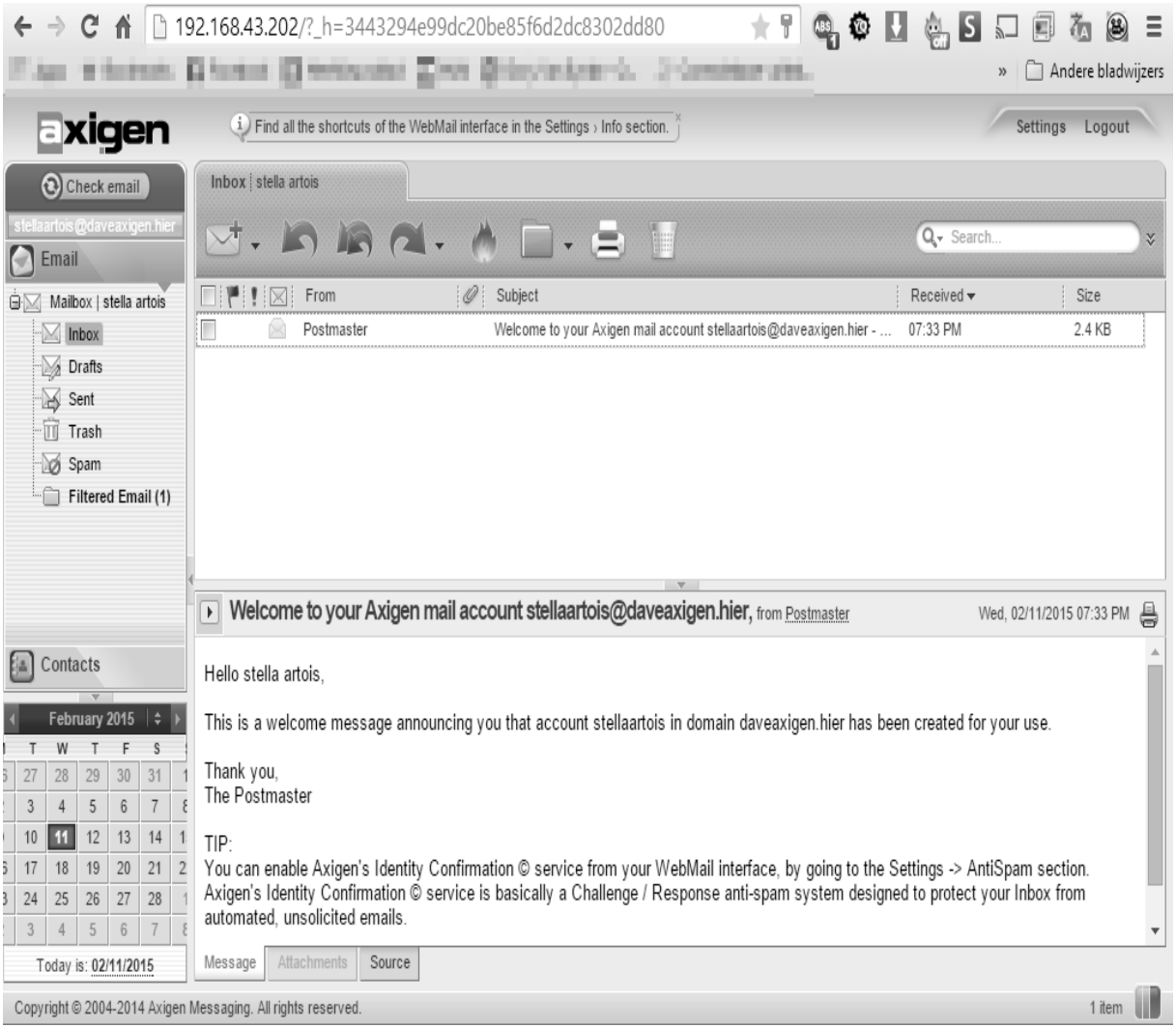
Eerst maakt men een domein aan via het administratiepaneel, waarna men accounts kan aanmaken.



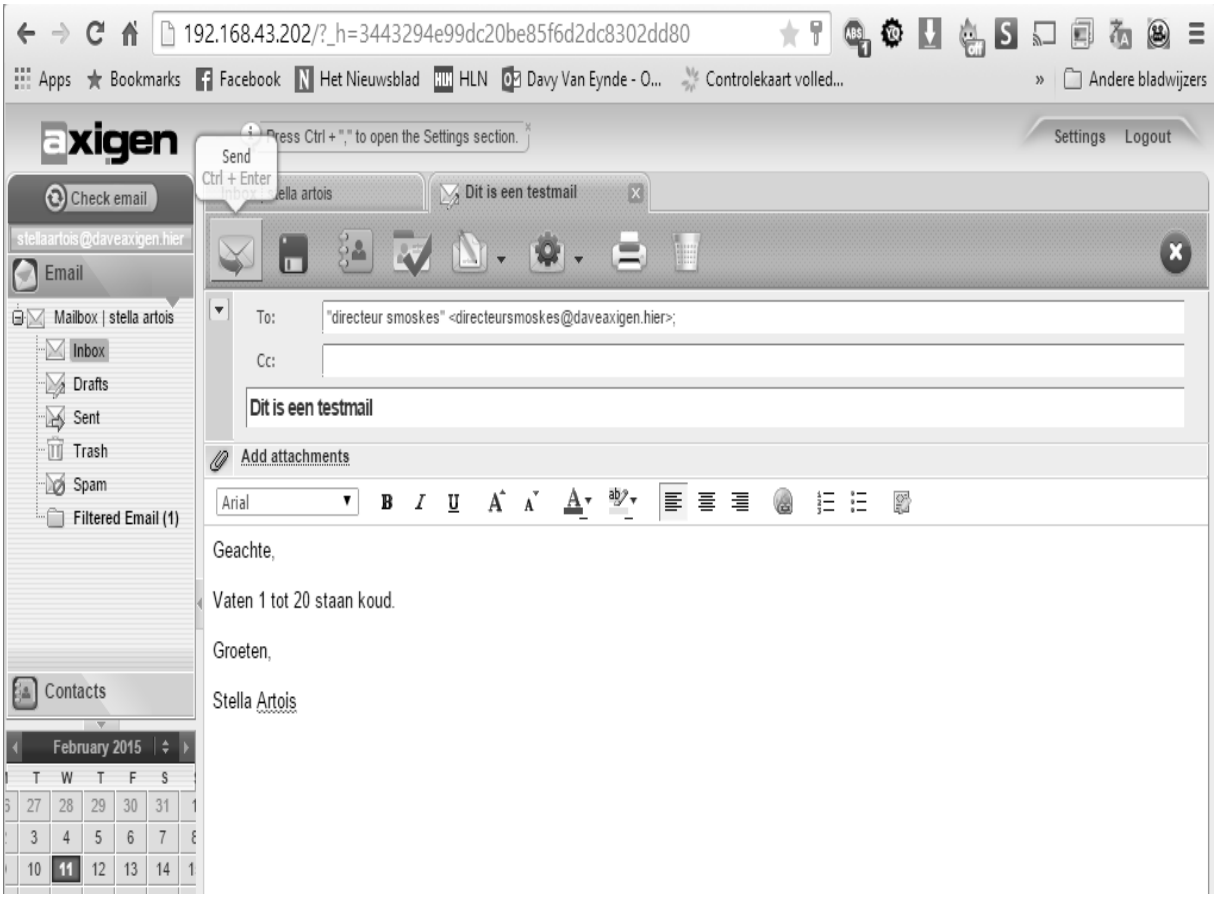


Via de aangemaakte accounts kan men dan inloggen en mail versturen.

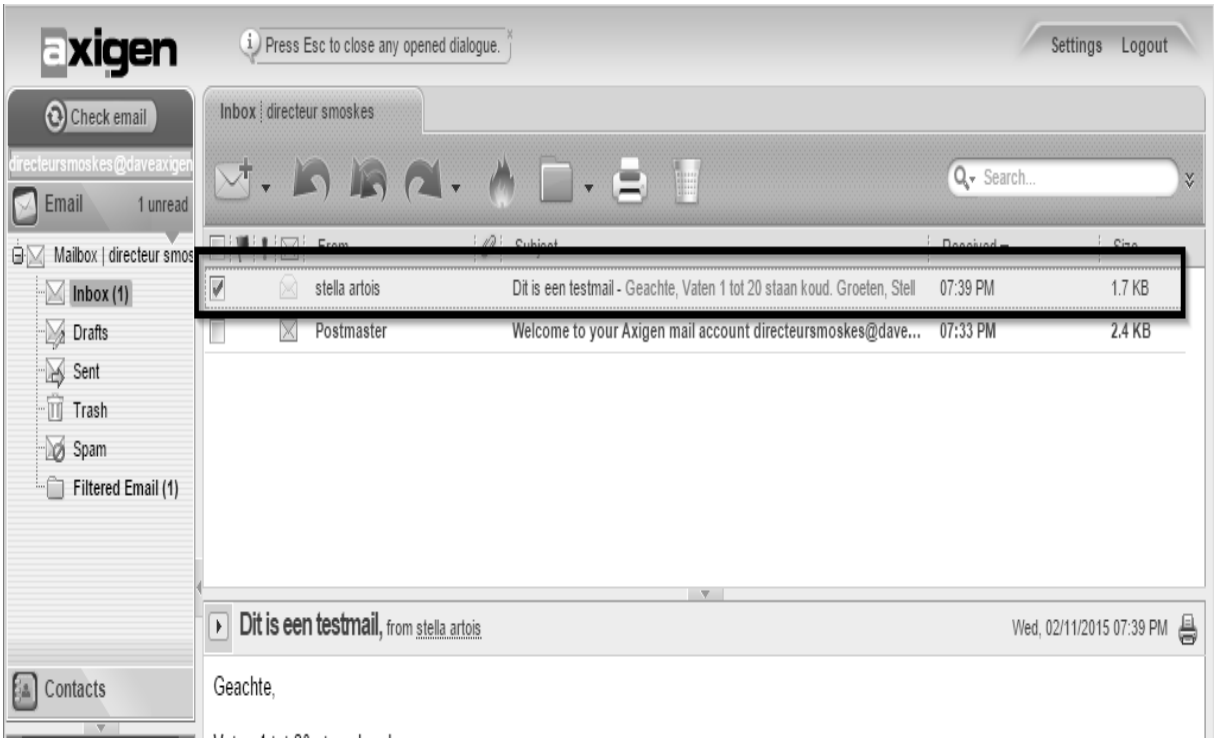




We versturen een mail van de stella-account naar de directeur-account:

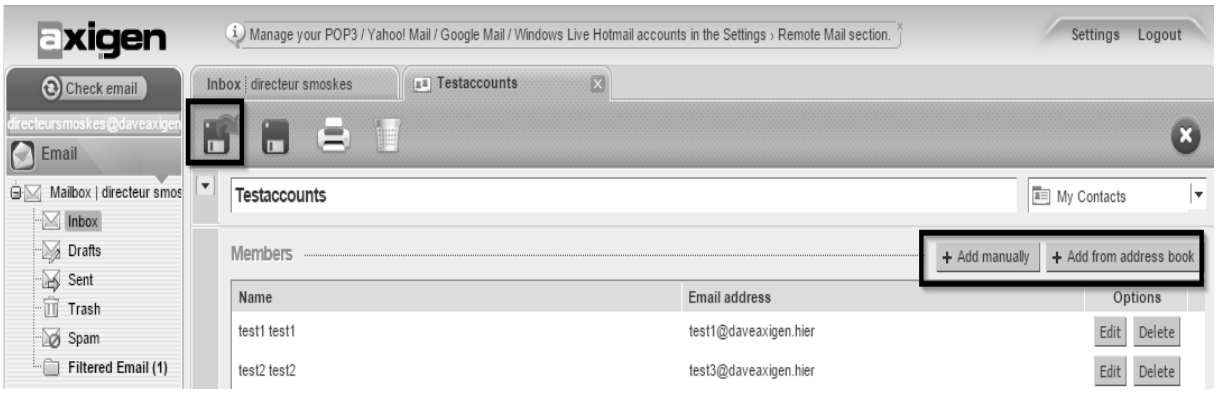

192.168.43.202/?_h=3443294e99dc20be85f6d2dc8302dd80
Apps
Bookmarks
Facebook
Het Nieuwsblad
HLN
Davy Van Eynde - O...
Controlekaart volled...
Andere bladwijzers
axigen
Press Ctrl + "," to open the Settings section.
Settings
Logout
Send
Ctrl + Enter
Check email
stellaartois@daveaxigen.hier
Email
Mailbox | stella artois
Inbox
Drafts
Sent
Trash
Spam
Filtered Email (1)
Contacts
February 2015
Dit is een testmail
To:
"directeur smoskes" <directeursmoskes@daveaxigen.hier>;
Cc:
Dit is een testmail
Add attachments
Arial
Geachte,
Vaten 1 tot 20 staan koud.
Groeten,
Stella Artois

Waarna we natuurlijk controleren of de mail is aangekomen op de directeur-account:

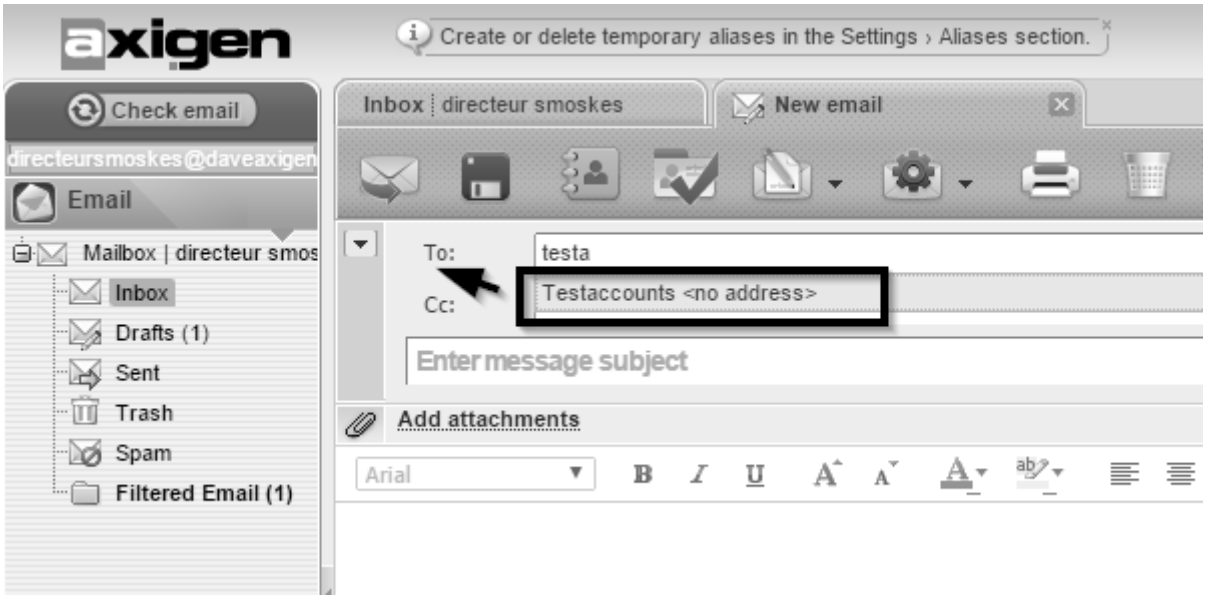


Distributielijst

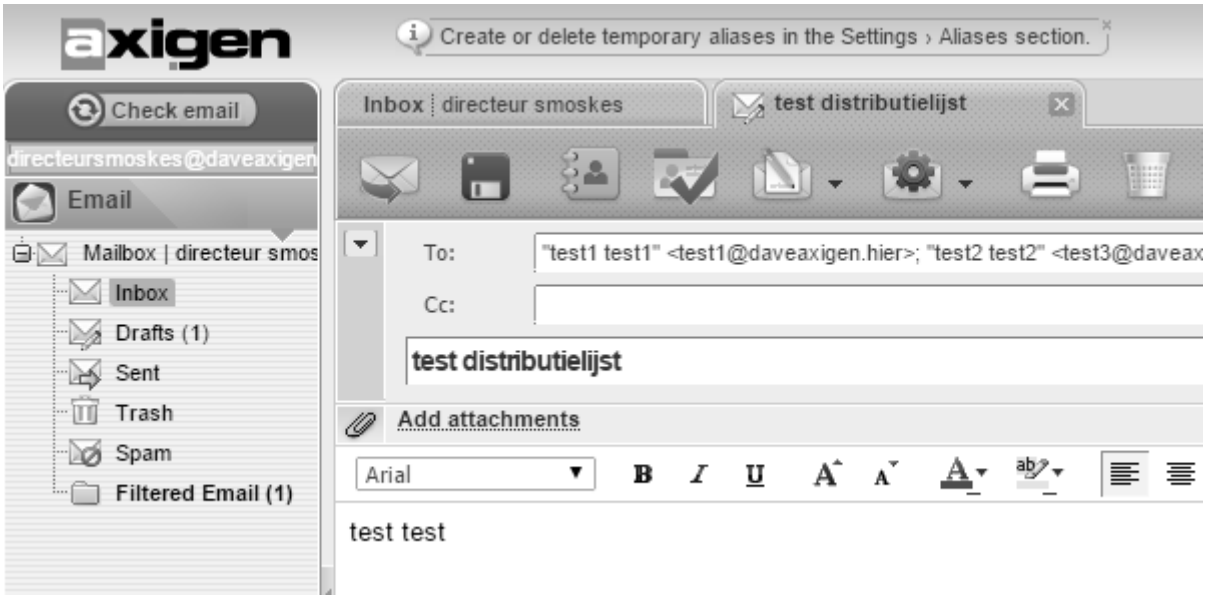
Een distributielijst kan men zien als een soort van “alias” voor meerdere adressen. Als men een mail stuurt naar dat alias komt de mail aan bij alle onderliggende adressen. Deze worden per account ingesteld, en worden dus op de webmail interface gemaakt.



Zeker niet vergeten op de save-button te klikken als je distributielijst klaar is.

