

Squid.conf configuration

```
#      WELCOME TO SQUID 2.6.STABLE4      Fedora core 8
#      -----
#
http_port 8080
icp_port 3130
# htcp_port 4827
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
cache_mem 300 MB
# cache_swap_low 90
# cache_swap_high 95
# maximum_object_size 4096 KB
# minimum_object_size 0 KB
# maximum_object_size_in_memory 8 KB
# ipcache_size 1024
# ipcache_low 90
# ipcache_high 95
# fqdn_cache_size 1024
cache_dir ufs /cache/squid 3000 64 128
logformat common {%Y-%b-
%d %H:%M:%S %z}t1 %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log common
#access_log /var/log/squid/access.log squid
# cache_log /var/log/squid/cache.log
# cache_store_log /var/log/squid/store.log
acl time_url url_regex -i clock.thaicert.org www.nod32upd.do.am/v3/*.*
U21.eset.com/eset_upd/update.ver
http_access allow time_url
#===== Program
Authentication=====
auth_param basic program /usr/lib64/squid/ncsa_auth /etc/shadow
auth_param basic children 5
auth_param basic realm ICT Center NSTA1
auth_param basic credentialsttl 1 minute
auth_param basic casesensitive off
#=====Authentication=====
==
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
acl SSL_ports port 443 563
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 8443
acl CONNECT method CONNECT
acl lan src 192.168.1.0/255.255.255.0
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
#http_access deny CONNECT !SSL_ports
# ===== block MSN MP3 =====
acl MSN req_mime_type ^application/x-msn-messenger$
http_access deny MSN
acl chatMSN rep_mime_type -i ^application/x-msn-messenger$
http_reply_access deny chatMSN
acl download urlpath_regex -i \.mp4$ \.wav$ \.iso$
http_access deny download
#acl block_url url_regex 'usr/local/etc/blacklists'
#http_access deny block_url
acl keyword url_regex -i messenger hi5 chat
http_access deny keyword
#=====skype=====
=====
#acl skype_user src "/etc/squid/user-skype"
acl skype_user src 192.168.1.0/255.255.255.0
acl numeric_IPs url_regex ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+:443
acl Skype_UA browser ^skype^
acl Skype_domain dstdomain skype.com
acl connect method CONNECT
http_access deny skype_user numeric_IPs
http_reply_access deny skype_user numeric_IPs
http_access deny skype_user Skype_UA
http_access deny Skype_domain
http_access deny connect numeric_IPs all
#===== ACL
Authentication=====
acl password proxy_auth REQUIRED
http_access allow password all
#=====Authentication=====
==
acl our_networks src 192.168.1.0/24
http_access allow our_networks
acl Safe_ports port 123
http_access allow localhost
http_access allow lan
http_access deny all
http_reply_access allow all
icp_access allow all
cache_effective_user squid
cache_effective_group squid
coredump_dir /var/spool/squid
visible_hostname nsta1.net

```

การ Block Squid.conf

1. การจำกัดเวลาลูกข่ายใช้อินเตอร์เน็ต

```
acl acl_net src 172.17.8.0/24 // วงที่ออกเน็ตได้
acl acl_client src 172.17.8.10 // IP ที่ต้องการห้ามออกเน็ตเป็นเวลา
acl acl_time time MTWHF 17:00-23:59
acl acl_time2 time MTWHF 0:00-7:00
http_access deny acl_client acl_time
http_access deny acl_client acl_time2
http_access allow acl_net
(M จันทร์ T อังคาร W พุธ H พฤหัส F ศุกร์ A เสาร์ S อาทิตย์)
```

2. การบล็อก MSN

คำตอบ ให้เพิ่ม เข้าไปใน squid.conf ส่วนของ ACCESS CONTROL

```
acl chatMSN req_mime_type -i ^application/x-msn-messenger$
http_reply_access deny chatMSN
```

```
acl msn1 req_mime_type -i ^application/x-msn-messenger$ //รุ่น 6.3
acl msn2 url_regex -i gateway.dll // รุ่น 7.X +
```

```
http_access deny msn1
http_access deny msn2
```

