Samba által hitelesített átjáró HOGYAN

Ricardo Alexandre Mattar v1.2, 2004.05.21

Ez a dokumentum bemutatja, miképpen készíthetsz tűzfalat/átjárót felhasználóhoz kötött szabályok alapján, ahol a felhasználók azonosítását egy Samba Primary Domain Controller végzi

1 Bevezető

Amint láthatod elég egyszerű a nyelvhasználatom, mert az angol nem az anyanyelvem. Ezt a dokumentumot angolul írom a Linux-közösség hasznára. Szóval, bocsássátok meg angol használatom egyszerűségét, és amennyiben beszélsz portugálul akkor azon a nyelven írj nekem levelet

Ez dokumentum azt igyekszik bemutatni neked (és magamnak), hogy miként építsünk olyan Linux átjárót vagy tűzfalat, mely kérésre módosítja a szabályokat, amikor a felhasználók be- illetve kijelentkeznek saját Windows munkaállomásukról.

Kellene írnom egy alkalmazást, de túl lusta vagyok. Remélem, ha az ötlet eljut másokhoz, akkor valakik majd készítenek pár intelligensen beépített csomagot. Addig pedig...

A dokumentumban megpróbálom megmutatni, hogy miképpen építsünk átjárót NAT-hoz vagy álcázott (MASQUERADE) Windows munkaállomásokhoz. Használd a képzelőerőd a módosításokhoz, a különböző hálózatkezelési szintek megvalósításához. Használhatod szolgáltatásokhoz, szerverekhez vagy alhálózatokhoz történő hozzáférés engedélyezésére vagy tiltására.

Képzeld el, hogy építened kell egy átjárót a Windows munkaállomásaid internet-hozzáférésének biztosítására, és előtte neked kell hitelesíteni minden felhasználót. Az első megoldás ami eszedbe jut az a Squid. Ez csakugyan nagyszerű megoldás, amennyiben a felhasználóidnak elég a http és az ftp hozzáférés. Amikor szóba kerül, hogyan férhetnek hozzá egyéb szolgáltatásokhoz is, mint pop, smtp, adatbázis szerver vagy bármi más, azonnal a NAT és MASQUERADE jut eszedbe. De mi történik a felhasználói hitelesítéssel?

Nos, ez az én megoldásom, mely lehetőséget ad a felhasználó hitelesítésére és finombeállítására amikor a külső hálózathoz kapcsolódik.

1.1 Áttekintés

Mint tudjuk a SAMBA képes Domain vezérlőként működni, és így hitelesíteni a felhasználókat a Windowsokról. Mint PDC a SAMBA képes végrehajtani a Windows munkaállomások bejelentkezési szkriptjeit. Fel tudjuk használni ezeket a hálózati bejelentkező-szkripteket annak kényszerítésére, hogy Windows munkaállomásainkat hozzákapcsolódjanak a Linux PDC megadott megosztásához. Ez a kényszerített megosztás fogja tartalmazni azokat az előtte- és utólag futtatandó szkripteket, amelyek a felhasználó ki- vagy bejelentkezésekor hajtódnak végre. Az smbstatus (ez a SAMBA része - a ford.) program kilistázza a használatban lévő megosztásokat, kiírja a felhasználó nevét és a munkaállomás IP címét is. Csak meg kell szűrnünk az smbstatus kimenetét és aktualizálni a tűzfal szabályokat.

1.2 A felelősség teljes kizárása

A dokumentum tartalma minden kötelezettség nélkül felhasználható. Használd az elvet, példát és egyéb tartalmát saját felelősségedre. Mivel ez a legújabb változat, lehetnek benne hibák, tévedések, amelyek károsíthatják a rendszeredet. Használd nagy figyelemmel és bár nagyon szomorú, de a szerző(k) semmilyen felelősséget nem vállalnak érte.

Minden szerzői jogot a megfelelő tulajdonos birtokol, hacsak másként nincs jelezve. Ebben a dokumentumban használt szakkifejezéseknek az érvényességi vonatkozása nem kell tekintettel legyenek semmilyen védjegynek vagy szerviz márkának.

Az egyéni termékekre vagy márkákra történő hivatkozás nem szabálysértés.

