Squid dengan authentikasi Active Directory Windows 2000

Asfihani (asfik@layangan.com) 12 Februari 2005

Dokumentasi ini akan menjelaskan bagaimana mengkonfigurasi squid dengan memanfaatkan helper dari samba (winbindd) untuk ber-authentikasi pada suatu Active Directory Microsoft Windows 2000 server (W2K AD). Versi squid dan samba yang saya gunakan adalah: samba-2.2.11 dan squid-2.5.STABLE6. Testing saya lakukan pada distro Fedora Core 1, dan seharusnya hal yang sama bisa dilakukan pada distro lain kesayangan anda, tentunya dengan sedikit keberuntungan *kidding* hehe :-). Seperti biasa, feedback always welcome, dan jangan lupa yah kalau sukses, buy me a CD from my wishlist *here* :-O. Enjoy.

Contents

Untuk ibu saya tercinta, guru pertama saya.

1 Pendahuluan

PERINGATAN: Jika anda ingin membuat sebuah proxy (squid) yang *transparent* dengan authentikasi, maka dokumentasi ini **TIDAK** ada gunanya. Hal ini telah dijelaskan pada FAQ squid.

Sebelum memulai, silakan diperiksa apakah ada squid atau samba yang sudah disertakan dalam distro. Untuk Redhat dan turunannya (termasuk Fedora), silakan diperiksa dengan perintah berikut ini (ouput dibawah ini hanyalah contoh) :

```
[root@darkside asfik]# rpm -qa | egrep '^(samba|squid)'
squid-2.5.STABLE3-93
samba-client-2.2.8a-107
samba-2.2.8a-107
```

Jika ada silakan dihapus terlebih dahulu, misalnya dengan perintah :

```
[root@darkside asfik]# rpm -e --nodeps squid-2.5.STABLE3-93 \
samba-client-2.2.8a-107 \
samba-2.2.8a-107
```

Kemudian buatlah username di W2K AD anda jika belum. Disini saya tidak akan membahasa cara membuat user (dan group) di W2K AD, karena apa? Ya karena tutorial ini tidak membahas hal itu :-).

2 Instalasi dan konfigurasi Samba

Ada baiknya membuat sebuah direktori untuk menyimpan file-file source terlebih dahulu, nama direktorinya sembarang, asal mudah untuk diingat :

```
[root@darkside asfik]# mkdir src
```

Pindah ke direktori src, kemudian download samba versi 2.x (kebetulan pada waktu testing samba 2.x yang paling akhir adalah versi 2.2.11) :

```
[root@darkside asfik]# cd src
[root@darkside src]# wget http://us1.samba.org/samba/ftp/old-versions/samba-2.2.11.tar.gz
```

Ekstrak source samba, pindah ke source samba, lakukan konfigurasi dan kompilasi :

```
[root@darkside src]# tar -zxvf samba-2.2.11.tar.gz
[root@darkside src]# cd samba-2.2.11/source/
[root@darkside source]# ./configure --prefix=/usr/local/samba-2.2.11 \
--with-winbind \
--with-winbind-auth-challenge
[root@darkside source]# make
[root@darkside source]# make install
```

Buat file konfigurasi untuk samba:

```
[root@darkside source]# vi /usr/local/samba-2.2.11/lib/smb.conf
```

Isinya adalah sebagai berikut, ganti **DARKSTAR** sesuai dengan domain pada W2K AD anda :

```
workgroup = DARKSTAR
password server = *
security = domain
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind use default domain = yes
encrypt passwords = yes
```

Joinkan samba dengan domain W2K AD anda. Perintah ini tentu saja membutuhkan hak user*Administrator* atau yang setara dengannya. Sesuaikan user Administrator, Domain (DARKSTAR) dan IP server W2K (10.126.10.10) dengan konfigurasi yang sesuai :

```
[root@darkside source]# /usr/local/samba-2.2.11/bin/smbpasswd \
-j DARKSTAR -r 10.126.10.10 -U Administrator
Password:
Joined domain DARKSTAR.
```

Buat file *lmhosts* :

```
[root@darkside source]# vi /usr/local/samba-2.2.11/lib/lmhosts
```

Isinya :

```
10.126.10.10 DARKSTAR
```

Jalankan daemon *nmbd* :

```
[root@darkside source]# /usr/local/samba-2.2.11/sbin/nmbd -D
```

Jalankan daemon *winbindd*, ada baiknya anda memulai dengan mode *debug* dan *non-interactive* untuk memastikan bahwa konfigurasi bekerja dengan baik dan sesuai yang diharapkan :

```
[root@darkside source]# /usr/local/samba-2.2.11/sbin/winbindd -i -d 5
```

Jika tidak terdapat error, jalankan daemon *winbindd* :

```
[root@darkside source]# /usr/local/samba-2.2.11/sbin/winbindd
```

Periksa apakah daemon-daemon tersebut sudah berjalan :

```
[root@darkside source]# ps ax | egrep '(nmbd|winbindd)'
5436 ?        S      0:00 /usr/local/samba-2.2.11/sbin/nmbd -D
5440 ?        S      0:00 /usr/local/samba-2.2.11/sbin/winbindd
```

Masukkan perintah ini ke file *rc.local*, sehingga setiap server direboot maka daemon-daemon tersebut akan berjalan secara otomatis :

```
[root@darkside source]# echo "/usr/local/samba-2.2.11/sbin/nmbd -D" >> /etc/rc.local
[root@darkside source]# echo "/usr/local/samba-2.2.11/sbin/winbindd" >> /etc/rc.local
```

Periksa apakah *trust account* ketika server samba ditambahkan ke domain bekerja dengan baik. Hasil perintah dibawah ini haruslah **Secret is good**, jika tidak maka jangan lakukan langkah berikutnya*(You have been warned :-))* :

```
[root@darkside source]# /usr/local/samba-2.2.11/bin/wbinfo -t
Secret is good
```

Jika langkah diatas sukses, mari kita coba hal yang menyenangkan. Test authentikasi dengan user yang telah ada (sudah dibuat terlebih dahulu tentunya). Misalnya adalah dengan contoh domain: DARKSTAR, username: Asfihani, password: rahasia. Perhatikan penulisan dengan format **DOMAIN\\Username%password** :

```
[root@darkside source]# /usr/local/samba-2.2.11/bin/wbinfo -a DARKSTAR\\Asfihani%rahasia
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

Jika output perintah anda tidak sesuai dengan output perintah diatas, jangan lakukan langkah berikutnya. Jika sukses, mari kita lanjutkan dengan mengkonfigurasi squid.

3 Instalasi dan konfigurasi Squid

Sebelum mengkonfigurasi squid, buatlah sebuah user untuk menghandle daemon squid, misalnya adalah user squid:

```
[root@darkside asfik]# adduser -d /no/home -s /no/shell squid
```

Ada baiknya user ini dikunci saja :

```
[root@darkside asfik]# passwd -l squid
```

Pindah ke direktori untuk menyimpan source yang telah dibuat sebelumnya, kemudian download squid versi 2.5.x yang paling baru (kebetulan pada waktu itu squid versi stable untuk 2.5 adalah squid-2.5.STABLE6):

```
[root@darkside asfik]# cd src
[root@darkside src]# wget http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE6.tar.gz
```

Ekstrak source squid, pindah ke source squid, konfigurasi kemudian lakukan kompilasi. Anda dapat menambahkan opsi lain sesuai dengan kebutuhan anda pada waktu melakukan perintah *./configure* :

```
[root@darkside src]# tar -xzvf squid-2.5.STABLE6.tar.gz
[root@darkside src]# cd squid-2.5.STABLE6
[root@darkside squid-2.5.STABLE6]# ./configure \
--prefix=/usr/local/squid-2.5.STABLE6 \
--enable-auth="ntlm,basic" \
--enable-basic-auth-helpers="winbind" \
--enable-ntlm-auth-helpers="winbind" \
--enable-external-acl-helpers="winbind_group"
[root@darkside squid-2.5.STABLE6]# make
[root@darkside squid-2.5.STABLE6]# make install
```

Buat simbolik link direktori squid-2.5.STABLE6 ke direktori squid pada direktori */usr/local* :

```
[root@darkside squid-2.5.STABLE6]# cd /usr/local
[root@darkside local]# ln -s squid-2.5.STABLE6 squid
```

Selanjutnya ada melakukan percobaan program *helper* dari squid apakah bisa berhubungan dengan daemon *winbindd.* Misalnya adalah dengan contoh domain: DARKSTAR, username: Asfihani, password: rahasia. Perhatikan penulisan dengan format **DOMAIN\Username password** :

```
[root@darkside asfik]# /usr/local/squid/libexec/wb_auth -d
/wb_auth[19383](wb_basic_auth.c:183): basic winbindd auth helper build Aug 19 2004, 23:38:08 starting u
DARKSTAR\Asfihani rahasia
/wb_auth[19383](wb_basic_auth.c:121): Got 'DARKSTAR\Asfihani rahasia' from squid (length: 24).
/wb_auth[19383](wb_basic_auth.c:54): winbindd result: 1
/wb_auth[19383](wb_basic_auth.c:57): sending 'OK' to squid OK
```

Jika konfigurasi anda benar, maka helper akan mengirimkan string **OK** (bukan **ERR**) kepada squid seperti pada output baris terakhir contoh diatas. Jika tidak, maka jangan meneruskan langkah anda berikutnya.

Langkah berikutnya adalah mengkonfigurasi squid untuk authentikasi ke W2K AD. Saya tidak akan membahas konfigurasi-konfigurasi squid secara menyeluruh, hanya bagian-bagian yang berhubungan dengan authentikasi dan ACL (*Access Control List*) saja. Edit file *squid.conf* :

```
[root@darkside asfik]# vi /usr/local/squid/etc/squid.conf
```

Tambahkan atau ubah pada bagian berikut ini. sesuaikan daemon squid dengan user yang telah dibuat sebelumnya :

```
cache_effective_user squid
```

Beritahu squid untuk menggunakan helper yang telah kita konfigurasi:

```
auth_param ntlm program /usr/local/squid/libexec/wb_ntlmauth
auth_param ntlm children 5
auth_param ntlm max_challenge_reuses 0
auth_param ntlm max_challenge_lifetime 2 minutes
auth_param basic program /usr/local/squid/libexec/wb_auth
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

Buatlah ACL untuk user yang telah sukses authentikasi dengan W2K AD di squid :

```
acl AuthorizedUsers proxy_auth REQUIRED
http_access allow all AuthorizedUsers
```

Jika sudah selesai, ganti kepemilikan direktori *var* pada squid sesuai dengan user yang menjalankan daemon squid :

```
[root@darkside asfik]# chown -R squid:squid /usr/local/squid/var/
```

Buatlah direktori swap squid :

```
[root@darkside asfik]# /usr/local/squid/sbin/squid -z
```

Jalankan daemon squid :

```
[root@darkside asfik]# /usr/local/squid/sbin/squid
```

Periksa apakah daemon squid dengan helpernya sudah berjalan dengan baik. Sekarang waktunya mencoba dengan browser kesayangan anda. Masukkan IP atau *hostname* server squid beserta portnya (default adalah 3128) pada konfigurasi proxy browser anda. Jika anda menggunakan *workstation* yang telah login pada sebuah domain di AD dan browser yang anda gunakan adalah Microsoft Internet Explorer, maka *popup window* **TIDAK** akan muncul untuk menanyakan username dan password. Namun anda bisa melihat pada file log squid domain dan user yang authentikasi tersebut dicatat. Jika anda menggunakan browser non Microsoft Internet Explorer, maka akan muncul *popup window* yang menanyakan username dan password. Masukkan **DOMAIN\Username** pada username dan password yang sesuai pada password.

Jika segalanya berjalan lancar, ada baiknya menambahkan pada file *rc.local* perintah untuk menjalankan squid :

```
[root@darkside asfik]# echo "/usr/local/squid/sbin/squid" >> /etc/rc.local
```

Selamat, Anda telah selesai mengkonfigurasi squid untuk authentikasi pada sebuah domain di W2K AD.

4 Penutup

Hal lain yang bisa dimanfaatkan adalah *helper wb_group.* Dengan *helper* ini, bisa dibuat sebuah ACL di squid berdasarkan group pada AD. Misalnya begini, ada tiga buah departemen misalnya: keuangan, teknikal, umum pada sebuah domain di AD. Departemen keuangan hanya bisa mengakses domain-domain tertentu misalnya untuk transaksi finansial suatu perusahaan. Departemen teknikal bisa mengakses semua domain, sedangkan departemen umum hanya bisa mengakses internet pada waktu tertentu. Maka dengan memanfaatkan ACL dengan type *regex* dan *time* di squid dan bantuan *helper* , hal tersebut bisa dilaksanakan. Namun, karena saya sudah ngantuk, hal tersebut mudah-mudahan bisa saya bahas lain waktu.

5 Changelog

- 2005/02/12 : Penulisan dokumen ini dimulai

6 Referensi

- http://www.squid-cache.org/Doc/FAQ/FAQ-23.html#ss23.5
- manual samba (winbindd, wbinfo)