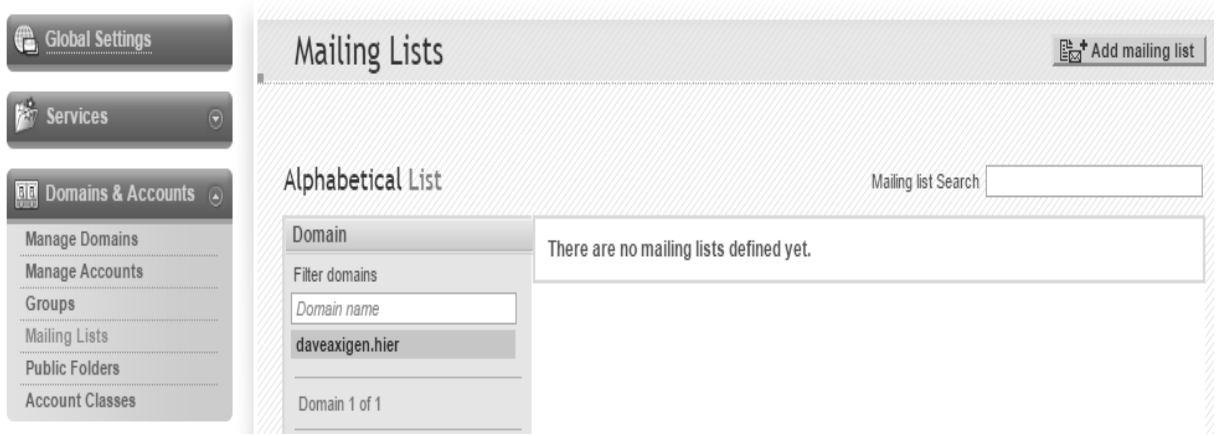


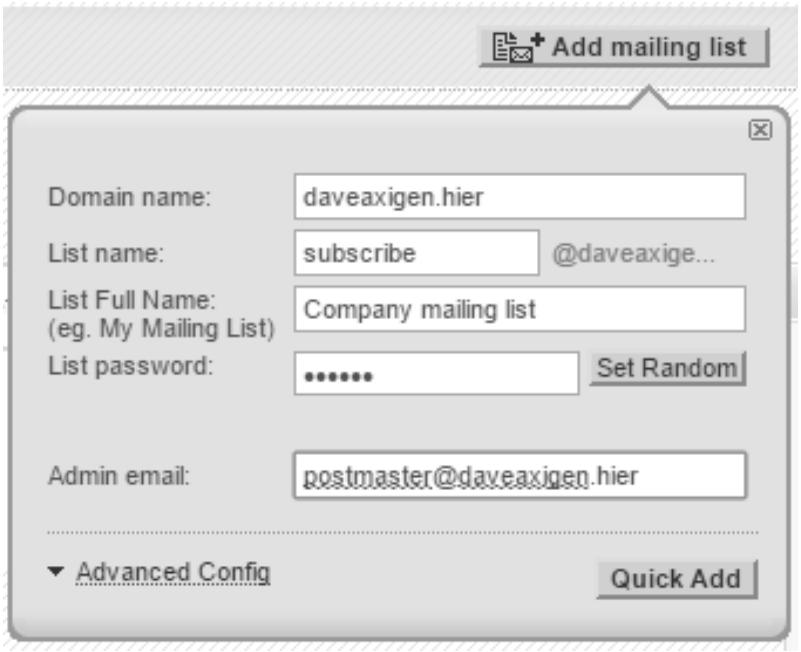
Als men de naam van de distributielijst ingeeft, vervangt Axigen deze automatisch door de adressen van de “deelnemers”:



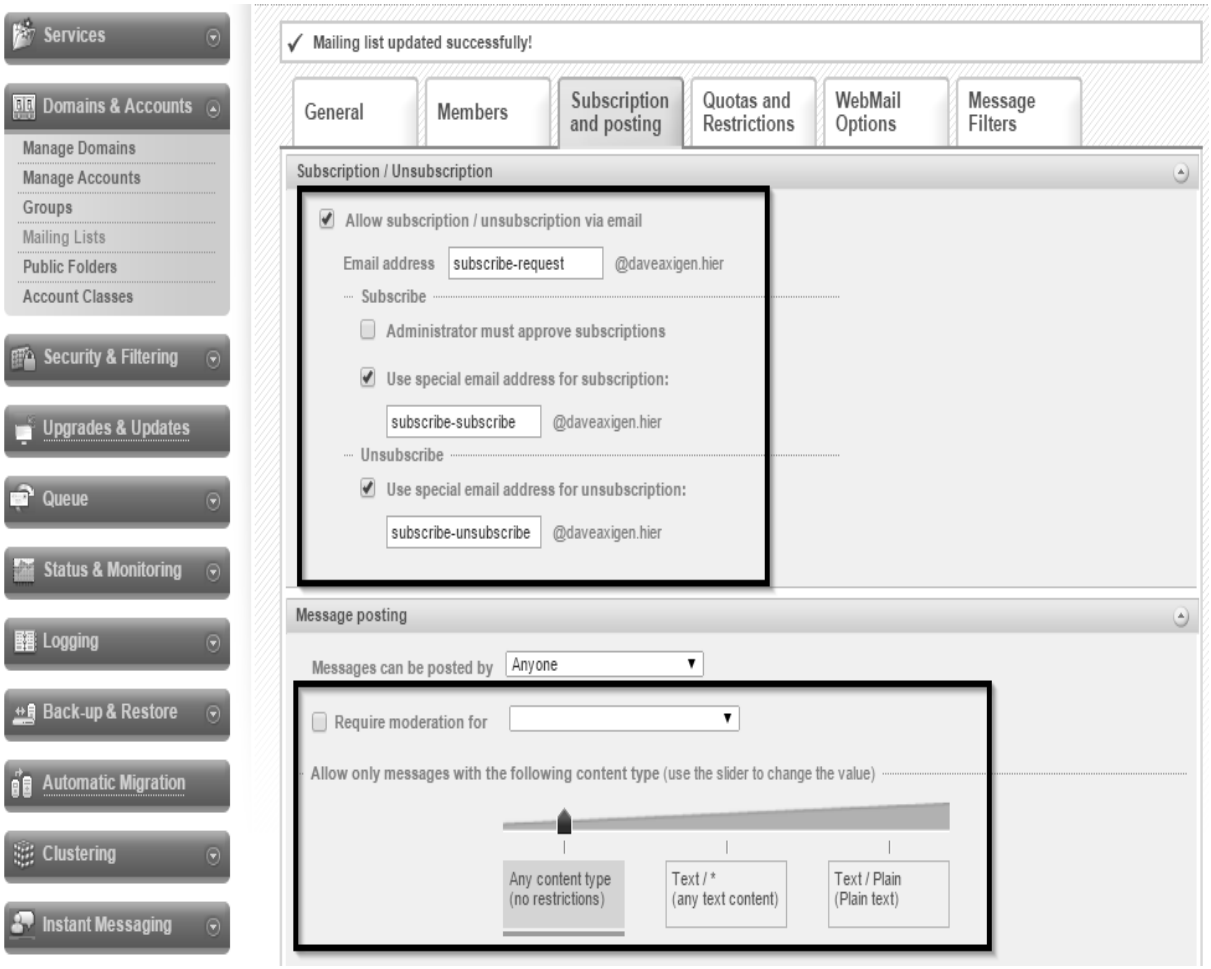
Mailinglijsten

Mailinglijsten zijn qua functionaliteit en configuratie anders als distributielijsten. Mailaccounts moeten zich inschrijven op mailinglijsten om berichten van deze mailinglijst te ontvangen. De configuratie gebeurt door de administrator van de Axigen-server, en naargelang de instellingen kunnen meerdere mensen berichten sturen naar de deelnemers.





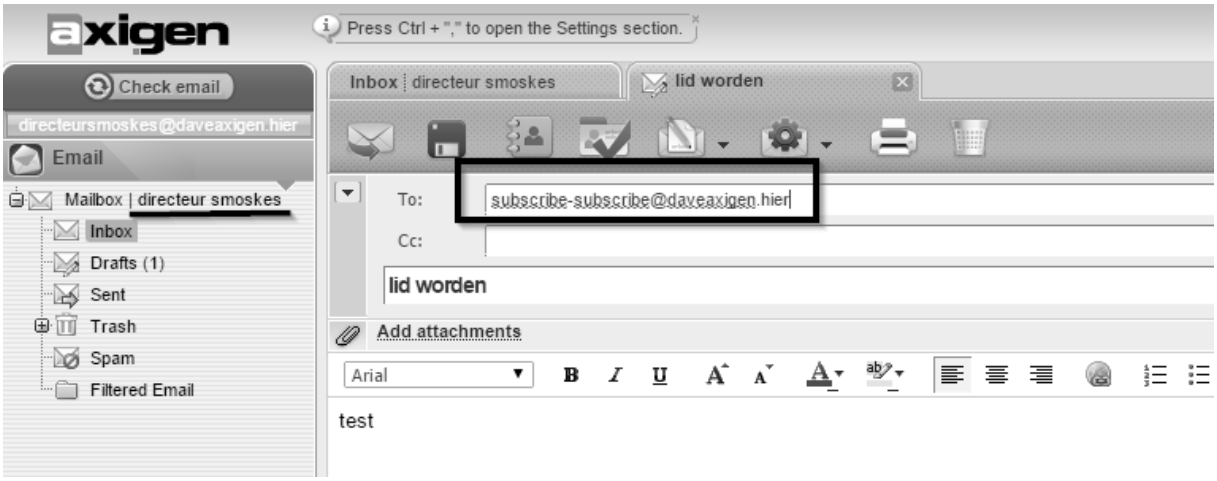
Nadat de mailinglijst is aangemaakt moet men ook de mailadressen configureren die dienen om in te schrijven op de mailinglijst.



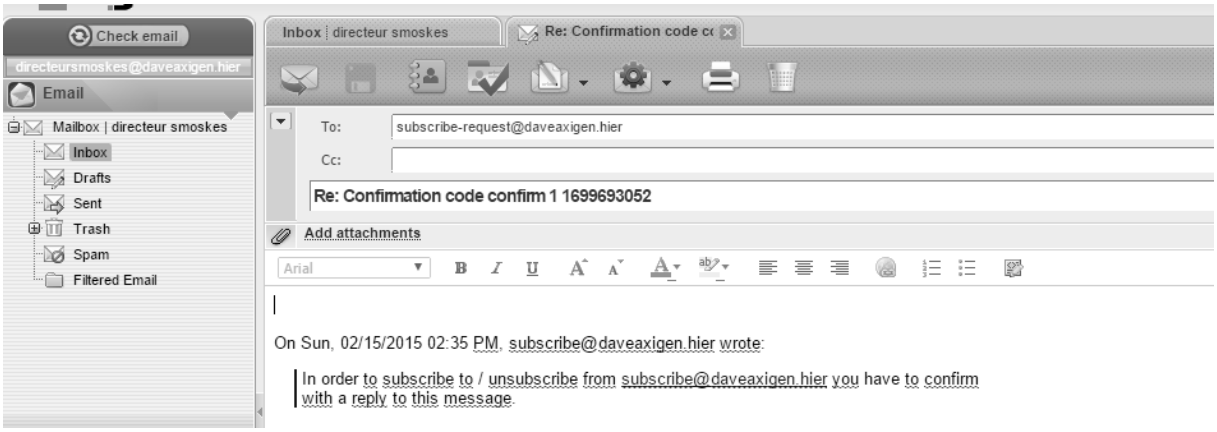
Let er op: aangezien het om een automatische mailinglijst gaat moet het vinkje voor “administrator must approve subscriptions” uitstaan en de content-type moet, zonder moderatie, op “any content type” staan.

Nu gaan we dit testen:

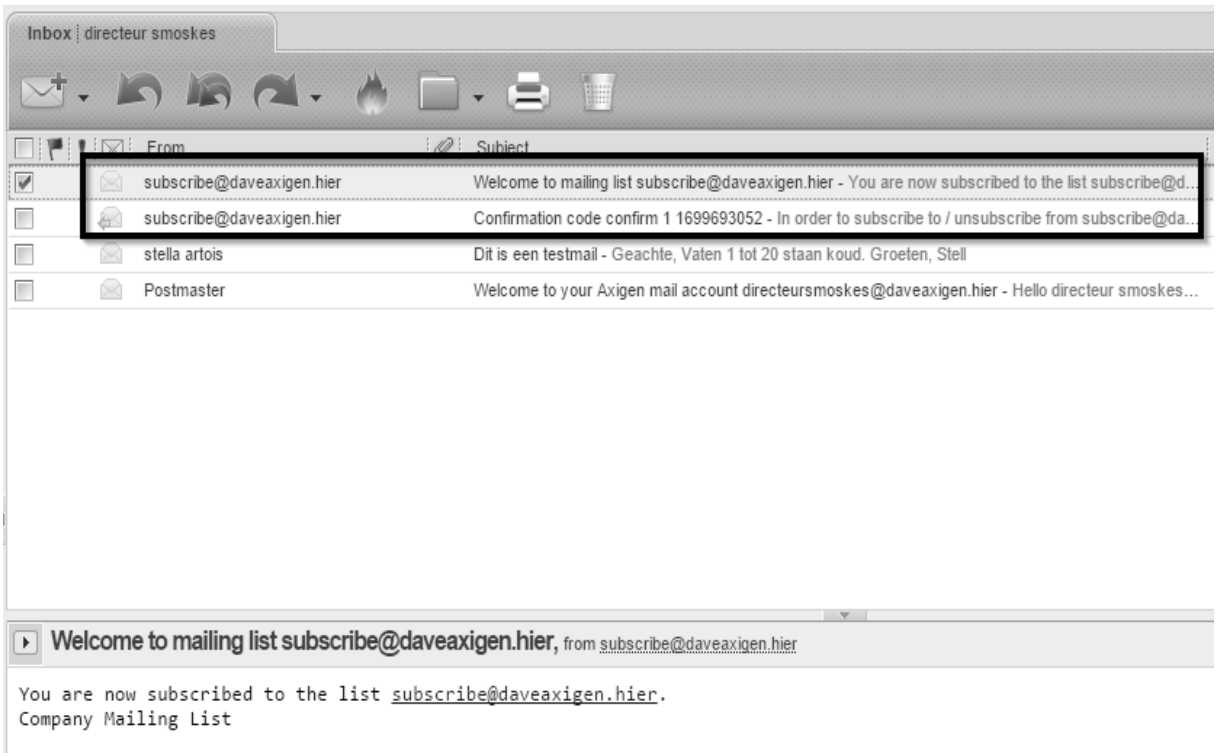
De account die lid wil worden stuurt een mail naar het subscribe-adres:



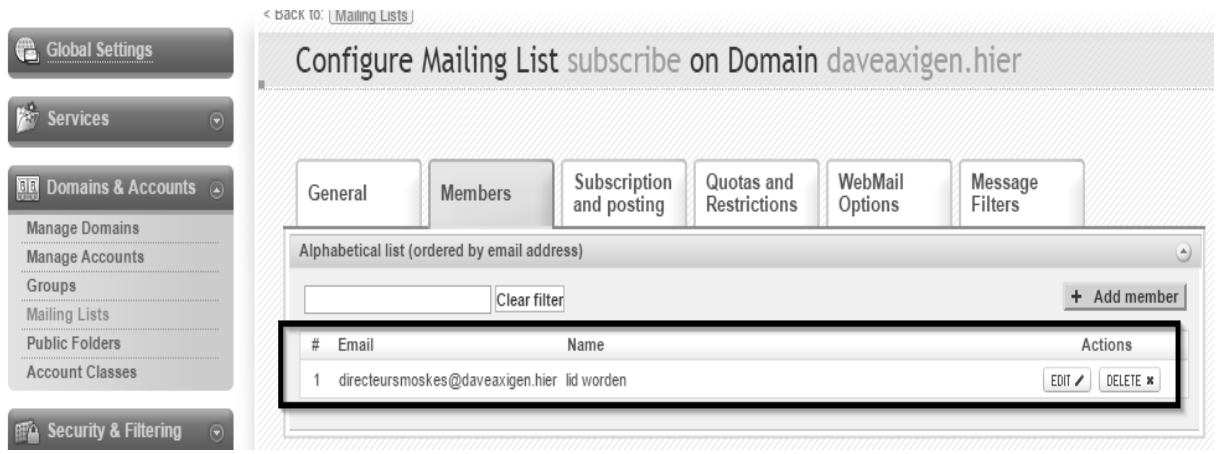
Hierna krijgt de account die lid wil worden een mail met een bevestigingscode, waarop hij zal moeten antwoorden om de inschrijvingsprocedure af te maken.



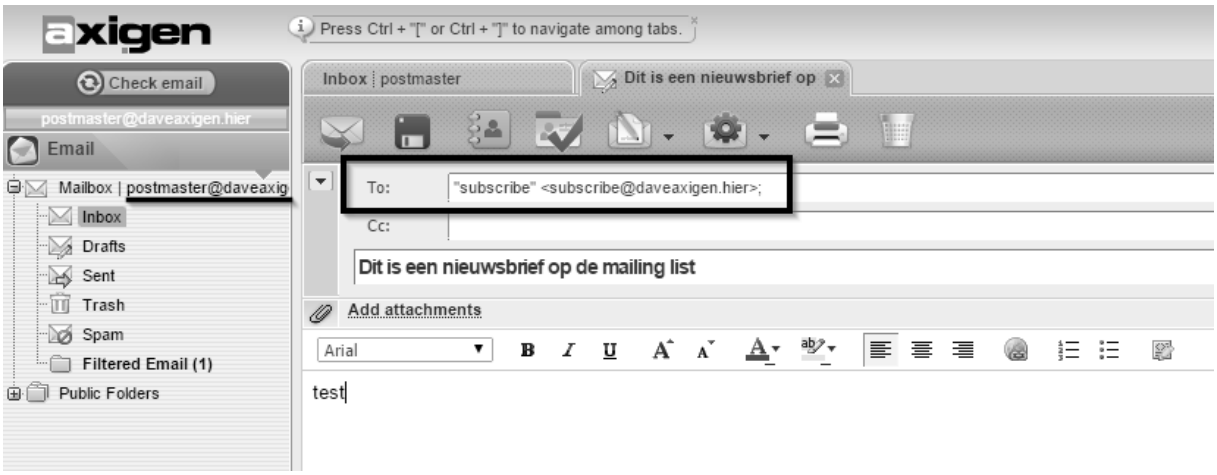
Na het inschrijven krijgt men een welkomst-mail. Deze kan eventueel aangepast worden aan de noden van het bedrijf



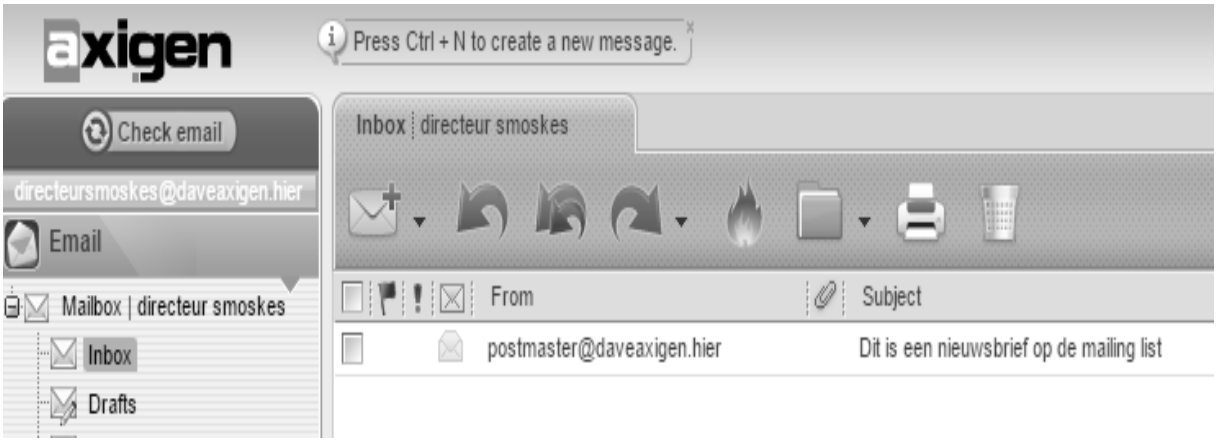
Als men op het admin-paneel gaat zien, ziet men wie er lid is van de mailing-lijst:



Nu gaan we een bericht naar de mailinglijst sturen. Dit doet men vanaf de webmail-account van de postmaster/administrator.

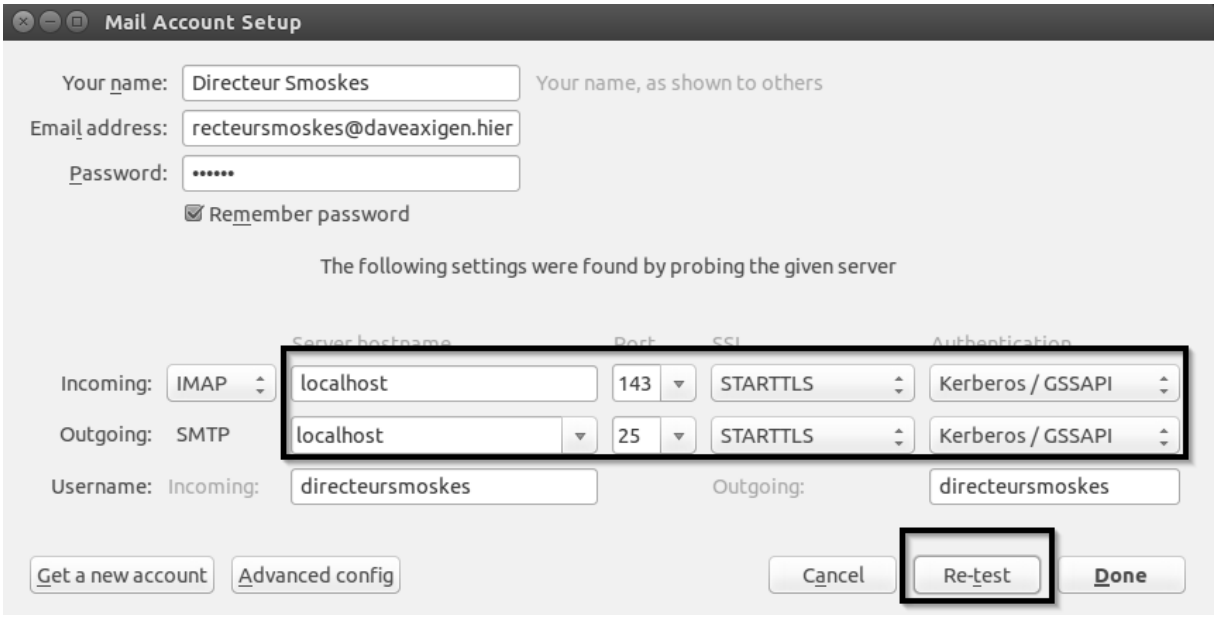


Daarna controleren we of de mail aangekomen is:

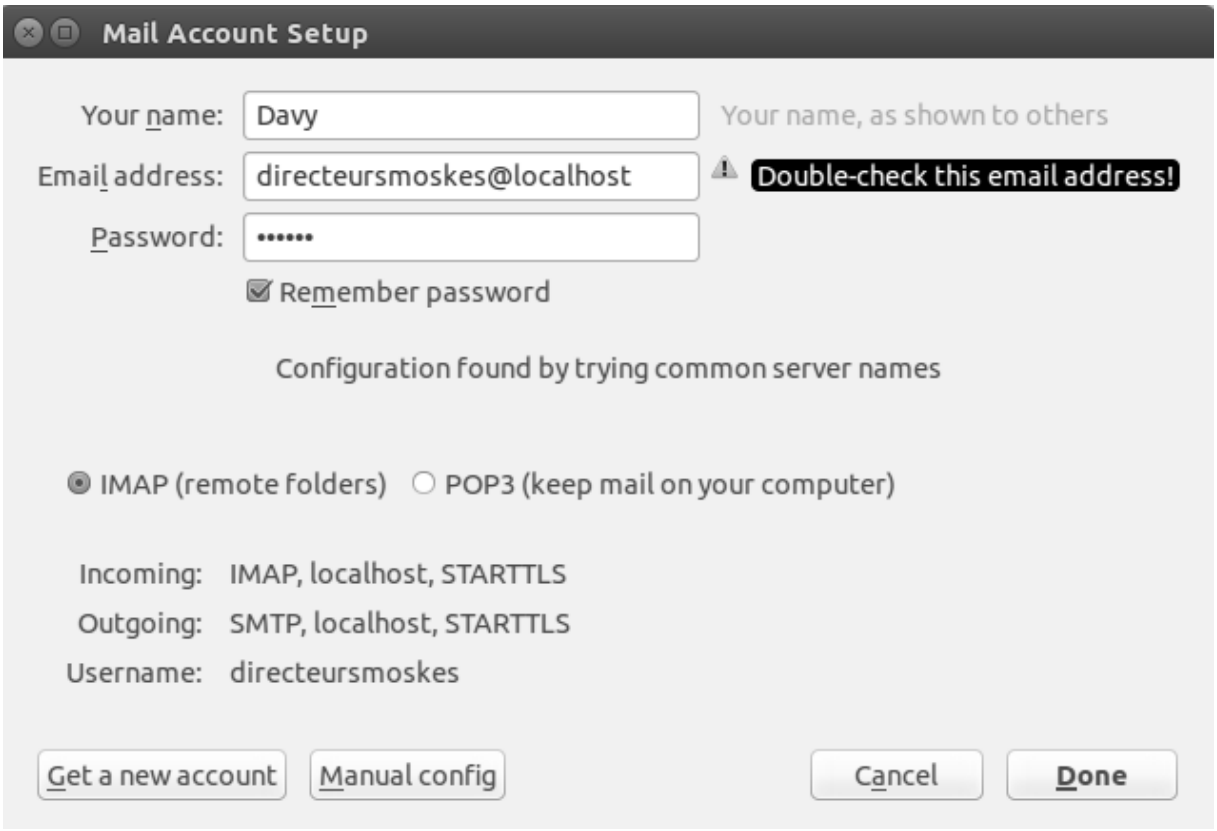


IMAP

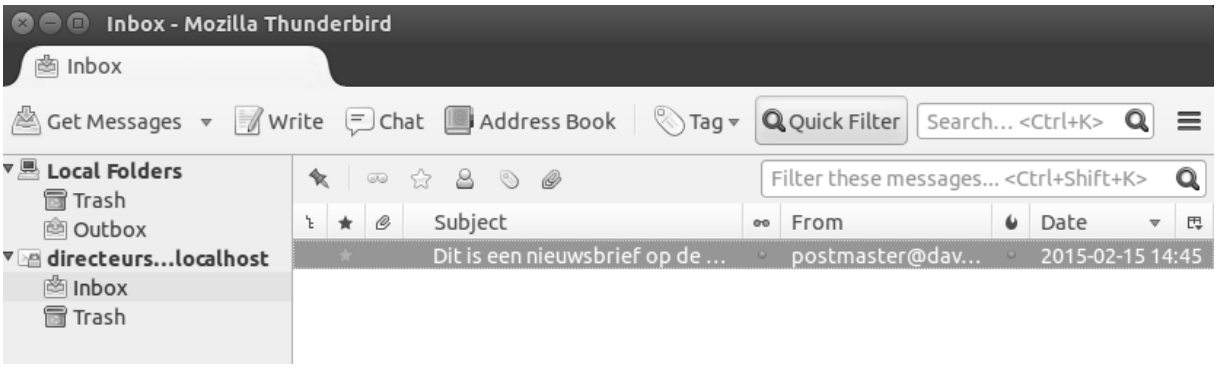
Mail-accounts bij Axigen kan men niet alleen via webmail bereiken, maar ook via IMAP. Om dit te bereiken, heb ik Thunderbird geïnstalleerd.



Aangezien ik op de Axigen-server zelf zat, moest ik als server-naam localhost ingeven.



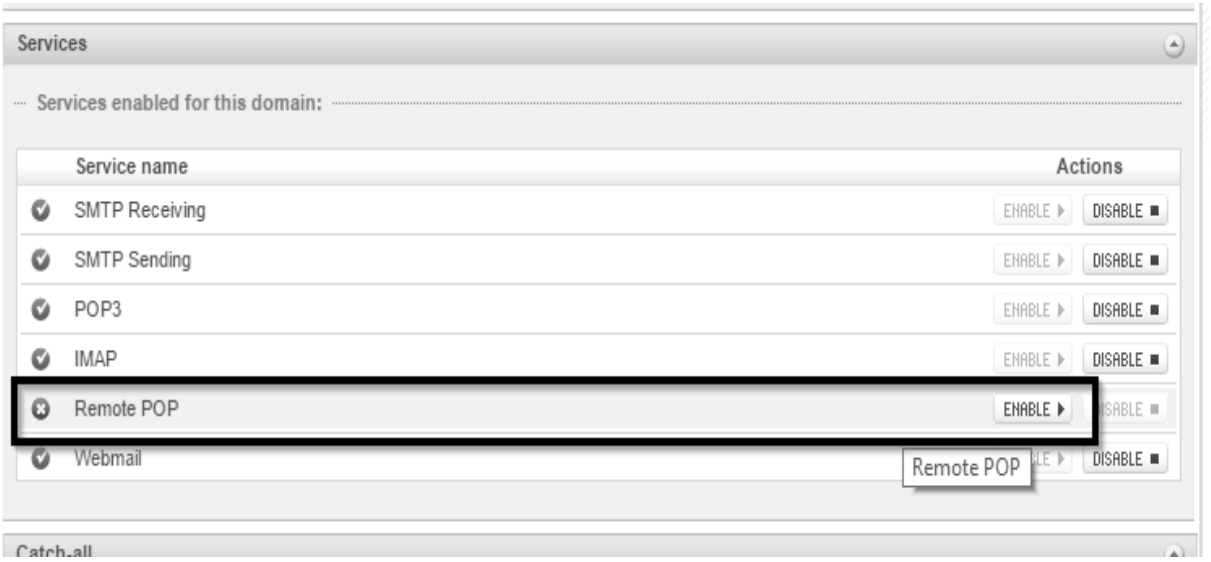
En zoals je ziet, komt de mail nu terecht in Thunderbird:

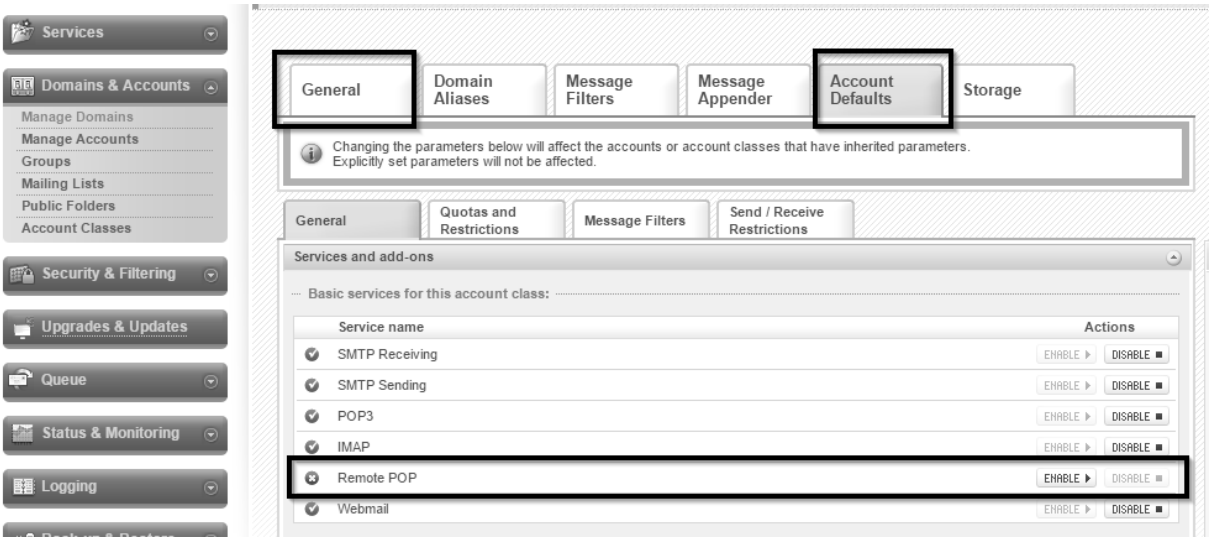


RPOP

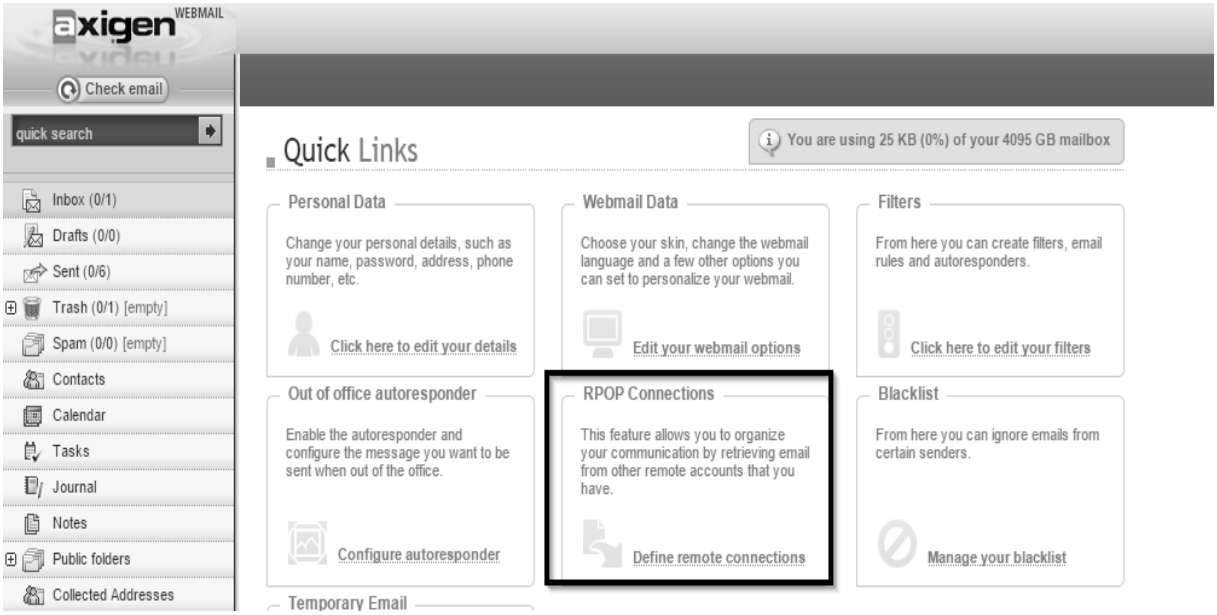
Met RPOP kan men mail van een bestaande e-mailprovider (bvb. Gmail) binnenhalen. Dit is mij niet gelukt, alhoewel de instellingen volgens hetgeen ik op internet vind (manual van Axigen) juist staan. Het probleem is dat er, alhoewel er nieuwe mail is, deze niet binnenkomt. Bij de RPOP-instellingen staat ook dat de RPOP-verbinding nog niet gedraaid heeft. De oplossing heb ik nog niet gevonden.

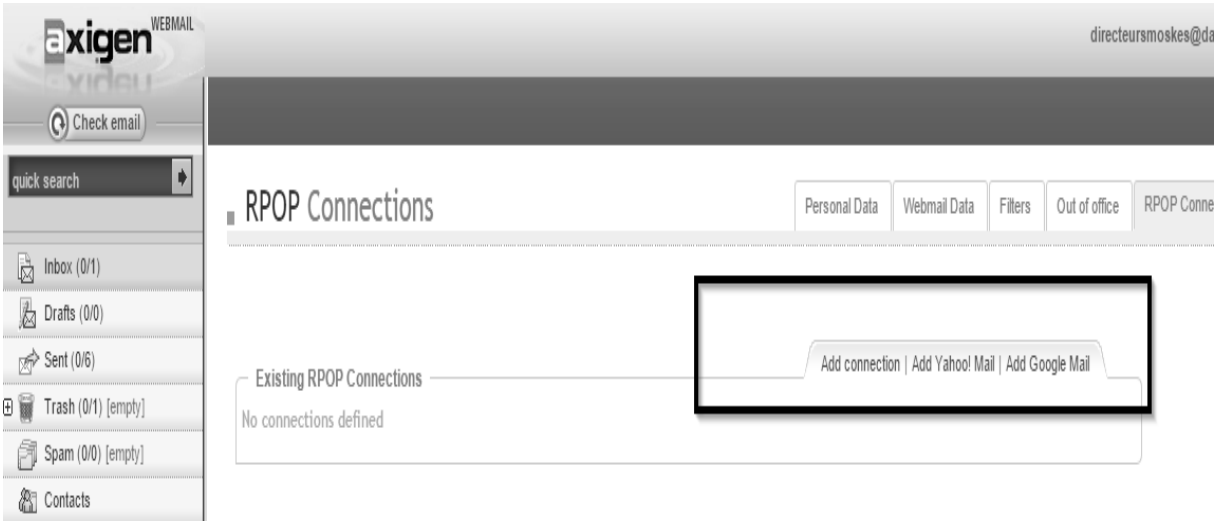
Bij de domein-instellingen moet RPOP geactiveerd zijn:



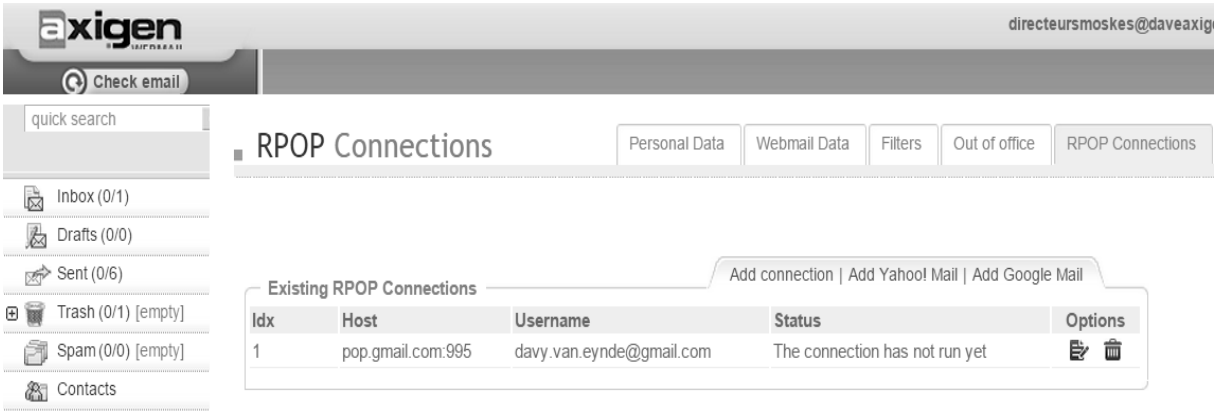


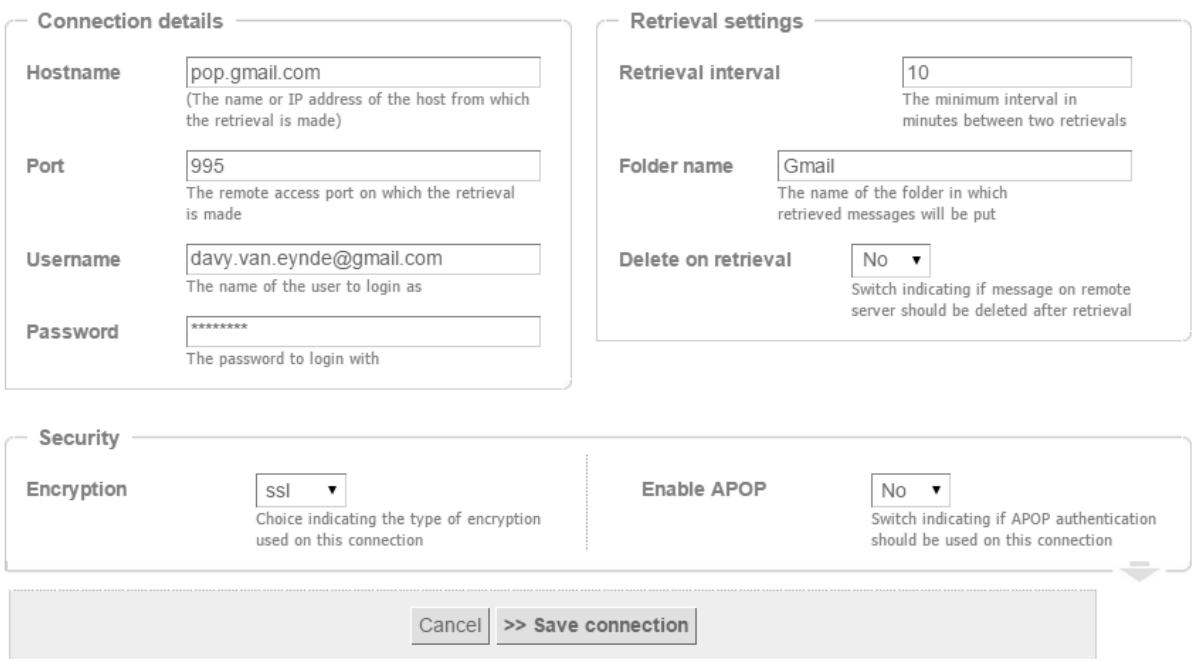
Nu best even Axigen herstarten, anders krijg je het volgende venster niet te zien bij de webmail:





Daarna moet je de gegevens ingeven (bij mij van Gmail), en zou er mail van de Gmail-account in de lokale Axigen-account moeten komen. Dit lukte dus voor mij niet. Bij de instellingen van Gmail staan zowel POP als IMAP als toegelaten aangevinkt.




Connection details
Hostname
pop.gmail.com
(The name or IP address of the host from which the retrieval is made)
Port
995
The remote access port on which the retrieval is made
Username
davy.van.eynde@gmail.com
The name of the user to login as
Password
****
The password to login with
Retrieval settings
Retrieval interval
10
The minimum interval in minutes between two retrievals
Folder name
Gmail
The name of the folder in which retrieved messages will be put
Delete on retrieval
No
Switch indicating if message on remote server should be deleted after retrieval
Security
Encryption
ssl
Choice indicating the type of encryption used on this connection
Enable APOP
No
Switch indicating if APOP authentication should be used on this connection
Cancel
>> Save connection

OpenLDAP

Post-installatie

Na het installeren we enkele testen

```
davy@server:~$ hostname -f
server.davy.hier
davy@server:~$ sudo ls -R /etc/ldap/slapd.d/
[sudo] password for davy:
/etc/ldap/slapd.d/:
cn=config  cn=config.ldif

/etc/ldap/slapd.d/cn=config:
cn=module{0}.ldif  olcBackend={0}hdb.ldif        olcDatabase={1}hdb.ldif
cn=schema          olcDatabase={0}config.ldif
cn=schema.ldif     olcDatabase={-1}frontend.ldif

/etc/ldap/slapd.d/cn=config/cn=schema:
cn={0}core.ldif    cn={2}nis.ldif
cn={1}cosine.ldif  cn={3}inetorgperson.ldif
davy@server:~$
```

```
davy@server:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config
dn
dn: cn=config

dn: cn=module{0},cn=config

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: olcBackend={0}hdb,cn=config

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config

dn: olcDatabase={1}hdb,cn=config
```

```
davy@server:~$ ldapsearch -x -LLL -H ldap:/// -b dc=davy,dc=hier dn
dn: dc=davy,dc=hier

dn: cn=admin,dc=davy,dc=hier

davy@server:~$
```

Shelldap

Via “shelldap” maken we de OU’s aan.

```
davy@server:~$ shelldap --server localhost --binddn cn=admin,dc=davy,dc=hier
Bind password:
Would you like to cache your connection information? [Yn]: y
Connection info cached to /home/davy/.shelldap.rc.
~ > ls
cn=admin
~ > mkdir Groups
Success
~ > mkdir People
Success
~ > mkdir Departments
Success
~ > ls
cn=admin
ou=Departments
ou=Groups
ou=People
~ >
```

Loglevels in LDAP

We kunnen het loglevel aanpassen. Eerst vragen we het huidige loglevel op:

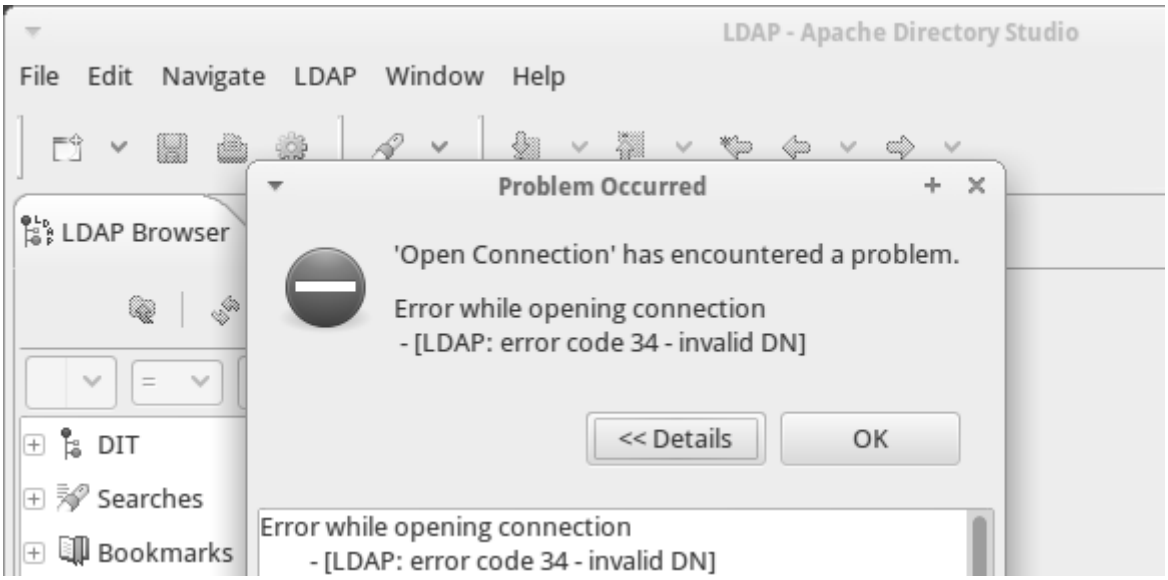
```
davy@server:~$ sudo ldapsearch -LLL -Q -Y EXTERNAL -H ldapi:/// -b "cn=config" -s bas
e | grep LogLevel
[sudo] password for davy:
olcLogLevel: none
```

Daarna wijzigen we het loglevel door middel van een ldif-bestand.

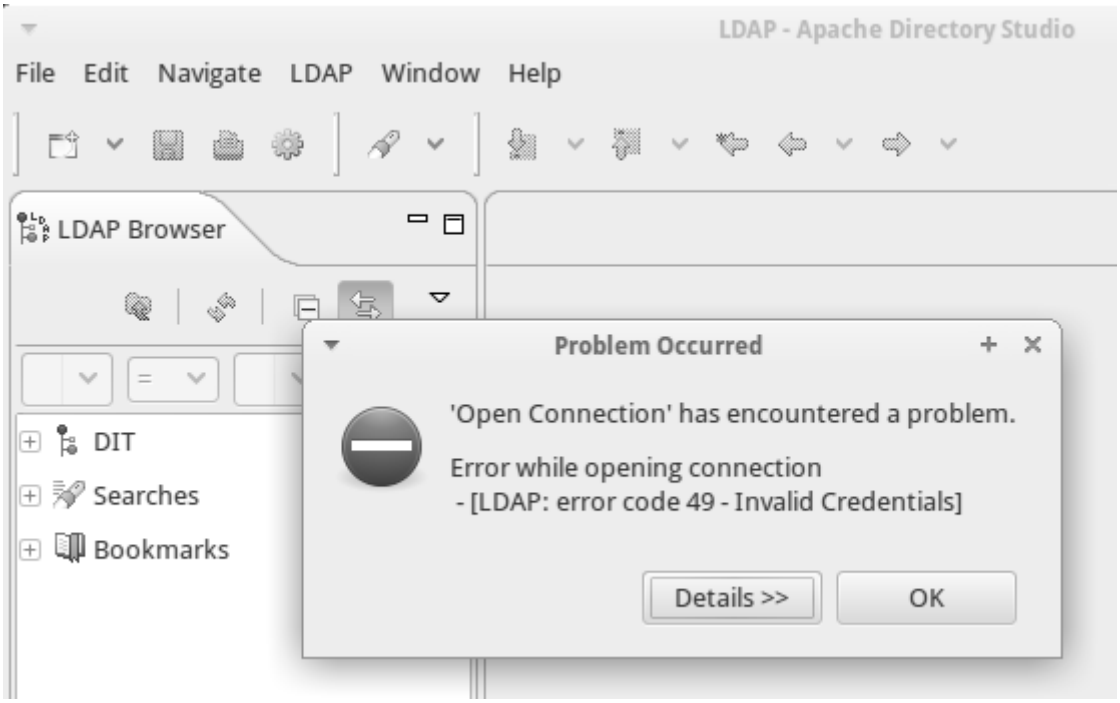
```
davy@server:~$ cat olcLogLevel_change.ldif
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: conns
davy@server:~$ sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f olcLogLevel_change.ldif
modifying entry "cn=config"

davy@server:~$ sudo ldapsearch -LLL -Q -Y EXTERNAL -H ldapi:/// -b "cn=config" -s bas
e | grep LogLevel
olcLogLevel: conns
davy@server:~$
```

Apache Directory Server

Alhoewel ik de stappen volgde in onze cursus lukte mij het niet om aan de praat te krijgen.



De eerste foutmelding kwam door een typefout van mezelf. Na correctie hiervan kreeg ik de “invalid credentials”-fout, alhoewel de gegeven credentials juist zijn.

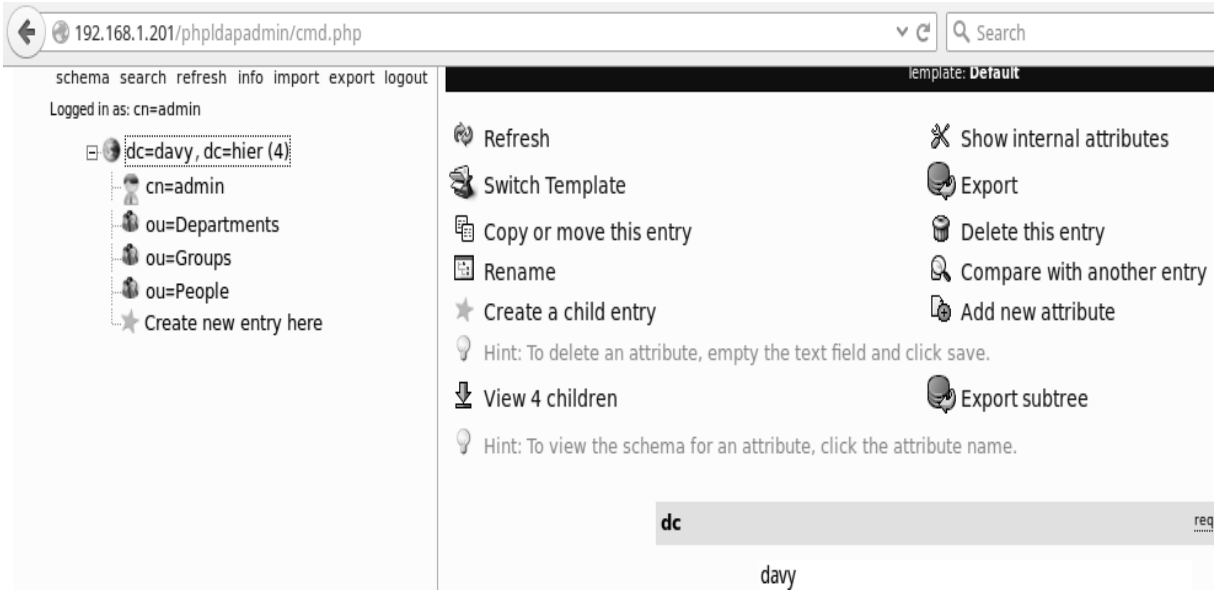


Bij research bleek dat dit te maken had met mijn installatie van Java, aangezien dat als ik op “Details” klikte een java.lang.exeption te zien kreeg.

PHPLDAPadmin

Een manier om een LDAP-installatie te beheren met een GUI is PHPLDAPadmin. Ik heb een LAMP-omgeving geïnstalleerd op mijn LDAP server, waarna ik PHPLDAPadmin installeerde.

```
davy@server:~$ sudo apt-get install phpldapadmin
```



Modifying and populating, punt 1, index toevoegen

```
davy@server:~$ cat uid_index.ldif
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: uid eq,pres,sub
davy@server:~$ sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f uid_index.ldif
[sudo] password for davy:
modifying entry "olcDatabase={1}hdb,cn=config"

davy@server:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
> cn=config '(olcDatabase={1}hdb)' olcDbIndex
dn: olcDatabase={1}hdb,cn=config
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub

davy@server:~$
```

Users en groepen toevoegen via LDIF

We hebben een ldif-bestand aangemaakt, groups.ldif.

```
davy@server:~$ ls
groups.ldif  olcLogLevel_change.ldif  uid_index.ldif
davy@server:~$ echo "Toevoegen groepen en users"
Toevoegen groepen en users
davy@server:~$ sudo ldapadd -x -D cn=admin,dc=davy,dc=hier -w -f groups.ldif
```

Als we het commando ldapadd uitvoeren, krijgen we dit resultaat:

```
davy@server:~$ sudo ldapadd -x -D cn=admin,dc=davy,dc=hier -W -f grc
Enter LDAP Password:
adding new entry "cn=Directie,ou=Groups,dc=davy,dc=hier"

adding new entry "cn=Docenten,ou=Groups,dc=davy,dc=hier"

adding new entry "cn=Secretariaat,ou=Groups,dc=davy,dc=hier"

adding new entry "cn=Studenten,ou=Groups,dc=davy,dc=hier"

adding new entry "cn=Support,ou=Groups,dc=davy,dc=hier"

adding new entry "cn=Bedrijfsbeheer,ou=Departments,dc=davy,dc=hier"
```

Een deel van het ldif-bestand zag er zo uit:

```
dn: cn=Talen,ou=Departments,dc=davy,dc=hier
objectClass: posixGroup
cn: Koken
gidNumber: 6007

dn: cn=Frans,ou=Talen,ou=Departments,dc=davy,dc=hier
objectClass: posixGroup
cn: Frans
gidNumber: 6008

dn: cn=Engels,ou=Talen,ou=Departments,dc=davy,dc=hier
objectClass: posixGroup
cn: Engels
gidNumber: 600

#Users
dn: uid=alain,ou=People,dc=davy,dc=hier
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: Alain
sn: Dhaene
givenName: Alain
cn: Alain
displayName: Alain Dhaene
uidNumber: 7000
gidNumber: 7000
userPassword: geheim
```

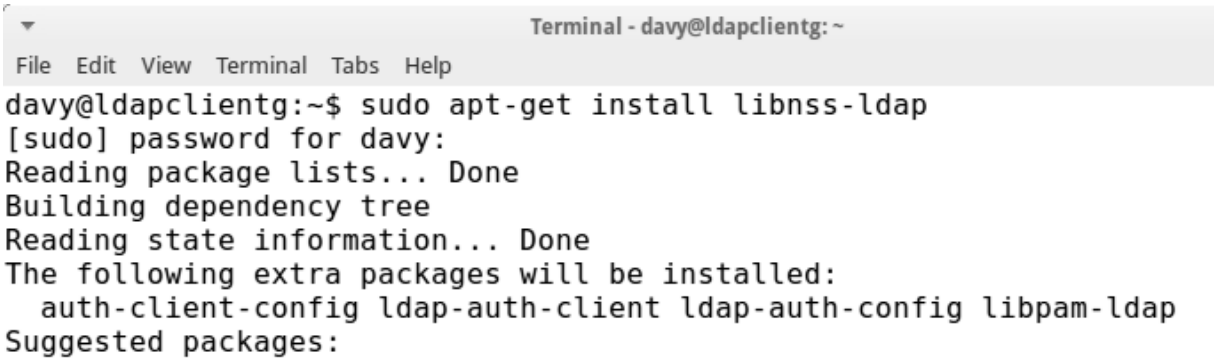
In de screenshot hierboven moet nog iets verandert worden, anders krijgt men foutmeldingen. Bij de groepen Frans en Engels moest ik nog meegeven dat de objectClass niet alleen “posixGroup” is, maar ook “top”.

Via ldapscripts kan men users toevoegen aan groepen:

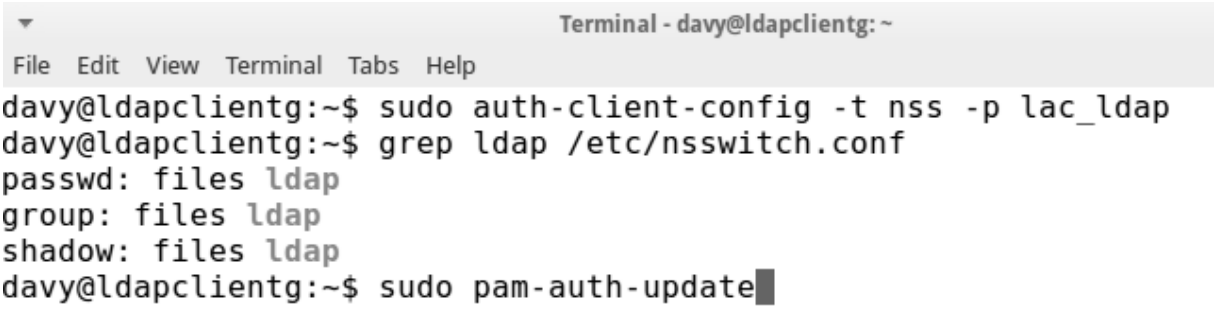
```
davy@server:~$ sudo ldapaddusertogroup alain Docenten
Successfully added user Alain to group cn=Docenten,ou=Groups,dc=davy,dc=hier
davy@server:~$ sudo ldapaddusertogroup bruno Docenten
Successfully added user Bruno to group cn=Docenten,ou=Groups,dc=davy,dc=hier
davy@server:~$ sudo ldapaddusertogroup dave Leerlingen
Group Leerlingen not found (or Dave already member of Leerlingen)
davy@server:~$ sudo ldapaddusertogroup dave Studenten
Successfully added user Dave to group cn=Studenten,ou=Groups,dc=davy,dc=hier
```

Inloggen met een cliënt-machine via LDAP

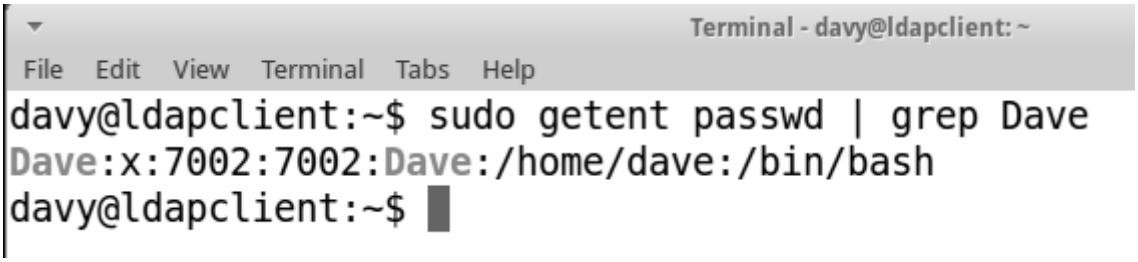
Op de cliënt:



Nu zorgen we ervoor dat men via ldap kan authoriseren.



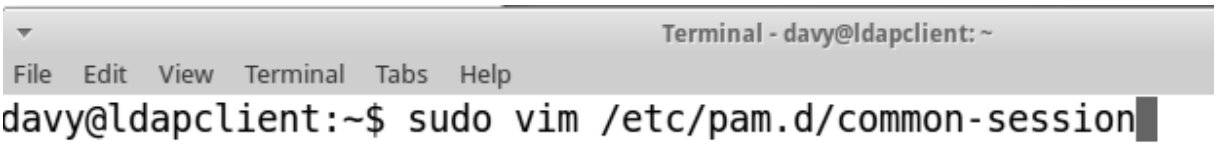
We testen of LDAP werkt, door met het getent-commando user-info opvraagt:



Ondertussen bekijken we met Wireshark het LDAP-verkeer:

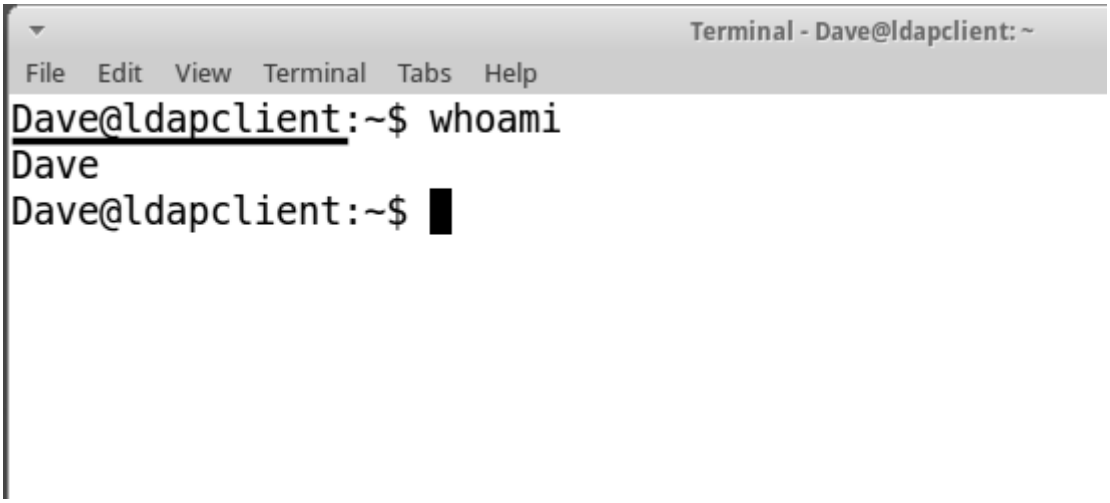
Source	Destination	Protocol	Info
192.168.1.103	192.168.1.201	LDAP	bindRequest(1) "<ROOT>" simple
192.168.1.201	192.168.1.103	LDAP	bindResponse(1) success
192.168.1.103	192.168.1.201	LDAP	searchRequest(2) "dc=davy,dc=hier" wholeSubtree
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Directie,ou=Groups,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Docenten,ou=Groups,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Secretariaat,ou=Groups,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Studenten,ou=Groups,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Support,ou=Groups,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Bedrijfsbeheer,ou=Departments,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Informatica,ou=Departments,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Koken,ou=Departments,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Talen,ou=Departments,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Frans,cn=Talen,ou=Departments,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "cn=Engels,cn=Talen,ou=Departments,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResDone(2) success [4 results]
192.168.1.103	192.168.1.201	LDAP	unbindRequest(3)
192.168.1.103	192.168.1.201	LDAP	bindRequest(1) "cn=admin,dc=davy,dc=hier" simple
192.168.1.201	192.168.1.103	LDAP	bindResponse(1) success
192.168.1.103	192.168.1.201	LDAP	searchRequest(2) "dc=davy,dc=hier" wholeSubtree
192.168.1.201	192.168.1.103	LDAP	searchResDone(2) success [0 results]
192.168.1.103	192.168.1.201	LDAP	searchRequest(3) "dc=davy,dc=hier" wholeSubtree
192.168.1.201	192.168.1.103	LDAP	searchResDone(3) success [0 results]
192.168.1.103	192.168.1.201	LDAP	bindRequest(1) "cn=admin,dc=davy,dc=hier" simple
192.168.1.201	192.168.1.103	LDAP	bindResponse(1) success
192.168.1.103	192.168.1.201	LDAP	searchRequest(2) "dc=davy,dc=hier" wholeSubtree
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "uid=alain,ou=People,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "uid=bruno,ou=People,dc=davy,dc=hier"
192.168.1.201	192.168.1.103	LDAP	searchResEntry(2) "uid=dave,ou=People,dc=davy,dc=hier"

Nu gaan we het bestand /etc/pam.d/common-session aanpassen, zodat er automatisch een homedirectory aangemaakt zal worden.

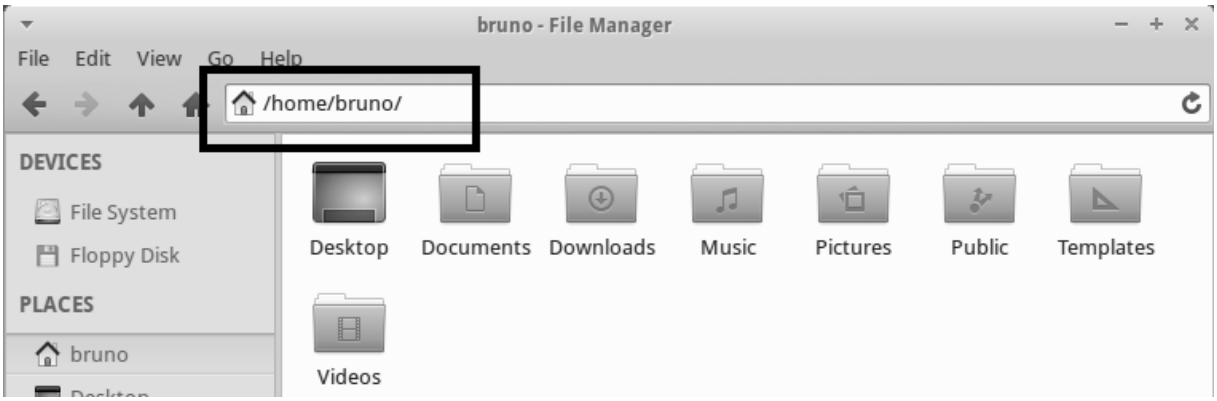


```
davy@ldapclient:~$ sudo cat /etc/pam.d/common-session
[sudo] password for davy:
#
# /etc/pam.d/common-session - session-related modules common
#
# This file is included from other service-specific PAM conf
# and should contain a list of modules that define tasks to
# at the start and end of sessions of *any* kind (both inter
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update
# To take advantage of this, it is recommended that you conf
# local modules either before or after the default block, an
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# Create homedir auto per user
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

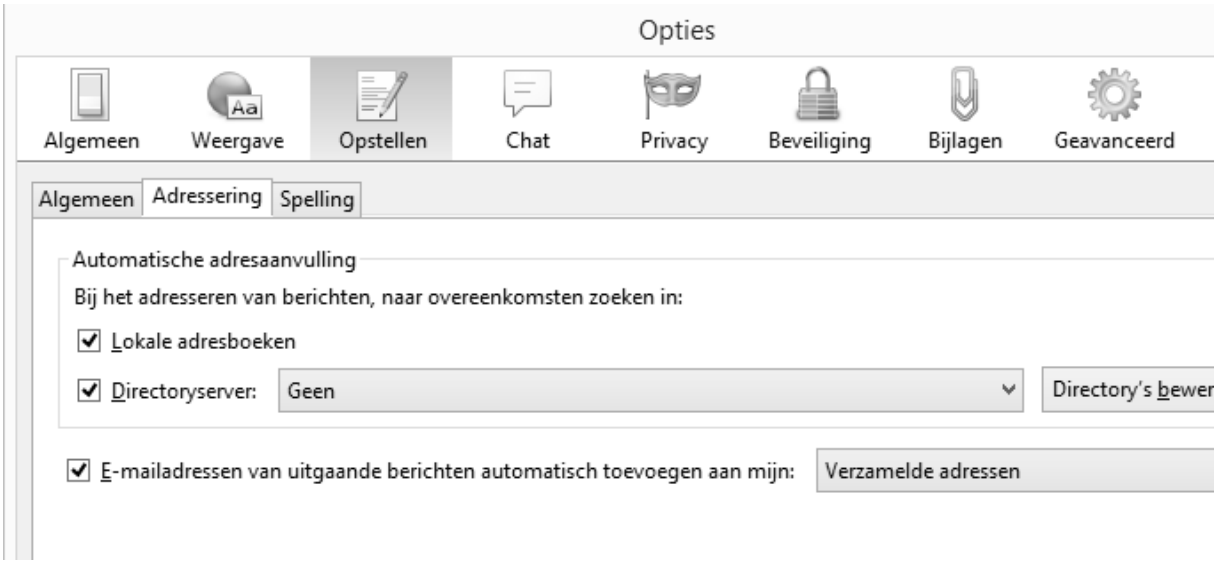
Nu dit gedaan is kunnen we testen. Ik log eerst in met LDAP-gebruiker “Dave”, daarna met “Bruno”.

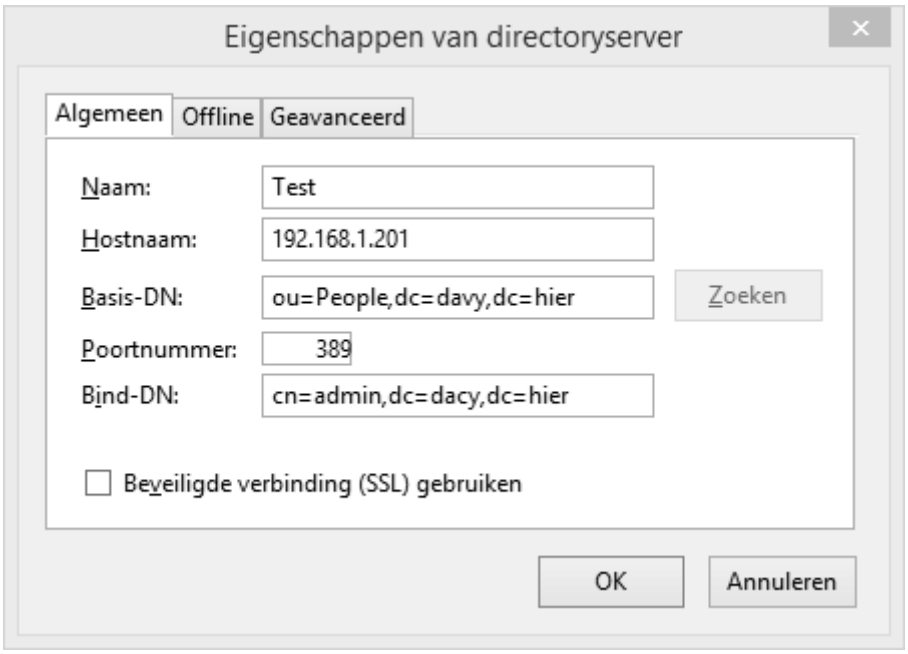


En nu met een andere gebruiker, die zoals je ziet een homedirectory krijgt.

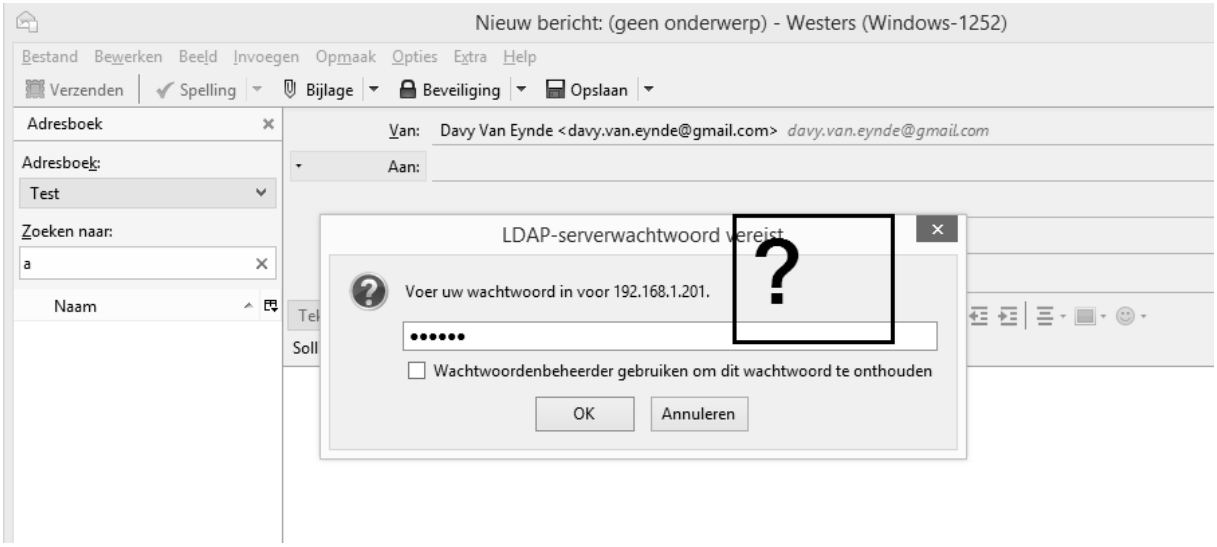


Thunderbird adresboek via LDAP

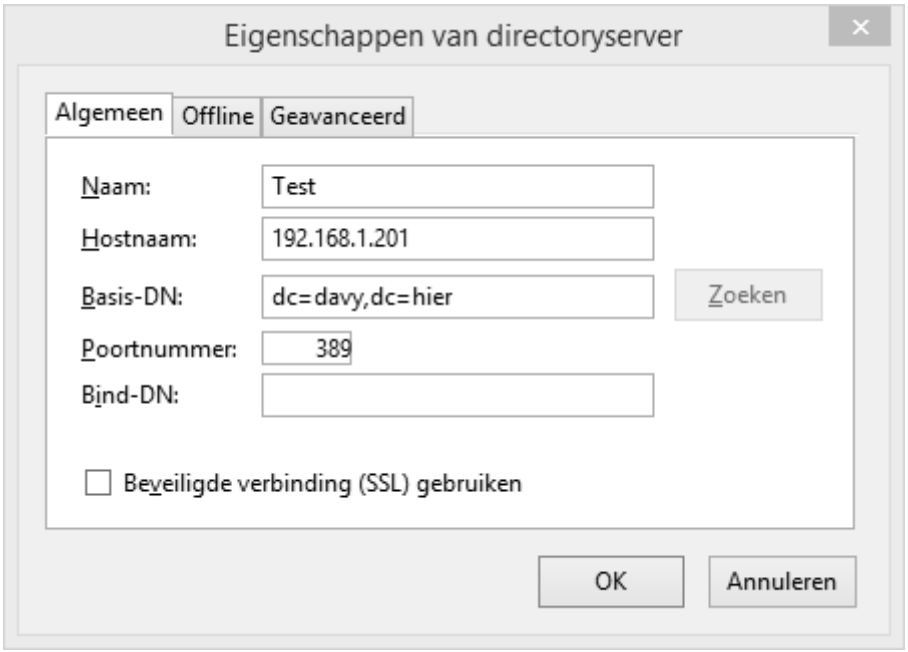


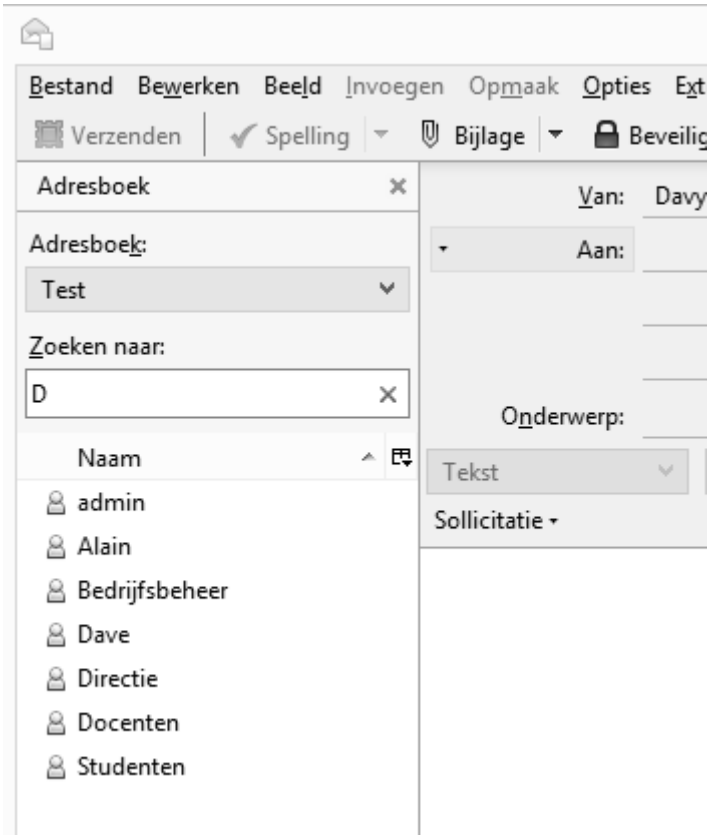

Eigenschappen van directoryserver
Algemeen
Offline
Geavanceerd
Naam:
Test
Hostnaam:
192.168.1.201
Basis-DN:
ou=People,dc=davy,dc=hier
Zoeken
Poortnummer:
389
Bind-DN:
cn=admin,dc=dacy,dc=hier
Beveiligde verbinding (SSL) gebruiken
OK
Annuleren


Opties
Algemeen
Weergave
Opstellen
Chat
Privacy
Beveiliging
Bijlagen
Geavanceerd
Agenda
Algemeen
Adressering
Spelling
Automatische adresaanvulling
Bij het adresseren van berichten, naar overeenkomsten zoeken in:
Lokale adresboeken
Directoryserver:
Test
Directory's bewerken...
E-mailadressen van uitgaande berichten automatisch toevoegen aan mijn:
Verzamelde adressen


Nieuw bericht: (geen onderwerp) - Westers (Windows-1252)
Bestand
Bewerken
Beeld
Invoegen
Opmaak
Opties
Extra
Help
Verzenden
Spelling
Bijlage
Beveiliging
Opslaan
Adresboek
Adresboek:
Test
Zoeken naar:
a
Naam
Van:
Davy Van Eynde <davy.van.eynde@gmail.com>
davy.van.eynde@gmail.com
Aan:
LDAP-serverwachtwoord vereist
?
Voer uw wachtwoord in voor 192.168.1.201.
Wachtwoordenbeheerder gebruiken om dit wachtwoord te onthouden
OK
Annuleren

Alhoewel ik hierboven het juiste wachtwoord ingeef, blijft de vraag naar het wachtwoord weerkeren. Dit heb ik kunnen oplossen door ten eerste op de ldap-server slapd te herstarten, en bij de settings van Thunderbird geen binddn te gebruiken.





Authenticatie bij een Apache virtual host

LDAP kan ook gebruikt worden om de toegang tot websites of delen er van te controleren. Alleen gebruikers die zich mits een juist paswoord kunnen authentiseren krijgen de inhoud te zien.

Eerst laden we in Apache de nodige modules:

```
davy@server:/$ sudo a2enmod ldap authnz_ldap auth_basic
Module ldap already enabled
Considering dependency ldap for authnz_ldap:
Module ldap already enabled
Enabling module authnz_ldap.
Considering dependency authn_core for auth_basic:
Module authn_core already enabled
Module auth_basic already enabled
To activate the new configuration, you need to run:
  service apache2 restart
davy@server:/$ sudo service apache2 restart
 * Restarting web server apache2                                          [ OK ]
davy@server:/$ _
```

Ik had eerst het a2enmod commando met een typefout uitgevoerd, waardoor je de melding ziet dat sommige modules al actief staan.

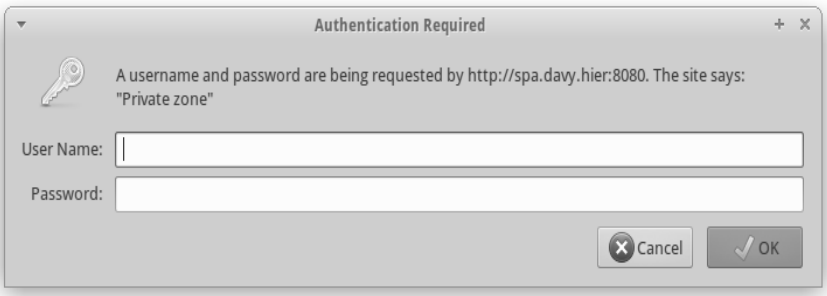
Na de herstart van de webserver ga ik het configuratiebestand van de virtuele host, in dit geval “spa”, aanpassen.

Ik vermeld daarin welke directory publiek toegankelijk is, en welke achter een login-scherm moet zitten. Bij het beveiligde stuk vertel ik daarna met welk mechanisme er geauthentiseerd moet worden (LDAP), en met welke parameters.

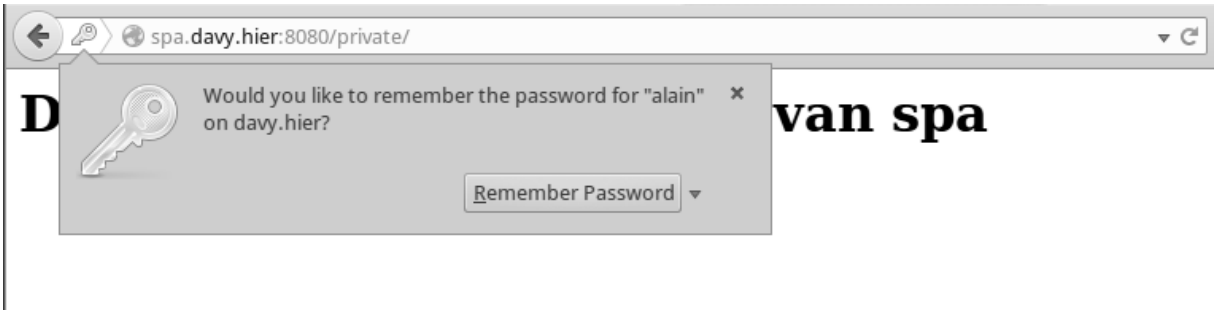
```
davy@server:~$ cat /etc/apache2/sites-available/spa.conf
<VirtualHost *:8080>
        ServerName spa.davy.hitek.hier
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/spa
        <Directory /var/www/spa>
                Order allow,deny
                Allow from all
        </Directory>
        <Directory /var/www/spa/private>
                Order deny,allow
                Deny from all
                AuthName "Private zone"
                AuthType basic
                AuthBasicProvider ldap
                AuthLDAPUrl ldap://127.0.0.1/dc=davy,dc=hier
                AuthLDAPBindDN "cn=admin,dc=davy,dc=hier"
                AuthLDAPBindPassword "geheim"
                Require valid-user
                Satisfy any
        </Directory>
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Daarna maak ik “spa” actief met “a2ensite”, en herstart ik voor de zekerheid mijn webserver. Op een cliënt surf ik naar het privaat gedeelte van de virtuele host.

Dit is spa



We geven daar de gebruikersnaam in en een wachtwoord, waarna we dit resultaat krijgen:



Gegevens opvragen

Gegevens opvragen via PHP kan via een anonieme bind.

search.html

```
<html>
<body>
<h3>Opvragen GSMnummer</h3>

<form action="search.php" method="post">
Name: <input type="text" name="name"><br /><br />
<input type="submit">
</form>

</body>
</html>
```

search.php

```
<?php
echo "<html><head><title>Opvragen GSMnummer</title></head><body>";
$name = $_POST["name"];

//connect en bind

echo "<h3>Opvragen GSMnummer</h3>";
$ds=ldap_connect("192.168.1.201");

if ($ds) {
   $r=ldap_bind($ds);    // anonieme bind voor read-only access
   $item = "uid=";
   $zoek = $item . $name;

   echo "Zoek naar de gebruiker waarvan " . $zoek . " ... <br /><br />";

   // Zoeken
   $sr=ldap_search($ds, "ou=People,dc=davy,dc=hier", $zoek);

   $info = ldap_get_entries($ds, $sr);

   for ($i=0; $i<$info["count"]; $i++) {
       echo "Het GSMnummer van " . $info[$i]["cn"][0] . " is " .
$info[$i]["mobile"][0] . "<br />";
      }

   ldap_close($ds);

} else {
   echo "<h4>Unable to connect to LDAP server</h4>";
}
echo "</body></html>";
?>
```

Opvragen GSMnummer

Name: alain

Verzenden

Opvragen GSMnummer

Zoek naar de gebruiker waarvan uid=alain ...

Het GSMnummer van Alain is 1111111

Via PHP-scripts kan men niet alleen gegevens opvragen, maar ook gegevens wijzigen. Ik heb een script gemaakt, waardoor dat gebruikers hun GSM-nummer op de LDAP-server kunnen veranderen.

