

# Transparent proxy with Squid

Last Updated Saturday, 03 February 2007

This section shows you howto setup transparent proxy with squid, redirecting http traffic to squid port. The howto is for FreeBSD setups that uses OpenBSD packet filter - pf, or ipfw firewall.

## Step 1

-----

Install squid from ports. If you use pf firewall you will need to compile Squid with support for pf.

```
cd /usr/ports/www/squid
make install
```

If you use pf firewall you must compile squid with transparent pf support. (there are also other options like support for diskd)

```
cd /usr/ports/www/squid/work/squid-2.5.STABLE12
```

```
./configure --bindir=/usr/local/sbin --sysconfdir=/usr/local/etc/squid --datadir=/usr/local/etc/squid --
libexecdir=/usr/local/libexec/squid --localstatedir=/usr/local/squid --enable-removal-policies=lru,heap --enable-
auth=basic,ntlm,digest --enable-basic-auth-helpers=NCSA,PAM,MSNT,SMB,winbind,YP --enable-digest-auth-
helpers=password --enable-external-acl-helpers=ip_user,unix_group,wbinfo_group,winbind_group --enable-ntlm-auth-
helpers=SMB,winbind --enable-storeio=ufs,diskd,null --enable-underscores --enable-err-languages=English --enable-
default-err-language=Romanian --with-large-files --enable-large-cache-files --enable-delay-pools --enable-ipf-transparent
--disable-ident-lookups --enable-snmp --enable-removal-policies --prefix=/usr/local i386-portbld-freebsd6.1
--enable-pf-transparent
```

```
make install
```

## Step 2

-----

a) If you are using pf firewall:

You should add the following rules in order to redirect http traffic to squid (assuming squid is running on port 8080):

```
# ----- pf.conf -----
int_if="fxp0"
ext_if="fxp1"

rdr on $int_if inet proto tcp from any to any port www -> 127.0.0.1 port 8080
pass in on $int_if inet proto tcp from any to 127.0.0.1 port 8080 keep state
pass out on $ext_if inet proto tcp from any to any port www keep state
# ----- end pf.conf -----
```

Also we must allow squid to access pf device.

```
chgrp _squid /dev/pf
chmod g+rw /dev/pf
```

b) If you are using ipfw firewall

Add your redirect rule in your ipfw config file:

```
int_if="fxp0"
ipfw add 1000 fwd 127.0.0.1,8080 tcp from any to any 80 in recv $int_if
```

In both setups, with pf or ipfw firewall if you are using pppoe servers or other setups in which you use ng netgraph or tun interfaces, the redirect rule must be on that particular ng interface.

When using ipfw you can redirect http traffic to ng\*. With pf using ng\* will not work.

Your squid.conf should look like that:

(please modify the path where your stored squid cache, the size of cache and also the allowed ip range for your squid daemon. Don't forget to do a 'squid -z' if you did not, at install time (for creating cache directories)).

```
#my settings
http_port 8080
icp_port 0
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_mem 128 MB

maximum_object_size 80000 KB
ipcache_size 1024
ipcache_low 90
ipcache_high 95
cache_dir diskd /mnt/squid 28000 32 512 Q1=72 Q2=64

log_fqdn off
logfile_rotate 10

dns_nameservers 10.0.0.1

auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320

#next, remove
acl localnet src 10.0.0.0/255.255.0.0
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 21 443 563 210 1025-65535 280 488 591 777
acl CONNECT method CONNECT
acl all src 0.0.0.0/0.0.0.0

http_access deny !Safe_ports

http_access allow localnet
http_reply_access allow all
visible_hostname localhost

httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on

coredump_dir /usr/local/squid/cache
```