واحد آموزش مرکز تحقیقاتی فناوری اطلاعات و ارتباطات پیشرفته دانشگاه صنعتی شریف
تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
E-mail: edu@aictc.ir ۶۶۰۸۶۰۱۹ - ۰۲۱

نصب و پیکربندی سرویس‌دهنده Squid

منبع مقاله: www.irantux.org

نویسنده مقاله: ایرج هدایتی

تاریخ ویرایش: ۳۰/۸/۸۸

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
E-mail: edu@aictc.ir ۶۶۰۸۶۰۱۹ - ۰۲۱

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 اولین برنامه Proxy-Cache با کارآیی بالا بود که به عنوان بخشی از پروژه ی Harvest توسعه داده شد. Squid راحتی نصب می شود و فایل پیکربندی پیش فرض آن برای نود درصد نصب ها درست است و نیازی نیست فایل را تغییر دهید و بهتر است بعضی انتخاب‌ها مثل قوانین نوسازی را تا زمانی که تجربه ی کافی به دست نیاورده‌اید، تغییر ندهید. در این مقاله بر روی انتخاب های پایه ی squidکار خواهیم کرد. در حقیقت در این مقاله انتخاب هایی را که در ده درصد ماشین های دیگر تغییر می کند، معرفی می‌کنیم.

نصب از طریق Pack

جهت نصب Squid ابتدا اطمینان حاصل نمایید که شما بعنوان root وارد شده اید. سپس از فرمان rpm به صورت زیر استفاده کنید:

```
#rpm –ivh /mnt/cdrom/RedHat/RPMS/squid-*.rpm
```

شما در هنگام نصب تعداد زیادی از هش (#) را مشاهده می کنید که نشان از نصب squid دارد. برای نصب Squid در توزیع دبیان و توزیع های مبتنی بر آن می‌توانید از دستور apt-get install squid استفاده نمایید.

نصب از طریق کد منبع

اگر شما مایل به نصب squid ز طریق فایل های source هستید، می‌توانید این کار را جهت همه نسخه‌های لینوکس انجام دهید. یادآور شوم که شما احتیاج به دریافت جدیدترین سورس پایدار squid از وب سایت آن هستید .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 و نصب Squid به صورت زیر دارید:

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
E-mail: edu@aictc.ir ۶۶۰۸۶۰۱۹ - ۰۲۱

#cd squid-2.3.STABLE4

 # ./configure
 # make all
 # make install

ی کسب اطلاعات بیشتر جهت نصب آن فایل INSTALL را که در سورس کد موجود است را می توانید مورد بررسی قرار دهید.

تنظیم نمودن Squid

، تنظیمات این پراکسی سرور در فایل پیکربندی آن است (squid.conf) که بستگی به نسخه لینوکس شما ممکن است در مسیر/usr/local/squid/etc/squid.conf یا /etc/squid.conf یا /etc/squid/squid.conf باشد. بل از انجام هرکاری شما باید مسیر این فایل را در سیستم تان پیدا نمایید:

#updatedb

 # locate squid.conf

فایل پیکربندی Squid ود دارای صد و بیست وپنج برچسب جهت انجام تنظیمات است که ما در اینجا همه آن ها را پوشش نخواهیم داد و به اصلی ترین آن ها اشاره خواهیم نمود.

شروع تنظیمات مقدماتی

در فایل پیکربندی squid.conf داد زیادی توضیح وجود دارد که قابل استفاده هستند که در این حالت حجم فایل در حدود ۷۶ کیلو بایت است که در صورت حذف این توضیحات حجم آن به ۶۰۰ بایت کاهش می یابد! که در این صورت ویرایش آن از طریق ویرایش گرها آسان تر خواهد شد.

تعیین درگاه squid

در این مرحله آدرس درگاهی را که squid آن به درخواست های سرویس‌گیرنده‌ها گوش می دهد را مشخص می کنیم:

http_port 3128

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ ۶۶۰۸۶۰۱۹ - ۰۲۱
(داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱ E-mail: edu@aictc.ir

در صورتی که squid cache ما به عنوان web server نیز عمل کند، شماره درگاه را ۸۰ قرار می دهیم.

همچنین می توان از چند درگاه برای این کار استفاده کرد:

```
http_port 80 3128
```

تنظیم محل ذخیره**object** های **Cache** شده:

```
cache_dir aufs /var/spool/squid/ 100 16 256
```

پارامتر اول نوع سیستم فابل جهت دایرکتوری ذخیرهobject ها را تعیین می کند. نوع قدیمی تر آن ufs می باشد. پارامتر دوم مسیر ذخیره داده‌ها را مشخص می‌کند. پارامتر سوم حجم داده بر روی دیسک بر حسب (مگابایت) را مشخص می کند. ترهای چهارم و پنجم تعداد زیر شاخه ها (اولین و دومین رده) برا ایجاد در این شاخه را مشخص می‌کنند. ین کار جستجو برای یافتن یک object را راحتتر می کند .

رای استفاده از دو هارد دیسک جهت ایجاد کارآیی بهتر و دسترسی سریعتر به صورت زیر عمل می کنیم:

```
cache_dir /var/spool/squid/ 100 16 256
cache_dir /mnt/hdb2 100 16 256
```

/mnt/hdb2نقطه اتصال هارد دیسک دوم است.

ID قابل اجرای گروه و کاربر:

Squid اگر به عنوان root روع شود، تنها می تواند به پورت های شماره پایین (مثل پورت ۸۰) بچسبد. در ضمن از لحاظ امنیتی هم صحیح نیست که پروسه ی به عنوان root در حال اجرا باشد. Squid به محض چسبیدن به پورت شبکه ID های گروه و کاربر را تغیر می دهد. این ID ها را به صورت زیر مشخص می کنیم:

```
cache_effective_user squid
cache_effective_group squid
```

e-mailبرای مدیر**cache**

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
۰۲۱ - ۶۶۰۸۶۰۱۹
E-mail: edu@aictc.ir

اگر Squid از کار بیفتد، یک e-mail به آدرس مشخص شده با برچسب cache_mgr ارسال می شود. همچنین آدرس به انتهای صفحه های خطایی که به کاربران ارسال می‌شود، اضافه می شود. (به حتم با این صفحات در ضمن کار با اینترنت در منزلتان برخورد کرده اید.)

cache_mgr i-support@mail.vru.ac.ir

اطلاعات FTP login

FTP جهت انتقال فایل های تصدیق شده (فایل هایی که احتیاج به نام کاربر و کلمه عبور دارند) نوشته شده است. برای دسترسی عمومی، یک حساب کاربر مخصوص به نام کاربر anonymouse ساخته شده است. وقتی که شما به یک سرور FTP می شوید، از آن به عنوان نام کاربری خود استفاده می کنید. عنوان کلمه ی عبور هم از آدرس email خود استفاده کنید. Squid به شما اجازه می دهد که آدرس e-mail که به این منظور استفاده می شود را به وسیله ی برچسب ftp_user تنظیم کنید:

frp_user squid@yourdomain.example

کنترل دسترسی و عملگرهای کنترل دسترسی:

access contro list یاACL جهت کنترل دسترسی به Cache مورد استفاده قرار می گیرد. در کنترل دسترسی دو عنصر وجود دارد: کلاس ها و عملگرها.

کلاس ها: یک کلاس معمولا به مجموعه ای از کاربرها ارجاع داده می‌شود.

عملگرها: برای مجموعه ای از acl ها برای ICP و HTTP عمل می کند. بنی شما می توانید مجموعه های مختلفی از پروتکل های مختلف داشته باشید. برای هر پروتکل یک acl_operator متفاوت وجود دارد. به عنوان مثال برچسب های icp_access و http_access و snmp_access.

acl name type (string|"filename") [string2][string3]["filename2"

Name-تعریف شده باید در فایل unique باشد.

String- می تواند یک رشته از IPها باشد:

acl mynet src 10.0.0.0/255.0.0.0

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
E-mail: edu@aictc.ir ۶۶۰۸۶۰۱۹ - ۰۲۱

-اگر دو string را پشت سر هم بیاوریم آنها را با or جدا می کنیم:

acl mynet src 10.0.0.0/255.0.0.0 10.1.0.0/255.255.0.0

-اگر String ها بسیا زرگ باشند آنها را در یک فایل ذخیره کرده و سپس نام فایل را به جای String می آوریم.

acl mynets src "/etc/squid/mynets"

در زیر انواع مشهور ACL که کاربرد فراوانی دارند تشریح می کینم:

۱. source/destination IP address

طابق آدرس های IP ر محدوده ی تعریف شده که کلمات کلیدی src ی آدرس های مبدا و src رای مقصد استفاده می شوند:

acl mynet dst--------/--------

acl mynet dst -------/--------

اینکه به جای ذکر فرمت استاندارد ماسک شبکه از فرمت غیر استاندارد، یعنی ذکر تعداد یک ها، استفاده کنید.

مثال:

acl mynet src 192.168.10.0/24

2.source/destination Domain address

ی محدودیت دامنه ها به کار می رود. کلمات کلیدی srcdomain برای دامنه های مبدا و dstdomain برای دامنه های مقصد استفاده می شود. مثال:

acl mydomain srcdomain .qualica.com .squid.cache.org

نکته: برای مسدود کردن یک سایت باید هم domain و هم آدرس IP آن را مسدود کنید.

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
E-mail: edu@aictc.ir ۶۶۰۸۶۰۱۹ - ۰۲۱

۳. regular expression match of requested domain

این نوع از ACL برای مسدود کردن سایت هایی که حاوی کلمات خاصی است، استفاده می شود. البته این دستور case sensitive است و برای گریز از آن باید از پارامتر-i استفاده کنید. مثال:

```
acl badurl url_regex –i sxx
```

همچنین نوع دیگری به نام urlpath_regex وجود دارد که فقط مسیر و نام فایل را چک می‌کند.

۴. current day/time

اجازه دسترسی در زمان خاص(روز-ساعت)

```
acl name time [day-list][start_hour:start_minute-end_hour:end_minute[
```

که روزهای هفته به صورت زیر است:

```
S(Sunday), M, T, W, H, F, A(Saturday(
```

مثال:

```
acl night time 17:00-24:00
acl week time SA
```

5. Destination port

تعریف مجموعه ای از پورت ها که قرار است به آنها دسترسی داشته باشید یا نداشته باشید.مثلا اگر بخواهیم دسترسی را فقط برای مجموعه خاصی از پورت ها تعریف کنیم به صورت زیر عمل می کنیم. مثال:

```
acl safe_port port 80 21 443 70 210 1025-65535
http_access deny !safe_port
```

6. protocol

برای مسدود کردن پروتکل ها با استفاده از پیشوند های سایت مثل http:// یا frp:// برای مثال:

```
acl ftp proto FTP
```

7. method

برای مسدود کردن methodها. مانند GET و POST. مثال:

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
۰۲۱ - ۶۶۰۸۶۰۱۹
E-mail: edu@aictc.ir

```
acl post_class method POST
```

سایر ACL_OPERATOR هایی که در فایل squid.conf مورد استفاده قرار می گیرند:

no_cache - برای جلوگیری از cache کردن موارد خاص.

miss_access - اگر بخواهیم یک سری اطلاعات داخل cache را غیر قابل دسترس کنیم.

مثالی از یک مجموعه acl و acl_operator:

```
acl nimda urlpath_regex –i \.eml
acl nimda2 urlpath_regex -i root.exe
acl localhost src 127.0.0.1/36
acl all src 0.0.0.0/0.0.0.0
http_access deny nimda
http_access deny nimda2
http_access allow localhost
http_access deny all
```

Logging -

به طور پیش فرض Squid فعالیت های انجام شده را در چندین فایل ذخیره می‌کند:

```
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 نام های خطا را در مسیر var/log/squid/cache.log/ پیغام های دسترسی به سرور را در var/log/squid/access.log/ ذخیره می‌کند که البته برنامه هایی نیز جهت آنالیز access.logقابل دریافت هستند که از آنها می توان به قابل دریافت هستند که از آن ها می توان به اشاره نمود. (که با نام sqmgrlog شهرت دارد). برای مشاهده ی نحوه گزارشگیری Squid از دستور tail استفاده می کنیم. دستور tail محتویات یک فایل گزارش را بر روی صفحه نمایش چاپ می کند.

#tail /var/log/squid/access.log

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
۶۶۰۸۶۰۱۹ - ۰۲۱ E-mail: edu@aictc.ir

برای انکه دستور tail را مجبور کنیداین عمل را به طور پیوسته انجام دهد از سوییچ F– استفاده کنید.

اندکی در مورد upstream Proxy

شاید یکی از برتری های Squid استفاده از upstream Proxy باشد که می تواند دسترسی به اینترنت تا حد قابل ملاحظه ای بالا ببرد. بعنوان مثال وقتی ISP شما دارای کش جهت کاربرانش می باشد کش سرور شما می تواند سایت ی 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 هم ارتباط داد که Squid این کار را از طریق پروتکول ICP انجام می دهد. ICP این اجازه را به کش سرورها می دهد که از طریق پکت های سریع UDP با هم ارتباط برقرار نمایند. خوب جهت استفاده از این مزایا شما اول باید مد نظر داشته باشید که آدرس کش سرور ها چیست (proxyserver.yourisp.com) و هم چنین از چه پورتی بدین منظور استفاده می کند . استفاده از upstream Proxy 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 ۳۱۳۰ "ICP"را مشخص می کند. اگر کش سرور شما پروتکل ICP را پشتیبانی نمیکند. از این خط استفاده نمایید:

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

Sharing Caches -

وجه داشته باشید که در مواقع ضروری که یک شرکت چندین ارتباط جهت دسترسی به اینترنت داشته باشد، Squid ش نمودن سرور ها در حالت اشتراک گذاری آن ها می‌پذیرد (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 باشد:

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

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

تهران، خیابان آزادی، بلوار شهید اکبری، خیابان شهید قاسمی (ضلع شمالی دانشگاه شریف) کوچه گلستان، پلاک ۹
تلفن: (مستقیم) ۶۶۰۳۵۱۲۵ - ۰۲۱ (داخلی ۱۲۴) ۶۶۱۶۵۱۶۹-۷۲ - ۰۲۱
E-mail: edu@aictc.ir ۶۶۰۸۶۰۱۹ - ۰۲۱

پراکسی به صورت ترانسپرنت

ترانسپرنت نمودن پراکسی یک روش است که شما می‌توانید که یک پراکسی سرور را بین شبکه و اینترنت بگذارید و بدون اینکه نیاز به تنظیمات خاصی باشد ما مستقیما به اینرنت وصل خواهیم گردید جهت نصب پراکسی به صورت ترانسپرنت شما به این چیزها احتیاج 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 ترانسپرنت عمل نماید.

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

```
#iptables –t nat –A PREROUTING –d 207.216.150.1 –p tcp –m tcp –dport 80 –j ACCEPT
# iptables –t nat –A PREROUTING –p tcp –m tcp –dport 80 –j REDIRECT –-to-ports 3128
```

تنظیمات مورد احتیاج Squid جهت فعال کردن Squid به صورت ترانسپرنت در اینجا ذکر شده اند:

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

راه اندازی Squid:

همانطور که اشاره شد هیچ مسیر پیش فرضی جهت دخیره داده ها برای Squid وجود ندارد و مسیر آن را قبلا در فایل squid.conf تعیین کرده ایم. اشیا download ده در شاخه های swap به صورت سلسه مراتبی ذخیره می‌شوند. برای ساخت شاخه های swap به صورت دستی از دستور زیر استفاده می کنیم:

```
#squid –z
```

راه اندازی پراسس squid با دستور زیر انجام می شود:

```
#squid –D –d 1
```

پارامتر 1 –d ی گزارش عملیات انجام شده مورد استفاده قرار می گیرد. حال می توانید از دستور tail برای تست کردن عملیات انجام شده استفاده کنید.