Squid Transparent Proxy

Ce tutoriel développe la mise en place d'un serveur proxy HTTP/FTP Transparent (sans demande d'authentification).

Installation des packages

Mandrake	debian
squid-2.5.STABLE4-1mdk.i586.rpm	squid_2.5.7-1_i386.deb squid-common_2.5.7-1_all.deb

Configuration de Squid

Editez le fichier **/etc/squid/squid.conf**

```
# WELCOME TO SQUID 2
# NETWORK OPTIONS
# -----------------------------

#  TAG: http_port
#    Usage:    port
#         hostname:port
#         1.2.3.4:port
#
#    The socket addresses where Squid will listen for HTTP client
#    requests.  You may specify multiple socket addresses.
#    There are three forms: port alone, hostname with port, and
#    IP address with port.  If you specify a hostname or IP
#    address, then Squid binds the socket to that specific
#    address.  This replaces the old 'tcp_incoming_address'
#    option.  Most likely, you do not need to bind to a specific
#    address, so you can use the port number alone.
#
#    The default port number is 3128.
#
#    If you are running Squid in accelerator mode, then you
#    probably want to listen on port 80 also, or instead.
#
#    The -a command line option will override the *first* port
#    number listed here.   That option will NOT override an IP
#    address, however.
#
#    You may specify multiple socket addresses on multiple lines.
#
#    If you run Squid on a dual-homed machine with an internal
#    and an external interface then we recommend you to specify the
#    internal address:port in http_port. This way Squid will only be
#    visible on the internal address.
#
#Default:
```

```
# http_port 3128
http_port 3128

#  TAG: icp_port
#    The port number where Squid sends and receives ICP queries to
#    and from neighbor caches.  Default is 3130.  To disable use
#    "0".  May be overridden with -u on the command line.
#
#Default:
# icp_port 3130
# Nous n'avons pas d'autres serveurs proxy.
icp_port 0

# OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
# -----------------------------

#  TAG: hierarchy_stoplist
#    A list of words which, if found in a URL, cause the object to
#    be handled directly by this cache.  In other words, use this
#    to not query neighbor caches for certain objects.  You may
#    list this option multiple times.
#We recommend you to use at least the following line.
hierarchy_stoplist cgi-bin ?

#  TAG: no_cache
#    A list of ACL elements which, if matched, cause the request to
#    not be satisfied from the cache and the reply to not be cached.
#    In other words, use this to force certain objects to never be cached.
#
#    You must use the word 'DENY' to indicate the ACL names which should
#    NOT be cached.
#
#We recommend you to use the following two lines.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY

# OPTIONS WHICH AFFECT THE CACHE SIZE
# -----------------------------

#  TAG: cache_mem   (bytes)
#    NOTE: THIS PARAMETER DOES NOT SPECIFY THE MAXIMUM PROCESS SIZE.
#    IT ONLY PLACES A LIMIT ON HOW MUCH ADDITIONAL MEMORY SQUID WILL
#    USE AS A MEMORY CACHE OF OBJECTS. SQUID USES MEMORY FOR OTHER
#    THINGS AS WELL. SEE THE SQUID FAQ SECTION 8 FOR DETAILS.
#
#    'cache_mem' specifies the ideal amount of memory to be used
#    for:
#         * In-Transit objects
#         * Hot Objects
#         * Negative-Cached objects
#
#    Data for these objects are stored in 4 KB blocks.  This
#    parameter specifies the ideal upper limit on the total size of
#    4 KB blocks allocated.  In-Transit objects take the highest
#    priority.
#
#    In-transit objects have priority over the others.  When
#    additional space is needed for incoming data, negative-cached
```

```
#    and hot objects will be released.  In other words, the
#    negative-cached and hot objects will fill up any unused space
#    not needed for in-transit objects.
#
#    If circumstances require, this limit will be exceeded.
#    Specifically, if your incoming request rate requires more than
#    'cache_mem' of memory to hold in-transit objects, Squid will
#    exceed this limit to satisfy the new requests.  When the load
#    decreases, blocks will be freed until the high-water mark is
#    reached.  Thereafter, blocks will be used to store hot
#    objects.
#
#Default:
# cache_mem 8 MB
cache_mem 16 MB

# LOGFILE PATHNAMES AND CACHE DIRECTORIES
# ------------------------------

#  TAG: cache_dir
#    Usage:
#
#    cache_dir Type Directory-Name Fs-specific-data [options]
#
#    You can specify multiple cache_dir lines to spread the
#    cache among different disk partitions.
#
#    Type specifies the kind of storage system to use. Only "ufs"
#    is built by default. To eanble any of the other storage systems
#    see the --enable-storeio configure option.
#
#    'Directory' is a top-level directory where cache swap
#    files will be stored.  If you want to use an entire disk
#    for caching, then this can be the mount-point directory.
#    The directory must exist and be writable by the Squid
#    process.  Squid will NOT create this directory for you.
#
#    The ufs store type:
#
#    "ufs" is the old well-known Squid storage format that has always
#    been there.
#
#    cache_dir ufs Directory-Name Mbytes L1 L2 [options]
#
#    'Mbytes' is the amount of disk space (MB) to use under this
#    directory.  The default is 100 MB.  Change this to suit your
#    configuration.  Do NOT put the size of your disk drive here.
#    Instead, if you want Squid to use the entire disk drive,
#    subtract 20% and use that value.
#
#    'Level-1' is the number of first-level subdirectories which
#    will be created under the 'Directory'.  The default is 16.
#
#    'Level-2' is the number of second-level subdirectories which
#    will be created under each first-level directory.  The default
#    is 256.
#
#    The aufs store type:
```

```
#
#    "aufs" uses the same storage format as "ufs", utilizing
#    POSIX-threads to avoid blocking the main Squid process on
#    disk-I/O. This was formerly known in Squid as async-io.
#
#    cache_dir aufs Directory-Name Mbytes L1 L2 [options]
#
#    see argument descriptions under ufs above
#
#    The diskd store type:
#
#    "diskd" uses the same storage format as "ufs", utilizing a
#    separate process to avoid blocking the main Squid process on
#    disk-I/O.
#
#    cache_dir diskd Directory-Name Mbytes L1 L2 [options] [Q1=n] [Q2=n]
#
#    see argument descriptions under ufs above
#
#    Q1 specifies the number of unacknowledged I/O requests when Squid
#    stops opening new files. If this many messages are in the queues,
#    Squid won't open new files. Default is 64
#
#    Q2 specifies the number of unacknowledged messages when Squid
#    starts blocking.  If this many messages are in the queues,
#    Squid blocks until it receives some replies. Default is 72
#
#    When Q1 < Q2 (the default), the cache directory is optimized
#    for lower response time at the expense of a decrease in hit
#    ratio.  If Q1 > Q2, the cache directory is optimized for
#    higher hit ratio at the expense of an increase in response
#    time.
#
#    The coss store type:
#
#    block-size=n defines the "block size" for COSS cache_dir's.
#    Squid uses file numbers as block numbers.  Since file numbers
#    are limited to 24 bits, the block size determines the maximum
#    size of the COSS partition.  The default is 512 bytes, which
#    leads to a maximum cache_dir size of 512<<24, or 8 GB.  Note
#    that you should not change the coss block size after Squid
#    has written some objects to the cache_dir.
#
#    Common options:
#
#    read-only, this cache_dir is read only.
#
#    max-size=n, refers to the max object size this storedir supports.
#    It is used to initially choose the storedir to dump the object.
#    Note: To make optimal use of the max-size limits you should order
#    the cache_dir lines with the smallest max-size value first and the
#    ones with no max-size specification last.
#
#    Note that for coss, max-size must be less than COSS_MEMBUF_SZ
#    (hard coded at 1 MB).
#
#Default:
# cache_dir ufs /var/spool/squid 100 16 256
```

```
cache_dir diskd /var/spool/squid 200 16 256

#  TAG: cache_access_log
#    Logs the client request activity.  Contains an entry for
#    every HTTP and ICP queries received. To disable, enter "none".
#
#Default:
# cache_access_log /var/log/squid/access.log
cache_access_log none

#  TAG: cache_log
#    Cache logging file. This is where general information about
#    your cache's behavior goes. You can increase the amount of data
#    logged to this file with the "debug_options" tag below.
#
#Default:
# cache_log /var/log/squid/cache.log
cache_log none

#  TAG: cache_store_log
#    Logs the activities of the storage manager.  Shows which
#    objects are ejected from the cache, and which objects are
#    saved and for how long.  To disable, enter "none". There are
#    not really utilities to analyze this data, so you can safely
#    disable it.
#
#Default:
# cache_store_log /var/log/squid/store.log
cache_store_log none

#  TAG: debug_options
#    Logging options are set as section,level where each source file
#    is assigned a unique section.  Lower levels result in less
#    output,  Full debugging (level 9) can result in a very large
#    log file, so be careful.  The magic word "ALL" sets debugging
#    levels for all sections.  We recommend normally running with
#    "ALL,1".
#
#Default:
# debug_options ALL,1
debug_options ALL,1

#  TAG: ftp_passive
#    If your firewall does not allow Squid to use passive
#    connections, then turn off this option.
#
#Default:
# ftp_passive on

# OPTIONS FOR TUNING THE CACHE
# ----------------------------

#  TAG: refresh_pattern
#    usage: refresh_pattern [-i] regex min percent max [options]
#
#    By default, regular expressions are CASE-SENSITIVE.  To make
#    them case-insensitive, use the -i option.
#
```

```
#    'Min' is the time (in minutes) an object without an explicit
#    expiry time should be considered fresh. The recommended
#    value is 0, any higher values may cause dynamic applications
#    to be erroneously cached unless the application designer
#    has taken the appropriate actions.
#
#    'Percent' is a percentage of the objects age (time since last
#    modification age) an object without explicit expiry time
#    will be considered fresh.
#
#    'Max' is an upper limit on how long objects without an explicit
#    expiry time will be considered fresh.
#
#    options: override-expire
#          override-lastmod
#          reload-into-ims
#          ignore-reload
#
#         override-expire enforces min age even if the server
#         sent a Expires: header. Doing this VIOLATES the HTTP
#         standard.  Enabling this feature could make you liable
#         for problems which it causes.
#
#         override-lastmod enforces min age even on objects
#         that was modified recently.
#
#         reload-into-ims changes client no-cache or ``reload''
#         to If-Modified-Since requests. Doing this VIOLATES the
#         HTTP standard. Enabling this feature could make you
#         liable for problems which it causes.
#
#         ignore-reload ignores a client no-cache or ``reload''
#         header. Doing this VIOLATES the HTTP standard. Enabling
#         this feature could make you liable for problems which
#         it causes.
#
#    Basically a cached object is:
#
#         FRESH if expires < now, else STALE
#         STALE if age > max
#         FRESH if lm-factor < percent, else STALE
#         FRESH if age < min
#         else STALE
#
#    The refresh_pattern lines are checked in the order listed here.
#    The first entry which matches is used.  If none of the entries
#    match, then the default will be used.
#
#    Note, you must uncomment all the default lines if you want
#    to change one. The default setting is only active if none is
#    used.
#
#Suggested default:
refresh_pattern ^ftp:    1440 20%  10080
refresh_pattern ^gopher: 1440 0%  1440
refresh_pattern .        0    20%  4320

# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS
```