1.3 A dokumentum új változatai

A legújabb változat megtalálható a *http://ram.eti.br* <http://ram.eti.br> vagy a *http://www.tldp.org* <http://www.tldp.org> webhelyen.

A kapcsolódó HOGYANok megtalálhatók a Linux Documentation Project webhelyén; *http://tldp.org* <http://tldp.org> . (Illetve a *Magyar LDP* <http://tldp.fsf.hu/> webhelyén - a lektor.)

1.4 Fordítás

Portugál verzió hozzáférhető.

A francia változat Guillaume Lelarge fordításában megtalálható a *http://www.traduc.org* <http://www.traduc.org/docs/HOWTO/lecture/Samba-Authenticated-Gateway-HOWTO.html> honlapon.

A magyar változat megtalálható a *http://tldp.fsf.hu* <http://tldp.fsf.hu/HOWTO/Samba-Authenticated-Gateway-HOWTO-hu/Samba-Authenticated-Gateway-HOWTO-hu.html> honlapon.

Ha segíteni szeretnél egy fordítással, akkor kérlek tedd.

1.5 Visszajelzés

Mindenféle közreműködést illetve bírálatot szívesen fogadok.

Az angol nyelvezet javításával kapcsolatos észrevételeket is szívesen veszem!

Ha bármilyen hibát fedezel fel a dokumentumban található szkriptekben, kérlek értesíts.

Megtalálsz a ricardo@ram.eti.br vagy ricardo.mattar@bol.com.br e-mail címen.

1.6 Szerzői jog és licenc

1.7 Visszajelzések és köszönetnyilvánítások

Köszönet Carlos Alberto Reis Ribeironak, hogy megmutatta nekem a Linuxot.

Köszönet Cesar Bremer Pinheironak, hogy motivált ezen dokumentum megírására.

Köszönet Guillaume Lelargenak az átdolgozásnál nyújtott (folyamatos) segítségért.

Köszönet Erik Esplundnak a további nyelvi korrekciókért.

Köszönet Albert Teixidsnek a kód tökéletesítéséért.

Köszönet Felipe Cordeiro Caetanonak, amiért segített a teszthelyem elkészítésében.

Köszönet a *RASEAC* <http://www.raseac.com.br> kommunikációs biztonsággal foglalkozó cégnek, amiért támogatja munkámat.

1.8 Magyar fordítás

A magyar fordítást *Kormos György* <mailto:kormos@mail.datatrans.hu_NO_SPAM> készítette (2003.12.16). A lektorálást *Daczi László* <mailto:dacas@freemail.hu_NO_SPAM> végezte el (2003.12.23). Utoljára frissítve 2004.05.24.-én. A dokumentum legfrissebb változata megtalálható a *Magyar Linux Dokumentációs Projekt* <http://tldp.fsf.hu/index.html> honlapján.

2 Követelmények

2.1 Ismeretek

Ez a dokumentum a tapasztalt rendszer-adminisztrátorokat célozza meg.

Elég jó tudásod kell legyen (nem utolsó sorban tudd, hogy mik ezek):

- TCP/IP;
- Linux netfilter;
- Egy szkript-nyelv (bash?);
- SAMBA és Windows hálózatok, Domain vezérlők;

Szerencsére bőséges dokumentáció található ezekből az Interneten.

2.2 Szoftver

Legalább ezek legyenek telepítve a szerveren:

- Samba;
- Iptables;
- Egy szkript-nyelv;

3 Linuxos gép beállítása

Ez a HOGYAN feltételezi, hogy van egy RENDSZERMAGOD a 2.4-es szériából ami használja az IPTable szolgáltatást. Azonkívül nincsenek ismert fejlemények miért ne működjön ez egy 2.2 rendszermagon azokkal a scriptekkel, amik az IPChains-hez lettek használva.

Természetesen telepítened kell az iptables userland eszközt, egy apache http szervert, ha CGI eszközt szeretnél futtatni a jelszócseréhez és SAMBA-hoz. Szükséged lesz egy olyan rendszermagra, amelyhez az iptables modul le lett fordítva.

