v0.9.0-20030601 by ari_stress (fajarpri@arinet.org)

Artikel ini dibuat karena terdorong keinginan untuk membuat sebuah sistem proxy yang mendukung fasilitas dial on demand dan transparent proxy. Kedua feature ini saya inginkan karena: ...

- dial on demand: otomatis dial ke internet jika dibutuhkan, dan disconnect otomatis jika sudah tidak diperlukan. irit pulsa :)
- transparent proxy: tidak perlu mengkonfigurasi setiap browser di client untuk menggunakan proxy. Bayangkan jika ada 50 client dan kita harus menyetelnya satu per satu untuk menggunakan proxy.

Catatan:
Artikel ini dibuat dengan asumsi bahwa kamu telah setidaknya mengetahui:
- Konsep internet, DNS.
- File system Linux
- Cara mengedit file menggukan text editor seperti vi, mc, emacs, dll.
- Cara memasak Indomie yang baik dan benar.

Spesifkasi system dan software:

Linux Mandrake 9.0 yang telah terinstall: XWindows, Squid, iptables
DNS yang telah berjalan dengan baik, yang mendukung forwarders.
eth0: 192.168.0.77
Sebuah modem external
Indomie rasa Sop Buntut 2(dua) bungkus dan Fanta merah 1 liter (sesuaikan dengan selera kamu)

Langkah-langkah:
---
1. Install pppd:
urpmi pppd

2a. Install wvdial:
urpmi wvdial

2b. Konfigurasi wvdial:
hidupkan modem
touch /etc/wvdial.conf
wvdialconf wvdial.conf

2c. Edit wvdial.conf dan tambahkan info username, password, dan nomor telpon ISP

[Dialer Defaults]
Modem = /dev/ttyS1
Baud = 115200
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2 S11=55 +FCLASS=0
; Phone = <Target Phone Number>
; Username = <Your Login Name>
; Password = <Your Password>
Phone = 21579000
Username = usernamekamu
Password = passwordkamu

[Dialer dod]
Modem = /dev/ttyS1
Baud = 115200
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2 S11=55 +FCLASS=0
Phone = 21579000
Username = usernamekamu
Password = passwordkamu

2d. Test wvdial:
wvdial dod

3a. Konfigurasi pppd:
cd /etc/ppp/peers
cp wvdial dod (atau nama apa saja yang kamu inginkan)

3b. Edit file /etc/ppp/peers/dod tersebut dan ketikkan:

noauth
name wvdial
connect "/usr/bin/wvdial --chat dod"
/dev/ttyS1
115200
modem
crtscts
defaultroute
usehostname
user usernamekamu
noipdefault
idle 180
persist
demand
logfd 6

3b. Buat sebuah file bernama ip-up.local di /etc/ppp untuk menjalankan script firewall
touch /etc/ppp/ip-up.local
chomd 755 /etc/ppp/ip-up.local

4a. Extract gShield-2.8.tgz. dalam hal ini saya taruh di /home/saya
tar -zxvf gShield-2.8.tgz

4b. Rename dan copy direktori gShield-2.8 ke /etc/firewall
mv /home/saya/gShield-2.8 /home/saya/firewall
cp -R firewall /etc

4c. Edit file /etc/firewall/gShield.conf sesuai kebutuhan kamu. disitu telah jelas keterangan-keterangannya. kamu bisa memilih port apa saja yang ingin kamu buka, tutup, enable NAT, dll. Juga edit file /etc/firewal/conf/NAT sesuai keperluan network kamu.

4d. buat link dari file /etc/ppp/ip-up.local ke file /etc/firewall/gShield.rc
ln -s /etc/firewall/gShield.rc /etc/ppp/ip-up.local

5a. Bila eth0 kamu disetel menggunakan default gateway, maka ada kemungkinan kamu tidak akan bisa browsing ke internet walau sudah terkonek. Untuk itu hapus default gateway dengan perintah:
route del default gw
atau bisa juga menggunakan linuxconf agar default gateway terhapus secara permanen.

