

Squid, Dansguardian, Iptables ve Webmin Kurulumu

Furkan Çalışkan

Temmuz, 2007

İçindekiler

1	Squid	2
1.1	Kurulum ve Ayarlar	2
1.2	Kullanımı	3
1.2.1	Squid'in Çalıştırılması ve Durdurulması	3
1.2.2	Erişim Kontrol Listeleri (Access Control Lists) Hakkında	3
1.2.3	Log Takibi	4
2	Dansguardian	4
2.1	Kurulum ve Ayarlar	4
2.2	Dansguardian'ın Çalıştırılması	5
2.3	Filtrelerin İşlenmesi	5
2.4	Log Takibi	5
3	Iptables	5
3.1	Kurulumu	6
3.2	Temel Kullanımı	6
4	Webmin	7
4.1	Kurulumu	8
4.2	Webmin'in Temel Kullanımı	8
5	Webmin'e Dansguardian Modülünün Kurulması	9

1 Squid

1.1 Kurulum ve Ayarlar

Öncelikle www.squid-cache.org adresinden squid programının kaynak kodlarını indiriyoruz. Ben kurulum sırasında programın squid-2.6.STABLE13 sürümünü¹ kullanacağım. Dosyayı indiriyoruz, indirdikten sonra sıkıştırılmış dosyayı açıyoruz ve konsoldan açtığımız klasöre girip sırasıyla;

```
groupadd squid
useradd -d /usr/local/squid -g squid squid
./configure
make
make install
```

komutlarını veriyoruz. Bu komutlarla gerekli grup ve kullanıcı oluşturma işlemlerini yapıp squid'i sistemimize kurduk. Sıra geldi gerekli konfigürasyonlara. Squid'in konfigürasyon dosyasının adı *squid.conf*'tur. Standart bir kurulum yapmış iseniz bu ayar dosyası */etc/squid/squid.conf* konumunda² bulunacaktır. Ayar dosyamızı herhangi bir editör ile açıp gerekli düzenlemeleri yapmaya başlıyoruz;

Öncelikle *squid.conf* dosyamızda *http_port 3128* satırının bulunduğundan ve önünde # işaretinin olmadığından emin oluyoruz. Bu işlemden sonra hata mesajlarını Türkçe alabilmek için *error_directory /usr/lib/squid/errors/Turkish* satırını ayar dosyamıza ekliyoruz. Dosyada yapmamız gereken diğer değişiklikler ise şu şekilde;

```
cache_dir aufs /var/spool/squid 1000 16 256 (cache belleği belirleme satırı olup 1000 rakamı MB cinsinden cache'lenecek veriyi temsil etmekte)
```

```
"visible_hostname hostadı" (Sunucuya vereceğimiz isim)
```

```
acl agimiz src 10.0.0.0/255.0.0.0 (Ağımızı tanımlıyoruz)
```

```
http_access allow agimiz (Bu satırla proxy server'ımıza tüm isteklere izin verdiriyoruz.)
```

¹<http://www.squid-cache.org/Versions/v2/2.6/squid-2.6.STABLE13.tar.gz>

²Dosyanın bulunduğu dizini konsoldan vereceğiniz *locate squid.conf* ile bulabilirsiniz.

1.2 Kullanımı

1.2.1 Squid'in Çalıştırılması ve Durdurulması

Squid'i konsoldan `/sbin/service squid start` yazarak başlatabilirsiniz. Yine tahmin edilebileceği gibi `/sbin/service squid stop` squid'i durdurur ve `/sbin/service squid restart` squid'i yeniden başlatır.

1.2.2 Erişim Kontrol Listeleri (Access Control Lists) Hakkında

Herhangi bir kullanıcıya/kullanıcı gruplarına ait kısıtlamaları erişim kontrol listeleri (ekl) ile sağlayabiliriz. Bu listelere ait kuralları `squid.conf`'un içine, ilgili bölüme yazabiliriz. squid, ayar dosyasını yukarıdan aşağıya incelediğinden dolayı burada dikkat edilmesi gereken izin verilmeyecek bir bağlantının altında ona benzer ve izin verilen bir bağlantının bulunmaması gerektirir.

Erişim Kontrol Listeleri Seçenekleri

src ip—adresi ağ-maskesi	İstemcinin ip adresi
src adr1—adr2 ağ-maskesi	Adres aralığı
dst ip—adresi ağ-maskesi	Hedef ip adresi
myip ip-adresi ağ-maskesi	Yerel socket ip adresi
srcdomain etki alanı	Ters arama, istemci ip'si
srcdom_regex [-i] deyim	İstemci adıyla eşleşen regular expression
dstdom_regex [-i] deyim	Hedefle eşleşen regular expression
url_regex [-i] deyim	URL'nin tamamıyla eşleşen regular expression
port portlar	Bir port yada port aralığını belirler
proto protokol	HTTP veya FTP gibi bir protokol belirler
method metot	GET ve POST gibi metotları belirler.

