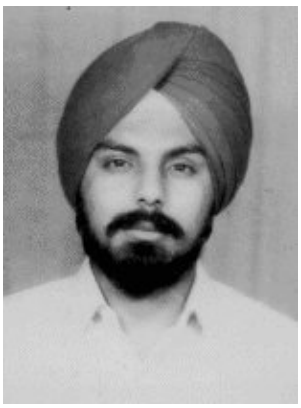
# Configurare un Proxy–Server con Squid



by D.S. Oberoi
<ds_oberoi/at/yahoo.com>

*About the author:*
D.S. Oberoi vive a Jammu (India). Attulmente ha problemi a collegarsi ad internet a cuasa delle attuali tensioni politiche nel suo paese.

*Abstract*:

Linux è divenuto un sinonimo per la rete. È utilizzato sia in ufficio che a casa in qualità di server per condivisione file, di stampa, di posta elettronica e per applicazioni. Sta anche aumentando il suo utilizzo come proxy server.

Un Proxy server fornisce accesso ad Internet a molteplici utenti allo stesso tempo, condividendo un singolo accesso ad Internet. Un buon proxy gestisce anche uno spazio per memorizzare le richieste (noto come cache), in modo da favorire il vostro accesso ai dati, utilizzando quelli presenti in questo spazio, che sono precedentemente stati già richiesti, piuttosto che chiederli direttamente al server web, contribuendo così a ridurre i tempi di accesso ed a conservare banda. Squid è un software che fa questo. Implementa una cache per l'http, l'ftp, il gopher, e molti altri protocolli... Squid supporta anche il protocollo SSL, politiche di accesso, cache delle richieste DNS e genera un log dettagliato delle richieste. Logi Sense fornisce anche una implementazione di Squid per ambienti WindowsNT.

Lo scopo di questo articolo è quello di dare al lettore una linea guida per configurare un server proxy e le modalità per gestire le politiche di accesso ad esso da parte degli utenti.

## Squid è installato nel nostro sistema?

Squid, in formato rpm, è presente nella distribuzione RedHat 7.1 e viene installato automaticamente se si seleziona la modalità di installazione come Sistema Operativo per l'uso in rete (Network OS). Si può controllare se esso sia difatti installato con il seguente comando:

```
rpm -q squid
```

L'ultima versione di Squid può esser scaricata dalla Homepage di Squid ed alcuni siti mirror. Squid può esser installato sul sistema desiderato con il seguente comando:

```
rpm -ivh squid-2.3.STABLE4-10.i386.rpm
```

# Configurare Squid

Il funzionamento ed il comportamento di Squid sono controllati per mezzo del proprio file di configurazione, squid.conf, che è assai dettagliato; questo file è di norma presente nella cartella /etc/squid. Il file di configurazione squid.conf è molto lungo, difatti si protrae per molteplici pagine, ed il suo aspetto positivo consiste nel fatto che tutte le opzioni sono chiaramente esposte all'interno del medesimo.

La prima cosa che si dovrà modificare è http_port, che specifica in che porta si debba creare il socket su cui Squid sia in attesa delle richieste dei client. Per default questo valore è pari a 3128, ma può esser modificato in un valore definito dall'utente medesimo. Assieme al valore della porta, si può anche specificare l'Indirizzo IP su cui effettuare questo socket nella macchina un cui è in esecuzione Squid; esso può esser cambiato in:

http_port 192.168.0.1:8080

Questa dichiarazione fa sì che Squid esegua un binding tra la porta 8080 e l' IP 192.168.0.1. Si può assegnare qualsiasi porta, ma siate sicuri che non vi sia alcuna applicazione che ne faccia uso. Con diverse righe simili possono esser assegnate più combinazioni di porte ed IP a cui si possa offrire il serivizio.