```
# ------------------------------
# TAG: redirect_program
# Specify the location of the executable for the URL redirector.
# Since they can perform almost any function there isn't one included.
# See the FAQ (section 15) for information on how to write one.
# By default, a redirector is not used.
#
#Default:
# none
#redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

# TIMEOUTS
# ------------------------------

#  TAG: half_closed_clients
#    Some clients may shutdown the sending side of their TCP
#    connections, while leaving their receiving sides open.     Sometimes,
#    Squid can not tell the difference between a half-closed and a
#    fully-closed TCP connection.  By default, half-closed client
#    connections are kept open until a read(2) or write(2) on the
#    socket returns an error.  Change this option to 'off' and Squid
#    will immediately close client connections when read(2) returns
#    "no more data to read."
#
#Default:
# half_closed_clients on
half_closed_clients off

# ACCESS CONTROLS
# ------------------------------

#  TAG: acl
#    Defining an Access List
#
#    acl aclname acltype string1 ...
#    acl aclname acltype "file" ...
#
#    when using "file", the file should contain one item per line
#
#    acltype is one of the types described below
#
#    By default, regular expressions are CASE-SENSITIVE.  To make
#    them case-insensitive, use the -i option.
#
#    acl aclname src      ip-address/netmask ... (clients IP address)
#    acl aclname src      addr1-addr2/netmask ... (range of addresses)
#    acl aclname dst      ip-address/netmask ... (URL host's IP address)
#    acl aclname myip     ip-address/netmask ... (local socket IP address)
#
#    acl aclname srcdomain   .foo.com ...    # reverse lookup, client IP
#    acl aclname dstdomain   .foo.com ...    # Destination server from URL
#    acl aclname srcdom_regex [-i] xxx ...   # regex matching client name
#    acl aclname dstdom_regex [-i] xxx ...   # regex matching server
#      # For dstdomain and dstdom_regex  a reverse lookup is tried if a IP
#      # based URL is used. The name "none" is used if the reverse lookup
#      # fails.
#
#    acl aclname time     [day-abbrevs]  [h1:m1-h2:m2]
```

```
#        day-abbrevs:
#         S – Sunday
#         M – Monday
#         T – Tuesday
#         W – Wednesday
#         H – Thursday
#         F – Friday
#         A – Saturday
#        h1:m1 must be less than h2:m2
#    acl aclname url_regex [-i] ^http:// ...# regex matching on whole URL
#    acl aclname urlpath_regex [-i] \.gif$ ...    # regex matching on URL
path
#    acl aclname urllogin [-i] [^a-zA-Z0-9] ...  # regex matching on URL
login field
#    acl aclname port     80 70 21 ...
#    acl aclname port     0-1024 ...         # ranges allowed
#    acl aclname myport   3128 ...      # (local socket TCP port)
#    acl aclname proto    HTTP FTP ...
#    acl aclname method   GET POST ...
#    acl aclname browser  [-i] regexp ...
#      # pattern match on User-Agent header
#        acl aclname referer_regex  [-i] regexp ...
#          # pattern match on Referer header
#          # Referer is highly unreliable, so use with care
#    acl aclname ident    username ...
#    acl aclname ident_regex [-i] pattern ...
#      # string match on ident output.
#      # use REQUIRED to accept any non-null ident.
#    acl aclname src_as   number ...
#    acl aclname dst_as   number ...
#      # Except for access control, AS numbers can be used for
#      # routing of requests to specific caches. Here's an
#      # example for routing all requests for AS#1241 and only
#      # those to mycache.mydomain.net:
#      # acl asexample dst_as 1241
#      # cache_peer_access mycache.mydomain.net allow asexample
#      # cache_peer_access mycache_mydomain.net deny all
#
#    acl aclname proxy_auth username ...
#    acl aclname proxy_auth_regex [-i] pattern ...
#      # list of valid usernames
#      # use REQUIRED to accept any valid username.
#      #
#      # NOTE: when a Proxy-Authentication header is sent but it is not
#      # needed during ACL checking the username is NOT logged
#      # in access.log.
#      #
#      # NOTE: proxy_auth requires a EXTERNAL authentication program
#      # to check username/password combinations (see
#      # auth_param directive).
#      #
#      # WARNING: proxy_auth can't be used in a transparent proxy. It
#      # collides with any authentication done by origin servers. It may
#      # seem like it works at first, but it doesn't.
#
#    acl aclname snmp_community string ...
#      # A community string to limit access to your SNMP Agent
#      # Example:
```

```
#      #
#      #  acl snmppublic snmp_community public
#
#    acl aclname maxconn number
#      # This will be matched when the client's IP address has
#      # more than <number> HTTP connections established.
#
#    acl aclname max_user_ip [-s] number
#      # This will be matched when the user attempts to log in from more
#      # than <number> different ip addresses. The authenticate_ip_ttl
#      # parameter controls the timeout on the ip entries.
#      # If -s is specified then the limit is strict, denying browsing
#      # from any further IP addresses until the ttl has expired. Without
#      # -s Squid will just annoy the user by "randomly" denying requests.
#      # (the counter is then reset each time the limit is reached and a
#      # request is denied)
#      # NOTE: in acceleration mode or where there is mesh of child
proxies,
#      # clients may appear to come from multiple addresses if they are
#      # going through proxy farms, so a limit of 1 may cause user
problems.
#
#    acl aclname req_mime_type mime-type1 ...
#      # regex match agains the mime type of the request generated
#      # by the client. Can be used to detect file upload or some
#      # types HTTP tunelling requests.
#      # NOTE: This does NOT match the reply. You cannot use this
#      # to match the returned file type.
#
#    acl aclname rep_mime_type mime-type1 ...
#      # regex match against the mime type of the reply recieved by
#      # squid. Can be used to detect file download or some
#      # types HTTP tunelling requests.
#      # NOTE: This has no effect in http_access rules. It only has
#      # effect in rules that affect the reply data stream such as
#      # http_reply_access.
#
#    acl acl_name external class_name [arguments...]
#      # external ACL lookup via a helper class defined by the
#      # external_acl_type directive.
#
#Examples:
#acl myexample dst_as 1241
#acl password proxy_auth REQUIRED
#acl fileupload req_mime_type -i ^multipart/form-data$
#acl javascript rep_mime_type -i ^application/x-javascript$
#

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 mynetwork src 192.168.0.0/255.255.0.0
acl SSL_ports port 443 563    # https, snews
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 CONNECT method CONNECT

#  TAG: http_access
#    Allowing or Denying access based on defined access lists
#
#    Access to the HTTP port:
#    http_access allow|deny [!]aclname ...
#
#    NOTE on default values:
#
#    If there are no "access" lines present, the default is to deny
#    the request.
#
#    If none of the "access" lines cause a match, the default is the
#    opposite of the last line in the list.  If the last line was
#    deny, then the default is allow.  Conversely, if the last line
#    is allow, the default will be deny.  For these reasons, it is a
#    good idea to have an "deny all" or "allow all" entry at the end
#    of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow mynetwork
http_access deny all

#  TAG: icp_access
#    Allowing or Denying access to the ICP port based on defined
#    access lists
#
#    icp_access  allow|deny [!]aclname ...
#
#    See http_access for details
#
#Default:
# icp_access deny all
#
#Allow ICP queries from everyone
icp_access allow all

#  TAG: miss_access
#    Use to force your neighbors to use you as a sibling instead of
#    a parent.  For example:
#
```

```
#         acl localclients src 172.16.0.0/16
#         miss_access allow localclients
#         miss_access deny  !localclients
#
#    This means that only your local clients are allowed to fetch
#    MISSES and all other clients can only fetch HITS.
#
#    By default, allow all clients who passed the http_access rules
#    to fetch MISSES from us.
#
#Default setting:
# miss_access allow all
miss_access allow all

# Autorise le protocole HTTP
acl protocole_web proto HTTP
http_access allow protocole_web

# Refuse le protocole FTP
acl protocole_ftp proto FTP
http_access deny protocole_ftp

# acl aclname time [day-abbrevs] [h1:m1-h2:m2]
# day-abbrevs:
# S – Sunday
# M – Monday
# T – Tuesday
# W – Wednesday
# H – Thursday
# F – Friday
# A – Saturday
# h1:m1 must be less than h2:m2

# Autorise l'accès au cache de 8h à 18h
acl horaire time M-F 08:00-18:00
http_access allow horaire

# Refuse l'accès au cache de 0h à 7h59
acl hors_horaire1 time MTWHF 00:00-07:59
http_access deny hors_horaire1

# Refuse l'accès au cache de 18h01 à 23h59
acl hors_horaire2 time MTWHF 18:01-23:59
http_access deny hors_horaire2

# Refuse l'accès au cache du samedi au dimanche.
acl week_end time A-S
http_access deny week_end

# Refuse l'accès aux domaines écrit dans ce fichier.
# le -i indique pas "sensible à la case"
# mettre un domaine par ligne sous cette forme :
# .microsoft.com
# .sco.com
acl bad_domain dstdomain -i "/etc/squid/baddomain.txt"
http_access deny bad_domain

# Refuse l'accès aux URL écrites dans ce fichier.
```

```
acl sex_site url_regex -i "/etc/squid/sexsite.txt"
http_access deny sex_site

acl warez_site url_regex -i "/etc/squid/warezsite.txt"
http_access deny warez_site

# Refuse l'accès aux extensions suivantes :
acl url_mp3 url_regex -i \.mp3$
http_access deny url_mp3
acl url_avi url_regex -i \.avi$
http_access deny url_avi
acl url_mpeg url_regex -i \.mpeg$
http_access deny url_mpeg
acl url_mpg url_regex -i \.mpg$
http_access deny url_mpg
acl url_mov url_regex -i \.mov$
http_access deny url_mov
acl url_exe url_regex -i \.exe$
http_access deny url_exe


# ADMINISTRATIVE PARAMETERS
# -----------------------------

#  TAG: cache_mgr
#    Email-address of local cache manager who will receive
#    mail if the cache dies.  The default is "webmaster."
#
#Default:
# cache_mgr webmaster
cache_mgr proxy@alex.fr

#  TAG: visible_hostname
#    If you want to present a special hostname in error messages, etc,
#    then define this.  Otherwise, the return value of gethostname()
#    will be used. If you have multiple caches in a cluster and
#    get errors about IP-forwarding you must set them to have individual
#    names with this setting.
#
#Default:
# none
visible_hostname proxy.alex.fr

# HTTPD-ACCELERATOR OPTIONS
# -----------------------------

#  TAG: httpd_accel_host
#  TAG: httpd_accel_port
#    If you want to run Squid as an httpd accelerator, define the
#    host name and port number where the real HTTP server is.
#
#    If you want IP based virtual host support then specify the
#    hostname as "virtual". This will make Squid use the IP address
#    where it accepted the request as hostname in the URL.
#
#    If you want virtual port support then specify the port as "0".
#
#    NOTE: enabling httpd_accel_host disables proxy-caching and
```

```
#    ICP.  If you want these features enabled also, then set
#    the 'httpd_accel_with_proxy' option.
#
#Default:
# httpd_accel_port 80
httpd_accel_host virtual

#  TAG: httpd_accel_with_proxy    on|off
#    If you want to use Squid as both a local httpd accelerator
#    and as a proxy, change this to 'on'. Note however that your
#    proxy users may have trouble to reach the accelerated domains
#    unless their browsers are configured not to use this proxy for
#    those domains (for example via the no_proxy browser configuration
#    setting)
#
#Default:
# httpd_accel_with_proxy off
httpd_accel_with_proxy  on

