

```
/******\
* Gökhan ALKAN
* gokhan [at] enderunix [dot] org
* EnderUNIX Yazılım Gelistirme Takımı
* http://www.enderunix.org
*
* Sürüm : 1.0
* Tarih : 06.08.2006
* Makalenin en yeni versiyonuna http://www.enderunix.org/squidguard.pdf
* adresinden elde edilebilir.
*****/
```

SquidGuard Kurulumu

Basit olarak Squid Guard ./configure , make , make install ile kurulabilir.SquidGuard kurulumu için Berkley DB 2.x sürümünün yüklü olması gerekmektedir. Yoksa kurulum esnasında aşağıdaki gibi hata alınacaktır.

```
** The Berkley DB library is required for squidGuard
to compile. Get it from http://www.sleepycat.com
use --with-db=DIR or --with-db-lib=DIR to specify
its location. (default is /usr/local/BerkeleyDB)
```

Öncelikle gerekli paket temin edilmelidir. www.sleepycat.com adresinden temin edilebilir. Basitçe kurulumu ;

```
# tar -zxvf db-4.4.20.NC.tar.gz
# ./db-4.4.20.NC/dist/configure
# make
# make install
# make clean (isteğe bağlı)
```

Ön tanımlı olarak /usr/local/BerkeleyDB dizini altına kurulmaktadır. İsteğe göre -prefix ile istenilen dizin belirtilebilir.

Berkley DB kurulumu tamamlandıktan sonra SquidGuard temin edilerek kurulum gerçekleştirilebilir. <http://www.squidguard.org/download/> adresinden SquidGuard temin edilerek

```
# wget http://ftp.tdcnorge.no/pub/www/proxy/squidGuard/squidGuard-1.2.0.tar.gz
# tar -zxvf squidGuard-1.2.0.tar.gz
# cd squidGuard-1.2.0
# ./configure
# make
# make install
# make clean
```

Burada SquidGuard için Berkley DB 4.4 sürümü kullanıldı. Eğer kurulumda sorun yaşanırsa sürüm 3.x yada sürüm 2.x denenmelidir. Sürüm 3.x için kurulum dizini /usr/local/BerkeleyDB.3.x 2.x sürümü için ise /usr/local/BerkeleyDB olacaktır. SquidGuard kurulumda

bu izinler dikkate alınarak kurulum gerçekleştirilmelidir. Ön tanımlı olarak SquidGuard /usr/local/BerkeleyDB dizinine bakar.

Sürüm 3.2.9 için kurulum için öncelikle gerekli paketler temin edilmelidir. Paketlerin /usr/local/src dizininde bulunduğu varsayılarak kurulum gerçekleştirilmiştir.

```
# mkdir /usr/local/src
# cd /usr/local/src
```

Berkley DB 3.2.9 sürümü www.sleepycat.com adresinden temin edilebilir.

```
# tar -zxvf db-3.2.9.tar.gz
# cd db-3.2.9
```

Gerekli yamalar <http://www.enderunix.org/docs/patch/squidguard/> adresinden yada <http://www.sleepycat.com/update/3.2.9/patch.3.2.9.html> adresinden temin edilebilir.

```
# wget http://www.enderunix.org/docs/patch/squidguard/patch.3.2.9-1
# wget http://www.enderunix.org/docs/patch/squidguard/patch.3.2.9-2
# patch -p0 < patch.3.2.9-1
# patch -p0 < patch.3.2.9-2
# cd build_unix
# ../dist/configure
# make
# make install
```

```
# wget http://ftp.tdcnorge.no/pub/www/proxy/squidGuard/squidGuard-1.2.0.tar.gz
# tar -zxvf squidGuard-1.2.0.tar.gz
# cd squidGuard-1.2.0
```

./configure betiğine verilebilecek değerler yukarıda anlatılmıştır. Tekrar burada anlatılmayacaktır. İsteğe göre gerekli değerler seçilebilir.

```
# ./configure
# make
# make install
# make clean
```

Bu şekilde de Berkley DB 3.2.9 sürümü ile squidGuard kurulumu tamamlanmış oldu SquidGuard kurulumu tamamlandıktan sonra log dosyalarını tutması için gerekli izin ve izinleri oluşturulmalıdır. Ön tanımlı olarak /usr/local/squidGuard/log/squidGuard.log dosyasına logları tutar.

```
# mkdir -p /usr/local/squidGuard/log
# chown squid:squid /usr/local/squidGuard/log/squidGuard.log
```

Son olarak da yapılandırma dosyası için /usr/local/squidGuard/squidGuard.conf dosyası oluşturulmalı ve isteğe göre yapılandırma değerleri verilmelidir. SquidGuard çalışması ile ilgili loglar buradan takip edilebilir.

```
# touch /usr/local/squidGuard/squidGuard.conf
```

SquidGuard Çalıştırılması

Öncelikle SquidGuard çalıştırılmadan önce yapılandırma dosyası için belirtilen girdilerin belirtilmesi gerekmektedir. Burada minimum yapılandırma dosyası ayarlamaları ile belirtim yapıp SquidGuard çalıştırılacaktır. Daha sonraki bölümde yapılandırma ile ilgili daha geniş bilgiler yer alacaktır. Aşağıda ön tanımlı olarak her şeyi kabul eden bir acl'e sahip bir yapılandırma dosyası mevcuttur.

```
logdir /usr/local/squidGuard/log
```

```
acl {
    default {
        pass all
    }
}
```

```
# squid -k reconfigure
```

Değişiklikler etkin hale getirilir. ps yada top komutu ile squidGuard süreçleri görüntülenebilir.

```
# ps -auwx | grep 'squidGuard'
squid 16152 0.0 0.2 692 940 ?? Is 10:42AM 0:00.59
(squidGuard) (squidGuard)
squid 14364 0.0 0.2 744 940 ?? Is 10:42AM 0:00.59
(squidGuard) (squidGuard)
squid 17389 0.0 0.2 824 884 ?? Is 10:42AM 0:00.60
(squidGuard) (squidGuard)
squid 15149 0.0 0.2 848 872 ?? Is 10:42AM 0:00.59
(squidGuard) (squidGuard)
squid 3981 0.0 0.2 756 884 ?? Is 10:42AM 0:00.61
(squidGuard) (squidGuard)
#
```

yada log dosyasından squidGuard çalışması ile ilgili bilgiler edinilebilir.

```
# tail -f /usr/local/squidGuard/log/squidGuard.log
...
...
2006-07-18 10:42:38 [15149] squidGuard 1.2.0 started (1153208544.367)
2006-07-18 10:42:38 [15149] squidGuard ready for requests (1153208558.220)
#
```

squidGuard ready for requests ile çalışmaya hazır olduğu belirtiliyor. SquidGuard çalışması ile ilgili hatalar örneğin yapılandırma dosyasından yapılabilecek hatalar log dosyasından takip edilebilir.

```
# tail -f /usr/local/squidGuard/log/squidGuard.log
...
...
2006-07-18 10:58:10 [8936] syntax error in configfile
/usr/local/squidGuard/squidGuard.conf line 9
2006-07-18 10:58:10 [8936] going into emergency mode
#
```

görüldüğü gibi yapılandırma dosyasının 9. satırında syntax hatası yapılmış.

NOT: squidGuard yapılandırma dosyasında belirtilecek olan logdir , dbhome , acl vs gibi bölümler sola dayalı olarak yapılandırma dosyasında belirtilmelidir. Yoksa belirtilen syntax hataları alınabilir.

SquidGuard Yapılandırması

Yol Belirtilimleri :

logdir : Standart log dosyalarının squidGuard.error ve squidGuard.log yerini belirtir.

dbhome : Yasaklanması istenen adreslerin bulunduğu dizin. Kara liste yada kişisel kullanım için oluşturulabilecek adreslerin bulunduğu dizin. Bu dizinler squidGuard yapılandırma dosyasında belirtilir. Ön tanımlı olarak /usr/local/squidGuard/db dizinidir.

Bu iki dizin için yapılandırma dosyasında önerilen belirtilimler aşağıda belirtilen şekildedir.

```
logdir /usr/local/squidGuard/logs
dbhome /usr/local/squidGuard/db
```

Zaman Belirtilimleri:

```
time isim {
    belirtim
    belirtim
}
```

Belirtilimler aşağıdaki şekilde olmaktadır.

weekly {smtwhfa} [HH:MM-HH:MM] veya **weekly günadı [...] [HH:MM-HH:MM]**

s=pazar, m=pazartesi, t =salı, w=çarşamba, h=perşembe, f=cuma, a=cumartesi günlerini temsil etmektedir.

"weekly mtwhf 00:00-08:00"

pazartesiden cumaya kadar sabah zamanlarını belirtir.

"weekly Sunday"

Pazar gününü belirtir.

"date *.02.01 12:00-13:00"

her yıl Şubat ayının 1. gününün saat 12:00 13:00 aralığını belirtir.

Kaynak Grup Belirtilimleri:

Belirtilimler ařađıdaki řekilde olmaktadır.

```
src|source isim within|outside zaman_belirtim_ismi {
    belirtim
    belirtim
    ...
} else {
    belirtim
    belirtim
    ...
}
```

Kaynak belirtilimlerinde src yada source kullanılır. İsteđe bađlı olarak seđim yapılabilir.

"ip 192.168.1.1" ile tek bir ip adresi belirtilir.

"ip 192.168.1.1-192.168.1.5" ile ip aralıđı belirtilir.

"ip 192.168.1.1/24" yada "ip 192.168.1.1/255.255.255.0" ile de netmask bilgisi kullanılabilir.

```
src tembel within tatil {
    ip          192.168.1.1
    domain      galkan.endersys.com
    user        root administrator galkan
}
```

Hedef Grup Belirtilimleri:

```
dest|destination isim within|outside zaman_belirtimi {
    belirtim
    belirtim
    ...
} else {
    belirtim
    belirtim
    ...
}
```

dst ve dest ikisi de kaynak belirtimi için kullanılabilir.

within ve outside zaman kısıtlaması için kullanılır.within ile belirtilen zaman dilimi içerisinde olduđu anlamına gelmektedir.

else ile de yine zaman kısıtlaması kullanımda kullanılır

"domainlist endersys/domains"
endersys/domains dosyasında istenen domainler belirtilebilir.

```
# cat ./endersys/domains
```

```
galatasaray.org
bjk.com.tr
fenerbahce.org
#
```

```
"urllist endersys/urls"
endersys/urls dosyasına istenen url'ler belirtilebilir.
```

```
# cat /usr/local/squidGuard/db/yasak/urls
trabzonspor.org.tr/altyapi
#
```

```
"expressionlist endersys/expressions"
endersys/expressions dosyasında istenen düzenli ifadeler belirtilebilir.
```

```
# cat db/endersys/expressions
(adultos|adultsight|adultsite|adultonly|adultweb)
#
```

```
"redirect 302:http://www.endersys.com"
hedef belirtiminde eşleşen domain , url ve düzenli ifadeler için
www.endersys.com yönlendirmesi gerçekleşir.
```

Erişim Kontrol Listeleri:

Default Kural Seti:

Default kural seti ön tanımlı kural setini tanımlar. Hiçbir erişim listesiyle eşleşmeyen istemciler için uygulanacak kural setini belirtir.

Pass Kuralı Seti :

Hedef belirtimleri için nasıl davranılacağını belirler. all , none , in-addr ve hedef değerlerini alır. Ön tanımlı erişimin engellenmesi isteniyorsa "pass none" kuralı uygulanabilir. Ön tanımlı olarak erişime açılması isteniyorsa "pass all" kullanılabilir. Bu değerlerin dışında "!" ile de değil anlamında kullanılmaktadır. "pass !yasak all" kuralı ile sadece yasak hedef belirtimi engellenmiş olur.

Örnek Yapılandırma Dosyası

```
logdir /usr/local/squidGuard/log
dbhome /usr/local/squidGuard/db
```

```
time tatil {
    weekly *          17:00-24:00
    weekly fridays 16:00-17:00
}
```

```
src endersys {
    ip    10.0.0.0/24
    user  galkan
}
```

```
src enderunix {
    ip    10.0.0.0/22
}
```

```
dest galkan {
    domainlist    galkan/domains
}
```

```
dest yasak {
    domainlist    yasak/domains
    urllist       yasak/urls
    expressionlist yasak/expressions
}
```

```
acl {
    endersys within tatil {
        pass all
    } else {
        pass !yasak all
    }

    enderunix {
        pass !yasak all
    }

    default {
        pass none
        redirect http://www.endersys.com
    }
}
```

```
# cat db/yasak/domains
galatasaray.org
bjk.com.tr
fenerbahce.org
#
```

```
src endersys {
    ip    10.0.0.0/24
}
```

```
src enderunix {
    ip 10.0.0.0/22
}
```

“endersys” ve “enderunix” adı ile 2 adet grup oluşturuluyor

```
time tatil {
    weekly * 17:00-24:00
}
```

tatil zamanı belirtimi yapılıyor.

```
endersys within tatil {
    pass all
} else {
    pass !yasak all
}
```

“endersys” grubu için “tatil” adlı zaman belirtimi süresi içerisinde (within tatil) erişim serbest tatil zamanı dışında (else) yasak/domain dosyasında belirtilen domainler için erişim sağlayamayacak.

```
enderunix {
    pass !yasak all
}
```

enderunix grubundaki istemciler yasak/domains dosyasında belirtilen domainler haricinde erişim sağlayabiliyor.

```
dest yasak {
    domainlist yasak/domains
    urllist yasak/urls
    expressionlist yasak/expressions
}
```