

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

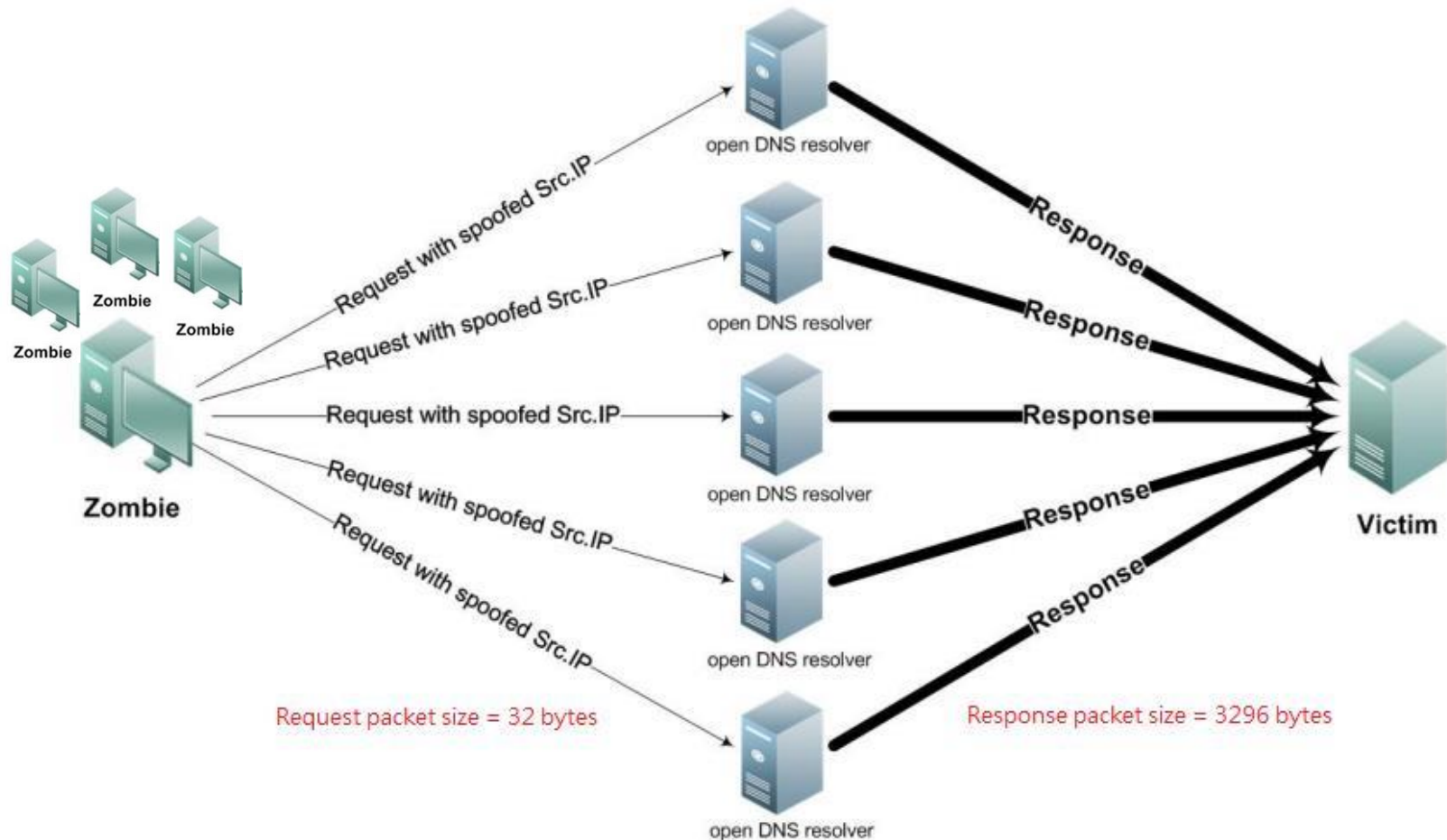
- * 內對外: 內部有 BOT 利用外部反射 Server 攻擊受害者

* 直接攻擊

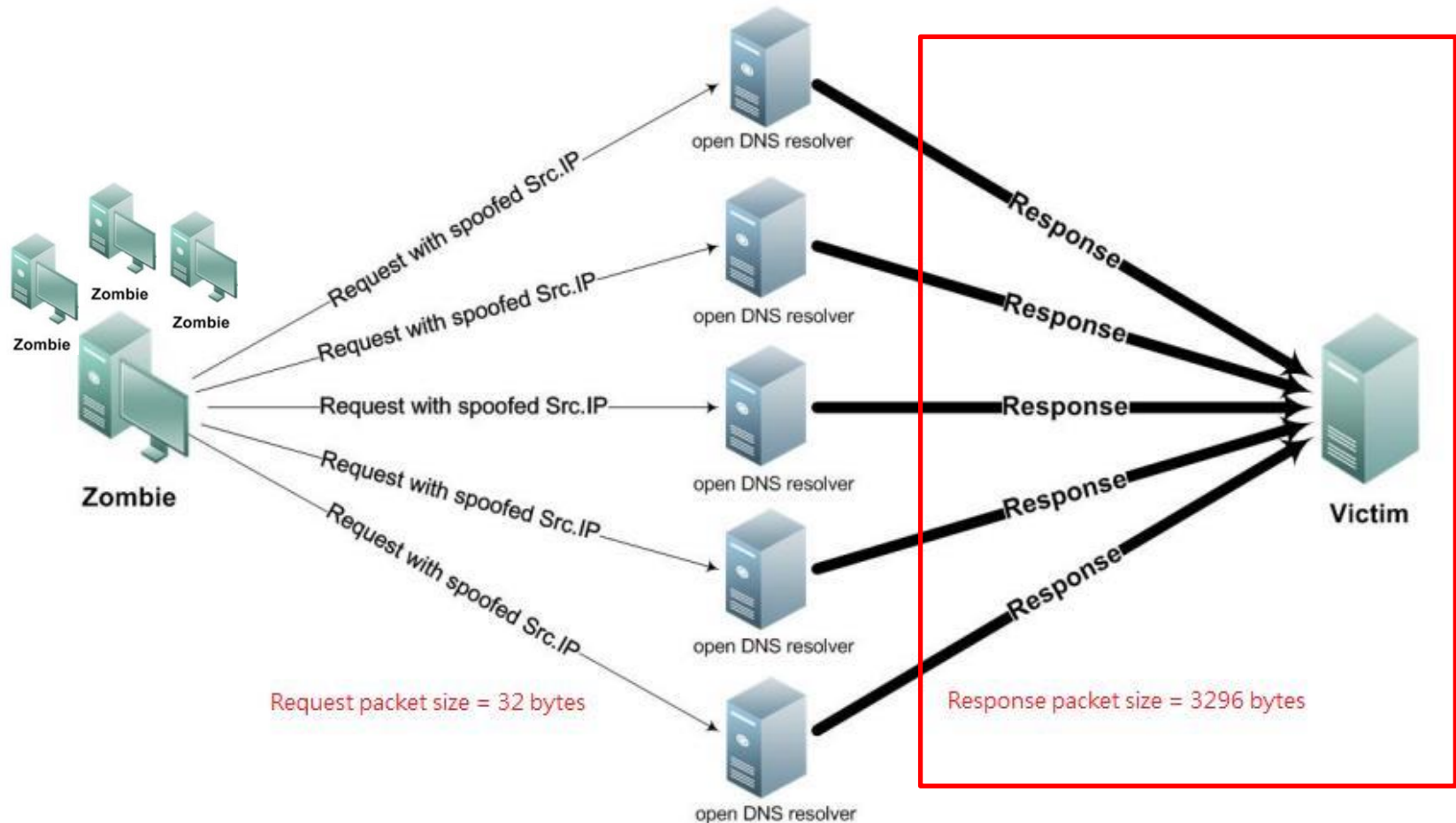
- * 外對內: 遭受攻擊

- * 內對外: 內部有 BOT 攻擊受害者

反射攻擊架構圖

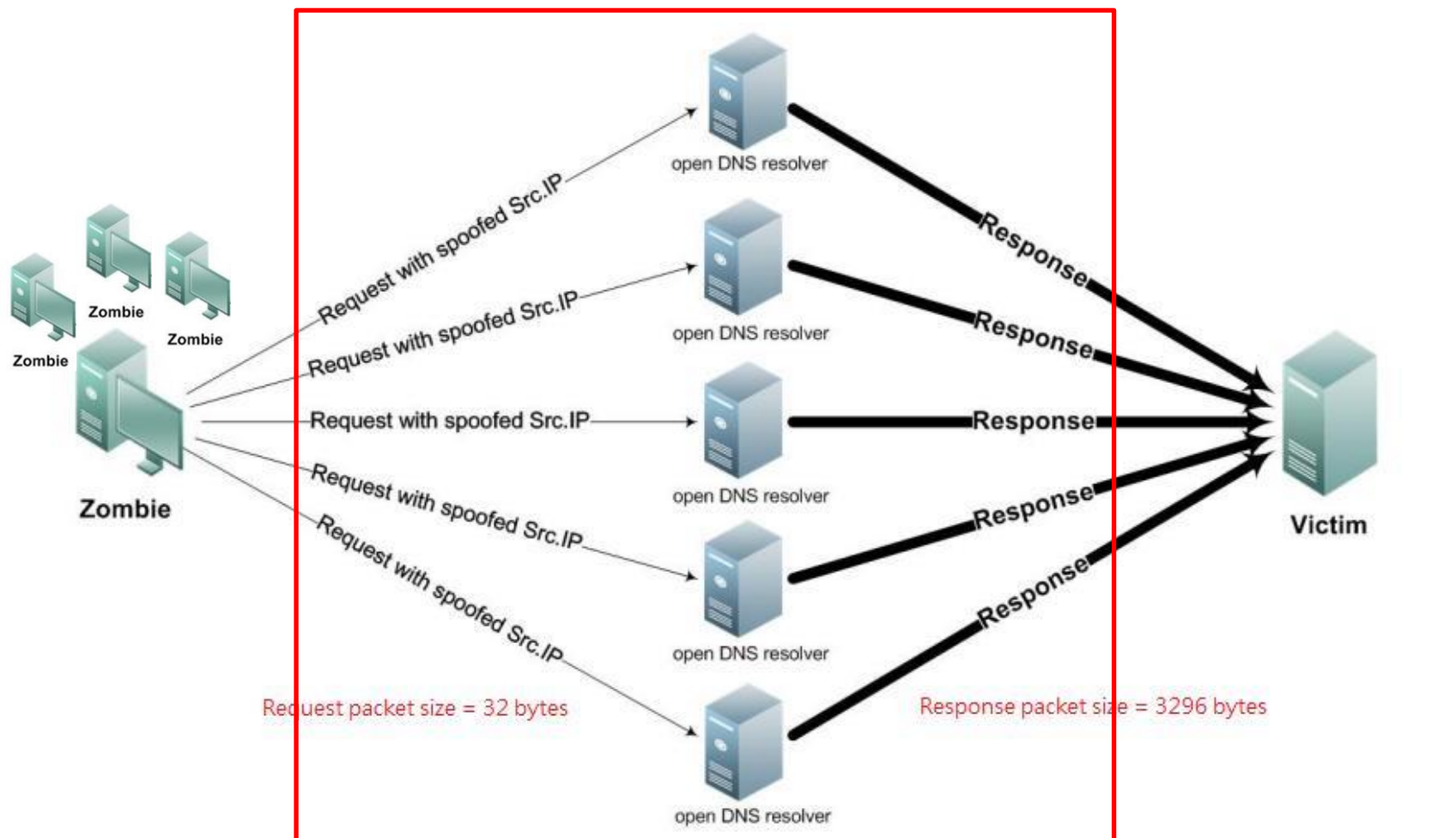


外對內: 遭受反射攻擊

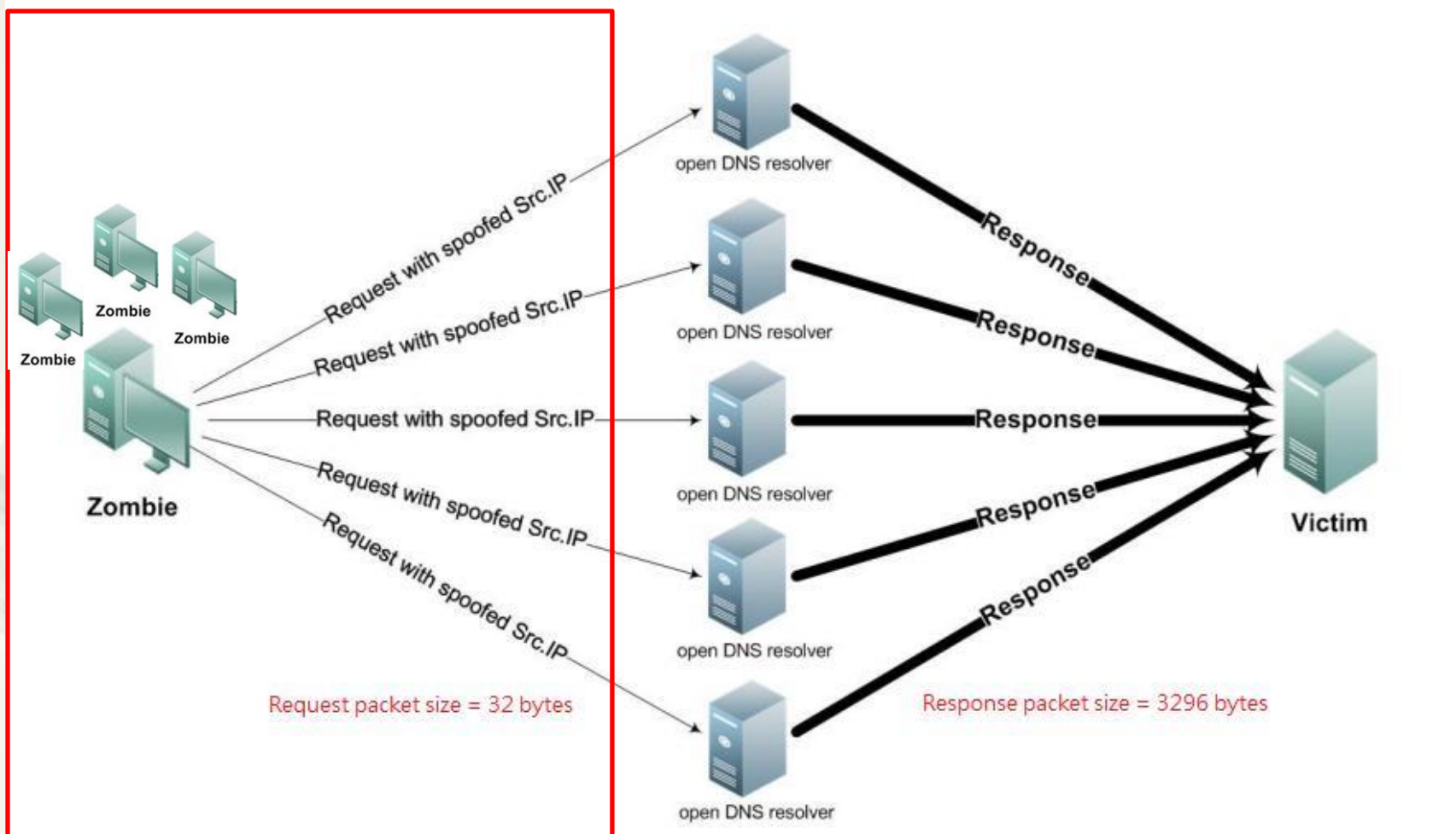


外對內 + 內對外

內部有反射 **Server** 被利用於攻擊受害者



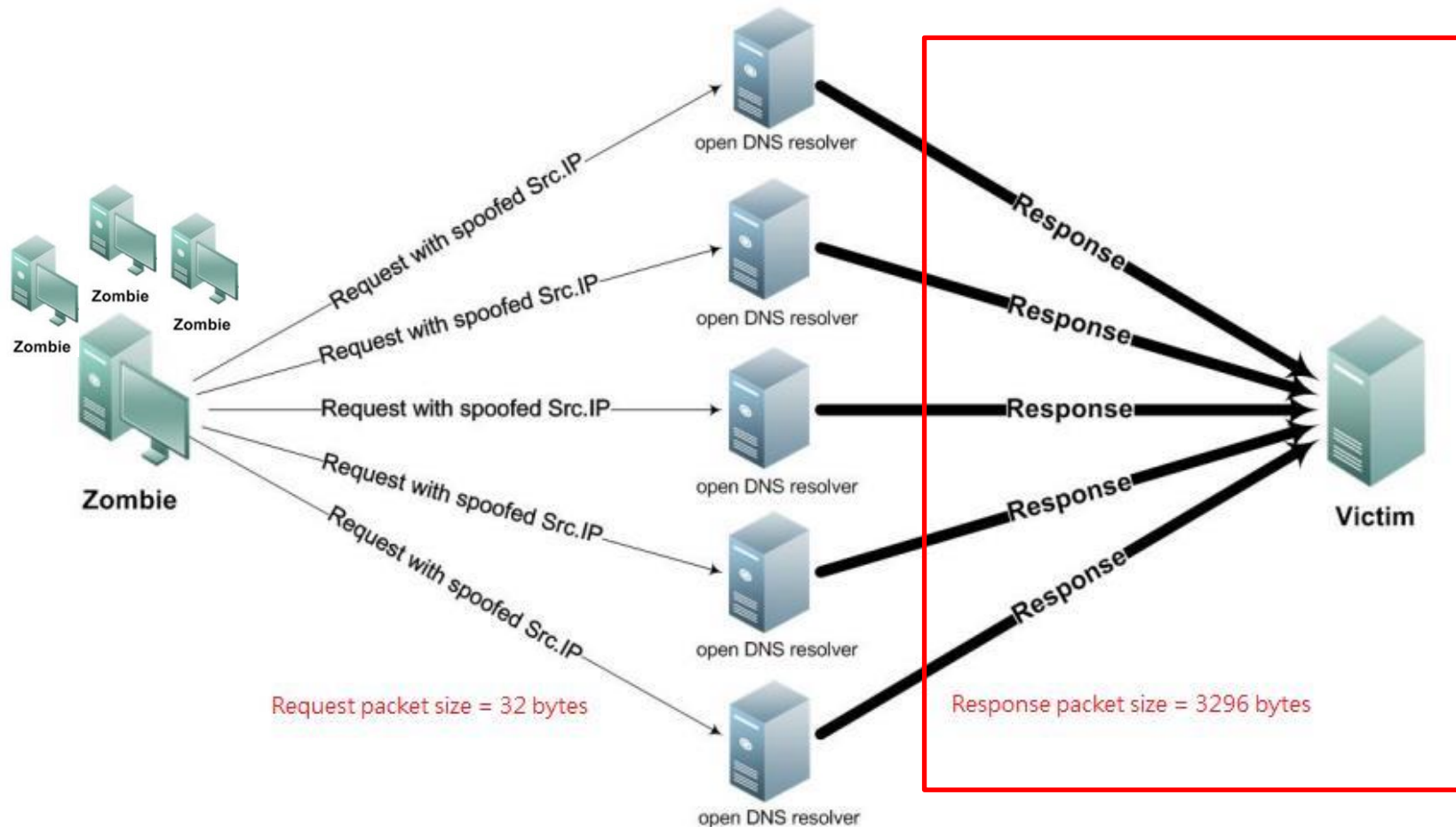
內對外: 內部有 **BOT** 利用外部反射 **Server** 攻擊受害者



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

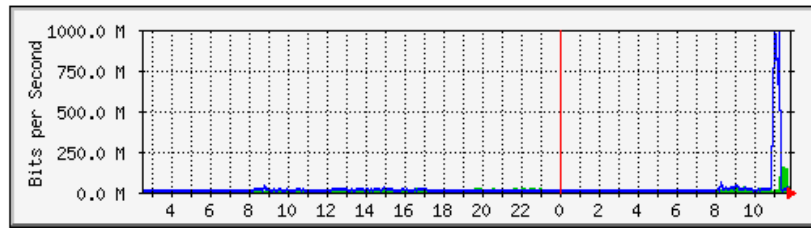
外對內: 遭受反射攻擊



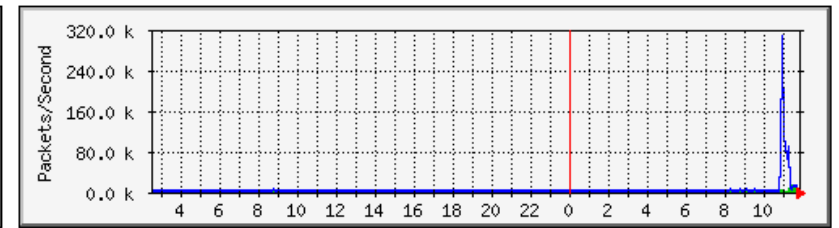
外對內: 遭受DNS反射攻擊 大考中心 20190124 考場公佈

* Bits Per Second & Pkts Per Second: 高

大學入學考試中心 流量(bit/sec)



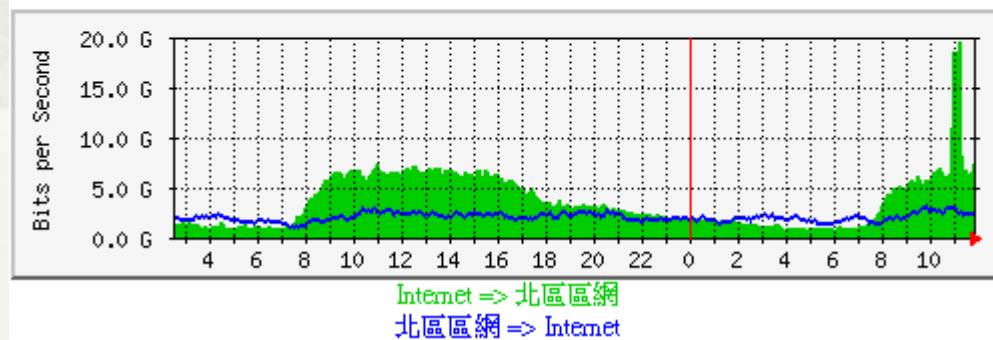
大學入學考試中心 封包(packet/sec)



* 區網骨幹

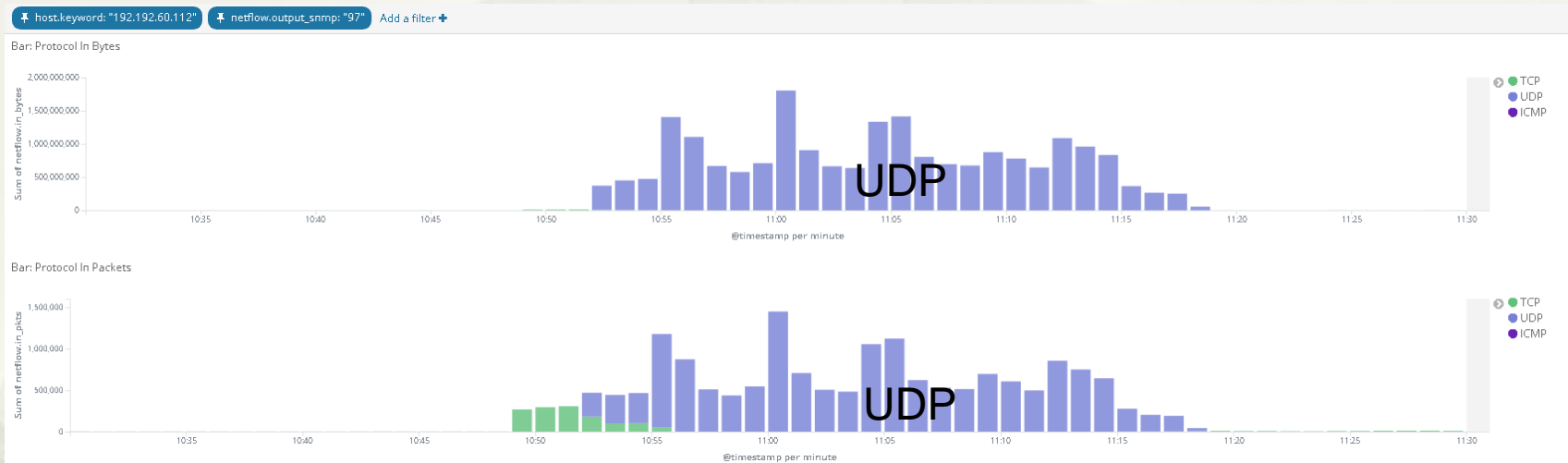
TPRC 北區區網 MRTG

北區區網總流量分析 流量分析 封包數分析



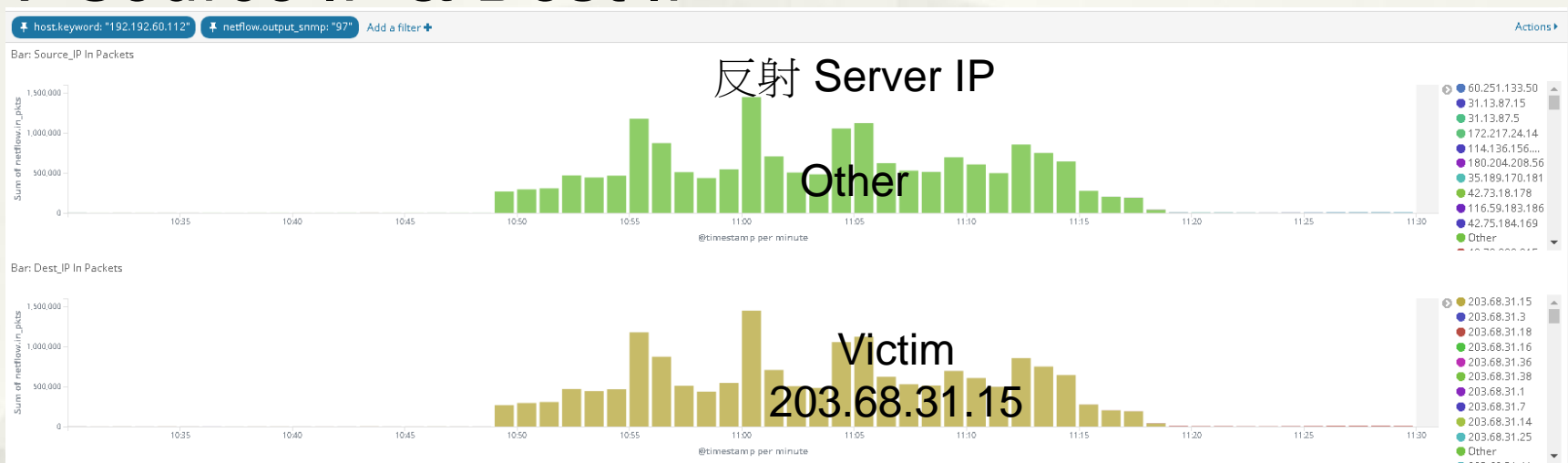
外對內: 遭受DNS反射攻擊

* Protocol: UDP

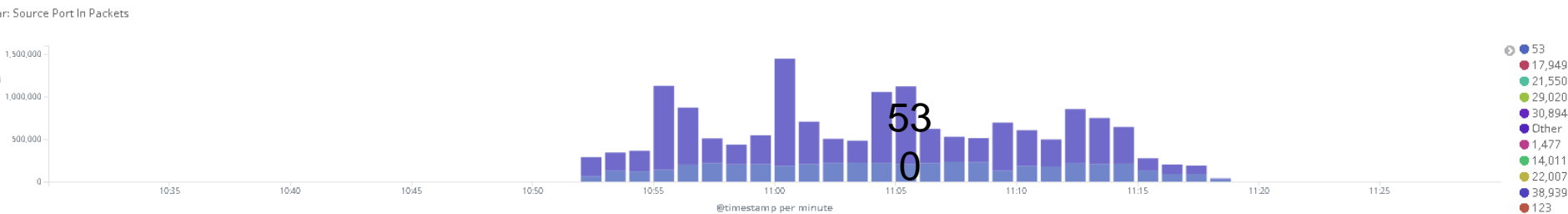


外對內: 遭受DNS反射攻擊

* Source IP & Dest IP

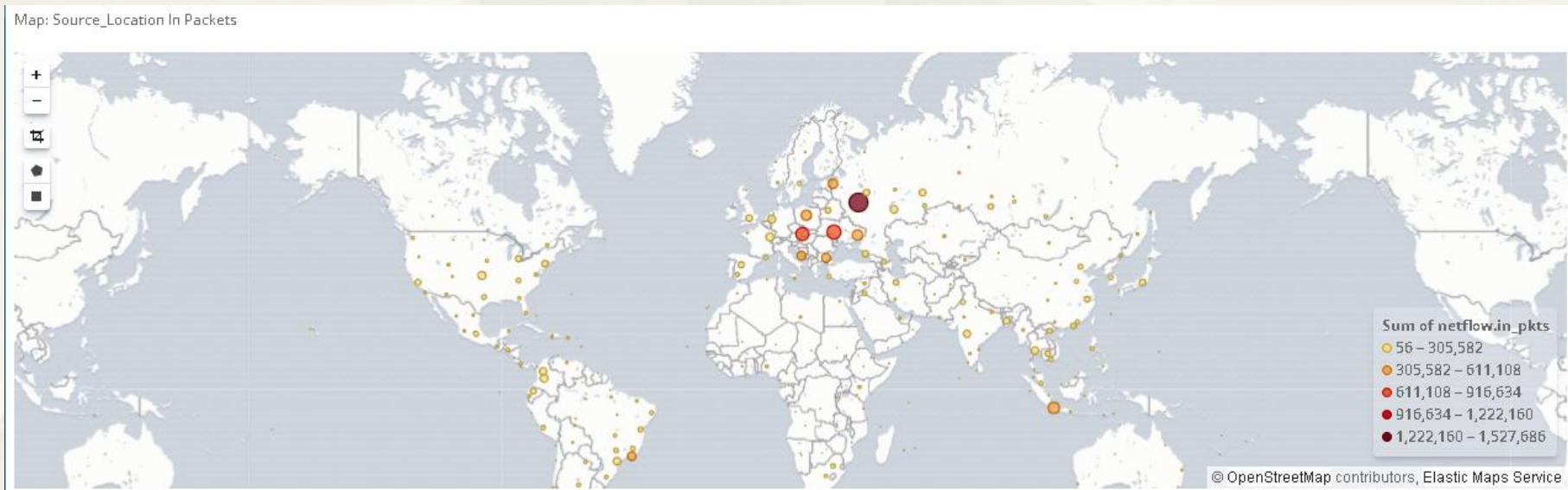


* Source Port

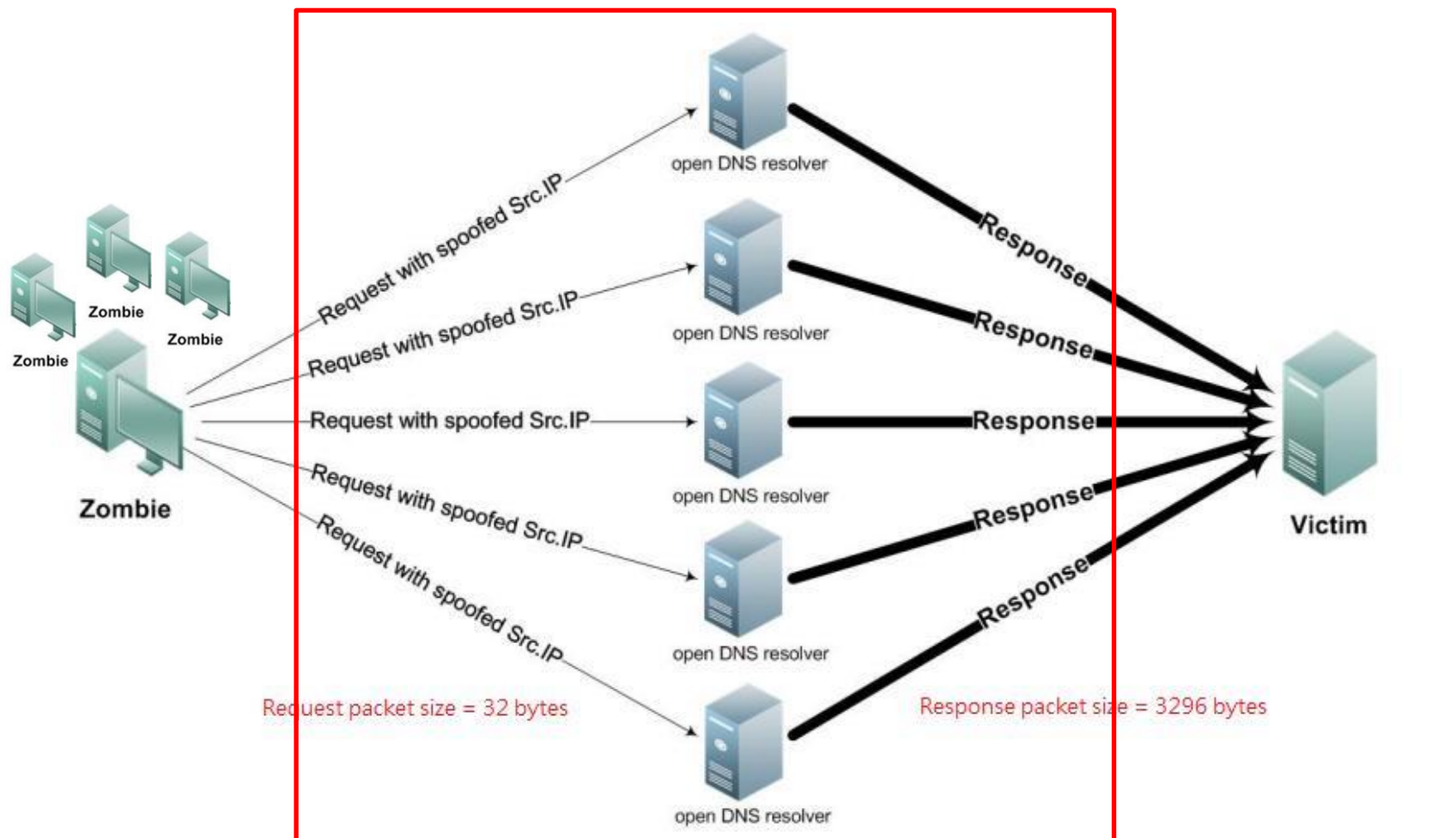


外對內: 遭受DNS反射攻擊

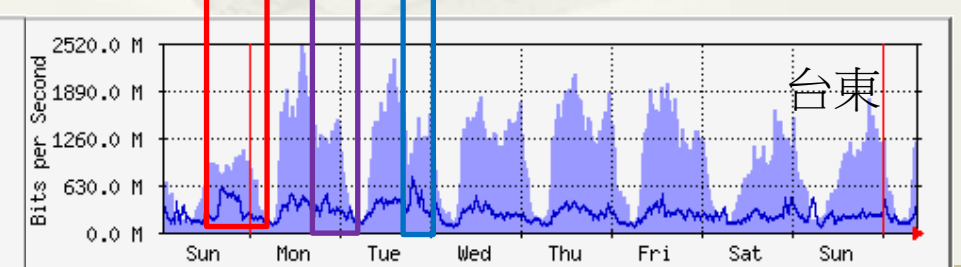
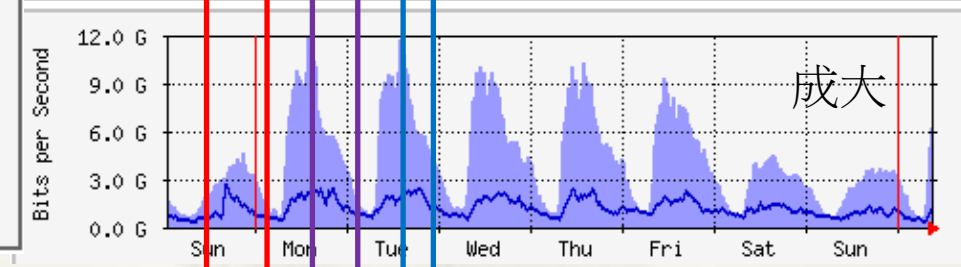
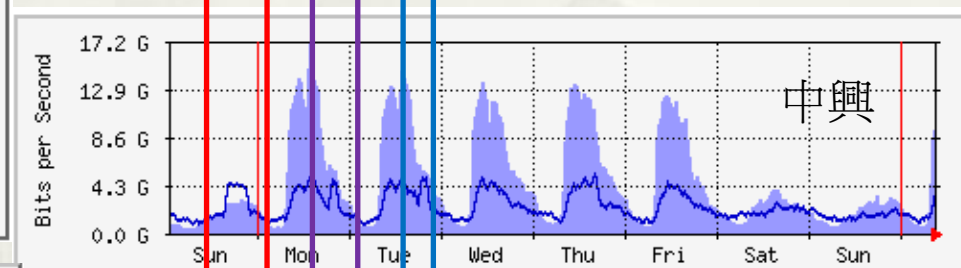
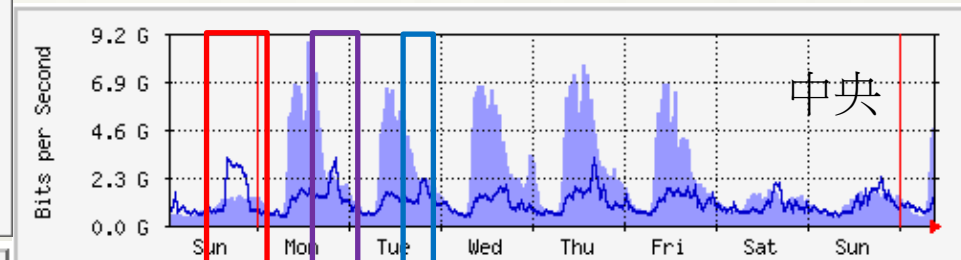
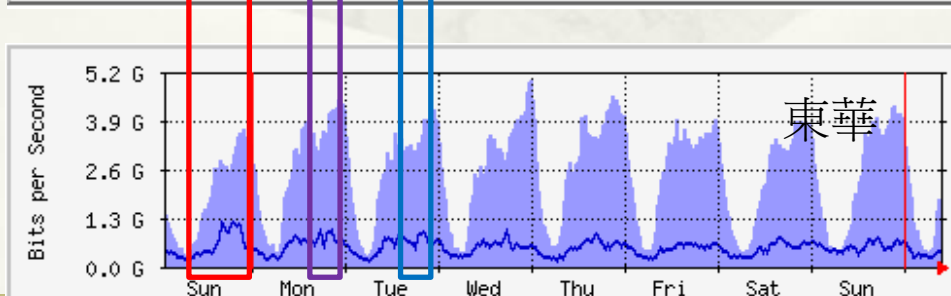
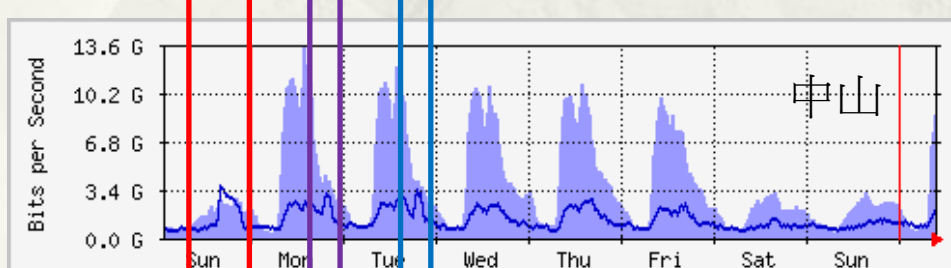
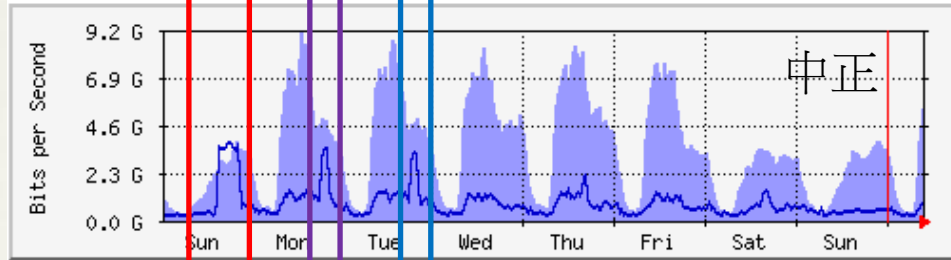
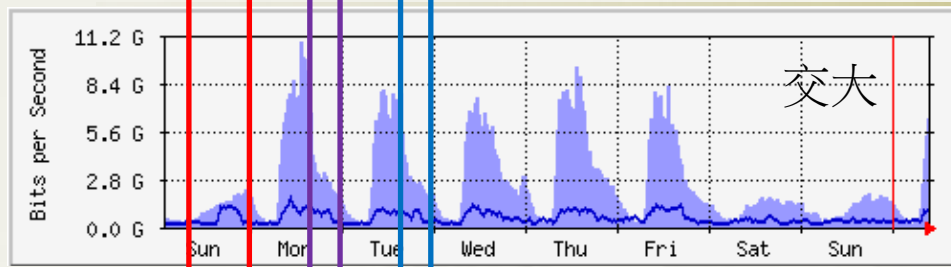
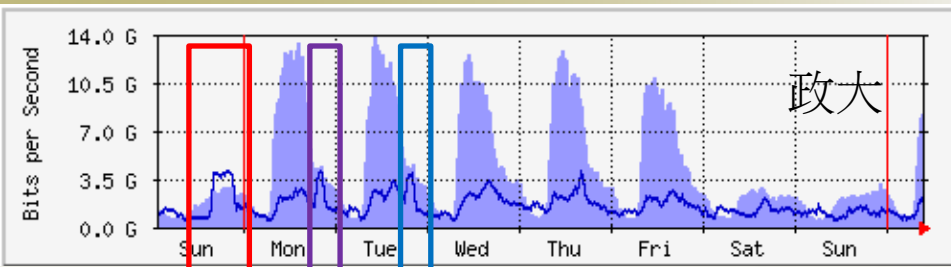
* 攻擊來源



外對內 + 內對外 內部有反射 **Server** 被利用於攻擊受害者



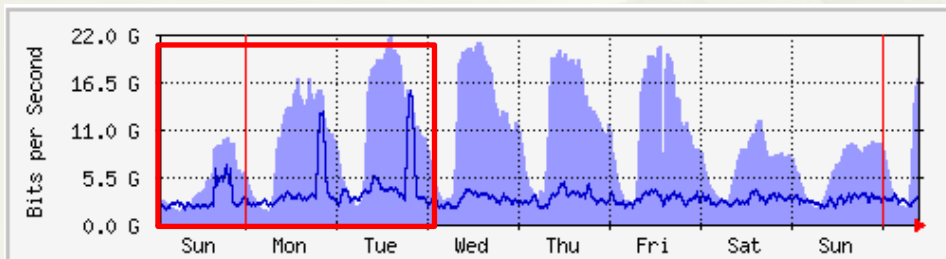
20190303~0305 各區網中心



TANet DDoS 攻擊出口

Max 25~30 Gbps

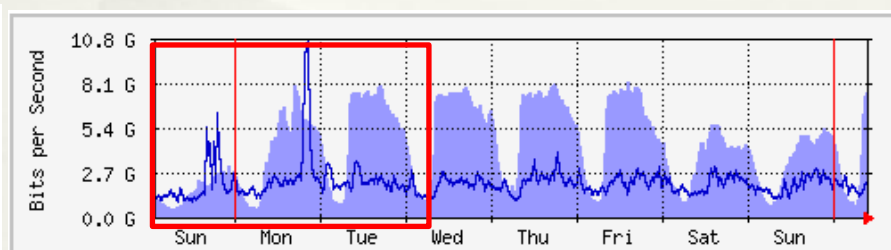
TANet to Internet IPv4 [30G]



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%) |

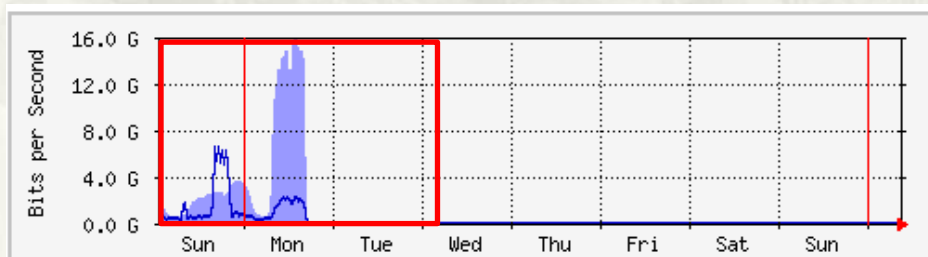
CHIEF Transit Service



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



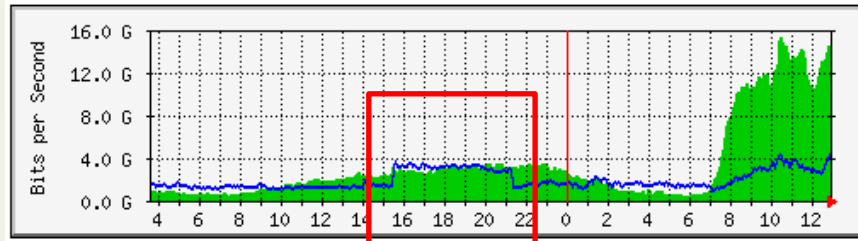
最大 平均 目前

| | | | |
|------------|---------------------|---------------------|----------------|
| 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%) |

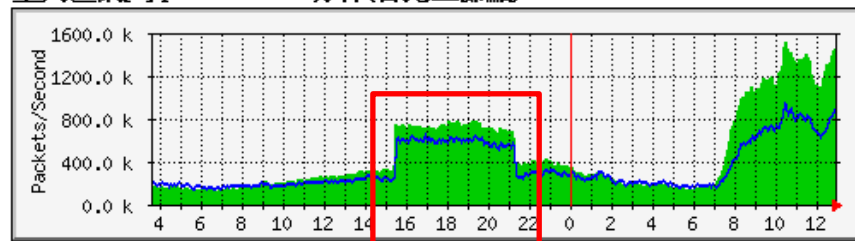
偵測方法 - MRTG

臺大區網骨幹

臺大區網11ipv4 - TANet骨幹(台北主節點)



臺大區網11ipv4 - TANet骨幹(台北主節點)



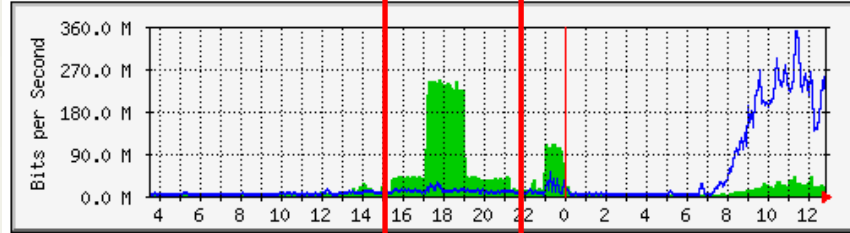
20190303 15:30~21:10

- * 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

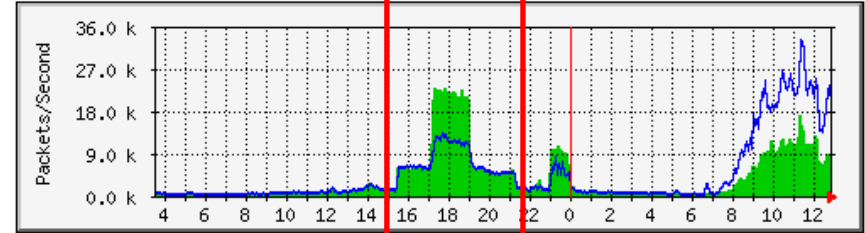
異常連線單位

20190303

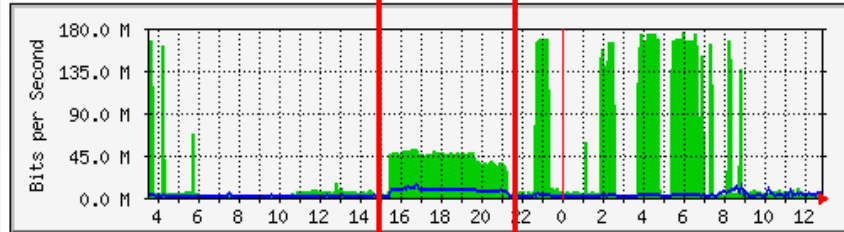
致理科技大學 流量(bit/sec)



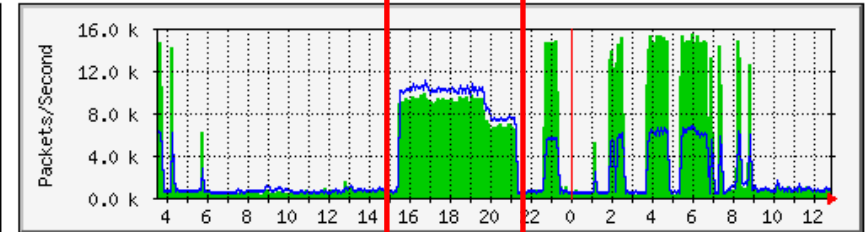
致理科技大學 封包(packet/sec)



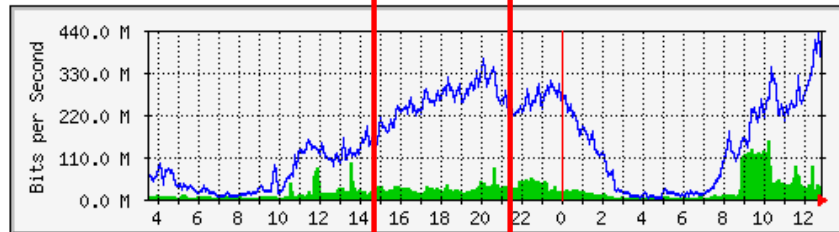
華夏科技大學 流量(bit/sec)



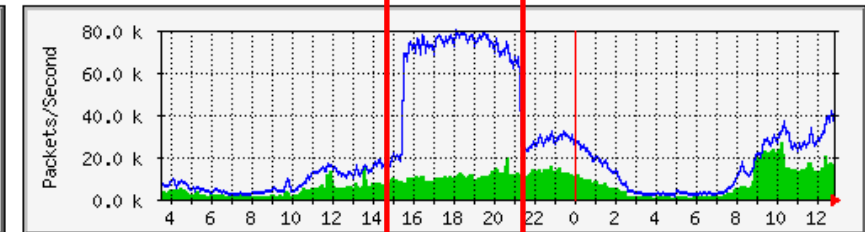
華夏科技大學 封包(packet/sec)



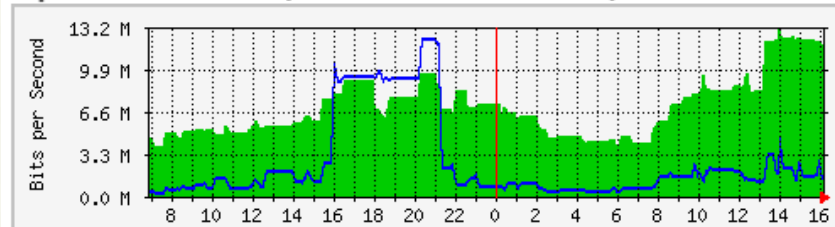
大同大學 流量(bit/sec)



大同大學 封包(packet/sec)



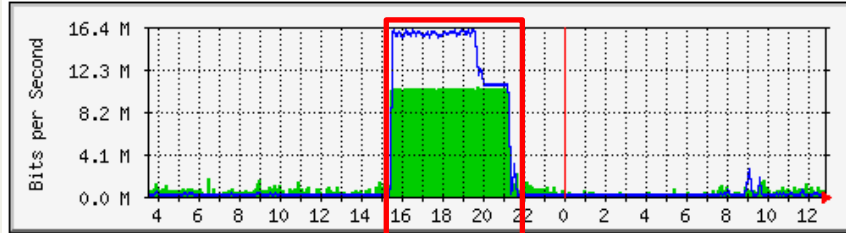
Uplink to 防火牆 (雲端 2960S G1/0/24)



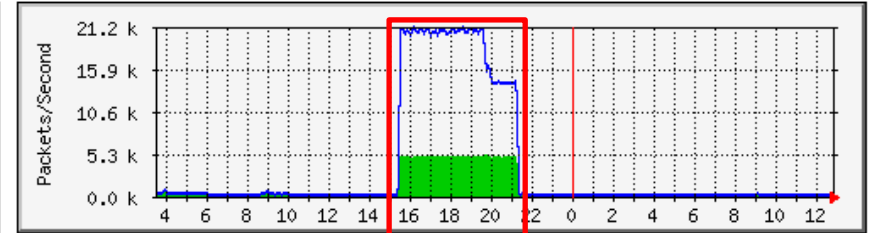
異常連線單位

20190303

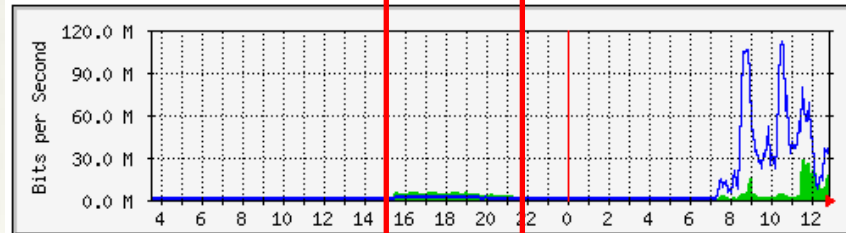
國北教大實小 流量(bit/sec)



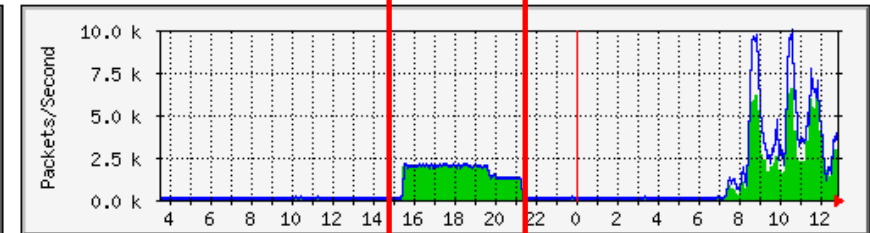
國北教大實小 封包(packet/sec)



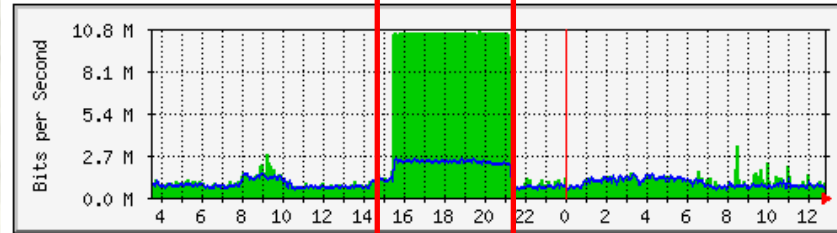
樹人家商 流量(bit/sec)



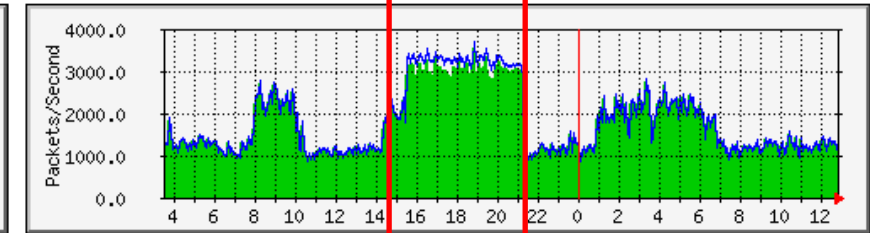
樹人家商 封包(packet/sec)



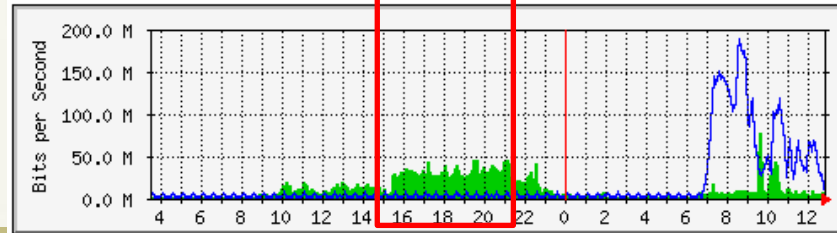
東海高中 流量(bit/sec)



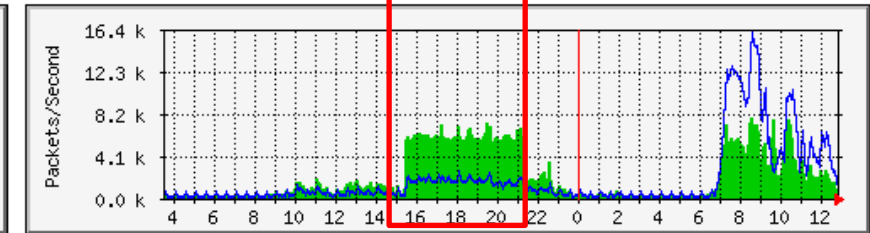
東海高中 封包(packet/sec)



南山高中 流量(bit/sec)



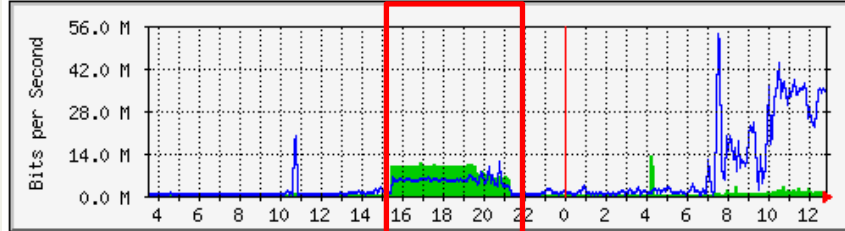
南山高中 封包(packet/sec)



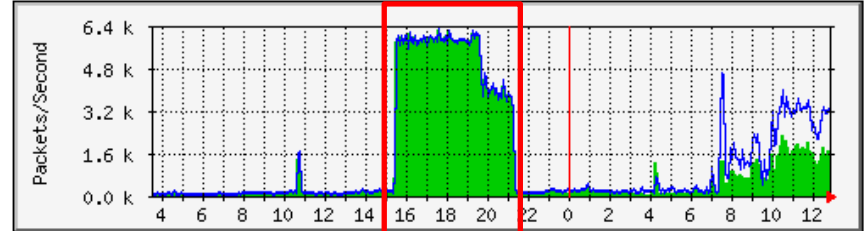
異常連線單位

20190303

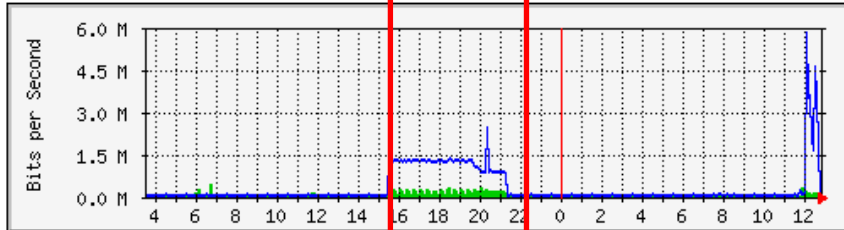
徐匯中學 流量(bit/sec)



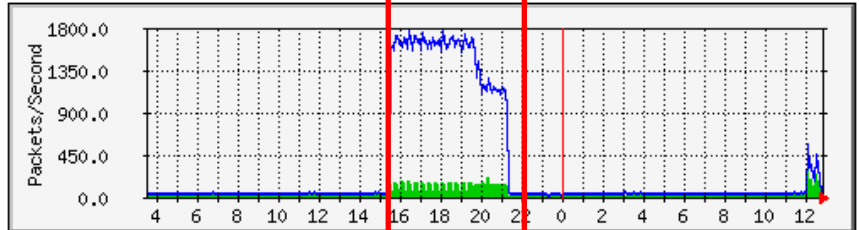
徐匯中學 封包(packet/sec)



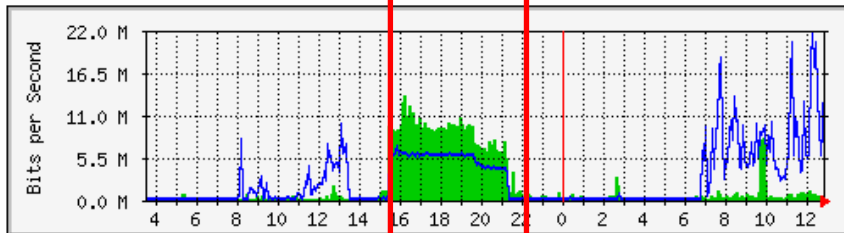
能仁家商 流量(bit/sec)



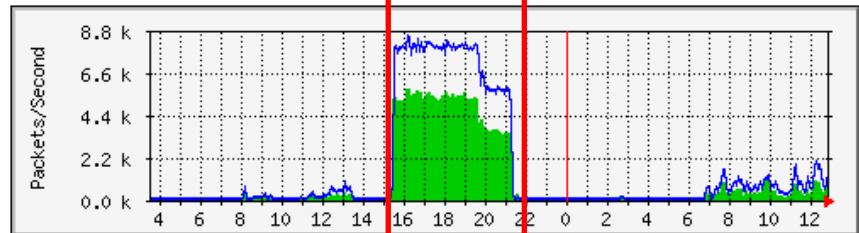
能仁家商 封包(packet/sec)



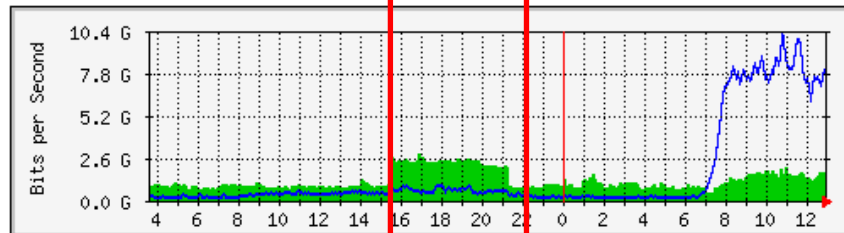
清傳高商 流量(bit/sec)



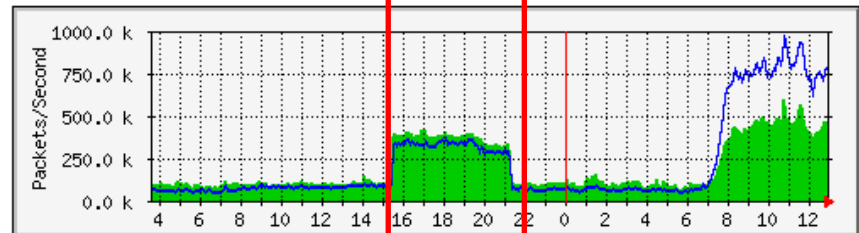
清傳商職 封包(packet/sec)



臺北市教育網路 TP via 亞太 10G ipv4 流量(bit/sec)



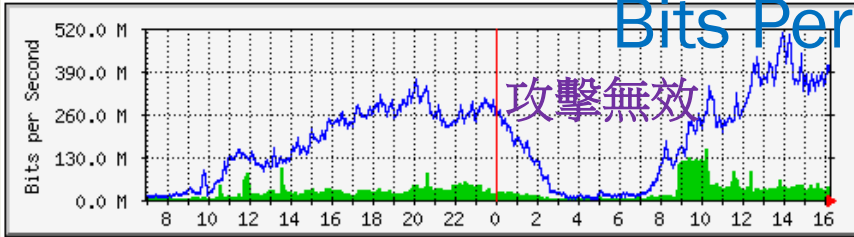
臺北市教育網路 TP via 亞太 10G ipv4 封包(packet/sec)



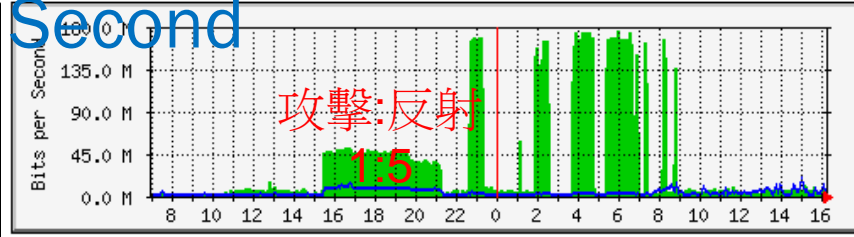
20190303

攻擊:反射 比例分析

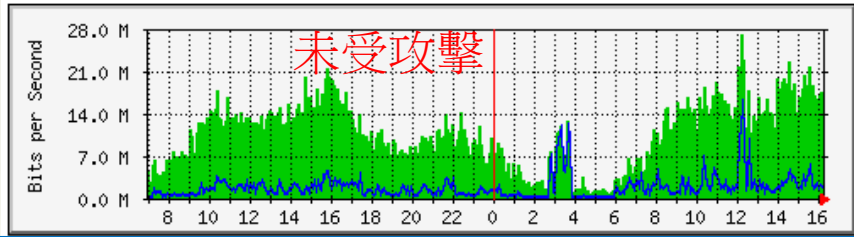
大同大學 流量圖



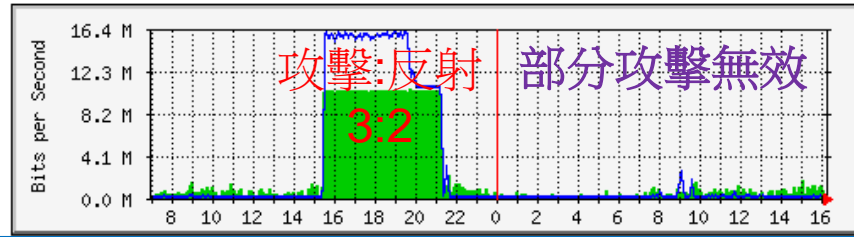
華夏科技大學 流量圖



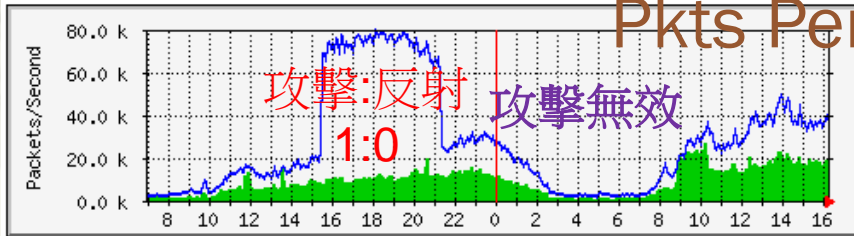
新北市立圖書館 流量圖



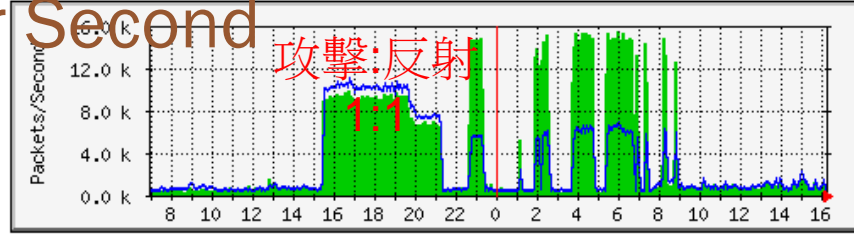
國北教大實小 流量圖



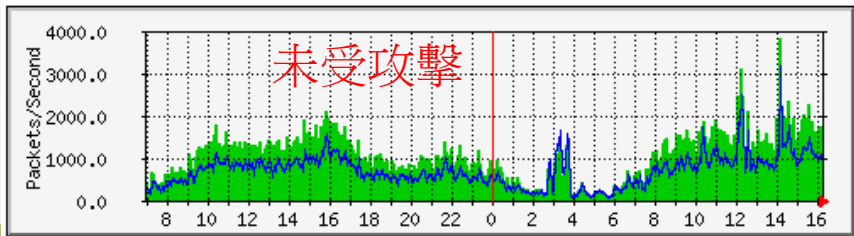
大同大學 封包數



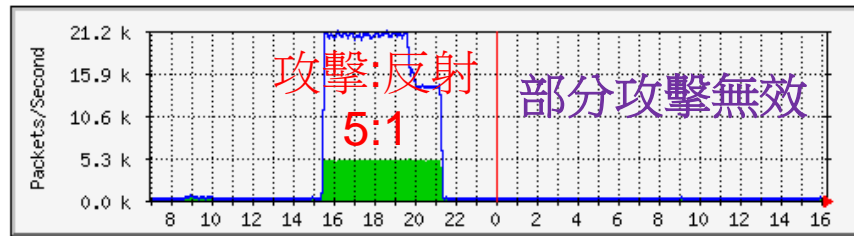
華夏科技大學 封包數



新北市立圖書館 封包數



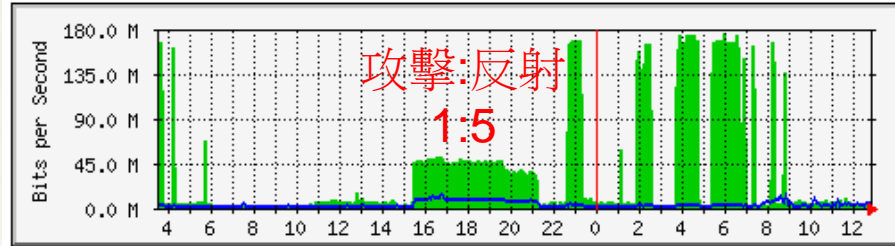
國北教大實小 封包數



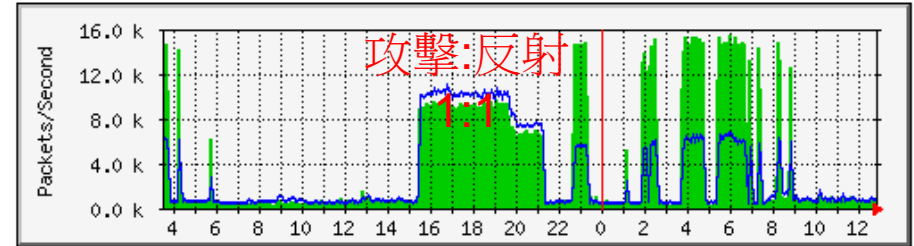
Case. 華夏科大 20190303

MRTG

華夏科技大學 流量(bit/sec)



華夏科技大學 封包(packet/sec)



Case. 華夏科大 20190303

外對內 Protocol

March 3rd 2019, 15:00:00.000 to March 3rd 2019, 16:00:00.000

netflow.input_snmp: "160"

netflow.output_snmp: "160"

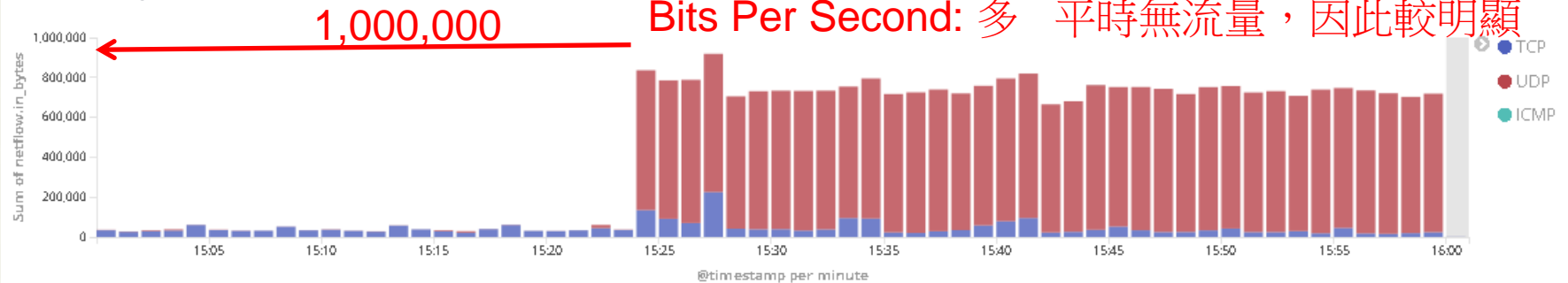
netflow.input_snmp: "257"

netflow.output_snmp: "257"

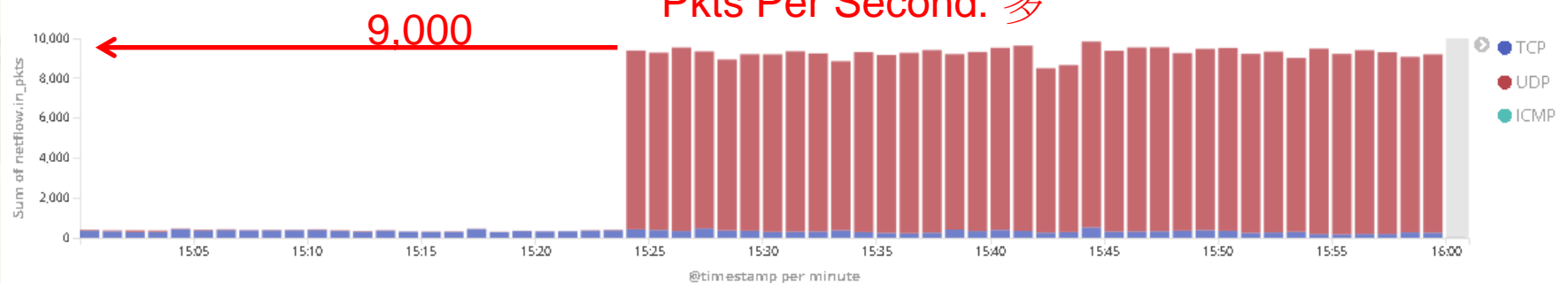
host: "192.192.60.112"

Add a filter +

Bar: Protocol In Bytes



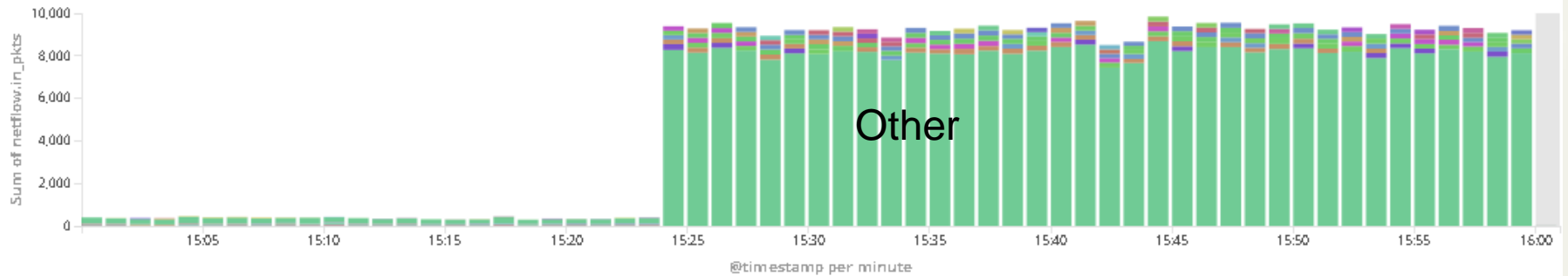
Bar: Protocol In Packets



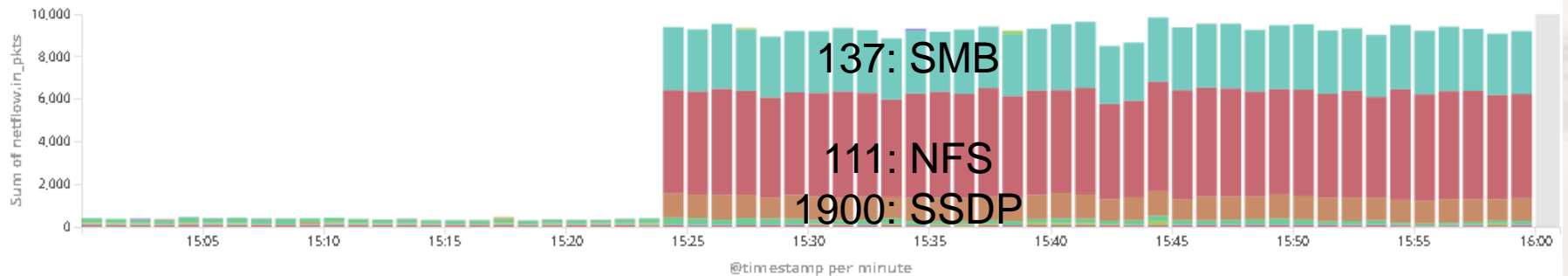
Case. 華夏科大 20190303

外對內 Port

Bar: Source Port In Packets



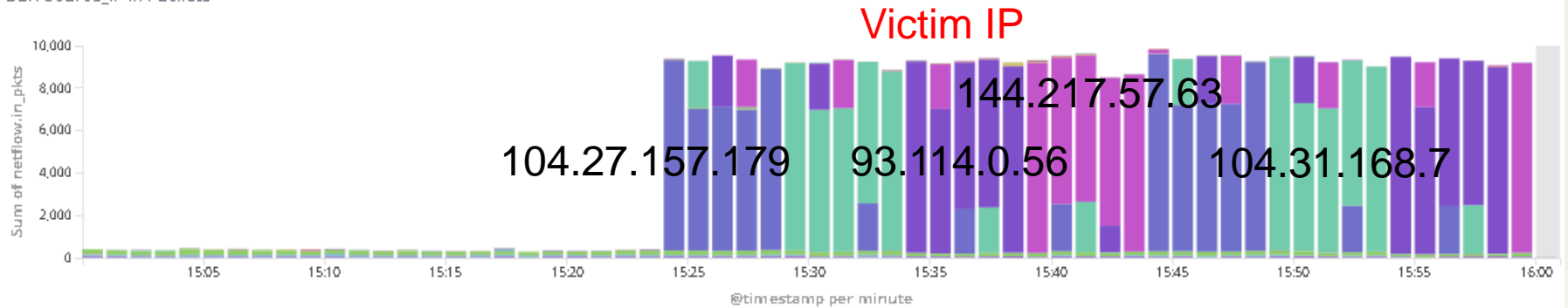
Bar: Dest_Port In Packets



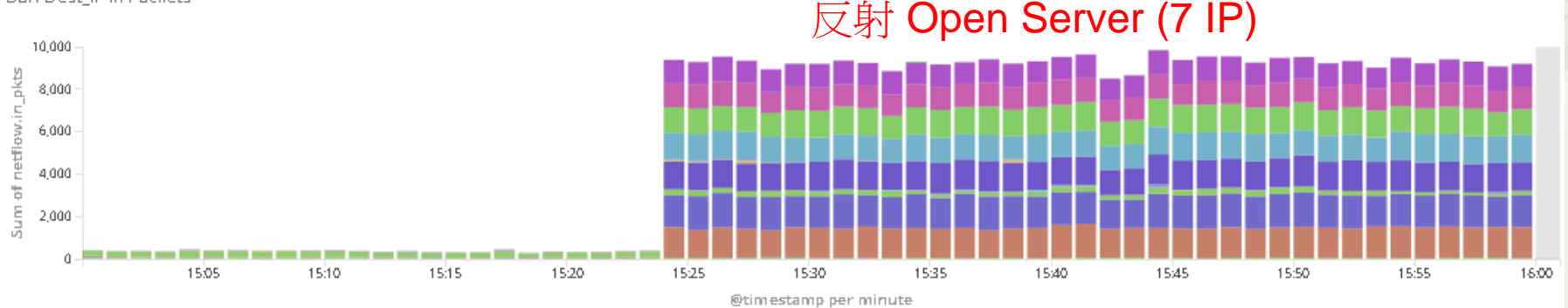
Case. 華夏科大 20190303

外對內 IP

Bar: Source_IP In Packets



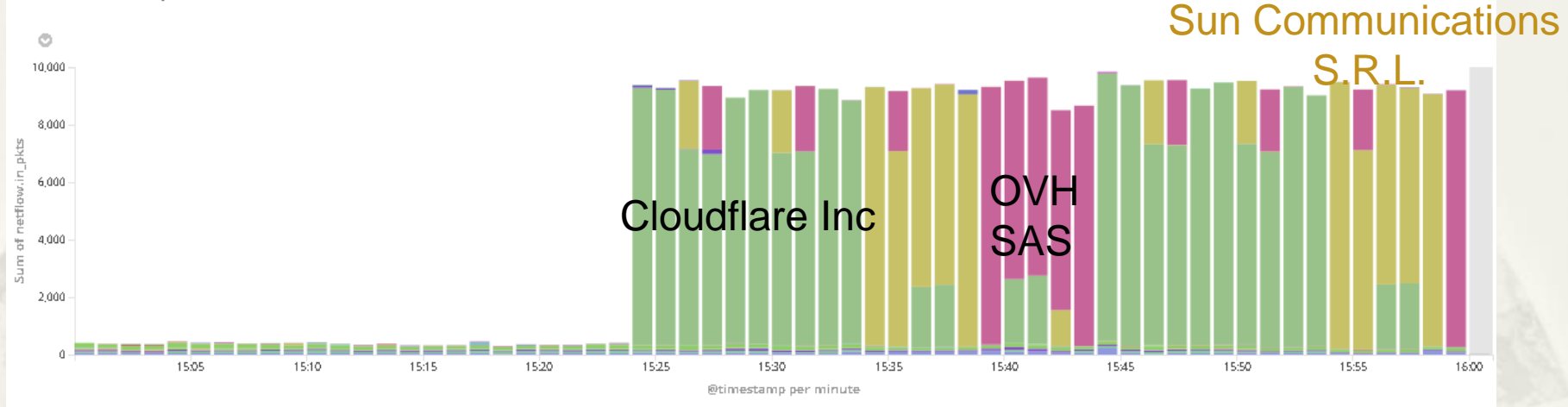
Bar: Dest_IP In Packets



Case. 華夏科大 20190303

外對內 AS

Bar: Source_AS History Packets



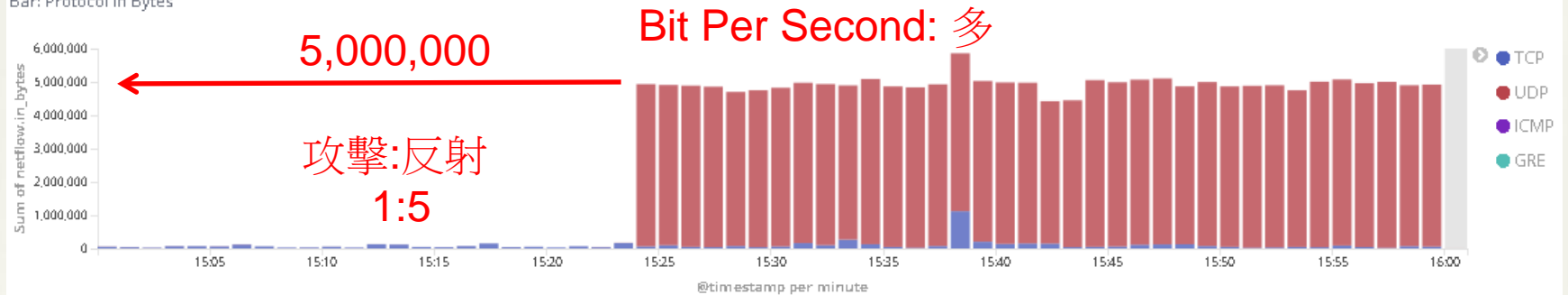
Case. 華夏科大 20190303

內對外 Protocol

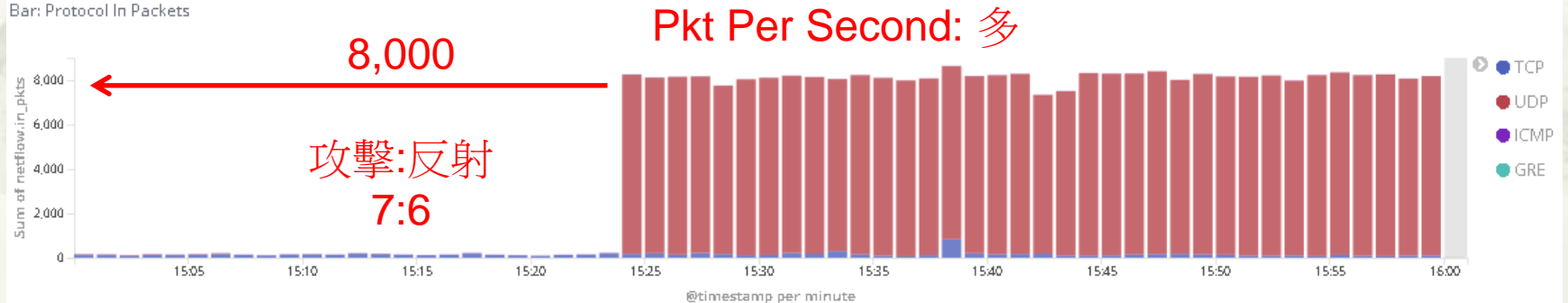
March 3rd 2019, 15:00:00.000 to March 3rd 2019, 16:00:00.000

netflow.input_snmp: "160" netflow.output_snmp: "160" netflow.input_snmp: "257" netflow.output_snmp: "257" host: "192.192.60.112" Add a filter +

Bar: Protocol In Bytes



Bar: Protocol In Packets

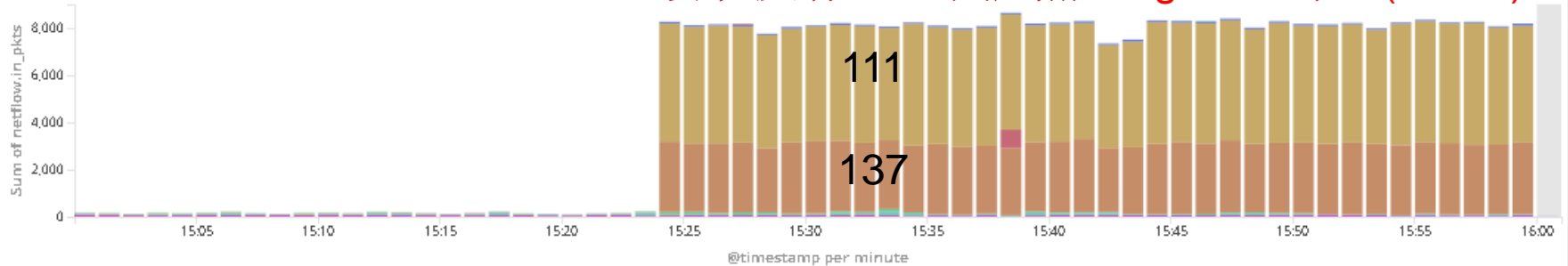


Case. 華夏科大 20190303

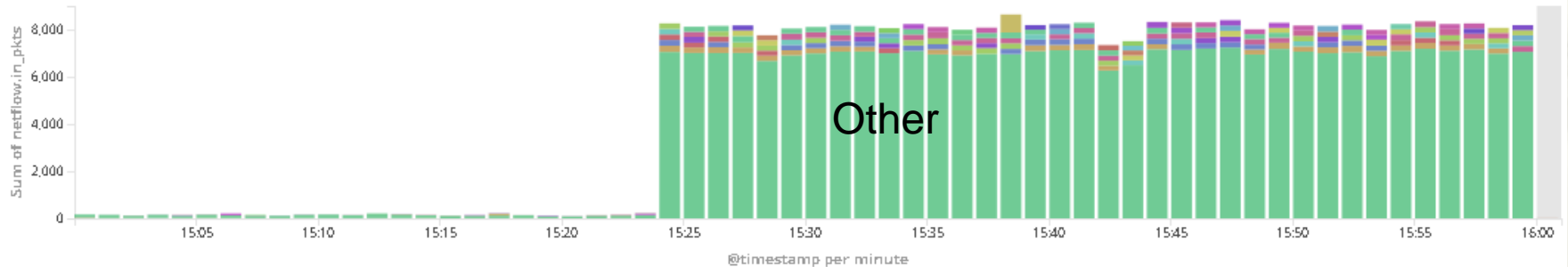
內對外 Port

Bar: Source Port In Packets

攻擊:反射=1:1 因此無 Fragment 封包 (Port:0)



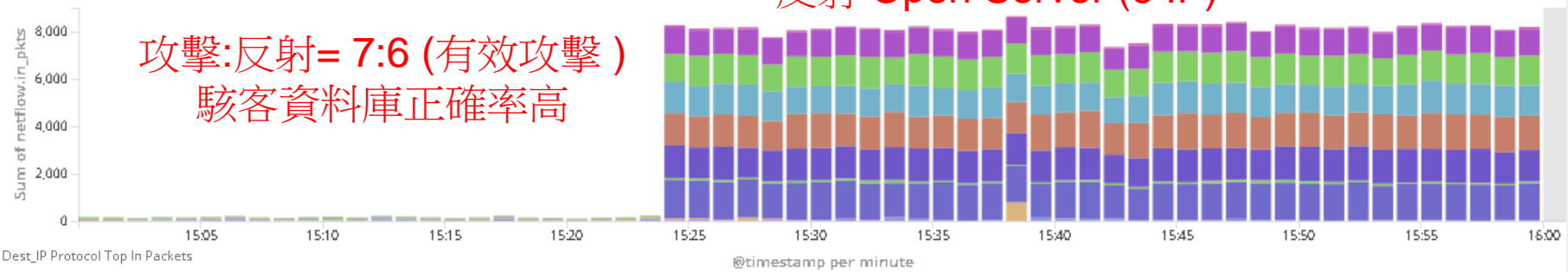
Bar: Dest_Port In Packets



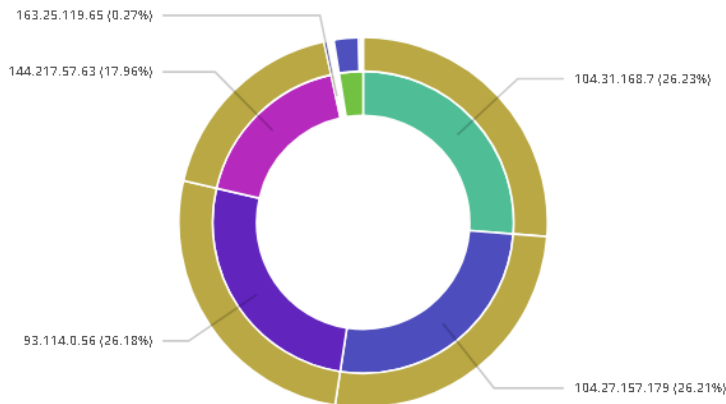
Case. 華夏科大 20190303

內對外 IP

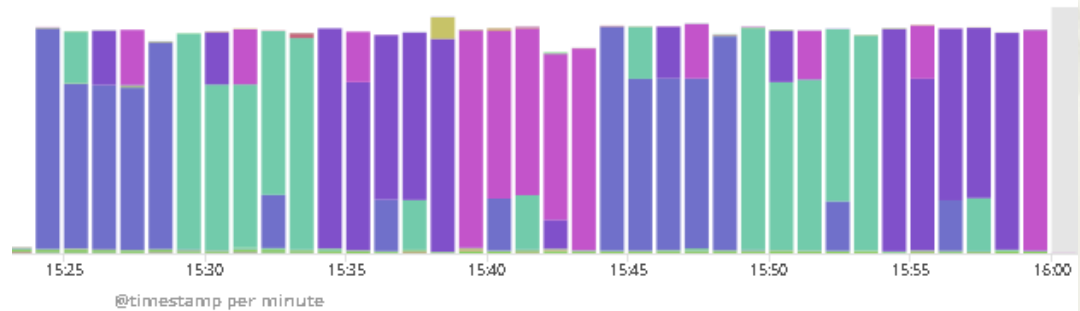
Bar: Source_IP In Packets



Pie: Dest_IP Protocol Top In Packets



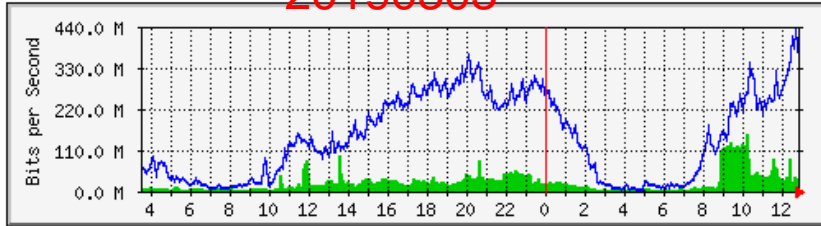
Victim IP



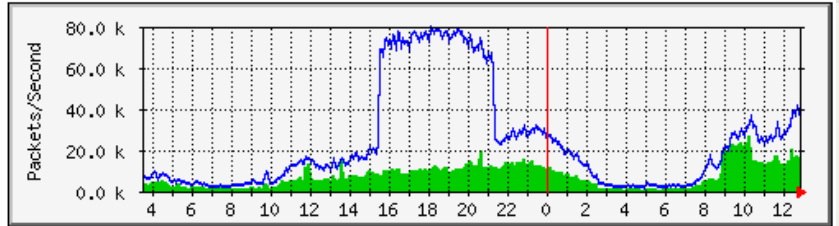
Case.大同大學 (無效反射)

MRTG

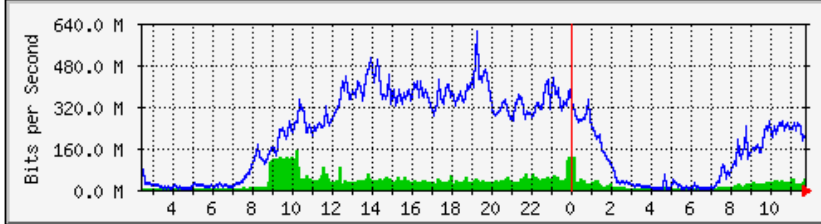
大同大學 流量(bit/sec) 20190303



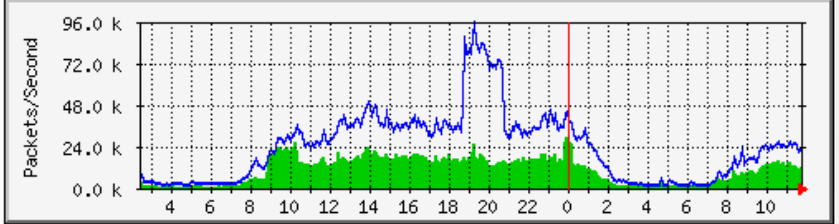
大同大學 封包(packet/sec)



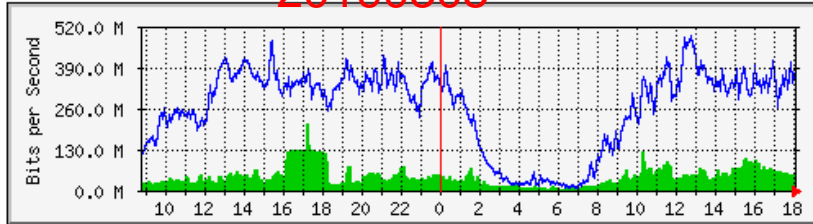
大同大學 流量圖 20190304



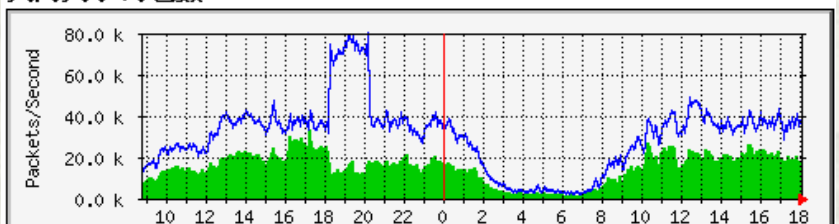
大同大學 封包數



大同大學 流量圖 20190305



大同大學 封包數



- * 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)

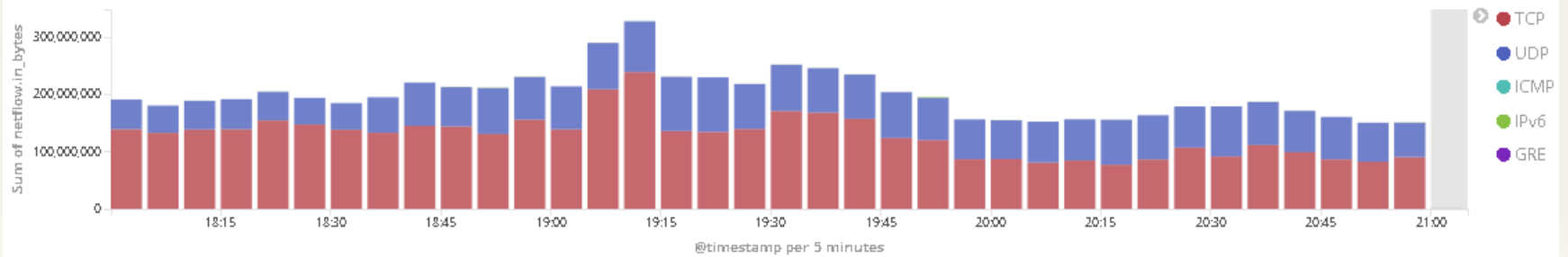
Case.大同大學20190304

外對內 Protocol

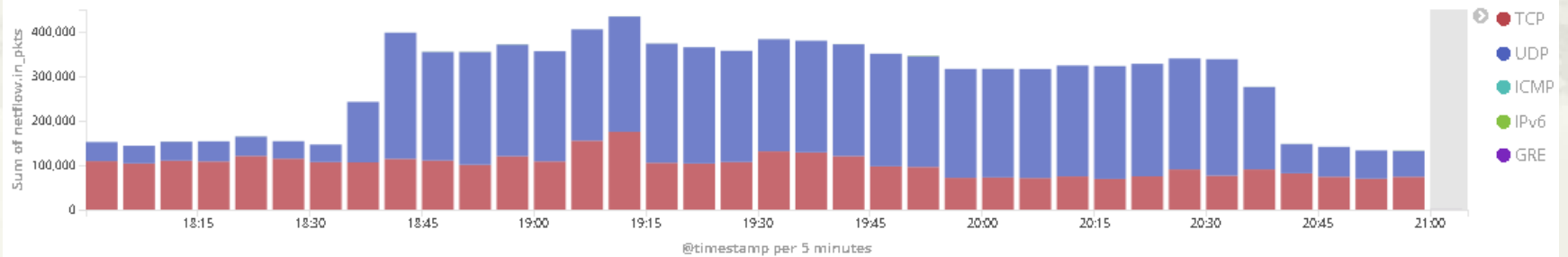
© March 4th 2019, 18:00:00.000 to March 4th 2019, 21:00:00.000

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

Bar: Protocol In Bytes



Bar: Protocol In Packets

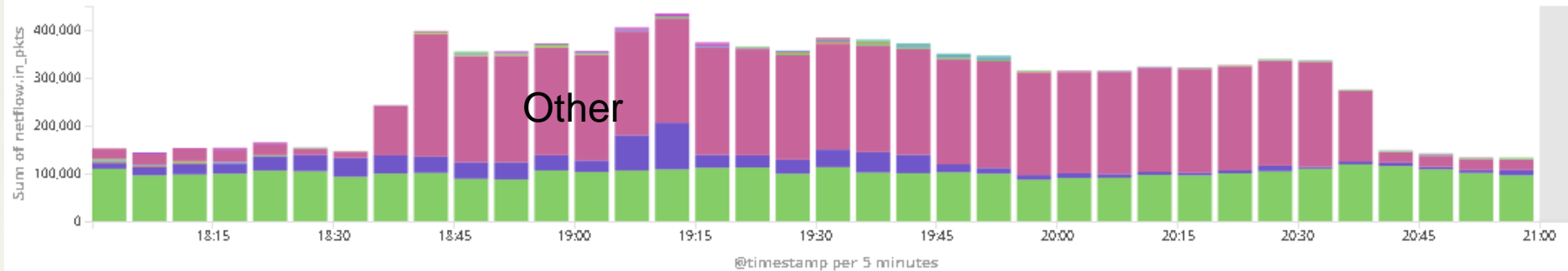


Case.大同大學20190304

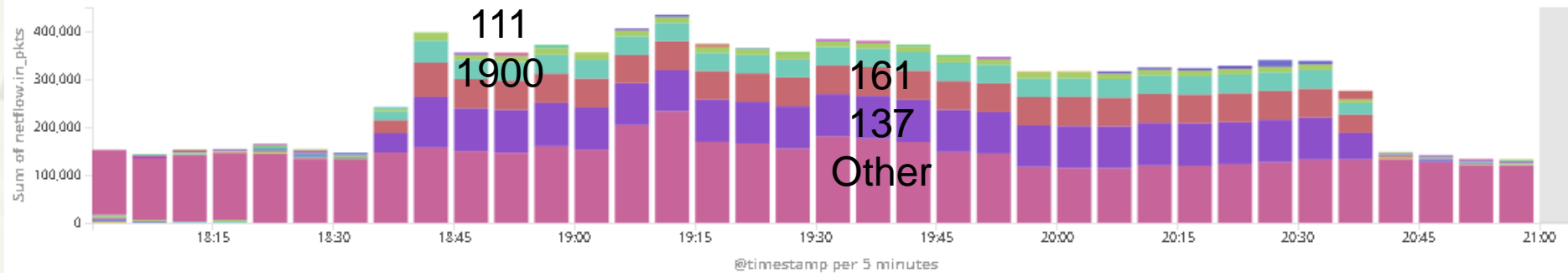
外對內 Port

Bar: Source Port In Packets

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

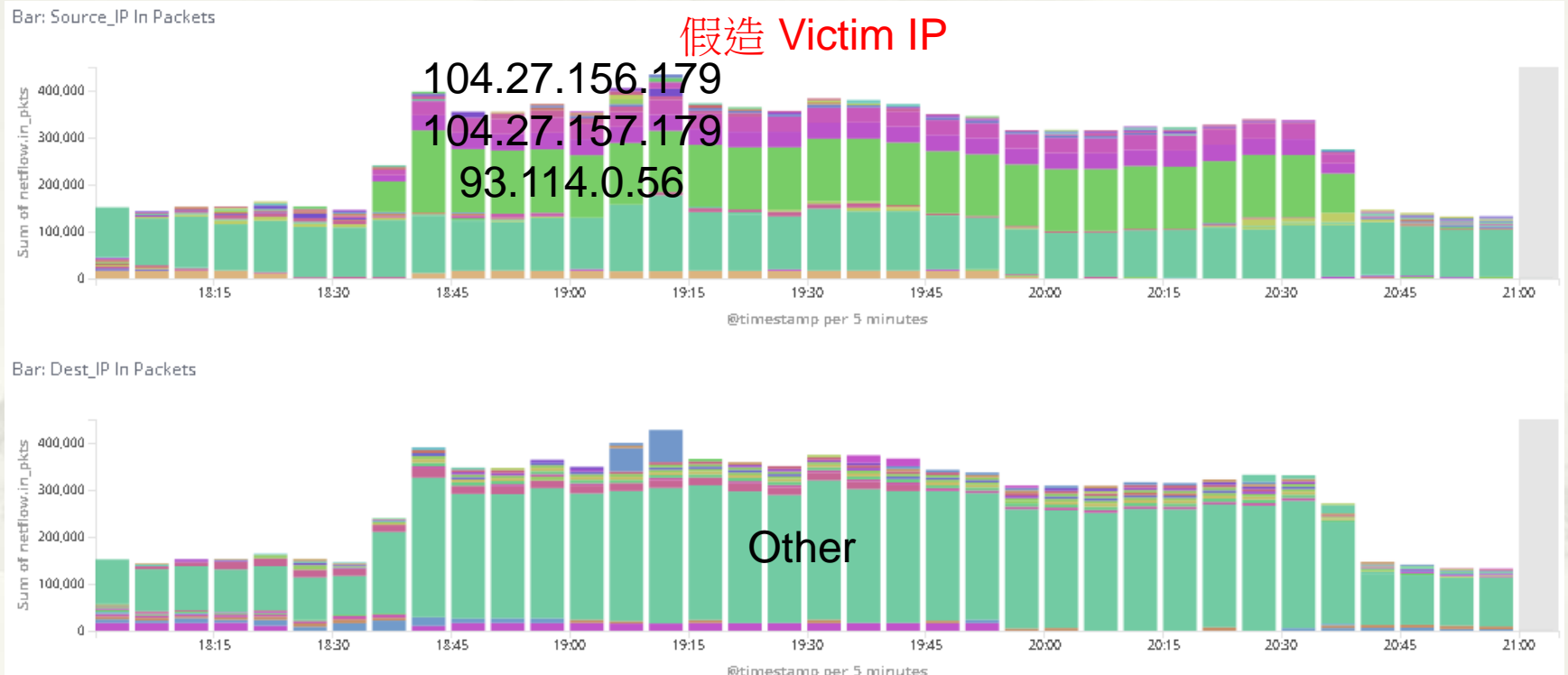


Bar: Dest_Port In Packets



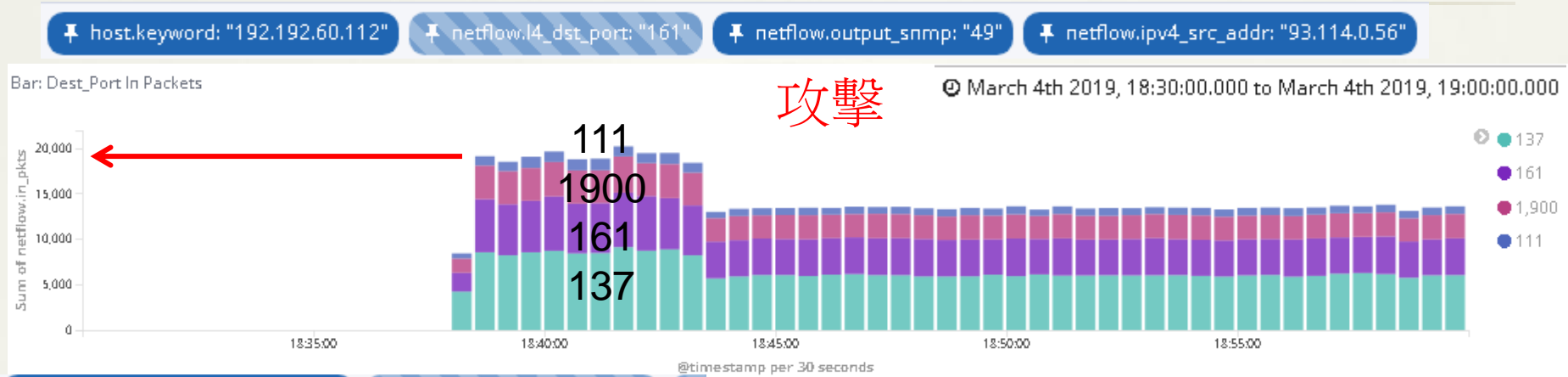
Case.大同大學20190304

外對內 IP

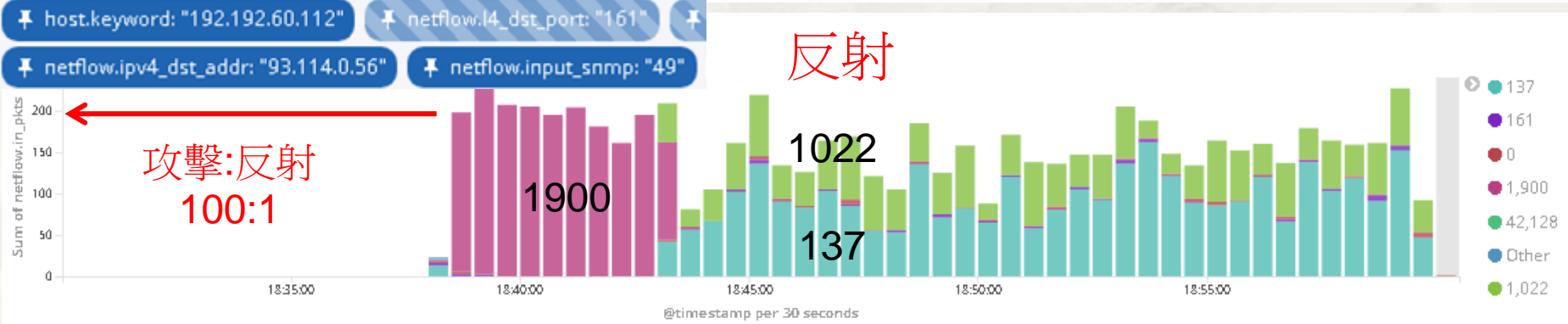


Case.大同大學20190304

93.114.0.56 Port



攻擊



反射

攻擊:反射
100:1

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)