Kívánság szerint használhatsz DHCP-t. Ez esetben könnyű a beállítása. Ne felejtsd el a dhcp szerveren beállítani, hogy szolgáltassa a névszerver IP címét és az átjáróét is. A windowsos gépek nagyon jól használják ezeket az információkat.

3.1 Alapvető rendszerbeállítás

Általánosan elmondható, hogy a legtöbb alapbeállítás a különböző Linux-terjesztésekben megegyezik, és illeszkednek ehhez az átjáró példához. Csak ellenőrizd le, ha van Sambád és IPTABLES-ed.

3.2 Kiegészítő tartalomjegyzék hierarchia

A kiegészítő tartalomjegyzék-hierarchia szükséges lesz az ebben a HOGYANban található példa megvalósításához.

Ezek használatosak a felhasználók és az IP címek nyomon követésére:

`/var/run/smbgate/`

A felhasználófüggő szkriptek könyvtára:

`/etc/smbgate/users/`

A csoportfüggő szkriptek könyvtára:

`/etc/smbgate/groups/`

Megosztott könyvtár a bejelentkezéshez:

`/home/samba/netlogon/`

A nyomkövetés megosztása:

`/home/samba/samba/`

Ez a könyvtárrendszer szükséges, hogy a példában szereplő szkriptek és démonok működjenek.

3.3 Tűzfal beállítás

Nagyon valószínűtlen, hogy az általad használt Linux-terjesztésbe ne lenne belefordítva az iptables, vagy éppen nem lennének telepítve a felhasználói eszközök. Mindenesetre, ha ezek nincsenek, akkor a programok és dokumentációk beszerzéséhez utalásokat találsz a *http://www.netfilter.org* <http://www.netfilter.org> vagy *http://www.iptables.org* <http://www.iptables.org> webhelyen.

Szükséged lesz az alapvető tűzfal beállításokra az átjáród működéséhez. Nézd meg az iptables kézikönyvében: *IPTABLES TUTORIAL* <http://www.netfilter.org/documentation/tutorials/blueflux/iptables-tutorial.html> . Nagyon érdekes olvasmány. Egyébként, ha nincs időd az olvasásra, a következő kód elégé általános ahhoz, hogy megfeleljen a szükségleteidhez.

```
#!/bin/sh
IPTABLES=/usr/sbin/iptables
/sbin/depmod -a
/sbin/insmod ip_tables
/sbin/insmod ip_conntrack
/sbin/insmod ip_conntrack_ftp
```

```
/sbin/insmod ip_conntrack_irc
/sbin/insmod iptable_nat
/sbin/insmod ip_nat_ftp
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/ip_dynaddr
$IPTABLES -P INPUT ACCEPT
$IPTABLES -F INPUT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -F OUTPUT
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -F FORWARD
$IPTABLES -t nat -F
```

Mint láthatod, ez a kód valójában nem csinál semmit. Eredményeképpen mégis betöltődnek a NAT és tűzfalhasználat moduljai, valamint bekapcsolja a csomag útvonal kijelölést. Elhelyezheted (el kéne helyzened) azokat a szabályokat, melyek meghatározzák az átjáród alapvető viselkedését. A "nagy varázslat" (big magic) a SAMBA démon által lefuttatott szkriptekkel lesz befejezett.

Figyelj! Emlékeztetlek, hogy ez a kód a legkevésbé sem biztonságos! Ne használd ezeket a példákat működő rendszerekben. Ezek a példák csak oktatási céllal készültek. Neked kell a rendszerednek legjobban megfelelő tűzfalszabályokat beállítanod

Figyelmeztetettelek!

3.4 SAMBA beállítás

Ellenőrizd, hogy a SAMBA telepítve legyen. Ha a te Linux-terjesztésed nem tartalmazza a SAMBA csomagot, akkor nézz körül a *http://www.samba.org* <http://www.samba.org> webhelyen. Innen beszerezheted a csomagot, valamint találsz útmutatót a telepítésről is. Nézz körül ezeken a weblapokon és tanulj belőlük. A webhelyen sok dokumentáció található. Valószínűleg a te Linux-terjesztésed is bőséges SAMBA dokumentációt tartalmaz.

