Squid

Çağrı Emer

Nisan, 2016

İçindekiler

1 Giriş

Squid, ilk sürümü 1996 yılında yayımlanan GNU GPL lisanslı özgür bir vekil sunucu/web önbelliğidir. C/C++ dilleri kullanılarak yazıldığından, her platformda çalışabilir. Duane Wessels'ın Ulusal Bilim Vakfı destekli nesne önbelleği projesinden türeyen Squid, günümüzde tamamen gönüllülerin çabalarıyla geliştirilmektedir. Proje, geliştiricileri lisans, altyapı vb. konularda desteklemek amacıyla kâr amacı gütmeyen Squid Yazılım Derneği'nin önderliğinde devam etmektedir.

Çokça yapılan istekleri belleyerek sayfa yüklenme süresini kısaltmaktan, DNS aramalarını hızlandırmaya kadar pek çok amaç için kullanılabilen Squid, genelde HTTP ve FTP için çalıştırılsa da HTTPS ve Gopher gibi protokolleri de destekler. Tarih itibariyle en güncel sürümü 3.2.6 olan Squid'in Ubuntu 12.04 LTS depolarındaki mevcut sürümü 3.1.19'dur. 3.1 serisindeki en güncel sürüm ise 9 Ocak 2013'te yayımlanan 3.1.23 sürümüdür. Squid'in bilinen büyük kullanıcıları arasında Wikipedia ve Flickr gibi siteler bulunmaktadır.

Oldukça kapsamlı yapılandırma ayarlarına ve pek çok meziyetlere sahip olan Squid'in üzerine yüzlerce sayfalık kitaplar yazılmış, onlarca saatlik eğitimler verilmiştir ve hâlâ da verilmektedir. Bu açıdan bakıldığında SUDO'daki kısıtlı alanda, kısıtlı vakitle yazılan bu yazı ancak temel ayarlara giriş düzeyinde kalacaktır. İleri düzey yapılandırmalar için okuyucuya yapılandırma referansı tavsiye edilir.[1]

Vekil sunucu, temelde istemci ile sunucu arasında oturarak, istemciden gelen istekleri sunucuya iletme ve sunucudan aldığı cevabı istemciye yönlendirme görevi yapar. Daha ileri düzeyde ise istemciden gelen istekleri, önceden tanımlanmış kurallara göre filtreleme, giden ya da gelen paket içeriklerini değiştirebilme gibi seçeneklere sahiptir. Squid bu sayılan özelliklere ek olarak çokça yapılan istekleri bellekleyerek o istekleri uzak bilgisayardan sunmaktansa yerel ağdan sunarak sayfa yüklenme zamanını kısaltma ve bant genişliğini optimum düzeyde kullandırma yeteneğine sahiptir. Bu özelliğe önbellekleme adı verilir.

Squid sunucu tarafında kullanıldığında -aslında bu ifade tam olarak doğru bir ifade değildir; aradaki farkı daha kolay anlatabilmek için kullanılmıştır- ters vekil "reverse proxy" olarak adlandırılır. Bu yöntem de normal vekil sunucuyla aynı çalışma prensibine sahiptir. Yoğun istekler hiç web sunucuya gitmeden önbellekten sunularak yük dağılımı ve sayfa yüklenme zamanının optimizasyonuna çalışılır.

[1] http://www.squid-cache.org/Doc/config/

2 Squid Yükleme

Ubuntu'ya Squid yüklemenin başka bir program yüklemekten farkı yoktur. Önce depoların durumu güncellenir ve ardından squid3 paketine istek yapılır. Bu işlemleri yapan iki komut artık çok iyi bilindiği üzere şöyledir:

```
1 sudo apt-get update
2 sudo apt-get install squid3
```

Paket depolarında bir de squid isimli bir paket bulunmakla birlikte bu paket squid3 isimli paketi gösteren -sahte- bir pakettir. Dolayısıyla komutta squid ya da squid3 demenin bir farkı olmayacak, iki paket de aynı sürümü kuracaktır. Paket kurulumunun ardından /etc, /usr/lib ve /usr/share/doc dizinleri altında bir /squid3 dizini oluşturulacaktır. Çalıştırılacak ikili dosya ise /usr/sbin altına squid3 adıyla kopyalanacaktır. Genel yapılandırma dosyası /etc/squid3 dizinindeki squid.conf dosyasıdır. /usr/lib/squid3 altına kopyalanan dosyalar genel olarak kimlik doğrulama mekanizmalarına ait küçük yardımcı programcıklardır.

3 Direktifler

squid.conf dosyasında kullanılabilecek temel olarak beş direktiften söz edilebilir. Bu direktifler yapılandırma dosyasının kurallarının yazımında kullanılacak direktiflerdir.

Tek değer alan direktifler
Adından da anlaşılacağı üzere bunlar tek bir değere sahip olabilen direktiflerdir. Eğer dosya içerisinde aynı direktif için birden fazla tanım yapılmışsa en sonda yapılmış olan geçerli olacaktır. Bu tip direktife örnek olarak pid_filename verilebilir.

```
1 pid_filename <dosya-yolu>
```

şeklinde tanımlanmakla birlikte squid sürecinin numarasını tutan dosya yolunu belirtir.

Açma kapama direktifleri
Bu tip direktifler "on" ya da "off" olacak şekilde iki değerden birini alabilirler. Örnek olarak log_uses_indirect_client verilebilir.

```
1 log_uses_indirect_client on
```

gibi tanımlanabilen bu direktif, vekil sunucuya gelirken arada başka noktalardan geçen paketlerin ne şekilde loglanacağını söyler.

Birden çok değer alabilen direktifler
Üçüncü genel direktif tipimiz yanına birden fazla değer alabilen direktiflerdir. Bu tip direktife örnek olarak dns_nameservers verilebilir.

```
1 dns_nameservers 8.8.8.8 8.8.4.4
```

şeklinde tanımlanan dns_nameservers, Squid'in DNS işlemleri için hangi sunucuları kullanacağını belirtir.

Zaman değeri alan direktifler
Yine adından da anlaşılacağı üzere bu tip direktifler değer olarak zaman birimlerini alırç Örnek olarak dns_timeout direktifi kullanılabilir.

```
1 dns_timeout 30 seconds
```

gibi yazılan dns_timeout direktifi, bir sorguya ne kadar süre içerisinde cevap gelmediğinde DNS sunucuların erişilemez olarak değerlendirilmesi gerektiğini belirtir.

Dosya ya da hafıza boyutu alan direktifler
Bu tip direktifler de kullanılacak dosyanın ya da hafızanın boyutunu değer olarak alır. Önbellek boyutunu ayarlayan cache_mem bu tip direktiflere bir örnektir. Kullanımına bir örnek şu şekildedir:

```
1 cache_mem 1024 MB
```

Genel olarak direktiflerin tanımı yapıldığına göre squid.conf dosyasında kullanılacak en önemli direktiflerden biri olan http_port'tan bahsedilebilir.

Squid kurulduğunda 3128 numaralı portu dinlemeye başlar. Eğer bu port dışında bir porttan çalışıtırılması gerekiyorsa kullanılması gereken direktif http_port'tur. http_port aşağıdaki gibi değerler alabilir:

```
1 http_port 8080
2 http_port 10.0.2.1:8080
3 http_port aggecidi.sirket.com:8080
```

Eğer birden fazla http_port direktifi kullanılmışsa, Squid, bu açılan portların hepsini dinleyecektir. http_port aynı zamanda dört adet mod değerinden birini alabilir. Modlar için alabileceği çeşitli seçenekler de vardır. Bu dört moddan en kafa karıştıran ikisi, benzer olduklarından, intercept ve tproxy modlarıdır. İkisi de transparan vekil sunucu olmakla birlikte intercept modunda istek yapılan sunucu Squid'in adresini görecek, tproxy modunda ise istemcinin adresini görebilecektir. Bunun için çekirdek desteği ve işletim sisteminin paketleri yönlendirebilme yeteneğinin olması gerekir. intercept ve tproxy modları kimlik doğrulamayı devre dışı bıraktığı için ilerleyen örneklerde kullanılmayacaktır.

4 Erişim kontrol listeleri

Squid'in bel kemiği olan erişim kontrol listeleri http_access ve benzeri direktiflerle kimin hangi kaynağa ulaşabileceğinin tanımlanmasına yarar. Her erişim kontrol listesinin bir tipi ve adı olmalıdır. Genel olarak şu yapıdadırlar:

```
1 acl <acl-adı> <acl-tipi> <değer>
2
3 acl sirketagi dstdomain sirket.com
```

Örneğin bir mesai saatleri içerisinde girişi engellenecek sitelerin adreslerini tutan bir dosya olsun. '/etc/squid3/yasakli_siteler.txt' Bu siteleri tanımlayan acl şu şekilde yazılabilir:

```
1 acl yasaklilar dstdomain '/etc/squid3/yasakli_siteler.txt'
```

acl için kullanılan isimler büyük küçük harf ayırımı olmaksızın çalışır. Birden çok yerde aynı acl adı kullanılmışsa bu kurallar birleştirilir. Fakat unutulmamalıdır ki bir acl birden fazla tipte kullanılamaz. Örneğin adı yasaklilar olan acl bir başka satırda src tipinde yazılmamalıdır.

Yasaklı siteleri tutan bir acl tanımlandığına göre artık bu direktif ile Squid'in ne yapması gerektiği söylenebilir. Bu işi görecek olan direktif http_access direktifidir. Genel olarak şu yapıda kullanılır:

```
1 http_access allow|deny [!] <acl-adı>
```

Yukarıdaki örnek için gereken hali ise şöyledir:

```
1 http_access deny yasaklilar
```

! işareti opsiyonel olmakla birlikte ile kapsanmayan tüm eşleşmeler için manasına gelir. Yani bir nevi "else" manasındadır.

Bütün acl kurallarından sonra diğer tüm erişimleri önlemek için en sonda aşağıdaki direktifin kullanılması önerilir:

```
1 http_access deny all
```

Bu sayede kurallar tarafından kapsanmayan tüm trafik engellenmiş olacaktır.

Şimdiye kadar acl'ler yardımı ile çeşitli erişim kurallarının nasıl tanımlanabileceği anlatıldı. Fakat bazı durumlarda sadece acl'ler yeterli olmayacak bir de kimlik doğrulama yapılması gerekecektir. Squid dört çeşit doğrulama şeması destekler. Bu yazıda "basic" olarak tanımlanan şemaya değinilecektir. Yapılandırması en kolay, fakat görece en güvensiz olan şema da basic şemasıdır. Bu şema ağdaki paketleri dinleyen birinin düz metin olarak kullanıcı adı ve şifrelere erişebilmesine imkan verdiğinden, küçük ve paket dinlenme riskinin az olduğu ya da olmadığı ağlarda kullanılması önerilir. Diğer üç sema "digest", "ntml" ve "negotiate" şemalarıdır. Detaylı bilgi için Squid referansına bakılmasında fayda vardır.

Basic şemasını kullanarak birkaç farklı method ile kimlik doğrulama yapılabilir. NCSA örnek olarak verilecektir. Bu kimlik doğrulama methodunda Apache htpasswd tarzı bir dosyadan kullanıcı adı ve şifreler okunacaktır. Dolayısıyla yapılması gereken önce bu özel formattaki dosyayı oluşturmak ardından da Squid'e bu dosyayı hangi yardımcı program ile okuyacağını söylemekten ibarettir. Bu kimlik doğrulama dosyasının /etc/squid3/squid-kullanicilari altında tutulacağı varsayılırsa;

```
1 htpasswd -cm /etc/squid3/squid-kullanicilari kullanıcı1
```

komutunun verilmesi kullanıcı1 için şifre soracak ve ardından md5 ile saklanmış şifreyi ve kullanıcı adını ilgili dosyaya yazacaktır. Sonraki kullanıcılar için -c parametresinin verilmesine gerek yoktur. Eğer verilirse dosya sıfırdan yaratılacak ve önceden tanımlanmış kullanıcılar silinecektir.

NCSA kimlik doğrulaması için kullanılacak yardımcı program Ubuntu'da /usr/lib/squid3/ncsa_auth yolunda bulunmaktadır. Dolayısıyla yapılandırma dosyasına verilecek satırlar şöyle olmalıdır:

```
auth_param basic program /usr/lib/squid3/ncsa_auth /usr/squid3/squid-kullanicilari
auth_param basic utf8 on
auth_param basic realm Squid Vekil Sunucu
acl authenticated proxy_auth REQUIRED
http_access allow authenticated
http_access deny all
```

Bunun dışında bakılabilecek children, credentialsttl, casesensitive gibi ayarlar da vardır. Özellikle çok sayıda kullanıcıya sunulacak bir hizmetse children önemli olacaktır. Squid sunucu yeniden başlatıldığında artık kimlik doğrulaması gerektirecektir. Bu işlemler ardından yapılması gereken tek şey, istemcilere ait bilgisayarlarda bulunan tarayıcıların proxy ayarlarını doğru şekilde düzenlemektir.

Umarım yazı basit ihtiyaçları görebilecek bir vekil sunucunun nasıl kurulacağını ve nasıl yapılandırılacağını anlatmaya yeterli olmuştur. Bu temel bilgiler sayesinde daha karmaşık yapılandırmalar için Squid referans dokümanının anlaşılması çok daha kolay olacaktır.

5 Kaynak: