

Netflow Sensor(NfSen) 系統安裝與使用

桃園區網 許時準
106/05/04

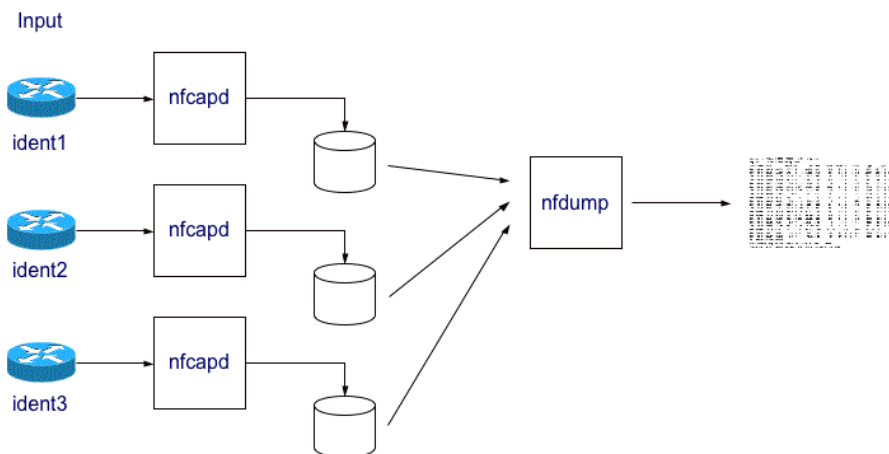


報告大綱

- ☐ 系統介紹
- ☐ 系統操作
- ☐ NfSen應用
- ☐ HostStats 套件
- ☐ 系統安裝

系統介紹

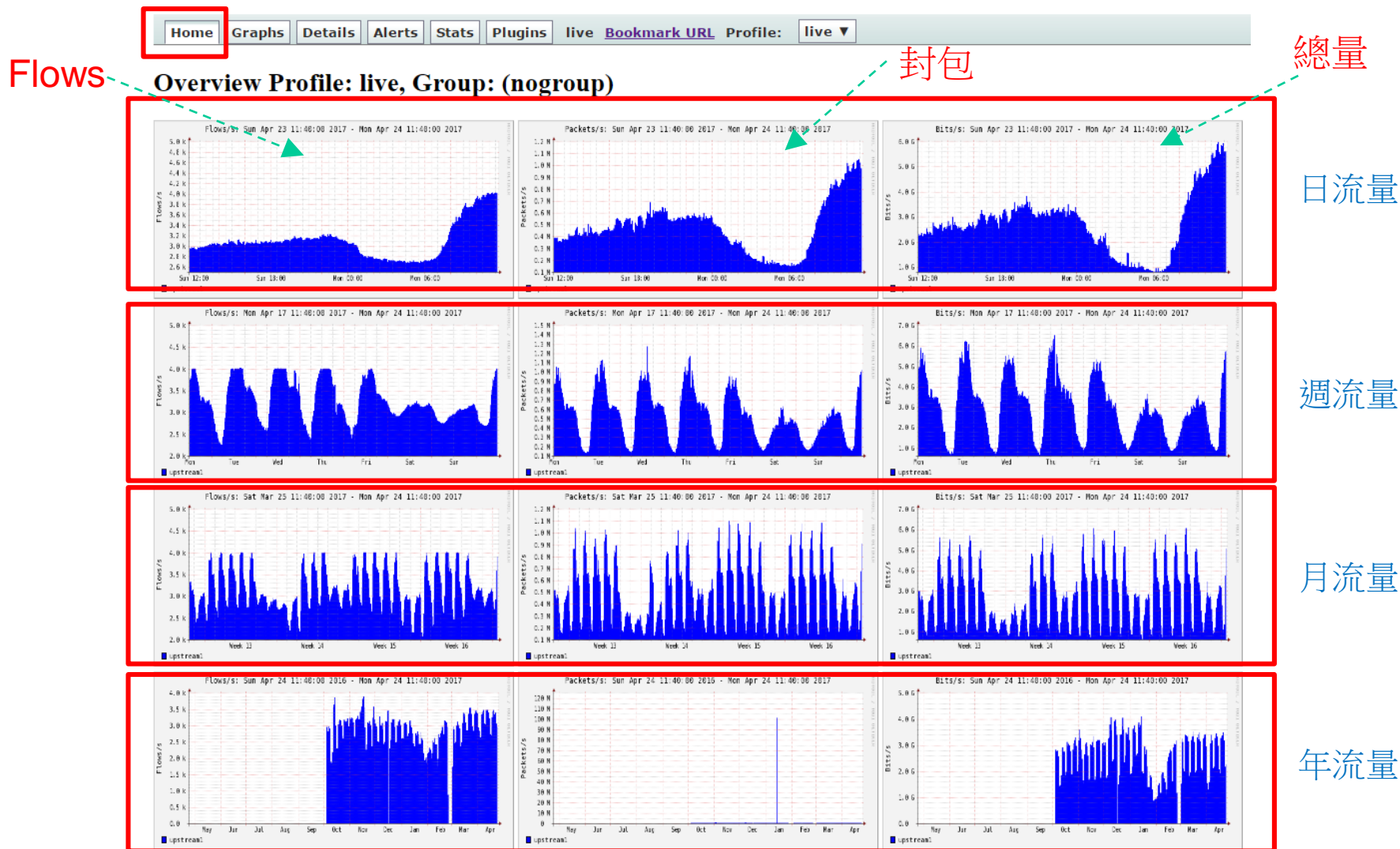
- ❑ Nfsen系統藉由nfcapd蒐集路由器產生 Netflow 資料，進而分析網路流量的 OpenSource軟體。
- ❑ 可查詢即時或指定區間的流量、封包、總量大小 (Flows, Packets and Bytes)
- ❑ 可自訂查詢分析規則及設定預警通知。
- ❑ 可加入其他分析套件(SurfMap、Nfsight、HostStats....)。



- ❑ 圖片來源 <http://nfdump.sourceforge.net/>

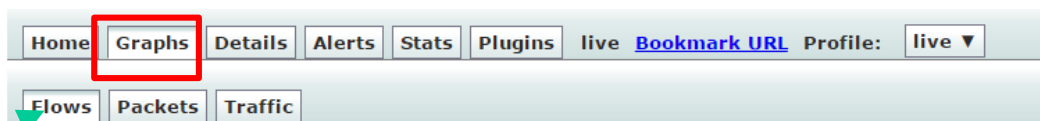


系統操作(1)-主畫面



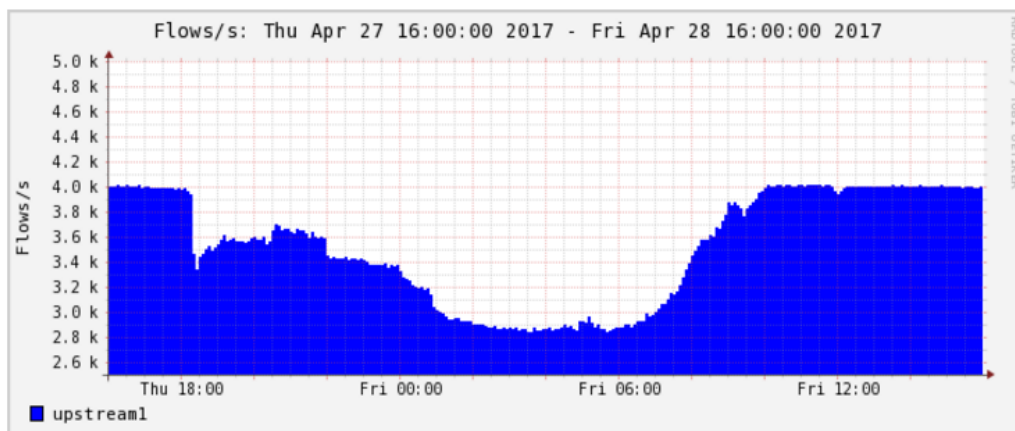


系統操作(2)- Graphs

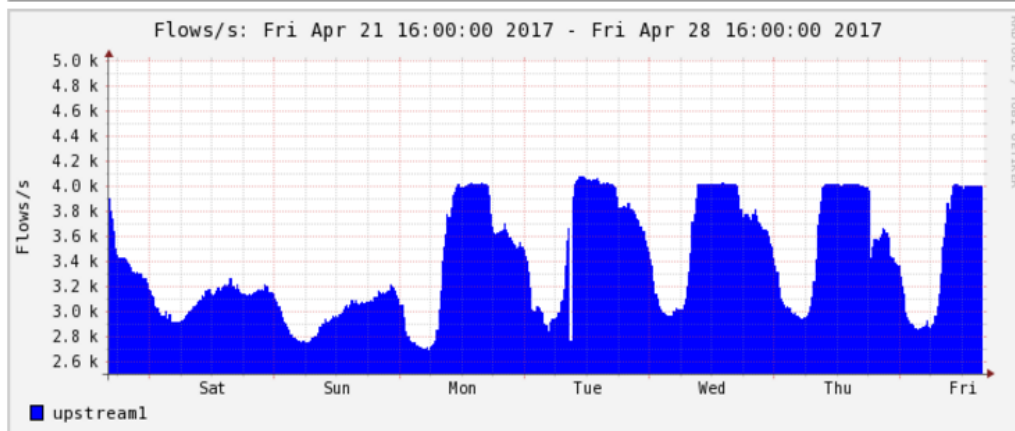


三種類型
分頁顯示

Profile: live, Group: (nogroup) - flows



日流量



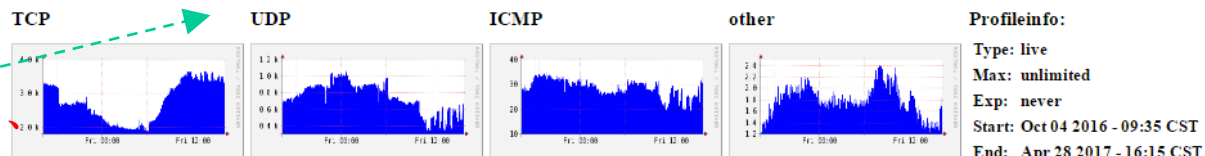
週流量



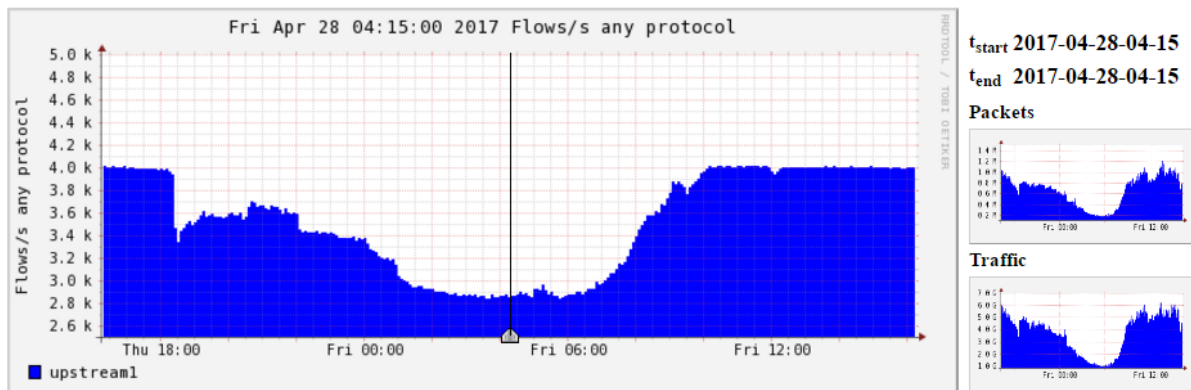
系統操作(3)- Details

Home Graphs **Details** Alerts Stats Plugins live [Bookmark URL](#) Profile: live ▼

Profile: live



TCP、UDP、
ICMP
各協定流量



Select Single Timeslot ▼

Display: 1 day << < | ^ > >> >|

☒ Lin Scale ☒ Stacked Graph
☐ Log Scale ☐ Line Graph

顯示8小時內的流量統計

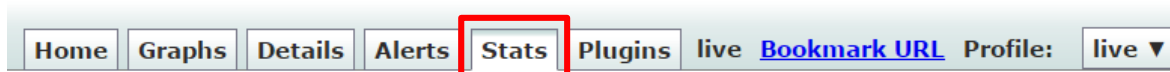
Statistics timeslot Apr 28 2017 - 04:15

| Channel: | Flows: | | | | | Packets: | | | | | Traffic: | | | | |
|---|---------|---------|----------|---------|--------|-----------|-----------|----------|---------|----------|----------|------------|------------|------------|------------|
| | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: |
| <input checked="" type="checkbox"/> upstream1 | 2.9 k/s | 1.9 k/s | 902.0 /s | 27.1 /s | 1.8 /s | 204.4 k/s | 115.1 k/s | 88.0 k/s | 1.1 k/s | 228.2 /s | 1.2 Gb/s | 627.1 Mb/s | 522.9 Mb/s | 638.0 kb/s | 277.2 kb/s |
| all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | |
| TOTAL | 2.9 k/s | 1.9 k/s | 902.0 /s | 27.1 /s | 1.8 /s | 204.4 k/s | 115.1 k/s | 88.0 k/s | 1.1 k/s | 228.2 /s | 1.2 Gb/s | 627.1 Mb/s | 522.9 Mb/s | 638.0 kb/s | 277.2 kb/s |

All None Display: ☐ Sum ☒ Rate



系統操作(4)-新增 profile



ERROR: A classic profile needs a valid filter and at least one selected channel!

| | | |
|---|--|---|
| Profile: | <input type="text" value="DNS"/> | ? |
| Group: | <input type="text" value="(nogroup)"/> | ? |
| Description: | <input type="text"/> | |
| Start: | <input type="text"/> Format: yyyy-mm-dd-HH-MM | ? |
| End: | <input type="text"/> Format: yyyy-mm-dd-HH-MM | ? |
| Max. Size: | <input type="text" value="10G"/> | ? |
| Expire: | <input type="text" value="60 Days"/> | ? |
| Channels: | <input type="radio"/> 1:1 channels from profile live <input checked="" type="radio"/> individual channels | ? |
| Type: | <input checked="" type="radio"/> Real Profile <input type="radio"/> Shadow Profile | ? |
| <input type="button" value="Cancel"/> <input type="button" value="Create Profile"/> | | |



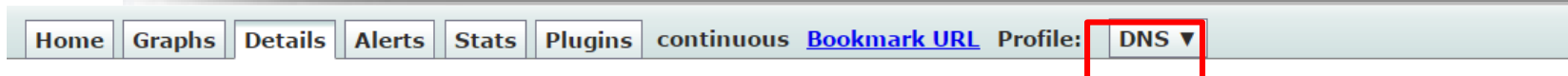
系統操作(5)-新增 channel

Home Graphs Details Alerts **Stats** Plugins continuous [Bookmarks](#)

| Channel name | | <input type="text" value="DNS"/> | | | | | | | |
|---|--|---|------------------------------------|-------------------|--|------------------|-------------|------------------------------|----------------------|
| Colour: | <input type="button" value="Enter new value"/> | <input type="text" value="#abcdef"/> or <input type="button" value="Select a colour from"/> | <input type="button" value="v"/> | | | | | | |
| Sign: | <input type="button" value="+ v"/> | Order: | <input type="button" value="1 v"/> | | | | | | |
| Filter: | <input type="text" value="port 53"/> | | | | | | | | |
| Sources: | <table border="1"><thead><tr><th>Available Sources</th><th></th><th>Selected Sources</th></tr></thead><tbody><tr><td><div></div></td><td><div><< >></div></td><td><div>upstream1</div></td></tr></tbody></table> | | | Available Sources | | Selected Sources | <div></div> | <div><< >></div> | <div>upstream1</div> |
| | Available Sources | | Selected Sources | | | | | | |
| <div></div> | <div><< >></div> | <div>upstream1</div> | | | | | | | |
| <div><input type="button" value="Cancel"/> <input type="button" value="Add Channel"/></div> | | | | | | | | | |

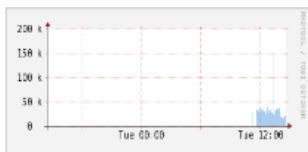


系統操作(6)-顯示不同 profile

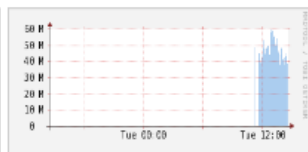


Profile: DNS

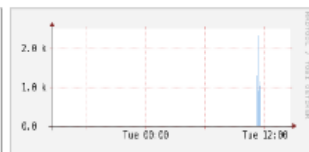
TCP



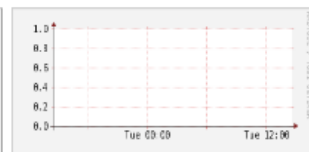
UDP



ICMP

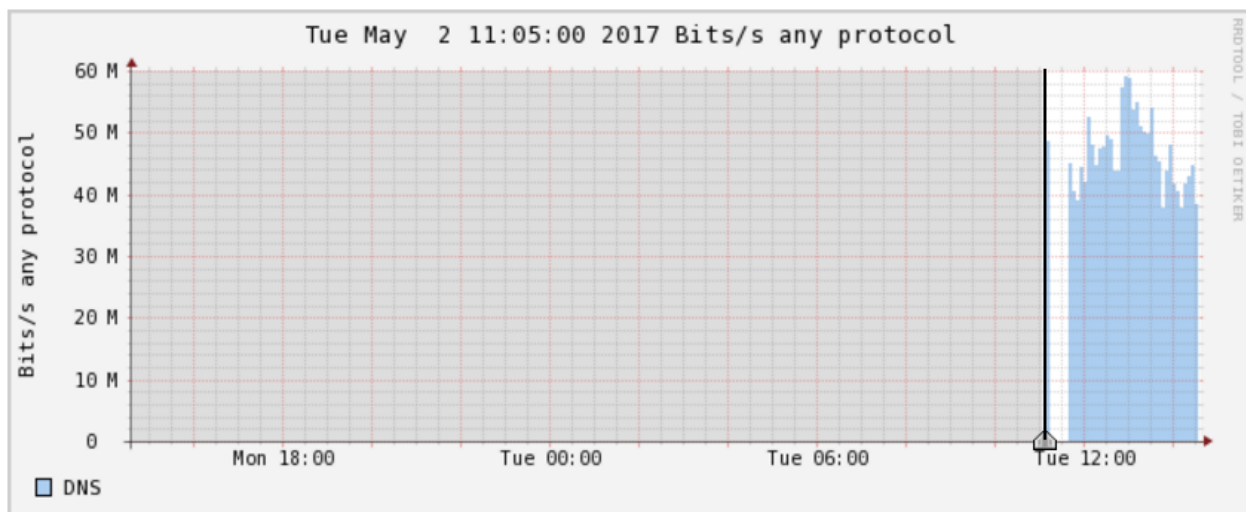


other



Profileinfo:

Type: continuous
Max: 10.0 GB
Exp: 60 days 0 hours
Start: May 02 2017 - 11:05 CST
End: May 02 2017 - 14:35 CST



t_{start} 2017-05-02-11-05
t_{end} 2017-05-02-11-05

Packets



Flows



Select Single Timeslot

Display: 1 day

☒ Lin Scale ☒ Stacked Graph
☐ Log Scale ☐ Line Graph



系統操作(7)-設定預警通知

Home Graphs Details **Alerts** Stats Plugins live [Bookmark URL](#) Profile: live ▼

New alert

Name bandwidth

Status ☒ enabled

Filter applied to 'live' profile:

upstream1

☒ **Conditions based on total flow summary:**

| | | | | | | |
|---|-------------|-------------|----------------------|----------------|---|---|
| 0 | Total bytes | > | 10 min average value | + | 6 | G |
| 1 | and | Total flows | > | Absolute value | 0 | - |

☐ **Conditions based on individual Top 1 statistics:**

☐ **Conditions based on plugin:**

Trigger:

Each time after 1 x condition = true, and block next trigger for 0 cycles

Action:

☐ No action

☒ Send alert email To:

Subject: Alert triggered

☐ Call plugin: No alert plugins available

Cancel Create Alert

設定條件



NfSen 應用(1)- IP流量排行

Netflow Processing

Source: upstream1 Filter: and <none>

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: Any IP Address

Limit: Any IP Address

Output: SRC IP Address

order by: bytes

0 -

Clear Form process

可自訂條件查詢
流量排行榜

```
** nfdump -M /opt/nfsen/profiles-data/live/upstream1 -T -r 2017/04/28/ 30 -n 10 -s ip/bytes
```

nfdump filter:

any

Top 10 IP Addr ordered by bytes:

| Date first seen | Duration | Proto | IP Addr | Flows(%) | Bytes(%) | pps | bps | bpp |
|-------------------------|----------|-------|-----------------|-------------|--------------|-------|---------|------|
| 2017-04-28 04:27:21.445 | 552.126 | any | 140.138.144.170 | 10965(1.3) | 12.1 G(28.6) | 15183 | 175.2 M | 1442 |
| 2017-04-28 04:27:22.754 | 543.924 | any | 163.28.51.13 | 486(0.1) | 1.9 G(4.5) | 3466 | 27.7 M | 998 |
| 2017-04-28 04:31:19.315 | 297.257 | any | 203.72.181.5 | 13(0.0) | 1.9 G(4.4) | 4494 | 50.6 M | 1406 |
| 2017-04-28 04:27:23.013 | 533.284 | any | 163.28.51.12 | 322(0.0) | 1.9 G(4.4) | 3619 | 28.1 M | 968 |
| 2017-04-28 04:27:23.625 | 534.441 | any | 163.28.51.14 | 267(0.0) | 1.9 G(4.4) | 3503 | 28.0 M | 998 |
| 2017-04-28 04:28:39.443 | 184.517 | any | 104.28.30.192 | 36064(4.2) | 1.8 G(4.1) | 20487 | 76.0 M | 463 |
| 2017-04-28 04:29:24.872 | 417.228 | any | 74.125.204.95 | 44(0.0) | 1.7 G(4.0) | 2871 | 32.2 M | 1403 |
| 2017-04-28 04:27:21.483 | 521.324 | any | 163.30.123.20 | 29738(3.5) | 1.5 G(3.5) | 6151 | 23.0 M | 467 |
| 2017-04-28 04:27:21.433 | 504.083 | any | 163.30.162.136 | 27545(3.2) | 1.4 G(3.3) | 5877 | 22.0 M | 467 |
| 2017-04-28 04:27:21.432 | 401.417 | any | 163.30.84.10 | 26409(3.1) | 1.3 G(3.0) | 6762 | 25.1 M | 464 |

Summary: total flows: 860771, total bytes: 42280218752, total packets: 58475376, avg bps: 611757146, avg pps: 105760, avg bpp: 723

Time window: 2017-04-28 04:27:21 - 2017-04-28 04:36:34

Total flows processed: 860771, Blocks skipped: 0, Bytes read: 51647300

Sys: 0.534s flows/second: 1609164.4 Wall: 0.600s flows/second: 1433194.7



NfSen 應用(2)-協定流量排行

Netflow Processing

Source: upstream1
Filter: and <none>

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: Flow Records order by bytes

Aggregate

☐ bi-directional

☒ proto

☐ srcPort srcIP

☐ dstPort dstIP

Limit: Packets > 0

Output: auto / IPv6 long

Clear Form process

依協定統計流量

```
** nfdump -M /opt/nfsen/profiles-data/live/upstream1 -T -r 2017/04/28/nfcapd.201704280430 -n 10 -s record/bytes -A proto
nfdump filter:
any
Aggregated flows 8
Top 10 flows ordered by bytes:
Date first seen    Duration  Proto  Packets  Bytes    bps    Bpp  Flows
2017-04-28 04:27:21.432 552.902 TCP    33.9 M   24.6 G   356.3 M  727 584398
2017-04-28 04:27:21.432 552.398 UDP    24.2 M   17.6 G   255.2 M  727 267868
2017-04-28 04:27:21.543 549.983 ICMP   313968   23.2 M   337090   73  7984
2017-04-28 04:27:22.554 534.891 GRE     58704    8.3 M   124154   141  398
2017-04-28 04:28:09.848 503.186 ESP      9712    1.8 M   28706    185  79
2017-04-28 04:27:27.085 507.345 VRRP     2096    1.2 M   19326    584  4
2017-04-28 04:27:24.892 514.276 IPv6     976   108016   1680    110  36
2017-04-28 04:28:08.750 332.964 OSPF     144    10496    252     72  4
Summary: total flows: 860771, total bytes: 42280218752, total packets: 58475376, avg bps: 611757146, avg pps: 105760, avg bpp: 723
Time window: 2017-04-28 04:27:21 - 2017-04-28 04:36:34
Total flows processed: 860771, Blocks skipped: 0, Bytes read: 51647300
Sys: 0.360s flows/second: 2384777.1 Wall: 0.360s flows/second: 2390685.2
```



NfSen 應用(3)-查詢特定IP流量

Netflow Processing

Source: upstream1 Filter: ip 140.115.1.31

All Sources and <none>

Options:

☒ List Flows ☐ Stat TopN

Limit to: 100 Flows

☒ bi-directional

Aggregate ☐ proto

☐ srcPort ☐ srcIP

☐ dstPort ☐ dstIP

Sort: ☒ start time of flows

Output: auto ☐ / IPv6 long

Clear Form process

指定特定IP

```
** nfdump -M /opt/nfsen/profiles-data/live/upstream1 -T -r 2017/05/02/nfcapd.201705021130 -a -B -m -c 100
nfdump filter:
ip 140.115.1.31
Option -m deprecated. Use '-O tstart' instead
```

| Date first seen | Duration | Proto | Src IP Addr:Port | Dst IP Addr:Port | Out Pkt | In Pkt | Out Byte | In Byte | Flows |
|-------------------------|----------|-------|------------------------|--------------------|---------|--------|----------|---------|-------|
| 2017-05-02 11:27:25.194 | 0.000 | UDP | 140.115.1.31:59101 <-> | 52.74.79.56:53 | 0 | 16 | 0 | 1200 | 1 |
| 2017-05-02 11:27:25.197 | 0.000 | UDP | 140.115.1.31:48163 <-> | 52.74.79.56:53 | 0 | 16 | 0 | 1184 | 1 |
| 2017-05-02 11:27:25.957 | 0.000 | UDP | 140.115.1.31:43653 <-> | 203.153.50.102:53 | 0 | 16 | 0 | 1072 | 1 |
| 2017-05-02 11:27:26.071 | 0.000 | UDP | 140.115.1.31:44690 <-> | 205.251.196.93:53 | 0 | 16 | 0 | 1280 | 1 |
| 2017-05-02 11:27:26.822 | 0.000 | UDP | 140.115.1.31:34014 <-> | 192.82.137.30:53 | 0 | 16 | 0 | 1456 | 1 |
| 2017-05-02 11:27:27.136 | 0.000 | UDP | 140.115.1.31:40560 <-> | 203.153.50.80:53 | 0 | 16 | 0 | 1072 | 1 |
| 2017-05-02 11:27:29.018 | 0.000 | UDP | 140.115.1.31:59349 <-> | 69.171.239.11:53 | 0 | 16 | 0 | 1216 | 1 |
| 2017-05-02 11:27:29.023 | 0.000 | UDP | 140.115.1.31:52300 <-> | 205.251.197.195:53 | 0 | 16 | 0 | 1872 | 1 |
| 2017-05-02 11:27:29.047 | 0.000 | UDP | 140.115.1.31:52297 <-> | 103.17.8.38:53 | 0 | 16 | 0 | 1344 | 1 |
| 2017-05-02 11:27:29.943 | 0.000 | UDP | 140.115.1.31:46477 <-> | 103.6.220.26:53 | 0 | 16 | 0 | 1152 | 1 |
| 2017-05-02 11:27:31.171 | 0.000 | UDP | 140.115.1.31:45393 <-> | 52.220.136.67:53 | 0 | 16 | 0 | 992 | 1 |
| 2017-05-02 11:27:32.155 | 0.000 | UDP | 140.115.1.31:55969 <-> | 203.153.50.80:53 | 0 | 16 | 0 | 1088 | 1 |
| 2017-05-02 11:27:33.933 | 0.000 | UDP | 140.115.1.31:45603 <-> | 193.138.29.11:53 | 0 | 16 | 0 | 1312 | 1 |
| 2017-05-02 11:27:35.007 | 0.000 | UDP | 140.115.1.31:42436 <-> | 52.74.79.56:53 | 0 | 16 | 0 | 1216 | 1 |
| 2017-05-02 11:27:36.098 | 0.000 | UDP | 140.115.1.31:37114 <-> | 103.17.8.21:53 | 0 | 16 | 0 | 1344 | 1 |
| 2017-05-02 11:27:36.115 | 0.000 | UDP | 140.115.1.31:42957 <-> | 103.1.220.11:53 | 16 | 0 | 1344 | 0 | 1 |
| 2017-05-02 11:27:36.159 | 0.000 | UDP | 140.115.1.31:35185 <-> | 203.153.50.103:53 | 0 | 16 | 0 | 1024 | 1 |
| 2017-05-02 11:27:36.160 | 0.000 | UDP | 140.115.1.31:37226 <-> | 192.35.51.30:53 | 0 | 16 | 0 | 1376 | 1 |
| 2017-05-02 11:27:38.029 | 0.000 | UDP | 140.115.1.31:43763 <-> | 203.153.50.82:53 | 0 | 16 | 0 | 1136 | 1 |
| 2017-05-02 11:27:38.107 | 0.000 | UDP | 140.115.1.31:33932 <-> | 203.153.50.82:53 | 0 | 16 | 0 | 1104 | 1 |
| 2017-05-02 11:27:40.184 | 0.000 | UDP | 140.115.1.31:34207 <-> | 192.35.51.30:53 | 0 | 16 | 0 | 1456 | 1 |
| 2017-05-02 11:27:40.832 | 0.000 | UDP | 140.115.1.31:60233 <-> | 205.251.196.6:53 | 0 | 16 | 0 | 1456 | 1 |
| 2017-05-02 11:27:41.063 | 0.000 | UDP | 140.115.1.31:50391 <-> | 208.109.255.2:53 | 0 | 16 | 0 | 1376 | 1 |



NfSen 應用(4)- Filter 語法

- ❑ Filter = expr, expr and expr, expr or expr, not expr, (expr), not (expr)
- ❑ expr can be one of the following filter primitives:
- ❑ protocol version
 - inet or ipv4 for IPv4 and inet6 or ipv6 for Ipv6
- ❑ protocol
 - proto TCP, UDP, ICMP, GRE, AH
- ❑ IP address
- ❑ Port

Examples:

proto tcp and (src ip 140.115.1.31 or dst ip 8.8.8.8)

proto tcp and (net 140.115/16 and src port > 1024 and dst port 80) and bytes > 2048



NfSen 應用(5)-限定網段及port查詢

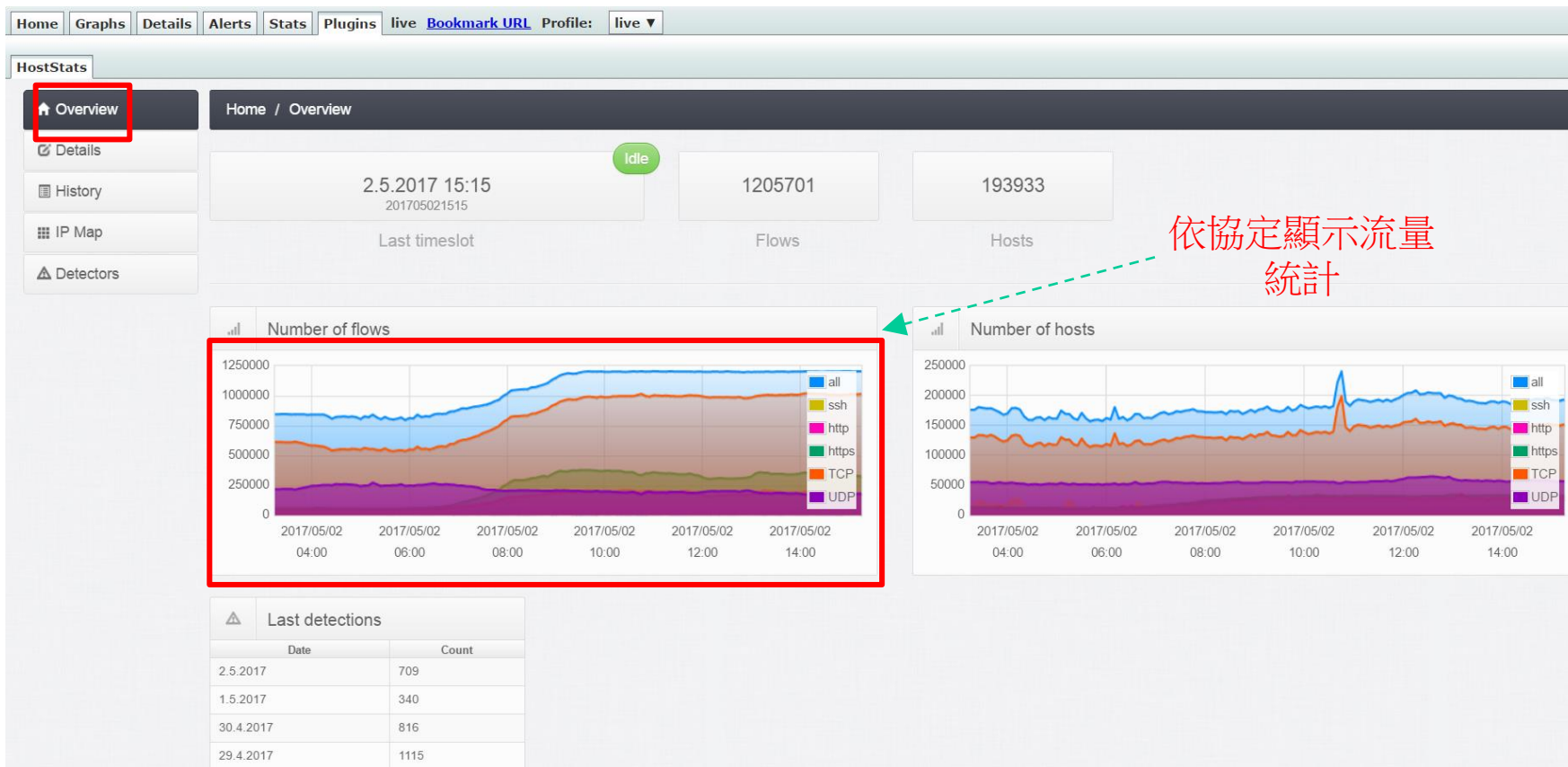
```
** nfdump -M /opt/nfsen/profiles-data/live/upstream1 -T -R 2017/05/02/nfcapd.201705020800:2017/05/02/nfcapd.201705021000 -a -B -c 50  
nfdump filter:
```

```
proto tcp and ( net 140.115/16 and src port > 1024 and dst port 80 ) and bytes > 2048
```

| Date first seen | Duration | Proto | Src IP Addr:Port | Dst IP Addr:Port | Out Pkt | In Pkt | Out Byte | In Byte | Flows |
|-------------------------|----------|-------|---------------------------|--------------------|---------|--------|----------|---------|-------|
| 2017-05-02 08:27:50.113 | 1.179 | TCP | 140.115.217.85:12873 <-> | 163.28.5.27:80 | 0 | 176 | 0 | 14800 | 1 |
| 2017-05-02 09:29:01.831 | 0.434 | TCP | 140.115.130.102:59115 <-> | 104.20.204.31:80 | 0 | 80 | 0 | 3776 | 1 |
| 2017-05-02 10:02:00.863 | 135.085 | TCP | 140.115.6.147:49433 <-> | 122.146.127.235:80 | 0 | 128 | 0 | 5136 | 1 |
| 2017-05-02 09:58:49.844 | 57.722 | TCP | 140.115.143.117:34568 <-> | 163.28.5.18:80 | 0 | 26032 | 0 | 1.6 M | 1 |
| 2017-05-02 08:44:04.816 | 4.120 | TCP | 140.115.216.140:61970 <-> | 163.28.224.17:80 | 0 | 592 | 0 | 31488 | 1 |
| 2017-05-02 09:50:14.814 | 23.971 | TCP | 140.115.204.109:64483 <-> | 113.29.47.227:80 | 0 | 1488 | 0 | 77408 | 1 |
| 2017-05-02 08:54:47.952 | 1.094 | TCP | 140.115.20.230:49852 <-> | 103.243.221.87:80 | 0 | 48 | 0 | 32560 | 1 |
| 2017-05-02 09:15:51.958 | 1.305 | TCP | 140.115.200.90:61119 <-> | 113.29.73.248:80 | 0 | 320 | 0 | 16256 | 1 |
| 2017-05-02 08:49:11.840 | 0.000 | TCP | 140.115.152.79:54305 <-> | 103.8.183.221:80 | 0 | 16 | 0 | 24000 | 1 |
| 2017-05-02 09:38:19.869 | 0.098 | TCP | 140.115.80.23:60270 <-> | 52.84.203.16:80 | 0 | 48 | 0 | 2752 | 1 |
| 2017-05-02 08:26:24.214 | 1.164 | TCP | 140.115.43.129:58565 <-> | 209.107.220.189:80 | 0 | 32 | 0 | 10032 | 1 |
| 2017-05-02 10:00:38.977 | 0.478 | TCP | 140.115.160.64:57382 <-> | 45.112.214.17:80 | 0 | 544 | 0 | 21760 | 1 |
| 2017-05-02 09:01:00.918 | 0.097 | TCP | 140.115.205.202:62256 <-> | 151.101.24.193:80 | 0 | 48 | 0 | 2112 | 1 |
| 2017-05-02 09:43:34.163 | 0.210 | TCP | 140.115.30.131:4829 <-> | 4.16.75.8:80 | 0 | 32 | 0 | 24640 | 1 |
| 2017-05-02 09:16:53.026 | 0.000 | TCP | 140.115.204.83:62792 <-> | 54.241.139.76:80 | 0 | 16 | 0 | 5024 | 1 |
| 2017-05-02 10:01:08.083 | 0.080 | TCP | 140.115.36.103:51608 <-> | 111.65.248.138:80 | 0 | 48 | 0 | 9744 | 1 |
| 2017-05-02 08:54:00.834 | 1.999 | TCP | 140.115.120.43:33114 <-> | 31.13.87.52:80 | 0 | 656 | 0 | 35648 | 1 |
| 2017-05-02 08:40:46.975 | 101.394 | TCP | 140.115.11.104:2082 <-> | 151.101.90.2:80 | 0 | 160 | 0 | 57376 | 1 |
| 2017-05-02 08:12:39.221 | 9.314 | TCP | 140.115.110.164:49400 <-> | 163.28.224.10:80 | 0 | 320 | 0 | 17152 | 1 |
| 2017-05-02 09:28:54.218 | 5.587 | TCP | 140.115.200.120:49624 <-> | 199.34.228.54:80 | 0 | 128 | 0 | 5120 | 1 |
| 2017-05-02 08:58:28.165 | 136.387 | TCP | 140.115.208.60:51316 <-> | 104.16.225.7:80 | 0 | 64 | 0 | 26112 | 1 |
| 2017-05-02 08:47:26.786 | 20.214 | TCP | 140.115.7.32:13765 <-> | 209.205.212.106:80 | 0 | 48 | 0 | 7072 | 1 |
| 2017-05-02 08:50:18.923 | 0.001 | TCP | 140.115.51.19:53611 <-> | 188.65.124.58:80 | 0 | 32 | 0 | 24640 | 1 |
| 2017-05-02 08:19:56.218 | 0.169 | TCP | 140.115.66.32:49414 <-> | 104.28.9.120:80 | 0 | 288 | 0 | 11520 | 1 |
| 2017-05-02 08:44:07.193 | 3.505 | TCP | 140.115.216.140:61968 <-> | 163.28.224.17:80 | 0 | 192 | 0 | 9600 | 1 |
| 2017-05-02 09:44:21.210 | 0.008 | TCP | 140.115.21.228:41126 <-> | 210.68.105.68:80 | 0 | 32 | 0 | 8976 | 1 |
| 2017-05-02 09:18:36.289 | 55.311 | TCP | 140.115.95.31:50443 <-> | 50.18.183.63:80 | 0 | 64 | 0 | 12192 | 1 |
| 2017-05-02 09:38:02.029 | 0.157 | TCP | 140.115.79.12:59227 <-> | 163.28.224.9:80 | 0 | 304 | 0 | 14336 | 1 |
| 2017-05-02 08:40:43.040 | 0.000 | TCP | 140.115.115.31:50656 <-> | 100.65.124.50:80 | 0 | 16 | 0 | 10152 | 1 |



HostStats 套件(1)-Overview





HostStats 套件(2)-Details

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

HostStats SURFmap

Overview
Details
History
IP Map
Detectors

Home / Details Profile: all ▼

< 1.5.2017 13:20 201705011320 >

Timeslot

Type filter

Filter

Results Number of results 20

| IP address | In | | | Out | | | In | | | | | | | Out | | | | | | | In | | Out | | Action |
|-------------|-------|---------|-------|-------|---------|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------------|---------|------------|---------|-----|--------|--------|
| | flows | packets | bytes | flows | packets | bytes | SYN | ACK | FIN | RST | PSH | URG | SYN | ACK | FIN | RST | PSH | URG | unique ips | sources | unique ips | sources | | | |
| 0.0.0.0 | 0 | 0 | 0 | 5 | 112 | 37712 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | Action | |
| 1.0.0.0 | 1 | 16 | 1120 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Action | |
| 1.0.0.127 | 2 | 32 | 1792 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Action | |
| 1.0.167.137 | 2 | 32 | 1408 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Action | |
| 1.0.220.150 | 1 | 16 | 640 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Action | |
| 1.0.221.148 | 1 | 16 | 5040 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Action | |
| 1.0.221.220 | 0 | 0 | 0 | 1 | 112 | 4480 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | Action | |
| 1.1.0.0 | 1 | 128 | 8960 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Action | |
| 1.1.1.1 | 4 | 64 | 6560 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | Action | |
| 1.1.1.4 | 1 | 32 | 3392 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Action | |

列出該時段
每個IP流量



HostStats 套件(3)-History

Home | Graphs | Details | Alerts | Stats | Plugins | live | [Bookmark URL](#) | Profile: live ▼

HostStats | SURFmap

Overview | Details | History | IP Map | Detectors

Home / History Profile: all ▼

140.115.1.31

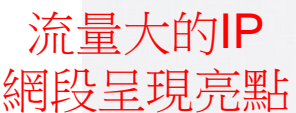
< Last hour 1.5.2017 12:30 - 1.5.2017 13:30 >

IP address Time window

History of IP address

| Timeslot | In | | | Out | | | In | | | | | | Out | | | | | | In | | Out | |
|------------------|-------|---------|--------|-------|---------|--------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------------|---------|------------|---------|
| | flows | packets | bytes | flows | packets | bytes | SYN | ACK | FIN | RST | PSH | URG | SYN | ACK | FIN | RST | PSH | URG | unique IPS | sources | unique IPS | sources |
| 2017-05-01 12:30 | 86 | 1376 | 149696 | 403 | 6544 | 601744 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 7 | 4 | 0 | 0 | 0 | 45 | ■ | 245 | ■ |
| 2017-05-01 12:35 | 78 | 1248 | 129568 | 467 | 7488 | 665712 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 41 | ■ | 280 | ■ |
| 2017-05-01 12:40 | 86 | 1376 | 142992 | 395 | 6352 | 579040 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 6 | 1 | 0 | 2 | 0 | 40 | ■ | 231 | ■ |
| 2017-05-01 12:45 | 91 | 1488 | 147296 | 415 | 6912 | 594064 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 13 | 1 | 0 | 3 | 0 | 37 | ■ | 251 | ■ |
| 2017-05-01 12:50 | 64 | 1024 | 109840 | 433 | 6992 | 583824 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 7 | 0 | 0 | 3 | 0 | 32 | ■ | 263 | ■ |
| 2017-05-01 12:55 | 92 | 1520 | 153296 | 471 | 7600 | 649968 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 8 | 0 | 0 | 1 | 0 | 43 | ■ | 271 | ■ |
| 2017-05-01 13:00 | 96 | 1536 | 165488 | 525 | 8496 | 775808 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 3 | 0 | 0 | 1 | 0 | 42 | ■ | 291 | ■ |
| 2017-05-01 13:05 | 89 | 1440 | 149840 | 500 | 8048 | 723840 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 9 | 3 | 0 | 1 | 0 | 43 | ■ | 306 | ■ |
| 2017-05-01 13:10 | 88 | 1424 | 157296 | 465 | 7568 | 698096 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 6 | 1 | 0 | 1 | 0 | 44 | ■ | 251 | ■ |
| 2017-05-01 13:15 | 77 | 1248 | 134528 | 435 | 7040 | 654624 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 3 | 0 | 0 | 0 | 0 | 32 | ■ | 269 | ■ |
| 2017-05-01 13:20 | 98 | 1584 | 171824 | 482 | 7984 | 764144 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 2 | 0 | 2 | 0 | 39 | ■ | 288 | ■ |

指定特定IP



指定Subnet



HostStats 套件(5)- Detectors

Home | Graphs | Details | Alerts | Stats | Plugins | live | [Bookmark URL](#) | Profile: live ▼

HostStats | SURFmap

Overview
Details
History
IP Map
Detectors

Home / Detectors

< 1.5.2017 >

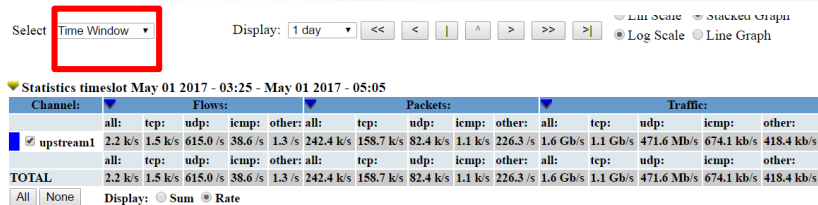
Date

Detection log

| Timeslot | Type | Protocol | Source IP | Destination IP | Source port | Destination port | Intensity | Note |
|------------------|---------------------|----------|------------------------|----------------|-------------|------------------|-----------|---------------------|
| 2017-05-01 13:30 | Horizontal portscan | TCP | 49.159.96.2 | | | | 402 | horizontal SYN scan |
| 2017-05-01 13:30 | Horizontal portscan | TCP | 106.187.91.129 | | | | 1623 | horizontal SYN scan |
| 2017-05-01 13:30 | Horizontal portscan | TCP | 140.115.32. [REDACTED] | | | | 433 | horizontal SYN scan |
| 2017-05-01 13:30 | Horizontal portscan | TCP | 175.19.209.140 | | | | 1442 | horizontal SYN scan |
| 2017-05-01 13:25 | Horizontal portscan | TCP | 106.187.91.129 | | | | 1825 | horizontal SYN scan |
| 2017-05-01 13:25 | Horizontal portscan | TCP | 123.116.110.154 | | | | 226 | horizontal SYN scan |
| 2017-05-01 13:20 | Horizontal portscan | TCP | 123.151.149.222 | | | | 293 | horizontal SYN scan |
| 2017-05-01 13:20 | Horizontal portscan | TCP | 106.187.91.129 | | | | 976 | horizontal SYN scan |
| 2017-05-01 13:20 | Horizontal portscan | TCP | 107.150.2.68 | | | | 247 | horizontal SYN scan |
| 2017-05-01 13:20 | Horizontal portscan | TCP | 198.74.113.172 | | | | 528 | horizontal SYN scan |
| 2017-05-01 13:20 | Horizontal portscan | TCP | 222.186.50.36 | | | | 1215 | horizontal SYN scan |



HostStats 套件(6)-追查可疑IP



Netflow Processing

Source: upstream1 Filter: IP 140.115.32.2

Options:

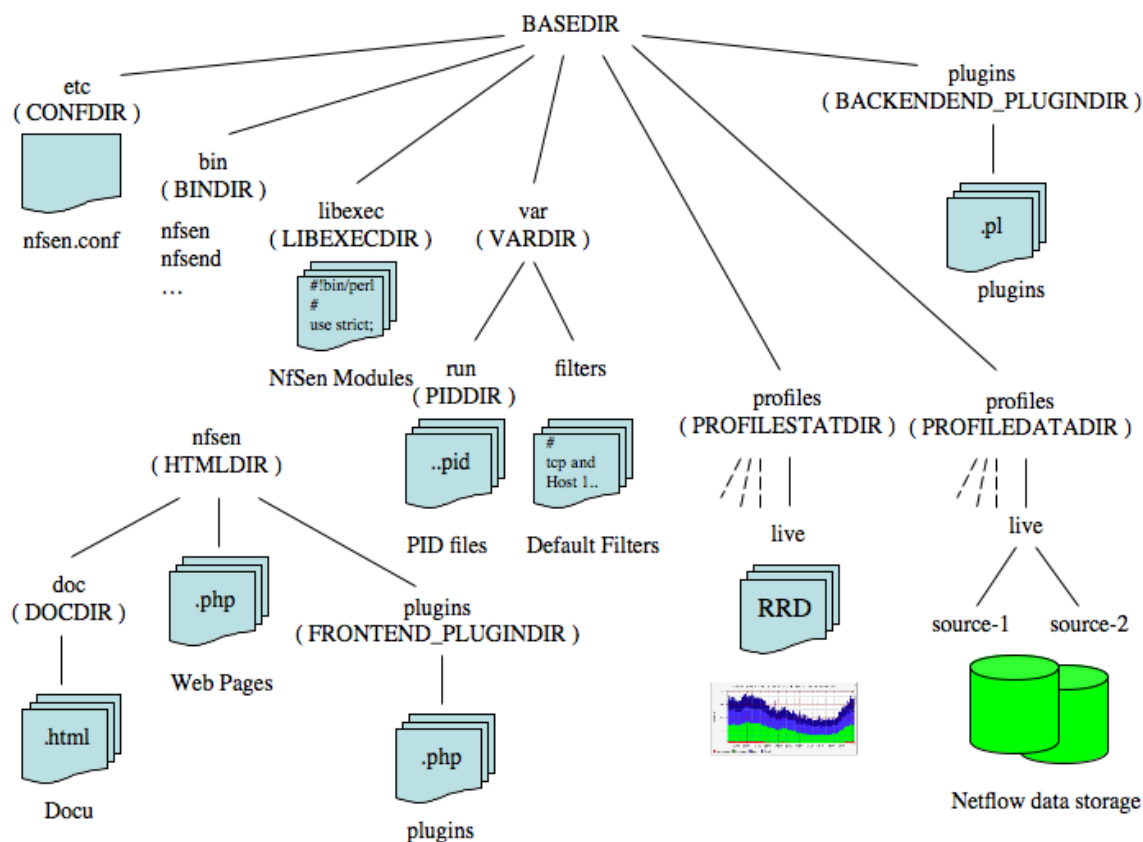
- ☒ List Flows ☐ Stat TopN
- Limit to: 100 Flows
- ☒ bi-directional
- Aggregate: ☐ proto ☐ srcPort ☐ srcIP ☐ dstPort ☐ dstIP
- Sort: ☒ start time of flows
- Output: auto ☐ IPv6 long

Clear Form process

| Date first seen | Duration | Proto | Src IP Addr:Port | Dst IP Addr:Port | Out |
|-------------------------|----------|-------|-----------------------|--------------------|-----|
| 2017-05-01 03:27:09.950 | 0.000 | TCP | 140.115.32.2:6666 <-> | 176.234.52.3:80 | |
| 2017-05-01 03:27:10.472 | 0.000 | TCP | 140.115.32.2:7916 <-> | 176.234.52.16:80 | |
| 2017-05-01 03:27:10.541 | 0.000 | TCP | 140.115.32.2:7677 <-> | 176.234.52.17:22 | |
| 2017-05-01 03:27:10.551 | 0.000 | TCP | 140.115.32.2:6089 <-> | 176.234.52.18:80 | |
| 2017-05-01 03:27:10.882 | 0.000 | TCP | 140.115.32.2:6280 <-> | 176.234.52.26:8080 | |
| 2017-05-01 03:27:10.931 | 0.000 | TCP | 140.115.32.2:6180 <-> | 176.234.52.27:21 | |
| 2017-05-01 03:27:11.041 | 0.000 | TCP | 140.115.32.2:7105 <-> | 176.234.52.30:8080 | |
| 2017-05-01 03:27:11.201 | 0.000 | TCP | 140.115.32.2:6596 <-> | 176.234.52.34:8080 | |
| 2017-05-01 03:27:11.509 | 0.000 | TCP | 140.115.32.2:6554 <-> | 176.234.52.42:80 | |
| 2017-05-01 03:27:11.560 | 0.000 | TCP | 140.115.32.2:7994 <-> | 176.234.52.43:8080 | |
| 2017-05-01 03:27:11.689 | 0.000 | TCP | 140.115.32.2:6089 <-> | 176.234.52.46:21 | |
| 2017-05-01 03:27:11.789 | 0.000 | TCP | 140.115.32.2:7874 <-> | 176.234.52.49:80 | |
| 2017-05-01 03:27:11.819 | 0.000 | TCP | 140.115.32.2:6329 <-> | 176.234.52.49:22 | |
| 2017-05-01 03:27:11.939 | 0.000 | TCP | 140.115.32.2:6066 <-> | 176.234.52.52:22 | |
| 2017-05-01 03:27:12.079 | 0.000 | TCP | 140.115.32.2:7677 <-> | 176.234.52.56:8080 | |
| 2017-05-01 03:27:12.150 | 0.000 | TCP | 140.115.32.2:6517 <-> | 176.234.52.58:80 | |
| 2017-05-01 03:27:12.219 | 0.000 | TCP | 140.115.32.2:7187 <-> | 176.234.52.59:22 | |
| 2017-05-01 03:27:12.231 | 0.000 | TCP | 140.115.32.2:7644 <-> | 176.234.52.60:80 | |
| 2017-05-01 03:27:12.278 | 0.000 | TCP | 140.115.32.2:6988 <-> | 176.234.52.61:8080 | |
| 2017-05-01 03:27:12.479 | 0.000 | TCP | 140.115.32.2:7840 <-> | 176.234.52.66:8080 | |
| 2017-05-01 03:27:12.538 | 0.000 | TCP | 140.115.32.2:6205 <-> | 176.234.52.67:22 | |
| 2017-05-01 03:27:12.907 | 0.000 | TCP | 140.115.32.2:7048 <-> | 176.234.52.77:80 | |
| 2017-05-01 03:27:13.127 | 0.000 | TCP | 140.115.32.2:7935 <-> | 176.234.52.82:21 | |
| 2017-05-01 03:27:13.177 | 0.000 | TCP | 140.115.32.2:7546 <-> | 176.234.52.83:22 | |
| 2017-05-01 03:27:13.715 | 0.000 | TCP | 140.115.32.2:6913 <-> | 176.234.52.97:8080 | |
| 2017-05-01 03:27:13.923 | 0.000 | TCP | 140.115.32.2:7047 <-> | 176.234.52.102:21 | |
| 2017-05-01 03:27:13.943 | 0.000 | TCP | 140.115.32.2:7306 <-> | 176.234.52.103:80 | |
| 2017-05-01 03:27:13.963 | 0.000 | TCP | 140.115.32.2:6470 <-> | 176.234.52.103:21 | |
| 2017-05-01 03:27:14.423 | 0.000 | TCP | 140.115.32.2:6891 <-> | 176.234.52.115:80 | |
| 2017-05-01 03:27:14.442 | 0.000 | TCP | 140.115.32.2:6514 <-> | 176.234.52.115:21 | |
| 2017-05-01 03:27:14.623 | 0.000 | TCP | 140.115.32.2:7501 <-> | 176.234.52.120:80 | |
| 2017-05-01 03:27:14.693 | 0.000 | TCP | 140.115.32.2:7375 <-> | 176.234.52.121:22 | |
| 2017-05-01 03:27:14.864 | 0.000 | TCP | 140.115.32.2:7871 <-> | 176.234.52.126:80 | |

指定特定IP

安裝(1)-NfSen 目錄結構



□ 圖片來源<http://nfsen.sourceforge.net/>



安裝(2)-安裝nfdump及相關軟體

- ❑ `# yum install httpd php`
- ❑ `# service httpd start`
- ❑ `# systemctl start httpd.service`
- ❑ `# yum install epel-release`
- ❑ `# yum install rrdtool-perl perl-Sys-Syslog perl-MailTools perl-Socket6 libpcap-devel`
- ❑ `# yum install -y make rrdtool-devel flexbyacc`
- ❑ `# yum install gcc`
- ❑ `# cd /opt`
- ❑ `# wget http://downloads.sourceforge.net/project/nfdump/stable/nfdump-1.6.11/nfdump-1.6.11.tar.gz`
- ❑ `# tar -zxvf nfdump-1.6.11.tar.gz`



安裝(3)-安裝 NfSen

- ☐ # cd nfdump-1.6.11
- ☐ # ./configure --enable-nfprofile --enable-nftrack --enable-sflow
- ☐ # make &&sudo make install

- ☐ # cd /opt
- ☐ # wget https://sourceforge.net/projects/nfsen/files/latest/download -O nfsen.tar.gz
- ☐ # tar xzf nfsen.tar.gz
- ☐ # cd nfsen-1.3.6p1
- ☐ # cp etc/nfsen-dist.conf etc/nfsen.conf



安裝(4)-設定

- ❑

```
# vi etc/nfsen.conf
$BASEDIR = "/opt/nfsen";
$HTMLDIR = "/var/www/nfsen/";
$PREFIX  = '/usr/local/bin';
$USER    = 'netflow';
$WWWUSER = "apache";
$WWWGROUP = "apache";
%sources = (
    'upstream1' => { 'port' => '9996', 'col' => '#0000ff', 'type' => 'netflow' }
);
```
- ❑

```
# useradd -r -g apache -s /sbin/nologin -d /opt/nfsen -M netflow
```
- ❑

```
# ./install.pl etc/nfsen.conf
```
- ❑

```
# /opt/nfsen/bin/nfsen start
```



安裝(5)-路由器設定

□ 設定如下：

```
flow monitor-map Netflow-IPv4
```

```
record ipv4 peer-as
```

```
exporter Netflow-01
```

```
cache entries 500000
```

```
cache timeout active 30
```

```
cache timeout inactive 15
```

```
!
```

```
flow exporter-map Netflow-01
```

```
version v9
```

```
options sampler-table timeout 60
```

```
template data timeout 60
```

```
template options timeout 60
```

```
!
```

```
transport udp 9996
```

```
source Loopback0
```

```
destination 10.11.1.1
```

```
!
```




安裝(6)-檢視 tcpdump

```
root@netflow:~  
[root@netflow ~]# tcpdump -i eth1 udp port 9996  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes  
11:22:24.163368 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 612  
11:22:24.163399 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156  
11:22:24.163805 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156  
11:22:24.165433 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 139  
2  
11:22:24.165592 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 612  
11:22:24.166056 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 139  
2  
11:22:24.166249 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 139  
2  
11:22:24.166388 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 544  
11:22:24.166474 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 416  
11:22:24.166514 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 92  
11:22:24.166608 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156  
11:22:24.166692 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 92  
11:22:24.166899 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156  
11:22:24.166961 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 92  
11:22:24.167017 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156  
11:22:24.167124 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156  
11:22:24.167180 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156  
11:22:24.167279 IP 192.192.60.115.25244 > 140.115.2.38.palace-5: UDP, length 156
```



安裝(7)- HostStats 套件

- ☐ #cd /opt
- ☐ #wget https://sourceforge.net/projects/hoststats/files/hoststats-1.1.5.tar.gz
- ☐ #tar zxvf hoststats-1.1.5.tar.gz
- ☐ #cd hoststats-1.1.5
- ☐ #./install-libnfdump.sh
- ☐ #mkdir -p /var/www/hoststats
- ☐ #yum install gcc-c++
- ☐ #./configure
- ☐ #make
- ☐ #make install
- 輸入安裝路徑 /var/www/hoststats/
輸入data 及 log 路徑
- ☐ #chown apache:apache -R /var/www/hoststats/
- ☐ #/var/www/hoststats/hoststats start



Computer Center, National Central University.



Thank You!