

بسمه حق

## معرفی و تنظیم squid

گرد آوری و تهیه: یاشار اسمعیل دخت

نام در انجمنها: royaflash

|

نام در سایتهای اجتماعی: royaflash

|

این مقاله رو تقدیم میکنم به جامعه اپن سورس امیدوارم این کار من گامی کوچک برای پیشرفت مملکتمون باشه

همچنین بنده یک گروه در زمینه لینوکس ایجاد کردم به نام

royaflash-linux خوشحال میشم که شما هم در این گروه باشید.

هرگونه نظر، انتقاد، و پیشنهاد رو میتونید به ایمیل بنده به آدرس

[royaflash@yahoo.com](mailto:royaflash@yahoo.com)

ارسال کنید

[گرفتن مطالب دیگر](#)

[ملحق شدن به گروه royaflash-linux](#)

[ملحق شدن به گروه لینوکس کاران تبریز](#)

با آرزوی موفقیت برای شما .

## SQUID

Squid یک شی در اینترنت است که به عنوان پراکسی سرور برای HTTP,FTP و دیگر تقاضاها عمل می کند

### Proxy Server

نوعی فایروال که ترافیک اینترنت ورودی به خروجی از یک شبکه را مدیریت می کند و ویژگیهای دیگری چون کش کردن سندها و کنترل دستیابی را فراهم می کند. این سرویس دهنده می تواند با تامین داده های پر مصرف مثلا یک صفحه وب مشهور، سبب افزایش کارایی می شود. همچنین می تواند درخواستهایی چون دستیابی به فایل های اختصاصی را که نامناسب به شمار می آیند را فیلتر کند و یا نادیده بگیرد

### Proxy

کامپیوتری که با ارائه تنها یک نشانی شبکه به سایت های خارجی ، همانند یک سد در بین یک شبکه و اینترنت عمل می کند. این کامپیوتر همچون میانجی عمل می نماید و نماینگر تمام کامپیوتر های داخلی است، در عین حالی که دستیابی به اینترنت را فراهم می کند، از موجودیت های شبکه نیز حفاظت می کند  
squid به صورت پیشفرض از شماره پورت 3128 استفاده میکند  
به منظور روشن کردن سرویس squid از فرمان روبرو استفاده می کنیم

```
[root@localhost /]#chkconfig
```

```
squid on
```

فایل پیکربندی squid در /etc/squid/squid.conf قرار دارد

### (ACL)(Access Control Lists

acl یا فهرست کنترل دستیابی ، فهرستی مرتبط با فایل حاوی اطلاعات مربوط به کاربران یا گروه هایی که مجوز دستیابی یا عدم دسترسی را دارند گفته می شود  
acl می تواند زمان ، روز و یا شبکه را به اطلاع squid در جهت اجازه و یا عدم دسترسی به http برساند

در این مثال به محدود کردن دسترسی کاربران در ساعت خاص می پردازیم

فرمانها را در قسمت acl اضافه مي كنيم

```
[root@localhost /]#vi
```

```
/etc/squid/squid.conf
```

```
acl pooya acl
```

```
192.168.10.0/255.255.255.0
```

```
acl mornings time 08:00-12:00
```

اکنون فرمان هاي ذیل را در قسمت بالايي http-access در جهت اجازه به کاربران وارد مي كنيم

```
http-access permit pooya or http-access permit
```

```
192.168.10.0
```

```
http-access allow mornings
```

مثلا اگر بخواهيم کاربر خاص 192.168.10.100 اجازه دسترسي به اينترنت را نداشته باشد بايد فرمان ذیل را وارد كنيم

```
http-access deny
```

```
192.168.10.100
```

میتوانیم محدودیت در دستيابي به وب سايت هاي خاصي را اعمال كنيم. به منظور وارد كردن نام سايت هايي كه قابل دسترسي مي توانند باشند از مسير روبرو استفاده مي كنيم

```
[root@localhost /]#usr/local/etc/allowed-  
sites.squid  
www.yahoo.com
```

به منظور عدم دسترسي به سايت هاي مورد نظر از مسير روبرو استفاده مي كنيم

```
[root@localhost /]#usr/local/restricted-  
sites.squid  
www.xyz.com
```

اکنون باید فرمان هاي ذیل را در قسمت acl وارد کنیم

```
[root@localhost /]#vi /etc/squid/squid.conf  
acl Good sites dstdomain "/usr/local/etc/allowed-  
sites.squid"  
acl Bad sites dstdomain "/usr/local/etc/resticted-  
sited.squid"
```

فرمان هاي روبرو در قسمت http-access را وارد مي كنيم

```
http-access deny Bad sites  
http-access allow pooya morning Good sites
```

---

نظيم لينوکس و Squid جهت يک پراکسي وب

## :: مقدمه

یک پراکسی سرور یک سرویس کارآمد جهت شبکه شما یا شبکه شما و اینترنت است که امنیت بالاتری را جهت کاربران اینترنت فراهم می کند و هم چنین می تواند بعنوان یک کش سرور هم استفاده شود که باعث بالا رفتن بازدهی سرور شما و سرعت آن در دسترسی به اینترنت می شود.

Squid خود یک پراکسی سرور ایمن با توانایی بسیار بالا است که قابلیت استفاده بعنوان کش سرور را نیز داراست و یکی از کاربردی ترین کش سرورها در شبکه اینترنت است . اطلاعاتی بیشتر در مورد این کش سرور از طریق سایت <http://www.squid-cache.org> قابل دریافت است .

## :: نصب لینوکس

قبل از نصب Squid نیاز دارید تا سیستم عامل لینوکس را بر روی سیستم در نظر گرفته شده برای آن نصب نمایید. بهترین راه جهت نصب لینوکس استفاده از نمونه های مختلف در دسترس است که **ردهت** و **دبیان** از مشهورترین آنهاست که راحتی از طریق اینترنت قابل دریافت هستند.

## :: نصب Squid

- نصب از طریق بسته های نرم افزاری

توجه داشته باشید که معمولاً بیشتر نسخه های لینوکس دارای یک بسته Squid به صورت آماده و قابل نصب هستند که ممکن است در موقعی که نسخه لینوکس شما نصب می شود نصب نگردد . بعنوان مثال بعد از نصب ردهت 7.1 شما متوجه می شوید که Squid نصب نگردیده است . خود Squid در CD #2 در فولدر RedHat/RPMS قرار گرفته است . جهت نصب آن ابتدا اطمینان حاصل نمایید که شما بعنوان کاربر ریشه وارد شده اید سپس از فرمان rpm به صورت زیر استفاده کنید:

```
mount /mnt/cdrom
```

```
rpm -Uhv /mnt/cdrom/RedHat/RPMS/squid-*.rpm
```

```
umount /mnt/cdrom
```

شما در هنگام نصب تعداد زیادی از هش (#) را مشاهده می کنید که نشان از نصب Squid دارد . در لینوکس دبیان شما می توانید از برنامه apt-get جهت دان لود و نصب Squid از اینترنت اقدام نمایید:

```
apt-get install squid
```

- نصب از طریق کد منبع

اگر شما مایل به نصب Squid از طریق فایل های کد منبع آن هستید، می توانید این کار را در تمامی نسخه های لینوکس انجام دهید. یادآور می شوم که شما نیاز دارید تا جدیدترین نسخه پایدار [Squid](#) را از وب سایت آن دریافت نمایید. سورس Squid به صورت فایل فشرده شده tar است که شما احتیاج دارید ابتدا آن را غیر فشرده نمایید :

```
Tar -zxf squid-2.3.STABLE4-src.tar.gz
```

هنگامی که شما فایل فشرده tar را غیر فشرده نمودید شما از این طریق احتیاج به تنظیم، کامپایل و نصب Squid دارید:

```
cd squid-2.3.STABLE4
```

```
./configure
```

```
make all
```

```
make install
```

جهت اطلاعات بیشتر جهت نصب آن فایل INSTALL را که در کد منبع Squid موجود است را مطالعه نمایید. البته به یاد داشته باشید که همیشه آسان ترین راه برای نصب Squid استفاده از بسته های نرم افزاری آماده آن است.

**:: تنظیم Squid**

همه تنظیمات این پراکسی سرور در فایل پیکربندی آن است ( squid.conf ) که بستگی به نسخه لینوکس شما ممکن است در پوشه /etc/squid/ یا /etc/squid/squid.conf باشد . قبل از انجام هرکاری شما باید مسیر این فایل را در سیستم تان پیدا کنید:

```
locate squid.conf
```

روش های متعددی جهت تنظیم Squid از طریق وب یا GUI ( اینترفیس کاربری گرافیکی ) وجود دارد . این GUI ها توانایی خواندن و تشخیص و نوشتن فایل پیکربندی در محل مربوطه را دارا هستند .

خوب ما در اینجا تنظیم نمودن Squid را به صورت دستی شرح می دهیم . جهت این کار شما یک ویرایش گر متن مانند emacs یا دیگر نرم افزار ها احتیاج دارید و اینکه فراموش نکنید جهت انجام فرامین مربوطه شما باید بصورت کاربر ریشه وارد سیستم شوید تا دسترسی به نوشتن در فایل پیکربندی را داشته باشید.

فایل پیکربندی Squid خود دارای پارامترهای تنظیماتی بسیاری است که ما در اینجا همه آن ها را پوشش نخواهیم داد و به اصلی ترین آن ها اشاره خواهیم نمود.

### :: تنظیمات پیش فرض

به صورت پیش فرض Squid همراه با یک فایل پیکربندی است که تقریباً جهت بیشتر سرورها صحیح و قابل استفاده است. جهت استفاده از Squid در شبکه بعنوان یک پراکسی باید برخی از تنظیمات پیش گزیده را تغییر داد.

### :: شروع تنظیمات مقدماتی

هنگام تنظیم Squid در فایل پیکربندی آن ( squid.conf ) تعداد زیادی توضیح وجود دارد که قابل استفاده هستند. در این حالت حجم فایل در حدود 76 کیلو بایت است که در صورت حذف این توضیحات حجم آن به 600 بایت کاهش می یابد! که در این صورت ویرایش آن از طریق ویرایش گر ها آسان تر خواهد شد. البته وجود این توضیحات می تواند کمک بزرگی برای تنظیم کننده باشد.

جهت تنظیمات مقدماتی در فایل پیکربندی این پارامترها را اضافه می کنیم :

```
acl privatenet src 192.168.0.0/255.255.0.0
```

```
http_access allow privatenet
```

```
cache_effective_user squid
```

```
cache_effective_group squid
```

نکته های قابل ذکر در این پارامترها:

• acl privatenet \* . برای مثال دو شبکه خصوصی در پشت فایروال وجود دارد که از IANA در شماره های 192.168.x.x به آن اختصاص داده شده است.

:: نمونه های تنظیمات فایل پیکربندی

دقت داشته باشید که تنظیمات اشاره شده در اینجا تنها بخش کوچکی از آن چه که شما می خواهید با پراکسی سرور Squid انجام دهید را شامل می شود .

- ثبت وقایع (logging)

به طور پیش فرض Squid فعالیت های انجام شده را در چندین Log فایل ذخیره می کند :

```
cache_access_log /var/log/squid/access.log
```

```
cache_log /var/log/squid/cache.log
```

```
cache_store_log none
```

با اضافه نمودن این پارامترها Squid پیغام های خطا را در مسیر `/var/log/squid/cache.log` و پیغام های دسترسی به سرور را در `/var/log/squid/access.log` ذخیره می کند که البته برنامه هایی نیز جهت آنالیز `access.log` قابل دریافت هستند که از آن ها می توان به [SARG](#) اشاره نمود ( که با نام `sqmgrlog` شهرت دارد ).

من چیز مفیدی را در مورد `squid's cache_store_log` پیدا نکردم که از همین جهت می توان توسط خط 3 بالا آن را غیر فعال نمود .

- Cache Access

شما می توانید استفاده از کش را در سرورتان مقدور سازید که این کار از طریق `http_access` امکان پذیر است . این را مد نظر داشته باشید که خط `acl` یک شبکه یا یک ابزار شبکه را تعریف می کند.

### :: اندکی در مورد Upstream Proxy

شاید یکی از برتری های Squid استفاده از Upstream Proxy باشد که می تواند سرعت دسترسی به اینترنت تا حد قابل ملاحظه ای بالا ببرد. بعنوان مثال وقتی ISP شما دارای کش جهت کاربران می باشد کش سرور شما می تواند سایت های بسیاری را در خود ذخیره کند که این خود تا حد زیادی بازدهی را در مواقع ضروری بالا می برد.

یکی دیگر از مزایای Squid پشتیبانی به صورت چندگانه است بدین مفهوم که می توان چندین کش سرور را با ارتباط داد که Squid این کار را از طریق پروتکول ICP انجام می دهد . ICP این اجازه را به کش سرورها می دهد که که طریق پکت های سریع UDP یا هم ارتباط برقرار نمایند .

خوب جهت استفاده از این مزایا شما اول باید مد نظر داشته باشید که آدرس کش سرور ها چیست )

Upstream Proxy از استفاده می کند . استفاده از proxyserver.yourisp.com ) و هم چنین از چه پورتی بدین منظور استفاده می کند .  
به راحتی امکان پذیر است :

```
cache_peer proxy.yourisp.com parent 3128 3130  
prefer_direct off
```

خط cache\_peer اسم هاستینگ و نوع کشینگ "parent" و پورت پراکسی "3128" و پورت "ICP" 3130 را مشخص می کند . اگر کش سرور شما پروتکل ICP را پشتیبانی نمی کند از این خط استفاده نمایید :

```
cache_peer proxy.yourisp.com parent 3128 7 no-query default  
prefer_direct off
```

#### - Sharing Caches

توجه داشته باشید که در مواقع ضروری که یک شرکت چندین ارتباط را جهت دسترسی به اینترنت را داشته باشد Squid کش نمودن سرور ها در حالت اشتراک گذاری آن ها می پذیرد ( بدین مفهوم که چندین کش سرور با هم ارتباط داشته باشند ). در این صورت باید هر کش سرور این خط را در فایل پیکربندی خود داشته باشند :

```
cache_peer theotherproxy.yournetwork.com sibling 3128 3130
```

که اگر دقت نمایید یکی از پارامترها به sibling تغییر یافته بدین مفهوم که فایل های کش را چنانچه در کش سرور دیگر باشد آن ها را آن ها دریافت می کند .

- رد نمودن فایل های آلوده

فایل هایی وجود دارند که به ویروس نیز آلوده هستند مانند WIN-BUGFIX.EXE که مربوط به ویروس Melissa می شد که با یک پارامتر ساده می توان دریافت چنین فایل هایی را از سرور رد نمود .

```
acl nastyfile dstdom_regex -i WIN[.*]BUG[.*]EXE  
http_access deny nastyfile
```

:: تنظیمات پیشرفته

ترنغد هایی نیز وجود دارند که شما می توانید جهت وب پراکسی خود اعمال نمایید مانند شناسایی کاربر و یا

پراکسی ترانسپرنت و یا عدم دسترسی کاربر به فایل های غیر مجاز در طی ساعات اداری . اما این را فراموش نکنید که فایل پیکربندی Squid بسیار آسیب پذیر است و با یک تنظیم ناصحیح کوچک کش سرور کار نمی کند!

- احراز هویت کاربران

این مرحله یکی از مهم ترین اجزا جهت مدیران شبکه است بعنوان مثال مواقعی که شرکت شما دسترسی به اینترنت را جهت کاربر امکان پذیر و یا رد می کند .

تنظیم نمودن یک acl جهت ورود یا رد نمودن کاربر به راحتی از طریق تغییر زیر در فایل پیکربندی امکان پذیر است :

```
authenticate_program /your/authentication/program
```

```
acl validusers proxy_auth REQUIRED
```

```
http_access allow validusers
```

و این را توجه داشته باشید که یک برنامه مناسب شناساگر پراکسی پیدا نمایید ( proxy authentication ) که قابل ذکر است Squid خود دارای شناساگری به صورت داخلی نمی باشد که شما باید در خط authenticate\_program تنظیمات مناسب را بر طبق برنامه احراز هویت مورد استفاده، تغییر دهید.

البته Squid همراه با چند برنامه احراز هویت نیز ارائه شده است که در مسیر /usr/lib/squid/ موجود هستند که شامل smb\_auth ( شناساگر جهت دومین NT ) و squid\_ldap\_auth ( جهت شناسایی دایرکتوری LDAP ) که در این میان شناساگر مورد انتخاب من pam\_auth می باشد که از لایبرری های PAM جهت شناسایی کاربران استفاده می کند.

برتری pam\_auth در شناسایی کاربران در روش های متعدد است و همه برنامه های شما ( نظیر XDM, Squid, Apache و .... ) بر روی آن قرار دارند ...

جهت تنظیم pam\_auth ( این روش جهت سیستم های ردهت است ):

- فایل /etc/pam.d/squid را ایجاد نمایید که باید این چنین باشد :

```
auth required /lib/security/pam_stack.so service=system-auth
```

```
auth required /lib/security/pam_nologin.so
```

```
account required /lib/security/pam_stack.so service=system-auth
```

```
password required /lib/security/pam_stack.so service=system-auth
session required /lib/security/pam_stack.so service=system-auth
```

- اطمینان حاصل نمایید که خط زیر را در فایل پیکربندی Squid گذارده اید:

```
authenticate_program /usr/lib/squid/pam_auth
```

- و اینکه authconfig در سرور شما اجرا شده است تا مشخص نماید شما از چه سرور شناساگر استفاده می نمایید که مورد LDAP مناسب به نظر می رسد ...

:: پراکسی به صورت ترانسپرننت

ترانسپرننت نمودن پراکسی یک روش است که شما می توانید که یک پراکسی سرور را بین شبکه و اینترنت بگذارید و بدون اینکه نیاز به تنظیمات خاصی باشد ما مستقیماً به اینترنت وصل خواهیم شد ( توجه داشته باشید که این روش فقط برای پروتکل WWW قابل اجراست ولی جهت سرویس FTP قابل استفاده نمی باشد. ) همچنین باید توجه داشته باشید که ترانسپرننت نمودن پراکسی و اضافه نمودن احراز هویت که در مرحله قبل توضیح داده شد هر دو با هم امکان پذیر نیست.

جهت نصب پراکسی به صورت ترانسپرننت شما به این موارد نیاز خواهید داشت :

- یک قانون فایروال ( Rule ) و Redirect نمودن ترافیک خروجی شبکه به پراکسی سرور .

- یک قانون Squid جهت فعال کردن Squid تا اینکه به صورت ترانسپرننت عمل نماید .

جهت اجرای یک قانون فایروال شما به قانونی نظیر زیر احتیاج خواهید داشت :

```
/sbin/ipchains -A input -p tcp -s 0/0 -d 0/0 80 -j REDIRECT 3128
```

جهت iptables ( هسته 2.4 لینوکس 2.4 به بالا ) ممکن است شما مایل به نصب iptables مبنی بر فایروال در Squid باشید . در قسمتی از نصب فایروال شما به ایجاد قانون DNAT جهت ارسال ترافیک بر روی پورت 80 به 3128 پراکسی سرور خواهید داشت . برای اطلاعات بیشتر جهت ایجاد قانون های NAT می توانید به وب سایت [NET FILTER](#) مراجعه کنید .

تنظیمات مورد نیاز Squid جهت فعال کردن Squid به صورت ترانسپرننت در اینجا ذکر شده اند :

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

### کنترل مصرف پهنای باند شبکه با استفاده از squid

یکی از مشکلاتی که معمولاً بر روی شبکه‌های داخلی وجود دارد، مصرف پهنای باند توسط کاربران خاص و عدم پخش مناسب آن بر روی کل شبکه است. به طوری که یک کاربر می‌تواند کل پهنای باند شبکه را مصرف کرده و سایر کاربران را دچار مشکل کند.

راه‌های متعددی برای کنترل مصرف پهنای باند مانند ابزارهای Traffic Shaper و... شبکه وجود دارد که از حوصله این مقاله خارج است. ما در این مقاله کوچک سعی داریم تا نحوه کنترل مصرف پهنای باند را توسط سرویس دهنده squid آموزش دهیم.

### قدم اول

فرض می‌کنیم که یک اتصال مودم یا DSL به شبکه اینترنت داریم که رابط آن ppp0 بوده، رابط شبکه محلی نیز eth0 و آدرس شبکه داخلی 192.168.0.0/24 می‌باشد. مواردی که برای پیاده‌سازی کنترل مصرف پهنای باند شبکه نیاز داریم عبارتند از یک سرویس دهنده squid و سیستم iptables که بر روی هر ماشین گنو/لینوکس وجود دارد. مراحل نصب، پیکربندی و تنظیم بسیار ساده است.

### Squid چگونه کار می‌کند؟

سرویس دهنده Squid پیشرفته‌ترین سرویس دهنده پراکسی موجود برای سیستم‌عامل گنو/لینوکس می‌باشد. این سرویس دهنده به دو روش می‌تواند در پهنای باند صرفه جویی نماید:

۱) نخست از طریق حفظ صفحات، تصاویر و سایر اقلام دریافت شده بر روی حافظه یا فضای دیسک. بنابراین در صورتی که کاربران تقاضای دریافت مجدد یک صفحه تکراری را نمایند، این صفحه از روی اینترنت دریافت نخواهد شد.

