/etc/named.conf

options{allow-query {any;};allow-transfer {any;};recursion yes; forwarders {192.168.16.8;};};

logging{channel default\_debug {syslog daemon; severity dynamic};};

zone “dom.be” IN {type master/slave; file “dom.be”; masters {192.168.65.1;};};

“65.168.192.in-addr.arpa”

zone

$TTL 60;@ IN SOA dom.be mail.be (1 60 1H 60 3H);

#serial refresh retry expire mini

SSH (/etc/ssh/sshd\_config)

~/.shosts (chmod og-w) of /etc/hosts.equiv (niet voor root)

HostBasedAuthentication yes

IgnoreRhosts no

client:ssh\_config of ~/.ssh/config

StrictHostKeyChecking y/n/a…

AllowUsers root@\* ;

AllowGroups root

naburige clients:

DenyUsers \*;AllowUsers \*@host

PubKeyAuthentication yes

ssh-keygen -t rsa ;; ssh-copy-id -i ~/.ssh/id\_rsa.pub user@host

beperken tot host: from=“host” …

hosts.allow voorrang op .deny

X11Forwarding yes; ssh -X

.xinitrc en startx

init 3; xhost ; exec xterm

Sendmail

/etc/aliases newaliases ~.forward

tiwi: ahlun@email.be

alias: .forward of virtusertable

makemap hash virtusertable.db < virtusertable

domein tegenhouden: access\_db

makemap hash access.db <access: dom.com OK/REJECT

domainmask:

makemap hash genericstable.db < genericstable : tiwi1 at@m.be

m4 sendmail.mc > sendmail.cf

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

OSTYPE(`linux')

define(`confMAX\_HOP',`25')

define(`confSMTP\_LOGIN\_MSG',`$j mailer ready at $b')

define(`confMIME\_FORMAT\_ERRORS',`False')dnl

FEATURE(`genericstable')dnl

F.(`generic\_entire\_domain')

F..(`promiscuous\_relay')

F.(`accept\_unqualified\_senders')

F.(`use\_cw\_file')dnl

F.(`virtusertable')dnl

F.(`access\_db')dnl

GENERICS\_DOMAIN(`dom.be')

MASQUERADE\_AS(email.be)

MAILER(smtp)dnl

PAM

enkel vanaf bepaalde computer:

auth requisite pam\_access.so assessfile=/etc/access.conf

+:gebruiker:192.168.65.0/24

-:ALL:ALL

tty beveiligen: /etc/securetty

account required pam\_time.so

/etc/security/time.conf

login;\*;\*;Th10000-1200

sshd;\*;us1|us2;MoFr0000-2400

PGP

gpg --gen-key | gpg --export –o export.bin | gpg --export –a –o export.txt | gpg --import keys.txt gpg --listkeys | gpg --delete-key | gpg --edit-key passwd/trust

encrypteren: gpg -c bestand.txt | gpg --cipher-algo AES256 -c f.txt

met pubkey van andere user:

gpg -e (--for-your-eyes-only) f.txt

gpg --symmetric -a file.txt

gpg --decrypt file.gpg

sign and encrypt: gpg -s -e file.txt

cleartext output: gpg --clearsign

gpg verify file.txt.asc

Apache SSL & S/MIME

openssl genrsa -des3 -out cert.key 1024 | openssl rsa -in cert.key -out cert.key.unsecure | openssl req -new -key cert.key -out cert.csr

openssl pkcs7 -print\_certs -in certnew.p7b -out cert.cer

openssl pkcs12 -export -out mailkey.pfx -inkey cert.key -in cert\_base64.cer -certfile CA.cer

#flush: iptables -F ;iptables -X; iptables -t nat -F; iptables -t mangle -F;iptables -t mangle -X;

iptables -P INPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -P OUTPUT ACCEPT

iptables -I INPUT -s 127.0.0.1 -p tcp --dport 20 -j ACCEPT

iptables -A INPUT -p tcp --dport 20 -j DROP

iptables -I INPUT -s 127.0.0.1 -p tcp -m multiport --dports 20,21 -j ACCEPT

iptables -A INPUT -p tcp -m multiport --dports 20,21-j REJECT --reject-with (zie man)

iptables -A OUTPUT -d 192.168.16.8 -p tcp -m multiport --dports 1024:65535 -j REJECT

iptables -A INPUT -p icmp --icmp-type echo-request -j …

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j REJECT

iptables -I INPUT -p tcp -s 193.190.126.66 -m conntrack --ctstate ESTABLISHED -m multiport --sports 80,443 -j ACCEPT

iptables -I OUTPUT -p tcp -d 193.190.126.66 -m multiport --dports 80,443 -j ACCEPT

-j LOG --log-prefix “blabla”

VPN (setkey -f file.vpn)

flush;spdflush;

add 192.168.65.1 192.168.82.1 esp 0x10001 -m transport -E des-cbc 0x3ffe05014819ffff;

add 192.168.65.1 192.168.82.1 ah 123456 -A hmac-sha1 "AH!";

spdadd 192.168.82.0/24 192.168.65.0/24 any -P in ipsec esp/transport//require ah/transport//require;

spdadd 192.168.82.0/24 192.168.65.0/24 any -P in ipsec esp/transport//require;

spdadd 192.168.65.0/24 192.168.82.0/24 any -P in ipsec esp/tunnel/192.168.65.254-192.168.82.254/require;

spdadd 192.168.65.0/24 192.168.82.0/24 any -P in ipsec esp/tunnel/192.168.16.174-192.168.16.171/require ah/tunnel/192.16865.254-192.168.82.254/require

gateway

sysctl –w net.ipv4.ip\_forward=1

route add default gw 10.1.1 eth0