

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

Introduzione

Linux si presta egregiamente ad ospitare un servizio Proxy perché è un sistema operativo molto leggero e non ha bisogno di particolari requisiti grafici.

L'implementazione che seguiremo si basa sulla distribuzione Ubuntu server versione 12.4 LTS con già installato e configurato webmin per la gestione remota.

Si presume che apt e wget siano pure già configurati per poter utilizzare un eventuale server proxy interno.

(ev. Vedere Ab-mod300-linux server installazione di webmin.doc)

Di implementazioni di servizi proxy in ambiente Linux ce ne sono molte ma il servizio proxy più conosciuto è sicuramente SQUID.

Oltre che essere un servizio diffuso e leggero, attorno a SQUID sono stati sviluppati diversi prodotti per il monitoraggio ed il controllo del traffico che permettono di configurare molto semplicemente le black e le whitelist, il controllod egli accessi e le ACL necessarie.

Uno di questi prodotti è SQUID Guard.

Particolarità:

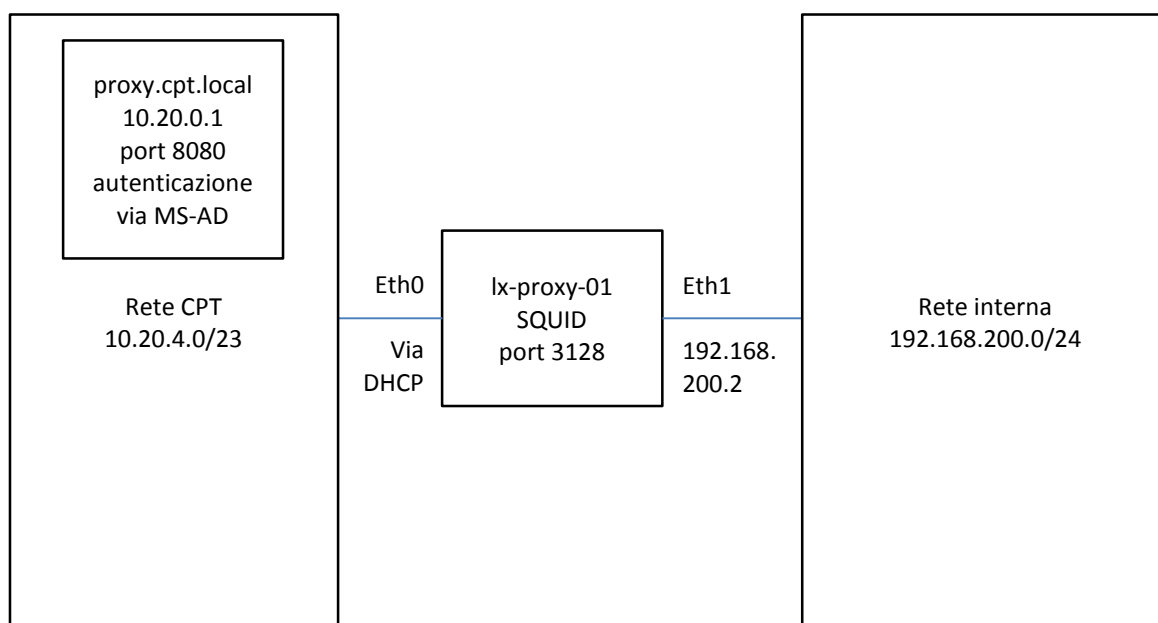
siccome il nostro proxy lavorerà dietro al proxy dell'istituto, bisognerà configurarlo come proxy "figlio" e prevedere il tipo di autenticazione presso il proxy "padre".

Questa parte non servirà se il proxy che si sta configurando è il solo all'interno della ditta e comunica direttamente con il router d'uscita.