۲) در کنار سیستم Caching معمولی، Squid دارای قابلیت‌هایی به نام delay pools است که از طریق آن می‌توانید ترافیک اینترنت را بطور معقولانه‌ای کنترل نمایید. این کار از طریق تعریف کلمات کلیدی موجود در آدرس‌های URL انجام می‌گیرد. برای مثال می‌توانید کلماتی مانند mp3، mpg، exe و... را بعنوان کلمات کلیدی تعریف نمایید. با استفاده از این کلمات کلیدی، می‌توانیم به Squid بگوییم تا آنها را حداکثر با سرعت خاصی دریافت نماید. می‌توان پهنای باند باقیمانده را برای سرویس‌های دیگر مانند مرور وب، پست الکترونیکی و... باقی گذاشت و یا حتی آنرا نیز محدود کرد.

### نصب و پیکربندی ابزارهای لازم

در این بخش به بررسی چگونگی نصب و پیکربندی ابزارهای لازم می‌پردازیم. مهمترین نکته در این بخش، فعال بودن ویژگی Delay Pools در Squid می‌باشد. در صورتی که Squid را از طریق کامپایل نصب کرده‌اید، حتما بررسی کنید که به همراه گزینه --enable-delay-pools کامپایل شده باشد، در غیر اینصورت باید آنرا مجدداً کامپایل کنید. معمولاً بسته‌هایی که به همراه توزیع‌ها ارائه می‌شود، دارای چنین ویژگی به صورت پیش‌گزیده می‌باشد. با فرض اینکه از توزیع دبیان استفاده می‌کنید، Squid را نصب می‌کنیم:

#### # apt-get install squid

سرویس‌دهنده Squid از روی مخازن مربوطه دریافت و نصب خواهد شد. در قدم دوم، باید این سرویس‌دهنده را برای مقاصد خودمان تنظیم کنیم. به همراه تنظیم Delay Pools، سرویس‌دهنده برای ارائه سرویس Transparent Proxy نیز تنظیم خواهد شد. فایل پیکربندی مورد استفاده در Squid به شکل زیر خواهد بود:

```
#SQUID PORT

http_port 8080

hierarchy_stoplist cgi-bin ?

acl QUERY urlpath_regex cgi-bin \?

no_cache deny QUERY

cache_mem 16 MB
```

```
maximum_object_size 4096 KB
maximum_object_size_in_memory 10 KB

#CACHE DIR CONFIG
cache_dir ufs /var/spool/squid 512 16 512

#LOGS
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log

hosts_file /etc/hosts

refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8

# OUR LOCAL LAN
acl local src 192.168.0.0/255.255.255.0

acl SSL_ports port 443 563
acl SSL_ports port 873
acl Safe_ports port 80 21 443 563 70 210 631 901 1025-65535
acl purge method PURGE
acl CONNECT method CONNECT

http_access allow manager localhost local
http_access deny manager
http_access allow purge localhost
```

```
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_reply_access allow all

#HOSTNAME
visible_hostname power

#TRANSPARENT PROXY
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on

store_avg_object_size 50 KB

coredump_dir /var/spool/squid

#DELAY POOLS
acl magic_words1 url_regex -i 192.168
acl magic_words2 url_regex -i ftp .exe .mp3 .vqf .rpm .zip .tar.gz .gz .rar .avi .mpeg
.mpe .mpg .qt .ram .rm .iso .raw .wav .mov .swf
acl day time 08:00-23:59

delay_pools 2

delay_class 1 2
delay_parameters 1 4500/40000 4500/40000
delay_access 1 allow magic_words1

delay_class 2 2
delay_parameters 2 4500/40000 4500/40000
delay_access 2 allow day
```

```
delay_access 2 deny !day
```

```
delay_access 2 allow magic_words2
```

این فایل پیکربندی در آدرس `/etc/squid/squid.conf` قرار می‌گیرد. مهمترین بخش این فایل برای کنترل ترافیک، بخش مشخص شده با `DELAY POOLS` است.

در خط نخست این بخش یک `acl` برای شبکه داخلی تعریف شده و در خط دوم انواع فایل‌هایی که مایل به محدود کردن دریافت آنها هستیم، مشخص شده است.

در خط سوم، ساعات کاری که محدودیت‌ها در آن اعمال می‌شوند مشخص شده و در خط بعدی، دو `Delay Pool` مختلف تعریف شده است.

خط `delay_class` مشخص کننده نوع کلاس `pool` بکار رفته می‌باشد. سه نوع کلاس `delay pool` وجود دارد که برای اطلاع دقیق از آنها می‌توانید به مستندات سرویس‌دهنده `Squid` مراجعه نمایید.

