Pardus ve NfSen ile Yönlendirici Netflow Kayıtlarının İncelenmesi

Murat SOYSAL
Ulak-CSIRT
msoysal@ulakbim.gov.tr
TÜBİTAK-ULAKBİM

Özet
Bu belgede ağ yönlendirici cihazlarının oluşturduğu ve üzerinden geçen trafiğe ait izleri barındıran NetFlow kayıtlarının depolanması ve incelenebilmesi için yapılması gerekenleri adım adım anlatacağız. Bu kayıtların tutulması ağımızdan dışarı çıkan trafiğin kaynak ve hedeflerinin belirlenmesi konusundaki hukuki sorumlulukları karşılama da yardımcı olacaktır. Ayrıca kurulumunu anlatacağımız NfSen ile de bu kayıtların detaylı analizini bir arayüz yardımıyla yaparak ağ trafiğinizi inceleyebilirsiniz.

Giriş
Adım adım yapılması gerekenlere geçmeden önce NetFlow datasının ne olduğunu açıklayalım:

Cisco tarafından geliştirilmiş açık bir protokol olan NetFlow, IP trafiği kayıtlarının toplanmasını sağlar. NetFlow kayıtları 5 temel içerikten oluşur: Kaynak IP adresi, hedef IP adresi, kaynak kapısı (PORT) ve hedef kapısı (PORT) ve protokol.

Örnek Kayıt:

Sif	SrcIPaddress	DIf	DstIPaddress	Pr	SrcP	DstP	Pkts	Octets	B/Pk	Ts	Fl
00c7	193.140.21.18	00fd	88.239.42.161	06	50	446	1	464	464	00	19

Burada *Sif* trafiğin geldiği arayüzün (interface) yönlendirici üzerindeki tanımlayıcısıdır. Aynı şekilde *Dif* de trafiğin yönlendirildiği arayüzün tanımlayıcısıdır. *Pr* trafiğin kullandığı protokolü göstermektedir. (6 - > TCP) Diğer alanlarda IP başlık bilgisinde elde edilen bilgilerdir. Ayrıca trafiğin başlangıç ve bitiş zamanlarına da NetFlow kayıtlarından ulaşılabilir.

A) Netflow Kayıtlarının Oluşturulması ve Bir PC'ye Yönlendirilmesi İçin Yapılması Gerekenler

Yönlendirici cihaza bağlanıp enable moduna geçtikten sonra:

Router#conf t
Router(config)#
Router(config)#ip flow-export version 5 origin-as
Router(config)#ip flow-export destination 192.168.1.10 9996

komutları ile NetFlow beşinci nesil flow kayıtlarının 192.168.1.10 nolu

makinanın 9996 nolu kapısına yönlendirilmesini sağladık. Şimdi hangi arayüzlerden geçen trafiğin kayıt altına alınacağı belirtmek için ilgili arayüzün altına gidip :
Router(config)#interface FastEthernet0/0
Router(config-if)#ip route-cache flow

Önemli Not: Bu analizlerin yapılacağı bir çok ağda yönlendirici ile kayıtların tutulacağı makine (örneğimizde 192.168.1.10 IP'li) arasında ateş duvarı (firewall) olduğunu düşünmekteyiz. Bu durum sizin ağınız için de geçerli ise, yönlendiricinizin iç ağa bakan arayüzünün IP'sinden kaynaklı ve hedefi kayıtların tutulacağı makinanın yönlendirici ayarlarında girilen kapısı olan UDP trafiğine izin vermeniz gerekmektedir.

Bizim örneğimiz için yönlendiricinin iç ağa bakan arayüz Ipsi kaynaklı 192.168.1.10:9996 hedefli trafiğin geçişine izin verilmelidir.

B) Netflow Kayıtlarının Saklanması ve Analizi İçin NfSen kurulumu

Bu çalışmamızda NfSen uygulamasını Pardus üzerine kurduk. Detaylarını aşağıda anlatacağız. Benzer şekillerde herhangi bir Linux dağıtımı ya da BSD işletim sisteminde de rahatlıkla kullanabilirsiniz. (FreeBSD'de nfsen bir port olarak bulunmakta).

