TÜBİTAK ULAKBİM

Ağ Yönetimi ve Trafik Analizi

IPv6 Geçiş Eğitimi

İçerik:

1. Akış İzi Kayıtları
   - Flow Nedir?, Akış izi kayıtları bölümleri
2. Kayıtların Oluşturulması
   - Yönlendiricilerin akış izi kayıtlarını oluşturması
   - Akış izi kayıtlarının dışarı aktarılması
3. Kayıtların Depolanması
   - NfDump
   - Netflow Sensor (NfSen Kurulumu)
   - Apache, php kurulumu
   - NfSen Yapılandırması
4. Kayıtların İşlenmesi
   - Nfsen sorguları
   - Nfsen filtreleri
   - Nfsen çıktı seçenekleri
5. Uygulama
   - Ubuntu Nfsen

Ağ İzi Kaydı - Flow

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

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes
2011-03-29 06:34:01.571	4294967.295	UDP	2001:470:0:f0::2.59555	->	2001:a98:10::251.53	15	910
2011-03-29 06:34:01.571	4294967.295	UDP	2001:a98:10::251.53	->	2001:470:0:f0::2.59555	10	206
2011-03-29 06:34:02.664	4294967.295	UDP	2001:470:0:fa::2.15780	->	2001:a98:10::252.53	1	93
2011-03-29 06:34:02.664	4294967.295	UDP	2001:a98:10::252.53	->	2001:470:0:fa::2.15780	12	164
2011-03-29 06:34:03.318	4294967.295	UDP	2001:470:0:17f::2.65250	->	2001:a98:10::251.53	1	93

:

Akış İzi Kaydı Oluşturulması - II

- BSD ya da Unix tabanlı yönlendiricilerden ya da güvenlik duvarlarından akış izlerinin alınması için softflowd programı kullanılmaktadır.
- Linux tabanlı bir güvenlik duvarında:

```
$ apt-cache search softflowd
softflowd - Flow-based network traffic analyser
$ apt-get install softflowd
```

- Softflowd FreeBSD portlarında da yer almaktadır ve kolayca kurulumu yapılabilmektedir.

```
$cd /usr/ports/net-mgmt/softflowd
$make install
```

Ağ İzi Kaydı Oluşturulması - II

➢Softflowd kurulduktan sonra üzerindeki ara yüzlerden geçen trafiğe ait izlerin aktarılması için:

IPv6:

```
$/usr/local/sbin/softflowd -v 9 -i interface -m 1000 -n[MonitorIPv6address]:port
$/usr/local/sbin/softflowd -v9 -i em0 -m 1000 -n[2001:a98:1f:f0::4]:9995
$/usr/local/sbin/softflowd -v9 -i em1 -m 1000 -n[2001:a98:1f:f0::4]:9996
$/usr/local/sbin/softflowd -v9 -i em2 -m 1000 -n[2001:a98:1f:f0::4]:9997
$/usr/local/sbin/softflowd -v9 -i em3 -m 1000 -n[2001:a98:1f:f0::4]:9998
$/usr/local/sbin/softflowd -v9 -i em4 -m 1000 -n[2001:a98:1f:f0::4]:9999
```

IPv4:

```
$/usr/local/sbin/softflowd -v 9 -i em0 -m 100000 -n10.1.4.4:9995
$/usr/local/sbin/softflowd -v 9 -i em1 -m 100000 -n10.1.4.4:9996
$/usr/local/sbin/softflowd -v 9 -i em2 -m 100000 -n10.1.4.4:9997
$/usr/local/sbin/softflowd -v 9 -i em3 -m 100000 -n10.1.4.4:9998
$/usr/local/sbin/softflowd -v 9 -i em4 -m 100000 -n10.1.4.4:9999
```

Nfsen Kurulumu

- Nfsen, yönlendiriciler tarafından dışa aktarılan akış izlerinin işlenmesi için kullanılan bir ara yüz yazılımıdır.
- Nfsen, kayıtların depolanması ve işlenmesi için Nfdump yazılımını kullanmaktadır.
- Ayrıca Nfsen ara yüzünün çalışması için Php, Apache, RRDtool ve bazı diğer paketlere (libpng12-dev, libfreetype6-dev, libart-2.0-dev, bison, flex) ihtiyaç duymaktadır.

Nfsen Bağımlılıkları Kurulumları

```
$ apt-get update
$apt-get install build-essential
$ apt-get install apache2
$ apt-get install php5 php5-cli
$ apt-get install rrdtool
$ apt-get install librrds-perl
$ apt-get install libpng12-dev libfreetype6-dev libart-2.0-dev bison flex
$apt-get install nfdump
$perl -MCPAN -eshell
cpan> install Mail::Header
cpan> install Mail::Internet
```

:

NfSen Kurulumu

- Adım adım kurulumunu ve ayarlarını anlatacağımız NfSen ile ilgili belgelere http://nfsen.sourceforge.net/ adresinden ulaşabilirsiniz.
- http://sourceforge.net/projects/nfsen/files/stable/nfsen-1.3.5/nfsen-1.3.5.tar.gz/download adresinden 27.03.2011 tarihinde en güncel sürüm olan Nfsen 1.3.5'i indirebilirsiniz. Nfsen kurulumuna geçmeden önce kaynak arşivi açılmalı ve varsayılan olarak gelen ayar dosyası nfsen.conf adıyla kopyalanmalıdır.

```
$tar zxvf nfsen-1.3.5.tar.gz
$cd nfsen-1.3.5
$cp etc/nfsen-dist.conf etc/nfsen.conf
$mkdir /data
```

Nfsen Ayar Dosyası Gerekli Değişiklikler

- Nfsen'in tar ile açıldığı dizin içinde etc/nfsen.conf dosyasında şu ayarların değiştirilmesi gerekmektedir:

```
$BASEDIR = "/data/nfsen";
$HTMLDIR    = "/var/www/nfsen/";
$PREFIX  = '/usr/bin';
$USER    = "www-data";
$WWWUSER  = "www-data";
$WWWGROUP = "www-data";
%sources = (
   'kaynak1'    => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
   'kaynak2'    => { 'port' => '9996', 'col' => '#ff00ff', 'type' => 'netflow' },
   'kaynak3'    => { 'port' => '9997', 'col' => '#ffff00', 'type' => 'netflow' },
   'kaynak4'    => { 'port' => '9998', 'col' => '#00ff00', 'type' => 'netflow' },
   'kaynak5'    => { 'port' => '9999', 'col' => '#00ffff', 'type' => 'netflow' },
);
```

Kurulumun tamamlanması ve çalıştırılması

```
$./install.pl etc/nfsen.conf
$ls -la /data/nfsen/etc/nfsen.conf
-rw-r--r-- 1 root www-data 9335 2011-03-25 14:27 /data/nfsen/etc/nfsen.conf
$echo -e "<?php\n\theader(\"Location: nfsen.php\");\n?>" > /var/www/nfsen/index.php
$/data/nfsen/bin/nfsen start
$cd /data/nfsen/profiles-data/live/kaynak1/
$ls -la nfcapd.current
-rw-r--r-- 1 www-data www-data 276 2011-03-31 10:25 nfcapd.current
```

Nfcapd.current dosyası en güncel trafik izlerinin saklandığı dosyadır ve eğer ağ trafik izleri doğru bir şekilde saklanıyorsa büyüklüğü artmalıdır. Bu dosya her 5 dakikada bir yine */data/nfsen/profiles-data/live/kaynak1* altında oluşturulmuş olan yıl/ay/gün şeklindeki dizine *nfcapd.yılaygunsaat formatında kopyalanacaktır.*

Nfsen ayar dosyası değişiklikleri

- Nfsen'in bilgisayar her açıldığında başlatılması için */etc/rc.local* dosyasına */data/nfsen/bin/nfsen start* satırının eklenmesi gerekmektedir.
- Nfsen ayarlarında bir değişiklik yapıldığında geçerli olması için aşağıdaki komut çalıştırılmalıdır.

```
$/data/nfsen/bin/nfsen reconfig
```

Nfsen ayar dosyası değişiklikleri

IPv6 uzak istemcilerinden http://**[2001:a98:1f:f0::4]/nfsen/nfsen.php** adresi görüntülediğinde NfSen ara yüzüne ulaşılacaktır.

Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: | live ▼

Profile: live

TCP

UDP

ICMP

other

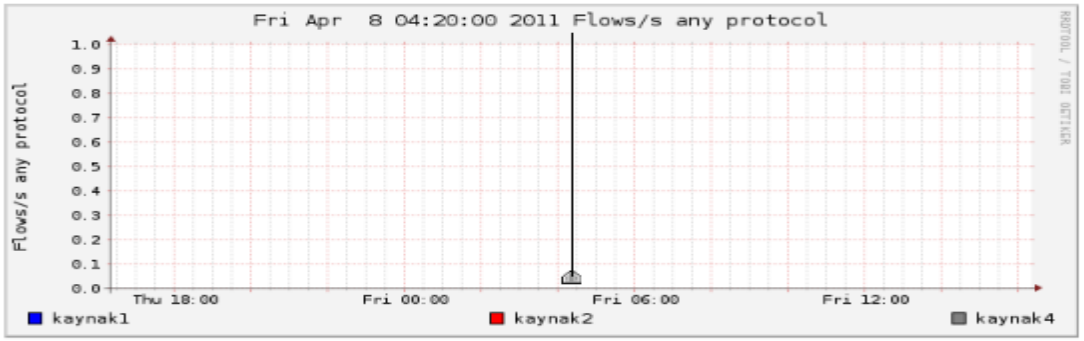
Profileinfo:

Type: live
Max: unlimited
Exp: never
Start: Mar 24 2011 - 10:09 EEST
End: Apr 08 2011 - 16:20 EEST

t_{start} 2011-04-08-04-20
t_{end} 2011-04-08-04-20

Packets

Traffic



Select Single Timeslot Display: 1 day << < | ^ > >> >|

◉ Lin Scale ◉ Stacked Graph
○ Log Scale ○ Line Graph

Statistics timeslot Apr 08 2011 - 04:20

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
☑ kaynak4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
☑ kaynak2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
☑ kaynak1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

All None **Display:** ○ Sum ◉ Rate **x: No Data available**

Netflow Processing

Source:

kaynak4
kaynak2
kaynak1

All Sources

Filter:

and <none>

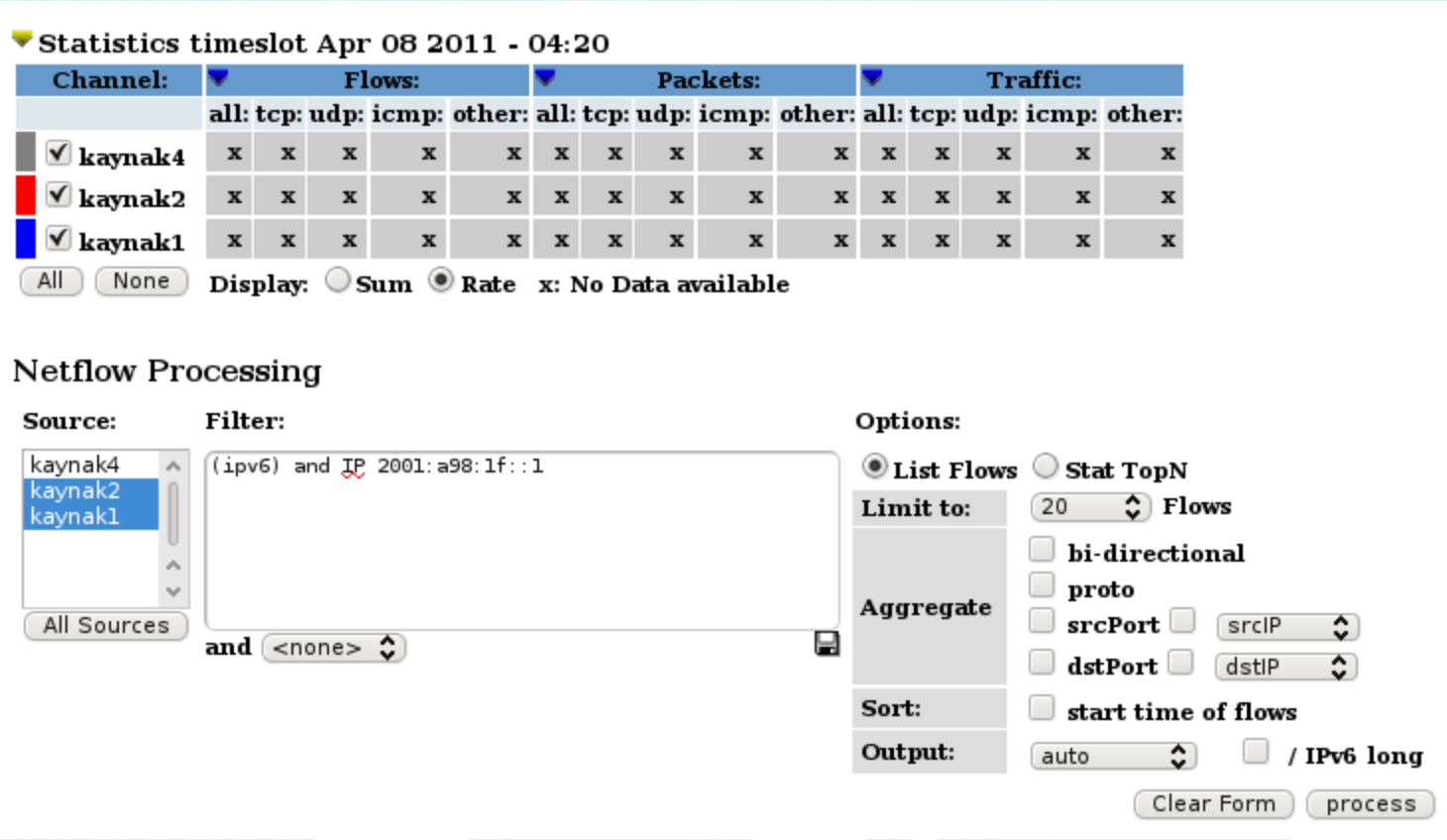
Options:

○ List Flows ◉ Stat TopN

Top: 10
Stat: Any IP Address order by flows
Limit: ☐ Packets > 0 -
Output: ☐ / IPv6 long

Clear Form process

Nfsen Filtreler



Nfsen Filtreler

Başlıkların altında verilen komutlar teker teker ya da birlikte Filters bölümüne yazılarak ilgili başlığa göre filtreleme yapılabilir. Filtreleri beraber uygulamak için şu yazım şekli kullanılmaktadır:

(Filtre1) and (Filter2)
(Filtre1) or (Filtre2)

Protokol nesli:
Ipv4 **ipv4**
Ipv6 **ipv6**

Protokol tipi:
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**

Nfsen Filtreler

➢Ağ Adresi:
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 Numarası:
PORT [**operator**] **port_no** (operator olarak =,>,< kullanılabilir)

➢Yönlendiricideki Ağ Arayüzü:
[inout] **IF arayuz_no** (başına eklenecek in ya da out ile trafiğin yönünü debelirtebilirsiniz)

➢Kayıtta Yer Alan Paket Sayısı:
packets [operator] **sayı** [scale] (scale değeri **k,m,g** olabilir. Kilo, mega ve giga için)

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

Nfsen Filtreler

➢ Saniyedeki Paket Sayısı: (Packets per second):
pps [operator] **num** [scale]
➢Trafik izinin oluştuğu süre:
duration [operator] **num**

