Monitorizacion de Netflow con NFSen

Gestion de Redes

Contents

1 Introduccion

1.1 Metas

- Aprender como instalar las herramientas Nfdump y Nfsen

Utilice NFSen para saber que hosts estan generando la mayor parte de trafico de entrada de salida de la red

1.2 Supuestos

El router esta enviando registros netflow a uno de sus equipos, y este PC ejecuta NFSen para recoger estos datos. Si esta trabajando en pareja, entonces ambos deben apuntar su navegador web al PC que recibe los flujos:

http://pcX.ws.nsrc.org/nfsen/nfsen.php

2 Generar un poco de trafico

En primer lugar, tenemos que generar algo de trafico que pase a traves de su router. En cualquiera de los PC (no tiene que ser donde esta funcionando NFSen), Iniciar sesion y escriba los siguientes comandos:

```
$ cd /tmp
$ wget http://noc.ws.nsrc.org/downloads/BigFile
$ rm BigFile
```

Tomara alrededor de 5 minutos antes de que se muestre un aumento en NFSen.

3 Explorando registros de flujo

Ahora vamos a usar NFSen para explorar los flujos de trafico en la red, con el objetivo de averiguar quien ha descargado la mayor cantidad de datos. Mire cuidadosamente en la salida generada en cada paso - pedir a un instructor explicar si no entiende lo que ve.

3.1 Vaya a la pagina Detalle

La pagina de inicio de NFSen muestra una matriz de graficos: flujos por segundo a la izquierda, paquetes por segundo en el medio, los bits por segundo a la derecha. hacer clic en el grafico de arriba a la derecha (bits por segundo, una vista por dia) para llegar a la pagina de Detalle.

Figure 1: Selecting time window

3.2 Seleccione ventana de tiempo

Cambiar de “Intervalo de tiempo individual” a “ventana de tiempo”:

Una vez hecho esto, la flecha de seleccion vertical y la linea en la ventana grafica se puede dividir. Tire de la mitad izquierda de la flecha hacia la izquierda y de la mitad derecha a la derecha para seleccionar el periodo de tiempo de interes. Entonces usted deberia ver algunas estadisticas de resumen aparecer en la tabla debajo del grafico, por el periodo de tiempo que haya seleccionado:

Statistics timeslot Jul 17 2013 - 20:50 - Jul 17 2013 - 21:00

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
✓ rtr1	4.7 /s	1.0 /s	3.7 /s	0.0 /s	0 /s	110.1 /s	105.3 /s	4.4 /s	0.3 /s	0 /s	313.0 kb/s	309.6 kb/s	3.1 kb/s	254.0 b/s	0 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	4.7 /s	1.0 /s	3.7 /s	0.0 /s	0 /s	110.1 /s	105.3 /s	4.4 /s	0.3 /s	0 /s	313.0 kb/s	309.6 kb/s	3.1 kb/s	254.0 b/s	0 b/s

Figure 2: Summary statistics

3.3 Lista de flujos individuales

Seleccione “Lista de flujos”, asegurese de que ninguna de las casillas “agregado” no se comprueban y, a continuacion, haga clic en ‘proceso’. Esto mostrara algunos flujos al comienzo del periodo de tiempo.

Aumentar el limite de 20 flujos hasta 100 flujos. Observe que la mayor parte de trafico de la red se compone de un gran numero de flujos muy pequeños - por ejemplo, una consulta/respuesta DNS sera dos flujos, uno desde el cliente al servidor DNS, y uno de vuelta.

Al seleccionar “bidireccional”, usted puede con Nfsen conseguir asociar los flujos de entrada y de salida en una sola linea:

Sin embargo, todavia es demasiado trabajo para vadear a traves de este en busca de trafico interesante. Desmarque la casilla “bidireccional” antes de continuar.

3.4 Caudales desde/hasta un host

Si sabemos que host queremos examinar, podemos aplicar un filtro para mostrar solo los flujos desde/hasta ese host. Hacer esto mediante la introduccion de

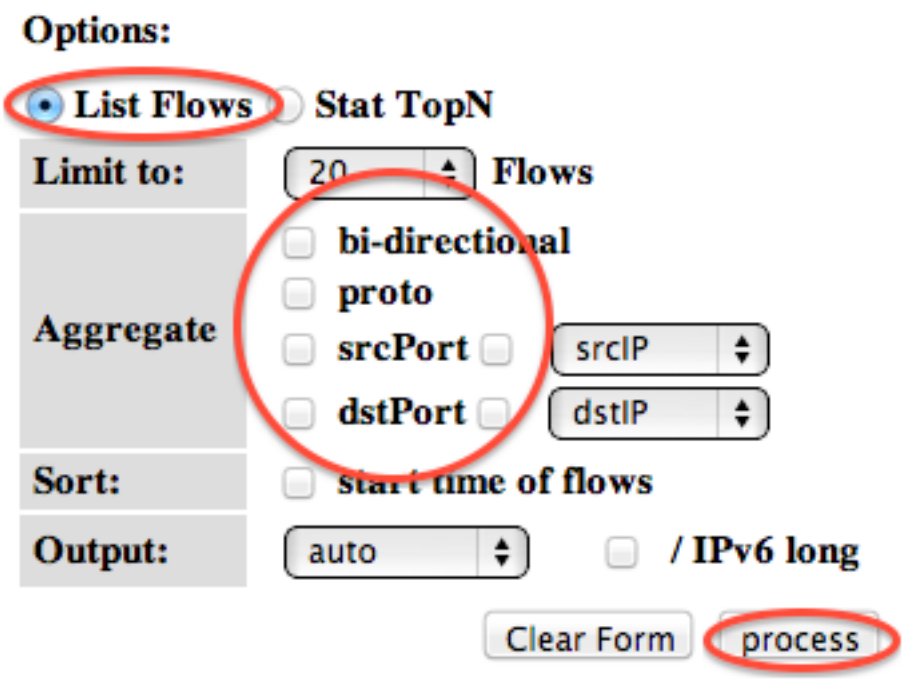

Figure 3: List flows

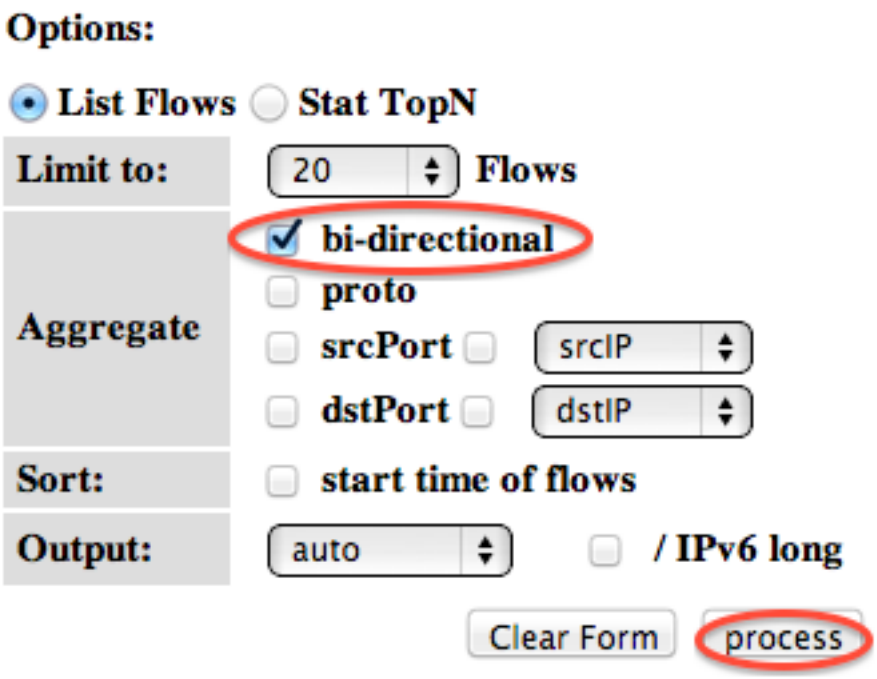

Figure 4: Bi-directional flows

“host 10.10.XY” en la caja de filtro, y despues ‘presionar’ proceso de nuevo. (Reemplace 10.10.XY con la direccion de uno de sus equipos)

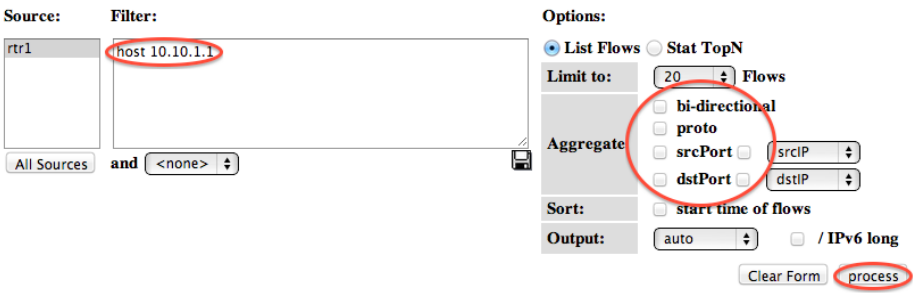

Figure 5: Flows to and from one host

Esto es un poco mejor, pero todavia tendria que vadear a traves de un monton de pequeños flujos para encontrar algo significativo. Tenemos que tomar un enfoque diferente.