หรือถ้าต้องการblock เป็นเวลา สามารถกำหนดดังนี้

```
acl msn1 rep_mime_type -i ^application/x-msn-messenger$
acl msn2 url_regex -i gateway.dll
acl morning time M T W H F 9:00-12:00
acl lunch time M T W H F 13:00-17:00
```

```
http_access deny msn1 morning
```

```
http_access deny msn1 lunch
```

```
http_access deny msn2 morning
```

```
http_access deny msn2 lunch
```

3. Block site (Domain)

```
acl block_url url_regex 'etc/squid/blacklists' //สร้างไฟล์ blacklist.txt
```

```
http_access deny block_url
```

(พิมพ์ชื่อ Domain ที่ต้องการบล็อกใส่ในแฟ้มที่สร้าง)

4. Block Key word

```
acl keyword url_regex -i messenger hi5 chat
```

```
http_access deny keyword
```

5. Block MP3 Download

```
acl download urlpath_regex -i \.mp4$ \.wav$ \.iso$
```

```
http_access deny download
```

6. การจำกัด bandwidth Download

```
acl blockfile url_regex -i ftp .exe .mp3 .vqf .tar.gz .gz .rpm .zip .rar .avi .mpeg .mpe .mpg .qt .ram  
.rm .iso
```

```
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 lan src 192.168.1.0/255.255.255.0 #กลุ่ม IP LAN ภายใน
```

```
http_access allow lan
```

```
http_access deny all
```

```
delay_pools 1
```

```
delay_class 1 1
```

```
delay_parameters 1 2500/2500 # จำกัดไม่เกิน 2.5 kbyte หากต้องการไม่เกิน 5.0 kbyte ก็เปลี่ยนเป็น
```

5000/5000 ไม่เกิน จะจำกัดเท่าไรก็เปลี่ยนเอาเลยครับ

```
delay_access 1 allow blockfile
```

7. การ download จาก ตัวอักษรหรือคำจาก website

```
acl magic_words url_regx -i .exe
```

```
delay_pools 1
```

```
delay_class 1 1
```

```
delay_parameters 1 4000/4000
```

```
delay_access 1 allow magic_words
```

(magic_world เป็นตัวแปลบออกว่าถ้ามีนามสกุล .exe (ส่วน -i คือ ตัวบอกว่าเป็น case-insensitive) ให้ download มาด้วยความเร็วไม่เกิน 32 Kbit/sec ก็ประมาณ 4 Kbyte/sec)

8. กำหนดให้ขนาด bandwidth ให้กับ User ภายใน network

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

```
delay_pool_count 1
```

```
delay_class 1 2
```

```
delay_parameters 1 12500/12500 2500/2500
```

```
delay_access 1 allow all
```

(อธิบายว่า มี Lease Line ขนาด 128K และต้องการจะเหลือไว้สักนิด สำหรับ SMTP server ซึ่งเป็น IP จริงไม่ได้ ต่อผ่านกับ gateway ตัวนี้ และให้ใช้สำหรับ NAT ภายใน องค์กร 100Kbit/sec เพื่อให้ทุกคน share กันใช้เท่าๆกัน และต้องการจะให้แต่ละคนใช้ Bandwidth ได้ไม่เกิน 2.5 Kbyte/sec)

9 กำหนดขนาด bandwidth ให้กับ group network

```
acl a_ll src 0.0.0.0/0.0.0.0
```

```
delay_class 1 3
```

```
delay_parameters 1 56000/56000 18750/18750 500/500
```

```
delay_access 1 allow all
```