Örnek: Audio/Video İndirilmesinin Yasaklanması Server'dan audio ve video indirilmesinin yasaklanabilmesi için `squid.conf`'a yazılması gereken satırlar şu şekildedir;

```
acl BlockExt url_regex -i /.mp3$ /.asx$ /.wma$ /.wmv$ /.avi$ /.mpeg$ /
.mpg$ /.qt$ /.ram$ /.rm$ /.iso$ /.wav$ /.exe$ (Bu kısım ACL bölümünün
alt kısmına girilecek) http_access deny BlockExt all (Bu kısım http_access
bölümünün üstüne girilecek)
```

Konu ile ilgili kullanılabilecek tüm komutlar `squid.conf`'un içinde açıklamalarıyla beraber bulunmaktadır.

1.2.3 Log Takibi

Squid çalışır olduğu zamanlarda tüm işlemleri `access.log` adı altında bir dosyaya kaydeder. Bu dosya standart kurulumda `/var/log/squid/access.log` konumunda bulunur. `tail -f /var/log/squid/access.log` komutuyla proxy'nin işleyişini dinamik olarak görebilirsiniz.

2 Dansguardian

Dansguardian bir içerik filtreleme (content-filtering) yazılımıdır. Squid ile entegre çalışabilir ve internetten gelecek tehlikelere karşı kullanıcıları korur. Ayrıca yine dansguardian ile kullanıcılara bir takım kısıtlamalar sağlanabilir. Programla gelen karalisteler(blacklist) kullanıcıları internetteki zararlı içeriklerden korur.

2.1 Kurulum ve Ayarlar

Kurulum için öncelikle dansguardian programının son sürümünü üreticinin sitesinden (<http://www.dansguardian.org>) indiriyoruz. Bu belge boyunca ben 2.9.8.0 sürümünü kullanacağım. İndirme işleminden sonra `tar.gz` uzantılı dosyayı bir klasöre açıp konsol ile aşağıdaki komutları veriyoruz;

```
./configure  
make  
make install
```

Bu işlemten sonra dansguardian kurulumumuz bitmiştir. Eğer kurulum ayarlarını varsayılan olarak bıraktıysak program `/usr/local/share/dansguardian/` konumunda, genel ayar dizini ise `/usr/local/etc/dansguardian/` konumunda bulunacaktır.

Şimdi programın ayarlamalarına geçelim. Ayarlar için genel ayar dizininden `dansguardian.conf`'u açıyoruz. Ayarlamalarda aşağıdaki kriterleri göz önüne alıyoruz.

```
filterip= Dansguardian'ın çalışacağı ip adresi yazılacak.  
filterport= 8080 (Buraya Dansguardian'ın çalışacağı port yazılacak)  
proxyip= 127.0.0.1 (Buraya Squid kurulu ise çalıştığı IP adresi yazılacak)  
proxyport= 3128 (Buraya Squid'in çalıştığı port yazılacak)
```

Dansguardian'ı squid ile beraber çalıştıracaksak ayrıca `dansguardian.conf`

dosyasına `authplugin='/usr/local/etc/dansguardian/authplugins/proxy-basic.conf'` satırını eklememiz gerekiyor.

2.2 Dansguardian'ın Çalıştırılması

Kurulum işlemi sorunsuz tamamlanmış işe konsoldan `dansguardian start` diyerek dansguardian'ı çalıştırabiliriz. Dansguardian'ın çalışıp çalışmadığını anlamak için ise yazmamız gereken komut ise `ps aux | grep dansguardian` olacaktır.

2.3 Filtrelerin İşlenmesi

Dansguardian'ın site kontrol listeleri standart kurulumda `/usr/local/etc/dansguardian/lists` altındadır. Bunlar şu şekildedir;

authplugins, bannedurllist, exceptionmimetyplist, greyurllist
bannedextensionlist, blacklists, exceptionphraselist, phraselists, bannediplist
contentregexplist, exceptionregexpurllist, pics, bannedmimetyplist
downloadmanagers, exceptionsitelist, urlregexplist, bannedphraselist
exceptionextensionlist exceptionurllist, weightedphraselist, bannedregexpurllist, exceptionfilesitelist, filtergroupplist, bannedsitelist, exceptioniplist, grey-sitelist

Bunlardan autplugins, blacklists, downloadmanagers, phraselists yine kendi içlerinde birer klasördürler ve içlerinde çeşitli filtre listeleri vardır.

2.4 Log Takibi

Dansguardian'ın log takip dosyaları `/var/log/dansguardian/access.log` konumunda kayıt altında tutulur. Gerekli takipleri buradan yapabilirsiniz.

3 Iptables

iptables, çekirdek içerisinde yer alan Netfilter sistemini denetlemek amacıyla kullanılan araçtır. Bir linux firewall'ı kurma işleminin temelinde iptables mantığı yatar. Iptables belirlediğimiz bir kaynağa giden yada belirlediğimiz bir kaynaktan gelen, paketler olarak hareket eden ağ trafiğini isteklerimize bağlı olarak onaylayan yada reddeden bir dizi kurallar dizisi tanımlamamıza imkan tanır. Bu kurallar dizisi doğru kullanıldığı takdirde son derece karmaşık ve güçlü bir güvenlik sağlar.

3.1 Kurulumu

Kurulumu yapmak için öncelikle <http://www.netfilters.org/downloads.html> adresinden iptables programının tar.bz2 formatlı kaynak kodu paketini³ çekiyoruz. Zipli dosyayı istediğimiz bir yere açıp konsolda açtığımız klasöre girerek sırasıyla;

```
/bin/sh -c make  
/bin/sh -c make install
```

komutlarını veriyoruz. Kurulum işlemi bittikten sonra `iptables -V` yazarak kurulumu kontrol ediyoruz. Bir hata ortaya çıkmıyorsa kurulum tamamdır. Eğer “*command not found*” benzeri bir hata alırsanız `cp ./iptables /sbin` komutunu deneyin.

3.2 Temel Kullanımı

O an iptables’ın uyguladığı kurallar listesini konsoldan `iptables -L` yazarak görüntüleyebilirsiniz. Kuralların uygulanabileceği değişik yerler vardır. Bu yerler chain (zincir) olarak tanımlanırlar.

- INPUT: Input(girdi) zinciri kuralları ağdan alınan paketlere uygular.
- OUTPUT: Output(çıktı) zinciri kuralları ağdan çıkan paketlere uygular.
- FORWARD: Forward(yönlendirme) zinciri kuralları aldığı fakat kullanmadan yönlendireceği paketlere uygular.
- PREROUTING: Gelen paketlerin yönlendirilmesi ve değiştirilmesi için kurallar (sadece NAT tablosu içindir)
- POSTROUTING: Giden paketlerin yönlendirilmesi veya değiştirilmesi için kurallar (sadece NAT tablosu içindir)

Kuralların nerde uygulandığından bağımsız olarak üç çeşit etkileri vardır. Bunlar;

- ACCEPT: Bu seçenek verilen bir paketi kabul eder ve içeri yada dışarı geçişine izin verir.
- DENY: Bu seçenek verilen bir paketin geçişine izin vermez ve yollanma bir hata mesajı döndürür.

³Bu belgeyi hazırlarken 1.3.8 versiyonunu kullandım

- DROP: Bu seçenek gelen paketi yollayanına bir hata mesajı vermeden görmezden gelir/geçişine izin vermez.
- REJECT: Erişimi reddeder ve gönderene bildirir.
- QUEUE: Paketleri kullanıcı alanına gönderir.
- RETURN: Zincirin sonuna atlar ve paketi varsayılan hedefin işlemesine izin verir.

Şimdi olayı biraz daha iyi anlatılabilmek için birkaç örnek yapalım.

```
iptables -A INPUT -s 200.200.200.1 -j DROP
```

Bu ifade 200.200.200.1'den gelen tüm paketleri gözardı eder ve içeri almaz. -s ile belirtilen parametre source(kaynak)'a karşılık gelmektedir ve istenirse buraya bir ip yerine bir ip aralığı da yazılabilir. (Örn: 200.200.200.1/24 gibi) Yine istenirse -s yerine -mac-source parametresi kullanılarak belirli bir mac adresine sahip bir makineden gelen paketlere kurallar konabilir.(Örn: 00:0B:DB:4F:37:42 gibi)

```
iptables -A INPUT -j DROP -p tcp --destination-port telnet
```

Yukarıdaki komut ise telnet portuna gelen tcp paketlerini görmezden geliyor. İstenirse belirli bir arabirime gelen/arabirimden giden paketlere de filtre koyulabilir.

```
iptables -A INPUT -j DENY -p tcp -i eth1
```

Yukarıdaki komut eth1'e gelen tcp paketlerini reddediyor.

Daha ayrıntılı kullanımlar ve ekstra parametreler yine iptables dökümantasyonunda bulunabilir.

4 Webmin

Webmin unix tabanlı sistemlerin yönetimi için perl ile yazılmış açık kaynak kodlu web tabanlı bir yazılımdır. Web tabanlı olduğundan uzaktan yönetimi oldukça kolaydır. Standart olarak TCP10000. porttan çalışır.

4.1 Kurulumu

Öncelikle <http://www.webmin.com/download.html> adresinden webmin'in son sürümünün⁴ kaynak kodlarını⁵sıkıştırılmış formatta indiriyoruz. Daha sonra root hakları ile sıkıştırılmış dosyayı açıp konsoldan klasöre giriyoruz ve;

```
./setup.sh /usr/local/webmin
```

komutuyla kurulumu başlıyoruz. Webmin bize bir takım sorular soracak;

Config file directory: Ayar dosyalarının nerede tutulacağı

Log directory: Günlük dosyalarının nerede tutulacağı

Full Path to Perl: Sistemde kurulu Perl'in tam yolu

Operating system type: İşletim sistemimizin türü

Web server port: Webmin'in çalışmasını istediğimiz port

Web server login and password: Giriş için gerekli kullanıcı adı ve şifre ayarları

Web server host name: Webmin'in çalışacağı makinenin adı

Start webmin at boot time: İşletim sistemi destekliyse webmin'in otomatik başlatılıp, başlatılmayacağı.

Bu sorulara çıkan yardımcı bilgiler doğrultusunda sistemimize ve isteğimize bağlı olarak cevaplar veriyoruz.

4.2 Webmin'in Temel Kullanımı

Webmin'i sorunsuz kurduğumuzu varsayarak devam ediyorum. Webmin'i açmak için tarayıcımızı açıp adres satırına `https://hostadı:10000` yazıyoruz ve başlangıçta belirlediğimiz şifreleri buraya yazarak giriş yapıyoruz. Öncelikle göze hoş gelen bir tema ve dil olarak Türkçe'yi seçiyoruz. Bu işlem Webmin>Dil ve Tema değiştir penceresinden yapılabilir. Buradan dili Türkçe temayı ise MSC Linux Theme olarak seçiyoruz.

Şimdi artık Webmin'e ait tüm işlemleri üst menüden yapabiliriz. Burada özellikle *sunucular* sekmesi önemli ve bizi ilgilendiriyor. Buradan sistemimizde

⁴Dökümanın yazılması sırasında son sürüm 1.350'idi.

⁵Sitede sadece kaynak kodlar değil .rpm, .deb formatta paketler de var, onları da kullanabilirsiniz fakat biz kaynaktan kurulumu tercih ediyoruz.

kurulu servisleri kontrol edebiliyor, onları başlatıp durdurabiliyor, sağladıkları imkanları görsel olarak sonuna kadar kullanabiliyor ve log kayıtlarını inceleyebiliyoruz.

5 Webmin'e Dansguardian Modülünün Kurulması

Standart olarak webmin sisteminizde dansguardian önceden kurulu olsa bile onu tanıyamaz. Bu sebeple dansguardian'ı webmin'e tanıtabilmek, sağladıklarından webmin arabirimi ile faydalanabilmek için *DansGuardian Webmin Module* adlı modülü webmin'e tanıtmak zorundayız. Bu tanıma işlemi oldukça basit. Öncelikle <http://puzzle.dl.sourceforge.net/sourceforge/dgwebminmodule/dg-0.5.10-pr5.wbm> adresinden ilgili modülü indiriyoruz. Daha sonra webmin arabirimini açıp anasayfadan Webmin Yapılandırması>Webmin Modülleri yolunu takip ederek modül kurulum penceresine geliyoruz. Buradan *Yüklenen Dosyadan*'ı seçip *Gözet*'a basarak indirdiğimiz modül paketimizi seçiyoruz ve *Dosyadan Modülü Kur* butonuna basıyoruz. İşlem tamam. Artık Webmin menüsünden Sunucular'a basarak ve akabinde çıkan menüden Dansguardian'ı seçerek normalde konfigürasyon dosyasını düzenleyerek yaptığımız gerekli ayarlamaları görsel olarak da yapabiliriz.

Kaynaklar

- [1] *Starting Squid - Squid User's Guide* http://www.deckle.co.za/squid-users-guide/Starting_Squid
- [2] *Squid ile Web Erişim Kontrolü - Lapis Wiki* http://wiki.linux-sevenler.org/index.php/NASIL:_Squid_ile_Web_Erisim_Kontrolu
- [3] *Dansguardian Kurulumu ve Yapılandırma Belgesi - Lapis Wiki* http://wiki.linux-sevenler.org/index.php/Dansguardian_Kurulumu_ve_Yapilandirma_Belgesi
- [4] *Installing and Configuring iptables* <http://www.cae.wisc.edu/site/public/?title=liniptables#iptables>
- [5] ALTIN, Enver. *IPTables/Netfilter nasıl çalışır?* <http://enveraltin.com/blog/iptables.html>