A SAMBA csomagot elsődleges domain vezérlőnek (Primary Domain Controller) kell beállítanod. Itt találhatsz egy beállítási példát, de szükséges a *Samba HOWTO Collection* <http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection.html> dokumentációt átolvasása, valamint tanulj meg mindent a PDC-ről amit csak lehet.

3.4.1 SAMBA alapbeállítás.

Mivel nem szeretném újraírni a SAMBA dokumentációt, ezért íme egy példa smb.conf fájl:

```
# Általános paraméterek
[global]
workgroup = DOMAIN
netbios name = LINUX
server string = Linux PDC
encrypt passwords = Yes
map to guest = Bad Password
passwd program = /usr/bin/passwd
unix password sync = Yes
max log size = 50
time server = Yes
```

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
add user script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -M %u
logon script = netlogon.bat
domain logons = Yes
os level = 64
lm announce = True
preferred master = True
domain master = True
dns proxy = No
printing = lprng
[homes]
comment = Home Directories
path = /home/%u
read only = No
[printers]
comment = All Printers
path = /var/spool/samba
printable = Yes
browseable = No
available = No
[netlogon]
comment = NetLogon ShARE
path = /home/samba/netlogon
guest account =
[samba]
comment = login tracking share
path = /home/samba/samba
browseable = No
root preexec = /usr/local/bin/netlogon.sh %u %I
root postexec = /usr/local/bin/netlogoff.sh %u
```

Ezeket kell beállítanod, vagy el kell olvasnod a SAMBA dokumentációt, ha valóban felügyelni szeretnéd a szervered és a hálózatod.

3.4.2 A hálózati bejelentkezés (netlogon) és a követés megosztásai (tracking shares)

A netlogon megosztásból töltik le a Windows munkaállomások a bejelentkeztető parancsfájlokat. Azért van szükségünk erre a megosztásra, hogy elhelyezzük itt a bejelentkeztető szkriptet. Ez jelzi a munkaállomásoknak, hogyan csatlakoztassanak egy megosztást, ahol a felhasználók IP címei lesznek követhetők.

Amint láthatod, szükséged lesz a smb.conf fájlban a következő bejegyzésre is.

```
logon script = netlogon.bat
```

Ez a sor jelzi a Windows kliensednek, hogy töltse le és futtassa a netlogon.bat szkriptet. Ennek a szkriptnek a netlogon megosztáson kell lennie. Szóval szintén szükséged lesz egy netlogon.bat szkriptre a Windows munkállomásokhoz. Használhatod a következő példát, elhelyezve a netlogon megosztáson, ami ebben az esetben a: /home/samba/netlogon/NETLOGON.BAT.

```
REM NETLOGON.BAT
net use z: \\linux\samba /yes
```

Ez a szkript fogja jelezni a Windows munkaállomásoknak, hogy csatlakoztassák a megadott megosztásokat. Az smbstatus program kimenetei alapján pedig képesek leszünk nyomon követni a felhasználót és a munkaállomást.

Egészen egyszerű! Azonban nem elég...

Amint láthatod, szükséged van még egy megosztásra (tracking share), amit - ebben a példában - samba-nak neveztem. Láthatod a követés megosztás (tracking share) beállításait az smb.conf fájlban:

```
[samba]
comment = login tracking share
path = /home/samba/samba
browseable = No
root preexec = /usr/local/bin/netlogon.sh %u %I
root postexec = /usr/local/bin/netlogoff.sh %u
```

Amint azt bizonyára már kitaláltad vagy elolvastad a SAMBA dokumentációban, a root preexec és a root postexec sorok jelzik a SAMBA-nak, hogy futtasson egy javasolt szkriptet, amikor a felhasználó fel- vagy lecsatol egy megosztást. Figyelj arra, hogy a %u a sorok végén van. Ezek a szkriptek a "szörnyek" (beasts), melyek meghívnak egy szkriptet, programot, hogy módosítsák az átjárónk csomagszűrő szabályait.

Figyelj, hogy a netlogon.sh szkriptnek ellenőriznie kell, hogy a hivatkozott munkaállomás már csatlakoztatva van-e a nyomkövetés megosztásához.

Vess egy pillantást a netlogon.sh és a netlogoff.sh szkriptekre:

```
#!/bin/sh
#
# netlogon.sh
#
# usage:
# netlogon.sh <username>
#
if [ -f /var/run/smbgate/$1 ] ; then
    exit 0
fi
echo $2 > /var/run/smbgate/$1
IPTABLES='/usr/sbin/iptables'
EXTIF='eth0'
COMMAND='-A'
ADDRESS=`cat /var/run/smbgate/$1`
GROUP=`groups $1 | gawk '// { print $3 }'`
if [ -f /etc/smbgate/users/$1 ] ; then
    /etc/smbgate/users/$1 $COMMAND $ADDRESS $EXTIF
else
    if [ -f /etc/smbgate/groups/$GROUP ] ; then
        /etc/smbgate/groups/$GROUP $COMMAND $ADDRESS $EXTIF
    else
        /etc/smbgate/users/default.sh $COMMAND $ADDRESS $EXTIF
    fi
fi
```

A netlogon.sh szkript a felhasználó belépésekor hajtódik végre. A végrehajtandó szkript a felhasználói név és a felhasználó csoportja alapján kerül kiválasztásra. A felhasználó IP címe bekerül a /var/run/smbgate

könyvtárba nyomkövetési célból. A fájl tartalmazza a felhasználó nevét, mely később a kijelentkezéskor szükséges. Az IP cím a felhasználói névvel együtt paraméterként kerül átadásra, amely végül frissíti a tűzfalat.

Figyelj arra, hogy a netlogon.sh futtatni próbálja a felhasználó szkriptjét. Ha nem találja, akkor próbálkozik a csoport szkripttel. Végül, ha nem találja a csoport szkriptet sem, akkor a default.sh szkriptet futtatja. Ezt a logikát és viselkedést módosíthatod ha szeretnéd vagy szükséges, de ne felejtsd el módosítani a többit is ennek megfelelően.

Valószínű, ha a felhasználó több csoportba tartozik, akkor ezek a szkriptek hibásan fognak működni. Nem volt időm jobb kódot írni.

```
#!/bin/sh
#
# netlogoff.sh
#
# usage:
# netlogoff.sh <username>
#
IPTABLES='/usr/sbin/iptables'
EXTIF='ppp0'
COMMAND='-D'
ADDRESS=`cat /var/run/smbgate/$1`
GROUP=`groups $1 | gawk '// { print $3 }'`
if [ -f /etc/smbgate/users/$1 ] ; then
    /etc/smbgate/users/$1 $COMMAND $ADDRESS $EXTIF
else
    if [ -f /etc/smbgate/groups/$GROUP ] ; then
        /etc/smbgate/groups/$GROUP $COMMAND $ADDRESS $EXTIF
    else
        /etc/smbgate/users/default.sh $COMMAND $ADDRESS $EXTIF
    fi
fi
rm -f /var/run/smbgate/$1
```

A netlogoff.sh szkript a felhasználó kilépésekor fut le. A /var/run/smbgate/user fájlból beolvasott cím, mint argumentum átadódik az /etc/smbgate/users/user szkriptnek, amely frissíti a tűzfalat és visszaállítja a felhasználó bejelentkezése előtti állapotot.

Néhány Windows verzió, mint a Windows 2000 többször felcsatolja a nyomkövető megosztást. Ez problémát okozhat azáltal, hogy többször hajtja végre a netlogon.sh és a netlogoff.sh szkripeket. Ez teljes zűrzavarhoz vezet. Nos, esetleg előnyösebb egy kilépés-ellenőrzés (logout checking) futtatása cronból, mint a netlogoff.sh végrehajtatása a SAMBA-val. Íme egy példa:

```
#!/bin/sh
# checklogout.sh
#
# usage:
# intended to run at cron (maybe each 10 minutes)

TRACKDIR="/var/run/smbgate"
DIRLENGTH=${#TRACKDIR}
```

```
TRACKSHARE="samba"
EXTIF='eth0'
COMMAND='-D'
if [ -d $TRACKDIR ]; then
  for n in $TRACKDIR/*; do
    [ -d $n ] && continue;
    if [ -f $n ] ; then
      IPADDRESS=`cat $n`
      USERNAME=${n:$DIRLENGTH+1}
      NMS=`smbstatus -u $USERNAME | grep $TRACKSHARE | grep $IPADDRESS | grep -v grep | wc -l`
      if [ $NMS == 0 ] ; then
        rm -f $n
        GROUP=`groups $USERNAME | gawk '// { print $3 }'`
        if [ -f /etc/smbgate/users/$USERNAME ] ; then
          /etc/smbgate/users/$USERNAME $COMMAND $IPADDRESS $EXTIF
        else
          if [ -f /etc/smbgate/groups/$GROUP ] ; then
            /etc/smbgate/groups/$GROUP $COMMAND $IPADDRESS $EXTIF
          else
            /etc/smbgate/users/default.sh $COMMAND $IPADDRESS $EXTIF
          fi
        fi
      fi
    else
      exit 0
    fi
  done
fi
```

Ebben az esetben el kell távolítanod a postexec bejegyzést az smb.conf nyomkövetö megosztásából:

```
root postexec = /usr/local/bin/netlogoff.sh %u
```

Íme egy általános /etc/smbgate/users/user szkript. Jelenleg ez az egyetlen, ami módosítja a tűzfal szabályait.

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
IPTABLES='/usr/sbin/iptables'
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF -j MASQUERADE
```

Az /etc/smbgate/users/ könyvtárba szintén kell egy default.sh szkript, hogy megadjuk az átjáró viselkedésének alapszabályait.

```
#!/bin/sh
#
# default.sh
COMMAND=$1
```

```
ADDRESS=$2
EXTIF=$3
IPTABLES='/usr/sbin/iptables'
#$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF -j MASQUERADE
exit 0
```

4 SSH beállítás

Talán azt szeretnéd, hogy a PDC (Primary Domain Controller; elsődleges tartományvezérlő) egy gépen fusson, egy másikon pedig egy átjáró (gateway), bármilyen okból. Ha így van, akkor az átjárót úgy kell beállítanod, hogy jelszó nélkül elfogadja a PDC-ről érkezett, rsa kulccsal hitelesített bejelentkezéseket (login).

Nézd át a *www.openssh.org* <http://www.openssh.org/manual.html>

webhelyen lévő dokumentációt az ssh szerver és kliens helyes beállításához.

4.1 Fontos

Az ssh dokumentációt el kell olvasnod. Bizonyosodj meg arról, hogy teljesen tisztában vagy az rsa, illetve más titkosított azonosítással kapcsolatos teendőkkel

Ha a biztonság nem fontos, akkor csak használd a példámat és lépj tovább.

4.2 Kulcspár generálás

Kulcspár létrehozásához a PDC-n a következő parancsot használd:

```
pdc:~# ssh-keygen -t rsa
```

Válaszolj a kérdésekre, majd a létrejött nyilvános kulcsot másold az átjáróra. A nyilvános kulcs általában a "~.ssh/id_rsa.pub" könyvtárba kerül.

```
pdc:~# cd .ssh
pdc:~# scp id_rsa.pub root@gateway:/root/.ssh/authorized_keys2
```

4.3 SSH-t engedélyező bejelentkező szkript

Következzen egy módosított /etc/smbgate/users/user szkript, amely az ssh titkosított bejelentkezést használja.

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
IPTABLES='/sbin/iptables'
ssh root@gateway $IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF -j MASQUERADE
```

Figyeld meg, hogy a bináris iptables az ssh-n keresztül kerül meghívásra a "gateway"-en. Megismétlem, olvasd el az ssh szerver dokumentációját.

5 A windowsos munkaállomások beállítása

5.1 Bevezető

Be fogjuk állítani a hálózatot, a felhasználók kezelését és a házirendet (policy) a windowsos munkaállomásokon.

Nem fogok ezeken a lépéseken teljesen végigmenni, megnevezni minden egyes párbeszédablakot. Feltételezem, hogy amennyiben el tudod olvasni és megérted ezt a dokumentumot, akkor megtalálod az utat az egyes lépések között.

5.2 Hálózati protokollok

Először is, hacsak valóban nincs szükséged rá, akkor távolíts el minden protokollt, kivéve a TCP/IP-t. A windowsos gépek még a saját protokolljuk hiányában is szeretnek sokat üzengetni, és ez nem mindenkinek tetszik. Egyébként is a TCP/IP-n kívül kinek kell bármi más?

5.3 DHCP beállítás

Ha szeretnél DHCP szervert a saját Linux rendszereden, ne feledd, hogy a Windows munkaállomások megkaphatják a névszerverek és az átjáró címét is a saját IP címükön felül. Szóval nem kell minden munkaállomáson beállítanod ezeket a jellemzőket.

5.4 Belépés a Linux szerver domain-be

A Windows munkaállomásokat Domain-be történő bejelentkezésre kell beállítani. A Linux szervernek pedig át kell adni a domain nevet. Ez alapvetően szükséges az átjáró működéséhez.

Tudnod kell! Ahhoz, hogy valamennyi windowsos verziós gép be tudjon jelentkezni, a SAMBA domain vezérlőhöz létre kell hoznod a gépek fiókjait a saját Linux PDC-den. (Amelyik nem tud feljelentkezni domain-be, az természetszerűleg nem: Win95, WinXP Home. - a ford.) Nézd meg a SAMBA leírást, hogy miképpen kell beállítani a PDC-t az általad használt Windowsokhoz.

5.4.1 Windows 95/98

Ezek a verziók úgy tűnik, hogy speciális beállítást igényelnek a Linux PDC domain-be történő belépéshez.

5.4.2 Windows NT és 2000

Ezen verziók esetében szükséges, hogy legyen a gépnek fiókja a Linux rendszerben. Újfent, nézd meg a SAMBA leírását.

5.4.3 Windows XP

Ezen a verzió esetén szükséges, hogy legyen a gépnek fiókja a Linux rendszeren, és egy kis módosításra is szükség van a registry-ben.

Keresd meg a "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOr
kulcsot. Az alapérték: 1, változtasd meg 0-ra. Többet nem fog panaszkodni a domain-be történő belépéskor.

Ha sok munkaállomásod van, melyeket be kell állítanod, akkor készíts egy fájlt. Legyen a neve anything.reg, amely a következőket tartalmazza. Használd ezt, a "hibás" regisztrációs bejegyzések módosításához.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
```

Ezen verzió esetén szintén szükséges egy kis módosítás a NETLOGON.BAT szkripten. Némely esetben makacsul és folyamatosan felcsatolásokat végez.

```
REM NETLOGON.BAT
net use z: \\linux\samba /yes /persistent:no
```

5.5 Házirend szerkesztő

Ez egy kis segédprogram, amit a Windows CD-n megtalálsz. A fájl neve poledit.exe. Ez egy olyan eszköz - mint a neve is sugallja -, mellyel felhasználói és rendszer házirend-fájlokat lehet készíteni

Sajnálatos módon ez az eszköz nem képes sima szöveges fájlt készíteni, így nem tudok itt példát bemutatni.

Használd a házirend szerkesztőt munkaállomások és felhasználók házirendjeinek elkészítéséhez. Le kell tiltanod a helyi és domain jelszó gyorsítótárat, a biztonság növelése érdekében. Tárold el config.pol néven a házirend-fájlt, és helyezd el a netlogon megosztáson. Ekkor a Windows munkaállomásaid letöltik és használni fogják a config.pol fájlt a saját házirendjük beállításához. Természetesen ennek a szálnak a windowsos gépeken kell futnia.

Ha nem használsz config.pol fájlt, a windowsos munkaállomások bosszantani fognak a Windows jelszó bekérésével, és megőrjítenek, amikor megpróbálod összhangba hozni és kezelni a domain-odat és Windows jelszavakat. Úgy néz ki, hogy az operációs rendszer nem tudja, hogy belépett egy domain-be. Ezt tudatnod kell vele, majd bele kell vágnod az arcába, így hinni fog neked.

6 Felhasználók kezelése

6.1 Felhasználó hozzáadása

Linux-felhasználó hozzáadás és a samba jelszó beállítása az smbpasswd segítségével működik. Ha bármilyen kétséged van, akkor olvasd el a SAMBA dokumentációt. Nem nehéz megcsinálni.

