Использование NfSen для определения самых активных пользователей

Contents

1 Введение

1.1 Цели

- Использовать NfSen для определения хостов, которые создают наибольший входящий и исходящий трафик в вашей сети

1.2 Допущение

Ваш роутер шлет записи netflow на одну из ваших машин, и на этой машине уже запущен NfSen для сбора данных. Если вы работаете в парах, то вы должны указать в броузере ту машину, которая работает коллектором.

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

2 Сгенерируем трафик

В начале нам нужно создать кое-какой трафик, проходящий через ваш роутер. Залогиньтесь на любую из ваших машин (это не обязательно машина, на которой работает NfSen) и выполните следующие команды:

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

Пройдет около 5 минут прежде чем трафик, созданный этими командами, появится как пик на графике в NfSen.

3 Изучение записей потоков

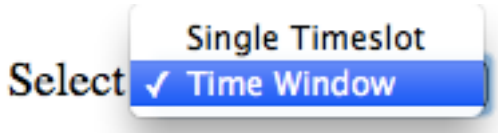
Теперь давайте используем NfSen для изучения потоков трафика в сети, с целью обнаружить, кто скачивал больше всех. Смотрите внимательно на вывод команд на каждом шаге – попросите преподавателя помочь, если вы не понимаете того, что вы видите.

3.1 Пойдите на страницу детальной информации

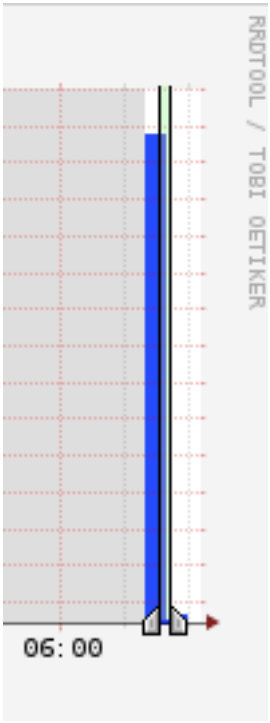
Главная страница NfSen показывает матрицу графиков: потоки в секунду слева, пакеты в секунду в середине, биты в секунду справа. Нажмите на график справа вверху (биты в секунду, график за день) для того чтобы перейти на страницу детальной информации.

3.2 Выберите временное окно

Поменяйте “Single Timeslot” на “Time Window”:



После этого, вертикальная стрелка выбора точки времени разделится надвое.



Потяните левую половинку стрелки налево, а правую направо. Таким образом вы можете выбрать интересующий вас период времени. Тогда вы должны увидеть, в таблице под графиком, статистическую сводку для выбранного периода времени:

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 1: Сводка

3.3 Просмотр индивидуальных потоков

Выберите “List Flows”, убедитесь, что ни один из флажков “Aggregate” не отмечен, и нажмите “process”. Это покажет потоки в начале выбранного интервала времени.

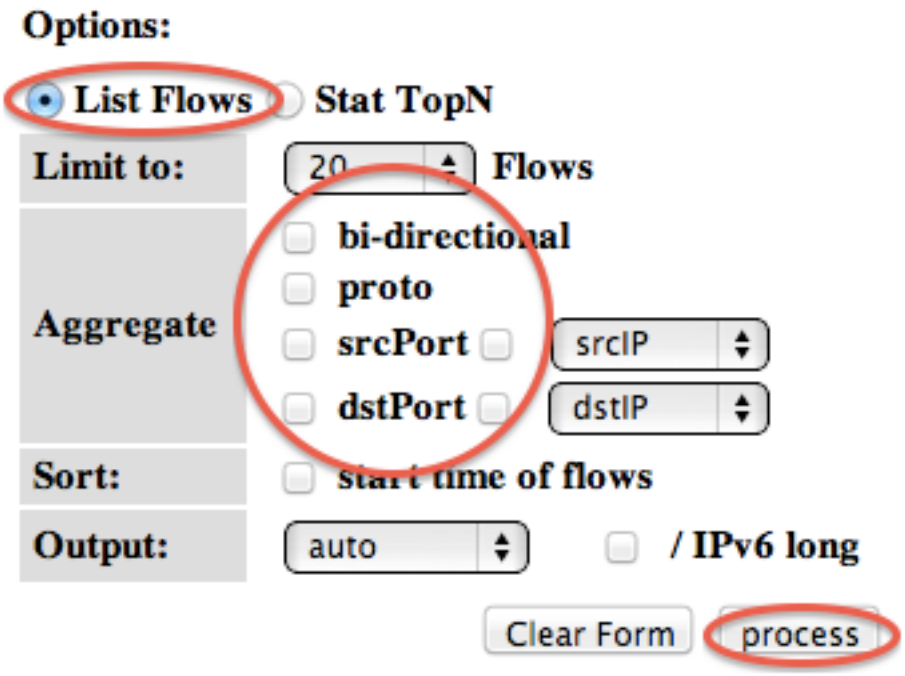


Figure 2: Список потоков

Увеличьте предел с 20 потоков до 100 потоков. Обратите внимание, что большая часть трафика в сети состоит из большого количества очень маленьких потоков – например, запрос/ответ DNS создаст два потока, один от клиента к DNS серверу, и второй в обратном направлении.

Выбрав “bi-directional”, вы скажете NfSen “схлопывать” потоки “туда” и “обратно” в одну строку:

Тем не менее, просмотр большого количества потоков в поисках интересного трафика довольно скучно. Перед тем как продолжить, очистите флажок “Bi-directional”.

3.4 Потоки в/с одного хоста

Если нам известно, какой хост мы хотим исследовать, мы можем применить фильтр для показа только потоков, имеющих отношение к этому хосту. Для

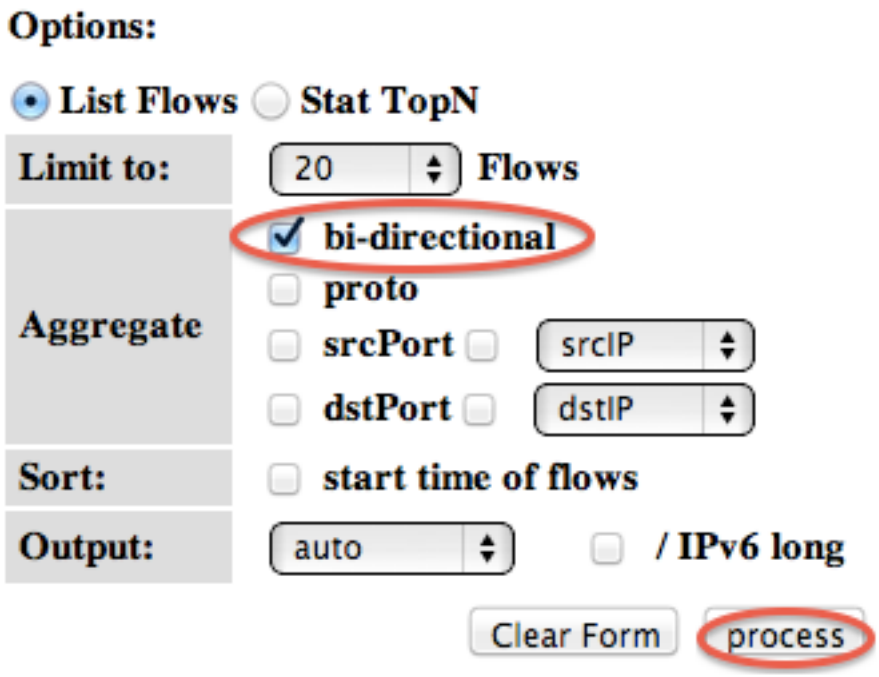


Figure 3: Двунаправленные потоки

этого введите “host 10.10.X.Y” в поле для фильтра, и снова нажмите “process”. (замените 10.10.X.Y на адрес одной из ваших машин)

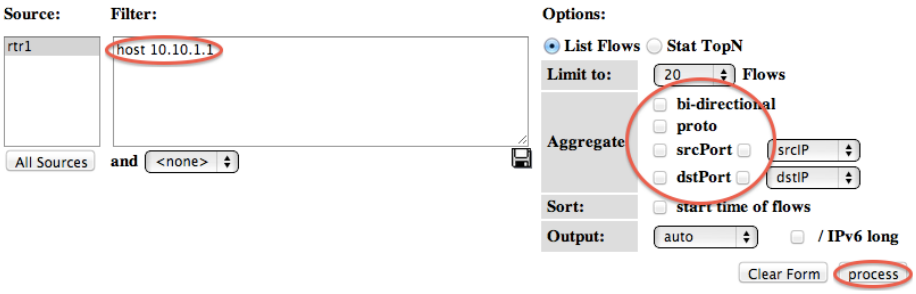


Figure 4: Потоки в/с одного хоста

Уже лучше, но нам все равно нужно просматривать слишком много небольших потоков для поиска чего-нибудь интересного. Нам нужно воспользоваться другим подходом.

4 Самые большие потоки

Следующим пунктом мы можем сказать NfSen сортировать потоки по количеству байт. Уберите фильтры поля для фильтров; выберите “Stat TopN”, “Stat:” -> “Flow Records”, “order by” -> “Bytes”. Убедитесь, что все агрегаторы по-прежнему не отмечены, и нажмите “process”.

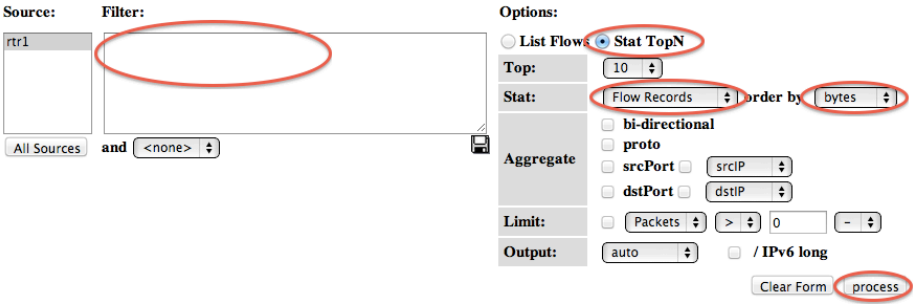


Figure 5: Найти наибольшие потоки

Это уже намного лучше, так как потоки с наибольшим количеством байт показываются в первую очередь. Однако, проблема остается – мы по-прежнему видим индивидуальные потоки. Возможна ситуация, при которой большое количество небольших потоков к одному хосту создадут большой трафик, а мы не будем видеть их вверху нашего списка.

```
** 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 6: Вывод: наибольшие потоки

5 Группировка приходящего трафик по адресу получателя

Что мы хотели бы увидеть, так это одну строчку на каждый хост в сети, показывающую общий трафик, доставленный хосту.

Для этого, “Stat:” -> “DST IP Address”, “order by” -> “bytes”.

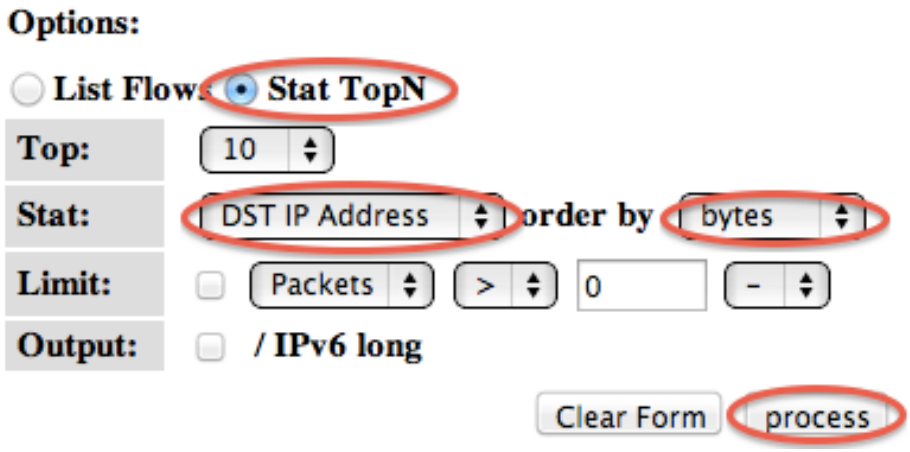


Figure 7: Группировка потоков по приходящему IP адресу

Теперь мы получили нечто, выглядящее гораздо более похожим на то, чего мы хотим: одна строчка для каждого IP получателся, и они отсортированы по суммарным байтам, в убывающем порядке.

У нас все еще осталась одна проблема – можете ли вы сказать, какая? Мы видим смесь входящих (адрес получателя в нашей сети) и исходящих (адрес получателся на интернете) потоков. Нам интересны только входящие потоки, поэтому задайте фильтр, который показывает только трафик в групповую сеть: dst net 10.10.X.0/24 (заменяя X на номер группы).

Наконец-то мы получили, что хотели. Первая запись покажет нам локальную машину, которая скачала больше всего данных в выбранный период времени.

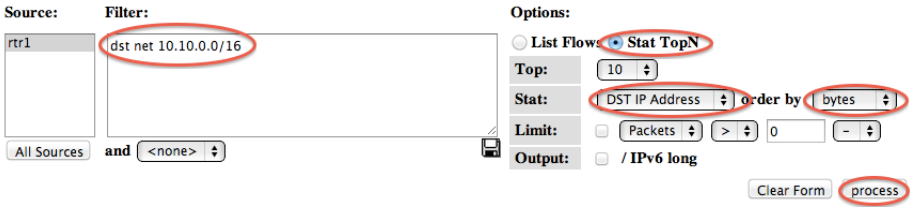


Figure 8: Потоки в локальную сеть, группированные по приходящему IP адресу

```
** 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)  151.4 M( 5.7)       2    13512   801
```

Figure 9: Вывод: Потоки в локальную сеть, группированные по приходящему IP адресу

5.1 Группировка исходящего трафика по IP адресу отправителя

Вопрос: какие изменения вам потребуется сделать, чтобы получить список машин в вашей сети, которые больше всего *закачивали* в Интернет?

6 Анализ трафика на единственную машину

Теперь, когда мы знаем, какая машина скачала больше всего данных, нам может захотеться узнать, откуда она их качала.

Давайте начнем с просмотра самых больших потоков для этого хоста. Поменяйте филтр на dst host 10.10.X.Y (только что найденный IP адрес). Затем выберите “Stat:” -> “Flow Records”, “order by” -> “bytes”, и “process”.

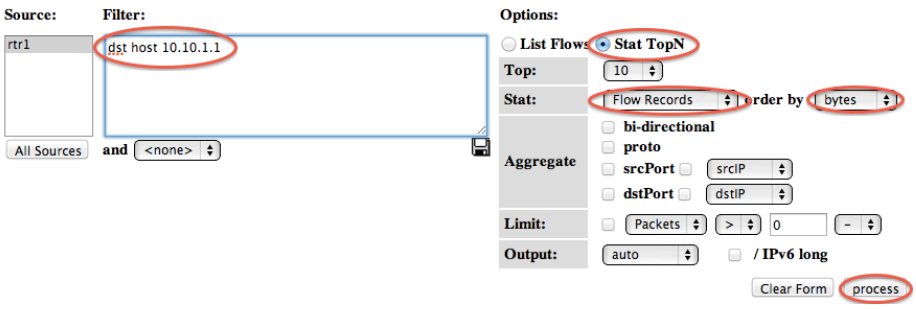


Figure 10: Наибольшие потоки на один хост

Вы должны увидеть входящие потоки для этой машины, начиная с самого большого. Как и раньше, мы видим только большие индивидуальные потоки, тогда как набор маленьких потоков может суммарно составлять больший трафик.

Поскольку мы рассматриваем только потоки к одному конкретному IP, мы можем сгруппировать эти записи по исходящему IP.

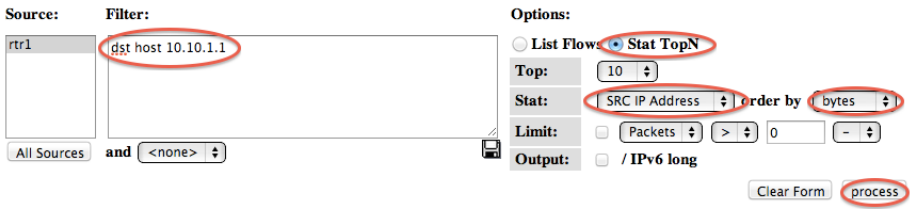


Figure 11: Потоки на один хост, сгруппированные по исходящему IP адресу

```
** 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 12: Вывод: Потоки на один хост, сгруппированные по исходящему IP адресу

Теперь у нас есть одна строка для каждого адреса с которого наша машина скачивала данные, с суммарным количеством скачанных байт для каждого исходящего адреса, от большего к меньшему.

6.1 Информация об IP адресе

Нажав на IP адрес, мы получим информацию из обратного DNS и из whois.

7 Дополнительное управление: агрегирование потоков

NfSen предлагает и другие методы для получения сводок о потоках, используя флажки Aggregate. В этом примере мы снова рассмотрим трафик, приходящий в нашу сеть.

Когда вы отметите один или несколько флажков Aggregate, NfSen скомбинирует все потоки, которые имеют одинаковые значения выбранных атрибутов.

Для начала, установите фильтр в dst net 10.10.X.0/24 (X = ваша группа). Выберите “Stat TopN”, “Stat:” -> “Flow Records”, “order by” -> “bytes”.

Figure 13: Информация whois

Затем попробуйте следующие агрегаторы, не забывая нажимать “process” после каждого.

- Отметьте “proto”. Вы получите одну строчку для TCP, одну для UDP, и одну для ICMP, показывающие общий трафик для каждого протокола. Иногда вы увидите и другие протоколы, активные в вашей сети (например, протокол 50 = IPSEC ESP; в Linux, файл /etc/protocols перечисляет все протоколы)
- Отметьте и “proto” и “srcPort”. Это скажет NfSen скомбинировать потоки, имеющие одинаковые протокол *и* исходящий порт. В зависимости от сетевой активности, вы увидите одну строчку для TCP порта 80, другую для TCP порта 443, третью для UDP порта 53, и так далее.
- Отметьте только “srcIP”. Вы получите одну строчку для каждого отдельного исходящего IP – точно так же, как если бы вы выбрали “Stat SRC IP”.
- Отметьте “srcIP” и “dstIP”. Вы получите отдельную строку для каждой пары “исходящий IP”/“входящий IP”, с общим трафиком между этими точками.

Как вы поменяете фильтр для того, чтобы смотреть на исходящий трафик, а не на входящий трафик?

Если у вас есть роутер с полной таблицей BGP, вы можете агрегировать записи потоков по номеру AS. Это поможет найти, с какими сетями вы обмениваетесь трафиком больше всего.