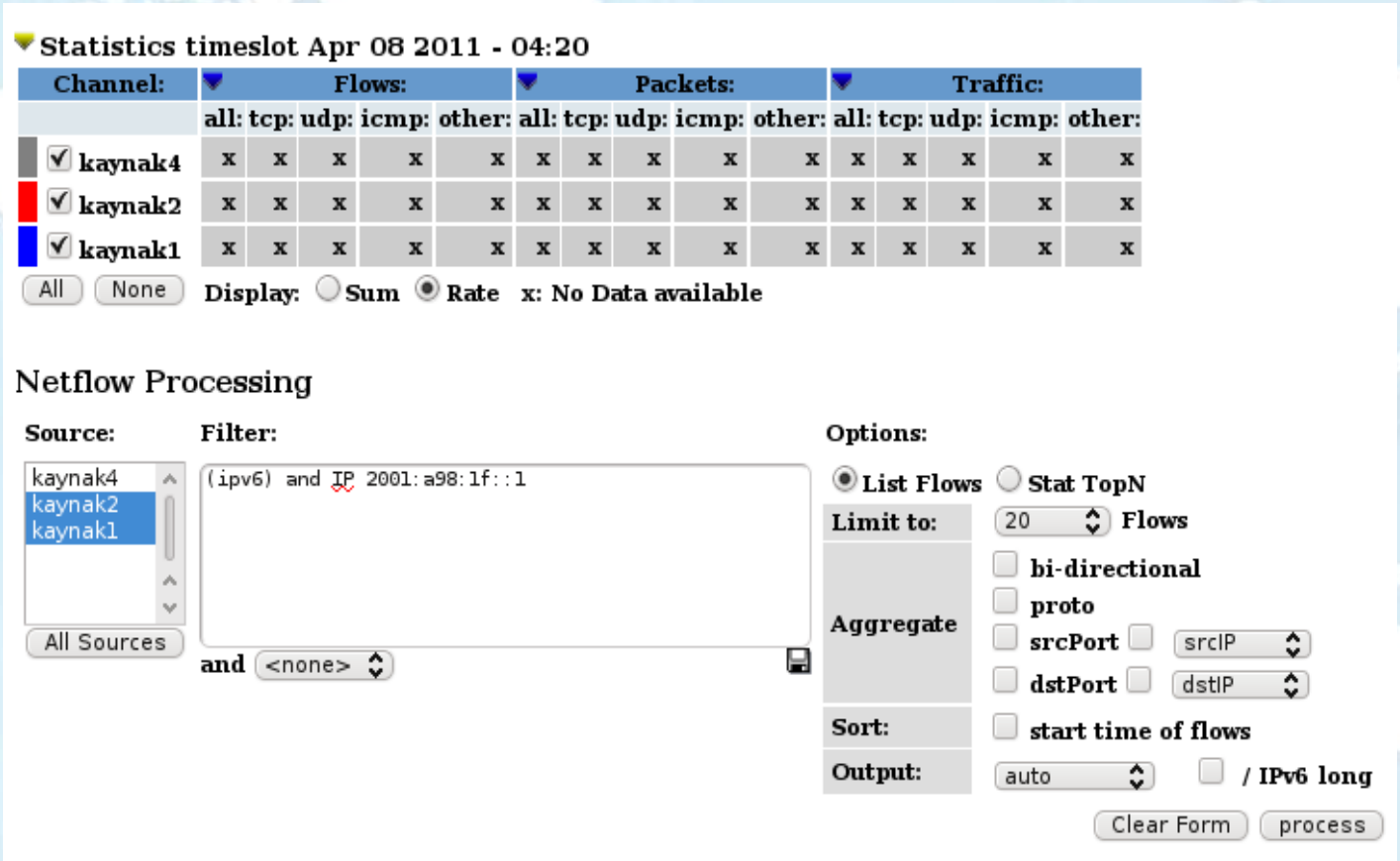
➢Saniyelik Bite Göre (Bits per second):
bps [operator] **num** [scale]

