



SQUID

A rendszergazda álma a felhasználók megregulázására ...öööö,
vagyis dehogy, hanem az Internet elérés biztosítása szeretett
felhasználóink részére. :)

Mi is ez, mire való és mire nem?

Proxy Cache:

- proxy -> kliens kérését továbbítja de adatot nem tárol /lehet transzparens vagy nem átlátszó/
- cache -> időlegesen tárol

Squid tudja mindkettőt, bár transzparens módban a user-t nem.

HTTP alapú proxy: a proxy-val HTTP-n kommunikálunk ez kötött!
(pl. ftp kliensnél HTTP-proxyt használjon /squid letölti ftp protokollal,
majd kliensnek odaadja http-vel/)

Célok:

- * elsődleges cél: http/https/ftp hozzáférés, szabályozás és cache
- * biztonság megteremtésére mint olyan, NEM alkalmas

...hogy miiii???

Nem bug, hanem feature!

Más protokollokat is tud közvetíteni: HTTP proxy protokoll: CONNECT összeköt a céllal, így lehet pl HTTPS-t átvinni. Na ezért nem alkalmas biztonságra! Connect method engedve gáz! Nem engedve nincs https! ...egészséges döntetlen. :)
...ezért van engedve csak safe protokra. ..persze hiába, hiszen rakhatok oda is egy ssh szerveret, utána meg úgy forwardolom a portokat, ahogy akarom.

A Squid, mint olyan beállításairól

- * Tegyük külön partícióra/meghajtóra a cache könyvtárat és használjunk 'noatime' opciót.
- * Ha lehet, tartsuk alacsonyan a diszk foglaltságát és használjunk olyan fájlrendszert, amely inkább a kis fájlok kezelésében hatékony. (Naplózó fájlrendszerek esetén a napló akár ki is kapcsolható.)
- * Nagyobb forgalom esetén több diszkre érdemes szétosztani a forgalmat. Squid esetén több 'cache_dir'-t is megadhatunk és a partíciók között a beállított terület függvényében osztja szét a forgalmat, tehát nincs szükség RAID0 támogatásra.
- * A cache által használható memória beállítására (cache_mem) érdemes a Squid-nek szánt memóriaterület harmadát megadni. Ugyanis a szoftver bizonyos esetekben (és ez főleg csúcsidőben fordul elő) jóval túllépheti a megadott mértéket.
- * A naplófile-okat érdemes külön partícióra, diszkre tenni. A naplózás mértékét csökkenteni lehet, és akár ki is kapcsolhatjuk, ha egyáltalán nincs szükségünk rá.

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

```
http_port 10.0.0.1:8080
```

```
cache_mem 32 MB
```

```
maximum_object_size 120000 KB
```

```
cache_dir diskd /var/spool/squid 14000 256 256
```

**Milyen IP-n és porton válaszoljon a proxy.
3128 a szabványos „squid port”,
de 8080 a proxy általában.**

**Mennyi memóriát használhasson. (x3, de
inkább x5)**

**Mekkora méretű objektumokat
tárol. (max)**

**Hol legyen a cache
könyvtár?
Mekkora legyen Mb?
Könyvtárak és az azon
belüli
könyvtárak száma.**

ACL: Access Control List

Majdhogynem itt a lényege a dolognak.

ACL hozzáférés vezérlési listák:

Feltételekhez szabunk dolgokat, hova megy a kérés, honnan jön a kérés, mikor stb
acl -> nem vezérel, hanem definiál!!! ...amit aztán majd később alkalmazok

pl: acl all src 0.0.0.0

alc | név(egyedi) | típus | paraméter

Jelen esetben minden olyan kérés, ami a megadott címről érkezik (minden)

ACL lehet:

dst -> cél

dst_domain -> név szerinti

url_regex -i -> szabályos kifejezéssel url

urlpath_regex -> gépnév utáni részt nézi csak

....stb...

Példák:

Minden olyan forrás IP, aminek az értéke bármely IP. :)

```
acl all src 0.0.0.0/0.0.0.0
```

„helyi” ACL értéke azon forrás IP címek, melyek a 10.0.0.0 hálózatban vannak.

```
acl helyi src 10.0.0.0/255.0.0.0
```

```
acl kiterjesztesek url_regex -i \.mp3$ \.vqf$ \.avi$ \.mpeg$ \.mpe$ \.mpg$ \.qt$ \.ram$ \.rm$ \.raw$ \.wav$ \.mov$ \.wmv$ \.vma$ \.divx$ \.asf$ \.au$ \.asx$
```

**„kiterjesztések” értéke azon reguláris kifejezésekkel egyenlő, melyek illeszkednek arra a mintára, ami fel van sorolva. A hivatkozások végére illeszti a mintákat.
(pl: www.lok.hu/akarmi/video.avi)**

```
acl webserver dst www.bercsenyi-bp.sulinet.hu
```

„webserver” azon cél domain, ami fel van sorolva.

```
acl kitiltott dstdomain .honfoglalo.hu .mellesleg.hu
```

„kitiltott” azon cél domének, amik fel vannak sorolva

```
acl engedett_user proxy_auth username muszashi eszter edit gyuri  
bumara
```

„engedett_user” azon felhasználói nevek, amik fel vannak sorolva.

```
acl szabalyzott src "/etc/squid/szabalyok"
```

„szabalyozott” azon forrás IP-k, melyek a megadott fájlban vannak.

```
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl SSL_ports port 443 563      # https, snews
```

„SSL_ports” értéke a 443 és az 563-as port

```
acl SSL_ports port 873          # rsync
```

HOPP! Ha acl ismétlés, akkor összeadódnak az értékek!!!!

```
acl ido time SMTWHFA 07:30-14:05
```

„ido” értéke idő. A hét minden napján a 7:30-14:05 intervallumra illik. (napok angolul)

Ha minden ACL-t definiáltunk, utána jönnek a szabályok, azaz, hogy mit kezdünk az ACL-ekkel!

Feldolgozás kérése a beírás sorrendjében történik. Ha talál egyezést az már nem megy tovább a láncon.

http_access deny all -> végére vágjuk oda!

```
# Deny requests to unknown ports
http_access deny !Safe_ports
```

Tiltjuk a hozzáférést, kivéve a Safe_port -ban felsorolt portokat.

```
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports !egroup_ports
```

Tiltjuk a „Connect” acl értékének megfelelő értékeket, kivéve ha az egyezik az SSL_ports vagy az egroup_ports értékével.

```
http_access allow localhost
```

Mindent engedek, ami „localhost”-ban van.

```
http_access allow kiterjesztesek engedett_user
```

engedem a „kiterjesztések” acl-t a megengedett felhasználóknak. (engedett_user)

http_access allow localhost

Mindent engedek, ami „localhost”-ban van.

Deny requests to unknown ports
http_access deny !Safe_ports

Tiltjuk a hozzáférést, kivéve a Safe_port -ban felsorolt portokat.

Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports !egroup_ports

Tiltjuk a „Connect” acl értékének megfelelő értékeket, kivéve ha az egyezik az SSL_ports vagy az egroup_ports értékével.

http_access allow kiterjesztesek engedett_user

**engedem a „kiterjesztések” acl-t a megengedett felhasználóknak.
(engedett_user)**

http_access deny szabalyzott

**Tiltom a
„szabalyozott”-ban
szereplő értékeket.**

http_access deny kiterjesztesek ido

**„kiterjesztesek”-ben
szereplő értékekre egyező
értékek tiltva, „ido” acl-ben
szereplő ideig.**

http_access allow ido2

Teljes konfig állomány a prezentáció végén.

További „extra” lehetőségek gondolatébresztőnek

Magyar nyelvű hibaüzenetek:

error_directory /usr/share/squid/errors/Hungarian

Személyre szabott hibaüzenetek:

deny_info HIBAUZENET szabalyzott

Sávszélesség szabályzás:

delay_pool -> lásd konfigurációs állomány

„Gyermekzár”:

redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

redirect_children 4

Internet elérés vezérlése webes vagy e-mailes formában.

nálunk e-mail van

...ha marad idő... tantermek elérésének korlátozása

- * DHCP segítségével a diák gépek statikus IP-ket kapnak, minden terem egy külön IP tartomány
- * Tanarak számára (4 fő) .mailfilter állomány és egy jelszó állomány a saját könyvtárban. (.mailfilterből a levél alapján paraméteresen meghívunk egy parancsállományt)
- * A parancsállomány, amely legenerálja a paraméterek alapján az aktuális „szabalyok”-at, naplózik és reloadolja a szerveret

Használat:

Saját e-mail címről a saját címre kell küldeni egy levelet, melynek tárgya „internet_ne_legyen_jelszó” vagy „internet_legyen_jelszó”, tartalma pedig a terem száma. (200,201,202,203,215)

A kért URL nem tölthető le! ...miért is? TANÁRI TILTÁS MIATT!

TANULJÁL, DOLGOZZÁL, A FELADATODAT CSINÁLD, NE A NETET AKARD NÉZEGETNI, MERT MEGBUX!!!!

Az alábbi URL letöltésekor: [%U](#)

a következő hiba lépett fel:

- **Hozzáférés megtagadva, tanári tiltás miatt!**

A hozzáférési konfigurációban beállítottak alapján kérését nem tudjuk teljesíteni. Kérjük, forduljon tanárához amennyiben a szerver helytelen beállításában látja a hiba okát. ...de hiába, hahahaha :)

Köszönöm a figyelmet!

Rózsár Gábor
gabor.rozsar@lok.hu

Felhasznált irodalom:

<http://www.szabilinux.hu/squid2/index.htm>

|

<http://www.szabilinux.hu/squid/index.html>

**Melléklet:
egy működő konfiguráció állomány:**

```
cat /etc/squid/squid.conf
http_port 10.0.0.1:8080
cache_mem 32 MB
maximum_object_size 120000 KB
cache_dir diskd /var/spool/squid 14000 256 256
diskd_program /usr/lib/squid/diskd

auth_param basic program /usr/lib/squid/pam_auth
```

#Suggested default:

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

```
acl password proxy_auth REQUIRED
```

```
acl all src 0.0.0.0/0.0.0.0
```

```
acl helyi src 10.0.0.0/255.0.0.0
```

```
acl mobilgepek src 10.0.2.100-10.0.2.110/255.0.0.0
```

```
acl intra dst 10.0.0.0/255.0.0.0
```

```
acl kiterjesztesek url_regex -i \.mp3$ \.vqf$ \.avi$ \.mpeg$ \.mpe$ \.mpg$ \.qt$ \.ram$  
\.rm$ \.raw$ \.wav$ \.mov$ \.wmv$ \.vma$ \.divx$ \.asf$ \.au$ \.asx$
```

```
acl webszerver dst www.bercsenyi-bp.sulinet.hu
```

```
acl windowsupdate dstdomain .microsoft.com .windowsupdate.com
```

```
acl kitiltott dstdomain "/etc/squid/kitiltott"
```

```
acl ezmehet dstdomain "/etc/squid/ezmehet"
```

```
acl korlatozott dstdomain "/etc/squid/korlatozott"
```

```
acl engedett_user proxy_auth username "/etc/squid/engedettuser"
```

```
acl manager proto cache_object
```

```
acl szabalyzott src "/etc/squid/szabalyok"
```

```
acl vipgepek src "/etc/squid/vipgepek"
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl to_localhost dst 127.0.0.0/8
```

```
acl SSL_ports port 443 563 # https, snews
acl egroup_ports port 4443
acl SSL_ports port 873      # rsync
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl Safe_ports port 631     # cups
acl Safe_ports port 873     # rsync
acl Safe_ports port 901     # SWAT
acl ido time SMTWHFA 07:30-14:05
acl ido2 time SMTWHFA 11:50-13:00
acl maxkapcsolat maxconn 5
acl purge method PURGE
acl CONNECT method CONNECT
```

```
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Only allow purge requests from localhost
http_access allow purge localhost
http_access deny purge
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports !egroup_ports
#http_access deny to_localhost
http_access allow localhost
```

```
delay_pools 3
delay_class 1 3
delay_class 2 3
delay_class 3 3
```

```
delay_parameters 1 300000/330000 400000/430000 90000/140000
delay_parameters 2 50000/70000 50000/70000 5000/7000
delay_parameters 3 200000/230000 100000/130000 10000/13000
```

```
delay_access 1 allow vipgepek
delay_access 1 deny all
delay_access 2 allow mobilgepek
delay_access 2 deny all
delay_access 3 allow helyi
delay_access 3 deny all
```

http_access deny korlatozott maxkapcsolat
http_access deny szabalyzott
http_access deny ido kitiltott
http_access allow ezmehet helyi
http_access allow intra helyi
http_access allow kiterjesztesek engedett_user helyi
http_access deny ido kiterjesztesek
http_access allow windowsupdate helyi
http_access allow password helyi
redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
redirect_children 4
http_access deny all
http_reply_access allow all
icp_access allow all
error_directory /usr/share/squid/errors/Hungarian
deny_info HIBAUZENET szabalyzott
deny_info HIBAUZENET2 kitiltott
deny_info HIBAUZENET2 kiterjesztesek
deny_info HIBAUZENET3 maxkapcsolat

cat kitiltott
.mellesleg.hu
.vivatv.hu
.chat.hu
.csajozas.hu
.habostorta.hu
.diszkoka.hu
.clubdream.hu

cat ezmehet
.sdt.sulinet.hu

cat vipgepek
10.0.0.160
10.0.0.161
10.0.0.162
10.0.0.163
10.0.0.164
10.0.0.165
10.0.0.166
10.0.0.167
10.0.0.168
10.0.0.169
10.0.0.60
10.0.0.30
10.0.0.90
10.0.0.120
10.0.0.2

cat korlatozott
myvip.com
#iwiw.hu
#wiw.hu