(อธิบายได้ดังนี้ มี Lease Line ขนาด 512K และต้องการเหลือ Bandwidth สำหรับ SMTP ไว้ 8Kbyte/sec ใช้ ภายใน network ไม่เกิน 448 Kbit/sec และแบ่งให้แต่ละ class ไม่เกิน 150 Kbit/sec และให้แต่ละ IP ไม่เกิน 4 Kbit/sec)

10. การจำกัดขนาด bandwidth และไม่จำกัดขนาด bandwidth

```
acl magic_words1 url_regex -i 202.29.14.1
```

```
#กำหนด acl กลุ่มที่มีสิทธิ์ทุกอย่าง acl magic_words2 url_regex -i ftp .exe .mp3 .vqf .tar.gz .gz .rpm .zip  
.rar .avi .mpeg .mpe .mpg .qt .ram .rm .iso .raw .wav .mov #กำหนด acl กลุ่มที่ต้องควบคุม traffic คือไฟล์  
บางประเภทที่ใหญ่ๆ
```

การกำหนดค่า Squid(Delay Pool)

```
# สำหรับ delay pool ที่คุณต้องการ --enable-delay-pools
```

```
delay_pools 2 #กำหนดให้มี 2 pool ที่ต้องใช้
```

```
#สมมุติมี link ขนาด 2Mbits ซึ่ง 2 mbits == 256 kbytes ต่อวินาที เราจะจำกัดให้ใช้ได้ไม่เกิน 5 KB/s ต่อโหนด
```

```
delay_class 1 2 #กำหนดให้ pool ที่ 1 เป็น class 2 ที่ถูกกำหนดค่าไว้ใน magic_word2 แบบจำกัด
```

```
delay_parameters 1 256000/256000 5000/256000
```

```
delay_access 1 allow magic_words2 #กลุ่มที่ดาวน์โหลดไฟล์ต่าง ๆ ที่กำหนดไว้
```

```
delay_access 1 allow rinet #กลุ่มที่มี ip ต้นทางเป็นเครือข่ายภายใน
```

```
# -1/-1 หมายความว่าไม่มีการจำกัดขนาดของ traffic.
```

```
delay_class 2 2 #กำหนดให้ pool ที่ 2 เป็น class 2 ที่ถูกกำหนดค่าไว้ใน magic_word1 แบบไม่จำกัด
```

```
delay_parameters 2 -1/-1 -1/-1
```

```
delay_access 2 allow magic_words1
```

ตัวอย่าง

```
acl download url_regex -i ftp .rar .wma .exe .mp3 .vqf .tar.gz .gz .rpm .zip .avi .mpeg .mpe .mpg .qt  
.ram .rm .iso .raw .wav .mov
```

```
delay_pools 2
```

```
acl day time 09:00-15:59
```

```
acl day2 time 16:00-09:00
```

```
delay_class 1 2
```

```
delay_parameters 1 10000/20000 10000/20000
```

```
delay_access 1 allow download day day2
```

```
delay_access 1 deny all
```

```
delay_class 2 2
delay_parameters 2 -1/-1 -1/-1
delay_access 2 allow localnet localhost !all
delay_access 2 deny !all
```

11. การบล็อก Port และ เลข IP

```
acl porttest port 5050 5222 5223
acl block_port port 5050 5222 5223
acl test src 172.27.162.43
http_access deny block_port test
http_access allow all
```

```
acl block_port port 5050 5222 5223
acl test src 172.27.162.43
http_access deny block_port test
http_access allow all
```

```
acl blockip src "/etc/squid/block.ip" //สร้างแฟ้ม block.ip ใส่เลข IP เข้าไป
```

12. Block skype Chat

```
acl skype_user src "/etc/squid/user-skype" //ใส่เลข ip เครื่องที่อนุญาตให้ใช้ได้
acl numeric_IPs url_regex ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+:443
acl Skype-UA browser ^skype^
http_access deny skype_user numeric_IPs
http_reply_access deny skype_user numeric_IPs
http_access deny skype_user Skype-UA
```