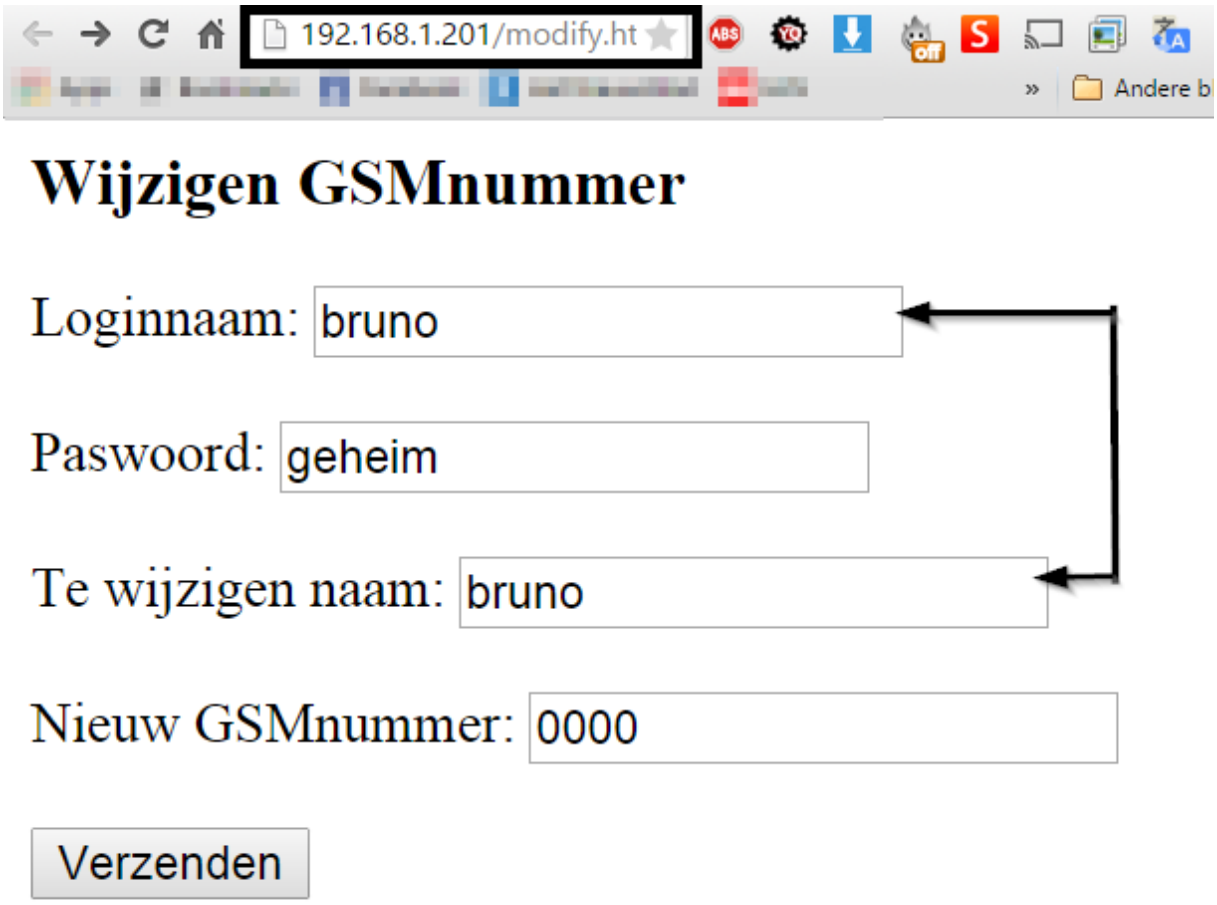
modify.html

```
<html>
<body>
<h3>Wijzigen GSMnummer</h3>

<form action="modify.php" method="post">
Loginnaam: <input type="text" name="login"><br /><br />
Paswoord: <input type="password" name="password"><br /><br />
Te wijzigen naam: <input type="text" name="name"><br /><br />
Nieuw GSMnummer: <input type="text" name="newnumber"><br /><br />
<input type="submit">
</form>

</body>
</html>
```

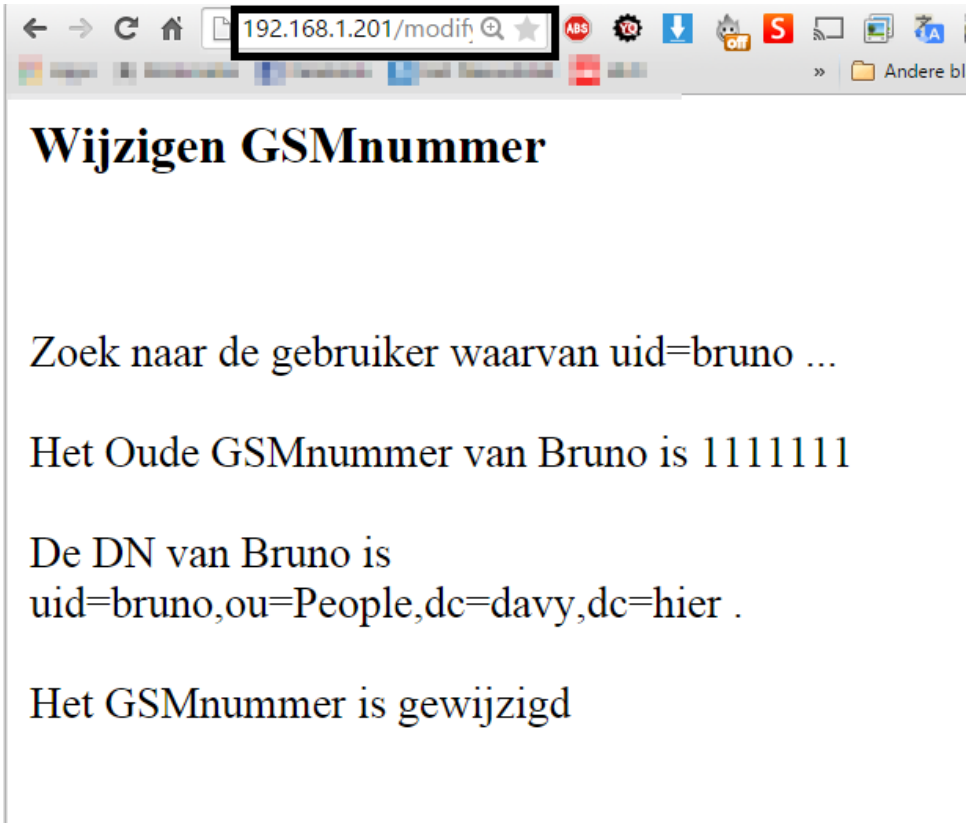
modify.php

```
<?php
echo "<html><head><title>Wijzigen GSMnummer</title></head><body>";
$login = $_POST["login"];
$password = $_POST["password"];
$name = $_POST["name"];
$newnumber = $_POST["newnumber"];
$root = ",ou=People,dc=davy,dc=hier";
$cn = "uid=" . $login . $root;
//connect en bind

echo "<h3>Wijzigen GSMnummer</h3>";
echo "<br />";
$ds=ldap_connect("192.168.1.201");
ldap_set_option($ds, LDAP_OPT_PROTOCOL_VERSION, 3);

if ($ds) {

      //binding to ldap server
      $r=ldap_bind($ds, $cn, $password);
      $item = "uid=";
      $zoek = $item . $name;
```

```
// verify binding
      if ($r) {
            if ($login == $name) {
                  echo "<br />Zoek naar de gebruiker waarvan " . $zoek .
" ... <br /><br />";
                  $sr=ldap_search($ds,"ou=People,dc=davy,dc=hier",
$zoek);
                  $info = ldap_get_entries($ds, $sr);
                  $srdn = $zoek . ",ou=People,dc=davy,dc=hier";

                  for ($i=0; $i<$info["count"]; $i++) {
                        echo "Het Oude GSMnummer van " .
$info[$i]["cn"][0] . " is " . $info[$i]["mobile"][0] . "<br /><br />";
                        echo "De DN van " . $info[$i]["cn"][0] . " is " .
$srdn . " . <br /><br />";

                        $attr["mobile"] = $newnumber;
                        $result = ldap_mod_replace($ds, $srdn, $attr);

                        if (TRUE === $result) {
                              echo "Het GSMnummer is gewijzigd";
                        } else {
                              echo "Het GSMnummer kon niet gewijzigd
worden";
                        }
                  }

            } else {
                  echo "U mag geen data wijzigen van deze persoon";
            }

      } else {
            echo "LDAP bind failed ...";
            echo "<br /><br />";
            echo "Error was: " . ldap_error($ds);
      }

   ldap_close($ds);

} else {
   echo "<h4>Unable to connect to LDAP server</h4>";
}
echo "</body></html>";
?>
```



De loginnaam en de te wijzigen naam moeten gelijk zijn, en dan krijgen we dit resultaat:



Als we nu met ons zoek-script de gegevens van de gebruiker opvragen, zien we dat de GSM-nummer gewijzigd is:

Ik heb op dit moment het HTML-formulier aangepast, zodat het ingegeven paswoord gemaskeerd is:

Aangezien PHP-scripts - naargelang de persoon die ze schrijft - onveilig kunnen zijn, is het beter om nog op onze LDAP-server toegangsrechten te gebruiken. Dit doet men via access control lists, of ACL's.

Om dit gedaan te krijgen zou ik met een ldif-bestand de LDAP-configuratie aanpassen met het commando "`sudo ldapmodify –Q –Y EXTERNAL –H ldapi:/// -f olcAccess_change.ldif`"

In dit ldif-bestand vermelden we dan welke waarden we willen veranderen, en welke inhoud.

Ik zou in het bestand bvb. dit zetten:

olcAccess_change.ldif

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: to attrs=userPassword by self write by anonymous auth by
dn="cn=admin,dc=davy,dc=hier" write by * none
olcAccess: to attrs=shadowLastChange by self write by anonymous auth by
dn="cn=admin,dc=davy,dc=hier" write by * none
olcAccess: to attrs=mobile by self write by dn="cn=admin,dc=davy,dc=hier"
write by * none
olcAccess: to * by self write by dn="cn=admin,dc=davy,dc=com" write by *
read
```

De eerste drie vermeldingen van olcAccess zorgen er voor dat:

- Men zijn eigen paswoord en Gsm-nummer kan veranderen
- Dat de admin-gebruiker het paswoord en Gsm-nummer van een gebruiker kan veranderen

Het stuk "by anonymous auth" bij de attributen "userPassword" en "shadowLastChange" zorgen er voor dat anoniem gebonden gebruikers de kans krijgen om zich toch te identificeren.

De laatste vermelding van olcAccess zorgt er voor dat de rest van de attributen van een gebruiker kan aangepast worden door de gebruiker zelf, of door de admin. Aangezien ik "by * read" vermeldt, kan een anonieme gebruiker wel onze directory information tree (DIT) lezen.

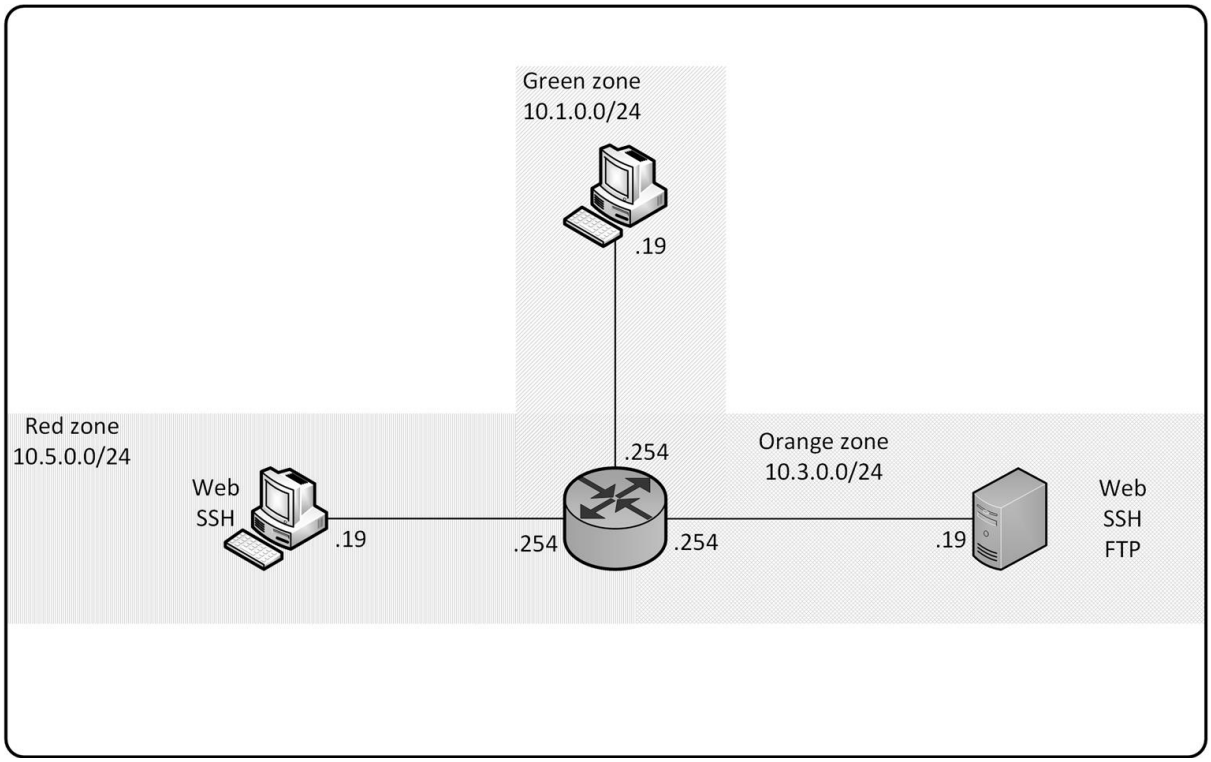
RouterOS firewall

Intro

Om deze oefening uit te voeren maak ik gebruik van volgende virtuele machines:

- 1 router/firewall met RouterOS
- 1 Lubuntu-machine, zonder server-software, als “groene” cliënt
- 1 Lubuntu-machine met lighttpd als webserver, OpenSSH als ssh-server en vsftpd als ftp-server (“oranje” cliënt)
- 1 Lubuntu-machine met lighttpd als webserver, OpenSSH als ssh-server (“rode” cliënt)

Deze worden in onderstaande topologie gezet:



Netwerkscan

Voordat ik NAT- en/of firewall-regels instel op de router, scan ik de hosts met nmap. De optie “-Pn” zorgt ervoor dat nmap alle hosts als online beschouwt, en geen host discovery doet door middel van een ping scan.

Vanop de rode host, scan ik de router, en zien we volgende services openstaan:

```
dave@REDBOX:~$ #nmap davyguard
dave@REDBOX:~$ nmap -Pn 10.5.0.254

Starting Nmap 6.46 ( http://nmap.org ) at 2015-03-22 12:17 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse D
 Try using --system-dns or specify valid servers with --dns-serve
Nmap scan report for 10.5.0.254
Host is up (0.024s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
2000/tcp open  cisco-sccp
8291/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
dave@REDBOX:~$
```

Daarna doen we hetzelfde voor de oranje host:

```
dave@REDBOX:~$ #nmap orange
dave@REDBOX:~$ nmap -Pn 10.3.0.19

Starting Nmap 6.46 ( http://nmap.org ) at 2015-03-22 12:19 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DN
 Try using --system-dns or specify valid servers with --dns-server
Nmap scan report for 10.3.0.19
Host is up (0.0044s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
dave@REDBOX:~$
```

Op deze oranje host zien we duidelijk de ftp-, ssh- en webserver draaien.

Nu scannen de groene host. Deze ligt in de safe zone, en mag geen open services hebben. En effectief, dit is het resultaat:

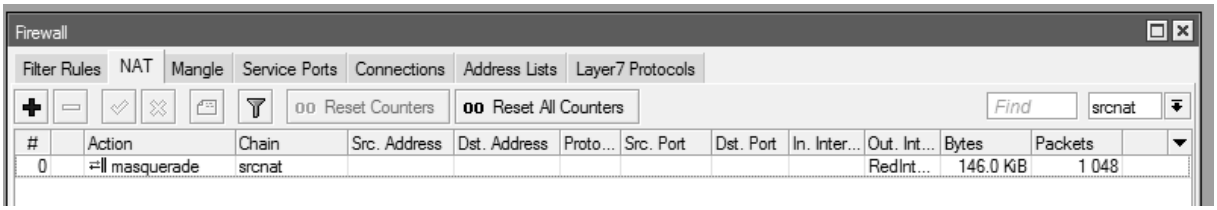
```
dave@REDBOX:~$ #nmap green
dave@REDBOX:~$ nmap -Pn 10.1.0.19

Starting Nmap 6.46 ( http://nmap.org ) at 2015-03-22 12:20 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS i
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.0.19
Host is up (0.0044s latency).
All 1000 scanned ports on 10.1.0.19 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
dave@REDBOX:~$
```

Als laatste scannen we de rode host:

```
dave@REDBOX:~$ #nmap red
dave@REDBOX:~$ nmap -Pn 10.5.0.19

Starting Nmap 6.46 ( http://nmap.org ) at 2015-03-22 12:22 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.5.0.19
Host is up (0.00021s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
dave@REDBOX:~$
```

Network Address Translation

Om de groene en oranje zone te verbergen, gaan we eerst aan source-NATting doen. De rode zone ziet alleen het openbaar IP-adres op de router, namelijk 10.5.0.254.

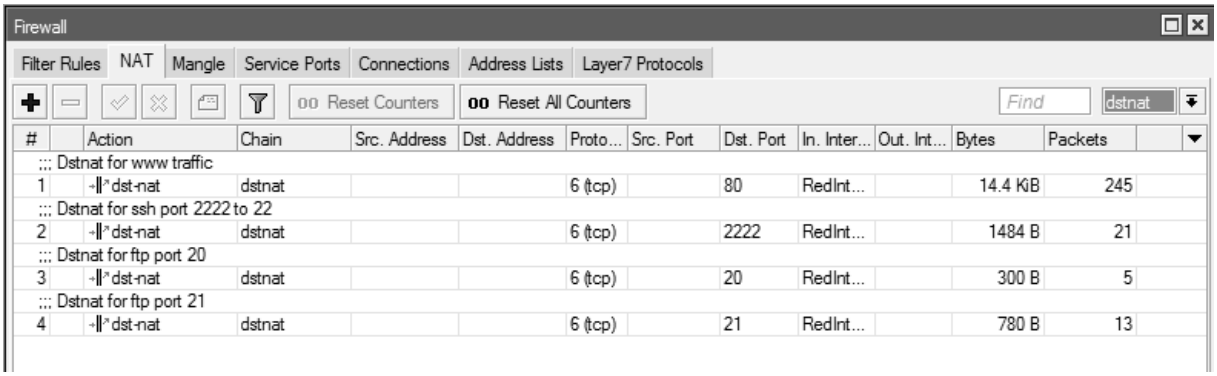


Als we pingen van green naar red, zien we dat het verkeer lijkt te komen van 10.5.0.254, en terug.

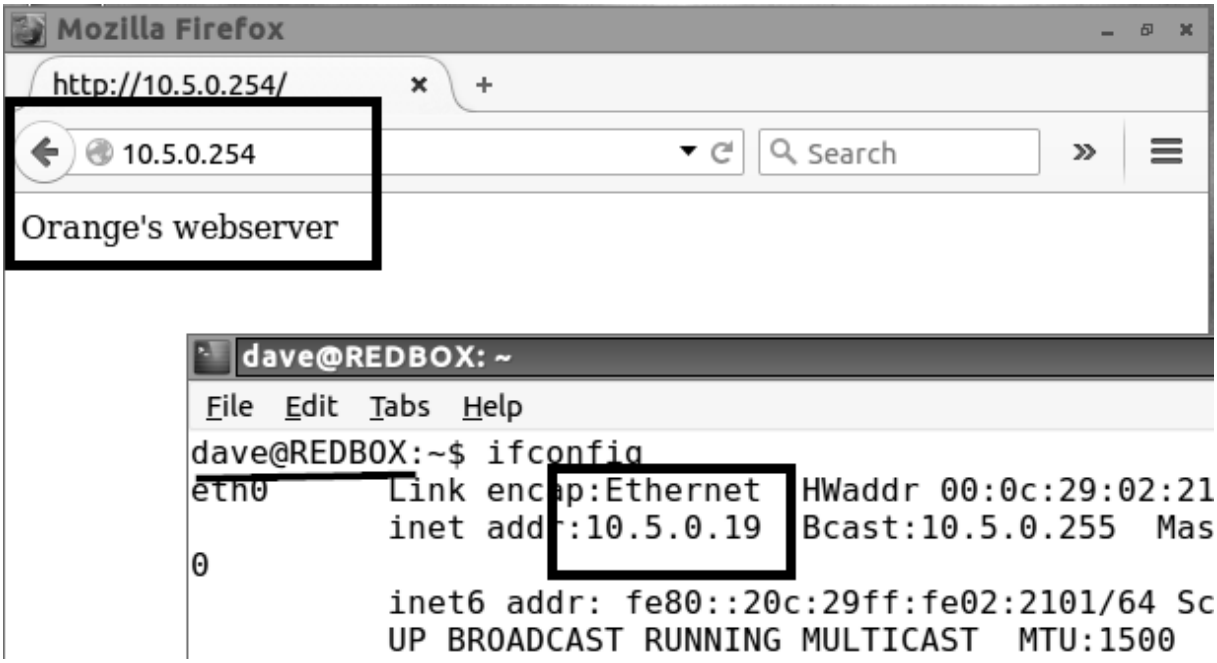
Source		Destination	Protocol	Info
10.5.0.254		10.5.0.19	ICMP	Echo (ping) request
10.5.0.19		10.5.0.254	ICMP	Echo (ping) reply
10.5.0.254		10.5.0.19	ICMP	Echo (ping) request
10.5.0.19	⟷	10.5.0.254	ICMP	Echo (ping) reply
10.5.0.254		10.5.0.19	ICMP	Echo (ping) request
10.5.0.19		10.5.0.254	ICMP	Echo (ping) reply
10.5.0.254		10.5.0.19	ICMP	Echo (ping) request
10.5.0.19		10.5.0.254	ICMP	Echo (ping) reply
10.5.0.254		10.5.0.19	ICMP	Echo (ping) request
10.5.0.19		10.5.0.254	ICMP	Echo (ping) reply

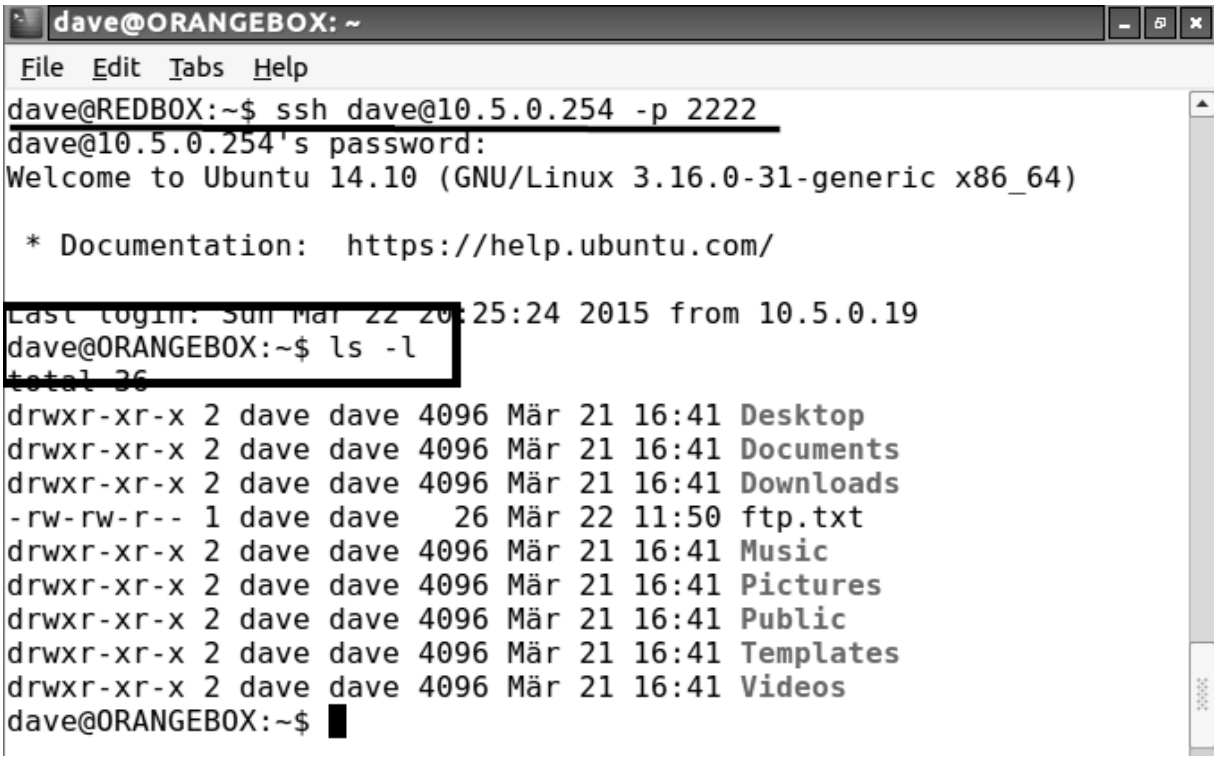
Om te zorgen dat men vanuit de rode zone de servers kan bereiken moeten we ook aan destination NATting doen of te wel port forwarding.

We sturen dus bvb. verkeer dat binnenkomt bij 10.5.0.254 op poort 80 naar poort 80 van 10.3.0.19



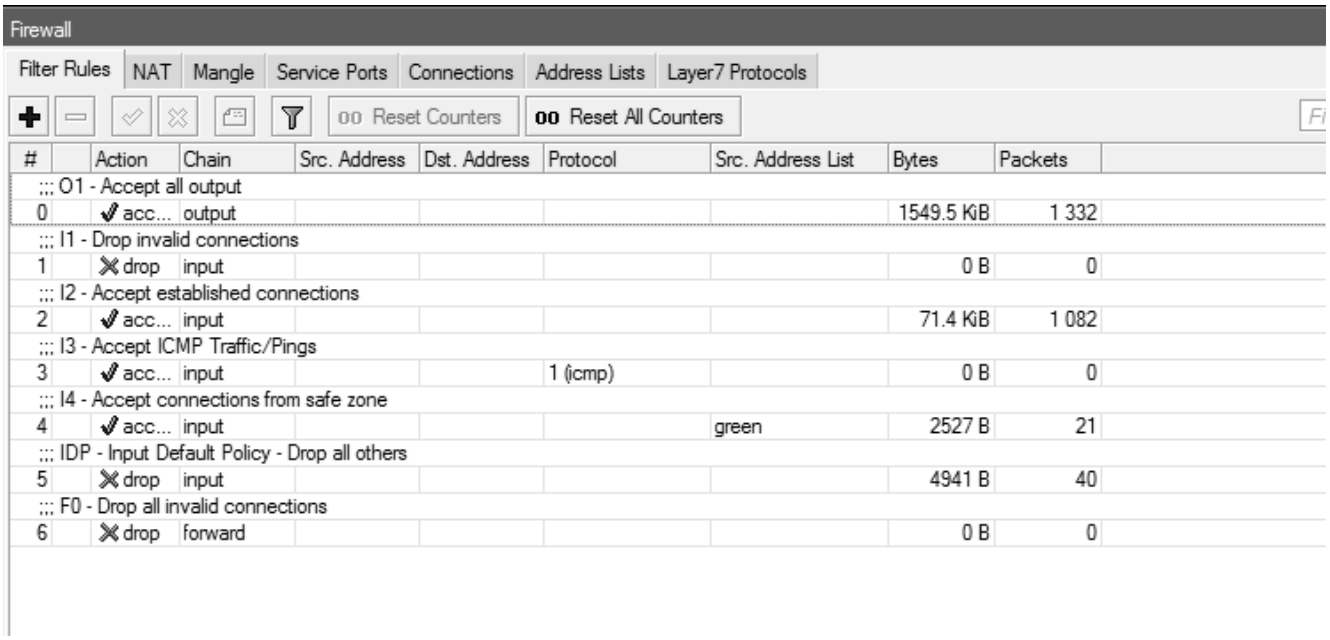
Nu gaan we de port forwards testen.




dave@ORANGEBOX: ~
File Edit Tabs Help
dave@REDBOX:~$ ssh dave@10.5.0.254 -p 2222
dave@10.5.0.254's password:
Welcome to Ubuntu 14.10 (GNU/Linux 3.16.0-31-generic x86_64)
* Documentation: https://help.ubuntu.com/
Last login: Sun Mar 22 20:25:24 2015 from 10.5.0.19
dave@ORANGEBOX:~$ ls -l
total 36
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Desktop
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Documents
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Downloads
-rw-rw-r-- 1 dave dave 26 Mär 22 11:50 ftp.txt
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Music
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Pictures
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Public
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Templates
drwxr-xr-x 2 dave dave 4096 Mär 21 16:41 Videos
dave@ORANGEBOX:~$

De router beschermen

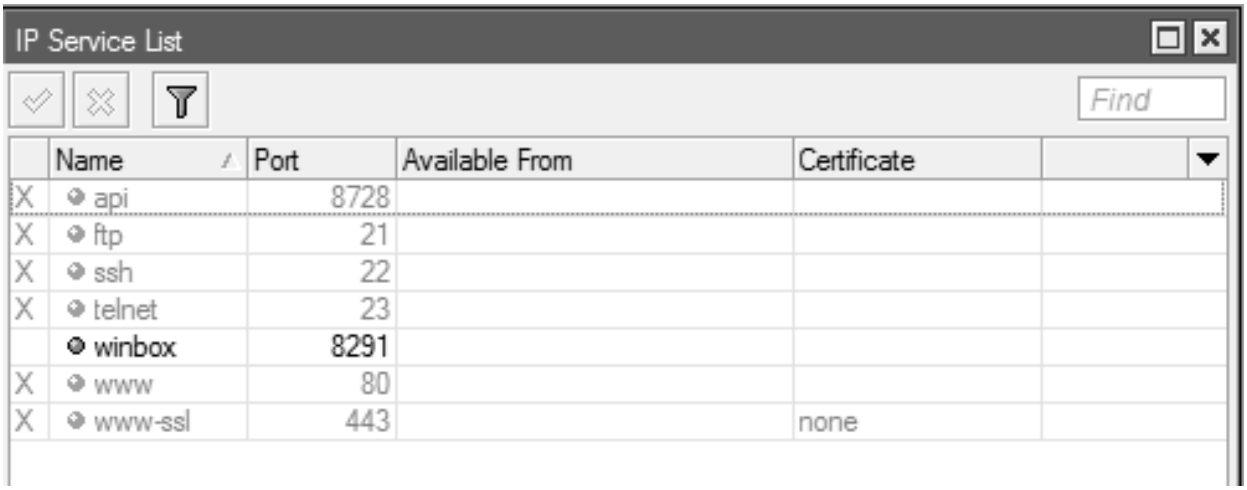
Om de router te beschermen, maken we enkele firewall-regels aan in de input-chain.



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Address List	Bytes	Packets
;;; O1 - Accept all output								
0	acc...	output					1549.5 KiB	1 332
;;; I1 - Drop invalid connections								
1	drop	input					0 B	0
;;; I2 - Accept established connections								
2	acc...	input					71.4 KiB	1 082
;;; I3 - Accept ICMP Traffic/Pings								
3	acc...	input			1 (icmp)		0 B	0
;;; I4 - Accept connections from safe zone								
4	acc...	input				green	2527 B	21
;;; IDP - Input Default Policy - Drop all others								
5	drop	input					4941 B	40
;;; F0 - Drop all invalid connections								
6	drop	forward					0 B	0

We laten alle output toe.

Ook zorgen we ervoor dat we de router alleen kunnen configureren met Winbox.



	Name	Port	Available From	Certificate	
X	api	8728			
X	ftp	21			
X	ssh	22			
X	telnet	23			
	winbox	8291			
X	www	80			
X	www-ssl	443		none	

Dit, samen met regel I4 zorgt ervoor dat we de router alleen kunnen configureren met Winbox, vanuit het 10.1.0.0/24 netwerk.

Forward regels

De regels die in de forward-chain staan regelen het heen- en weer-verkeer naar of van de hosts. Deze regels zal ik vermelden in de configuratie (volgend hoofdstuk).

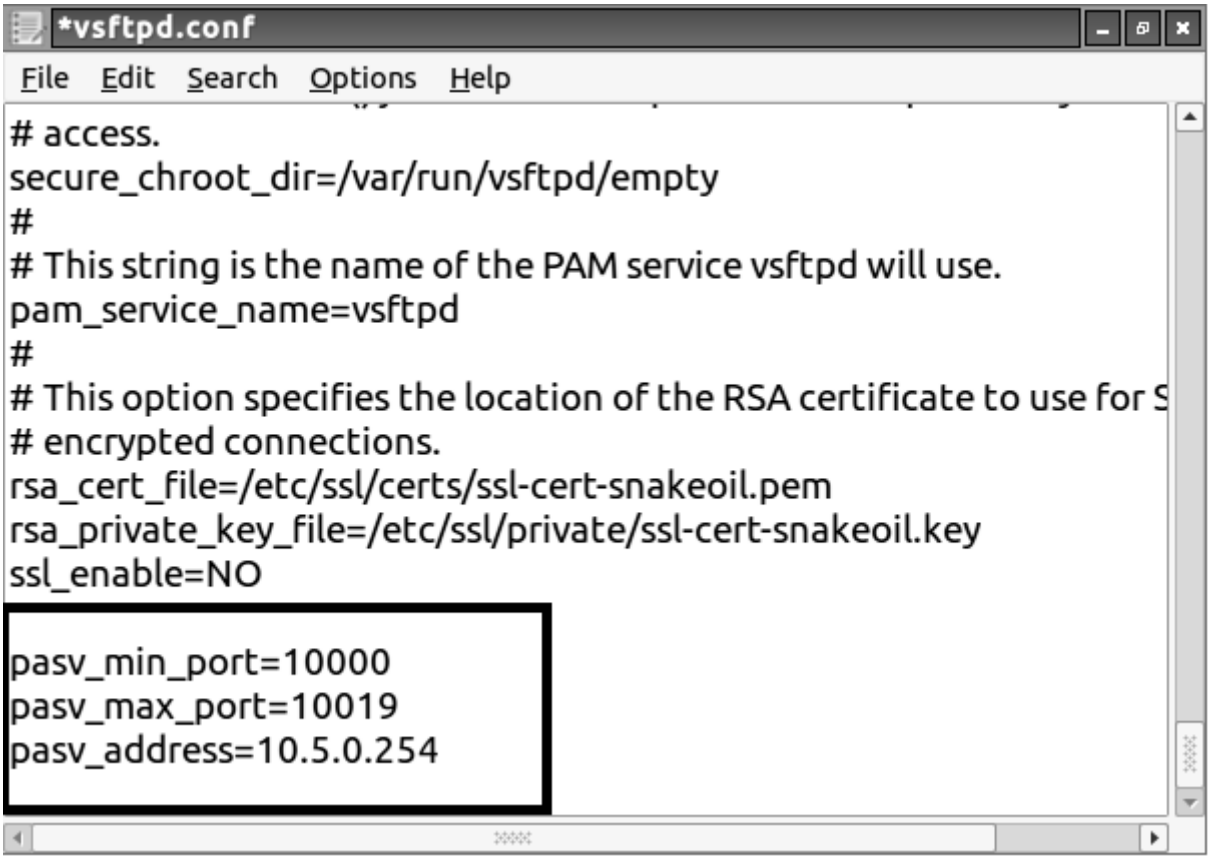
We testen de ftp-server:

```
dave@REDBOX:~$ ftp 10.5.0.254
Connected to 10.5.0.254.
220 Welcome to Orange FTP service.
Name (10.5.0.254:dave): dave
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get ftp.txt
local: ftp.txt remote: ftp.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp.txt (26 bytes
226 Transfer complete.
26 bytes received in 0.03 secs (0.8210 kB/s)
ftp>
```

Om FTP aan de gang te krijgen moest ik in de configuratiebestand (vsftpd.conf) van vsftpd wel zeggen welke poorten er gebruikt mochten worden voor passieve communicatie. Ik koos hiervoor voor 10000 en 10019. Zo kon ik FTP gebruiken, maar toch nog het aantal open poorten beperken.

De pasv_address parameter moeten we zetten zodat we FTP met NAT kunnen gebruiken. Dit zorgt ervoor dat het opgegeven IP-adres wordt gebruikt, in plaats van het IP-adres van de server.

De instelling bij vsftpd:

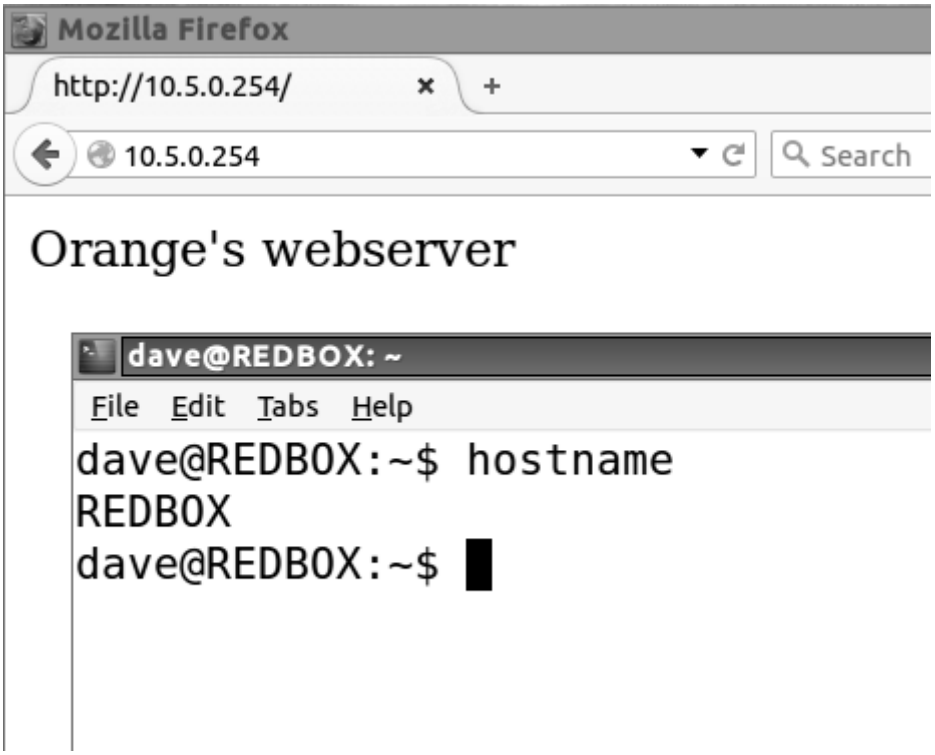


Nu dat FTP werkt, testen we ssh:

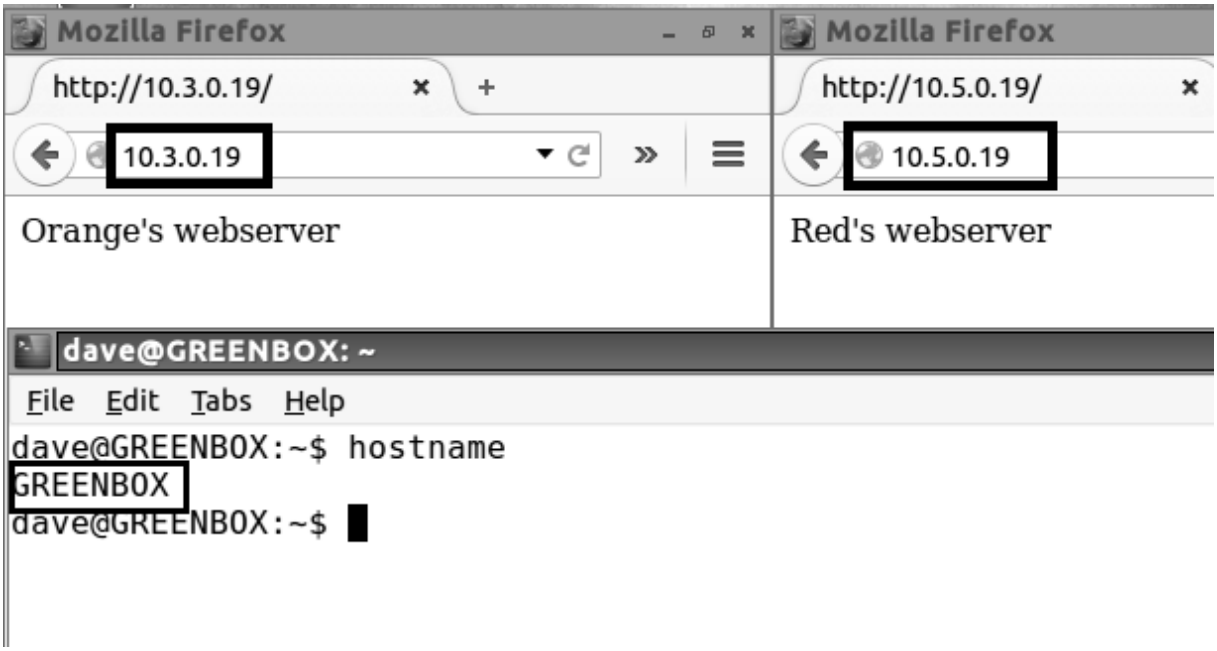
```
dave@REDBOX:~$ ssh dave@10.5.0.254 -p 2222
dave@10.5.0.254's password:
Welcome to Ubuntu 14.10 (GNU/Linux 3.16.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Sun Mar 22 20:32:11 2015 from 10.5.0.19
dave@ORANGEBOX:~$ exit
logout
Connection to 10.5.0.254 closed.
dave@REDBOX:~$ ssh dave@10.5.0.254
^C
dave@REDBOX:~$
```

Op poort 2222 werkt ssh perfect, maar als we op poort 22 proberen te verbinden, lukt dit niet.

Ook webverkeer werkt:



En dan vanaf de groene host:



Netwerkscan na de instelling van de firewall

Na het instellen van de firewall deed ik opnieuw nmap-scans vanaf de rode host.

Eerst scande ik de router:

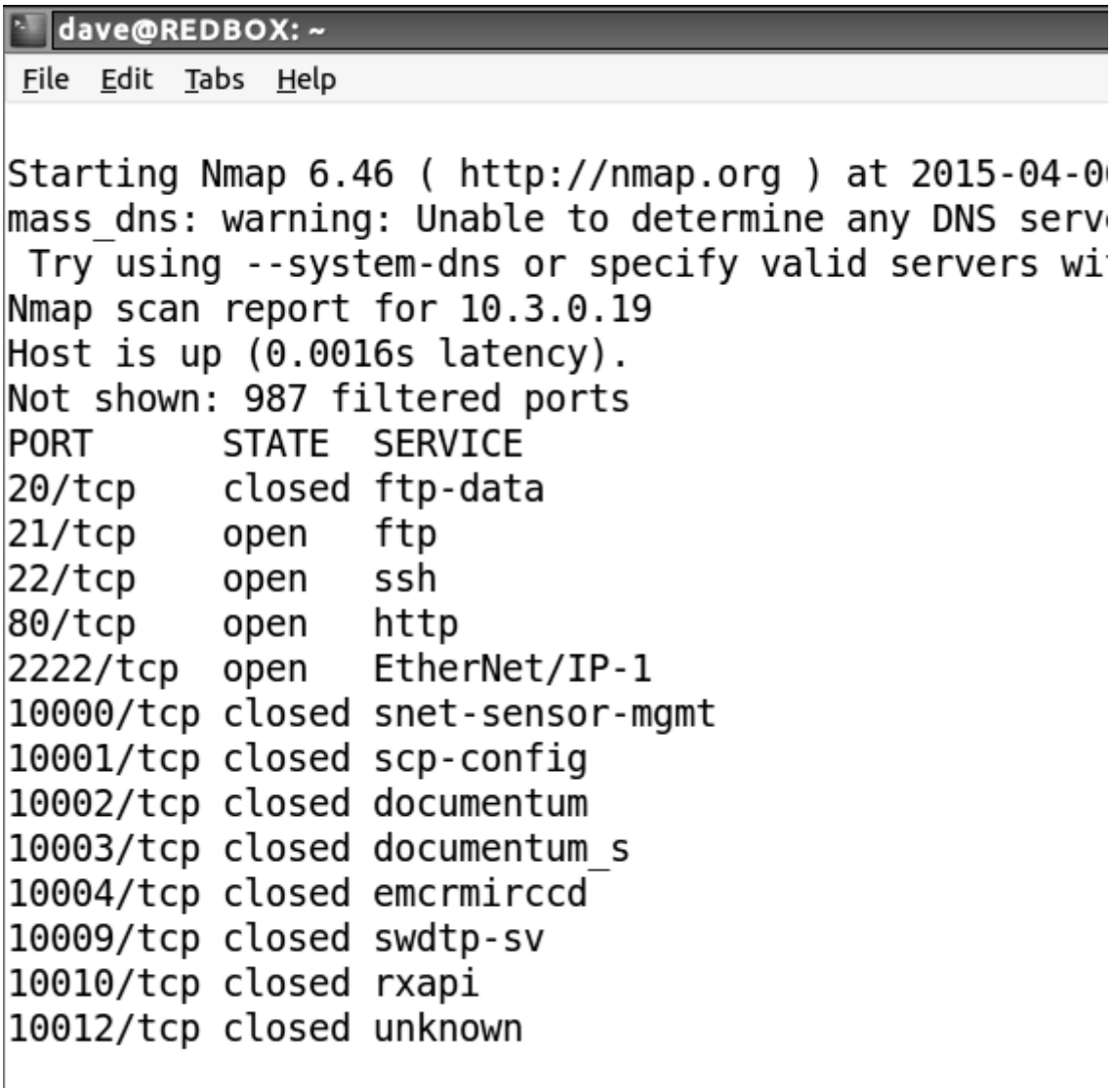
```
dave@REDBOX:~$ #nmap davyguard red side
dave@REDBOX:~$ nmap -Pn 10.5.0.254

Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-06 13:20 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is d
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.5.0.254
Host is up (0.0012s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
80/tcp   open   http
2222/tcp open   EtherNet/IP-1

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
dave@REDBOX:~$
```

Daarna scande ik de groene host. Ik merkte op dat het resultaat net hetzelfde was als de vorige scan.

```
dave@REDBOX:~$ #nmap green host from red side
dave@REDBOX:~$ nmap -Pn 10.1.0.19

Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-06 13:22 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is d
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.0.19
Host is up (0.0015s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
80/tcp   open   http
2222/tcp open   EtherNet/IP-1

Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds
dave@REDBOX:~$
```

Resultaat van davyguard?

Maar als ik dan de oranje host scan, zie ik het volgende:



Ik heb niet kunnen ontdekken of dit gewenst is of niet. Ik vind dit minder gewenst, alhoewel het niet zeker is dat iemand die van buiten af een Nmap-scan uitvoert interne IP's kent

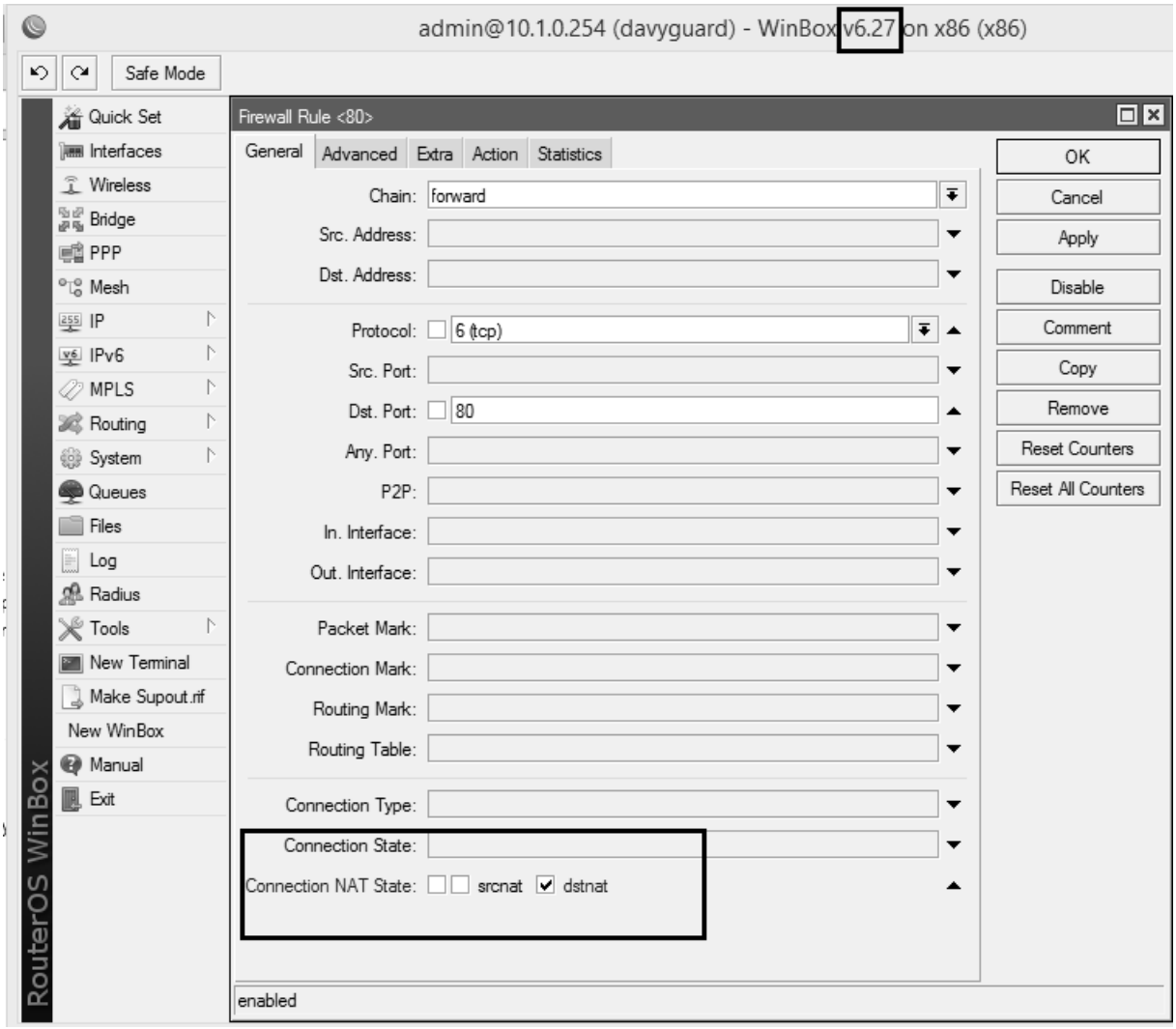
Surf probleem

Nadat ik de oefening had uitgevoerd zag ik dat er ongewenst gedrag qua http-verkeer voorkwam. Dit bestond uit twee zaken:

1. Als ik van Red Host naar Orange Host surfte met het rechtstreekse IP-nummer van de Orange Host, kreeg ik toch de webpage van Orange Host te zien.
2. Als ik van Red Host naar Green Host surfte met het rechtstreekse IP-nummer van de Green Host, kreeg ik toch de webpage van Orange Host te zien.

Hier heb ik lang op zitten zoeken. De oplossing had ik nooit kunnen vinden zonder de hulpvolle tips van Eroovia. Deze persoon, in bezit van de Mikrotik-certificaten MTCNA, MTCWE, MTCTCE en MTCUME wees mij er op dat vanaf versie 6.22 er in RouterOS een "connection NAT state" –matcher bestond.

Deze optie gaat na of de pakketten door een NAT-regel gaan. We laten in deze regel dus alleen verkeer toe dat door de dst-nat gaat.



Nadat ik mijn RouterOS ge-upgradet had, merkte ik dat probleempunt 1 opgelost was, maar probleempunt 2 bleef bestaan.

Dit heb ik uiteindelijk opgelost door de dstnat-regel aan te passen: ik voegde een dst-address-list toe.

De regel die gedisabled staat in mijn firewall-configuratie, is nog een overblijfsel van het proberen op te lossen van deze problemen.

Firewall code

Uiteindelijke firewall configuratie

```
/ip firewall address-list
add address=10.1.0.0/24 list=green
add address=10.5.0.0/24 list=red
add address=10.3.0.0/24 list=orange
/ip firewall filter
add chain=output comment="O1 - Accept all output"
add action=drop chain=input comment="I1 - Drop invalid connections" \
    connection-state=invalid
add chain=input comment="I2 - Accept established connections" \
    connection-state=established
add chain=input comment="I3 - Accept ICMP Traffic/Pings" protocol=icmp
add chain=input comment="I4 - Accept connections from safe zone" \
    src-address-list=green
add action=drop chain=input comment=\
    "IDP - Input Default Policy - Drop all others"
add action=drop chain=forward comment="F0 - Drop all invalid connections"
\
    connection-state=invalid
add chain=forward comment="F1 - Established and related connections" \
    connection-state=established,related
add action=drop chain=forward comment=\
    "F2 - Block incoming new www with dst green" connection-state=new \
    disabled=yes dst-address-list=green dst-port=80 protocol=tcp
add chain=forward comment="F3 - Green www out" dst-port=80 protocol=tcp \
    src-address-list=green
add chain=forward comment="F4 - Orange to Red www" dst-address-list=red \
    dst-port=80 protocol=tcp src-address-list=orange
add chain=forward comment="F5 - Red to Orange www update" \
    connection-nat-state=dstnat dst-address-list=orange dst-port=80
protocol=\
    tcp src-address-list=red
add chain=forward comment="F6 - Accept SSH from outside to Orange" \
    dst-address-list=orange dst-port=22 protocol=tcp
add chain=forward comment="F7 - Accept SSH from Green" dst-port=22
protocol=\
    tcp src-address-list=green
add chain=forward comment="F8 - Accept FTP port 20 to Orange" dst-
address=\
    10.3.0.19 dst-port=20 protocol=tcp
add chain=forward comment="F9 - Accept FTP port 21 to Orange" dst-
address=\
    10.3.0.19 dst-port=21 protocol=tcp
add chain=forward comment="F10 - Accept FTP PSV limited on SRV" dst-
address=\
    10.3.0.19 dst-port=10000-10019 protocol=tcp
add action=drop chain=forward comment="F11 - Drop all others"
/ip firewall nat
add action=masquerade chain=srcnat comment=Srcnat out-
interface=RedInterface
```

```
add action=dst-nat chain=dstnat comment="Dstnat for SSH to Orange" dst-
port=\
    2222 in-interface=RedInterface protocol=tcp src-address-list=red \
    to-addresses=10.3.0.19 to-ports=22
add action=dst-nat chain=dstnat comment="Dstnat for www" dst-address-
list=red \
    dst-port=80 in-interface=RedInterface protocol=tcp to-
addresses=10.3.0.19 \
    to-ports=80
add action=dst-nat chain=dstnat comment="Dstnat for ftp port 20" dst-
port=20 \
    in-interface=RedInterface protocol=tcp src-address-list=red to-
addresses=\
    10.3.0.19
add action=dst-nat chain=dstnat comment="Dstnat for ftp port 21" dst-
port=21 \
    in-interface=RedInterface protocol=tcp src-address-list=red to-
addresses=\
    10.3.0.19
/ip firewall service-port
set ftp disabled=yes
set tftp disabled=yes
set irc disabled=yes
set h323 disabled=yes
set sip disabled=yes
set pptp disabled=yes
```

Extra: chatten tussen twee hosts met netcat

We gaan nu tussen red host en orange host een chat-sessie opzetten, door middel van netcat. Netcat is een veelzijdige service die naar netwerkconnecties kan lezen en schrijven.

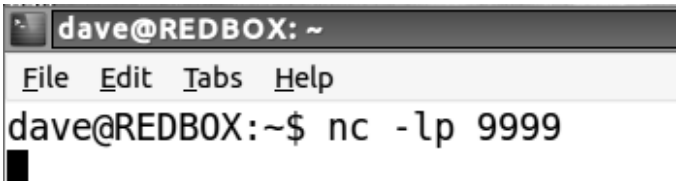
Bij de red host wordt netcat opgezet als “listener”, terwijl we op orange host een connectie gaan maken. De listener luistert op TCP poort 9999.

Om dit mogelijk te maken heb ik op de firewall regel F11 (de default drop voor de forward chain) naar F12 verplaatst. Daarna heb ik een nieuwe F11 gemaakt:

```
/ip firewall filter add chain=forward comment="F11 - Chat test to red
9999" dst-address-list=red dst-port=9999 protocol=tcp src-address-
list=orange
```

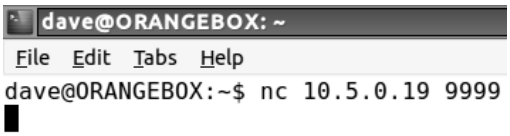
Dit is logisch, want de enige connectie die we toe moeten laten is die waarin de orange host probeert te communiceren met de red host, op poort 9999. Het luisteren zelf van de red host is geen actie die door de firewall gaat, en het antwoord terug naar orange behoort tot de “established” connecties.

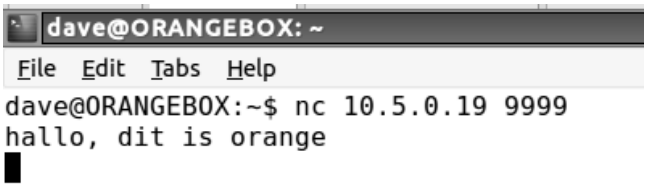
De chat-sessie ziet er dan zo uit:



Op REDBOX starten we de listener

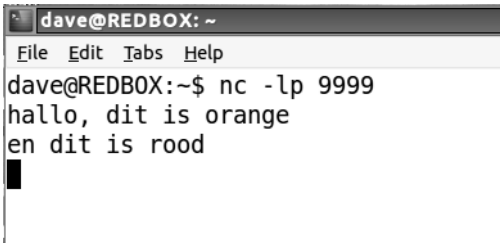
Daarna zetten we een connectie op met REDBOX, vanaf ORANGEBOX

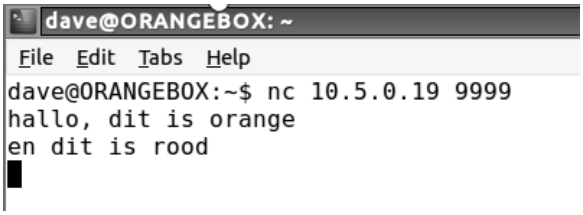




ORANGEBOX verstuurt een bericht

Waarna REDBOX dit bericht ontvangt, en een antwoord verstuurt.





ORANGEBOX krijgt het bericht binnen.

Observaties

Tijdens de realisatie van deze projecten in 2015 heb ik diverse technische en procesmatige inzichten opgedaan. Onderstaande punten vatten mijn belangrijkste leerervaringen samen:

Theoretische Fundering & CLI

- **Theorie als basis**: theoretische kennis is onmisbaar bij troubleshooting. Zonder begrip van de onderliggende architectuur (zoals OSPF area-types) is het onmogelijk om de oorzaak van een fout te herleiden.
- **Efficiëntie CLI:** Zodra de juiste commando's gekend zijn, werkt het aansturen via de commandline interface (CLI) soms sneller dan via een grafische interface (GUI)..

Documentatie & Softwareversies

- **Impact van versieverschillen:** Het is cruciaal om op softwareversies te letten bij het raadplegen van handleidingen en fora. Kleine verschillen tussen versies (zoals Apache 2.2 vs. 2.4) kunnen bepalend zijn voor een goede werking.
- **Bronkeuze:** Ik heb geleerd om eerst de originele manuals te raadplegen alvorens fora te bezoeken. Daarnaast loont het om changelogs te controleren; bij de MikroTik-firewalls loste een nieuwere versie bijvoorbeeld een specifiek probleem op.
- **Risico-afweging bij upgrades:** Een nieuwe versie kan een probleem oplossen, maar ook nieuwe complicaties veroorzaken. Het is essentieel om na te gaan of alle benodigde functionaliteit behouden blijft.

Projectaanpak & Beheersing

- **Voorbereiding:** Het vooraf uitwerken van persoonlijke schema's en tabellen was voor mij essentieel om dagelijks het overzicht te bewaren.
- **Stapsgewijs opbouwen:** Begin klein. Het heeft geen zin om een complexe DNS-structuur (masters, slaves) op te zetten als een simpele basisopstelling met één zone nog niet correct functioneert.
- **Zekerheid door back-ups:** De kracht van regelmatige back-ups en snapshots is onmisbaar. Het stelt je in staat om bij incidenten snel en gemakkelijk stappen ongedaan te maken en terug te keren naar een werkend punt.

Bronnen

1. Postfix: The Definitive Guide (Kyle D Dent), O'reilly
2. Advanced Linux Programming (Mark Mitchell, Jeffrey Oldham, Alex Samuel), New Riders Publishing
3. Inter Process Communication: http://www.tldp.org/LDP/lpg/node7.html
4. Inter Process Communication: http://www.tldp.org/LDP/tlk/ipc/ipc.html
5. Bind9: https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-14-04
6. Bind9: https://www.madboa.com/geek/soho-bind/#localdomain
7. Bind9: http://mixeduperic.com/ubuntu/seven-easy-steps-to-setting-up-an-interal-dns-server-on-ubuntu.html
8. Bash-guide: http://mywiki.wooledge.org/BashGuide
9. Het originele NoIP-updater script: https://github.com/AntonioCS/no-ip.com-bashupdater/blob/master/noipupdater.sh
10. Cronjob manual: https://help.ubuntu.com/community/CronHowto
11. Wikipedia: http://en.wikipedia.org/wiki/Here_document#Here_strings
12. Bash-guide: http://mywiki.wooledge.org/BashGuide/InputAndOutput#Heredocs_And_Herestrings
13. Bash CGI programming: http://www.team2053.org/docs/bashcgi/gettingstarted.html
14. W3 Schools CSS how-to: http://www.w3schools.com/Css/css_howto.asp
15. Install packages from cd: http://askubuntu.com/questions/129942/installing-packages-from-ubuntu-cd
16. Add a network card, commandline: https://bowerstudios.com/node/1015
17. Manual ifup: http://manpages.ubuntu.com/manpages/oneiric/man8/ifdown.8.html
18. Ubuntu server hostname: http://askubuntu.com/questions/9540/how-do-i-change-the-computer-name
19. Apt-get remove: http://askubuntu.com/questions/231562/what-is-the-difference-between-apt-get-purge-and-apt-get-remove
20. Firefox proxy-types: http://kb.mozillazine.org/Network.proxy.type#5_5
21. Rootless Android SSH tunneling: https://www.youtube.com/watch?v=KKhhBttwUpI
22. SSH Copy ID: http://linux.die.net/man/1/ssh-copy-id
23. Log in at SSH without passwords: http://www.thegeekstuff.com/2008/11/3-steps-to-perform-ssh-login-without-password-using-ssh-keygen-ssh-copy-id/
24. Unison: https://www.howtoforge.com/setting-up-unison-file-synchronization-between-two-servers-on-debian-squeeze
25. Incron 1: https://www.howtoforge.com/triggering-commands-on-file-or-directory-changes-with-incron
26. Incron 2: http://inotify.aiken.cz/?section=incron&page=doc
27. LDAP-scripts: http://www.meso.northwestern.edu/intranet/recipies/useful-computer-files-and-programs/configuring-group-linux-servers-and-terminals-with-ldap-kerberos-and-nfs/ldap-user-and-group-management

28. PHP LDAP: http://www.phpdig.net/ref/rn33re626.html
29. PHP LDAP: http://www.phpdig.net/ref/rn33re638.html
30. PHP LDAP scripting: http://www.oit.uci.edu/idm/campusids/ldap-query-code-example-php/
31. LDAP Theory: http://www.zytrax.com/books/ldap/apa/dn-rdn.html
32. LDAP ACL: http://www.zytrax.com/books/ldap/ch6/
33. LDAP Theory and ACL: https://help.ubuntu.com/lts/serverguide/openldap-server.html
34. LDIF,LDAP and ACL: http://serverfault.com/questions/316838/ldap-acls-with-ldapmodify-ldif-file-grand-user-access-only
35. Beginning PHP and MySQL: From Novice to Professional, door W. Jason Gilmore
36. PHP Functions Essential Reference, door Zack Greant
37. Ubuntu 14, Apache en LDAP: http://askubuntu.com/questions/481917/apache2-4-7-ldap-url-authentication-on-ubuntu-14-04
38. Apache en LDAP: http://technedigitale.com/archives/254
39. Mod_authnz_ldap: http://httpd.apache.org/docs/2.4/mod/mod_authnz_ldap.html
40. Apache authorization guide: http://httpd.apache.org/docs/2.4/howto/auth.html
41. Nmap: http://nmap.org/book/man-host-discovery.html
42. FTP en firewalls: http://www.whitneytechnologies.com/?p=23
43. Eroviaa, MikroTik Certified Network Associate, Wireless Engineer, Traffic Control Engineer, User Management Engineer, Hongarije
44. Squirrelmail: http://www.krizna.com/ubuntu/setup-mail-server-ubuntu-14-04/#squirrelmail
45. Fetchmail: https://www.linode.com/docs/email/clients/using-fetchmail-to-retrieve-email
46. Postfix,courier,SASL: http://jonsview.com/setting-up-email-services-on-ubuntu-hardy-using-postfix-and-courier
47. Courier: https://help.ubuntu.com/community/Courier
48. Postfix: https://help.ubuntu.com/community/PostfixBasicSetupHowto#Install_Postfix
49. Onofficiële RouterOS changelog verzameling: http://www.tnsolutions.ro/routeros-changelog/
50.