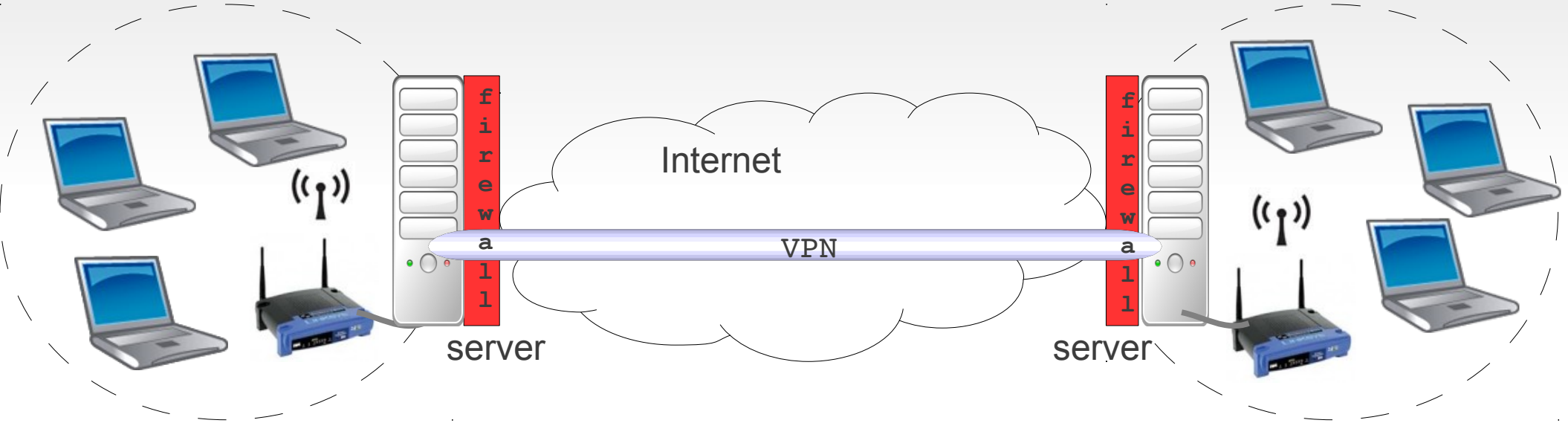
Workshop OpenVPN

openvpn configuraties (1/3)

office <-> office (connect afdelingen)



Office

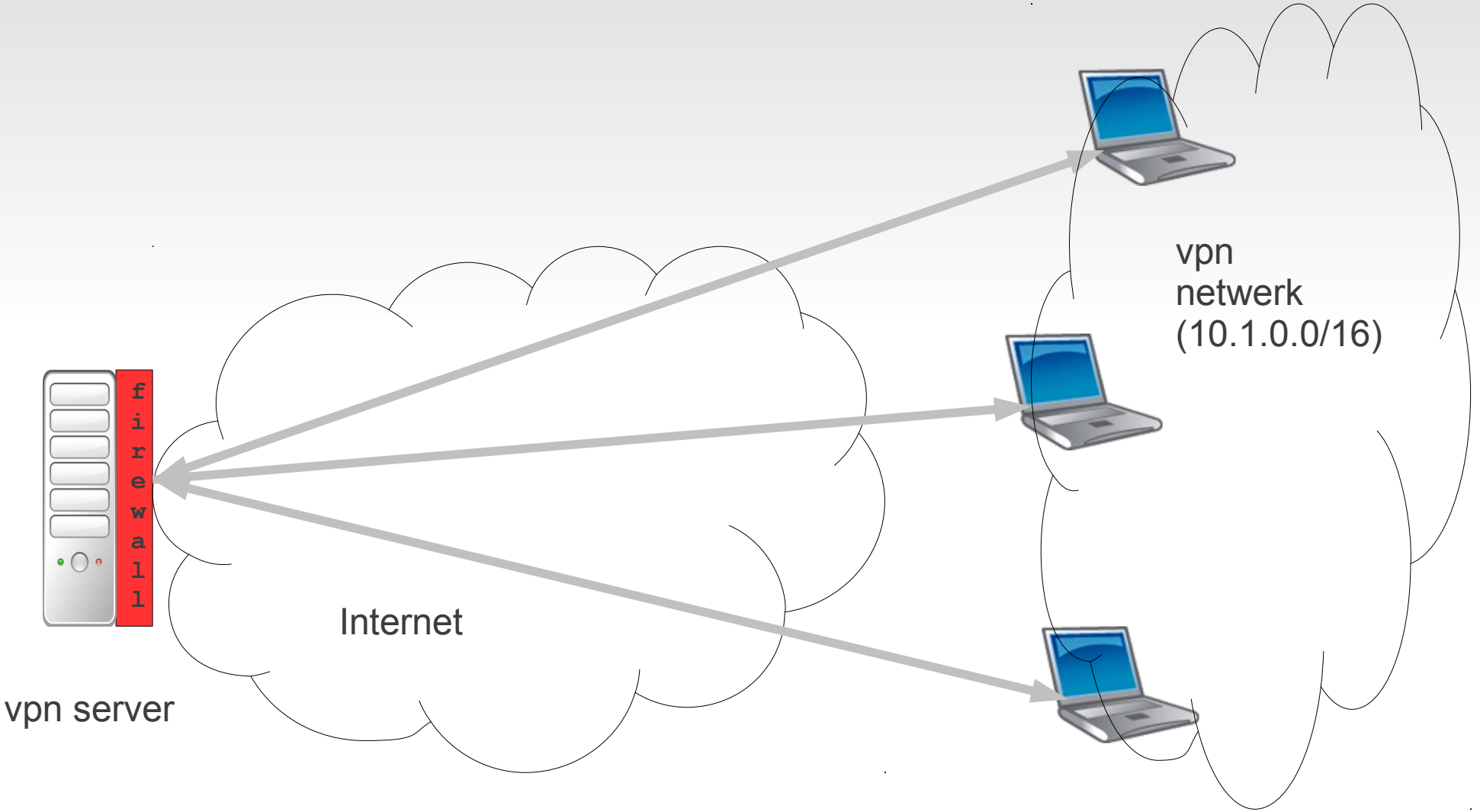
192.168.1.0/24

Office

10.5.0.0/16

openvpn configuraties (2/3)

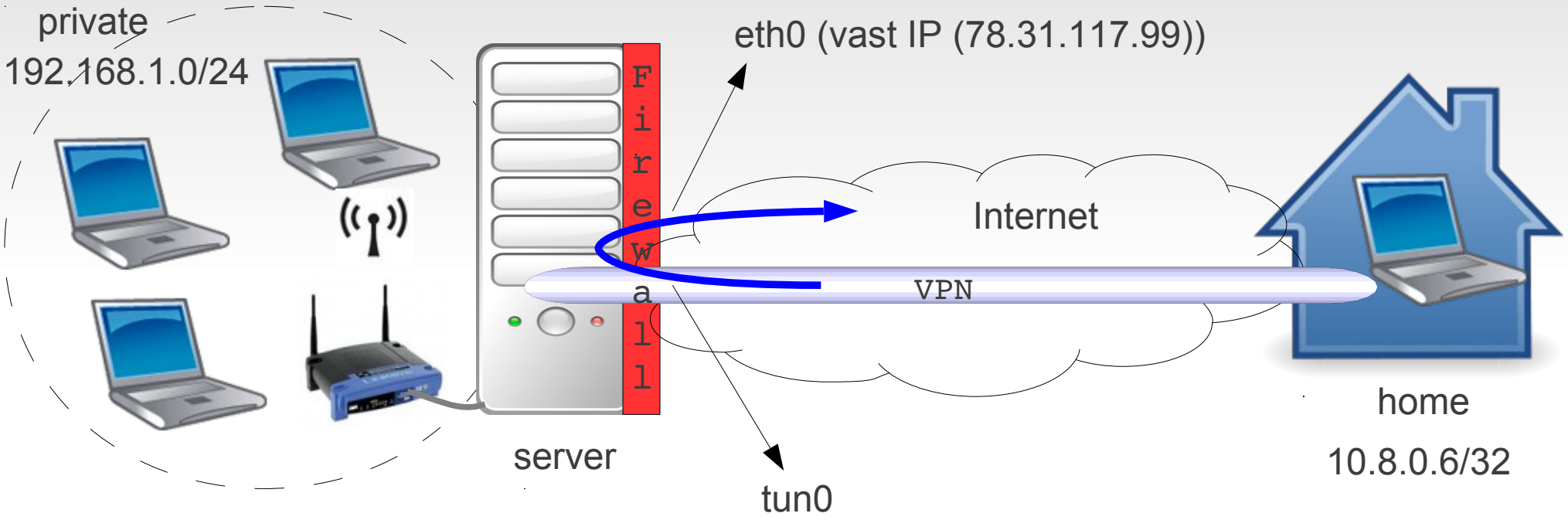
server <-> clients (maak vpn netwerk)



openvpn configuraties (3/3)

server <-> home (thuiswerkers, ”road warriors”

(alle verkeer of alleen extra routes door tunnel)



Let op: verkeer voor ”internet” komt binnen op tun0 (10.1.0.0/23) en moet naar buiten via eth0 (78.31.117.99/32) -> S(ource)NAT nodig voor dit verkeer:

```
/sbin/iptables -t nat -A POSTROUTING -o eth0 -s 10.1.0.0/23 -j SNAT --to-source 78.31.117.99
```

Je komt dan richting Internet vanaf vast IP-adres 78.31.117.99. Dit is handig voor toegang (ssh/imap/smtp/http/https) en/of firewalls.
Denk bv. ook aan blokkeren van buitelandse IP's voor internetbankieren..

routering en DNS

Alle verkeer door de tunnel (default gateway -> tunnel):

- kan server-side geset worden
- client-side kan dit ook regelen (en overruled de server-side setting)

Zorg ook dat de client kan resolven:

- geef DNS-servers mee in de server-config:
  - `push "dhcp-option DNS \"217.149.196.6 217.149.192.6\""`
- of kies bv. voor open DNS servers op de client in `/etc/resolv.conf` (maar pas op overwrites op de desktop van je NetworkManager!)

openvpn server configuratie (1/2)

- 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
tls-auth ta.key 0 # This file is secret
status openvpn-status.log
log openvpn.log
```

openvpn server configuratie (2/2)

- voorbeeld client <-> server

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

- voorbeeld met extra routering voor 1 client

```
root@babu:~# cat /etc/openvpn/clients/home_alice
ifconfig-push 10.1.1.115 10.1.1.116
# abnamro servers
push "route 78.31.117.0 255.255.255.128"
# osgn net
push "route 217.149.194.128 255.255.255.224"
```

  - routetabel

```
alice@mtoto:~$ 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.osgn.nl 1194
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
ca /etc/openvpn/certs/ca.crt
cert /etc/openvpn/certs/home_alice.crt
key /etc/openvpn/certs/home_alice.key
ns-cert-type server
tls-auth /etc/openvpn/certs/ta.key 1
comp-lzo
verb 3
```

Referenties

- http://openvpn.net
- network <-> netwerk vpn: http://backreference.org/2009/11/15/openvpn-and-iroute/