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

➢AS numarası
[SourceDestination] **AS sayı**

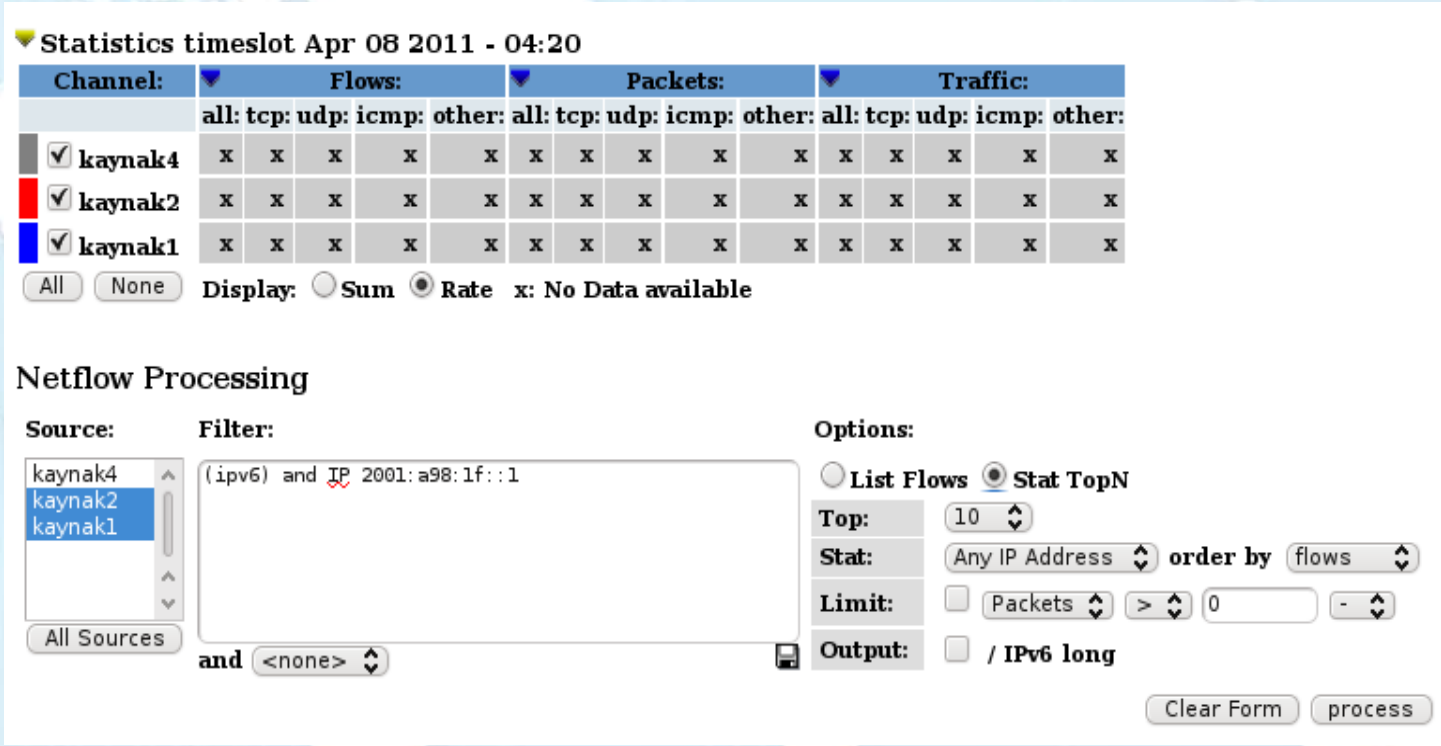
Nfsen İnceleme Sonuçları

List seçeneğini seçilen kaynaktan gelen akış izlerine hazırladığınız filtrenin uygulanmasını ve sonuçların görüntülenmesini sağlamaktadır. Sonuçlarda yer alacak izlerin sayısını ve formatını belirlemenin yanında, ortaya çıkan bu izleri "Aggregate" bölümünde seçtiğiniz bir başlık bölümüne göre (kapı, hedefe ya da kaynak IP adresi) saydırılabilir. Bu seçeneğin en temel kullanımı belirli bir zaman aralığında bir IP adresine ait trafik izlerinin izlenmesidir.



Nfsen İnceleme Sonuçları

Akış izlerinin işlenmesinde ikinci seçenek olan *Stat TopN* istatistiki bilgiler sağlamaktadır. Seçilen zaman aralığında kapılar ya da IP adresleri oluşturdukları flow, paket ya da trafik büyüklüğüne göre listelenebilmektedir. Kaynak IP, hedef IP, Kapı, AS numarası v.s. için çıkacak istatistikler byte, ağ izi sayısı, pps v.s. için sıralatılabilir.



Uygulama

Önemli Not:

Üzerinde çalışılan ağ ile ilgili tüm trafiğin bilgilerini barındıran akış izlerinin tutulması ve analiz edilmesi ağ yönetimi için çok önemlidir. Bununla birlikte bu kayıtlar hassas bilgiler içerdiğinden ağ yöneticileri dışındaki 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.

UYGULAMA 5-2: Ağ Trafiği Analizi
Görev 1: Monitör Üzerinde Ön Kurulu NFSEN'nin İncelenmesi ve Değiştirilmesi
Görev 2: NFSEN ile Akış İzlerinin İncelenmesi

: