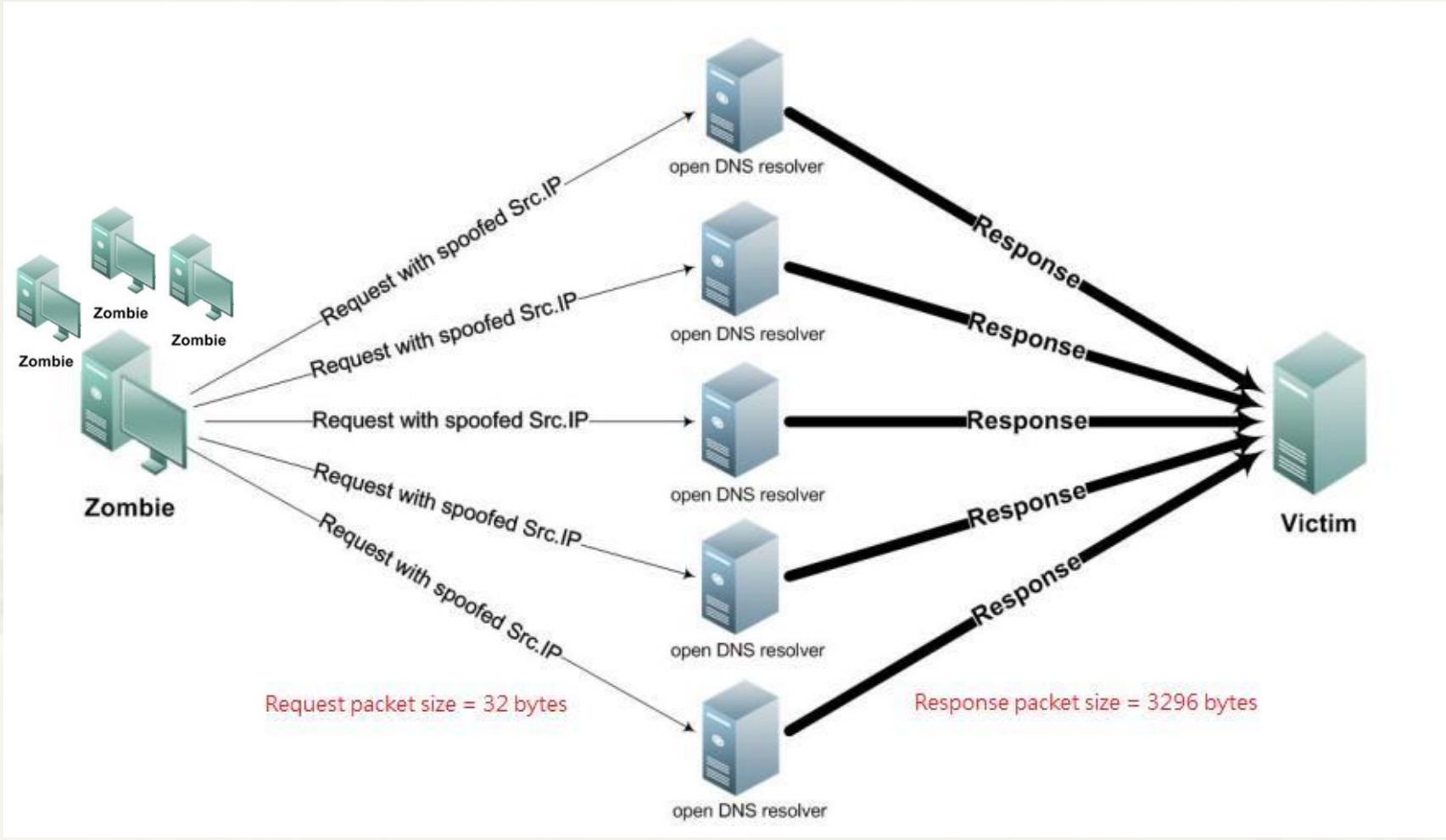
# DDoS 事件分析

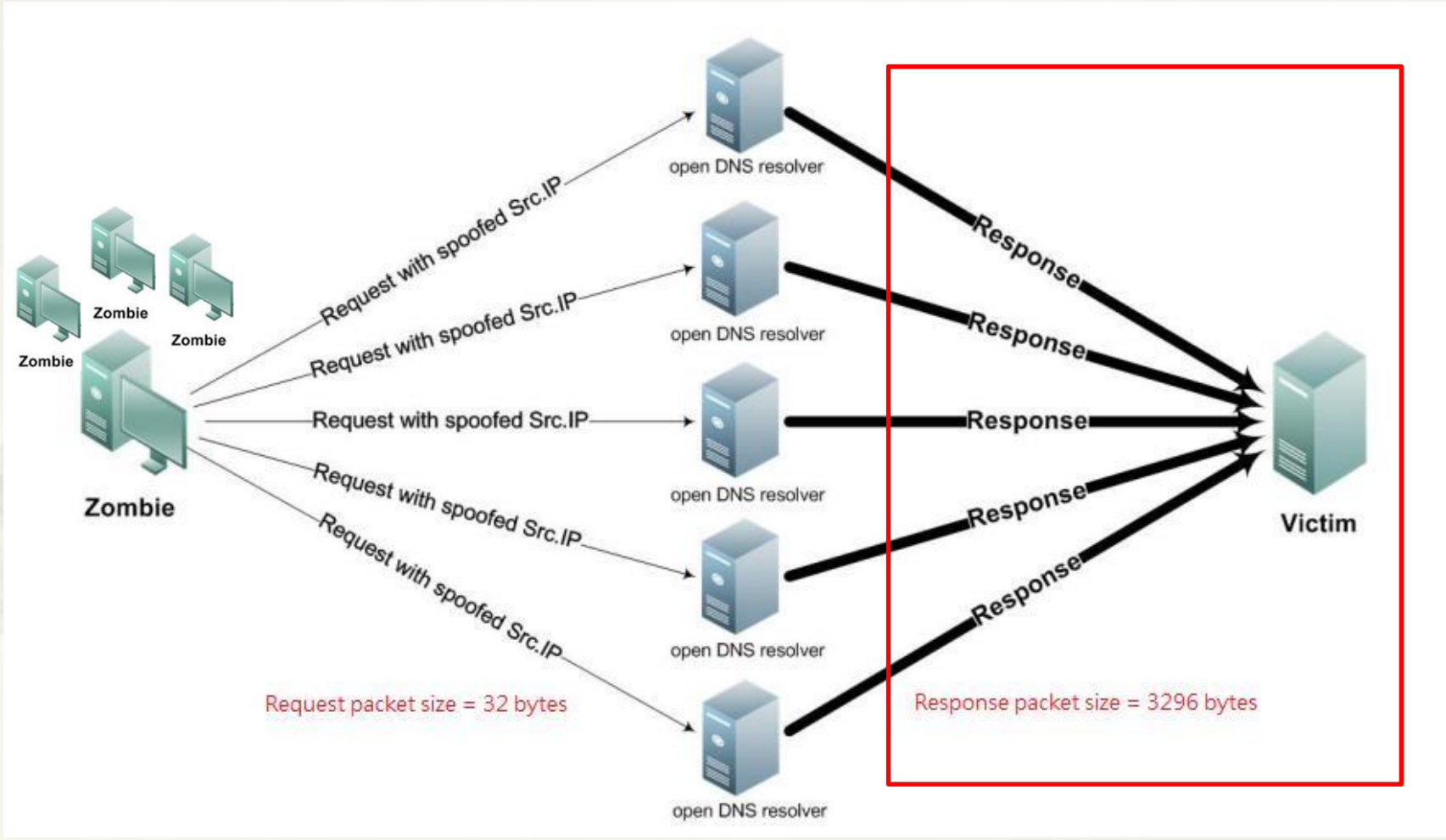
# DDoS 攻擊方式

- 反射攻擊
  - 外對內: 遭受反射攻擊
  - 外對內 + 內對外: 內部有反射 Server 被利用於攻擊受害者
  - 內對外: 內部有 BOT 利用外部反射 Server 攻擊受害者
- 直接攻擊
  - 外對內: 遭受攻擊
  - 內對外: 內部有 BOT 攻擊受害者

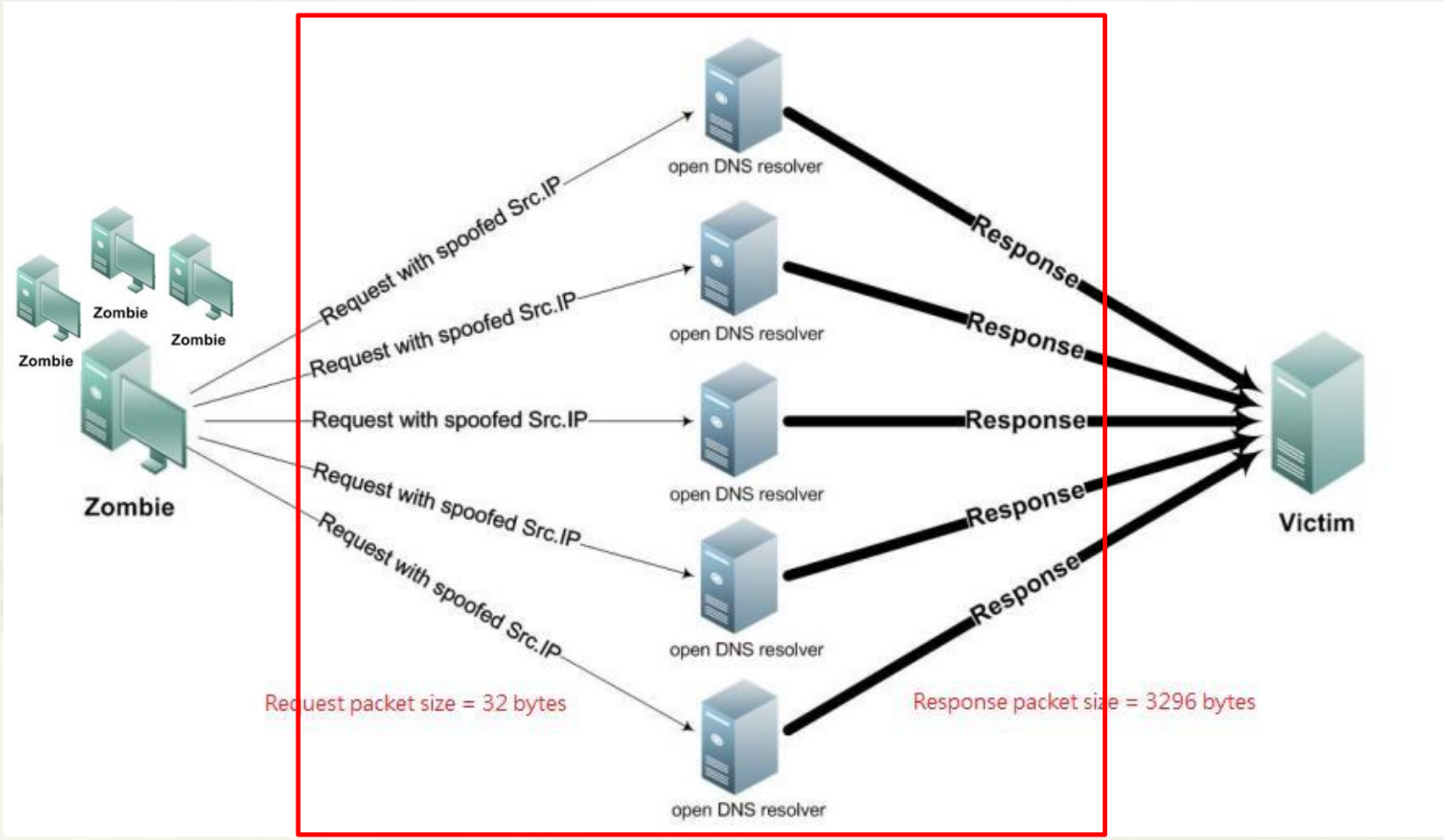
# 反射攻擊架構圖


Zombie
Zombie
Zombie
Zombie
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
Response
Response
Response
Response
Response
Victim
Request packet size = 32 bytes
Response packet size = 3296 bytes

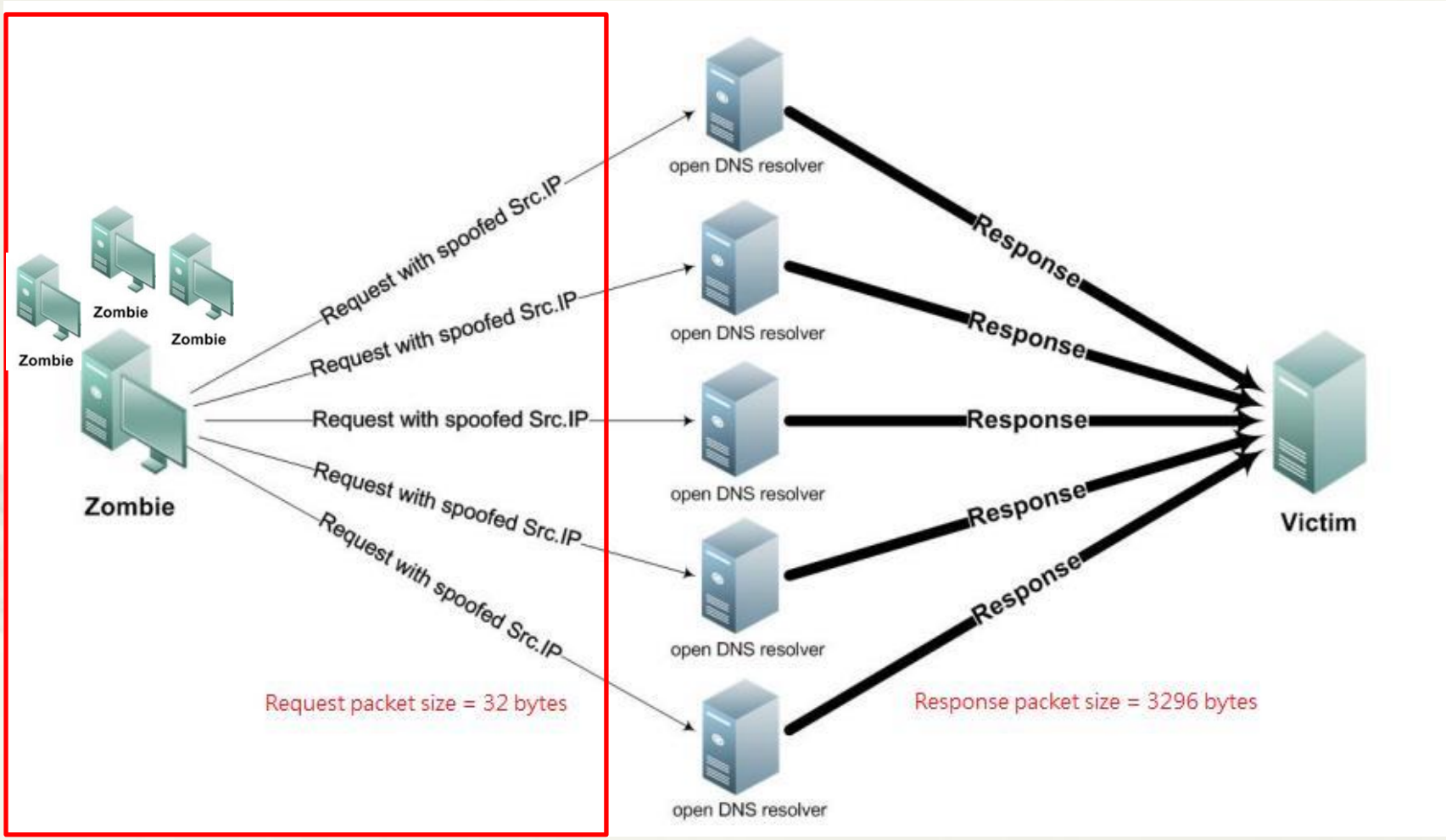
# 外對內: 遭受反射攻擊


Zombie
Zombie
Zombie
Zombie
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
Response
Response
Response
Response
Response
Victim
Request packet size = 32 bytes
Response packet size = 3296 bytes

# 外對內 + 內對外
# 內部有反射 **Server** 被利用於攻擊受害者



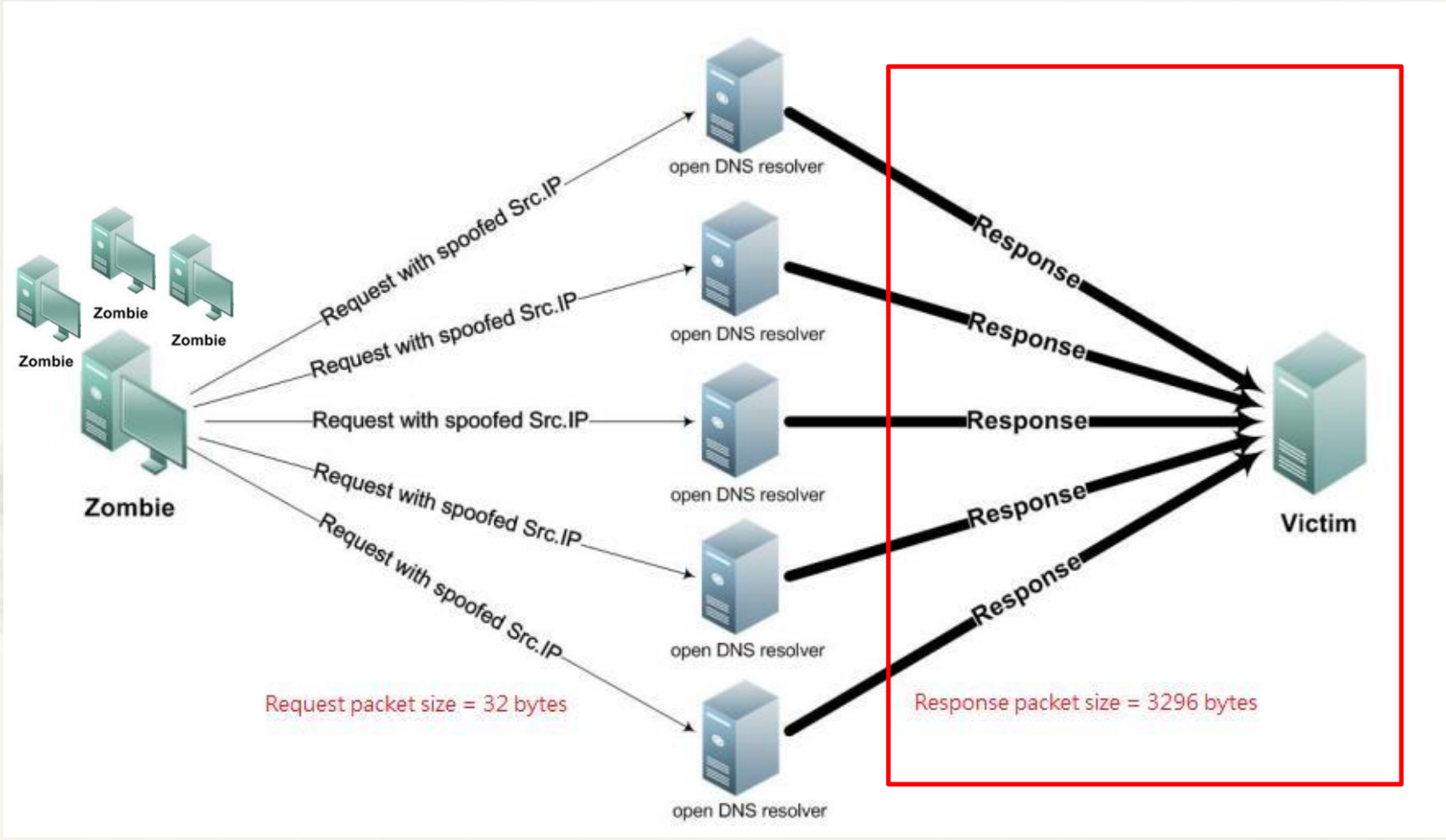
# 內對外: 內部有 **BOT** 利用外部反射 **Server** 攻擊受害者



# 反射攻擊類型

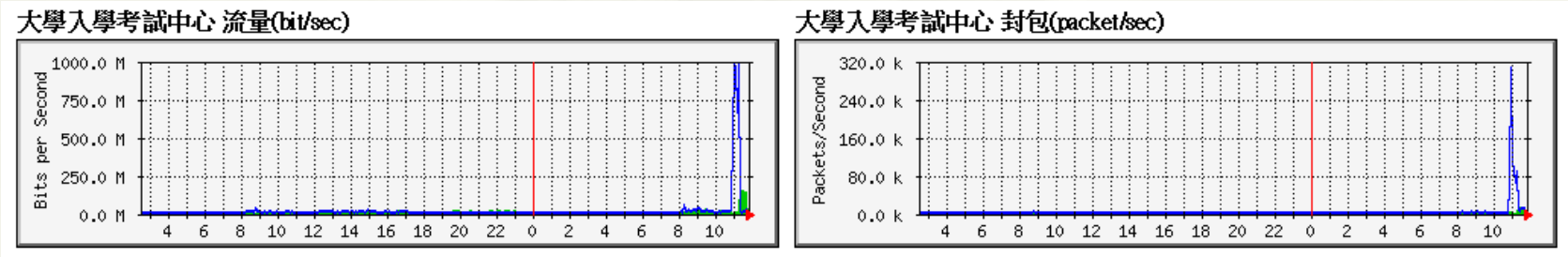
- Protocol: UDP
- 反射類型與 Port
  - DNS (Query Any Record): 53
  - RPC(Remote Procedure Call)/Port Mapper/NFS: 111
  - NTP (Mon List): 123
  - NetBIOS/SMB: 137
  - SNMP: 161
  - LDAP (CLDAP Query Root): 389
  - SSDP: 1900
  - Memcached: 11211

# 外對內: 遭受反射攻擊

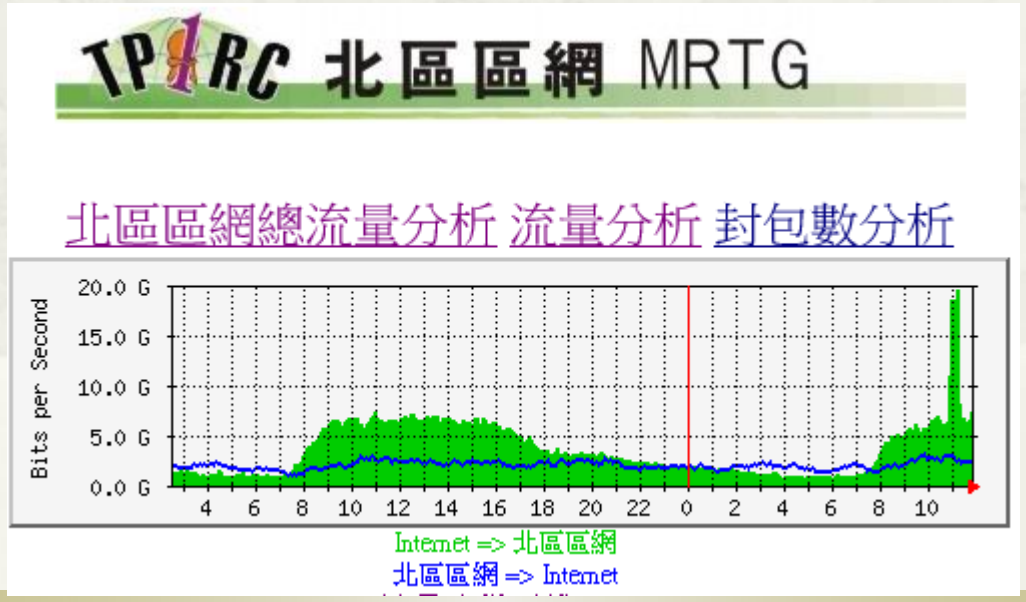

Zombie
Zombie
Zombie
Zombie
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
Response
Response
Response
Response
Response
Victim
Request packet size = 32 bytes
Response packet size = 3296 bytes

# 外對內: 遭受DNS反射攻擊
# 大考中心 20190124 考場公佈

* Bits Per Second & Pkts Per Second: 高

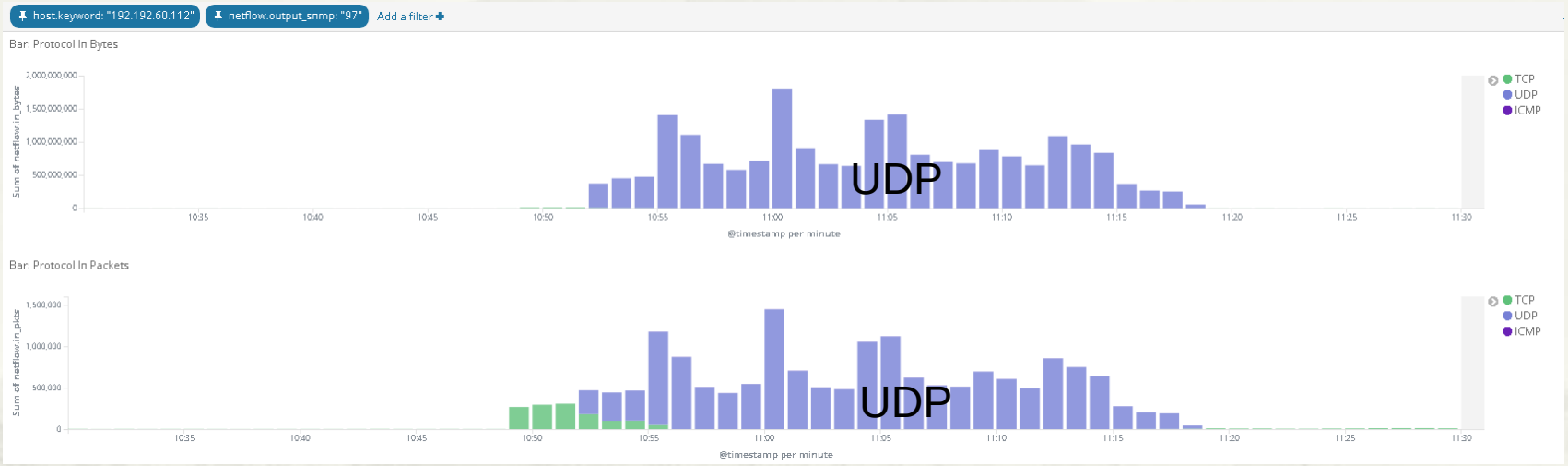



* 區網骨幹



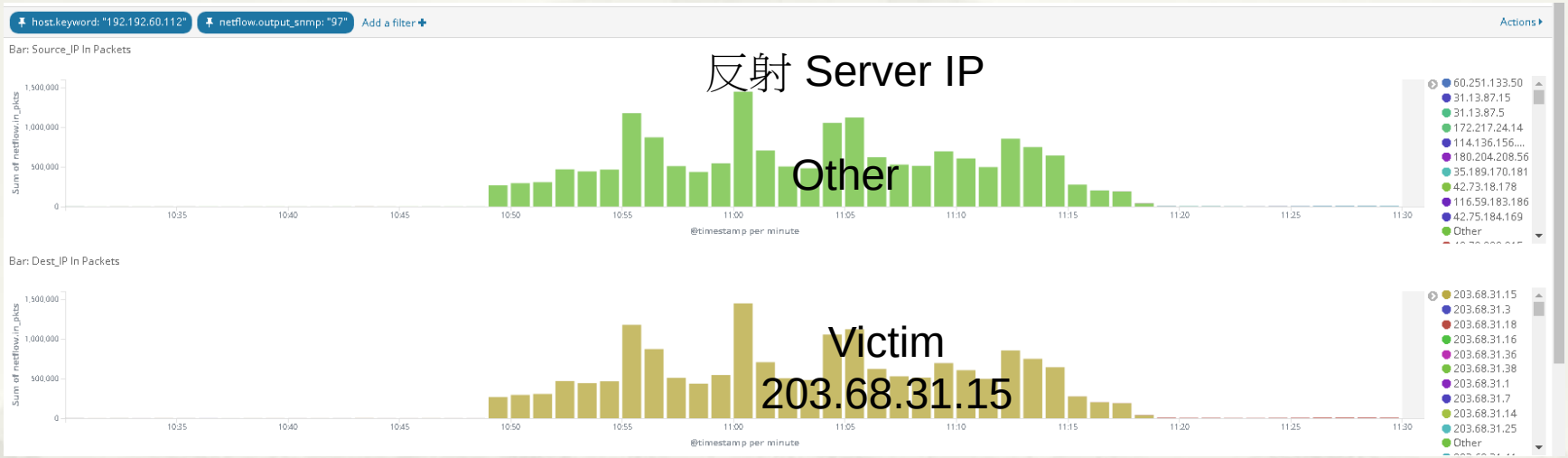
# 外對內: 遭受**DNS**反射攻擊

* Protocol: UDP

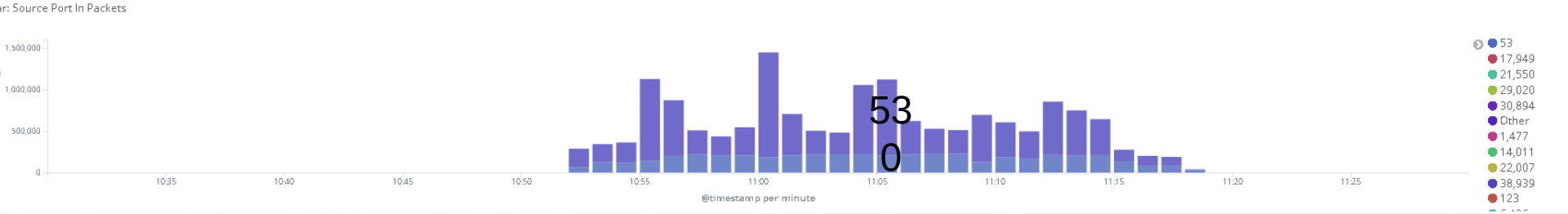


# 外對內: 遭受DNS反射攻擊

- Source IP & Dest IP

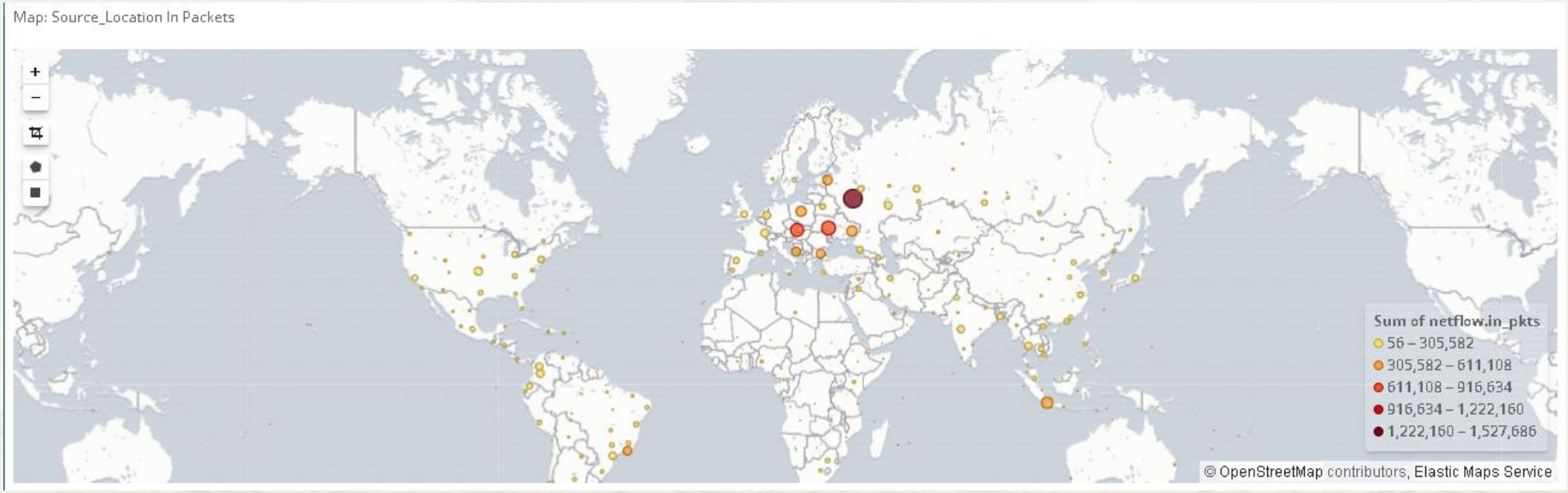



- Source Port

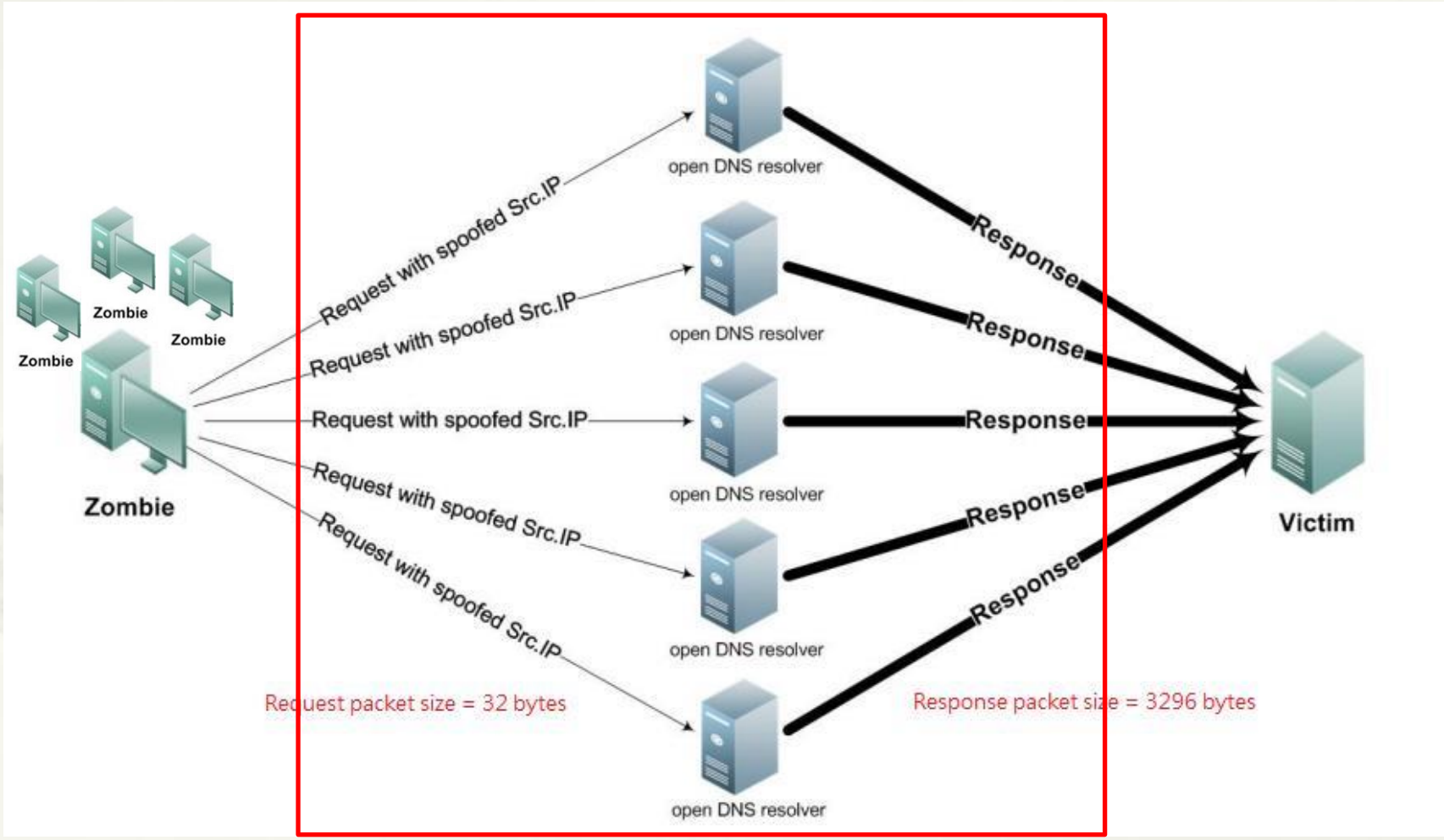


# 外對內: 遭受DNS反射攻擊

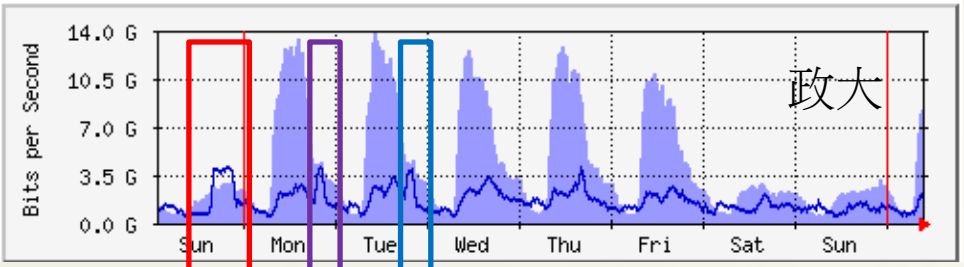
* 攻擊來源

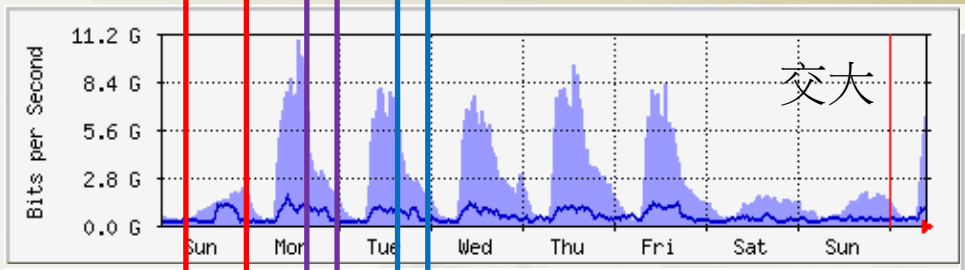


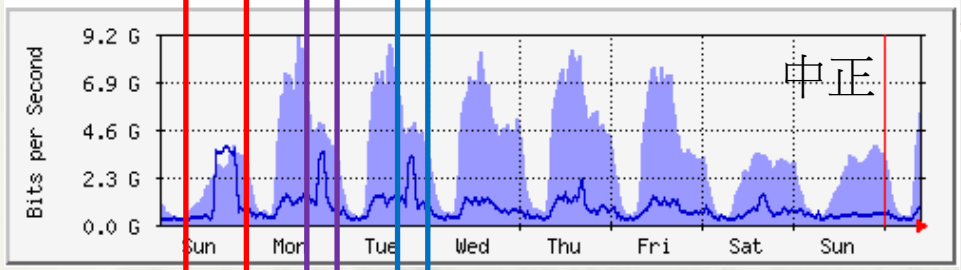
# 外對內 + 內對外
# 內部有反射 **Server** 被利用於攻擊受害者

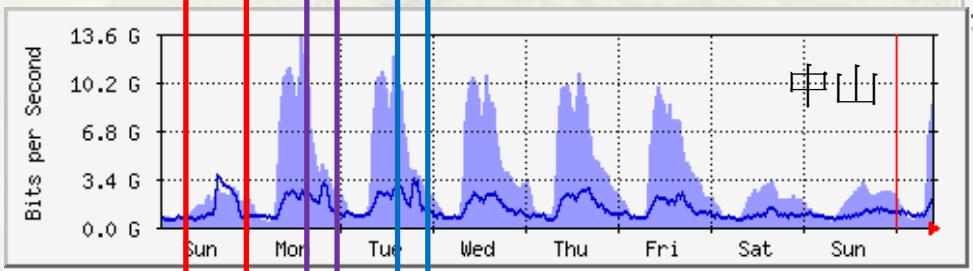


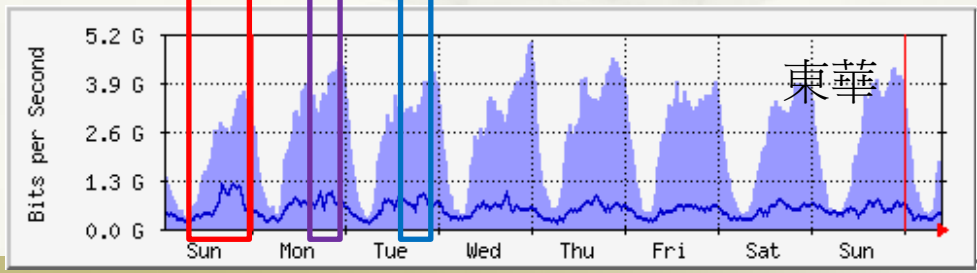
# 20190303~0305
# 各區網中心

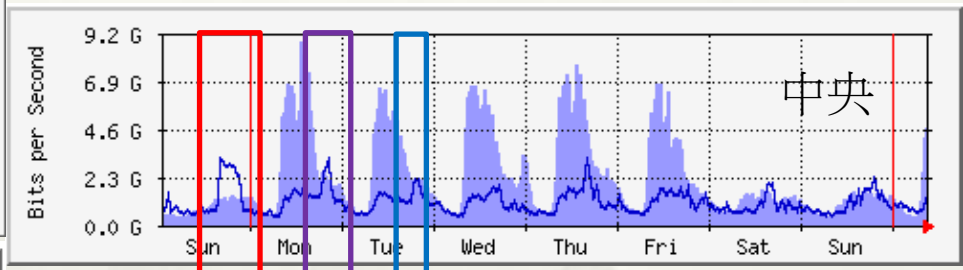


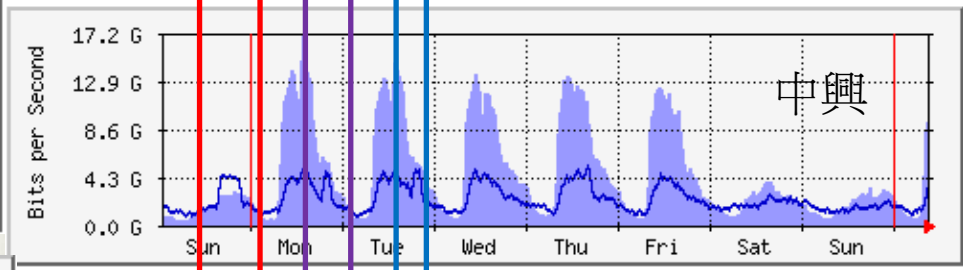



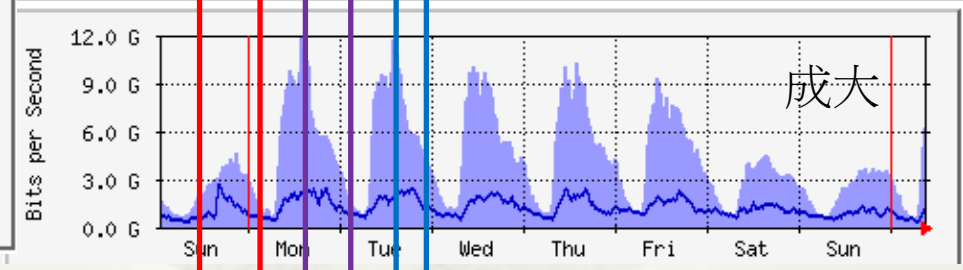



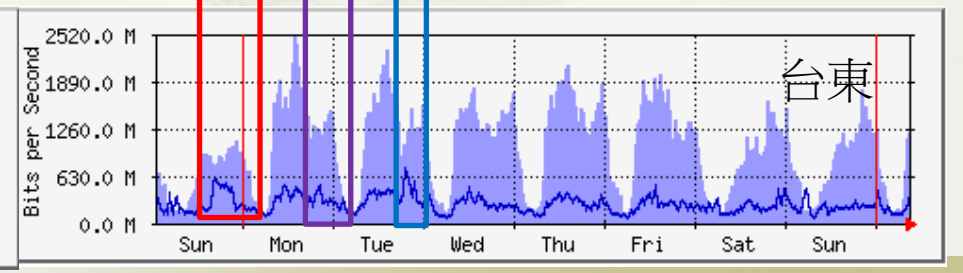



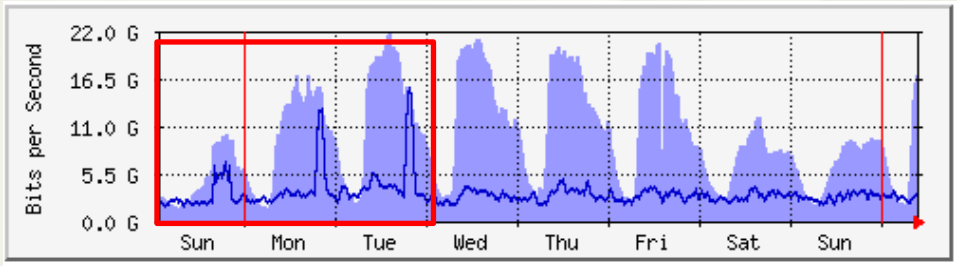



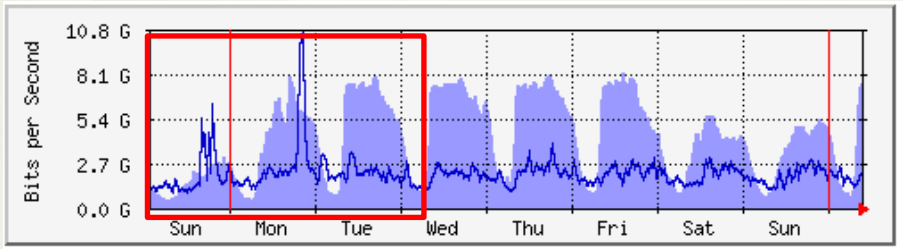
# TANet DDoS 攻擊出口
# Max 25~30 Gbps

TANet to Internet IPv4 [30G]



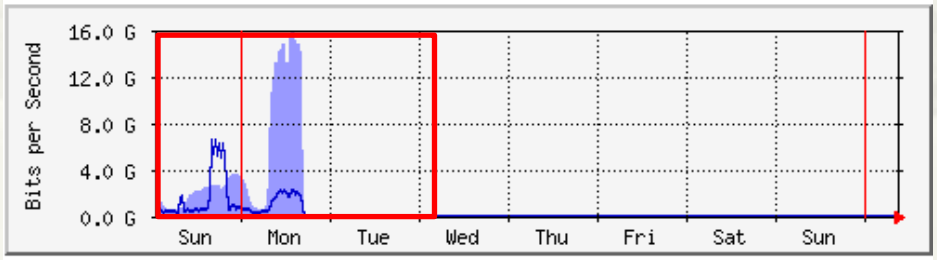

| | 最大 | 平均 | 目前 |
|---|---|---|---|
| Internet ⇒ TANet | 21.8 Gb/秒 (67.7%) | 9419.5 Mb/秒 (29.2%) | 16.9 Gb/秒 (52.4%) |
| TANet ⇒ Internet | 15.2 Gb/秒 (47.2%) | 3093.5 Mb/秒 (9.6%) | 3132.5 Mb/秒 (9.7%) |

CHIEF Transit Service



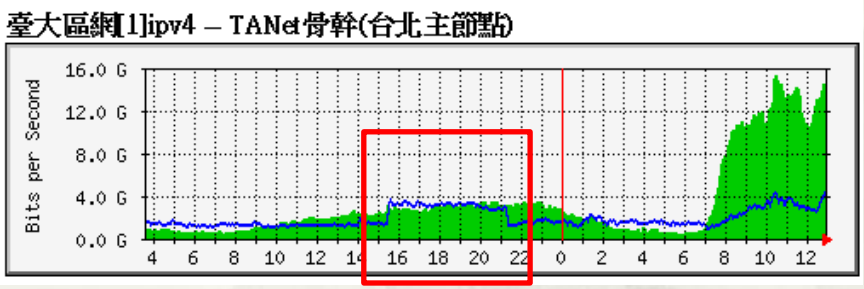

| | 最大 | 平均 | 目前 |
|---|---|---|---|
| CHIEF ⇒ TANet | 8180.1 Mb/秒 (76.2%) | 4144.9 Mb/秒 (38.6%) | 7496.5 Mb/秒 (69.8%) |
| TANet ⇒ CHIEF | 10.6 Gb/秒 (98.3%) | 2016.8 Mb/秒 (18.8%) | 2007.1 Mb/秒 (18.7%) |

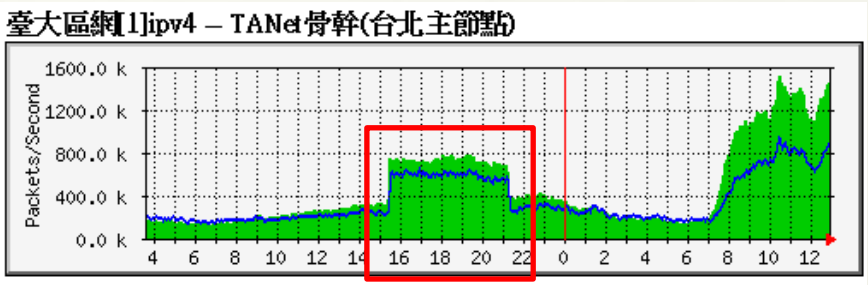
TPIX




| | 最大 | 平均 | 目前 |
|---|---|---|---|
| TPIX ⇒ 教育部 : | 15.9 Gb/秒 (49.5%) | 4318.9 Mb/秒 (13.4%) | 0.0 b/秒 (0.0%) |
| 教育部 ⇒ TPIX : | 6513.3 Mb/秒 (20.2%) | 1369.3 Mb/秒 (4.3%) | 0.0 b/秒 (0.0%) |

# 偵測方法 – MRTG
# 臺大區網骨幹



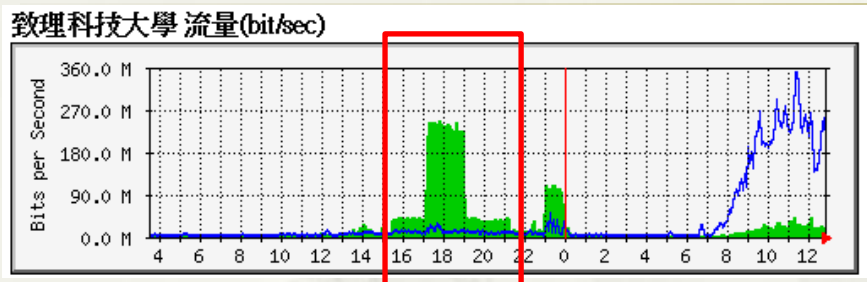



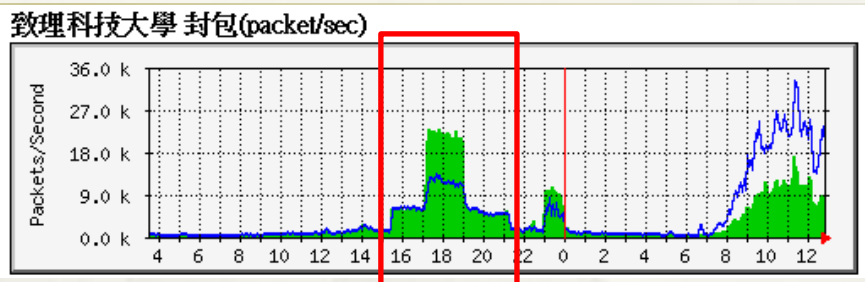

20190303 15:30~21:10

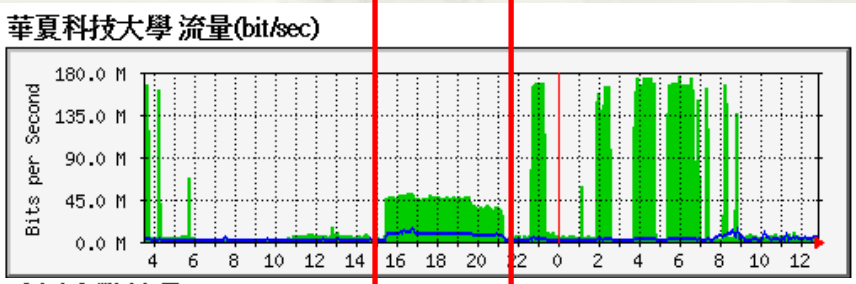
* TANet連線單位_反射攻擊_20190303_bps.mht
* TANet連線單位_反射攻擊_20190303_pps.mht
* TANet連線單位_反射攻擊_20190304_bps.mht
* TANet連線單位_反射攻擊_20190304_pps.mht
* TANet連線單位_反射攻擊_20190305_bps.mht
* TANet連線單位_反射攻擊_20190305_pps.mht

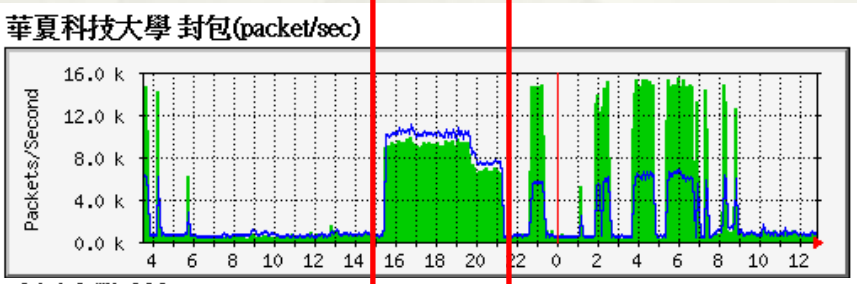
# 異常連線單位

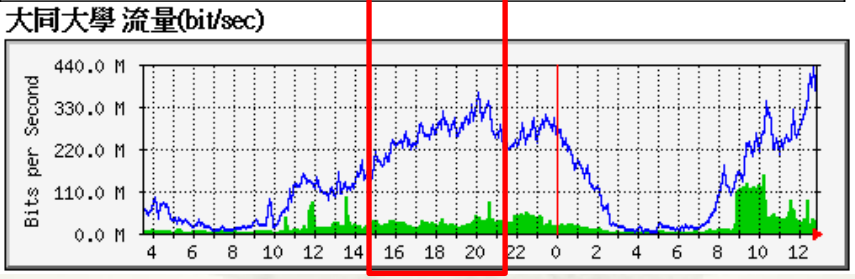
# 20190303

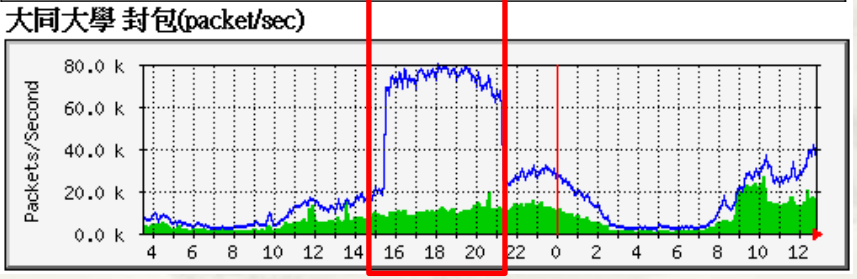


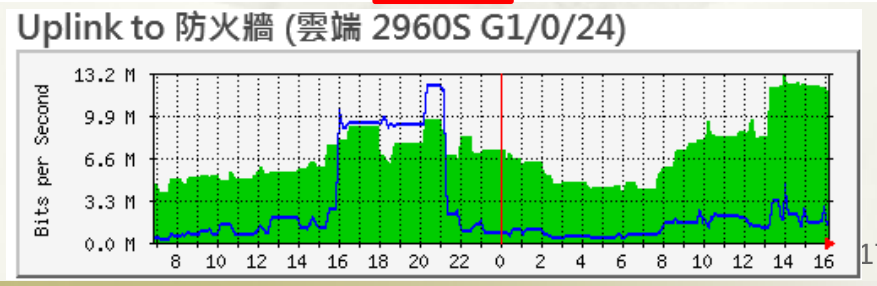



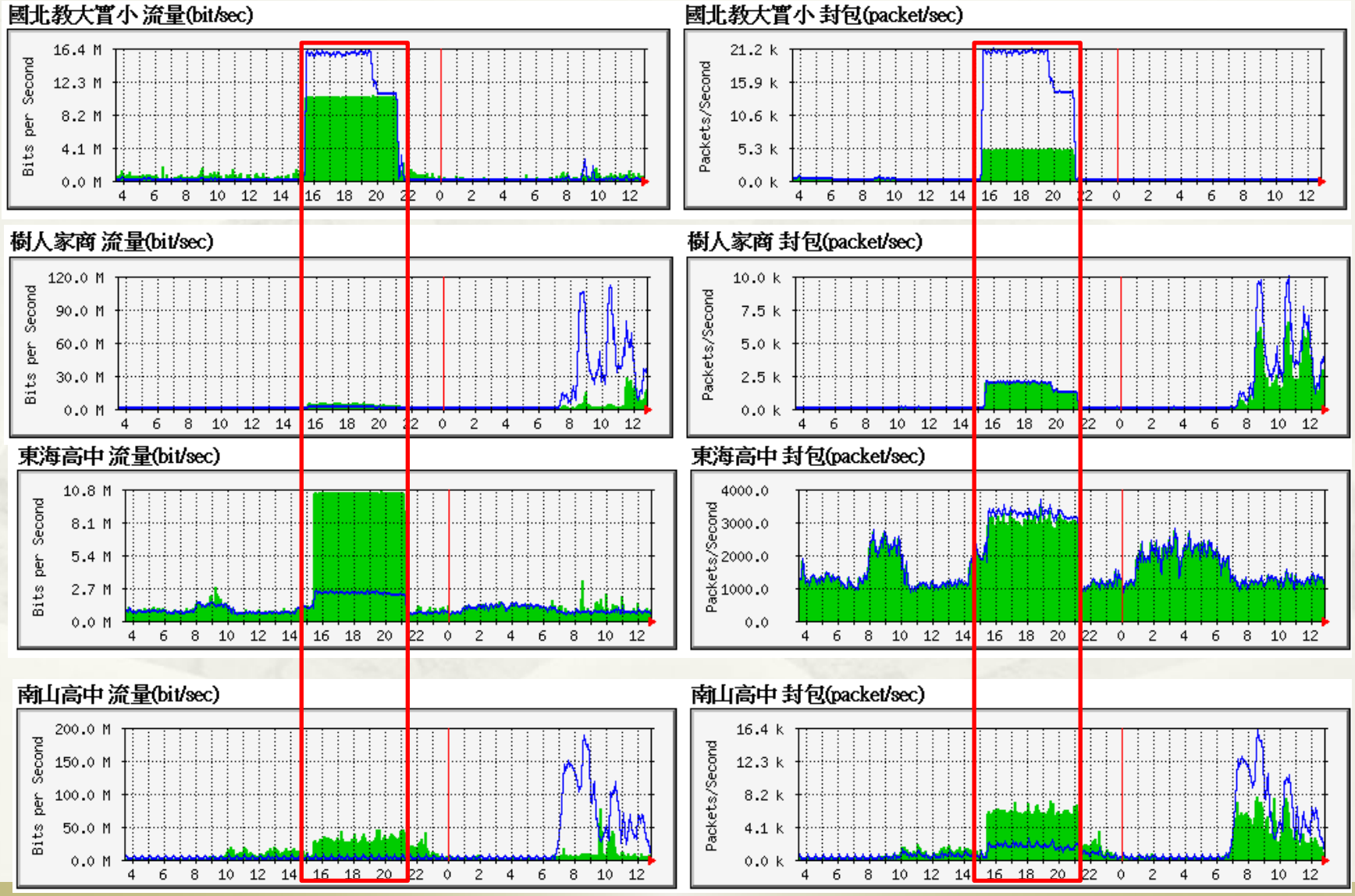



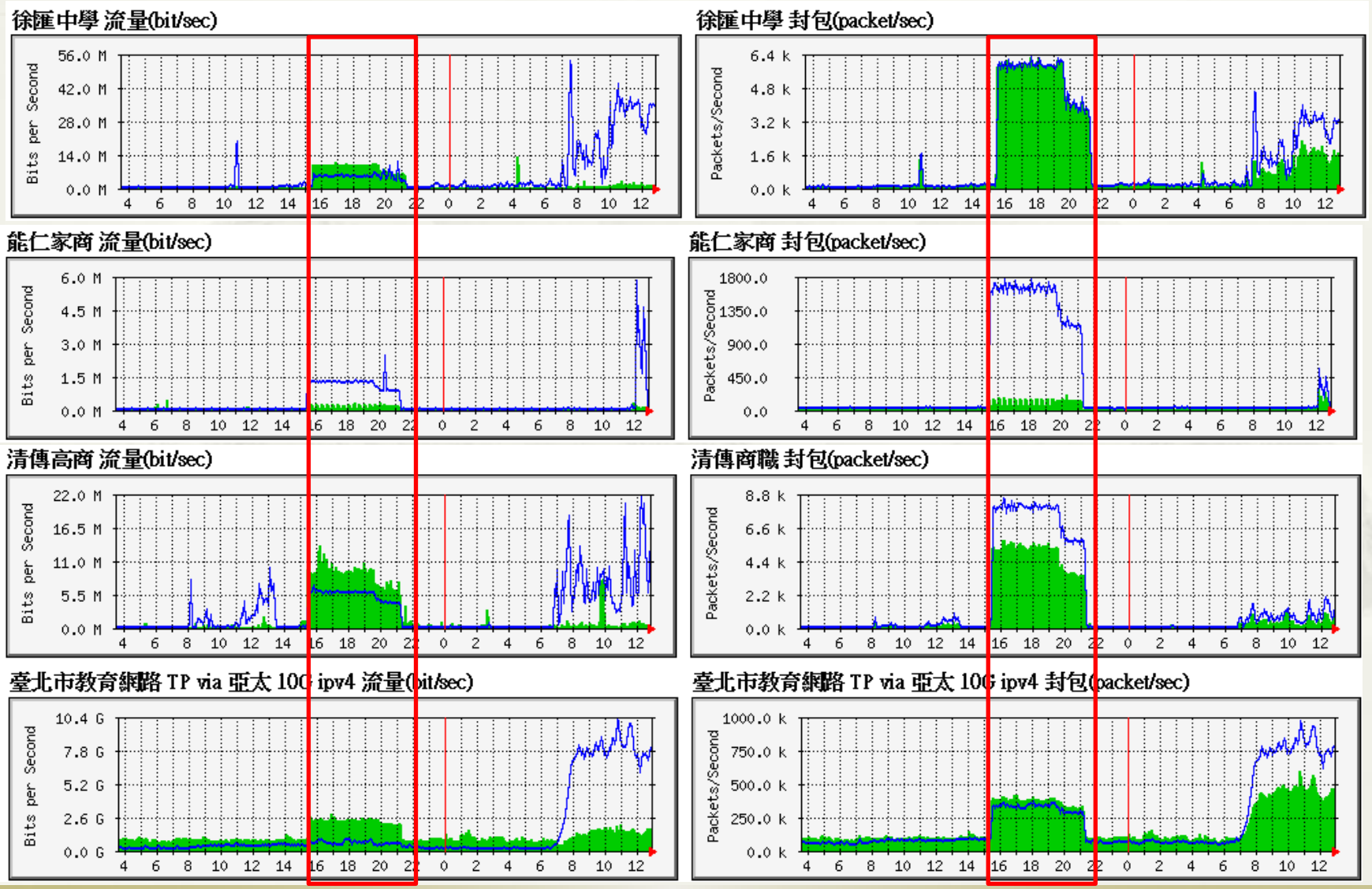
# 異常連線單位

# 20190303



# 異常連線單位

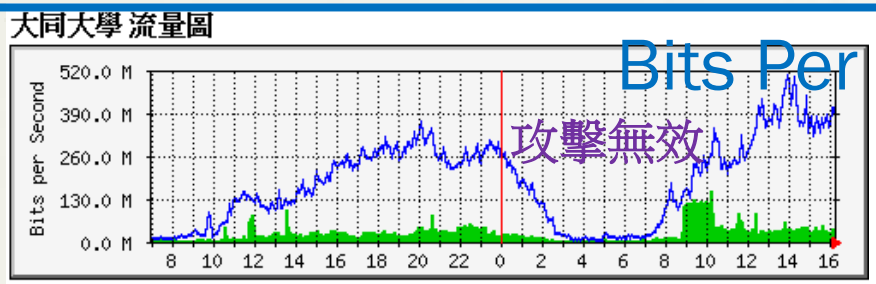
# 20190303

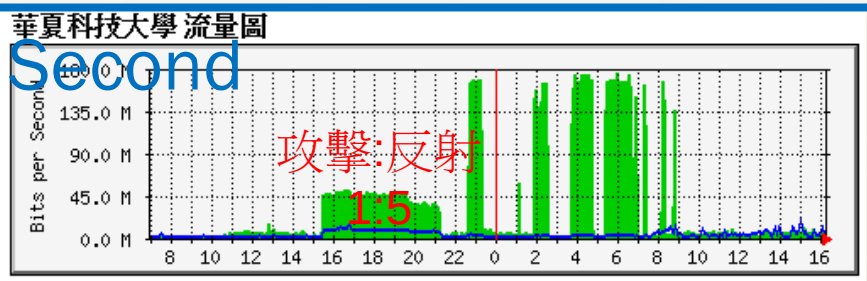


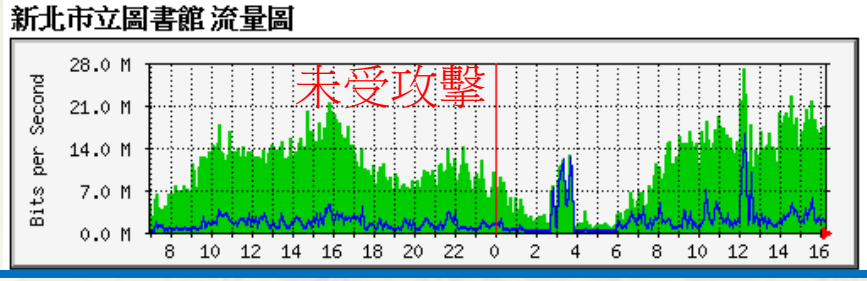
# 20190303

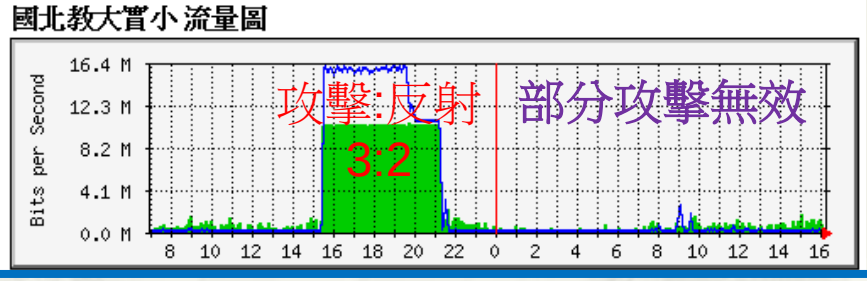
# 攻擊:反射 比例分析

## Bits Per Second

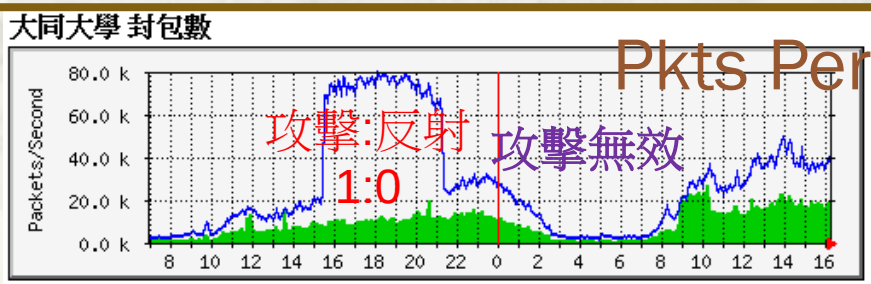


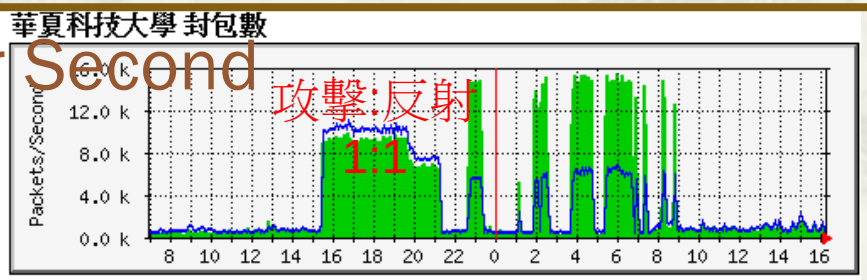



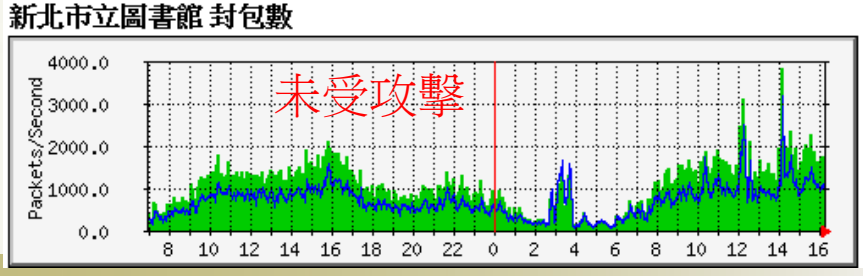



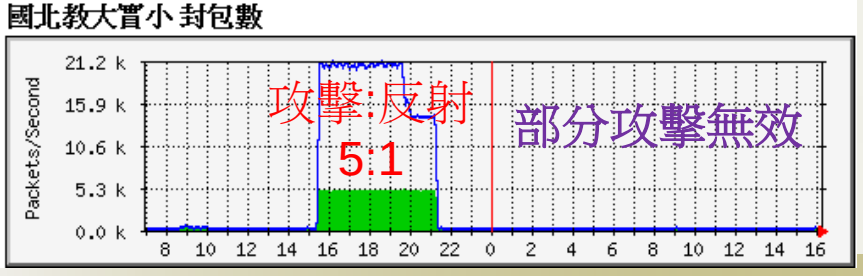




## Pkts Per Second

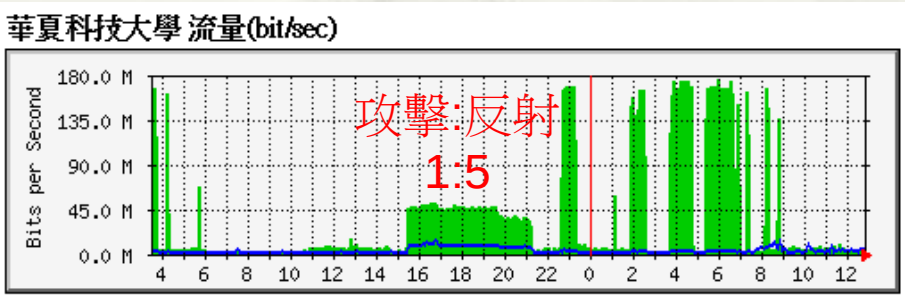


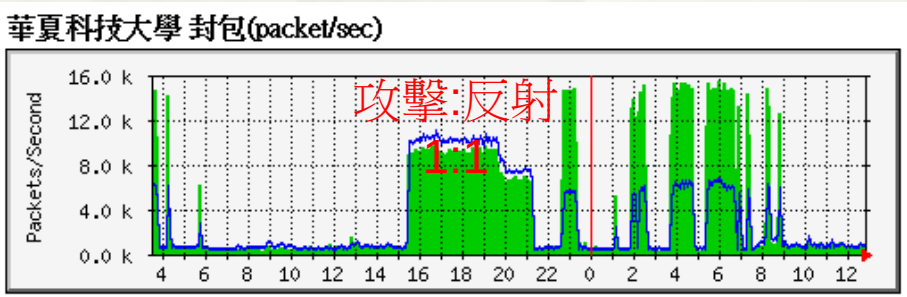



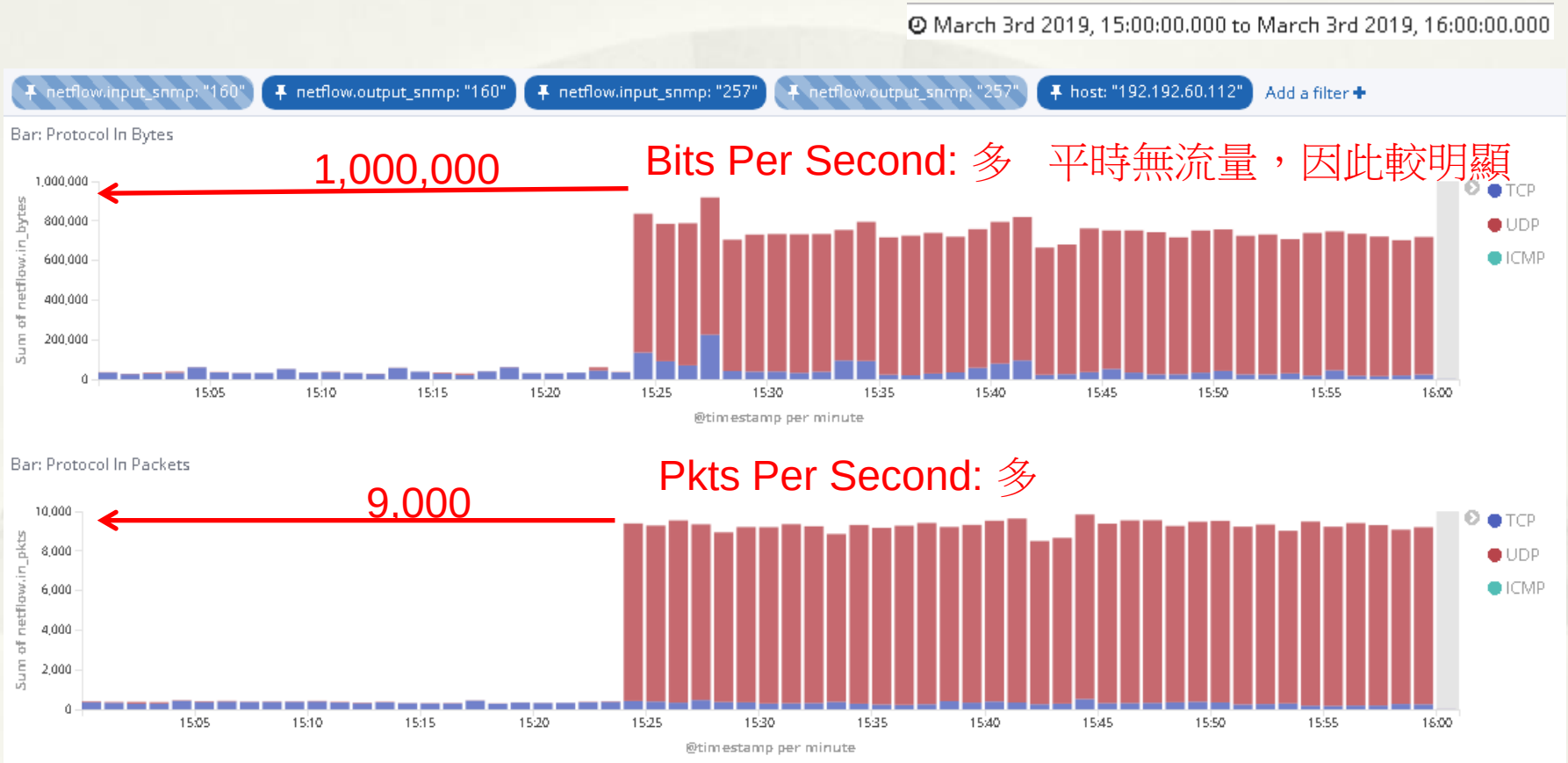



# Case. 華夏科大 20190303
# MRTG



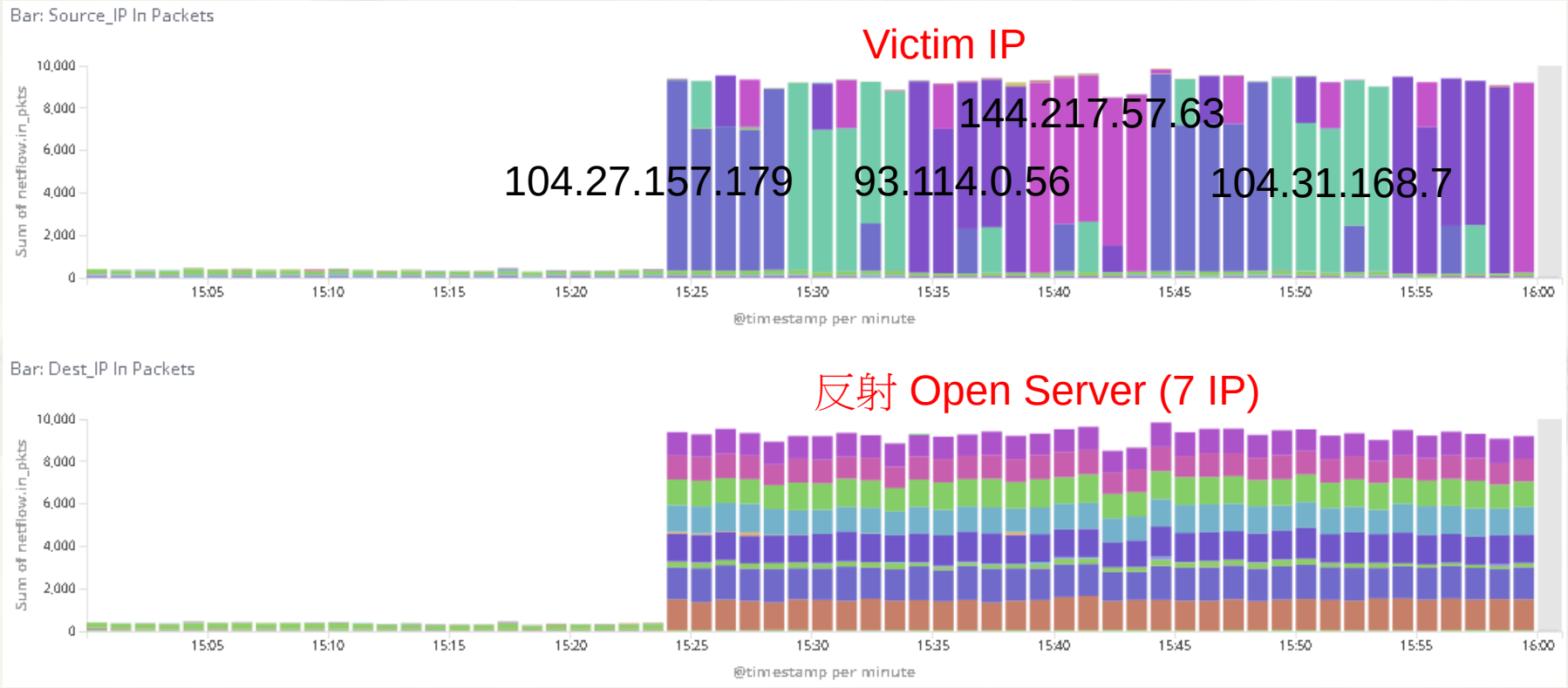



# Case. 華夏科大 20190303
# 外對內 Protocol

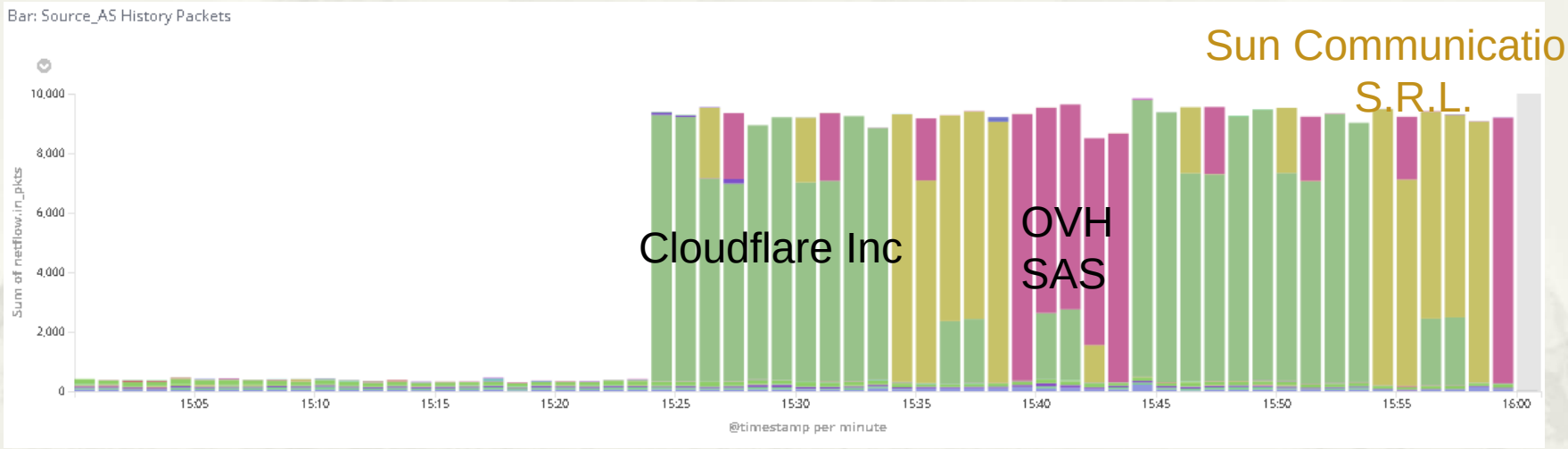


# Case. 華夏科大 20190303
# 外對內 Port

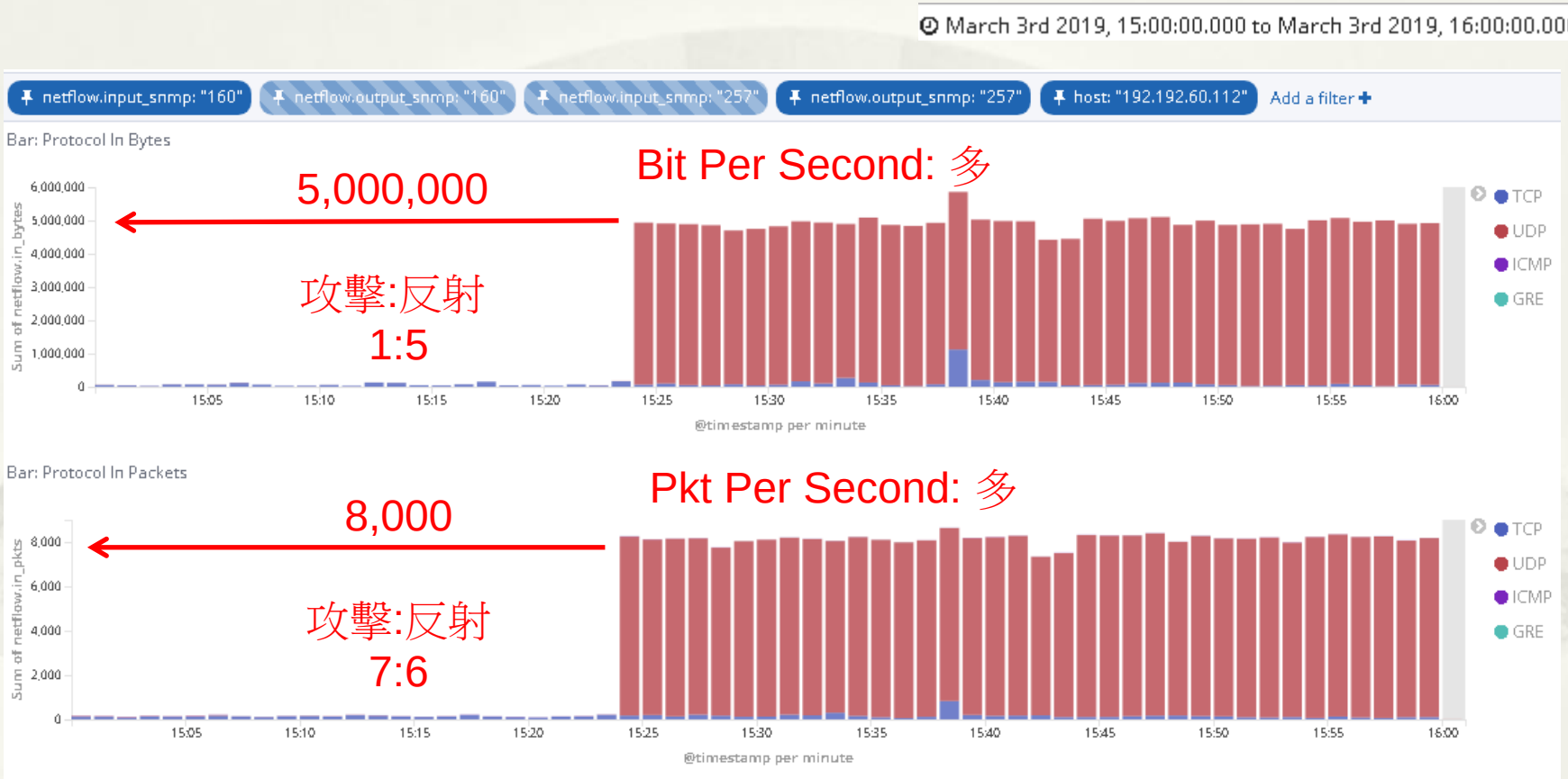
# Case. 華夏科大 20190303
# 外對內 IP



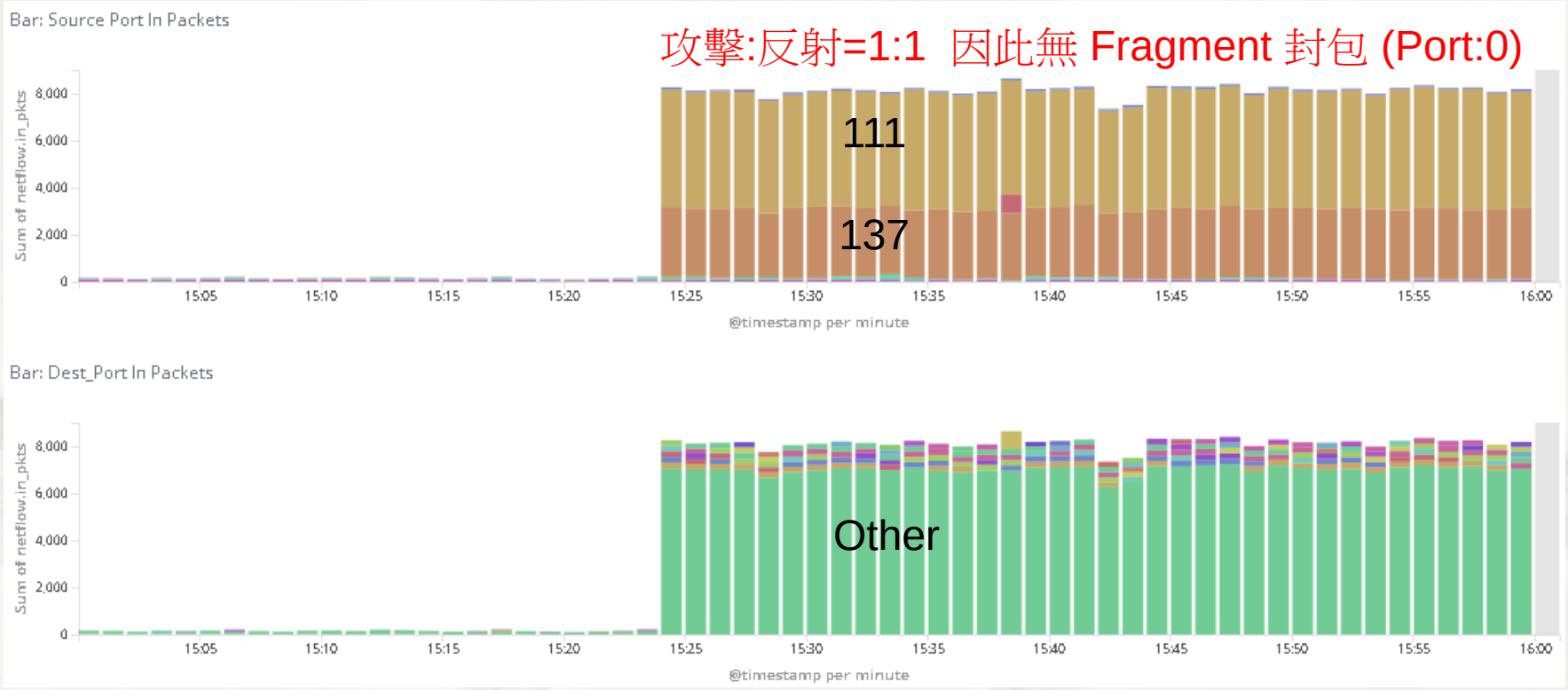
# Case. 華夏科大 20190303
# 外對內 AS



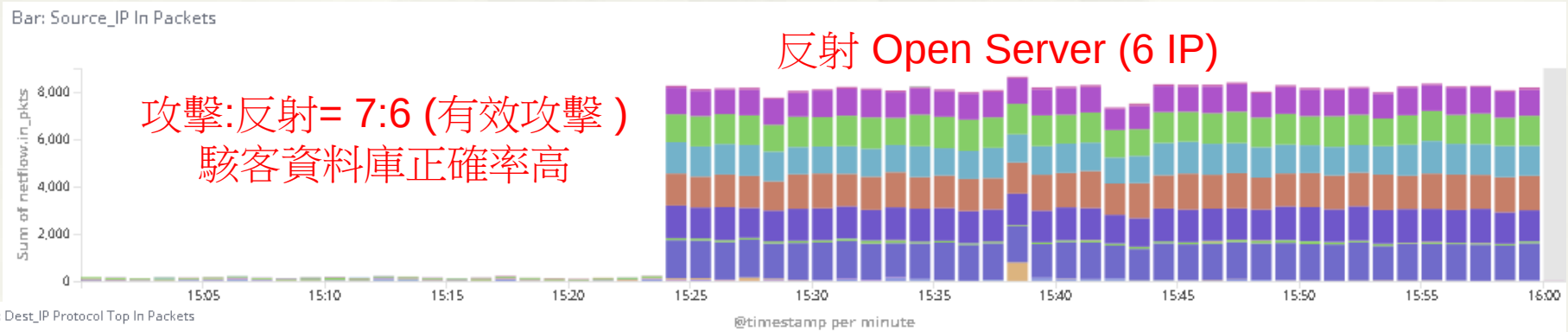
# Case. 華夏科大 20190303
# 內對外 Protocol



# Case. 華夏科大 20190303 內對外 Port

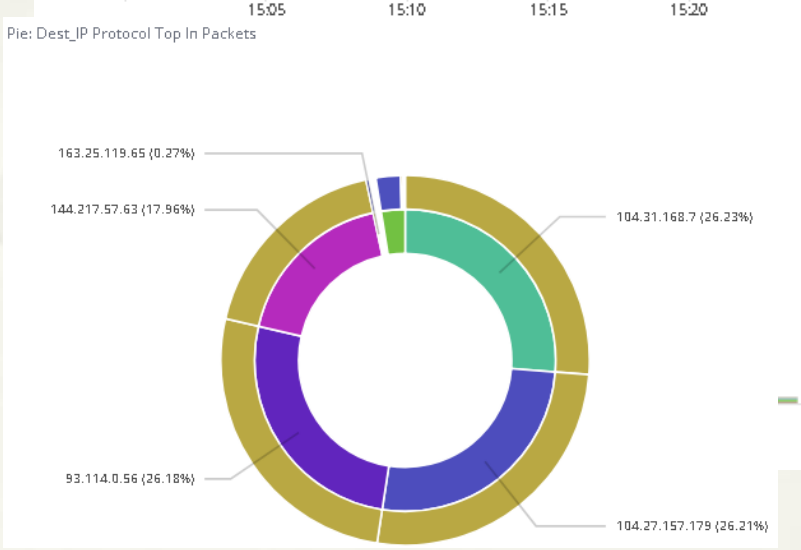


# Case. 華夏科大 20190303 內對外 IP

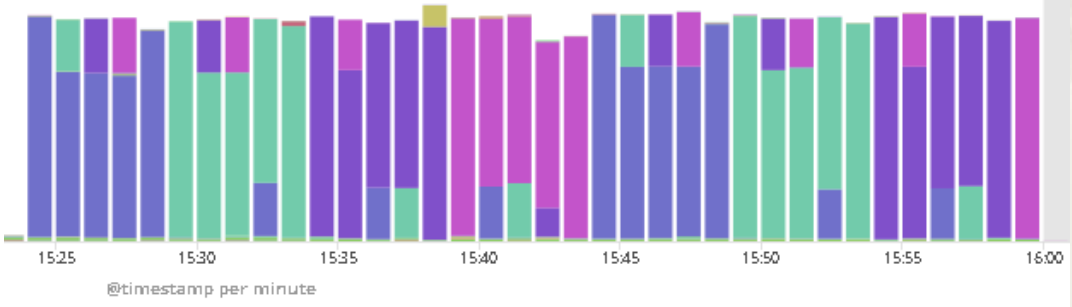



攻擊:反射= 7:6 (有效攻擊 )
駭客資料庫正確率高

反射 Open Server (6 IP)

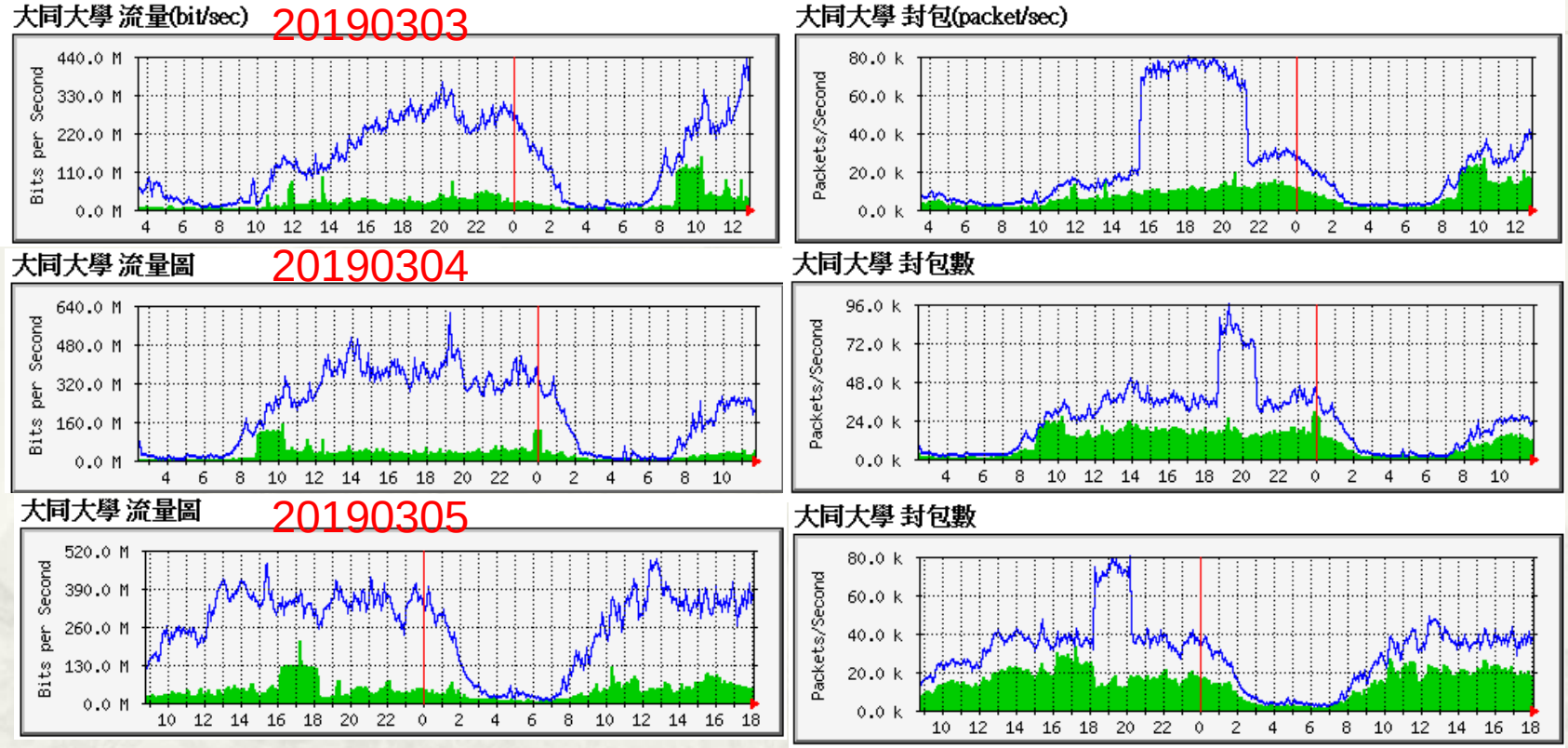



Victim IP



# Case.大同大學 (無效反射)

## MRTG

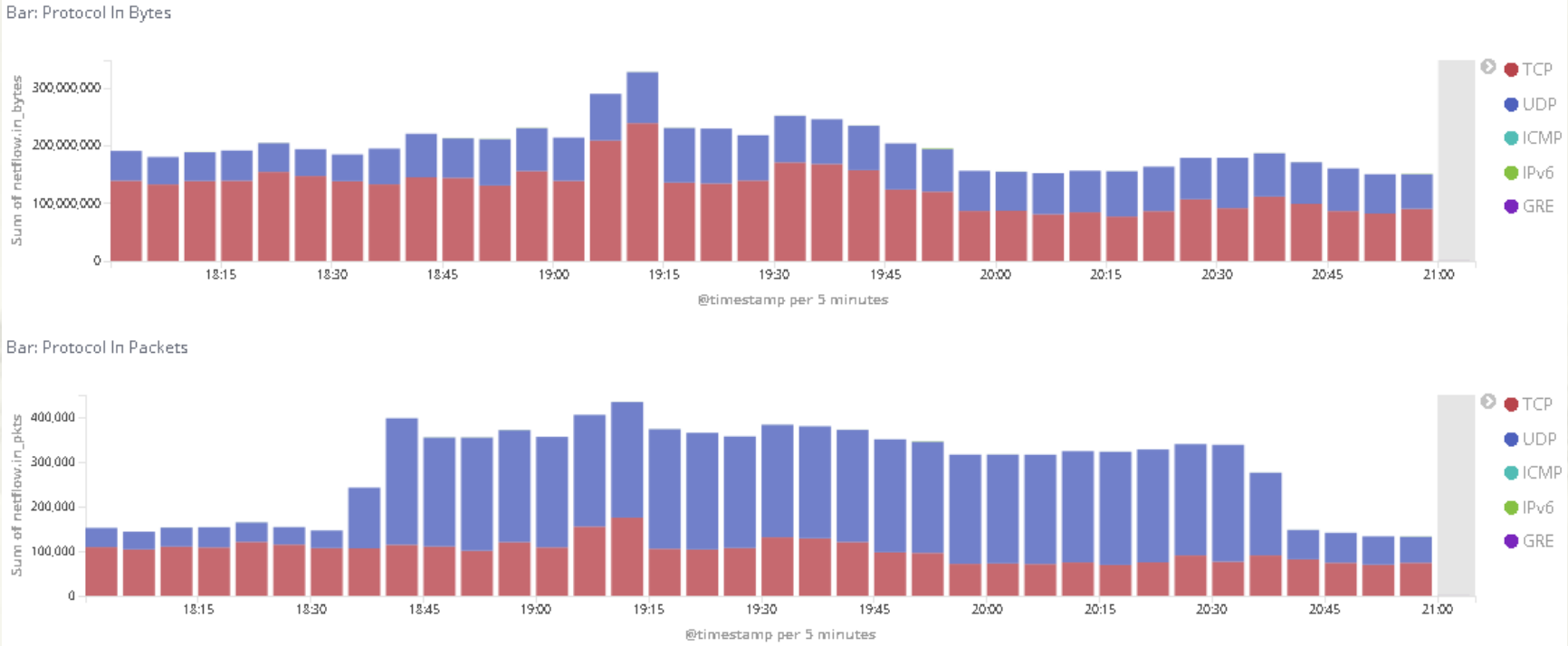



- 無效的反射攻擊，可能原因:
  - 反射 Open Server 無效
  - 校內有 DDoS 設備: A10 3030S (Inline)

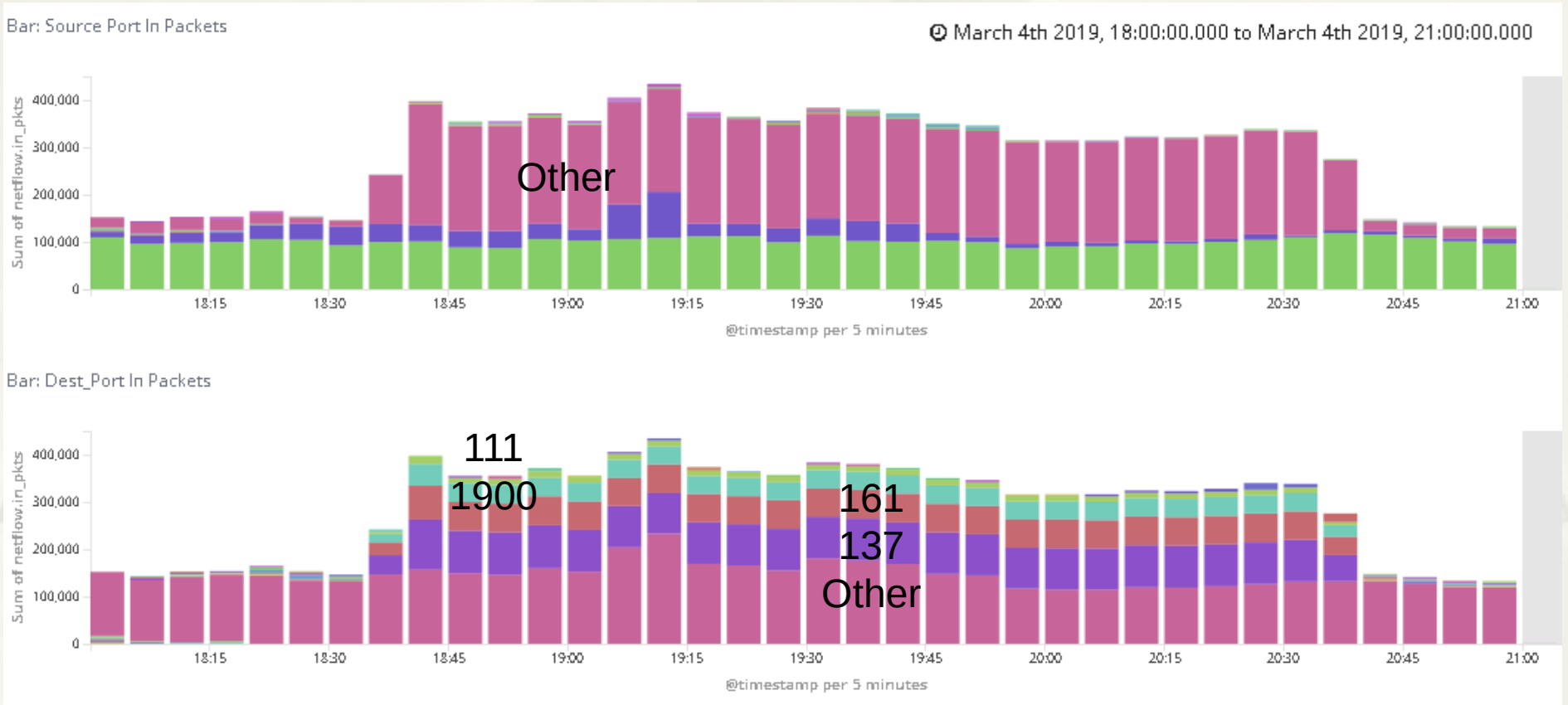
# Case.大同大學20190304
# 外對內 Protocol

March 4th 2019, 18:00:00.000 to March 4th 2019, 21:00:00.000

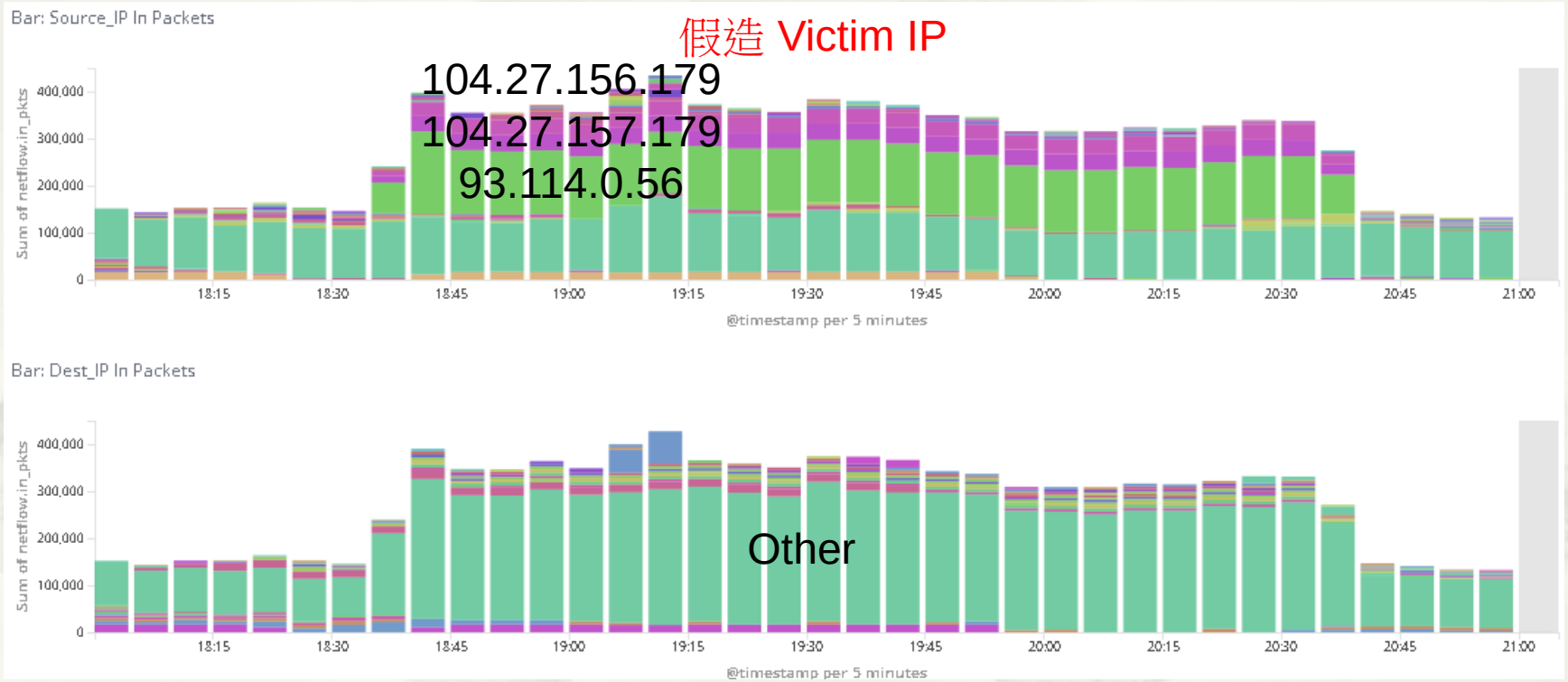
host.keyword: "192.192.60.112" | netflow.l4_dst_port: "161" | netflow.output_snmp: "49" | Add a filter +



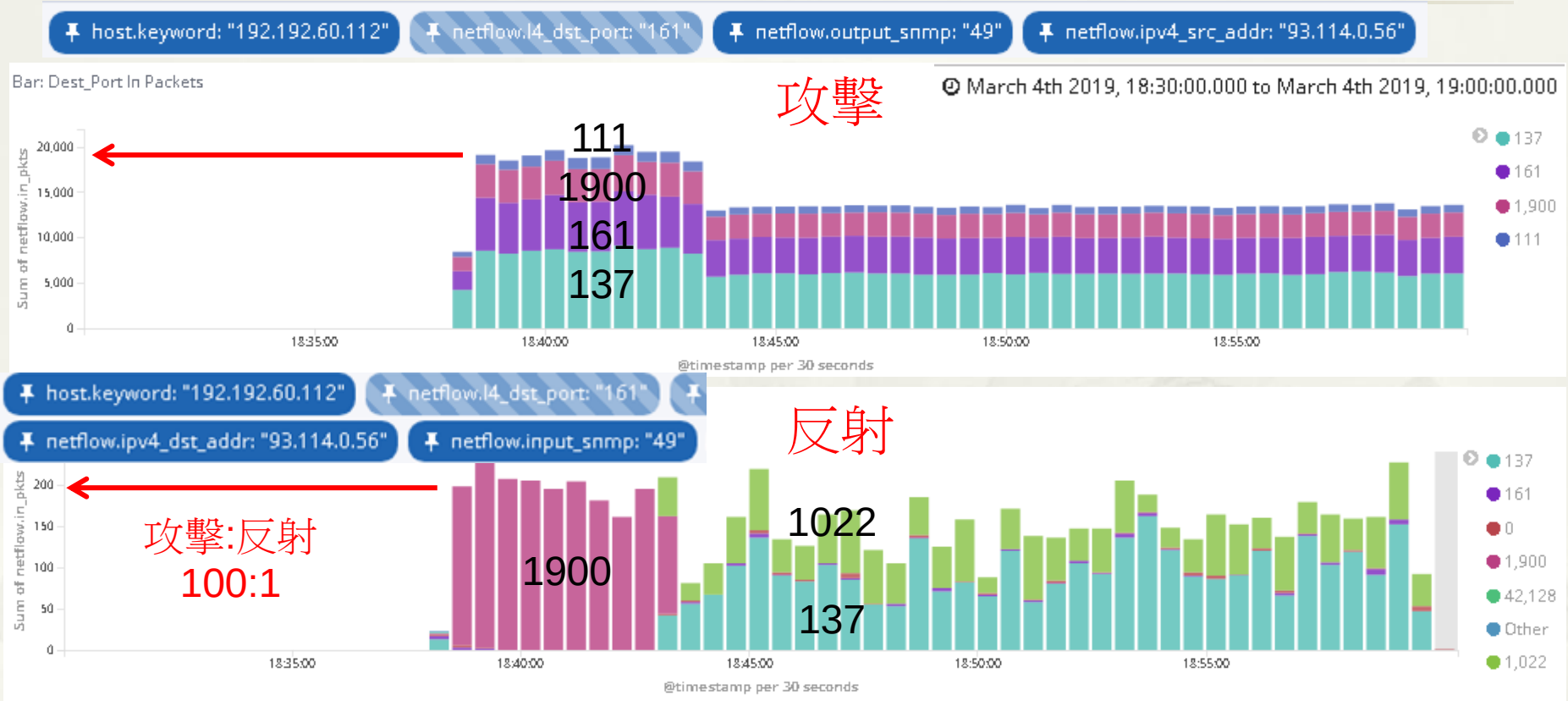
# Case.大同大學20190304
# 外對內 Port



# Case.大同大學20190304
# 外對內 IP



# Case.大同大學20190304
# 93.114.0.56 Port




Port 137: 攻擊後五分鐘，剩下 1/60 (200/12000)
Port 161: 攻擊後五分鐘，剩下 1/1000 (4/4000)
Port 1900: 攻擊後五分鐘，完全消失
Port 111: 完全消失
Port 1022: Port 137 之反射 (140.129.29.195)