Prerequisito per l'installazione di SQUID

- macchina fisica/virtuale con installato webmin
- due schede di rete, uno per la rete esterna, l'altra per la rete interna
- webmin, apt e wget configurati per l'uscita da un eventuale proxy di sede
- per questo esempio eth0 sarà la scheda esterna e eth1 la scheda interna

Schema di rete:



SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

Configurazione del server per squid:

Il server è configurato con due schede di rete:

- eth0, scheda esterna, indirizzo dinamico ricevuto dal dhcp della rete CPT
- eth1, scheda interna, indirizzo statico 192.168.200.2

Per questo, editare il file /etc/network/interfaces come segue:

```
Sudo nano /etc/network/interfaces
```

Configurandolo con i dati necessari:

```
#Scheda esterna, rete VL-104 del CPT
auto eth0
iface eth0 inet dhcp

#Scheda interna, rete 192.168.200/24
auto eth1
iface eth1 inet static
address 192.168.200.2
netmask 255.255.255.0
```

Attenzione!!

Sulla scheda interna non va mai configurato il gateway, pena problemi e collisioni sulla rete.

Riavviare in seguito il servizi di rete per le differenti schede:

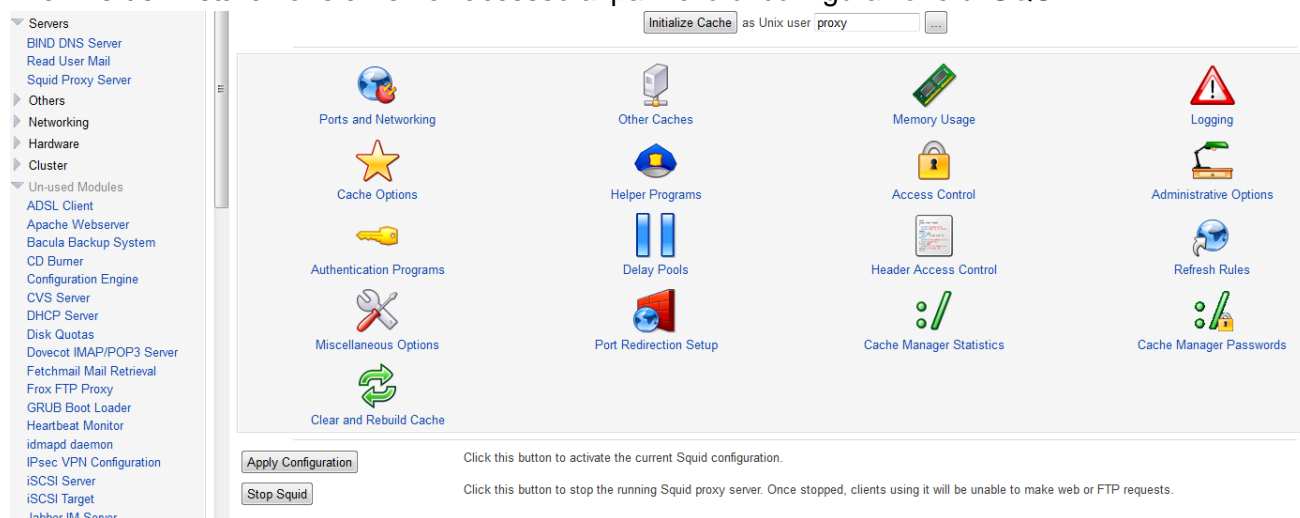
```
sudo ifdown eth0
sudo ifup eth0
sudo ifdown eth1
sudo ifup eth1
```

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

Installazione di SQUID:

- A partire da webmin, selezionare un-used Modules e quindi selezionare SQUID.
- Non essendo installato, webmin presenterà la pagina con l'avviso della possibilità di installazione.
- Scegliere l'installazione (apt deve essere correttamente configurato) ed il sistema scaricherà SQUID dai repository di Ubuntu e provvederà all'installazione.
- Ricaricare la pagina e la voce Squid server comparirà nel menu di sinistra sotto la voce servers.


Alla fine dell'installazione avremo l'accesso al pannello di configurazione di SQUID.



Ricordo sempre che webmin è solo un'interfaccia grafica che va a modificare i files di configurazione che si trovano nella cartella /etc del server che si sta amministrando. In questo caso /etc/squid3/squid.conf

Configurazione di squid:

Quando è installato SQUID ascolta su tutte le schede di rete alla porta di default 3128. Per sicurezza, si può limitare l'accesso alla parte amministrativa solo dalla rete interna. In questo caso bisognerà configurare SQUID come segue:



Ports and Networking

selezionare Ports and networking ed inserire l'indirizzo della scheda della rete interna. In questo modo SQUID ascolterà solo su quella scheda.

in seguito salvare ed aggiornare (Apply) i cambiamenti.

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

Se SQUID non è connesso direttamente ad un router ma si trova dietro ad un altro proxy che richiede l'autenticazione, seguire il prossimo punto.

Se invece SQUID si trova connesso direttamente ad un router, saltare il prossimo punto e continuare da 2).

1. Configurazione di SQUID dietro ad un proxy che richiede l'autenticazione. In questo caso, questo proxy sarà il proxy "figlio" (sun) mentre il proxy del CPT sarà il proxy padre (parent).

- a. Dal menu di SQUID, selezionare Other caches ed nella maschera successiva,

[Module Index](#)
[Help..](#)

No other caches defined.

[Add another cache.](#)

Cache Selection Options

Directly fetch URLs containing ICP query timeout ☒ Default ☐ ms

Dead peer timeout ☒ Default ☐ secs

No direct fetch ACLs defined
[Add ACLs to fetch directly.](#)

Other (selezionare Add another cache.

In seguito, nella maschera successiva, introdurre il nome del proxy per esteso del proxy parent, la sua porta d'ascolto e la porta per il protocollo di controllo ICMP. Di solito questa porta ha il medesimo valore di quella d'ascolto.

[Module Index](#) **Create Cache Host** [Apply Changes](#) [Stop Squid](#)

Cache Host Options

Hostname Type

Proxy port ICP port

Proxy only? ☐ Yes ☒ No

Default cache? ☐ Yes ☒ No

ICP time-to-live ☒ Default ☐

Closest only? ☐ Yes ☒ No

No NetDB exchange? ☐ Yes ☒ No

Login to proxy ☐ No login

☒ User: Pass:

☐ Pass on client authentication to this cache

Send ICP queries? ☒ Yes ☐ No

Round-robin cache? ☐ Yes ☒ No

Cache weighting ☒ Default ☐

No digest? ☐ Yes ☒ No

No delay? ☐ Yes ☒ No

Si tratta ora di decidere come trattare l'autenticazione richiesta dal proxy parent.

Ci sono due possibilità:

- i. User, autenticazione fissa:

Ogni richiesta proveniente dalla rete interna viene inoltrata da questo proxy che si autentica tramite un account conosciuto dal proxy parent.

In questo modo, i clients della rete interna non devono autenticarsi e tutto il traffico risulta originato dal medesimo account.

Può essere vantaggioso quando si installano o aggiornano applicazioni che non hanno la possibilità di autenticarsi.

Lo svantaggio è che presso il proxy parent, non vi è più la possibilità di controllare chi genera il traffico.

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

- ii. Pass on client authentication to this cache, autenticazione dinamica:
Questo proxy inoltra al proxy parent la richiesta mentre ritorna al client la richiesta di autenticazione.
In questo modo, ogni utente della rete interna deve autenticarsi ed il proxy esterno può svolgere il suo lavoro di monitoraggio.

- b. Una volta scelto il modo di autenticazione, salvare e aggiornare (Apply)
- c. Ora si tratta di indicare a questo proxy che tutto il traffico della rete interna lo deve inoltrare al proxy parent senza cercare di collegarsi direttamente.
Dal menu sottostante, scegliere **Add ACLs never to fetch directly**

Nella maschera successiva indicare che tutto il traffico deve essere inoltrato al proxy parent.

Potrebbe succedere che si voglia raggiungere un server che si trovi tra il nostro proxy ed il proxy parent. Potrebbe essere un web server interno.
In questo caso, bisognerà definire un ACL con il nome o l'indirizzo del web server ed indicare in questa maschera che le richieste verso questo non devono essere inoltrate verso il proxy parent ma gestite direttamente da questo proxy.
In tal caso si utilizzerà l'opzione **Add ACLs to fetch directly**.