5b. Test pppd:
pppd call dod

5c. Cek di /var/log/messages:
tail -f /var/log/messages

Jun 1 10:30:43 server pppd[3032]: pppd 2.4.1 started by root, uid 0
Jun 1 10:30:43 server pppd[3032]: Using interface ppp0
Jun 1 10:30:43 server pppd[3032]: local IP address 10.64.64.64
Jun 1 10:30:43 server pppd[3032]: remote IP address 10.112.112.112
Jun 1 10:30:44 server /etc/hotplug/net.agent: assuming ppp0 is already up

5d. Test dial on demand dengan menghidupkan browser dan membuka website misalnya linux.arinet.org, maka di /var/log/messages akan muncul:

Jun 1 10:32:05 server pppd[3032]: Starting link
Jun 1 10:32:06 server WvDial: WvDial: Internet dialer version 1.42
Jun 1 10:32:06 server WvDial: Initializing modem.
Jun 1 10:32:07 server WvDial: Sending: ATZ
Jun 1 10:32:07 server WvDial: OK
Jun 1 10:32:07 server WvDial: Sending: ATQ0 V1 E1 S0=0 &C1 &D2 S11=55 +FCLASS=0
Jun 1 10:32:07 server WvDial: OK

Jun 1 10:32:07 server WvDial: Modem initialized.
Jun 1 10:32:07 server WvDial: Sending: ATDT 21579000
Jun 1 10:32:07 server WvDial: Waiting for carrier.
Jun 1 10:32:07 server WvDial: ATDT 21579000
Jun 1 10:32:31 server WvDial: CONNECT 45333/ARQ/V90/LAPM/V42BIS
Jun 1 10:32:31 server WvDial: Carrier detected. Waiting for prompt.
Jun 1 10:32:32 server WvDial: Welcome to 3Com Total Control HiPer ARC (TM)
Jun 1 10:32:32 server WvDial: Networks That Go The Distance (TM)
Jun 1 10:32:32 server WvDial: login:
Jun 1 10:32:32 server WvDial: Looks like a login prompt.
Jun 1 10:32:32 server WvDial: Sending: usernamekamu
Jun 1 10:32:32 server WvDial: usernamekamu
Jun 1 10:32:32 server WvDial: Password:
Jun 1 10:32:32 server WvDial: Looks like a password prompt.
Jun 1 10:32:32 server WvDial: Sending: (password)
Jun 1 10:32:33 server WvDial: ~[7f]}#@!}!}!}
}8}!}$}%j}"}&[7f][7f][7f][7f]}%}&p3}'O}'}"}(}"};5~
Jun 1 10:32:33 server WvDial: PPP negotiation detected.
Jun 1 10:32:33 server pppd[3032]: Serial connection established.
Jun 1 10:32:33 server pppd[3032]: Connect: ppp0 <--> /dev/ttyS1
Jun 1 10:32:36 server kernel: PPP BSD Compression module registered
Jun 1 10:32:36 server kernel: PPP Deflate Compression module registered
Jun 1 10:32:36 server pppd[3032]: Local IP address changed to 202.158.113.232
Jun 1 10:32:36 server pppd[3032]: Remote IP address changed to 202.158.2.211
Jun 1 10:32:36 server ip-up.local[3066]: initializing v2.8
Jun 1 10:32:36 server ip-up.local[3066]: default TCP response set to REJECT with tcp-reset
Jun 1 10:32:36 server ip-up.local[3066]: default UDP response set to REJECT with
icmp-port-unreachable
Jun 1 10:32:36 server ip-up.local[3066]: default logging rate limit set to 20/m
Jun 1 10:32:36 server ip-up.local[3066]: not logging ICMP
Jun 1 10:32:36 server ip-up.local[3066]: no reserved drop logging
Jun 1 10:32:36 server ip-up.local[3066]: dropping multicasts
Jun 1 10:32:36 server ip-up.local[3066]: Enabling IRC connection tracking for 6666,6667
Jun 1 10:32:37 server ip-up.local[3066]: 192.168.0.0/24 authorized for NAT
Jun 1 10:32:37 server ip-up.local[3066]: Custom forwards DISabled
Jun 1 10:32:37 server ip-up.local[3066]: Allowing all ICMP at rate of 60/m
Jun 1 10:32:37 server ip-up.local[3066]: Allowing all traceroutes
Jun 1 10:32:37 server ip-up.local[3066]: ftpd publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: httpd publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: httpd-ssl publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: SMTP daemon publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: POP3 daemon publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: IMAP daemon publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: IMAP daemon (ssl) publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: BIND publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: SSH daemon publically accessible

Jun 1 10:32:37 server ip-up.local[3066]: identd publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: mysql publically accessible
Jun 1 10:32:37 server ip-up.local[3066]: socks publically accessible

5e. Koneksi akan mati sendiri setelah 180 detik bila idle. Namun bila kamu ingin mematikannya segera, ketik: killall pppd

6. Konfigurasi squid. Edit filenya di /etc/squid/squid.conf. Konfirgurasi squid ini cukup panjang, kamu bisa melihatnya sendiri dengan bantuan keterangan yang ada di dalamnya dan sesuaikan dengan kebutuhan network kamu. Namun intinya untuk mendukung Transparent proxy, kamu harus mengedit line berikut ini menjadi:

httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on

7a. Edit file /etc/firewall/gShield.rc utk mendukung transparent proxy.
cari baris yang berisikan:

Transparent proxy stuff -- since it's part of the NAT munch
we add it here
if ["$ENABLE_TRANSPROXY" = "YES" -o
"$ENABLE_TRANSPROXY" = "yes"]; then
if ["X$PROXY_HOST" != "X"]
then
$IPTABLES -t nat -A PREROUTING -i $INTERNAL -p tcp -s ! $PROXY_HOST --dport 80 -j
DNAT --to $PROXY_HOST:$PROXY_PORT
$IPTABLES -t nat -A PREROUTING -i $INTERNAL -p udp -s ! $PROXY_HOST --dport 80 -j
DNAT --to $PROXY_HOST:$PROXY_PORT

dan tambahkan command berikut ini di baris selanjutnya:
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128

sehingga sekarang menjadi:

if ["$ENABLE_TRANSPROXY" = "YES" -o
"$ENABLE_TRANSPROXY" = "yes"]; then
if ["X$PROXY_HOST" != "X"]
then
$IPTABLES -t nat -A PREROUTING -i $INTERNAL -p tcp -s ! $PROXY_HOST --dport 80 -j
DNAT --to $PROXY_HOST:$PROXY_PORT
$IPTABLES -t nat -A PREROUTING -i $INTERNAL -p udp -s ! $PROXY_HOST --dport 80 -j
DNAT --to $PROXY_HOST:$PROXY_PORT
$IPTABLES -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128

7b. Test konfigurasi:
pppd call dod
buka browser misalnya ke www.yahoo.com. koneksi terjadi. script firewall dijalankan otomatis.
iptables -L -t nat

harus muncul REDIRECT di situ:
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
DNAT tcp -- !nama.server.kamu anywhere tcp dpt:http to:192.168.0.77:3128
DNAT udp -- !nama server.kamu anywhere udp dpt:http to:192.168.0.77:3128
REDIRECT tcp -- anywhere anywhere tcp dpt:http redir ports 3128

8. Test konfigurasi transparent proxy di squid dengan memantau aktivitas di file /etc/var/log/squid/access.log dan /etc/var/log/squid/store.log. Lakukan test dengan browsing-browsing di internet. Tandanya bahwa transparent proxy telah jalan adalah dengan adanya aktivitas di dalam file log tersebut.

tail -f /var/log/squid/acces.log
tail -f /var/log/squid/store.log

Demikianlah artikel yang singkat dan belum sempurna ini. Semoga dapat bermanfaat. Akhir kata, terima kasih banyak kepada xenogears yang telah memberikan penjelasan mengenai penggunaan wvdial untuk dial on demand dengan pppd, dan oom-oom di channel #indolinux DALNET, terutama oom kuit yang telah menerangkan kesalahan saya di dalam setting Transparent proxy di iptables. Terima kasih kepada istri tersayang yang telah merelakan saya untuk begadang sampai pagi dan belum mandi sampai jam 12 siang ini. :)

Terima kasih kepada dunia opensource.
Ilmu Pengetahuan adalah Milik Bersama.

URL terkait:
---
http://www.linux-mandrake.com
http://www.squid-cache.org
http://www.netfilters.org
http://www.sourceforge.net
http://muse.linuxmafia.org/gshield.html

Lisensi: GNU Public License