#  TAG: httpd_accel_uses_host_header   on|off
#    HTTP/1.1 requests include a Host: header which is basically the
#    hostname from the URL.  The Host: header is used for domain based
#    virutal hosts. If your accelerator needs to provide domain based
#    virtual hosts on the same IP address then you will need to turn this
#    on.
#
#    Note that Squid does NOT check the value of the Host header matches
#    any of your accelerated server, so it may open a big security hole
#    unless you take care to set up access controls proper.  We recommend
#    that this option remain disabled unless you are sure of what you
#    are doing.
#
#    However, you will need to enable this option if you run Squid
#    as a transparent proxy.  Otherwise, virtual servers which
#    require the Host: header will not be properly cached.
#
#Default:
# httpd_accel_uses_host_header off
httpd_accel_uses_host_header on

# MISCELLANEOUS
# -----------------------------

#  TAG: append_domain
#    Appends local domain name to hostnames without any dots in
#    them.  append_domain must begin with a period.
#
#    Be warned that there today is Internet names with no dots in
#    them using only top-domain names, so setting this may
#    cause some Internet sites to become unavailable.
#
#Example:
# append_domain .yourdomain.com
#
#Default:
# none
append_domain .alex.fr
```

```
#  TAG: err_html_text
#    HTML text to include in error messages.  Make this a "mailto"
#    URL to your admin address, or maybe just a link to your
#    organizations Web page.
#
#    To include this in your error messages, you must rewrite
#    the error template files (found in the "errors" directory).
#    Wherever you want the 'err_html_text' line to appear,
#    insert a %L tag in the error template file.
#
#Default:
# none
err_html_text proxy@alex.fr

#  TAG: memory_pools     on|off
#    If set, Squid will keep pools of allocated (but unused) memory
#    available for future use.  If memory is a premium on your
#    system and you believe your malloc library outperforms Squid
#    routines, disable this.
#
#Default:
# memory_pools on
memory_pools off

#  TAG: deny_info
#    Usage:   deny_info err_page_name acl
#    or       deny_info http://... acl
#    Example: deny_info ERR_CUSTOM_ACCESS_DENIED bad_guys
#
#    This can be used to return a ERR_ page for requests which
#    do not pass the 'http_access' rules.  A single ACL will cause
#    the http_access check to fail.  If a 'deny_info' line exists
#    for that ACL then Squid returns a corresponding error page.
#
#    You may use ERR_ pages that come with Squid or create your own pages
#    and put them into the configured errors/ directory.
#
#    Alternatively you can specify an error URL. The browsers will then
#    get redirected (302) to the specified URL. %s in the redirection
#    URL will be replaced by the requested URL.
#
#    Alternatively you can tell Squid to reset the TCP connection
#    by specifying TCP_RESET.
#
#Default:
# none
#deny_info ERR_CUSTOM_ACCESS_DENIED all

#  TAG: error_directory
#    If you wish to create your own versions of the default
#    (English) error files, either to customize them to suit your
#    language or company copy the template English files to another
#    directory and point this tag at them.
#
#Default:
# error_directory /usr/share/squid/errors/English
# Mandrake :
#error_directory /usr/lib/squid/errors/French
```

```
# Debian :
error_directory /usr/share/squid/errors/French

# DELAY POOL PARAMETERS (all require DELAY_POOLS compilation option)
# -----------------------------

#  TAG: coredump_dir
#    By default Squid leaves core files in the directory from where
#    it was started. If you set 'coredump_dir' to a directory
#    that exists, Squid will chdir() to that directory at startup
#    and coredump files will be left there.
#
#Default:
# coredump_dir none
#
# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid
```

Configuration de /etc/resolv.conf

Pour une meilleure résolution des noms de domaine vers internet, installez un serveur DNS cache sur la machine ou vous avez installé Squid. Ce serveur DNS cache n'aura pas de relations directe avec les deux autres serveurs DNS dédiés à la résolution des noms des machines de votre réseau local et ne sera pas informé, ni mit à jour par eux.

```
# N'indiquez pas les adresses de vos serveurs DNS si vous avez
# installé un serveur DNS cache sur le proxy.
nameserver 127.0.0.1
```

Il suffit de configurer les navigateurs de vos utilisateurs pour qu'ils utilisent le serveur Proxy 192.168.1.4 sur le port 3128.

Si vous souhaitez filtrer **le contenu des pages** affichées et d'autres options encore, reportez vous à la configuration de DansGuardian.

Document mis à jour : 03/05/05