In seguito, salvare e aggiornare (Apply) la nuova configurazione.

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

d. Definizione della liste di controllo d'accesso (ACL, Access Control Lists)

Dal menu di SQUID selezionare Access Control:

[Module Index](#)
[Help..](#)

Access Control

Access control lists			Proxy restrictions	ICP restrictions	External ACL programs	Reply proxy restrictions
Name	Type	Matching..				
manager	URL Protocol	cache_object				
localhost	Client Address	127.0.0.1/32 ::1				
to_localhost	Web Server Address	127.0.0.0/8 0.0.0.0/32 ::1				
SSL_ports	URL Port	443				
Safe_ports	URL Port	80				
Safe_ports	URL Port	21				
Safe_ports	URL Port	443				
Safe_ports	URL Port	70				
Safe_ports	URL Port	210				
Safe_ports	URL Port	1025-65535				
Safe_ports	URL Port	280				
Safe_ports	URL Port	488				
Safe_ports	URL Port	591				
Safe_ports	URL Port	777				
CONNECT	Request Method	CONNECT				
Rete_Bluesky	Client Address	192.168.200.0/24				
Create new ACL			Browser Regexp			

In queste scheda si possono definire delle voci corrispondenti ad indirizzi IP, porte, nomi di client, reti complete o sottoreti, orari ecc.

Questi verranno poi utilizzati nella tabella Proxy restrictions per definire le priorità ed i diritti.

Nel nostro caso, dovremo definire che l'accesso al proxy sia possibile solamente per i clients che si trovano sulla rete interna.

i. Dal pulldown selezionare il tipo di ACL, in questo caso "Client Address" e poi "Create new ACL"

localhost	Client Address	127.0.0.1/32 ::1
to_localhost	Browser Regexp	127.0.0.0/8 0.0.0.0/32 ::1
SSL_ports	Client Address	443
Safe_ports	Client Hostname	80
Safe_ports	Client Regexp	21
Safe_ports	Date and Time	443
Safe_ports	Dest AS Number	70
Safe_ports	Ethernet Address	210
Safe_ports	External Auth	1025-65535
Safe_ports	External Auth Regexp	280
Safe_ports	External Program	488
Safe_ports	Max User IP	591
Safe_ports	Maximum Connections	777
Safe_ports	Proxy IP Address	CONNECT
Safe_ports	Proxy Port	
Safe_ports	RFC931 User	
Safe_ports	RFC931 User Regexp	
Safe_ports	Reply MIME Type	
Safe_ports	Request MIME Type	
Safe_ports	Request Method	
Safe_ports	SNMP Community	
Create new ACL		
Browser Regexp		

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

- ii. Dare un nome a questa rete ed Inserirne poi i dati sotto forma di indirizzo di rete e maschera di rete.

[Module Index](#)

Create ACL

Client Address ACL

ACL Name:

From IP: To IP: Netmask:

Failure URL:

Store ACL values in file: ☒ Squid configuration ☐ Separate file

☐ Just use existing contents of file?

[Return to ACLs](#) | [Return to index](#)

Salvare ed aggiornare (Apply)

localhost	Client Address	127.0.0.1/32 ::1
to_localhost	Web Server Address	127.0.0.0/8 0.0.0.0/32 ::1
SSL_ports	URL Port	443
Safe_ports	URL Port	80
Safe_ports	URL Port	21
Safe_ports	URL Port	443
Safe_ports	URL Port	70
Safe_ports	URL Port	210
Safe_ports	URL Port	1025-65535
Safe_ports	URL Port	280
Safe_ports	URL Port	488
Safe_ports	URL Port	591
Safe_ports	URL Port	777
CONNECT	Request Method	CONNECT
Rete_Bluesky	Client Address	192.168.200.0/24

la nuova voce si troverà in fondo alla lista.

In questa scheda, la posizione di ogni singola voce non ha valenza.

Come abbiamo definito una rete, possiamo inserire anche un solo indirizzo oppure un pool d'indirizzi. Possiamo anche definire un periodo di tempo che servirà poi per bloccare o sbloccare il Proxy.

- iii. Uso delle ACL nella scheda Proxy restrictions

Questa scheda utilizza le voci definite della precedente per poter decidere se abilitarle (allow) al traffico o meno (deny).

[Help..](#)

[Access control lists](#) **Proxy restrictions** [ICP restrictions](#) [External ACL programs](#) [Reply proxy restrictions](#)

Add proxy restriction.

Action	ACLs	Move
<input type="checkbox"/> Allow	manager localhost	↓
<input type="checkbox"/> Deny	manager	↓↑
<input type="checkbox"/> Deny	!Safe_ports	↓↑
<input type="checkbox"/> Deny	CONNECT !SSL_ports	↓↑
<input type="checkbox"/> Allow	localhost	↓↑
<input type="checkbox"/> Deny	all	↑

Add proxy restriction.

il criterio di lettura è il seguente:

1. Sempre dall'alto al basso con una logica OR, la lettura si ferma alla prima condizione rispettata.

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria

2. In orizzontale, sulla medesima riga, con una logica OR
3. Importante!
l'ultima riga deve sempre indicare deny ALL. In questa maniera, se nessuna delle regole espresse nelle righe precedenti è stata onorata, tutto il traffico viene bloccato.

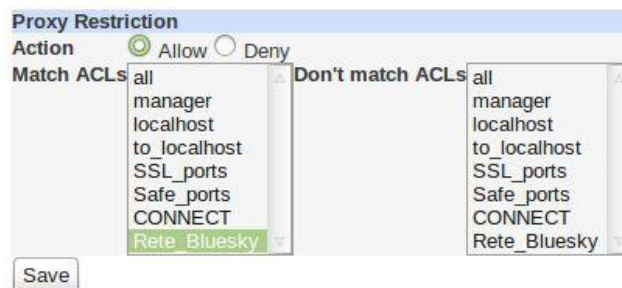
iv. Spiegazione inerente la definizione delle regole nella scheda Proxy restrictions:



1. Il traffico è permesso per l'utente "manager" solo se fa l'accesso da localhost.
2. Il traffico è bloccato per l'utente manager che fa l'accesso da qualsiasi altra parte
3. Il traffico è bloccato verso tutte le porte non sicure
Il traffico è bloccato per tutte le connessioni verso le porte non sicure
4. Il traffico è permesso da localhost
5. Il traffico è bloccato per tutti e tutto se le regole precedenti non sono state onorate.

v. Inserimento della nostra rete locale:

selezionare Add Proxy restriction e scegliere la voce Rete_Bluesky dal menu MATCH ACLs, l'altro menu Don't match ACLs corrisponde alla negazione. Selezionare Action Allow.



In seguito salvare.

Per sicurezza, le nuove voci vengono sempre accodate dopo Deny ALL.

In questo modo, se si dovesse inserire una regola sbagliata, non andrebbe a perturbare quelle esistenti.

SCUOLA D'ARTI E MESTIERI	Informatica modulo 300 Integrare in una rete servizi di più piattaforme	18 dicembre 2012
CLASSE 4	Installazione di un proxy server basato su Squid	Teoria



Ora, con le frecce destra, spostare in su la nuova voce fino alla posizione richiesta per rispettare la nuova regola.

In questo caso, subito prima di allow localhost.

Alla fine, salvare ed aggiornare (apply).

- e. Configurare il browser in modo che possa utilizzare il proxy.
Se un utente dovesse connettersi e ricevere un messaggio di tipo "Access denied" controllare che l'utente abbia i diritti di farlo e che le regole siano impostate correttamente.

Il proxy configurato in questo modo non è un router e tratterà solamente il traffico di tipo http:
Per permettere ad un DNS esterno di fare delle richieste ad un DNS esterno alla nostra rete, vi sono due possibilità:

- Aggiungere il servizio di routing al server, configurando IPSEC
- Installare un server DNS (BIND9) al solo scopo di inoltrare le richieste ricevute dall'interno verso l'esterno. In questo caso, l'unica configurazione necessaria su Bind 9 è l'indicazione di Forwarding,