1-Pardus Kurulumu

ftp://ftp.pardus.org.tr/pub/pardus/kurulan/2007.1 adresinden edineceğiniz kaynak kod ile Pardus kurumunu standart şekilde yapmanız yeterli olacaktır.

Sorun yaşamanız durumunda http://www.pardus.org.tr/belgeler/kurulum_nasil.html adresindeki belgeye başvurabilirsiniz.

2-Php ve Apache

Root erişimine geçtikten sonra:

$ pisi update-repo (depo güncellemesi)
$ sudo pisi it apache mod_php
$service apache on (açılışta apache başlasın)

3-RRd Tools

http://oss.oetiker.ch/rrdtool/download.en.html adresindeki herhangi bir yansıdan rrdtool.tar.gz son sürümünü edinebilirsiniz. (rrdtool-1.2.15)

$tar -zxvf rrdtool.tar.gz
$cd rrdtool-1.2.15
$./configure
$make
$make install

Pardus 2007.1 üzerinde sorunsuz derleniyor.

4-NfDump

http://sourceforge.net/project/showfiles.php?group_id=119350
$tar -zxvf nfdump-1.5.2.tar.gz
$cd nfdump-1.5.2
$./configure
$make
$make install

5-Nfsen

Adım adım kurulumunu ve ayarlarını anlatacağımız NfSen ile ilgili belgelere http://nfsen.sourceforge.net/ adresinden ulaşabilirsiniz.

http://sourceforge.net/project/showfiles.php?group_id=134525

$tar -zxvf nfsen-1.2.4.tar.gz
$cd nfsen-1.2.4/etc
$cp nfsen-dist.conf nfsen.conf
$vi nfsen.conf

$HTMLDIR değerini aşağıdaki şekilde değiştirin...
$HTMLDIR= "/var/www/localhost/htdocs/nfsen/";

%sources Netflow bilgisini yollayan kaynakları içermemiz gerekiyor. Buradaki port değeri yönlendirici ayarlarında NetFlow datasının yollandığı portu ifade ediyor.

```
%sources = (
    'deneme'    => { 'port'    => '9996', 'col' => '#0000ff' },
);
```

:wq (vi dan kaydederek çıkın**)**

$cd..
$groupadd www
$useradd www -g www
$useradd netflow -g www

$vi /etc/apache2/httpd.conf

Ayarlar dosyasındaki User ve Group değerlerini apache yerine www ile değiştireniz gerekiyor.

User www
Group www

$./install.pl etc/nfsen.conf   (perl yolu /usr/bin/perl)

Bu komutla birlikte NfSen için gerekli klasörleri oluşturacak, nfsen.conf da belirlediğimiz HTMLDIR altına php/html dosyalarını kopyalayacak, live profile 'ı yaratacaktır. Bu komut sonrasında nfsen.conf dosyasının CONFDIR altında da konduğunu bir kontrol edelim.

$ls -la /data/nfsen/etc/nfsen.conf
-rw-r--r-- 1 root root 4451 Mar 28 16:47 /data/nfsen/etc/nfsen.conf

$cd /var/www/localhost/htdocs/nfsen
$chmod 755 nfsen.php
$cd /data/nfsen/bin/
$pwd
/data/nfsen/bin
$./nfsen.rc start

Kullandığınız profile'ın şu an ki durumunu izlemek için:

$./nfsen -l live

name   live
tstart Wed Mar 28 16:55:00 2007
tend   Thu Mar 29 10:15:00 2007
updated Wed Mar 28 16:50:00 2007
filter <none>
expire 0 hours
size   0
maxsize 0
sources deneme
type   live
locked 0
status OK

Eğer locked değeriniz 1 görünüyor ise aşağıdaki komut ile tekrar analiz prosedürünü başlatabilirsiniz:

$./nfsen -m live -U
$pwd
/data/nfsen/bin

Tüm nfsen komutlarını /data/nfsen/bin altında çalıştırdık. Bu klasörü genel yola eklemek için (PATH):

$EXPORT PATH=$PATH:/data/nfsen/bin

Nfsen ile analizlerin açılışta başlatılması için local.start dosyasını değiştirmeniz gerekmektedir:

$vi /etc/conf.d/local.start

/data/nfsen/bin/nfsen.rc start (Bu satırı dosyanın sonuna eklemeniz yeterlidir)

C) NfSen ile Analiz

Artık Pardus kurduğumuz makinada Firefox ya da benzeri uygulamalar ile: http://localhost/nfsen/nfsen.php adresini görüntülediğimizde NfSen arayüzü ile karşılaşacağız.

Detail bölümünden ilgilendiğimiz zaman aralığını seçerek (grafik üstünde) ilgili kayıtları ayıklayabiliriz. Bunun için grafiğin altında yer alan *Processing* bölümünü kullanmanı gerekiyor. Source bölümde ayarlar dosyasında UDP portlarına göre ayırdığımız kaynaklar listeleniyor.

Buradan bir kayna seçtikten sonra *Filter* bölümde özel olarak ilgilendiğimiz bir eleman için (Ip adresi, arayüz, AS, Port v.s) filtreleme yapabiliriz. Bu alanının kullanım şekli Nfdump datasının kullanım şekli ile aynı. (http://nfdump.sourceforge.net/) adresinden Filter bölümünde detaylara ulaşabilirsiniz. Bazı alanlar için filtreleme şeklini aşağıda bulabilirsiniz.

*1-Filtreler***:**
Başlıkların altında verilen komutları teker teker ya da bir kaçını birden Filters bölümüne yazarak ilgili başlığa göre filtreleme yapabilirsiniz.
protokol nesli
Ipv4 için **inet** yada **ipv4**
Ipv6 için **inet6** ya da **ipv6**

protokol
TCP, UDP, ICMP, GRE, ESP, AH, RSVP yada **PROTO <protokol_numarası>**
IP Adresi
Kaynak Ipsi için: **IP a.b.c.d**
Kaynak ya da hedef: **HOST a.b.c.d**

Ağ
NET a.b.c.d m.n.r.s (m.n.r.s ağ maskesi)
NET a.b.c.d / num (Ya da / gösterimi ile)

Kapı
PORT [**operator**] **port_no** (operator olarak =,>,< kullanılabilir)

Arayüz
[inout] **IF arayuz_no** (başına eklenecek in ya da out ile trafiğin yönünü de belirtebilirsiniz)

Pakete göre
packets [operator] **sayı** [scale] (scale değeri **k,m,g** olabilir. Kilo, mega ve giga için)

Byte değerine göre
bytes [operator] **sayı** [scale]

Saniyelik Paket (Packets per second):
pps [operator] **num** [scale]

Flow zamanına göre:
duration [operator] **num**

Saniyelik Bite Göre (Bits per second):
bps [operator] **num** [scale] .

Paketlerine Byte cinsinden büyüklüğüne göre (Bytes per packet):
bpp [operator] **num** [scale]

AS numarası
[SourceDestination] **AS sayı**

2-Show Bölümü

Kaynağı ve filtreleri hallettikten sonra şimdi NetFlow dökebilir ya da istatistiğini alabilirsiniz. *List* seçeneğinde dökeceğiniz flowların sayısını ve formatını belirleyebiliyorken, *Stat* seçeneğinde kaynak IP, hedef Ip, Kapı, AS numarası v.s. için çıkacak istatistikleri byte,paket,pps v.s. için sıralatabilirsiniz.

Önemli Not:
Ağınız ile ilgili tüm trafiğin bilgilerini barındıran Netflow kayıtlarının tutulması ve analiz edilmesi ağ yönetimi için çok önemlidir. Bununla birlikte bu kayıtlar kurum çalışanlarınızın kişisel bilgilerini de içerdiğinden ağ yöneticileri dışında kişilerin erişimine izin verilmemelidir. Bunun için en pratik çözüm olarak *.htaccess* dosyası yardımı ile web sunucusuna erişimi kullanıcı tabanlı yapmak sayılabilir. Ayrıca sunucuya *ssh* erişiminin de çok dikkatli yapılması gerekmektedir.