Iptables ile p2p Trafik Algılama Yolları

Linux, Iptables ile beraber , network yönetimi konusunda bizlere eşsiz imkanlar sunmakta. Iptables , birbirinden bağımsız yürütülen açık kaynak kodlu projeler ile de kabiliyetlerini genişletebilen modüler bir yazılımdır. Herşeyden önemlisi ,ücretsiz olan bu yazılım ile yüksek meblağlar ödenerek kurulacak sistemleri, sadece uygun sunucu ve kaliteli ağ kartları ile çözerek, büyük tasarruf sağlayabiliyoruz. Bu çerçevede kampüs ağlarında karşımıza çıkan p2p trafiğini yönetebilme sorununa iptables ile getirilebilen çözümlerden, test ettiğimiz ve halen faal kullandığımız iki tanesini sizlerle paylaşmak istiyorum.

Layer 7 Classifier kurulumu:

L7 Classifier iptables projesinden bağımsız geliştirilen bir iptables modülüdür. Bu modül sayesinde iptables geçen paketlerin içeriğini algılayabilme kabiliyeti kazanmaktadır. Bu sayede bizlere port bağımsız çalışan protokollerin trafiklerini şekillendirebilme fırsatını verir.Açıkçası zahmetli bir derleme prosedürü olmasına rağmen birkez kurulduktan sonra olası güncellemeler için bu prosedürün tekrarlanmasına gerek yoktur. Zira L7 paket tanımları text dosyaları halindedir ve bunların güncellenmesi yeni protokollerin tanımlanması için yeterlidir.

Kurulum için gerekenler;

Linux çekirdeği 2.4 ya da 2.6	ftp://ftp.ulakbim.gov.tr/linux/kernel
Iptables kaynak kodu	http://www.netfilter.org/projects/iptables/
L7 patch paketi ve tanımları	http://sourceforge.net/project/showfiles.php?group_id=80085

Not : Şu andaki L7 kodu 2.6.14 çekirdeği ve iptables 1.3.3 için uygun. Iptables için daha yeni sürümlerde problem yaratmamakla beraber linux çekirdeğinin daha yeni versiyonlarında patch uygulandıktan sonra Kconfig dosyasında manuel ayar yapmak gerekiyor.

İndirdiğimiz linux çekirdeğini /usr/src dizinine kopyalayalım ve açalım.

```
cp linux-2.6.14.tar.bz2 /usr/src
cd /usr/src
tar jxvf linux-2.6.14.tar.bz2
```

L7 patch kodunu aynı dizine kopyalayalım , açalım ve içindeki uygun patch çekirdek kodunun dizinine kopyalalım.

```
cp netfilter-layer7-v2.1.tar.gz /usr/src
cd /usr/src
tar zxvf netfilter-layer7-v2.1.tar.gz
cp netfilter-layer7-v2.1/kernel-2.6.13-2.6.15-layer7-2.1.patch  linux-2.6.14/
```

Simdi kopyaladığımız patchi koda uygulayalım.

```
cd linux-2.6.14/
patch -p1 <  kernel-2.6.13-2.6.15-layer7-2.1.patch
```

Çekirdeğimiz konfigurasyon için hazır.Eğer gateway olarak kullandığınız bir makinada kurulum yapıyorsanız hazırda kullanılan ayarlarınızı kullanabilirsiniz. Bunun için;

```
make oldconfig
```

yazmanız yeterli.Komutu yazdıktan sonra kullanılan ayar dosyasında olmayan veya yeni eklenmiş opsiyonlar size sorulacaktır. Bunları dikkatle okuyun ve eğer bir fikriniz yoksa enter ile geçin.L7 patchinden sonra ,bu prosedür sırasında size sorulacak sorular arasına ;

Layer 7 match support

eklenecektir.Buna “Yes” deyin.Ayrıca ;

Code maturity level options → Prompt for development and/or incomplete code/drivers

Device Drivers → Networking support → Networking Options → Network packet filtering
Network packet filtering → IP: Netfilter Configuration → Connection tracking
Network packet filtering → IP: Netfilter Configuration → Connection tracking flow accounting
Network packet filtering → IP: Netfilter Configuration → IP tables support

Mutlaka “Yes” olmalıdır.

Eğer çekirdeğini hazırdaki konfigurasyonunuz ile değil yepyeni bir konfigurasyon ile ayarlamak isterseniz;

```
make menuconfig
```

ile karşınıza gelecek olan konsol tabanlı arayüz ile uygun ayarları yapınız ve yukarıda yazılı seçenekleri işaretlemeyi unutmayınız.
Konfigurasyon işlemi bitince:

```
make bzImage && make modules && make modules_install && make install
```

Bu uzun işlemler zinciri sonucunda , herşey yolunda gittiyse makinenizde yeni çekirdeğiniz (/boot dizini altında) ve ayarlı bir önyükleyiciniz (/etc/grub.conf) olmalı.Artık yeni çekirdeğimiz ile makinemizi başlatabiliriz.

Sunucumuzu yeni çekirdek ile başlattıktan sonra , iptables kaynak kodunu /usr/src ye kopyalayalım.

```
cp iptables-1.3.3.tar.bz2 /usr/src
cd /usr/src
tar jxvf  iptables-1.3.3.tar.bz2
```

L7 patch paketindeki iptables yamasını iptables kaynak dizinine kopyalayalım ve uygulayalım.

```
cp  netfilter-layer7-v2.1/iptables-layer7-2.1.patch /usr/src/iptables-1.3.3
cd /usr/src/iptables-1.3.3
patch -p1 <  iptables-layer7-2.1.patch
```

Iptables derlenmeye hazır. Eğer sistemimizde kurulu bir iptables varsa bunu daha önce kaldırmamız faydalı olacaktır.

```
chmod +x extensions/.layer7-test
make KERNEL_DIR=/usr/src/ linux-2.6.14
make install KERNEL_DIR=/usr/src/ linux-2.6.14
```

Iptables derlendi ve sisteme kuruldu.Şimdi yapmamız gereken işlem ,tanımlama dosyalarını uygun tere koymak.

```
tar zxvf l7-protocols-2006-04-09.tar.gz
cd  l7-protocols-2006-04-09/
make install
```

Kurulum işlemi tamamlanmıştır.Kurulumunuzu şu şekilde test edebilirisiniz.

```
modprobe  ipt_layer7
iptables -A OUTPUT  -m layer7 --l7proto http -j LOG –log-prefix=***http***
```

Bu komuttan sonra makinenizden dışarıya yaptığınız http trafiği /var/log/messages dosyasında loglanmalıdır. Artık ihtiyaçlarınız doğrultusunda iptables konfigurasyonunuzu özelleştirebilirsiniz.

Örneğin basitçe yönlendirilen Ares p2p trafiği kesmek için;
```
iptables -A FORWARD -m layer7 --l7proto ares -j DROP
```

Ya da tc ile hız kontrolü yapabilmek amacıyla bittorrent paketlerini işaretlemek için;
```
iptables -t mangle -A POSTROUTING -m layer7 --l7proto bittorrent -j MARK --set-mark 3
```

Ipp2p kurulumu:

L7 classifier dan farklı olarak ipp2p projesinin tek amacı p2p trafiği yakalamaktır. L7'nin p2p haricinde tanımlayabiliği birçok protokol olmasına rağmen ipp2p sadece p2p eşler.Ayrıca ipp2p sadece TCP paketleri yakalar. O nedenle UDP protokolü kullanan paylaşım programları yakalayamaz.Olası güncellemeler için ipp2p in tekrar derlenmesi gerekir. Ipp2p de L7 gibi iptablestan bağımsız bir modüldür.Kurulumu L7 ye göre daha kolaydır.