flujos mas grandes #

La siguiente cosa que podemos hacer es conseguir NFSen para ordenar los flujos segun el numero de bytes. Quite cualquier filtro de la caja de filtro, seleccione “Stat TopN”, las estadisticas “Flow Records”, orden por “Bytes”. Asegurese de que todas las casillas de agregados estan sin control, a continuacion, pulse `proceso`

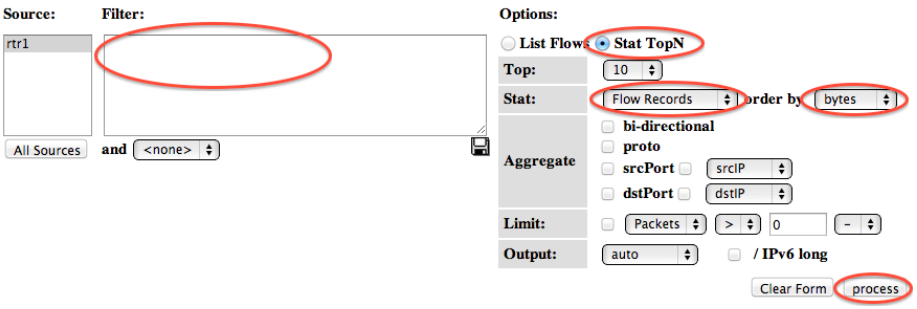

Figure 6: Find top flows by bytes

Esta es una mejora definitiva, ya que los flujos con el mayor numero de bytes se muestran primero. Sin embargo hay un problema - todavia estamos viendo flujos individuales. Es posible que muchos pequeños caudales hacia la misma maquina se sumen a una gran cantidad de trafico, pero no los veriamos en la parte superior de la lista.

```
** nfdump -M /var/nfsen/profiles-data/live/rtr1  -T  -R 2013/07/17/nfcapd.201307172050:2013/07/17/nfcapd.201307172
nfdump filter:
any
Verify map id 0: ERROR: Expected 7 elements in map, but found 2!
Aggregated flows 4194
Top 10 flows ordered by bytes:
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2013-07-17 18:34:59.964  8104.200 TCP         10.10.0.98:22    ->      10.10.0.241:56511    55346   31.8 M     1
2013-07-17 18:34:59.964  8104.200 TCP        10.10.0.241:56511 ->       10.10.0.98:22       29340    1.6 M     1
2013-07-17 20:28:46.766  1272.078 TCP         10.10.0.98:22    ->      10.10.0.241:56517     2669   389844     1
2013-07-17 20:28:46.766  1272.078 TCP        10.10.0.241:56517 ->       10.10.0.98:22        3383   224316     1
2013-07-17 20:50:29.950    15.832 TCP         10.10.0.98:80    ->      10.10.0.241:37764      57    73003     1
```

Figure 7: Output: top flows by bytes

4 El trafico entrante agrupado por la direccion IP del receptor

Lo que queremos ver es una sola linea para cada host en la red, que muestre la cantidad total de trafico entregado a ese host.

para hacer esto, Stat "DST IP Address", order by "bytes".

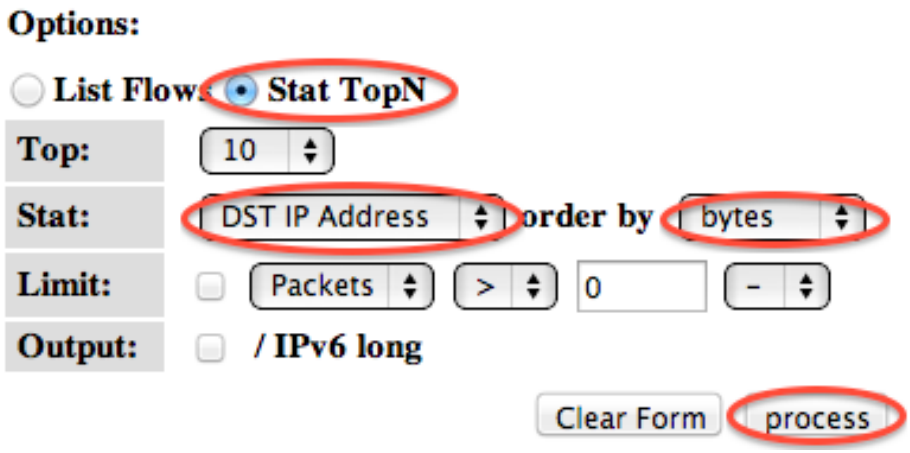

Figure 8: Group flows by DST IP Address

Esto es ahora mucho mas cerca de lo que queremos: hay una linea para cada direccion IP de destino, y que estan clasificadas por el total de bytes, el mayor primero.

Pero todavia hay un problema - se puede ver lo que es? Estamos viendo una mezcla de los flujos de entrada (donde la IP de destino esta dentro de la red) y de flujos salientes (cuando la IP de destino esta en la Internet). Solo estamos interesados ??en los flujos de entrada, por lo que se aplica un filtro que solo muestra el trafico a la red de su grupo: "dst net 10.10.X.0/24" (reemplece X con el numero de su grupo)

Por fin tenemos lo que queremos. El primer registro que ves deberia decir la

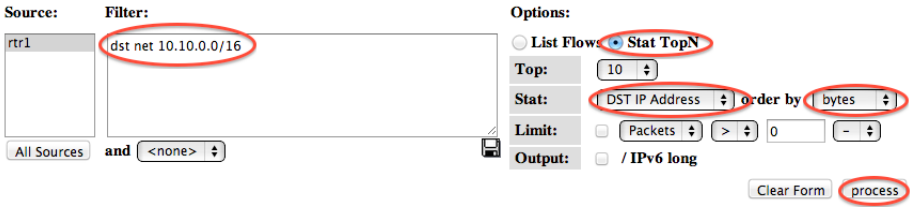

Figure 9: Flows to local network, grouped by DST IP Address

```
** nfdump -M /var/nfsen/profiles-data/live/gw-rtr  -T  -R 2013/04/17/nfcapd.201304170855:2013/04/17/nfcapd.201304171215 -n 10 -
nfdump filter:
dst net 10.10.0.0/16
Top 10 Dst IP Addr ordered by bytes:
Date first seen          Duration Proto       Dst IP Addr   Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2013-04-16 11:12:42.978 90437.613 any        10.10.0.135   92280(44.6)    1.9 M(41.8)  551.6 M(20.4)      20    48791   290
2013-04-17 06:55:42.339 19428.094 any        10.10.0.121    3924( 1.9)   303950( 6.7)  366.6 M(13.5)      15   150948  1206
2013-04-17 06:43:13.857 20201.599 any        10.10.0.115    2436( 1.2)   206384( 4.5)  288.9 M(10.7)      10   114424  1400
2013-04-17 08:52:41.704 12178.594 any        10.10.0.118    1044( 0.5)   111910( 2.5)  159.8 M( 5.9)       9   104992  1428
2013-04-16 10:56:01.483 91435.087 any        10.10.0.110   10446( 5.0)   192597( 4.2)  154.4 M( 5.7)       2    13512   801
```

Figure 10: Output: Flows to local network, grouped by DST IP Address

maquina local que ha descargado mas datos en el periodo seleccionado.

4.1 El trafico saliente agrupado por la direccion IP del emisor

Pregunta: que cambios hay que hacer a esta consulta para averiguar que maquinas de la red estan subiendo la mayor cantidad de datos a la Internet

5 Analisis de trafico en un solo host

Ahora que sabemos que host ha descargado mas datos, podriamos querer ver desde donde el anfitrion ha estado descargando.

Vamos a empezar mirando los mejores flujos hacia ese host. Cambie el filtro "dst host 10.10.XY" (la direccion IP que acaba de encontrar). A continuacion, seleccione las estadisticas "Flow Records", ordenadas por "bytes", y 'proceso'.

Ahora debe ver los flujos de entrada a ese host, el mayor primero. Pero, de nuevo, solo estamos viendo grandes flujos individuales; una coleccion de pequeños flujos puede sumar a una gran cantidad de trafico.

Ya que solo estamos viendo los registros de flujo a una direccion IP de destino particular, podemos agrupar los registros por la direccion IP de origen

Y ahora tenemos una fila para cada direccion IP de donde este host ha estado descargando, con el numero total de bytes descargados de cada IP, el mayor total de primero.

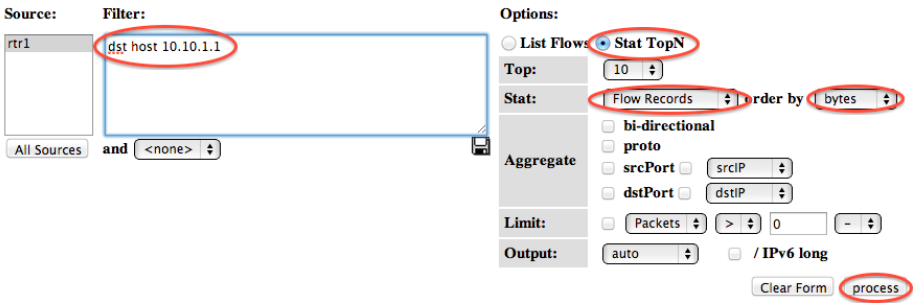

Figure 11: Largest flows to one host

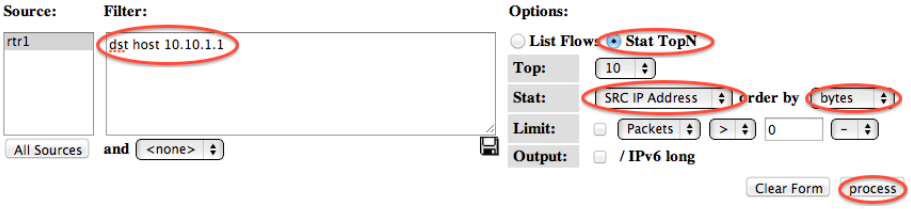

Figure 12: Flows to one host, grouped by SRC IP address

```
** nfdump -M /var/nfsen/profiles-data/live/gw-rtr  -T  -R 2013/04/17/nfcapd.201304170855:2013/04/17/nfcapd.201304171215 -n 10 -
nfdump filter:
dst host 10.10.0.135
Top 10 Src IP Addr ordered by bytes:
Date first seen          Duration Proto      Src IP Addr   Flows(%)     Packets(%)       Bytes(%)       pps      bps   bpp
2013-04-17 09:59:37.965  7177.308 any      86.135.63.204    70( 0.1)   133384( 7.0)   166.0 M(30.1)        18   185002  1244
2013-04-17 11:58:22.389   652.388 any     155.232.240.14    16( 0.0)    41268( 2.2)    57.4 M(10.4)        63   703269  1389
2013-04-17 09:49:27.947  4725.000 any      39.52.237.91     4( 0.0)    38278( 2.0)    46.9 M( 8.5)         8    79376  1224
2013-04-17 10:02:47.530  2510.000 any     109.65.3.106      4( 0.0)    35506( 1.9)    36.9 M( 6.7)        14   117603  1039
2013-04-17 11:00:02.692  4285.997 any     168.172.196.248   8( 0.0)    21956( 1.2)    32.9 M( 6.0)         5    61352  1497
```

Figure 13: Output: Flows to one host, grouped by SRC IP address

5.1 Informacion de la direccion IP

Al hacer clic en una direccion IP, podra obtener informacion del DNS inverso y del whois.

Figure 14: Whois information

6 Ejercicio Adicional: aggregating flows

NFSen ofrece algunas otras maneras de resumir los flujos, utilizando los Aggregatecheckboxes. En este ejemplo vamos a ver de nuevo en el trafico de entrada a la red.

Al hacer clic en una o mas de las casillas de agregados, NFSen combina todas flujos que comparten los mismos valores del atributo (s) que ha seleccionado.

Para comenzar este ejercicio, configurar el filtro para “dst net 10.10.X.0/24” (X = el grupo). Seleccione “Stat TopN” Estadisticas “Flow Records”, ordenados por “bytes”. A continuacion, intente los siguientes agregados, recordando hacer clic en ‘proceso’ despues de cada uno.

- Marque “proto”. Usted debe obtener una sola fila para TCP, UDP e ICMP, mostrando la cantidad total de trafico que utiliza cada protocolo. A veces esto puede mostrar otros protocolos que estan activos en la red (por ejemplo, el protocolo 50 = IPSEC ESP, en Linux el archivo ‘/etc/protocols’ tiene una lista de los servicios)
- marque tanto “proto” y “srcport”. Esto le dice a NFSen que combine conjuntamente flujos que tienen el mismo proto * y * el mismo srcport. Dependiendo de la actividad que ha estado sucediendo, es posible que vea una linea que da el total para el puerto TCP 80, una linea para el puerto TCP 443, una linea para el puerto UDP 53, y asi sucesivamente.

- Marque “SrcIP” por si mismo. Esto le da una fila para cada direccion IP de origen/distinto, y es lo mismo que seleccionar Estadistica SRCIP.
- marque tanto “SrcIP” y “dstip”. Usted recibira una fila para cada par unico de SrcIP y dstip visto, con el trafico total entre esos dos extremos.

Como cambiar el filtro para mirar el trafico de salida, en lugar de trafico de entrada

Si usted tiene un router con una tabla BGP, puede agregar registros netflow registros por numero AS. Esta es una manera util para saber con que redes esta intercambiando la mayor parte del trafico.