# Controllo d'Acesso

Le politche di accesso ad internet possano basarsi su particolari orari o lassi di tempo, di cache, particolari siti o gruppi di siti e molte altre opzioni... Il sistema di accesso è basato su due specifici componenti: elementi di ACL e liste d'acesso.. Difatti una lista d'accesso permette di autorizzare o negare l'utilizzo del servizio stesso. Alcuni tipi e definizioni delle politche di ACL sono qui elencati

- src : Origine: Indirizzo IP del client
- dst : Destinazione: Indirizzo IP del server
- srcdomain : Dominio di origine: Dominio del client
- dstdomain : Dominio di destinazione: il dominio del server
- time : Ora del giorno e giorno della settimana
- url_regex : Ricerca una sottostringa nell'URL
- urlpath_regex: Rierca una sottosrtinga nell'URL, escudendo dalla ricerca e il protocollo e l'hostname
- proxy_auth : Autentifica il client per mezzo di procedure esterne
- maxconn : Numero massimo di connessioni concomitati dall'IP di un client

Per utilizzare i controlli di acesso, si debbono prima definire delle politiche di acesso ed applicare le regole a queste ultime. Il formato di una dicharazione ACL è

acl  nome_elemento_acl  tipo_di_elemento_acl valore_della_acl

Nota :

1. nome_elemento_acl è un nome, defino a piacere da un utente, assegnato ad una ACL.
2. Non vi possono essere due elementi ACL con lo stesso nome.
3. Ogni ACL consiste in una lista di valori. Quando viene eseguita la ricerca di riscontro, molteplici valori sono considerati con l'operatore logico OR. Ciò significa che, si ha un riscontro positivo allorchè si abbia almeno un elmento che risponda alla rchiesta.
4. Non tutti gli elementi ACL possono esser usati in congiunzione con le liste di accesso.
5. Più elementi ACL possono essere definiti creando molteplici righe di definizione. Squid li combinerà poi in una singola lista.

Sono disponibili diverse liste di accesso. Quelle che noi ora andremo a considerare per la nostra configurazione sono:

- **http_access:** Permette ai client che effettuino richieste di tipo HTTP di accedere alla porta HTTP. Questa è la lista di controllo di accesso controllo primario.
- **no_cache:** Definisce il metodo della cache basandosi sulle risposte.

Una lista di regole di accesso consiste in un gruppo di parole chiave come allow(permetti) e deny(vieta), autorizzando o negando l'utlizzo di un servizio ad una particolare ACL o ad un gruppo delle medesime.
Nota:

1. Le regole sono controllate nell'ordine in cui esse sono definite (ovvero scritte nel file di configurazione). Appena si ha un riscontro positivo con una regola la ricerca termina.
2. Una lista di accesso è formata da più regole.
3. Se non si ha alcun riscontro tra le regole definite, il comportamento del server sarà pari al contrario dell'ultima regola espressa. È, quindi bene, definire un comportamento predefinito.
4. Tutti gli elementi di una voce di accesso sono trattati con l'operatore logico AND. Il tutto viene trattato come di seguito evidenziato:
   http_access Azione dichiarazione1 AND dichiarazione2 AND dicharazione
   OR.
   http_access Azione dichiarazone3
   Più dichiazioni http_access sono trattate con l'operatore logico OR.
5. Mi raccomando ancora... vi ricordo che le regole sono lette dalla prima scritta all'ultima.

# Torniamo alla configurazione

Come regola predefinita Squid non permette l'accesso a nessun client. Si deve quindi modificare la lista di controllo accessi. Ognuno deve decidere la propria lista contente le proprie regole di accesso. Scorrete il file squid.conf ed aggiungiete le seguenti righe subito prima della riga che inizia con http_access deny all

```
acl mynetwork 192.168.0.1/255.255.255.0
http_access allow mynetwork
```

mynetwork è il nome dato all'acl e la riga seguente definisce la regola applicata alla particolare acl che ho definito. Essa si riferisce alla mia rete. 192.168.0.1 si riferisce ad un indirizzo della mia rete che ha come maschera 255.255.255.0. mynetwork essenzialmente è un nome che raggruppa tutte le macchine della mia rete e la regola subito sotto definita ne permette l'accesso. Questa modifica assieme quella fatta inerente la definizione http_port è sufficiente per permettere a Squid di funzionare. Dopo aver effettuato questi cambiamenti Squid può essere attivato con il seguente comando:

```
service squid start
```

