Proxy Server - 啟動使用者認證機制

參考文件

- http://forum.icst.org.tw/phpBB2/viewtopic.php?t=8646

當 Proxy Server 有很多 Client 在使用時，或許您會想要開始做認證機制，也就是說當使用者在輸入帳號密碼之後才可以使用 Proxy 服務，同時，藉由帳號密碼的管制，也可以了解使用者大部份都是連到那一個網站，並且做適當的流量控管。

Squid 支援使用者認證的方法有很多，包含了以 htpasswd 方式的帳號密碼檔認證 (NCSA)、LDAP、PAM、SASL、SMB (就是 Samba)、YP (就是 NIS)和 MSNT 等方式，在這裡我示範 NCSA 的基本方式，當然若有時間的話我將會測試 LDAP 的方式來認證，屆時將會歸類到 LDAP 應用。

重新編譯 NCSA Module

若您的 Proxy 已經上線的話，那麼要重新編譯整個 squid 再安裝似乎是一件不可能的事，這個時候或許你可以直接編譯 NCSA 這個模組並掛載上去就可以了。

重新編譯

若你要重新編譯整個 squid 套件，可以參考 Proxy Server - 安裝與基本設定，當然，你還必需加入 --enable-auth="basic" 和 --enable-basic-auth-helpers="NCSA" 這兩個選項。

```
root # ./configure --enable-auth="basic" \
> --enable-basic-auth-helpers="NCSA"
```

只編譯 NCSA 套件

在同一個版本的 squid 套件中，請到 squid 原始碼的目錄裡找到 helpers/basic_auth/NCSA 目錄，執行 make 後再複製到 squid 的模組目錄裡就可以了。我的 squid 是在 /usr/local/squid 目錄裡。

```
root # cd /misc/squid-2.6.STABLE3/helpers/basic_auth/NCSA
root # make
root # cp ncsa_auth /usr/local/squid/libexec
```

如此就可以了。

取得 htpasswd 程式

htpasswd 是在 Apache 套件裡的一個小程式，主要的用法你可以在 Apache 安全設定 參考到。你可以從別的 Apache Server 取得 (但是要注意相關的 library)，或是直接再載 Apache 然後編譯 htpasswd 這個程式。

若你從別台機器複制過來的 htpasswd 無法用的話，請使用 ldd 看看有沒有缺少的 library。

```
root # ldd htpasswd
libz.so.1 => /usr/lib/libz.so.1 (0x00781000)
libssl.so.4 => /lib/libssl.so.4 (0x00a6c000)
libcrypto.so.4 => /lib/libcrypto.so.4 (0x008b4000)
libgssapi_krb5.so.2 => /usr/lib/libgssapi_krb5.so.2 (0x0089e000)
libkrb5.so.3 => /usr/lib/libkrb5.so.3 (0x00814000)
libcom_err.so.2 => /lib/libcom_err.so.2 (0x00793000)
libk5crypto.so.3 => /usr/lib/libk5crypto.so.3 (0x0087b000)
libresolv.so.2 => /lib/libresolv.so.2 (0x007d3000)
librt.so.1 => /lib/tls/librt.so.1 (0x007a3000)
libm.so.6 => /lib/tls/libm.so.6 (0x0075c000)
libcrypt.so.1 => /lib/libcrypt.so.1 (0x00111000)
libnsl.so.1 => /lib/libnsl.so.1 (0x007fc000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x007e8000)
libdl.so.2 => /lib/libdl.so.2 (0x00756000)
libc.so.6 => /lib/tls/libc.so.6 (0x0062b000)
/lib/ld-linux.so.2 (0x00612000)
root #
```

若你要重新編譯 Apache 的話，在編譯完成之後，可以在 support 目錄找到一個 htpasswd 這個程式可以直接使用。

```
root # cp support/htpasswd /usr/bin
```

設定 squid.conf

我的 squid.conf 是放在 /usr/local/squid/etc 目錄裡，所以以下只要說到 squid.conf 都是在這個目錄中編輯。你可以先看看 squid.conf 的設定是怎麼樣子。

下面是去掉註解並加入行號的樣子。

```
root # cat squid.conf | sed -e '/^#.*/d' -e '/^$/d' | nl
    1  http_port 3128
    2  hierarchy_stoplist cgi-bin ?
    3  acl QUERY urlpath_regex cgi-bin \?
    4  cache deny QUERY
    5  acl apache rep_header Server ^Apache
    6  broken_vary_encoding allow apache
    7  cache_dir ufs /usr/local/squid/var/cache 100 16 256
    8  access_log /usr/local/squid/var/logs/access.log squid
```

```
 9  refresh_pattern ^ftp:         1440    20%    10080
10  refresh_pattern ^gopher:       1440    0%     1440
11  refresh_pattern .             0      20%    4320
12  acl all src 0.0.0.0/0.0.0.0
13  acl manager proto cache_object
14  acl localhost src 127.0.0.1/255.255.255.255
15  acl to_localhost dst 127.0.0.0/8
16  acl SSL_ports port 443 563
17  acl Safe_ports port 80        # http
18  acl Safe_ports port 21        # ftp
19  acl Safe_ports port 443 563    # https, snews
20  acl Safe_ports port 70        # gopher
21  acl Safe_ports port 210       # wais
22  acl Safe_ports port 1025-65535  # unregistered ports
23  acl Safe_ports port 280       # http-mgmt
24  acl Safe_ports port 488       # gss-http
25  acl Safe_ports port 591       # filemaker
26  acl Safe_ports port 777       # multiling http
27  acl CONNECT method CONNECT
28  http_access allow manager localhost
29  http_access deny manager
30  http_access deny !Safe_ports
31  http_access deny CONNECT !SSL_ports
32  acl l-penguin src 192.168.1./24
33  http_access allow l-penguin
34  http_access deny all
35  http_reply_access allow all
36  icp_access allow all
37  cache_effective_user nobody
38  coredump_dir /usr/local/squid/var/cache
root #
```

你列出設定檔之後，應該更了清楚的看到到底設定了那些東西，現在就來加入 ncsa 支援。

```
root # vi squid.conf
-----------------------------------------------------------------
# 認證時出現的提示
auth_param basic realm Welcome to l-penguin's proxy service, please enter
your name and password.
# 指定是由 ncsa_auth 認證，帳號密碼檔為 squid-passwd
auth_param basic program /usr/local/squid/libexec/ncsa_auth
/usr/local/squid/etc/squid-passwd

# 設定使用 proxy_auth
acl squid-passwd proxy_auth REQUIRED
# 允許通過認證的者用者使用用 Proxy
http_access allow squid-passwd
-----------------------------------------------------------------
root #
```

請注意，在設定 http_access allow squid-passwd 時，一定要放在 http_access deny all 的前面，否則會全部都被 deny 掉。

新增一個使用者

因為在剛剛的設定檔裡我指定了帳號密碼檔是放在 /usr/local/squid/etc/squid-passwd 這個檔案裡面，所以現在就使用 htpasswd 這個程式來新增使用者。

```
root # cd /usr/local/squid/etc; htpasswd -c squid-passwd steven
New password: your_password <- 不會顯示出來
Re-type new password: your_password <- 不會顯示出來
Adding password for user steven
root #
```

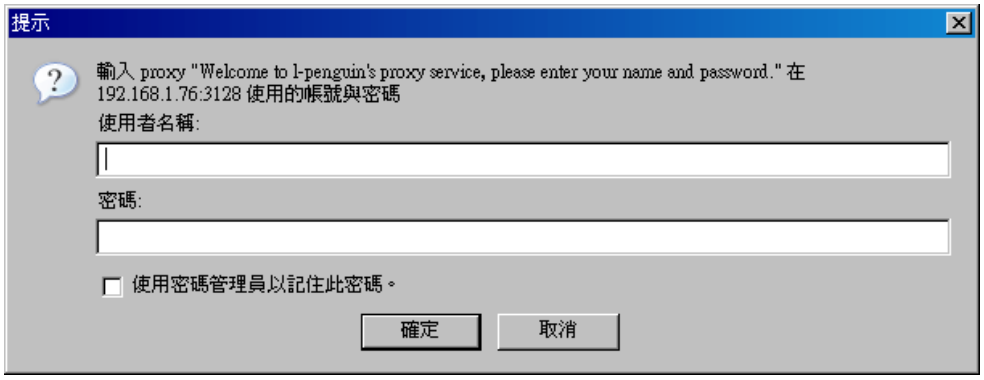
好了，現在請重新開啟 squid，所有設定都會生效。

```
root # /usr/local/squid/bin/RunCache &
root #
```

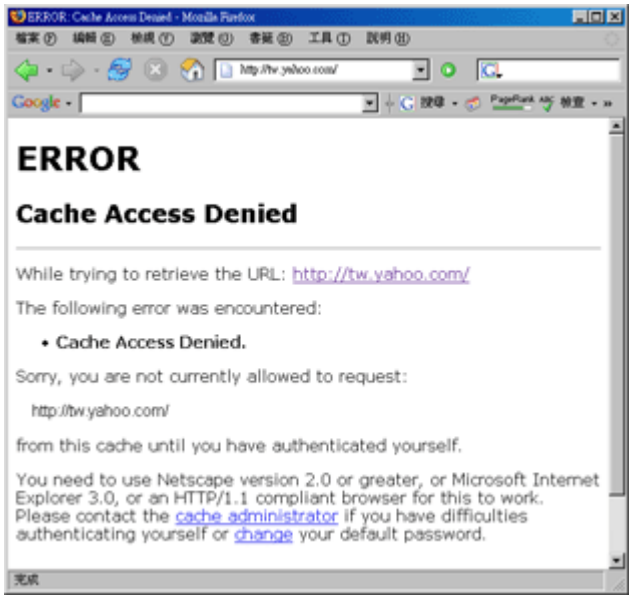
請注意，若是在啟動中發現任錯誤，可以查看 /usr/local/squid/var/squid.out 這檔案的記錄。

測試

現在，請使用者開啟 Browser 看看，在連線之前會尋問帳號密碼。



若是驗證不成功就會出現以下畫面。



查看使用者的動作

我想一個忙碌的管理員應該不會去看那個使用看了那些網站，但除非必要，還是可以查得出來那些使用者瀏覽過那些網頁，要查看這些資訊只要開啟 access.log 就可了。

```
root # /usr/local/squid/var/logs/access.log
~ 以上略 ~
1157818446.454 833 192.168.1.3 TCP_MISS/200 3479 GET
http://cmxml.tw.yahoo.p.
overture.com/d/search/p/standard/js/flat/ctxt/? steven
DIRECT/61.213.167.216 app
lication/x-javascript
1157818448.084 19 192.168.1.3 TCP_NEGATIVE_HIT/404 3779 GET
```

```
http://tw.rd.yah
oo.com/referurl/hp/ steven NONE/- text/html
1157818448.815 2025 192.168.1.3 TCP_MISS/200 480 GET
http://row.bc.yahoo.com/b
? steven DIRECT/211.115.107.126 image/gif
1157818448.901 2107 192.168.1.3 TCP_MISS/200 480 GET
http://row.bc.yahoo.com/b
? steven DIRECT/211.115.107.126 image/gif
1157818449.059 2258 192.168.1.3 TCP_MISS/200 480 GET
http://row.bc.yahoo.com/b
? steven DIRECT/211.115.107.126 image/gif
1157818591.126 788 192.168.1.3 TCP_MISS/200 3112 GET
http://rad.msn.com/ADSAd
Client31.dll? steven DIRECT/207.68.178.16 text/html
1157818592.176 837 192.168.1.3 TCP_MISS/200 15831 GET
http://global.msads.net
/ads/5722/0000005722_00000000000000337454.swf? steven
DIRECT/210.201.139.93 app
lication/x-shockwave-flash
1157818654.284 2 192.168.1.3 TCP_DENIED/407 1828 GET
http://tw.news.yahoo.c
om/rss/realtime - NONE/- text/html
1157818657.428 127 192.168.1.3 TCP_DENIED/407 1777 GET
http://tw.yahoo.com/ -
NONE/- text/html
1157818668.765 41 192.168.1.3 TCP_DENIED/407 1933 GET
http://newsrss.bbc.co.
uk/rss/newsonline_world_edition/front_page/rss.xml - NONE/- text/html
~ 以下略 ~
root #
```

如此就可以看到 steven 曾經看過那些網頁或檔案了。

For more articles, please visit http://www.l-penguin.idv.tw/

作者：廖子儀 (Tzu-Yi Liao)
Certified：LPIC Level I、LPIC Level II、RHCE
E-mail：steven@l-penguin.idv.tw
Web site：http://www.l-penguin.idv.tw/