Squid proxy menggunakan Authentikasi LDAP

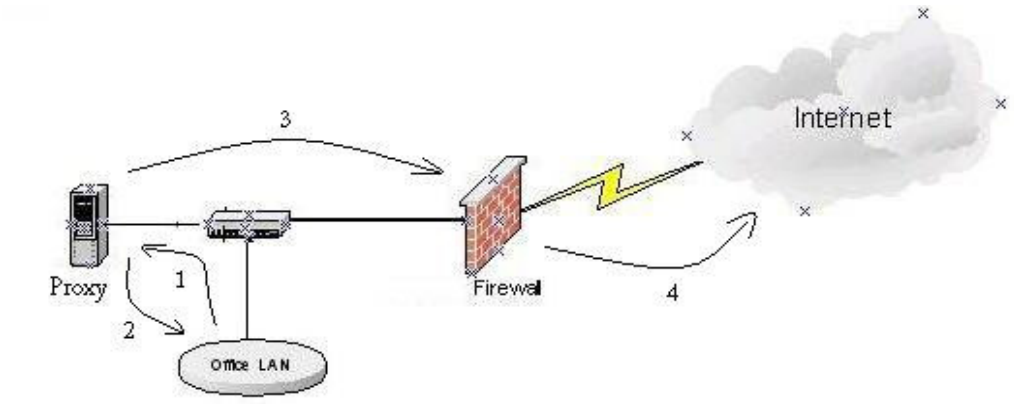
Ratdhian Cipta Sukmana
ratdix@yahoo.com
http:/ratdix.wordpress.com

Pendahuluan

Artikel ini merupakan materi lanjutan dari artikel tentang LDAP yang telah Penulis tulis sebelumnya. Untuk itu silahkan Anda membaca artikel "Pengenalan LDAP" agar lebih memudahkan pemahaman Anda tentang LDAP dan di lanjutkan dengan artikel "Implementasi Samba PDC menggunakan backend LDAP". Dan pada artikel ini penulis hanya akan menjelaskan kegunaan LDAP sebagai Autentikasi User pada Squid Proxy dan silahkan anda kembangkan lagi squid proxy anda nantinya sesuai dengan kebutuhan anda.

Pada awalnya ARPA-funded Harvest Project (http://harvest.cs.colorado.edu) mengembangkan proxy-cache program di awal tahun 1990-an, hingga akhirnya Squid Project didirikan oleh NSF grant (NCR-9796082) yang memfokuskan untuk pengembangan *high-performance cache daemon* atau *cached* untuk me-re-indexing halaman-halaman web. Dan hingga sekarang Squid merupakan salah satu aplikasi web-cache proxy yang paling banyak di gunakan karena ke handalan, kestabilan dan performanya.

Konsep Dasar



Squid menggunakan metode caching yang berorientasi kepada client, yaitu dengan menempatkan object-object web yang diakses ke tempat-tempat penyimpanan yang telah di sediakan. Untuk lebih jelasnya lihat gambar di atas dan penjelasan berikut ini :

Pada saat browser Client mengirimkan header permintaan (Ket Angka 1), sinyal http request dikirimkan ke server. Header tersebut diterima squid dan dibaca. Dari hasil pembacaan, squid akan memparsing URL yang dibutuhkan, lalu URL ini dicocokkan dengan database cache yang ada. Database cache ini berupa kumpulan metadata (semacam header) dari object yang telah di simpan oleh squid. Jika ada, object akan dikirimkan ke klien (Ket Angka 2) dan tercatat dalam logging bahwa client telah mendapatkan object yang diminta. Dalam log kejadian tersebut akan dicatat sebagai TCP_HIT.

Sebaliknya, jika object yang diminta ternyata tidak ada, squid akan mencarinya dari peer atau langsung ke server tujuan (Ket Angka 3 & 4). Setelah mendapatkan objectnya, squid akan menyimpan object tersebut ke dalam cache. Selama dalam proses download object ini dinamakan “object in transit” yang sementara akan menghuni ruang memori. Dalam masa download tadi, object mulai dikirimkan ke client dan setelah selesai, kejadian ini tercatat dalam log sebagai TCP_MISS.

Squid proxy server dalam suatu jaringan memiliki tiga fungsi utama yaitu sebagai Connection Sharing, Filtering dan Caching.

- Connection sharing merupakan fungsi proxy server sebagai gateway ke internet, jadi semua komputer client yang berada di bawahnya akan dapat mengakses internet melalui gateway ini.
- Fungsi proxy server sebagai Filtering merupakan sebuah usaha pengamanan atau pembatasan sehingga proxy server dapat membatasi hak akses client selain itu

dengan adanya hal ini jaringan privat dapat terlindungi dari serangan yang disebabkan internet. Dengan filtering ini maka kita juga dapat memasang aturan-aturan yang berfungsi diantaranya :

- Dengan mengkonfigurasikan ACL maka dapat melakukan pembatasan untuk client atau ip yang di tentukan
- Dapat melakukan pembatasan untuk file-file tertentu Dapat melakukan pembatasan akses kepada situs-situs tertentu.
- Dapat melakukan pembatasan waktu-waktu yang diperbolehkan untuk mengakses internet.
- Dengan mengkonfigurasikan Delay Pool maka anda dapat mengatur kecepatan bandwidth yang di gunakan.
- Bila di gabungkan dengan Anti Virus maka dapat juga menangkal infeksi virus dari halaman web yang di akses.
- Dapat menambahkan fasilitas Authentikasi

- Fungsi Caching dapat mempercepat pengaksesan halaman-halaman web karena client tidak harus melakukan kontak dengan server (di internet) untuk meminta layanan akan tetapi client dapat mendapatkan *(data)* layanan yang sudah tersimpan pada proxy server, dengan hal ini maka akses akan semakin cepat. Sehingga dengan fungsi ini maka Squid juga dapat menghemat penggunaan bandwith internet di jaringan anda.

Instalasi dan Basic Konfigurasi squid dengan Authentikasi LDAP

Untuk mengimplementasikan squid agar dapat menggunakan Autentikasi dari LDAP maka paket-paket LDAP (Openldap) dan Squid mutlak harus di install. Dan agar pembahasannya jadi tidak melebar penulis mengsumsikan anda menginstall squid di mesin Samba-LDAP yang telah anda bangun, sehingga penulis tidak membahas cara instalasi dan konfigurasi ldap kembali (Silahkan and abaca artikel *Implementasi Samba PDC menggunakan backend LDAP*)

```
[root@ldap ~]# yum install squid
Loading "installonlyn" plugin
Setting up Install Process
Parsing package install arguments
local-repository          100% |=========================|  951 B     00:00
Resolving Dependencies
---> Running transaction check
---> Package squid.i386 7:2.6.STABLE12-1.fc7 set to be updated

Dependencies Resolved

================================================================
 Package                Arch        Version                 Repository        Size
================================================================
```

```
Installing:
 squid                    i386         7:2.6.STABLE12-1.fc7   local-repository   1.2 M

Transaction Summary
================================================================================
Install       1 Package(s)
Update        0 Package(s)
Remove        0 Package(s)

Total download size: 1.2 M
Is this ok [y/N]: y
Downloading Packages:
(1/1): squid-2.6.STABLE12 100% |=========================| 1.2 MB
00:00
Running Transaction Test
warning: squid-2.6.STABLE12-1.fc7: Header V3 DSA signature: NOKEY, key ID
4f2a6fd2
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: squid                        ########################## [1/1]

Installed: squid.i386 7:2.6.STABLE12-1.fc7
Complete!
```

Pastikan file squid/squid_ldap_auth dan squid/squid_ldap_group sudah berada di /usr/lib/squid

```
[root@ldap ~]# ll /usr/lib/squid/
total 368
-rwxr-xr-x 1 root root   24020 2007-03-27 21:10 cachemgr.cgi
-rwxr-xr-x 1 root root   17432 2007-03-27 21:10 digest_pw_auth
-rwxr-xr-x 1 root root   15728 2007-03-27 21:10 diskd-daemon
-rwxr-xr-x 1 root root   15524 2007-03-27 21:10 fakeauth_auth
-rwxr-xr-x 1 root root   12752 2007-03-27 21:10 getpwname_auth
-rwxr-xr-x 1 root root   14140 2007-03-27 21:10 ip_user_check
-rwxr-xr-x 1 root root   33908 2007-03-27 21:10 msnt_auth
-rwsr-x---   1 root squid 17612 2007-03-27 21:10 ncsa_auth
-rwxr-xr-x 1 root root   44916 2007-03-27 21:10 ntlm_auth
-rwsr-x--- 1 root squid 15576 2007-03-27 21:10 pam_auth
-rwxr-xr-x 1 root root   13260 2007-03-27 21:10 sasl_auth
-rwxr-xr-x 1 root root   14196 2007-03-27 21:10 smb_auth
-rwxr-xr-x 1 root root    4010 2007-03-27 21:09 smb_auth.pl
-rwxr-xr-x 1 root root    2280 2007-03-27 21:09 smb_auth.sh
-rwxr-xr-x 1 root root   20228 2007-03-27 21:10 squid_ldap_auth
-rwxr-xr-x 1 root root   21112 2007-03-27 21:10 squid_ldap_group
-rwxr-xr-x 1 root root   14500 2007-03-27 21:10 squid_unix_group
```

```
-rwxr-xr-x 1 root root     5392 2007-03-27 21:10 unlinkd
-rwxr-xr-x 1 root root     2359 2007-03-27 21:09 wbinfo_group.pl
-rwxr-xr-x 1 root root    13340 2007-03-27 21:10 yp_auth
```

Dari user LDAP yang telah ada, kita akan meng-*sekenariokan hanya user* (*UID*) *rsukmana dan htrisnadi yang dapat menggunakan internet melalui squid, maka buatlah file user*_proxy.*ldif sbb* :

```
[root@ldap ~]# cd /etc/squid
[root@ldap squid]# vim user_proxy.ldif
```

```
dn: cn=user_proxy,ou=Group,dc=smartbee,dc=com
cn: user_proxy
gidNumber: 1136
description: Internet Access user list
objectClass: top
objectClass: posixGroup
memberUid: rsukmana
memberUid: htrisnadi
```

Setelah itu masukan data tersebut ke dalam database LDAP

```
[root@ldap squid]# ldapadd -x –D "cn=Manager,dc=smartbee,dc=com" -w rahasia –f user_proxy.ldif
```

adding new entry " cn=user_proxy,ou=Group,dc=smartbee,dc=com "

Lalu cek apakah data yang anda input sudah masuk ke dalam database ldap

```
[root@ldap squid]# ldapsearch -x cn=user_proxy
```

```
# extended LDIF
#
# LDAPv3
# base <> with scope subtree
# filter: cn=user_proxy
# requesting: ALL
#

# user_proxy, Group, smartbee.com
dn: cn=user_proxy,ou=Groups,dc=smartbee,dc=com
cn: matari_proxy
gidNumber: 1136
description: Internet Access user list
objectClass: top
objectClass: posixGroup
memberUid: rsukmana
```

memberUid: htrisnadi

Ok, Setelah selesai semua sekarang kita konfigurasikan squid.conf

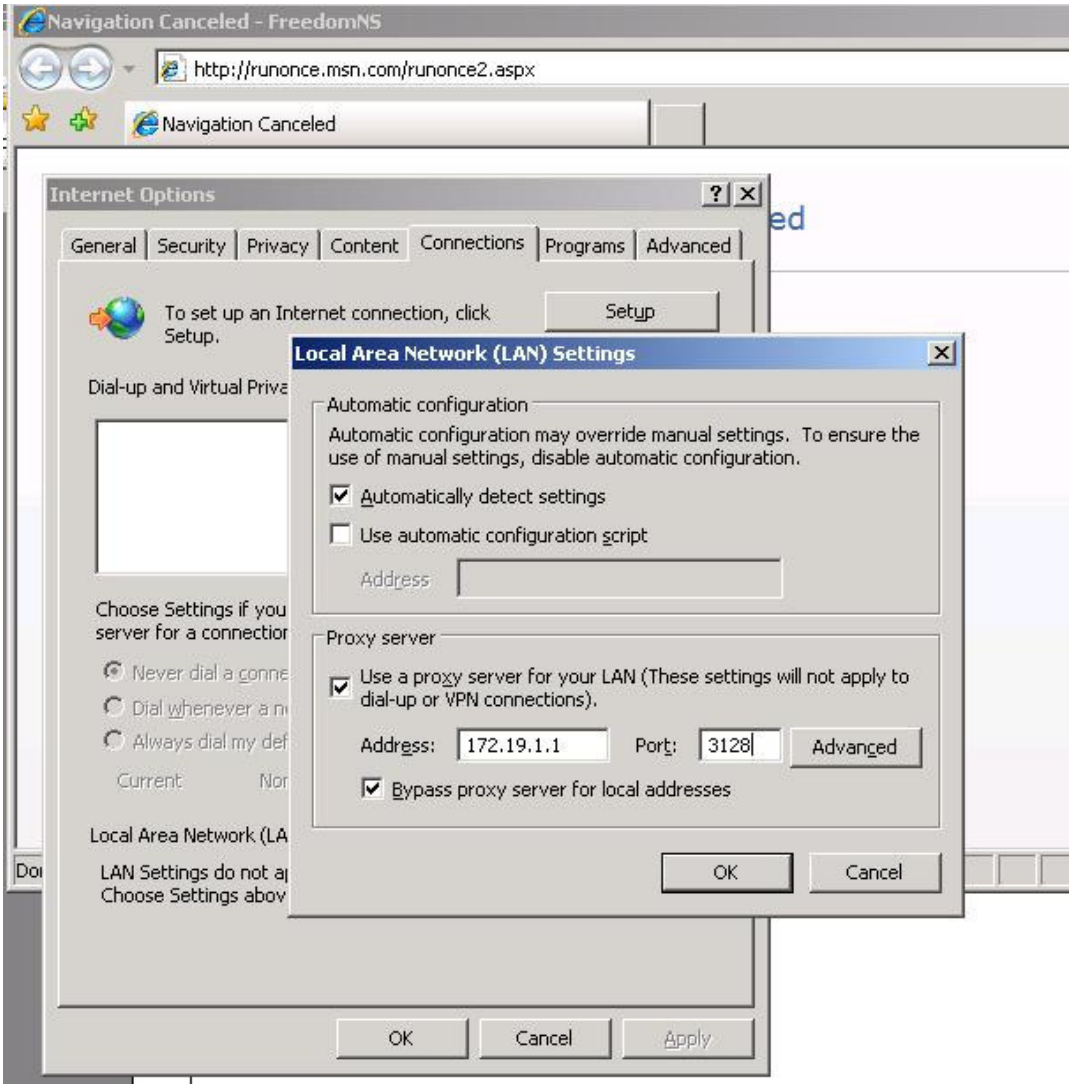
```
[root@ldap squid]# vim squid.conf
```

```
#Author by ratdix@yahoo.com
http_port 3128

cache_mem 32 MB
cache_swap_low 80
cache_swap_high 95
maximum_object_size 4096 KB
minimum_object_size 4 KB
cache_dir ufs /var/spool/squid 1600 4 256
cache_access_log /var/log/squid/access.log
cache_store_log /var/log/squid/store.log
cache_log /var/log/squid/cache.log

auth_param basic program /usr/lib/squid/squid_ldap_auth -b "dc=smartbee,dc=com" -f (&(objectclass=posixAccount)(uid=%s)) 127.0.0.1
external_acl_type ldapgroup %LOGIN /usr/lib/squid/squid_ldap_group -b "dc=smartbee,dc=com" -f "(&(objectclass=posixGroup)(cn=user_proxy)(memberUid=%v))" 127.0.0.1

acl all src 0.0.0.0/0.0.0.0
acl lan src 172.19.0.0/255.255.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 536 # http Ftp https snews
aacl Safe_ports port 70 210 # gopher wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 488 591 777 # http-mgmt gss-http filemaker multiling-http
acl CONNECT method CONNECT
acl proxyuser external ldapgroup user_proxy

http_access allow manager localhost
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow proxyuser
http_access allow lan
http_reply_access allow all
icp_access allow all

cache_mgr ratdix@yahoo.com
visible_hostname proxy.smartbee.com
```

Setelah selesai mengkonfigurasi dan menyimpan perubahan file squid.conf, anda jalankan perintah squid –z untuk membuat semua direktori swap yang telah di tentukan lalu jalankan squid proxy yang telah anda bangun

```
[root@ldap squid]# squid –z
[root@ldap squid]# service squid start
```

Setelah konfigurasi di sisi server selesai, maka anda tinggal mengkonfigurasikan internet browser di komputer client yang akan menggunakan proxy dalam berinternet
Utk Firefox : Tools -> Options -> Advanced -> Network -> Settings
Utk IE : Tools -> Internet options -> Connection -> Lan settings -> Proxy server
Lalu ketikan alamat server squid anda dan port yang di gunakan.



Keterangan dari konfigurasi squid :

http_port 3128

Port HTTP yang gunakan oleh Squid. Defaultnya adalah 3128. Biasanya port yang umum untuk sebuah proxy server adalah 8080. Terkadang Squid juga memakai port 80 kalau sedang berfungsi sebagai reverse proxy server

```
cache_mem 32 MB
```

Memory fisik ideal yang digunakan Squid untuk menangani objek-objek *In-Transit (*object yang dalam masa transisi antara waktu cache mendownload sampai object disampaikan ke klien) , *Hot Object (*object yang sering diakses.), dan *Negative Cache Object.* Jika anda memiliki memory yang berlebih, maka disarankan untuk menaikkannya dan ada yang berpendapat bahwa nilai ini didapat dari sepertiga memory bebas bagi squid.

```
cache_swap_low 80
cache_swap_high 95
```

Squid akan menghapus object yang ada didalam hardisknya jika media tersebut mulai penuh. Ukuran penuh ini yang diset pada cache_swap_low dan cache_swap_high (menggunakan ukuran Persen). Bila batas swap_low telah tercapai maka squid mulai menghapus dan jika batas swap_high tercapai maka squid akan semakin sering menghapus.

```
maximum_object_size 4096 KB
minimum_object_size 4 KB
```

Dengan option ini, ukuran file maksimum yang disimpan oleh squid cache bisa dibatasi. Dengan kata lain objek yang lebih besar dari nilai maximum_object_size tidak akan disaved ke dalam disk yang sudah disisihkan buat cache dan objek yang lebih kecil dari nilai minimum_object_size tidak akan disaved ke dalam disk yang sudah disisihkan buat cache

```
cache_dir ufs /var/spool/squid 1600 4 256
```

Option pada cache_dir menentukan sistem penyimpanan seperti apa yang akan digunakan (ufs), nama direktori tempat penyimpanan cache (/var/spool/squid), ukuran disk dalam megabytes yang digunakan oleh direktori tempat penyimpanan cache (1600 Mbytes), jumlah subdirektori pertama yang akan dibuat di bawah /var/spool/squid (4), dan jumlah subdirektori kedua yang akan diciptakan di bawah subdirektori pertama tadi (256). Nilai pada option cache_dir tadi harus disesuaikan dengan sistem yang anda miliki.

Nilai tersebut dapat kita peroleh dari rumus berikut :

- Gunakan 80% atau kurang dari setiap kapasitas cache direktori yang telah kita siapkan. Jika kita mengeset ukuran cache_dir kita melebihi nilai ini, maka kita akan dapat melihat penurunan performansi squid.
- Untuk menentukan jumlah subdirektori pertama yang akan dibuat, dapat menggunakan rumus ini:

x=Ukuran cache dir dalam KB (misal 6GB=~6,000,000KB)
y=Average object size (gunakan saja 13KB)
z= Jumlah subdirektori pertama = (((x / y) / 256) / 256) * 2 = ? direktori
Sebagai contoh, misal saya menggunakan 6 GB dari untuk /cache (setelah disisihkan 80% nya), maka: 6,000,000 / 13 = 461538.5 / 256 = 1802.9 / 256 = 7 * 2 = 14
Sehingga baris cache_dir akan menjadi seperti ini: cache_dir ufs 6000 14 256

```
cache_access_log /var/log/squid/access.log
cache_store_log /var/log/squid/store.log
cache_log /var/log/squid/cache.log
```

Merupakan tempat dimana file log-log squid di letakkan

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b "dc=smartbee,dc=com" -f
(&(objectclass=posixAccount)(uid=%s)) 127.0.0.1
external_acl_type ldapgroup %LOGIN /usr/lib/squid/squid_ldap_group -b "dc=smartbee,dc=com" -f
"(&(objectclass=posixGroup)(cn=user_proxy)(memberUid=%v))" 127.0.0.1
```

Merupakan Konfigurasi agar menggunakan backend LDAP untuk authentikasinya.

```
acl all src 0.0.0.0/0.0.0.0
acl lan src 172.19.0.0/255.255.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 536 # http Ftp https snews
aacl Safe_ports port 70 210 # gopher wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 488 591 777 # http-mgmt gss-http filemaker multiling-http
acl CONNECT method CONNECT
acl proxyuser external ldapgroup user_proxy

http_access allow manager localhost
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow proxyuser
http_access allow lan
http_reply_access allow all
icp_access allow all
```

Ini merupakan opsi Access Control List. Aturannya adalah bahwa sesuatu yang telah dieksekusi pada baris yang lebih atas maka dia tidak dieksekusi lagi dibaris yang paling bawah, walaupun dalam parameter ACL yang dibawah tersebut dia juga termasuk contoh pada opsi "http_access allow proxyuser" maka squid akan meminta Autentikasi dan bila user tersebut tidak terdaftar maka user tersebut tidak akan bias menggunakan internet walaupun ada rule "http_access allow lan" dibawahnya.

```
cache_mgr ratdix@yahoo.com
visible_hostname proxy.smartbee.com
```

Opsi ini merupakan keterangan dari Administrator, sehingga apabila ada kendala dalam pengaksesan web melalui squid (misal, situs yang di blok, dll) maka squid akan menampilkan informasi-informasi diatas.

Biografi Penulis

Ratdhian Cipta Sukmana.
Mempelajari Ilmu Komputer berawal dari hobi, sejak SMU telah mengikuti pelatihan-pelatihan komputer hingga akhirnya dapat menyelesaikan S1 pada jurusan System Komputer Universitas Gunadarma Jakarta di akhir tahun 2001. Memulai karirnya sebagai Technical Support di beberapa perusahaan dan hingga kini masih aktif sebagai System Administrator di salah satu perusahaan Advertising di Jakarta. Sangat tertarik dengan Open Source dan Networking. Kopetensi inti pada bidang IT Support, Network Security, Administrator dan System Developer. Aktif di berbagai milis, dan selalu berusaha menggemakan konsep keterbukaan akan ilmu pengetahuan dengan semangat "Open Content". Berbagai artikel komputasi menarik lain yang di tuliskan berdasarkan pengalaman tersedia di situs blog *http://ratdix.wordpress.com*