NETFlows

All about analyzing flows while preserving privacy

Thilina Pathirana

Introduction

- Privacy concerns today
- Analyzing traffic usually is done by examining packets – Deep packet inspection or by UTM devices
- Looking at “calling information” can reveal much:
  - Source IP address and port
  - Destination IP address and port
  - Protocol, Timestamps
  - Number of packets, Bytes
- Can be used as an IDS
- Can be use as policy enforcement

How to do it

- This can be monitored using NETflows…
- Developed by Cisco
- It can characterize traffic
- Account for how and where it flows
- Help optimize network investment
- Traffic engineering/network planning
- Provide usage-based billing

Netflow Basics

- Netflow characteristics must:
  - Be scalable
  - Be manageable
  - Be reliable

Example

- Lets consider a Computer A Web browses to Computer B this will generate 2 flows:
- Request Flow:
  - A: (TCP) 10.2.3.4:3863 -> 10.3.2.1: 80
- Reply Flow:
  - B: (TCP) 10.3.2.1:80 -> 10.2.3.4:3863

Exercise: Identify Flows

- Which of these six packets are in the same (bidirectional) flows?

No	SRC IP	DST IP	Proto	SRC Port	DST Port
1	10.10.10.1	10.10.10.2	6	3546	80
2	10.10.10.2	10.10.10.1	6	80	3546
3	192.168.2.5	172.16.1.6	6	6726	443
4	192.168.2.5	172.16.1.6	6	6727	443
5	172.16.110.3	172.16.0.1	17	4553	53
6	172.16.0.1	172.16.110.3	17	53	4553

Exercise: Identify Flows

- Which of these six packets are in the same (bidirectional) flows?

No	SRC IP	DST IP	Proto	SRC Port	DST Port
1	10.10.10.1	10.10.10.2	6 (TCP)	3546	80
2	10.10.10.2	10.10.10.1	6 (TCP)	80	3546
3	192.168.2.5	172.16.1.6	6 (TCP)	6726	443
4	192.168.2.5	172.16.1.6	6 (TCP)	6727	443
5	172.16.110.3	172.16.0.1	17 (UDP)	4553	53
6	172.16.0.1	172.16.110.3	17 (UDP)	53	4553

Exercise: Identify Flows

- Which of these six packets are in the same (bidirectional) flows?

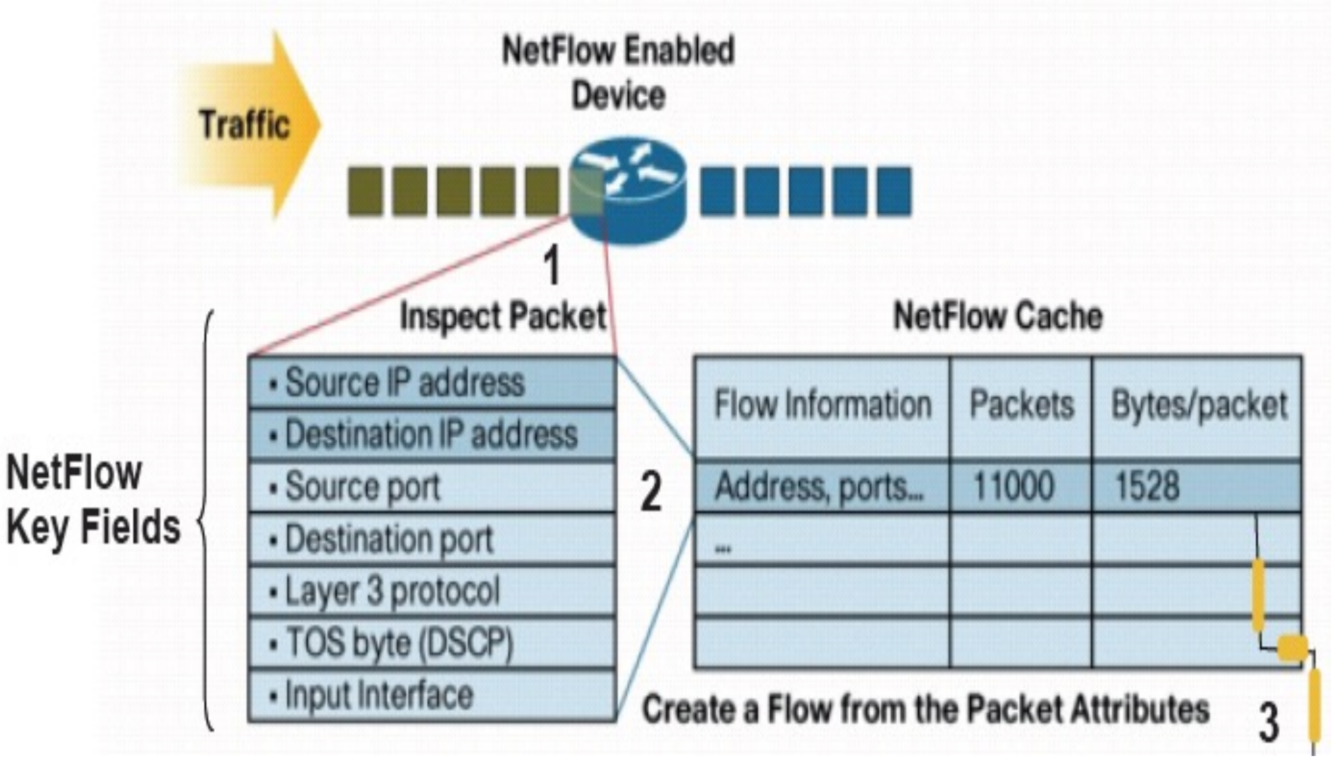
No	SRC IP	DST IP	Proto	SRC Port	DST Port
1	10.10.10.1	10.10.10.2	6 (TCP)	3546	80
2	10.10.10.2	10.10.10.1	6 (TCP)	80	3546
3	192.168.2.5	172.16.1.6	6 (TCP)	6726	443
4	192.168.2.5	172.16.1.6	6 (TCP)	6727	443
5	172.16.110.3	172.16.0.1	17 (UDP)	4553	53
6	172.16.0.1	172.16.110.3	17 (UDP)	53	4553

NetFlow Typical Record

- Source and destination IP address
- Source and destination ports
- Transport protocol: TCP,UDP, ICMP, etc.
- Type of service (ToS)
- Packet and byte counts
- Start and end timestamps
- Input and output interface numbers
- TCP flags
- Routing information (next-hop address, source autonomous system (AS) number, destination AS number, source prefix mask, destination prefix mask)

NetFlow Typical Record

- Flow path (source Cisco.com)



Inspect Packet

NetFlow Key Fields

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol
- TOS byte (DSCP)
- Input Interface

NetFlow Cache

Flow Information	Packets	Bytes/packet
Address, ports...	11000	1528
...		

Create a Flow from the Packet Attributes

NetFlow Data Cache

- Available on Cisco routers/switches
- Available on Juniper/Huwai routers
- Cached on devices
- Netflow like sflow for HP devices

- WARNING! Not all devices are NetFlow-enabled!

NetFlow Data Cache

```
#show ip cache flow
IP packet size distribution (78630M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .002 .448 .062 .027 .013 .011 .008 .011 .003 .003 .002 .006 .005 .003 .002
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .002 .003 .015 .033 .331 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 6553988 bytes
  32929 active, 32607 inactive, 524367786 added
  4111490554 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 794824 bytes
  32895 active, 16257 Inactive, 519171584 added, 519168554 added to flow
  0 alloc failures, 12911870 force free
  3 chunks, 1155 chunks added
  last clearing of statistics never
--More—
```

NetFlow Data Cache

```
Protocol        Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------        Flows     /Sec      /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet     3833510      0.8          10   179      9.2        9.0       26.8
TCP-FTP       12511306       2.9         6   132     19.7        6.3      16.5
TCP-FTPD       1194796       0.2       544   866    151.5       86.7      21.2
TCP-WWW      944754736     219.9        13   627   2871.0        3.2      23.7
TCP-SMTP      53320030      12.4        14   399    185.8        6.6      19.2
TCP-X           913841       0.2        41   631      8.9       19.2      24.5
TCP-BGP           1867       0.0         1    49      0.0        0.5      20.5
TCP-NNTP       1086658       0.2       252   874     63.8       15.2      26.8
TCP-Frag        228697      0.0          9   131      0.5        6.5       25.3
TCP-other   2264274585    527.1         23   568  12466.6       12.9       24.4
UDP-DNS      231113128      53.8         2    79    114.7        3.6      26.0
--More—
```

NetFlow Limitations of Cache

- Difficult to read
- Only shows recent activity
- No automation on devices for analysis
- No accounting of flows (besides overall totals)

NetFlow Export of Data

- Greatly enhances NetFlow and turns the technology into a analysis tool!
- Data sent to external collector(s)
- Analyzed by one or more systems
- Archived for other concerns
- Efficient: Uses multiple records per UDP packet

NetFlow Export: Establish Policies!

- Ensure policies are in place before deploying covering:
    - Retention of network usage statistics
    - Establish a retention policy.
    - Privacy protection of the data, who is authorized, no offloading without sanitizing personal data (the host portion)
- While the contents of the packet are not recorded, the calling information can still be a concern.
- However, with virtual servers, it is impossible to know the true destination
- Mostly it can only be used as verification that something occurred.

Netflow Export Versions

- Multiple netflow export options (v5,v9,v10)
- Each version defines their own “common properties” and export packet format
- Most common is v5, does not support IPv6 traffic, MAC addresses, VLANs or other extension fields.
- v9 used as basis for the standard IPFIX (IP flow information export), described in RFC 3954 known also as flexible NetFlow. It supports IPv6 as well as the fields missing in NetFlow v5.
- v10 IPFIX, standardized by IETF, extended version of NetFlow v9 that supports variable length fields (e.g. HTTP hostname or HTTP URL) as well as Enterprise-defined fields.
- sFlow: Sampling based, commonly found on HP switches and routers
- jFlow: Juniper

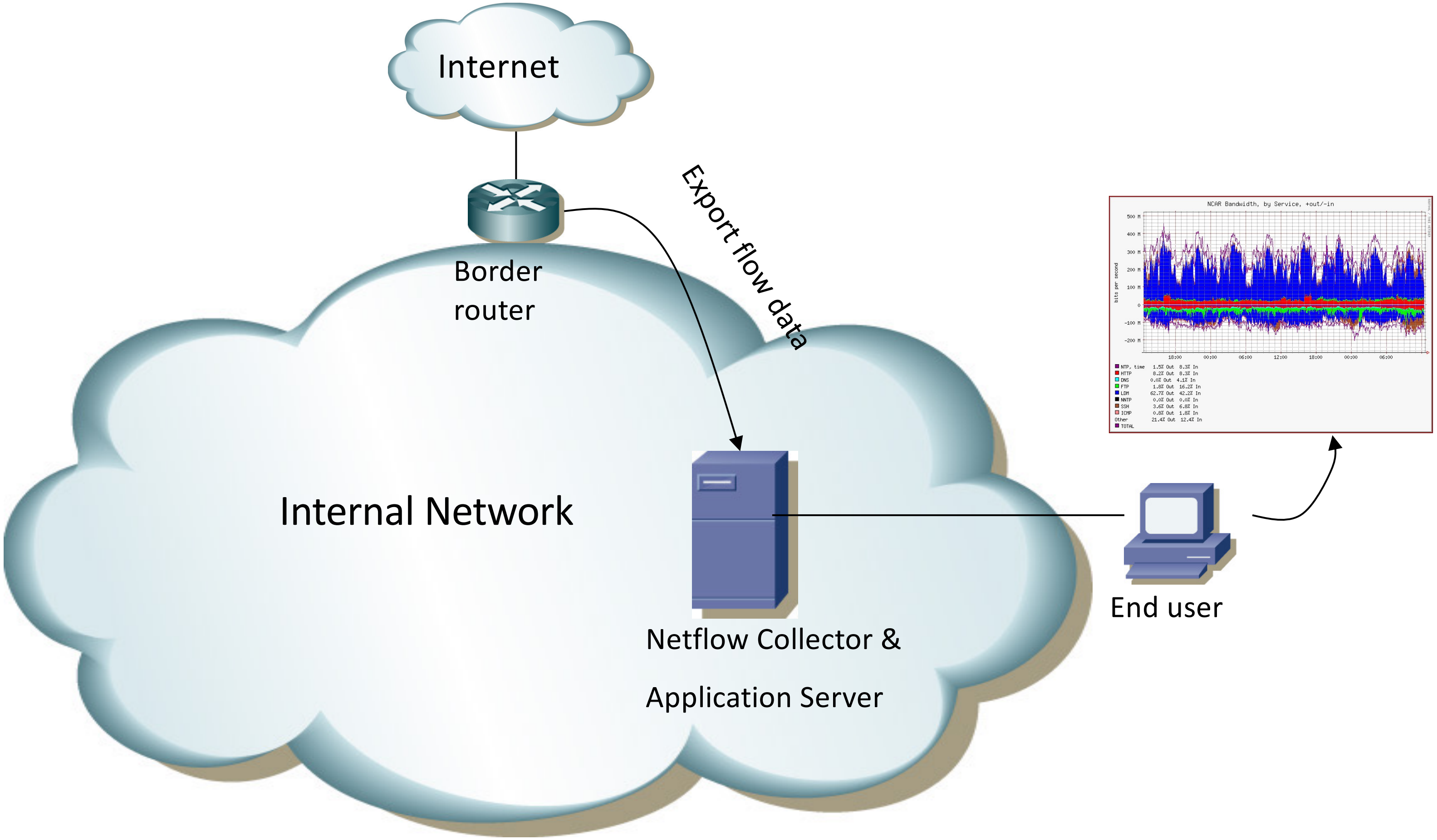
Deploying Netflow

Overview – Typical Deployment

Basic steps to Deploy Netflow

- Determine which routers/interfaces to enable netflow
- Configure Routers
- Setup netflow collectors
- Choose and configure an application

Overview - Typical Deployment

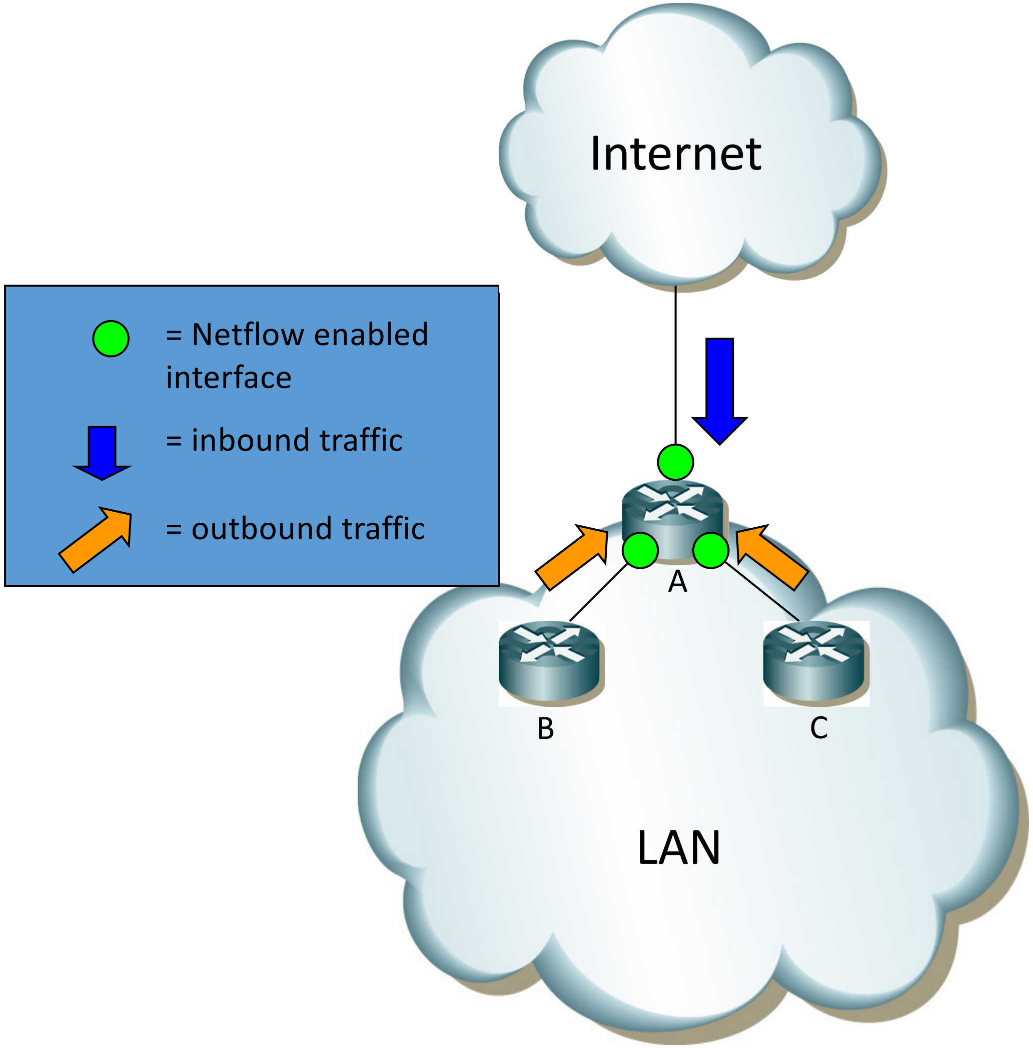


Determine which routers/interfaces to enable netflow

Enable netflow on selected interfaces to capture all inbound/outbound traffic

Neflow only enabled inbound on an interface

Avoid double counting!!



Collector Hardware

Minimum for us:

- CPU i5 or better
- RAM 4GB or better
- HDD 500GB or better
  (more space – more retention time)
- Network 1Gbps

Looking at collected flow data: nfcapd/nfdump

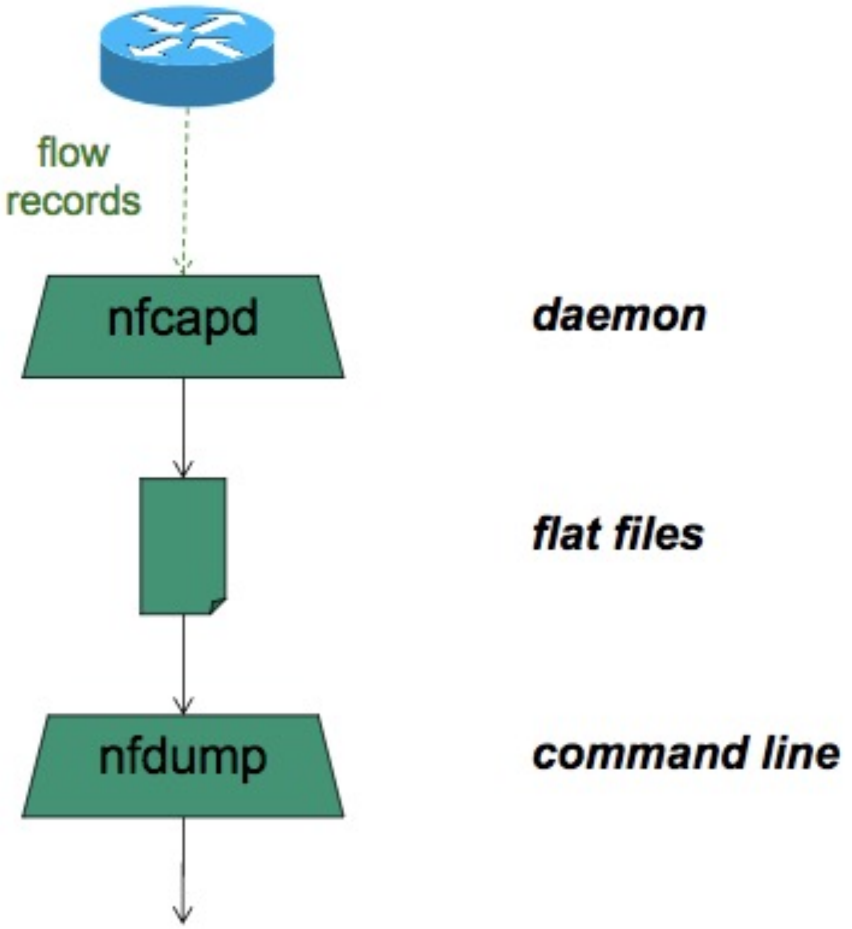
Free and open source – Runs on collector

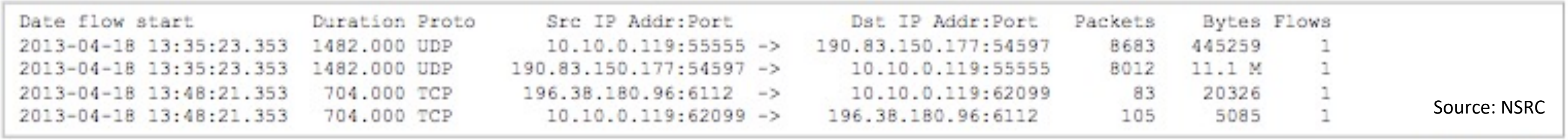
nfcapd listens for incoming flow records and writes them to disk (flat files)- typically starts a new file every 5 minutes

nfdump reads the files and turns them into human-readable output

nfdump has command line options to filter and aggregate the flows

Looking at collected flow data: nfcapd/nfdump





```
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2013-04-18 13:35:23.353  1482.000 UDP      10.10.0.119:55555 ->  190.83.150.177:54597     8683   445259     1
2013-04-18 13:35:23.353  1482.000 UDP   190.83.150.177:54597 ->     10.10.0.119:55555     8012   11.1 M     1
2013-04-18 13:48:21.353   704.000 TCP    196.38.180.96:6112  ->     10.10.0.119:62099       83    20326     1
2013-04-18 13:48:21.353   704.000 TCP      10.10.0.119:62099 ->   196.38.180.96:6112       105     5085     1
```

Source: NSRC

Looking at collected flow data: nfsen

Companion to NfDump tools

NfDump tools collect netflow data and store them in files

Processing netflow data with NfDump tools can only be done on the command line

NfSen is a graphical (Web Based) front end to NfDump

Creates RRD graphs based on stored data

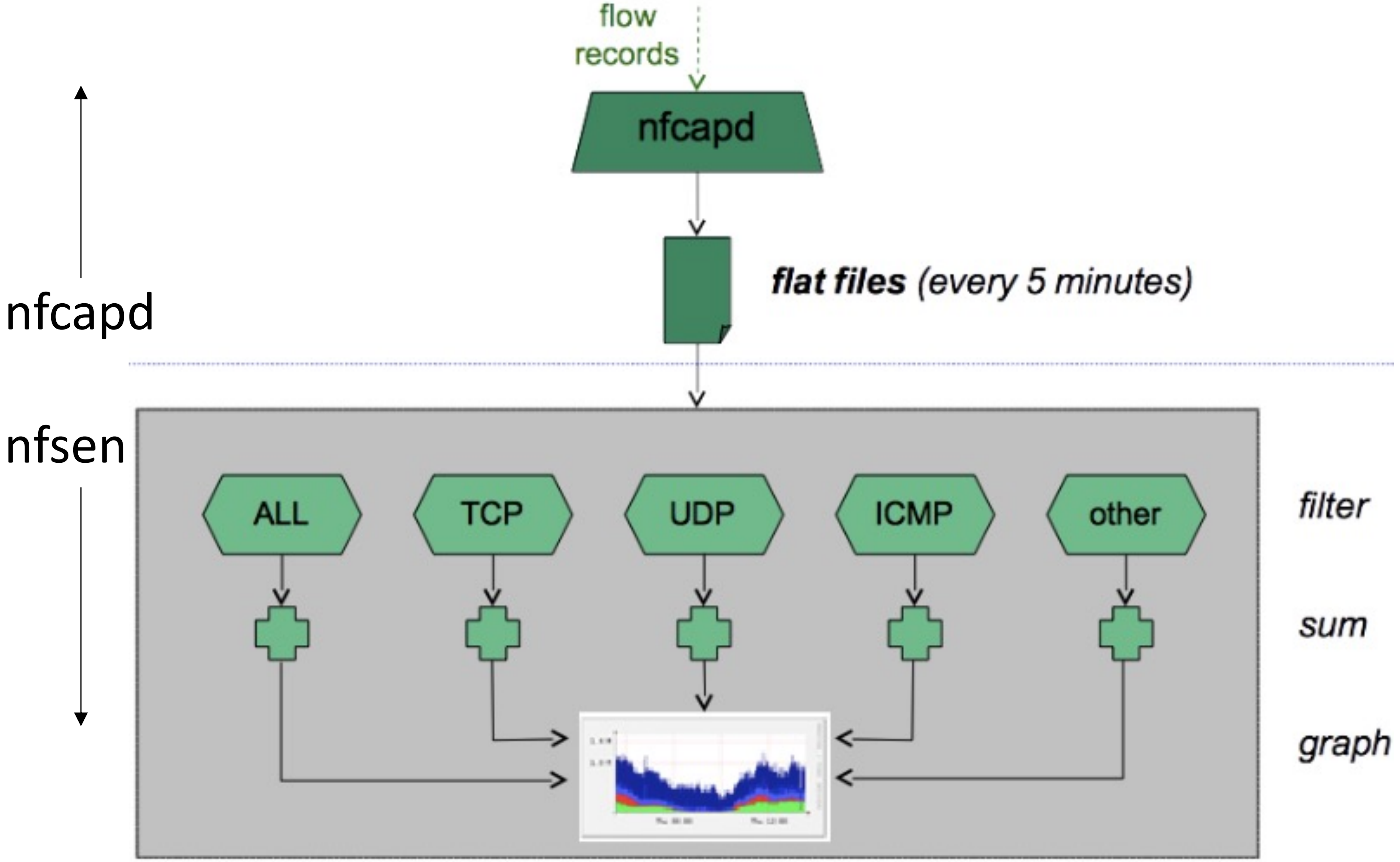
Plugins extend the functionality of base (e.g. PortTracker and SURFmap)

Looking at collected flow data: nfsen

NfSen allows you to:

- Easily navigate through the netflow data
- Process the netflow data within the specified time span
- Create history as well as continuous profiles
- Set alerts, based on various conditions
- Write your own plugins to process netflow data on a regular interval

Looking at collected flow data: nfsen



Source: NSRC

NFSEN structure

Configuration file - nfsen.conf

NfDump files - Netflow files containing collected flows stored in the directory:

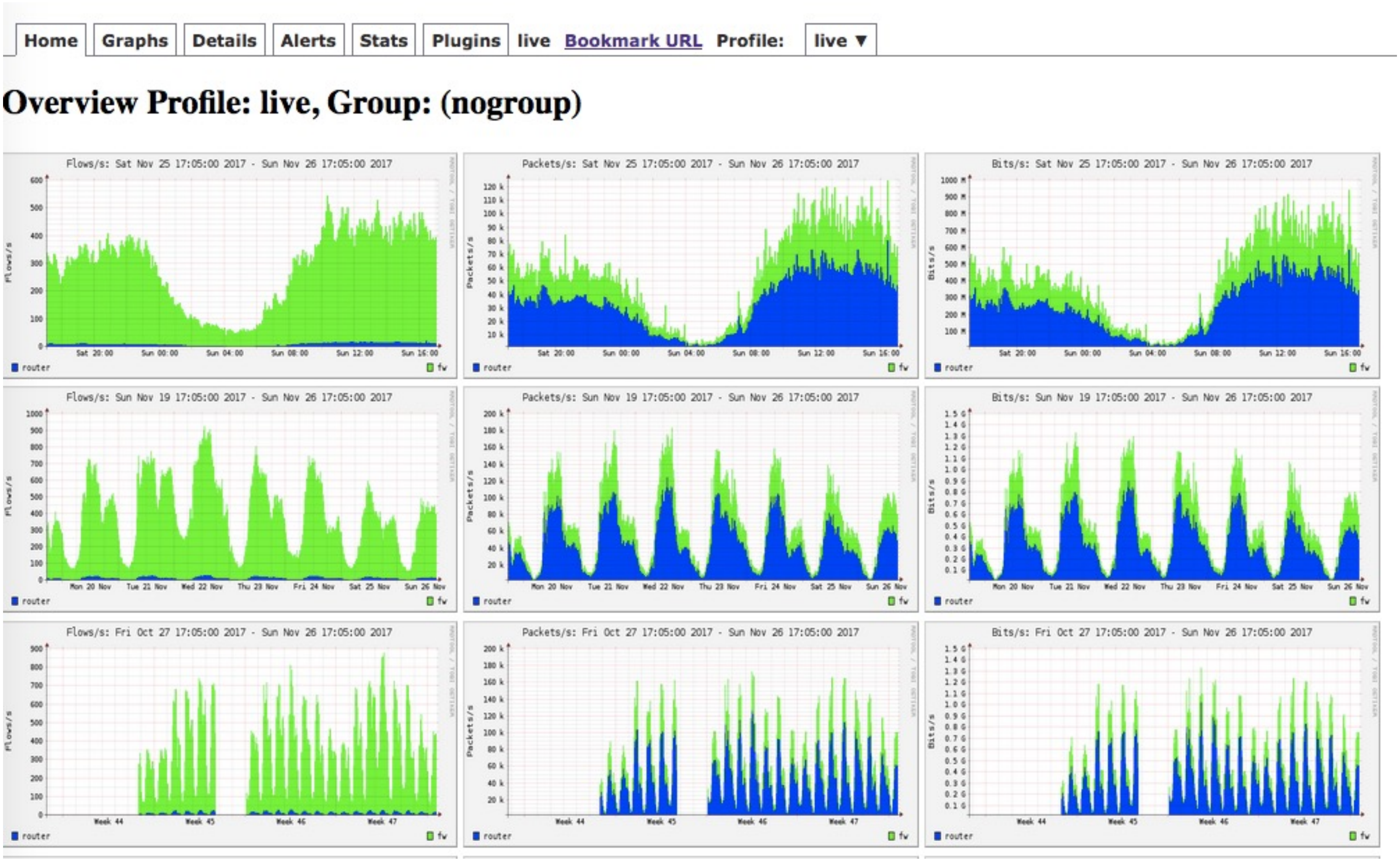
/var/nfsen/profiles-data

Note: It is possible for other programs to read NFDump files but don't store them for too long as they can fill up your drive

Actual graphs stored in the directory:

/var/nfsen/profiles-stat

NFSEN Home page



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

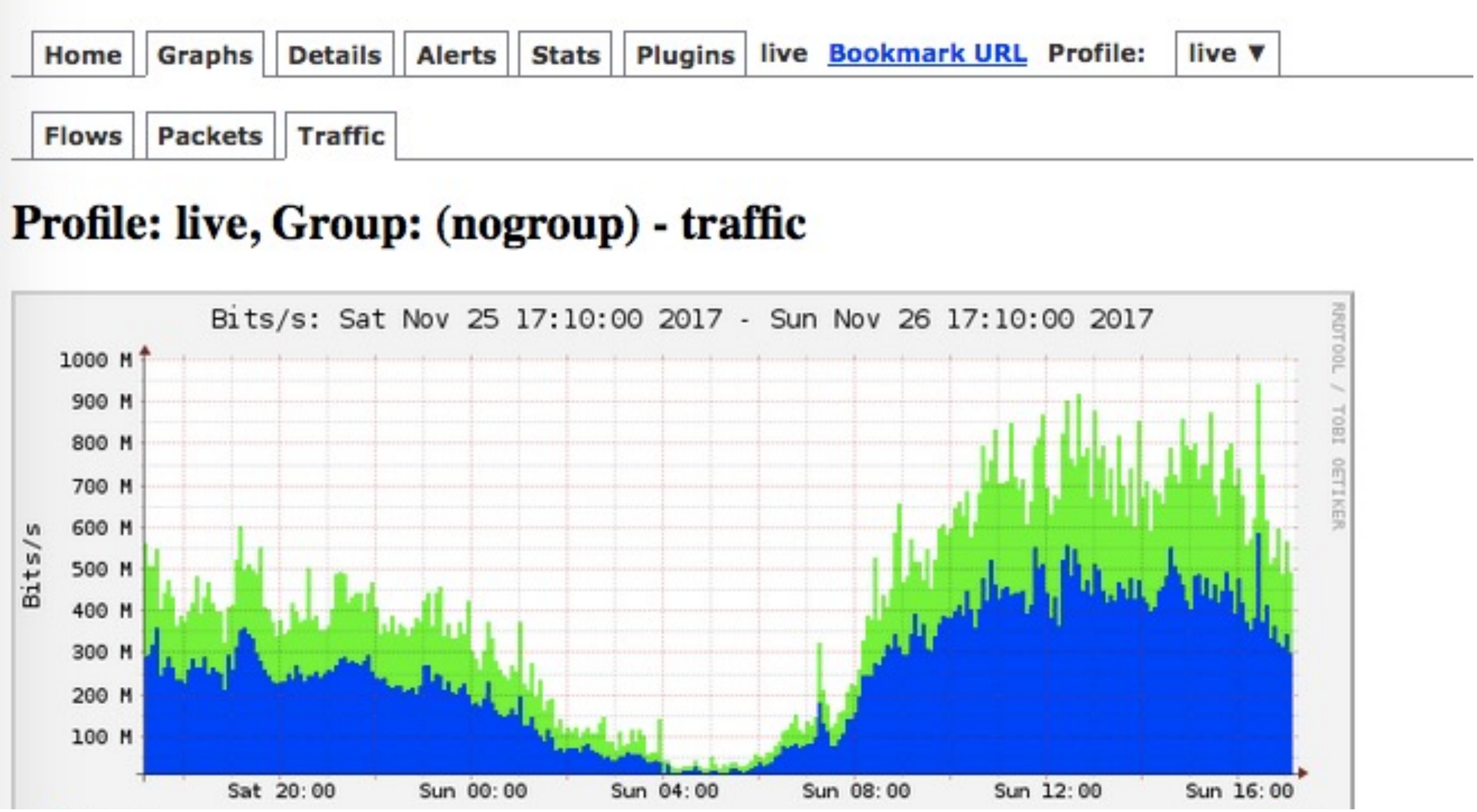
Overview Profile: live, Group: (nogroup)

Flows/s: Sat Nov 25 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Packets/s: Sat Nov 25 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Bits/s: Sat Nov 25 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Flows/s: Sun Nov 19 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Packets/s: Sun Nov 19 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Bits/s: Sun Nov 19 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Flows/s: Fri Oct 27 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Packets/s: Fri Oct 27 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Bits/s: Fri Oct 27 17:05:00 2017 - Sun Nov 26 17:05:00 2017
Flows/s
Packets/s
Bits/s
Sat 20:00
Sun 00:00
Sun 04:00
Sun 08:00
Sun 12:00
Sun 16:00
Mon 20 Nov
Tue 21 Nov
Wed 22 Nov
Thu 23 Nov
Fri 24 Nov
Sat 25 Nov
Sun 26 Nov
Week 44
Week 45
Week 46
Week 47
router
fw

Graphs page

Graphs of flows, packets and traffic based on interface with NetFlow activated

What is seen under Traffic should closely match what your NMS shows for the same interface



Profile: live, Group: (nogroup) - traffic

Bits/s: Sat Nov 25 17:10:00 2017 - Sun Nov 26 17:10:00 2017

Details page

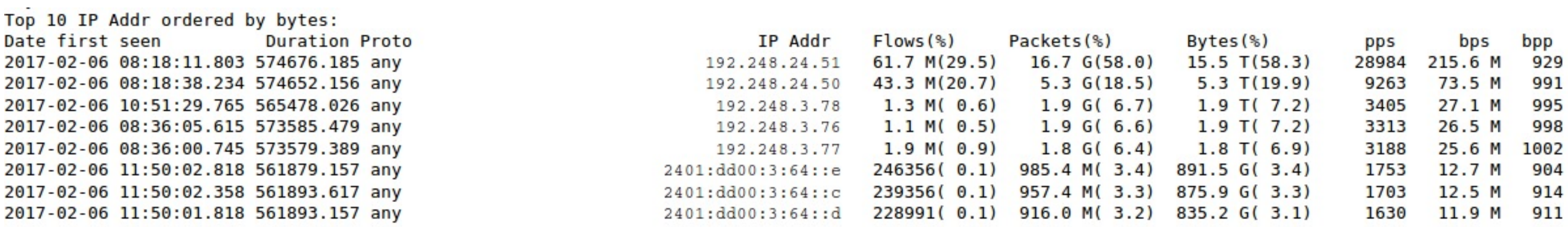
Most interesting page

Can view present flow information or stored flow information

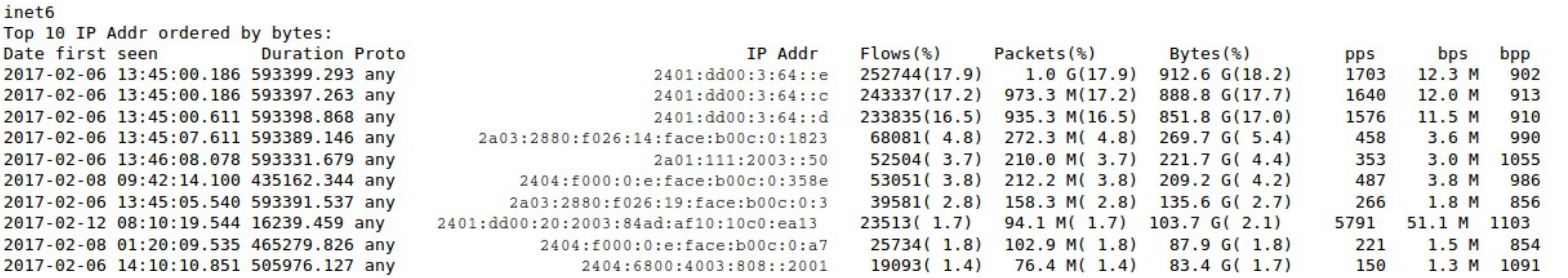
Can view detailed NetFlow information such as

- Src hosts/ports, destination hosts and ports
- Unidirectional or Bi-directional flows
- Flows on specific interfaces
- Protocols and TOS

Example measurements



```
Top 10 IP Addr ordered by bytes:
Date first seen          Duration Proto                                IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2017-02-06 08:18:11.803 574676.185 any                           192.248.24.51   61.7 M(29.5)   16.7 G(58.0)   15.5 T(58.3)   28984  215.6 M   929
2017-02-06 08:18:38.234 574652.156 any                           192.248.24.50   43.3 M(20.7)    5.3 G(18.5)    5.3 T(19.9)    9263   73.5 M   991
2017-02-06 10:51:29.765 565478.026 any                            192.248.3.78    1.3 M( 0.6)    1.9 G( 6.7)    1.9 T( 7.2)    3405   27.1 M   995
2017-02-06 08:36:05.615 573585.479 any                            192.248.3.76    1.1 M( 0.5)    1.9 G( 6.6)    1.9 T( 7.2)    3313   26.5 M   998
2017-02-06 08:36:00.745 573579.389 any                            192.248.3.77    1.9 M( 0.9)    1.8 G( 6.4)    1.8 T( 6.9)    3188   25.6 M  1002
2017-02-06 11:50:02.818 561879.157 any                        2401:dd00:3:64::e   246356( 0.1)  985.4 M( 3.4)  891.5 G( 3.4)    1753   12.7 M   904
2017-02-06 11:50:02.358 561893.617 any                        2401:dd00:3:64::c   239356( 0.1)  957.4 M( 3.3)  875.9 G( 3.3)    1703   12.5 M   914
2017-02-06 11:50:01.818 561893.157 any                        2401:dd00:3:64::d   228991( 0.1)  916.0 M( 3.2)  835.2 G( 3.1)    1630   11.9 M   911
```



```
inet6
Top 10 IP Addr ordered by bytes:
Date first seen          Duration Proto                                IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2017-02-06 13:45:00.186 593399.293 any                        2401:dd00:3:64::e   252744(17.9)    1.0 G(17.9)  912.6 G(18.2)    1703   12.3 M   902
2017-02-06 13:45:00.186 593397.263 any                        2401:dd00:3:64::c   243337(17.2)  973.3 M(17.2)  888.8 G(17.7)    1640   12.0 M   913
2017-02-06 13:45:00.611 593398.868 any                        2401:dd00:3:64::d   233835(16.5)  935.3 M(16.5)  851.8 G(17.0)    1576   11.5 M   910
2017-02-06 13:45:07.611 593389.146 any        2a03:2880:f026:14:face:b00c:0:1823    68081( 4.8)  272.3 M( 4.8)  269.7 G( 5.4)     458    3.6 M   990
2017-02-06 13:46:08.078 593331.679 any                        2a01:111:2003::50    52504( 3.7)  210.0 M( 3.7)  221.7 G( 4.4)     353    3.0 M  1055
2017-02-08 09:42:14.100 435162.344 any             2404:f000:0:e:face:b00c:0:358e    53051( 3.8)  212.2 M( 3.8)  209.2 G( 4.2)     487    3.8 M   986
2017-02-06 13:45:05.540 593391.537 any           2a03:2880:f026:19:face:b00c:0:3    39581( 2.8)  158.3 M( 2.8)  135.6 G( 2.7)     266    1.8 M   856
2017-02-12 08:10:19.544 16239.459 any     2401:dd00:20:2003:84ad:af10:10c0:ea13    23513( 1.7)   94.1 M( 1.7)  103.7 G( 2.1)    5791   51.1 M  1103
2017-02-08 01:20:09.535 465279.826 any               2404:f000:0:e:face:b00c:0:a7    25734( 1.8)  102.9 M( 1.8)   87.9 G( 1.8)     221    1.5 M   854
2017-02-06 14:10:10.851 505976.127 any                  2404:6800:4003:808::2001    19093( 1.4)   76.4 M( 1.4)   83.4 G( 1.7)     150    1.3 M  1091
```

Flow Analysis

Know Thy Network!

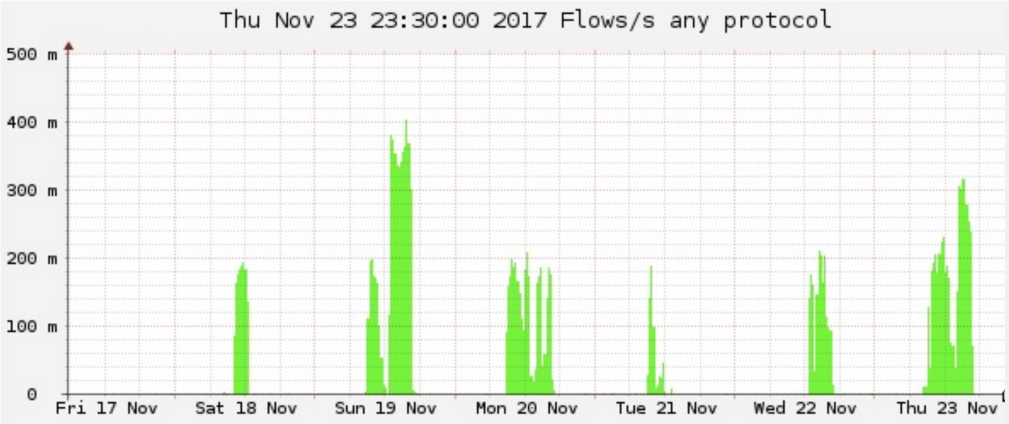
- NetFlow records the communication between systems
- Quickly tells you what is happening on your network at a high level
- Can be used to spot anomalies
- Simple IDS capabilities
- Locate all stations doing the same thing on the network
- Policy enforcement
- Who is using various services
- Impact on closing down ports
- Location of servers

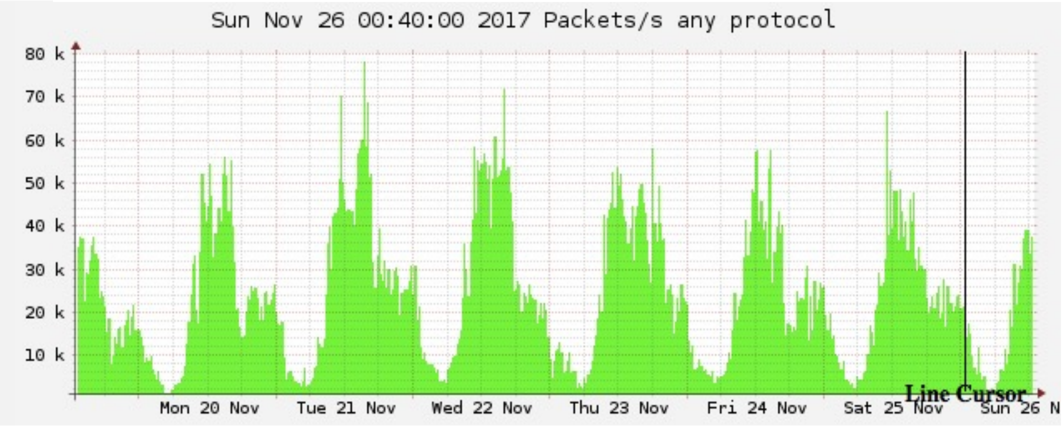
Planning/Policies Make for Success

- Establish policies as to what traffic is allowed
- Establish specific pathways or gateways for traffic like SMTP, Proxy - HTTP, etc.
- Any traffic not flowing through these gateways are your indicator for problems
- Segregate servers and workstations with subnets.

Flow Size Can Tell a Story

- Always keep an eye on the NetFlow sizes
- Works best after a baseline of a few days or weeks of observation.
- General fluctuations are normal traffic patterns, but a sudden surge indicates something new is going on.
- Sudden drops could indicate network problems.



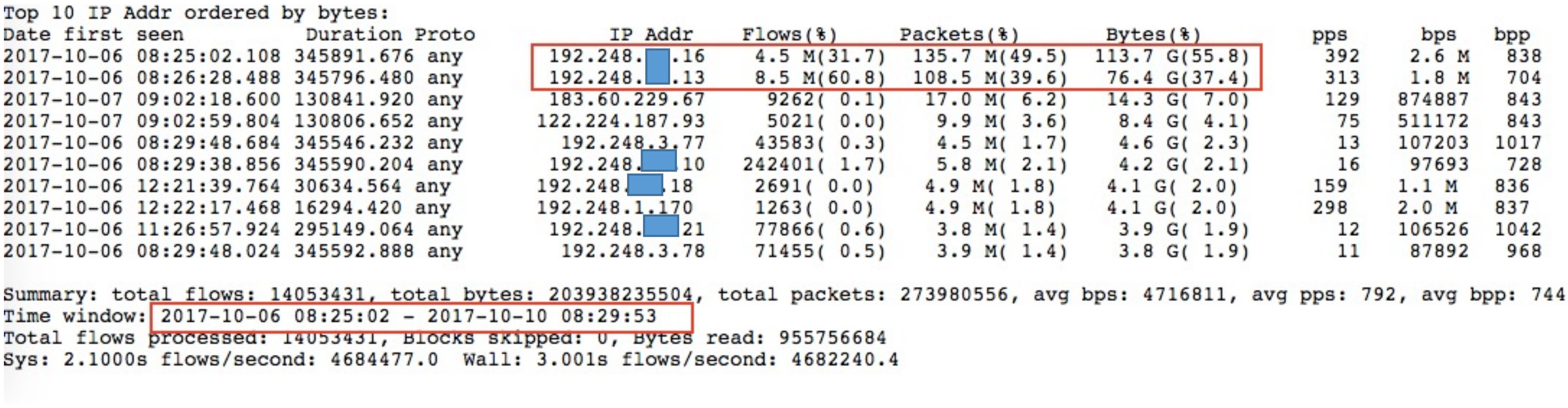


Analysis: Finding the Needles

- Which Port, Source, Destination?
- Which County?
- Which Source?
- Which Destination?
- How many flows/bytes?

Recent Example

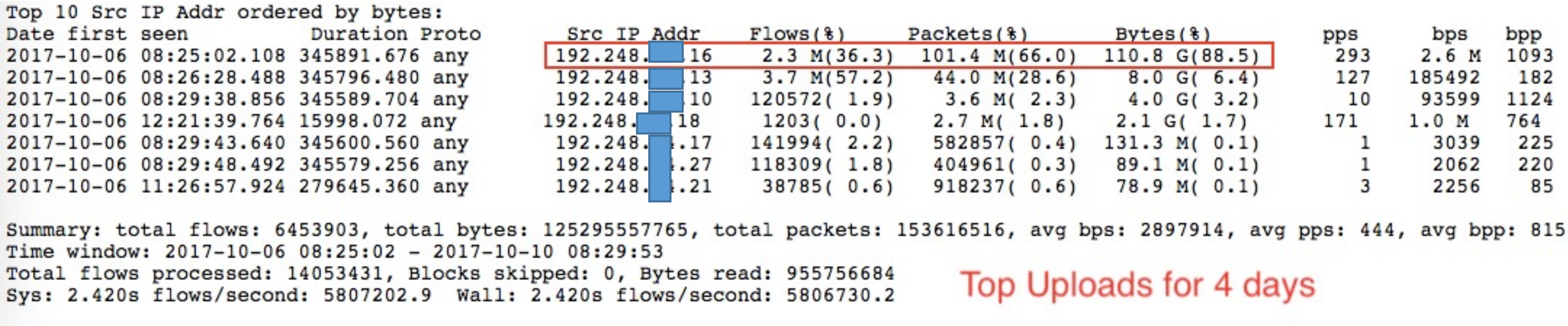
- Unusual upload detected from one of the vpls links, we were interested finding what's going on as it resulted in having losses in video conference calls among institutes.



```
Top 10 IP Addr ordered by bytes:
Date first seen          Duration Proto          IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2017-10-06 08:25:02.108 345891.676 any     192.248.[redacted].16    4.5 M(31.7)   135.7 M(49.5)   113.7 G(55.8)     392    2.6 M   838
2017-10-06 08:26:28.488 345796.480 any     192.248.[redacted].13    8.5 M(60.8)   108.5 M(39.6)    76.4 G(37.4)     313    1.8 M   704
2017-10-07 09:02:18.600 130841.920 any    183.60.229.67     9262( 0.1)    17.0 M( 6.2)    14.3 G( 7.0)     129   874887   843
2017-10-07 09:02:59.804 130806.652 any   122.224.187.93     5021( 0.0)     9.9 M( 3.6)     8.4 G( 4.1)      75   511172   843
2017-10-06 08:29:48.684 345546.232 any      192.248.3.77    43583( 0.3)     4.5 M( 1.7)     4.6 G( 2.3)      13   107203  1017
2017-10-06 08:29:38.856 345590.204 any     192.248.[redacted]10   242401( 1.7)     5.8 M( 2.1)     4.2 G( 2.1)      16    97693   728
2017-10-06 12:21:39.764 30634.564 any     192.248[redacted].18     2691( 0.0)    4.9 M( 1.8)    4.1 G( 2.0)     159    1.1 M   836
2017-10-06 12:22:17.468 16294.420 any     192.248.1.170     1263( 0.0)    4.9 M( 1.8)    4.1 G( 2.0)     298    2.0 M   837
2017-10-06 11:26:57.924 295149.064 any     192.248.[redacted]21    77866( 0.6)     3.8 M( 1.4)     3.9 G( 1.9)      12   106526  1042
2017-10-06 08:29:48.024 345592.888 any      192.248.3.78    71455( 0.5)     3.9 M( 1.4)     3.8 G( 1.9)      11    87892   968

Summary: total flows: 14053431, total bytes: 203938235504, total packets: 273980556, avg bps: 4716811, avg pps: 792, avg bpp: 744
Time window: 2017-10-06 08:25:02 - 2017-10-10 08:29:53
Total flows processed: 14053431, Blocks skipped: 0, Bytes read: 955756684
Sys: 2.1000s flows/second: 4684477.0  Wall: 3.001s flows/second: 4682240.4
```

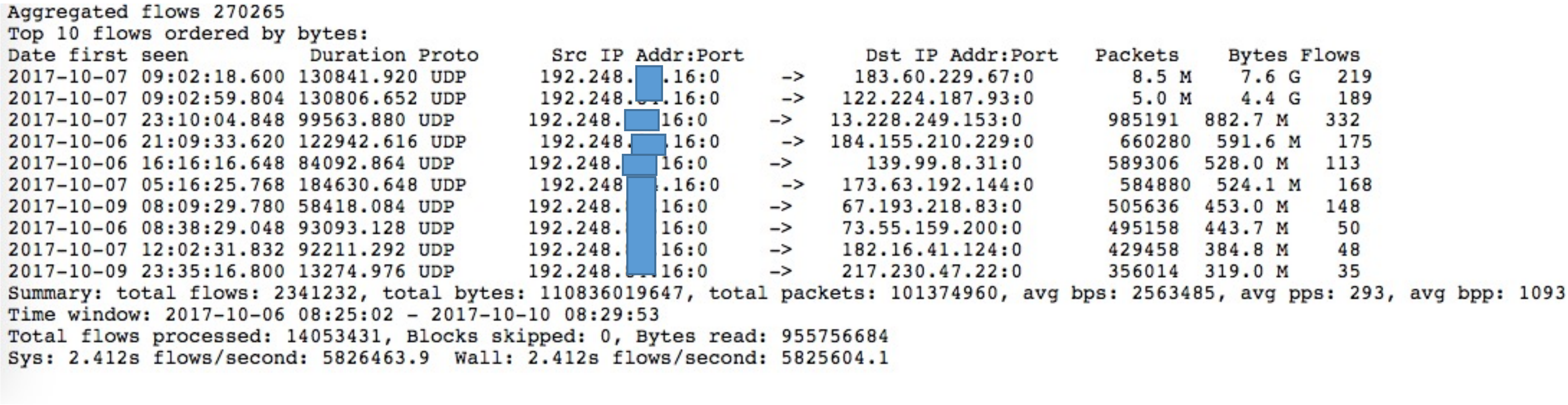
Recent Example cont…



```
Top 10 Src IP Addr ordered by bytes:
Date first seen          Duration Proto       Src IP Addr        Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2017-10-06 08:25:02.108 345891.676 any      192.248.[redacted].16     2.3 M(36.3)  101.4 M(66.0)  110.8 G(88.5)     293    2.6 M  1093
2017-10-06 08:26:28.488 345796.480 any      192.248.[redacted].13     3.7 M(57.2)   44.0 M(28.6)    8.0 G( 6.4)     127   185492   182
2017-10-06 08:29:38.856 345589.704 any      192.248.[redacted].10   120572( 1.9)     3.6 M( 2.3)    4.0 G( 3.2)      10    93599  1124
2017-10-06 12:21:39.764 15998.072 any      192.248.[redacted]18      1203( 0.0)    2.7 M( 1.8)    2.1 G( 1.7)    171    1.0 M   764
2017-10-06 08:29:43.640 345600.560 any      192.248.[redacted].17   141994( 2.2)   582857( 0.4)  131.3 M( 0.1)       1     3039   225
2017-10-06 08:29:48.492 345579.256 any      192.248.[redacted].27   118309( 1.8)   404961( 0.3)   89.1 M( 0.1)       1     2062   220
2017-10-06 11:26:57.924 279645.360 any      192.248.[redacted].21    38785( 0.6)   918237( 0.6)   78.9 M( 0.1)       3     2256    85

Summary: total flows: 6453903, total bytes: 125295557765, total packets: 153616516, avg bps: 2897914, avg pps: 444, avg bpp: 815
Time window: 2017-10-06 08:25:02 - 2017-10-10 08:29:53
Total flows processed: 14053431, Blocks skipped: 0, Bytes read: 955756684
Sys: 2.420s flows/second: 5807202.9  Wall: 2.420s flows/second: 5806730.2
```

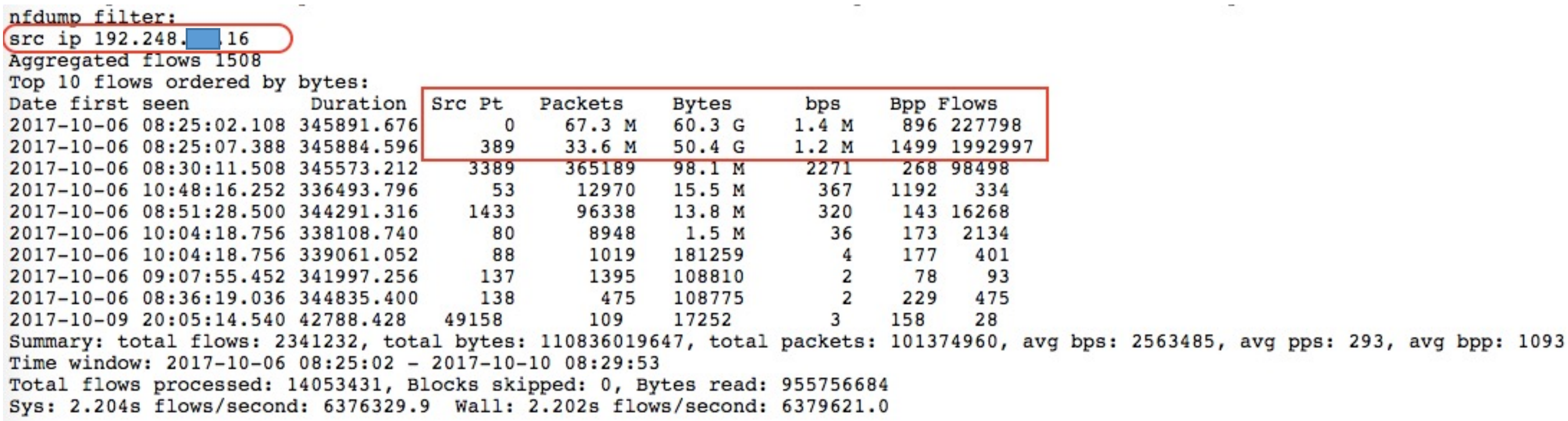
Top Uploads for 4 days



```
Aggregated flows 270265
Top 10 flows ordered by bytes:
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2017-10-07 09:02:18.600 130841.920 UDP     192.248.[redacted].16:0    ->    183.60.229.67:0      8.5 M    7.6 G   219
2017-10-07 09:02:59.804 130806.652 UDP     192.248.[redacted].16:0    ->   122.224.187.93:0      5.0 M    4.4 G   189
2017-10-07 23:10:04.848 99563.880 UDP     192.248.[redacted]16:0    ->  13.228.249.153:0     985191  882.7 M   332
2017-10-06 21:09:33.620 122942.616 UDP     192.248.[redacted].16:0    ->  184.155.210.229:0     660280  591.6 M   175
2017-10-06 16:16:16.648 84092.864 UDP     192.248.[redacted]16:0    ->      139.99.8.31:0     589306  528.0 M   113
2017-10-07 05:16:25.768 184630.648 UDP     192.248[redacted].16:0    ->   173.63.192.144:0     584880  524.1 M   168
2017-10-09 08:09:29.780 58418.084 UDP     192.248.[redacted]16:0    ->    67.193.218.83:0     505636  453.0 M   148
2017-10-06 08:38:29.048 93093.128 UDP     192.248.[redacted]16:0    ->    73.55.159.200:0     495158  443.7 M    50
2017-10-07 12:02:31.832 92211.292 UDP     192.248.[redacted]16:0    ->    182.16.41.124:0     429458  384.8 M    48
2017-10-09 23:35:16.800 13274.976 UDP     192.248.[redacted]16:0    ->    217.230.47.22:0     356014  319.0 M    35
Summary: total flows: 2341232, total bytes: 110836019647, total packets: 101374960, avg bps: 2563485, avg pps: 293, avg bpp: 1093
Time window: 2017-10-06 08:25:02 - 2017-10-10 08:29:53
Total flows processed: 14053431, Blocks skipped: 0, Bytes read: 955756684
Sys: 2.412s flows/second: 5826463.9  Wall: 2.412s flows/second: 5825604.1
```

Recent Example cont…

- Finally, look deep into the selected source.



```
nfdump filter:
src ip 192.248.[redacted].16
Aggregated flows 1508
Top 10 flows ordered by bytes:
Date first seen          Duration  Src Pt    Packets     Bytes       bps    Bpp Flows
2017-10-06 08:25:02.108 345891.676       0    67.3 M    60.3 G     1.4 M    896 227798
2017-10-06 08:25:07.388 345884.596     389    33.6 M    50.4 G     1.2 M   1499 1992997
2017-10-06 08:30:11.508 345573.212    3389    365189    98.1 M      2271    268 98498
2017-10-06 10:48:16.252 336493.796      53     12970    15.5 M       367   1192   334
2017-10-06 08:51:28.500 344291.316    1433     96338    13.8 M       320    143 16268
2017-10-06 10:04:18.756 338108.740      80      8948     1.5 M        36    173  2134
2017-10-06 10:04:18.756 339061.052      88      1019    181259         4    177   401
2017-10-06 09:07:55.452 341997.256     137      1395    108810         2     78    93
2017-10-06 08:36:19.036 344835.400     138       475    108775         2    229   475
2017-10-09 20:05:14.540 42788.428  49158       109    17252          3    158    28
Summary: total flows: 2341232, total bytes: 110836019647, total packets: 101374960, avg bps: 2563485, avg pps: 293, avg bpp: 1093
Time window: 2017-10-06 08:25:02 - 2017-10-10 08:29:53
Total flows processed: 14053431, Blocks skipped: 0, Bytes read: 955756684
Sys: 2.204s flows/second: 6376329.9  Wall: 2.202s flows/second: 6379621.0
```

- Why port ZERO?
- What are the next steps?

Filters

A filter is a collection of expressions

- expr1, expr2 and expr3, expr4 or expr5, not expr6, (expr7), not (expr8)

Each expression can specify things like

IP version:

- inet, ipv4, inet6, ipv6

Protocol:

- {proto} tcp, udp, icmp, gre, ...

IP Address:

- [src|dst] ip 10.10.10.1
- [src|dst] ip in <addr1> <addr2> <addr3>

Filters cont…

IP Network:

- [src|dst] net 172.16/16

Port:

- [src|dst] port 80
- [src|dst] port > 1024

TCP Flags:

- flags S
- flags S and not flags AFPRU

TOS:

- tos 8

Filters cont…

Bytes:

- bytes > 1024
- bytes = 64

Packets per second:

- pps > 10

Bits per second:

- bps > 10m

Bits per packet:

- bpp > 15

Duration of flow:

- duration > 36000000

AS Number:

- [src|dst] 23456

All numbers can have scaling factors:

k, m, g, t with 1024 as factor

Filters Examples

any	all traffic
proto tcp	only TCP traffic
dst ip 1.2.3.4	only traffic to 1.2.3.4
dst ip 2401:dd00:1::161	only traffic to 2401:dd00:1::161
dst net 10.10.1.0/24	only traffic to that range
not dst net 10.10.1.0/24	only traffic not to that range
proto tcp and src port 80	only TCP with source port 80
dst net 10.10.1.0/24 or dst net 10.10.2.0/24	only traffic to those nets
dst net 10.10.1.0/24 and proto tcp and src port 80	only HTTP response traffic to that net

(dst net 10.10.1.0/24 or dst net 10.10.2.0/24) and proto tcp and src port 80

Find a Worm using NetFlow

Can use different protocols

High flow count

Low packet count – 3 packets or less per flow

Downside: If the stations generate other traffic, it can obscure the worm activity

Email Virus Detection

- Systems infected with Email viruses can be detected via NetFlow due to:
  - Multiple mail messages per host in the same flow file (over 15 messages in 5 min)
  - Mail going directly to the border instead of authorized servers (requires policies).
    - Policy enforcement example!

IFRAME Exploit

- System suddenly generated a virus warning after visiting a well known, trusted website.
- System scan removed the known virus and downloader, but an undetectable trojan was downloaded during the event.
- Trojan NOT detectable after virus definition update and full system scan.
- System now displays ads and runs very slow
- Analysis of system required. Noted traffic involving LEARN-LAB IP address.

IFRAME Exploit: Examining traffic

srcIP	dstIP	proto	srcPort	dstPort	packets
10.10.10.23	192.248.6.45	6	3585	80	23
192.248.6.45	10.10.10.23	6	3585	80	34
10.10.10.23	192.248.6.41	6	3586	80	313
192.248.6.41	10.10.10.23	6	80	3586	590
10.10.10.23	192.248.6.53	6	3587	80	7
192.248.6.53	10.10.10.23	6	80	3587	6

We know the approximate time of the event.

Search on the network portion of the IP address in question.

Three systems on suspected network are involved in the exploit.

Banned IP range to contain problem.

Now we can search an entire day's logs to find the number of infected systems.

Other Types of Detection

- Spyware
- Verify claims on traffic from your network
  - DMCA reports
  - Attacks reports
  - Scanning reports
  - Email – spoofed or real
- Can aid with determining access controls and Firewall rules

Reference

- Cisco: http://www.cisco.com
- Selection of links for various NetFlow tools: http://www.switch.ch/tf-tant/floma/software.html
- Well known IP ports: http://www.iana.org/assignments/port-numbers
- Network tutorials from http://NSRC.org/workshop
- APAN meeting slides (https://apan.net/meetings/)
- Network analysis by Karl F. Lutzen ,Information Security Officer kfl@mst.edu
- NCAR-SCD netflow training
- http://en.wikipedia.org/wiki/Netflow

Reference

- http://nfdump.sourceforge.net/
- http://nfsen.sourceforge.net/
- http://nfsen-plugins.sourceforge.net/
- http://indico.wacren.com
- https://nfsen.kln.ac.lk
- IETF standards
- Cisco Centric Open Source Community

Questions

Thank You

Thilina Pathirana

Email: thilina@learn.ac.lk