خط `delay_parameters 1` مشخص کننده محدودیت‌های اعمالی برای شبکه داخلی است. در این خط مشخص شده که در صورتی که کل شبکه یا یک آدرس `IP` خاص مقدار حجم دریافتی معادل ۴۰ مگابایت داشت، از آن پس، سرعت دریافت آن به ۴/۵ کیلوبایت در ثانیه کاهش یابد. در صورتی که مایلید تا محدودیت برای مرور صفحات وجود نداشته باشد و در هنگام مرور صفحات، همیشه حداکثر سرعت در اختیار باشد، این خط را به صورت زیر تغییر دهید:

```
delay_parameters 1 -1/-1 -1/-1
```

عدد منفی یک مشخص کننده عدم وجود محدودیت است. همانطور که در مثال بالا می‌بینید، محدودیت ساعت در خطوط تنظیم کننده مربوط به `delay_parameters 2` اعمال شده است. توجه داشته باشید که اعدادی فایل پیکربندی فوق تماماً مثال بوده و آنها را باید بنا به شرایط شبکه خودتان تنظیم کنید.

پس از اعمال تنظیمات فوق، سرویس‌دهنده `Squid` را راه‌اندازی می‌کنیم:

```
squid -z #
```

```
etc/init.d/squid start/ #
```

در مرحله بعدی تنظیم و پیکربندی، باید اشتراک اینترنت و تنظیمات `iptables` را برای `transparent proxy` انجام دهیم. برای این کار می‌توان از یک اسکریپت ساده مانند زیر استفاده کرد:

```
#!/bin/sh
```

```
IPTABLES=/sbin/iptables
```

```
$IPTABLES -F
```

```
$IPTABLES -t nat -A PREROUTING -i lan1 -p tcp --dport 80 -j REDIRECT --to-port 8080
```

```
$IPTABLES -A POSTROUTING -t nat -o ppp0 -j MASQUERADE
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
echo Starting Internet Connection Sharing...
```

کافی است این اسکریپت را در شاخه `/etc/init.d` با نامی مانند `ics` ذخیره کرده و آنرا با `chmod +x` اجرایی کنید. سپس برای اینکه در هنگام بوت اجرا شود، از دستور زیر استفاده نمایید:

```
# ln -s /etc/init.d/ics /etc/rc2.d/S99ics
```

از این پس هنگام بوت سیستم (سطح اجرایی ۲ در دبیان) اسکریپت `ics` اجرا خواهد شد و می‌توانید ببینید که تنظیمات کنترلی به خوبی کار می‌کنند. برای اطلاعات دقیق‌تر در مورد چگونگی اعمال محدودیت‌های ترافیکی با استفاده از Traffic shaper می‌توانید به [این آدرس](#) مراجعه کنید.

---

This is a collection of example Squid Configurations intended to demonstrate the flexibility of Squid.

**Warning:** Any example presented here is provided "as-is" with no support or guarantee of suitability. If you have any further questions about these examples please email the squid-users mailing list.

Contents

1. [Online Manuals](#)

2. [Current configuration examples](#)
  1. [Authentication](#)
  2. [Interception](#)
  3. [Reverse Proxy \(Acceleration\)](#)
  4. [Instant Messaging / Chat Program filtering](#)
  5. [Multimedia and Data Stream filtering](#)
  6. [General](#)
  7. [Strange and Weird configurations](#)
3. [External configuration examples](#)
4. [Create new configuration example](#)

## **Online Manuals**

We now provide an the Authoritative Configuration Manual for each version of squid. These manuals are built daily and directly from the squid source code to provide the most up to date information on squid options.

For Squid-2.6 the Manual is at <http://www.squid-cache.org/Versions/v2/2.6/cfgman/>

For Squid-2.7 the Manual is at <http://www.squid-cache.org/Versions/v2/2.7/cfgman/>

For Squid-3.0 the Manual is at <http://www.squid-cache.org/Versions/v3/3.0/cfgman/>

For Squid-3.1 the Manual is at <http://www.squid-cache.org/Versions/v3/3.1/cfgman/>

A combined Squid Manual can be found at <http://www.squid-cache.org/Doc/config/> with details on each option supported in Squid, and what differences can be encountered between major Squid releases.

## **Current configuration examples**

### **Authentication**

## Overview and explanation

1. [ConfigExamples/Authenticate/Bypass](#)
2. [ConfigExamples/Authenticate/Kerberos](#)
3. [ConfigExamples/Authenticate/Ldap](#)
4. [ConfigExamples/Authenticate/LoggingOnly](#)
5. [ConfigExamples/Authenticate/MultipleSources](#)
6. [ConfigExamples/Authenticate/Mysql](#)
7. [ConfigExamples/Authenticate/Ntlm](#)
8. [ConfigExamples/Authenticate/NtlmCentOS5](#)
9. [ConfigExamples/Authenticate/NtlmWithGroups](#)
10. [ConfigExamples/Authenticate/Radius](#)
11. [ConfigExamples/Authenticate/WindowsActiveDirectory](#)

## **Interception**

### Overview and explanation

#### WCCP v1 overview

#### WCCP v2 overview

1. [ConfigExamples/Intercept/AtSource](#)
2. [ConfigExamples/Intercept/CentOsTproxy4](#)
3. [ConfigExamples/Intercept/Cisco2501PolicyRoute](#)
4. [ConfigExamples/Intercept/Cisco3640Wccp2](#)
5. [ConfigExamples/Intercept/CiscoAsaWccp2](#)
6. [ConfigExamples/Intercept/CiscoIOSv11Wccp1](#)
7. [ConfigExamples/Intercept/CiscoIOSv12Wccp1](#)
8. [ConfigExamples/Intercept/CiscoIos1246T2Wccp2](#)
9. [ConfigExamples/Intercept/CiscoPixWccp2](#)
10. [ConfigExamples/Intercept/FedoraCoreWccp2Receiver](#)
11. [ConfigExamples/Intercept/FreeBsdIpfw](#)

12. [ConfigExamples/Intercept/FreeBsdWccp2Receiver](#)
13. [ConfigExamples/Intercept/IptablesPolicyRoute](#)
14. [ConfigExamples/Intercept/LinuxDnat](#)
15. [ConfigExamples/Intercept/LinuxIpfwadm](#)
16. [ConfigExamples/Intercept/LinuxLocalhost](#)
17. [ConfigExamples/Intercept/LinuxRedirect](#)
18. [ConfigExamples/Intercept/OpenBsdPf](#)

### **Reverse Proxy (Acceleration)**

1. [ConfigExamples/Reverse/BasicAccelerator](#)
2. [ConfigExamples/Reverse/ExchangeRpc](#)
3. [ConfigExamples/Reverse/MultipleWebservers](#)
4. [ConfigExamples/Reverse/OutlookWebAccess](#)
5. [ConfigExamples/Reverse/SslWithWildcardCertificate](#)
6. [ConfigExamples/Reverse/VirtualHosting](#)

### **Instant Messaging / Chat Program filtering**

#### Overview and explanation

1. [ConfigExamples/Chat/Aim](#)
2. [ConfigExamples/Chat/Aol](#)
3. [ConfigExamples/Chat/Gizmo](#)
4. [ConfigExamples/Chat/Icq](#)
5. [ConfigExamples/Chat/MsnMessenger](#)
6. [ConfigExamples/Chat/Skype](#)
7. [ConfigExamples/Chat/Trillian](#)
8. [ConfigExamples/Chat/YahooMessenger](#)

### **Multimedia and Data Stream filtering**

1. [ConfigExamples/Streams/Other](#)
2. [ConfigExamples/Streams/RealAudio](#)
3. [ConfigExamples/Streams/YouTube](#)

## **General**

1. [ConfigExamples/BlockingMimeType](#)
2. [ConfigExamples/ChrootJail](#)
3. [ConfigExamples/DynamicContent](#)
4. [ConfigExamples/DynamicContent/YouTube](#)
5. [ConfigExamples/DynamicContent/YouTube/Discussion](#)
6. [ConfigExamples/FullyTransparentWithTPROXY](#)
7. [ConfigExamples/MultiCpuSystem](#)
8. [ConfigExamples/MultiplePortsWithWccp2](#)
9. [ConfigExamples/NatAndWccp2](#)
10. [ConfigExamples/PhpRedirectors](#)
11. [ConfigExamples/SquidAndWccp2](#)
12. [ConfigExamples/Wccp2AndNat](#)
13. [ConfigExamples/Webwasher](#)

## **Strange and Weird configurations**

This is a section for weird (and sometimes wonderful) configurations Squid is capable of. Clued in admin often find no actual useful benefits from going to this much trouble, but well, people seems to occasionally ask for them...

1. [ConfigExamples/Strange/RotatingIPs](#)

## **External configuration examples**

\* <http://freshmeat.net/articles/view/1433/> - Configuring a Transparent Proxy/Webcache in a Bridge

using Squid and ebttables (Jan 1st, 2005)

### **Create new configuration example**

Choose a good [WikiName](#) for your new example and enter it here: