# OpenBSD Pf ve Squid ile Transparent Proxy Kurulumu

**!!Bu yazıda OpenBSD 3.7 işletim sistemi kullanılmıştır.**

## Transparent(saydam) Proxy nedir?

Transparent(seffaf, saydam) proxy kullanıcı tarafında herhangi ek ayar  gerektirmeden kullanıcıdan gelen istekleri bir proxy aracılığı ile yönetmektir. Kısacası kullanıcıdan habersiz kullanıcı ile orjinal sunucu arasına girmektir.

Resimleyecek olursak;

*Kullanıcı----->Seffaf_proxy---->orjinal_web_sunucu*

Burada kullanıcı "orjinal_web_sunucu" ile haberleştiğini düşünür ve istekleri orjinal  sunucuya gönderir, araya yerleştirilen seffaf proxy kullanıcıdan gelen isteği yakalayarak kendisi bu isteği yerine getirir ve cevabını kullanıcıya sanki orjinal sunucudan geliyormuş gibi döndürür.

## Squid transparent modda nasıl çalışır?

Squid'i seffaf proxy modunda kullanmak istedigimizde bir filtreleme aracı ile proxy makinesine gelen 80. port isteklerini squid'in çalıştığı porta yönlendirmek gerekir. Squid ile filtreleme aracı farklı makinelerde olabilir.

Linux uzerinde netfilter/iptables, *BSD ler üzerinde PF(Packet Filter), IPF gibi araçlarla yapılabilir. Squid bu farklı filtreleme araçları için farklı derleme seçenekleri sunar. Mesela squid ile iptables kullanılacaksa --enable-

netfilter, squid ile pf kullanılacaksa --enable-pf-transparent seçenekleri kullanılabilir. Bu derleme seçeneklerinin kullanılmaması squid'in şeffaf proxy özelliğini yerine getirmesini engellemez ama ilerde yaşanabilecek bazı problemler için baştan çözüm sunar.

Evet derleme esnasındaki --enable-netfilter ya da --enable-pf squid'e ne sağlar? Squid istemciden gelen istekteki orjinal sunucu Ip adresini ***Host başlığına*** bakarak alır, eğer host başlığı gönderilmemişse squid --enable-netfilter ile derlendiği için bu derlemede kendisine katılan Linux/UNIX spesifik ag ozellikleri ile orjinal sunucunun IP adresini öğrenebilir. Günümüze bakıldığında tüm http istemciler host başlığını göndermektedir. Yani bu derleme seçenekleri sadece işi sağlama alma amaçlıdır.

**Squid Kurulumu**

OpenBSD altında Squid iki farklı şekilde kurulabilir. Biri klasik kaynak koddan derleme şeklinde , diğeri ise OpenBSD port sistemi kullanarak. OpenBSD Port sistemi kurulacak paketlerin bağımlılık sorunlarını kolayca çözen ve sisteme kurulan paketlerin kontrolünün kolay takip edilmesini sağlayan bir yapı sunar. Klasik yöntemi tercih edenler http://www.squid-cache.org/ adresinden son sürüm squid paketini indirerek kurabilir. Bu yazıda Squid OpenBSD port ağacından kurulacaktır.

OpenBSD port sistemini kullanarak squid'i transparent proxy işlevi görecek şekilde kurmak için aşağıdaki komutlar verilir.

**#cd /usr/ports/www/squid/**

Kurulum seçeneklerini sorgulamak için;

**#make show=FLAVORS**
transparent snmp

Kurulum için;

**#env "FLAVOR=transparent" make install**

komutları verilir.

**NOT: /usr/ports/www/squid dizinideki Makefile dosyasi incelenerek Squid'in hangi secenekler ile kurulacagi belirlenebilir. CONFIGURE_ARGS+ ile baslayan satir Squid'in derleme seceneklerini belirtir.**

**Kurulum Sonrası genel yapılandırma**

Kurulum sonrasında Squid aşağıdaki dosyaları oluşturur:

Yapılandırma dosyaları **/etc/squid**
Örnek yapılandırma dosyaları /usr/local/share/examples/squid
Hata mesajları **/usr/local/share/squid/errors**
Örnek hata mesajları /usr/local/share/examples/squid/errors
Simgeler **/usr/local/share/squid/icons**
Örnek simgeler /usr/local/share/examples/squid/icons
Cache dizini **/var/squid/cache**
Log dizini **/var/squid/logs**
Squid kullanici ve grubu **_squid:_squid**

Kurulum sonrasında Squid'in hangi seçeneklerle kurulduğunu görmek için –v parametresi kullanılır.

**#squid -v**
Squid Cache: Version 2.5.STABLE9
***configure options:*** *--datadir=/usr/local/share/squid '--enable-auth=basic digest' '--enable-basic-auth-helpers=NCSA YP' --enable-digest-auth-helpers=password '--enable-external-acl-helpers=ip_user unix_group' '--enable-removal-policies=lru heap' --enable-ssl '--enable-storeio=ufs diskd' --localstatedir=/var/squid --enable-pf-transparent --prefix=/usr/local --sysconfdir=/etc*

Kurulum tamamlandıktan sonra **/etc/squid/squid.conf** dosyasında bazı değişiklikler yapılması gerekmekte.

Squid.conf dosyası herhangi bir editör ile açılarak aşağıdaki satırlar eklenmeli/değiştirilmelidir.

***http_port 127.0.0.1:3128***
***acl our_networks src 10.0.0.0/8***
***#10.0.0.0/8 benim local ağım, burayı kendinize göre düzenleyin***
***httpd_accel_host virtual***
***httpd_accel_port 80***
***httpd_accel_with_proxy on***
***httpd_accel_uses_host_header on***
***http_access allow our_networks***

Bundan sonra squid'in kullanacağı gerekli takas

dizinlerinini oluşturmak için **squid -z** komutu çalıştırılmalıdır.

**#/usr/local/sbin/squid -z**
2005/09/13 19:09:46| Creating Swap Directories

Squid'in sistemin her açılışında çalışmasını sağlamak için

**/etc/rc.conf** dosyasına
***squid=YES***

satırı eklenmeli . Ardından /etc/rc.local dosyasında **echo** "." Satırının ustune aşağıdaki satırlar eklenmeli.

```
  if [ -f /etc/squid/squid.conf ]; then
       if [ X"${squid}" = X"YES" -a -x /usr/local/sbin/squid ];
then
           echo -n ' squid';    /usr/local/sbin/squid
       fi
   fi
```

*Squid yapılandırma dosyasında yapılan değişikliklerin aktif olması için*

***#squid –k reconfigure***

Komutu verilmelidir.

**Squid Loglama mekanizması**

Squid tum loglarını 3 farklı dosyada tutar. Bunlar cache.log, access.log, store.log. Useragent.log ve referrar.log dosyalarıda seçimliktir ve access.log benzeridir fakat daha detayli bilgi icerirler.

**Cache.log :** Squid'in yapılandırma dosyasına ait hatalar, performans uyarıları gibi bilgiler içerir. Yapilandirma dosyasindaki cache_log anahtarı ile belirlenir.

**Access.log :** Bu dosya squid üzerinden yapılan her isteğin loglandığı dosyadır. Yapılandırma dosyasındaki cache_access_log yönergesi tarafından belirlenir.

**Store.log** :Cache'e eklenen nesneler için düşük seviye bilgi verir.

Squid her erişilen siteyi detaylı bir şekilde loglamaktadır. Squid'in oluşturduğu erişim logları gün

geçtikçe büyüyecektir bu da log dosyalarından rapor çıkarmayı zorlaştıracaktır. Squid'in logları günlük olarak döndürülürse(rotate) raporlama işi daha kolay ve düzenli yapılabilir.

Logları günlük döndürmek için /etc/daily.conf dosyasına aşağıdaki satırlar eklenmelidir.

```
if [ -x /usr/local/sbin/squid -a -f
/var/squid/logs/squid.pid ]; then
     /usr/local/sbin/squid -k rotate
fi
```

**Sorun giderme**

Squid beklediğiniz gibi çalışmıyorsa yapılandırma dosyasında hata yapmışsınızdır. Bu hatayı bulmanın en kolay yolu squid.conf'taki debug_options değerini artırmaktır.

**debug_options ALL,1 32,2**

Hata bulmanın bir diğer yolu da squid'i çalıştırırken tam debug modda çalıştırmaktır. Bunun için Squid'e –X parametresi verilir ve hatanın sebebi araştırılır.

**#squid –X**

**Firewall(PF) Ayarları**

OpenBSD Packet Filter kullanarak istemciden gelen istekleri Squid'e yonlendirmek için gerekli kurallar;

**NOT: OpenBSD Packet Filter hakkında detaylı bilgi için http://www.enderunix.org/docs/pf.pdf ve http://www.enderunix.org/docs/pf_tr.pdf adreslerinden faydalanılabilir.**

-----Pf.conf-----

```
ic_ag="x10"   #sizin ag arabiriminiz farkli olabilir
dis_ag="r10"

rdr on $ic_ag inet proto tcp from 10.0.0.0/8 to any port
www -> 127.0.0.1 port 3128

pass in on $dis_ag inet proto tcp from any to 127.0.0.1
```

*port 3128 keep state*

*pass out on $dis_ag inet proto tcp from any to any port www keep state*

*---pf.conf----*

gerekli kurallar eklendikten sonra

**#pfctl -f /etc/pf.conf**

komutu ile yeni kuralların aktif olması sağlanmalı.

Bundan sonra yapılacak iş Squid'in packet filteri sorgulayabilmesi için /dev/pf dosyasına erişim sağlamasını ayarlamak . /dev/pf dosyasının öntanımlı sahibi root dur. Squid ise **_squid/_squid** kullanici adi/grubu şeklinde çalışır. /dev/pf dosyasının grubunu, Squid okuyacak şekilde yapılandırmak için aşağıdaki komutlar verilmelidir.

**#chgrp _squid /dev/pf**
**#chmod g+rw /dev/pf**

**Eklenecekler:**

- FreeBSD Pf Squid Seffaf proxy kurulumu
- Linux Iptables Seffaf proxy kurulumu
- Squid acl kullanımı

**Kaynaklar:**

http://www.benzedrine.cx/transquid.html
http://ezine.daemonnews.org/200207/transpfobsd.html
http://www.averillpark.net/OpenBSD/FW-HowTo.html
$man pf
$man squid

Huzeyfe ÖNAL @ EnderUNIX
huzeyfe@enderunix.org