Kurulum için gerekenler;

Ipp2p in en son versiyonu	www.ipp2p.org
Linux çekirdeği 2.4 ya da 2.6	ftp://ftp.ulakbim.gov.tr/linux/kernel
Iptables kaynak kodu	http://www.netfilter.org/projects/iptables/

Eğer sisteminizde hazırda kurulu bir iptables çalışıyorsa, aynı versiyonun kaynak kodunu indirmeniz yeterlidir. Ayrıca ipp2p i derleyebilmek için kullandığınız çekirdeğinizin header dosyalarının sisteminizde bulunması lazım. Eğer Yukarıda anlattılan gibi yeni çekirdek derlemiş iseniz bu `/usr/src/linux-2.6.14` dizinidir.Eğer kayanak çekirdek kaynak kodlarınız yoksa bu genelde (Suse , Redhat ve türevi sistemler için) kurulum cd lerindeki development paketlerinde bulunur.Debian tabanlı bir sistemde ise `apt-get install linux-headers-386` komutu ile kurulabilir.

Ipp2p modülünü L7 kurulumunun devamı olarak kurduğumuzu varsayarak , derleme için ipp2p paketinin açalım ve içine girelim.

```
tar zxvf ipp2p-0.8.1_rc1.tar.gz
cd ipp2p-0.8.1_rc1
```

Şimdi derlemeyelim.

```
make KERNEL_SRC=/usr/src/linux-2.6.14 IPTABLES_SRC=/usr/src/iptables-1.3.3
```

Herşey yolunda giderse bulunduğumuz dizinde iki adet önemli dosya elde ederiz.Birisi `ipt_ipp2p.ko` , diğeri `libipt_ipp2p.so` dur.Bunları sistemimizdeki uygun yerelere kopyalamamız lazım.Bu işlem kullandığınız sisteme göre değişiklik gösterir.

libipt_ipp2p.so dosyasını iptables kütüphanelerinin olduğu klasöre kopyalayalım.

```
cp libipt_ipp2p.so /usr/local/lib/iptables/
```

ipt_ipp2p.ko dosyasını netfilter modüllerinin olduğu klasöre kopyalayalım.

```
cp ipt_ipp2p.ko /lib/modules/2.6.14/kernel/net/ipv4/netfilter
depmod -a
```

Kurulumumuz tamamlandı. Kurulumumuzu denemek için;

```
modprobe ipt_ipp2p
iptables -m ipp2p –help
```

Karşımıza ipp2p kullanımı ile ilgili küçük bir kılavuzun gelmesi lazım. Eğer bunu görebiliyorsanız kurulumuz sorunsuz tamamlanmıştır.

Ipp2p kullanımı L7 den çok farklı değildir. Yönlendirilen p2p trafiği kesmek için basitçe;

```
iptables -A FORWARD -m ipp2p --ipp2p -j DROP
```

komutu yeterlidir.Protokolleri ayrı ayrı kullanmak için (örneğin kazaa);

```
iptables -A FORWARD -m ipp2p --kazaa -j DROP
```

Yada trafik şekillendirmek üzere işaretlemek için;

```
iptables -A PREROUTING -p tcp -m ipp2p --ipp2p -j MARK --set-mark 1
```

Performans:

Ipp2p UDP trafiği yakalayamadığı için en başından başarı yüzdesi düşüyor.Ancak L7 ye göre kıyaslanmayacak şekilde kaynakları tutuumlu kullanıyor. L7 paketleri yakalama konusuna çok daha başarılı ve güncellenmesi kolay olmasına rağmen sistem kaynaklarını bazen fazlasıyla kullanabiliyor. Ayrıca son sürümündeki (v2.1) bir problemden dolayı büyük paketleri bazen işleme sokmuyor.

Sistemimizde yaptığımız testlerde L7 ile logladığımız paketleri aynı zamanda ipp2p ile de logladık.Iptables counterlarını ise “iptables -nvxL” ile izledik. L7 nin ipp2p in 7-8 katına kadar daha fazla p2p trafik yakaladığını gördük.

Kaynaklar:

http://www.ipp2p.org

http://www.kernel.org

http://www.netfilter.org

http://l7-filter.sourceforge.net

Hazırlayan:

Volkan Oransoy

oransoy_v@ibu.edu.tr

Abant İzzet Baysal Üniversitesi

Bilgi İşlem Daire Başkanlığı - BOLU

Tarih : 02/05/2006