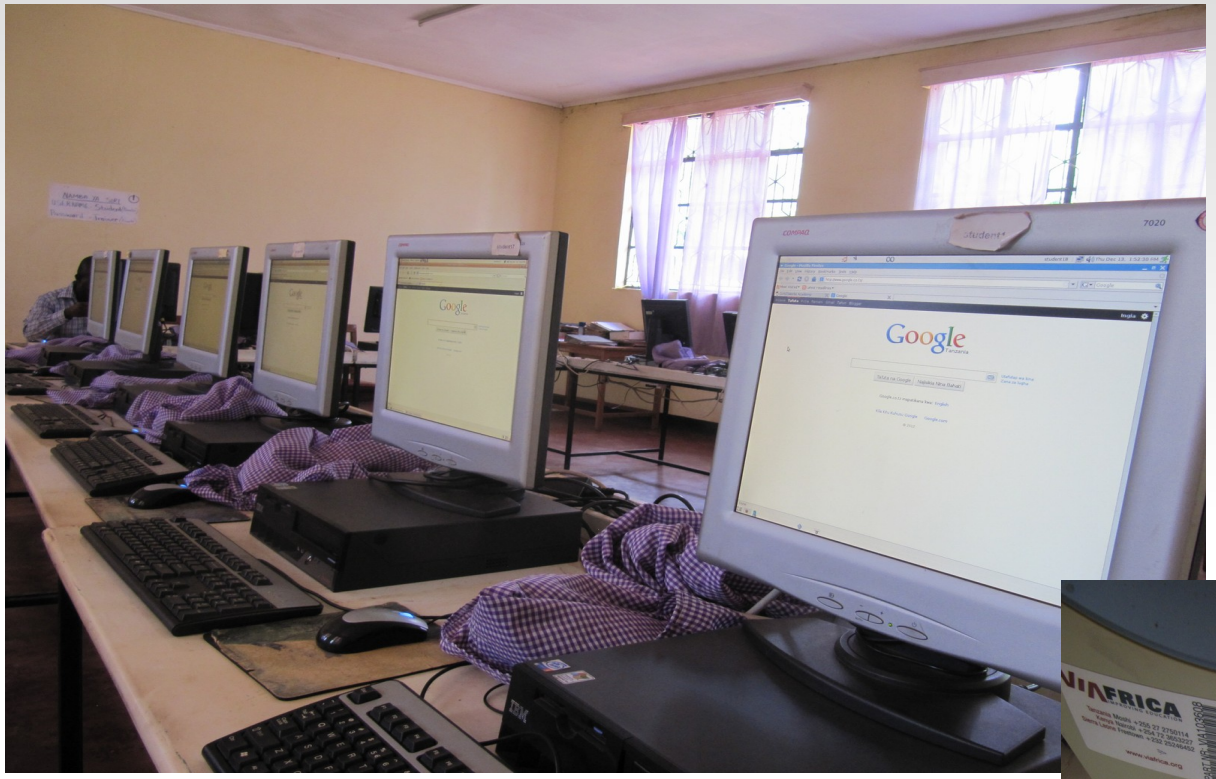
Een Afrikaanse schoolserver



Condities (in Tanzania)

- oude computers
- stroomuitval
- stof
- vooral 3G Internet (als er dekking is)
  - vrijwel geen vaste lijn infrastructuur (is aan het veranderen)
  - beperkte bandbreedte
  - veelal prepaid
  - relatief goedkoop!
- beperkte computer kennis
- veelal grote afstanden en slechte wegen
- weinig geld

Eisen

- LAN
- als internet dekking:
  - Optimaal gebruik beperkte bandbreedte
  - Remote monitoring en beheer
- ondersteuning van diverse clients in het LAN (PC's, tablets, (smart)phones)
  - minimale client configuratie
- toegang tot (educatieve) software
- centrale file opslag voor studenten en leraren
- backup functionaliteit
- veilig

LAN en (bij dekking) Internet connectiviteit

- gebruik network-interface for LAN
- gebruik 3G modem for internet (prepaid)
  - opwaarderen via mobiele telefoon
- autodetectie en inbellen met een udev rule

```
# cat /etc/udev/rules.d/modem.rules

ACTION=="add", ATTRS{idVendor}=="12d1", RUN+="/usr/local/bin/dial"
```

- ip forwarding (/etc/sysctl.conf)

```
net.ipv4.ip_forward=1
```

- NAT voor het LAN


```
/sbin/iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -j MASQUERADE
```

Optimimaal gebruik beperkte bandbreedte

- ”mirror” websites naar lokale disk (httrack)
  - is alleen een momentopname, niet ideaal voor veel veranderende en/of dynamische sites
  - uiteraard toestemming nodig
- gebruik een ”caching proxy” (squid) voor web verkeer
- maak deze proxy transparant (minder client configuratie)
  - in squid.conf:

```
http_port 3128 transparent
```

  - in /etc/rc.local:

```
/sbin/iptables -t nat -A PREROUTING -i eth1 -p tcp \
        --dport 80 -j DNAT --to 192.168.3.1:3128
```

Ondersteuning van diverse clients (PC's, tablets, (smart) phones)

- gebruik een wireless access point (AP)
  - bv. een 3G modem met AP functionaliteit (nu nog niet)
- gebruik een lokale dns-server
  - authoratative voor de gemirrorde websites
  - geen aanpassing nodig van host files (minder client configuratie, is soms zelfs niet of moeilijk mogelijk)
- gebruik een lokale dhcp-server
  - automatisch IP's uitdelen (minder client configuratie)
  - wijs naar de lokale dns-server
- gebruik zoveel mogelijk ”web based” content
- maak proxy transparant (minder client configuratie)

Toegang tot (educatieve) software

- Edubuntu op clients (GCompris, Tux4Kids, ...)
- lokale website
- gemirrorde websites voor lokaal (en ”offline”) gebruik
  - www.elearningforkids.org, www.sheppardsoftware.com, www.animations.physics.unsw.edu.au, ...
    - gebruik de dns-server (bind) als master voor de gemirrorde sites:

```
www.elearningforkids.org -> 192.168.3.1
www.sheppardsoftware.com -> 192.168.3.1
...
```

  - ”wikipedia for schools” (oud, wordt vervangen door de ”simple English Wikpedia” en mogelijk ook de Swahili wikipedia)

Centrale file opslag voor studenten en leraren

- samba
  - stukje uit /etc/samba/smb.conf:

```
[students]
comment = students share
path = /shares/students
guest ok = no
public = no
valid users = @students, teacher
admin users = teacher
browseable = yes
writeable = yes

[lessons]
comment = lessons share
path = /shares/lessons
guest ok = no
public = no
valid users = @students, teacher
admin users = teacher
browseable = yes
writeable = yes
read list = @students
write list = teacher
```

Let op: Linux permissies gaan *voor* samba permissies!

Backup functionaliteit

- backup-script (rsync) in cron, in te toekomst misschien backuppc
- backup naar lokale usb-disk
- indien internet: backup over internet naar een centrale server (let op bandbreedte gebruik, bv rsync met --bwlimit).

Veilig

- geen login toegestaan
- anti-virus (clamav voor samba shares)
- run services alleen lokaal (apache/dns/dhcp op LAN-interface, mysql op localhost, ...)
- ”normaal” is 3G ”ge-NAT”
- gebruik een packetfilter (bv. m.b.v. shorewall)
- gebruik tcp-wrapping (/etc/hosts.allow, /etc/hosts.deny)
- remote beheer met ssh

Remote monitoring en beheer

- afstanden en toestand wegen
- voor connectie met het 3G IP-adres wordt een (open)vpn tunnel gebruikt:
  - 3G IP-addressen zijn veelal dynamisch
  - 3G IP-addressen kunnen ”ge-NAT” zijn (..)
- vpn *server* is openvpn.viafrica.net
  - de school*server* is de *client*
- monitoring met nagios en nrpe (door de vpn tunnel)
- login met ssh (door de vpn tunnel)
- updates met rsync (door de vpn tunnel)

```
rsync -aze ssh --delete --bwlimit=256 \
  /var/www/mirrors/ new.site.org \
  10.1.1.113:/var/www/mirrors
```

openvpn server configuratie (1)

- veel mogelijkheden
  - client <-> server (onze configuratie)
  - speciale routering per client
  - client-to-client: clients in een vpn *netwerk*

openvpn server configuratie (2)

- voorbeeld /etc/openvpn/server.conf

```
dev tun0
tls-server
dh dh1024.pem
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
comp-lzo
daemon
persist-tun
persist-key
keepalive 10 60
verb 3
server 10.1.0.0 255.255.255.0
max-clients 1000
port 1194
proto udp
ifconfig-pool-persist ipp.txt
client-config-dir clients
route 10.1.0.0 255.255.0.0
tls-auth ta.key 0 # This file is secret
status openvpn-status.log
log openvpn.log
```

openvpn server configuratie (3)

- voorbeeld simpele client <-> server

```
root@simba:~# cat /etc/openvpn/clients/Mwereni
ifconfig-push 10.1.1.113 10.1.1.114
```

- voorbeeld met extra routering voor 1 client

```
root@simba:~# cat /etc/openvpn/clients/samsung
ifconfig-push 10.1.1.115 10.1.1.116
# colo net
push "route 217.149.194.128 255.255.255.224"
# viafrica servers
push "route 78.31.117.0 255.255.255.128"
```

  - routetabel

```
oscar@samsung:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.5.11    0.0.0.0         UG    0      0        0 wlan0
10.1.0.1        10.1.1.116      255.255.255.255 UGH   0      0        0 tun0
10.1.1.116      0.0.0.0         255.255.255.255 UH    0      0        0 tun0
78.31.117.0     10.1.1.116      255.255.255.128 UG    0      0        0 tun0
78.31.117.99    192.168.5.11    255.255.255.255 UGH   0      0        0 wlan0
192.168.5.0     0.0.0.0         255.255.255.0   U     2      0        0 wlan0
217.149.194.128 10.1.1.116      255.255.255.224 UG    0      0        0 tun0
```

openvpn client configuratie

- voorbeeld /etc/openvpn/client.conf

```
client
dev tun
proto udp
remote openvpn.viafrica.net 1194
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
ca /etc/openvpn/certs/ca.crt
cert
/etc/openvpn/certs/schoolserver.crt
key /etc/openvpn/certs/schoolserver.key
ns-cert-type server
tls-auth /etc/openvpn/certs/ta.key 1
comp-lzo
verb 3
```

Samenvatting ingredienten

oude computers

beperkte bandbreedte

apache / mysql / php

routering / firewall: iptables / shorewall

caching proxy (squid)

beperkt budget

automatisch inbellen (udev / wvdial)

nagios client, nrpe

scripting (backup met rsync)

dhcp-server

dns-server

veilig (geen virussen)

openvpn

centrale opslag (samba)

ssh toegang

Linux! :)

Referenties

- OpenVPN opties:
  - http://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.html
- BackupPC
  - http://backuppc.sourceforge.net/
- meer over 3G en udev:
  - http://www.kwalinux.nl/3g-in-afrika/2529/