Nota :
Squid può anche venire attivato automaticamente all'avvio del sistema abilitando l'esecuzione del servizio in ntsysv o per mezzo del comando setup (System Service Menu). Dopo aver eseguito qualsiasi modifica nel file di configurazione di Squid il processo attualmente attivo deve essere fermato e riavviato affinchè le modifiche abbiano effetto. I comandi per effettuare il riavvio del serivizio Squid possono essere due:

1. service squid restart
2. /etc/rc.d/init.d/squid restart

# Configurazione della macchina client

Siccome le richieste del client devono essere rivolte ad una particolar porta del server proxy, la macchina client deve essere configurata per interagire correttamente. Si presuppone che le macchine client siano già correttamente collegate alla LAN (abbiano, cioè, un indirizzo IP valido) e siano in grado di comunicare col nostro server linux (potere usare il comando ping per verificare la comunicazione con il server suddetto).
Per le macchine che utilizzano Internet Explorer

1. Scegliete il menù Strumenti –> Opzioni Internet
2. Selezionate la voce Connessione e premete sul tasto Impostazioni LAN
3. Attivate la funzionalità Utilizza proxy Server ed inserite l'indirizzo IP del server e la porta su cui Squid offre il servizio(http_port address).

Per le macchine che utilizzano Netscape Navigator

1. Scegliete il menù Modifica –> Preferenze –> Avanzate –> Proxy.
2. Selezionate Configurazione Manuale del Proxy.
3. Premete il tasto Mostra. &
4. inserite l'indirizzo IP del server e la porta su cui Squid offre il servizio(http_port address).

# Utilizzare la funzionalità di controllo di accesso

Molte ACL e regole permettono di controllare l'accesso ad Internet dei client in maniera molto flessibile e funzionale. Esempi di metodi di controllo sono qui riportati. Non esistono solo queste regole di controllo, non consideratele quindi come le uniche appliccabili.

1. Autorizzare un gruppo di macchine di accedere ad Internet:

   ```
   acl allowed_clients src 192.168.0.10 192.168.0.20 192.168.0.30
   http_access allow allowed_clients
   http_access deny !allowed_clients
   ```

   Queste definizioni permettono solo alle macchine che hanno come indirizzo IP 192.168.0.20, 192.168.0.10 e 192.168.0.30 di accedere ad Internet e negare l'accesso ad Internet alle altre macchine (che non sono presenti nella dichiarazione allowed_clients).
2. Restringere l'accesso durante determinati periodi della giornata.

   ```
   acl allowed_clients src 192.168.0.1/255.255.255.0
   acl regular_days time MTWHF 10:00–16:00
   http_access allow allowed_clients regular_days
   http_access deny allowed_clients
   ```

   Questo permette di accedere ad Internet a tutte le macchine della classe di rete 192.168.0.1 dalle ore 10:00 alle ore 16:00 nei giorni dal Lunedì al Venerdì.
3. Accesso differenziato per orari e client

```
acl hosts1 src 192.168.0.10
acl hosts2 src 192.168.0.20
acl hosts3 src 192.168.0.30
acl mattino time 10:00−13:00
acl ora_di_pranzo time 13:30−14:30
acl sera time 15:00−18:00
http_access allow host1 mattino
http_access allow host1 sera
http_access allow host2 ora_di_pranzo
http_access allow host3 sera
http_access deny all
```

Queste dichiarazioni permettono al client host1 di accedere ad Internet sia la mattina sia la sera; i client host2 ed host3 possono invece accedere al servizio rispettivamente solo all'ora di pranzo e la sera.

Nota:
Tutte le definizioni di accesso sono unite tra loro con un AND logico ed eseguite con la seguente modalità

http_access Action statement1 AND staement2 AND statement OR.