6.2 Jelszavak kezelése

Úgy gondolom ez egy fontos téma, mert én sem tanultam még meg, hogy miképpen kezeljük a felhasználót és a jelszavát a Windows munkaállomásokról a web-es felület használata nélkül. Nem találtam és nem tudom, hogy miképpen hozzak létre egy beépített eszközt ezen probléma megoldására. Nos, ezért én egy CGI programot használok ennek megvalósítására.

Próbáld ki a *http://changepassword.sourceforge.net* <http://changepassword.sourceforge.net> webhelyről letölthető csomagot. Ez jó megoldásnak tűnik.

6.3 Felhasználói hozzáférés engedélyezése, tiltása

Amint azt az előző fejezetekben láthattad a SAMBA démon meg fogja hívni a netlogon.sh szkriptet minden alkalommal, amikor a nyomkövető megosztás felcsatlakozik. Ez a netlogon.sh szkript fog meghívni egy másik szkriptet a felhasználó nevével és a munkaállomás IP címével, mint átadott paraméterrel. Ez a felhasználói szkript fogja beállítani a kívánt szabályokat.

Például, ha teljes hozzáférést akarsz a felhasználónak az internethez, a következőket állítsd be:

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
IPTABLES='/usr/sbin/iptables'
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF -j MASQUERADE
```

Ha nem akarsz semmit sem megváltoztatni bizonyos felhasználók esetében, akkor készíts nekik egy üres szkriptet:

```
#/bin/sh
#
exit 0
```

Esetleg ne is készíts semmilyen szkriptet a kevesebb joggal rendelkező felhasználóknak. Így ők a default.sh szkriptet kapják, mely akár üres is lehet mint az előző példa, vagy korlátozott jogkörű, mint lejjebb látható:

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
EXTIFADDRESS=$4
IPTABLES='/usr/sbin/iptables'
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF --dport 25 -j SNAT --to-source $EXTIFADD
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF --dport 110 -j SNAT --to-source $EXTIFAD
```

Figyelj arra, hogy ezen szkript miatt módosítanod kell az összes előző szkriptet, hogy tartalmazza az extra paramétereket, vagy egyszerűen csak módosítsd ezt a szkriptet. Ne feledd azt sem, hogy nem mész ezzel a HOGYANnal semmire, ha nem érted az iptables működését.

7 Csoport kezelése

7.1 Csoport létrehozás

Egyszerűen hozd létre a csoportot a Linux PDC-n, majd rendeld a felhasználókat az egyes csoportokhoz. Ez van.

Ne feledd azt a példa szkriptet ebben a HOGYANban, ami valószínűleg hibát eredményez, ha egy felhasználó több csoportnak is a tagja. Ha szeretnéd (egy felhasználó több csoportba tartozhasson - a ford.), akkor ne felejtsd el a szkriptet megváltoztatni.

7.2 Csoport házirend

Csoportfüggő szkripteket kell létrehoznod és elhelyezni őket az "/etc/smbgate/groups/" könyvtárban. Figyelj arra, hogy a fájl nevének a csoport nevét add, ha ennek a HOGYANnak a példáját akarod követni.

Ezen HOGYAN felfogása szerint először ellenőrizd a felhasználói szkriptet, majd a csoport és végül az alapértelmezett szkriptet. Ha ezen alapviselkedésen módosítani szeretnél, akkor ne felejtsd el ehhez igazítani a netlogon.sh, netlogoff.sh (vagy checklogout.sh) szkripteket. Az egész logikája ezekben a szkriptekben van.

8 Irodalomjegyzék

Oskar Andreasson: *IPTABLES TUTORIAL* <http://www.netfilter.org/documentation/tutorials/blueflux/iptables-tutorial.html>

The SAMBA Team: *Samba HOWTO Collection* <http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection.html>

9 GNU Free Documentation License

GNU Free Documentation License Version 1.2, November 2002

0. Bevezetés

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies

you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission. B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement. C. State on the Title page the name of the publisher of the Modified Version, as the publisher. D. Preserve all the copyright notices of the Document. E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices. F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below. G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice. H. Include an unaltered copy of this License. I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence. J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was

based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission. K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein. L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles. M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version. N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section. O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warrany Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.