Più dichiarazioni http_access sono valutate con operatore logico OR mentre le dichiarazioni in una singola riga sono trattate con l'operatore AND. Per questo motivo la riga

http_access allow host1 mattino sera

non avrebbe di certo fatto accedere al client sia la mattina che la sera in quanto non può verificarsi la condizione data dall'ora (mattino AND sera).

4. Interdizione verso alcuni siti
Squid può vietare l'accesso a particolari siti o a siti che contengono specifiche parole. Ciò può essere implementato nella seguente maniera:

```
acl allowed_clients src 192.168.0.1/255.255.255.0
acl banned_sites url_regex abc.com *()(*.com
http_access deny banned_sites
http_access allow allowed_clients
```

La stessa operezione può essere attuata bloccando l'accesso a siti che contengono specifiche parole. Per esempio le parole dummy , fake

```
acl allowed_clients src 192.168.0.1/255.255.255.0
acl banned_sites url_regex dummy fake
http_access deny banned_sites
http_access allow allowed_machines
```

Risulta poco funzionale inserire tutti siti e le parole che si vogliano bloccare all'interno del file di configuarazione. Possiamo invece includere questa lista in un file esterno (per esempio il file /etc/banned.list) e la ACL può inglobare queste informazioni prelevandole dal file da noi definito.

```
acl allowed_clients src 192.168.0.1/255.255.255.0
acl banned_sites url_regex "/etc/banned.list"
```

http_access deny banned_sites
http_access allow allowed_clients

5. Ottimizzarne l'uso
   Squid può limitare il numero di connessioni da un client; questa funzionalità si attiva per mezzo della definizione maxconn. Per poter utlizzare questa limitazione si deve prima attivare la funzionalità client_db.

   acl mynetwork 192.168.0.1/255.255.255.0
   acl numconn maxconn 5
   http_access deny mynetwork numconn

   Nota:
   La ACL maxconn utilizza un confronto basato su minore di. Essa quindi è vera allorquando il numero di connessioni supera il valore (numconn) da noi definito. Questo è il motivo per cui non abbiamo una dichiarazione http_access allow.
6. Memorizzazione dei dati richiesti
   Le risposte alle richieste sono immediamente messe in cache. Questa è una ottima cosa se tratta di pagine il cui contenuto sia statico. Non vi è, dall`altro canto, la minima utlità di memorizzare localmente pagine cgi o Servlet. Si può prevenire la memorizzazione locale di queste pagine per mezzo della ACL no_cache.

   acl cache_prevent1 url_regex cgi−bin /?
   acl cache_prevent2 url_regex Servlet
   no_cache deny cache_prevent1
   no_cache deny cache_prevent2
7. Personalizzare i messaggi d'errore.
   È possibile creare i propri messaggi di errore associati ad una regola di divieto. Questo viene implementato per mezzo della dichiarazione deny_info. Tutti i messaggi d'errore di Squid sono memorizzati in /etc/squid/errors/ La cartella contenente i messaggi d'errore può essere cambiata con un'altra per mezzo della dichiarazione error_directory. Un'altra soluzione è quella di ricorrere alla modifica dei messagi d'errore già presenti.

   acl allowed_clients src 192.168.0.1/255.255.255.0
   acl banned_sites url_regex abc.com *()(*.com
   http_access deny banned_sites
   deny_info ERR_BANNED_SITE banned_sites
   http_access allow allowed_clients

   Nell'esempio precedente, un messaggio personalizzato verrà visualizzato allorquando un utente cercherà di accedere al sito contenente i termini che vogliamo interdire. Il file che viene dato come parametro (in tal caso ERR_BANNED_SITE) deve esistere nella cartella degli errori. Questo tipo di file deve esser scritto con codice HTML. Gli esempi qui esposti sono solo alcune opzioni, capacità e delle dichiarazioni di una ACL. Il lettore può trovare nella sezione inerente le FAQ *(sito in inglese)* molte altre spiegazioni su un uso più complesso e funzionale delle opzioni inerenti le dichiarazioni ACL e le poltiche di accesso al servizio.

# I file di log

Tutti i file di log di Squid sono contenuti nella cartella /var/log/squid; ivi sono contenuti i log della cache, degli accessi e il file store.log. Il file access.log tiene traccia delle richieste dei client, inserendo una voce per

ogni richiesta HTTP e ICP fatta dal proxy server, l'indirizzo IP del client, il metodo usato per la richiesta, l'URL richiesto ed altri parametri. I dati contenuti in questo file possono essere utlizzati per effettuare delle analisi inerenti gli accessi. Molteplici programmi, come per esempio sarg, calamaris, Squid−Log−Analyzer sono in grado di analizzare i dati presenti in questi file di log e generare dei report, di norma in formato HTML. I report possono esser basati, per esempio, sugli utenti, sugli indirizzi IP, sui siti visitati...

Il percorso ed il nome del file di questi file può esser cambiato per mezzo delle seguenti opzioni:

```
cache_access_log      Per il file access.log
cache_log             Per il file cache.log
cache_store_log       Per il file store.log (Store manager)
pid_filename          Per il file che regista il PID del processo.
```

# Metodi di autentificazione

Squid, nella sua configurazione di base, permette a tutti gli utenti che rispettino le regole di accedere al servizio senza bisogno di autentificarsi. L'autentificazione degli utenti, per esempio per permettere solo a determinati utenti (che si possono quindi collegare da qualsiasi macchina) di accedere al servizio. Squid permette l'utilizzi di metodi di autentificazione per mezzo di applicativi esterni, inserendo, per esempio, uno username ed una password. Questa funzione è attivabile per mezzo delle dichiarazioni proxy_auth e authenticate_program, che obbliga un untente a registrarsi per verificare le credenziali dello username e della password prima che possa accedere al servizio. Sono molteplici i programmi che sono disponibili per Squid:

1. LDAP : Utlizza il protocollo LDAP
2. NCSA : Utilizza un file contenente username e password secondo lo standard NCSA
3. SMB : Utilizza il protocollo SMB (implentato su server Samba o WindowsNT)
4. MSNT : Utilizza il protocollo di autentifica dei domini WindowsNT
5. PAM : Utlizza il protocollo PAM
6. getpwam : Ricorre all'autentifica per mezzo del file di password di sistema.

Si deve specificare il programma che si vuole utlizzare per l' autentificazione. Questo viene fatto per mezzo dell'opzione authenticate_program. Assicuratevi che il programma che andrete ad utlizzare sia installato e funzionante.

I cambi che verranno effettuati nel file di configurazione (squid.conf) dovrebbero ora rispecchiare lo stesso programma di autentificazione che abbiamo scelto (ad esempio authenticate_program /usr/local/bin/pam_auth)

acl pass proxy_auth REQUIRED
acl mynetwork src 192.168.0.1/255.255.255.0
http_access deny !mynetwork
http_access allow pass
http_access deny all

In questo caso un utente per accedere al servizio deve inserire il proprio username e password di sistema prima di poter accedere ad Internet.

Opzioni come authenticate_ttl e authenticate_ip_ttl posso anche esser utlizzate per variare il comportamento del processo di autentificazione, ovvero richiedendo all'utente di validare nuovamente le proprie credenziali.

# Riferimenti e Bibliografia

Questo articolo svela al lettore solo la punta dell'iceberg. Per maggiori informazioni e riferimenti vi consiglio di accedere a questi siti web *(le informazioni contenute sono, di norma, in lingua inglese)*


- Il sito di Squid, www.squid−cache.org
- Il progetto della documentazione inerente Squid, squid−docs.sourceforge.net
- visolve.com
- Sistemi di autentificazione per Proxy, home.iae.nl/users/devet/squid/proxy_auth


---




2005−01−10, generated by lfparser_pdf version 2.51