108年度第一次
台北區網(臺大)網管會議

臺灣大學計資中心
游子興
davisyou@ntu.edu.tw
3366-5008

項目	時 間	主持人／報告人	報 告 內 容
主席報告	14:00~14:05	組長：謝宏昀教授	
業務報告	14:05~14:20	游子興	區網營運業務報告
	14:20~14:30	李墨軒	弱掃平台相關說明
	14:30~14:50	李美雯	資安Case Study分享
專題研討	14:50~15:30	游子興	BGP Hijacking 事件探討
	15:40~17:00	北區ASOC	Openvas 與 shodan 簡介及應用實例
臨時動議		出列席人員	

圖書館日治時期統計資料庫
WAF 阻擋封包分析

Test port 80 81

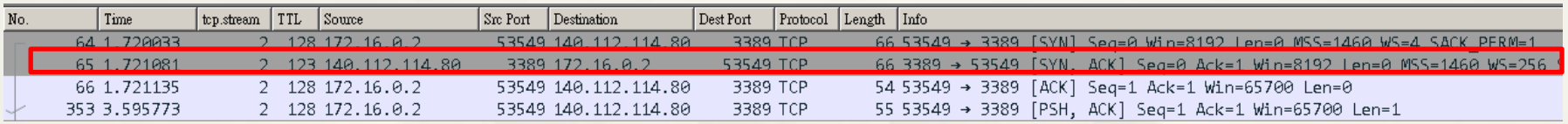
```
C:\Windows\System32>telnet  140.112.114.80 80
正連線到 140.112.114.80...無法開啟到主機的連線， 在連接埠 80: 連線失敗

C:\Windows\System32>telnet  140.112.114.80 81
正連線到 140.112.114.80...無法開啟到主機的連線， 在連接埠 81: 連線失敗
```

* Port 80 很快出現錯誤
* Port 81 Timeout 才出現錯誤

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
127	2.594903	4	128	172.16.0.2	50815	140.112.114.80	80	TCP	66	50815 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
128	2.595441	4	250	140.112.114.80	80	172.16.0.2	50815	TCP	60	80 → 50815 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
163	3.089076	4	128	172.16.0.2	50815	140.112.114.80	80	TCP	66	[TCP Retransmission] 50815 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_
164	3.090029	4	250	140.112.114.80	80	172.16.0.2	50815	TCP	60	80 → 50815 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	3.589163	4	128	172.16.0.2	50815	140.112.114.80	80	TCP	62	[TCP Retransmission] 50815 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=
187	3.589807	4	250	140.112.114.80	80	172.16.0.2	50815	TCP	60	80 → 50815 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
334	6.544895	11	128	172.16.0.2	50818	140.112.114.80	81	TCP	66	50818 → 81 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
825	9.546256	11	128	172.16.0.2	50818	140.112.114.80	81	TCP	66	[TCP Retransmission] 50818 → 81 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_
1482	15.546509	11	128	172.16.0.2	50818	140.112.114.80	81	TCP	62	[TCP Retransmission] 50818 → 81 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=

* Port 80 被 reset. (TTL=250)
  * RST 封包間隔很短
* Port 81 Timeout
  * 間隔 3 秒、6 秒 重送 SYN

Test port 3389

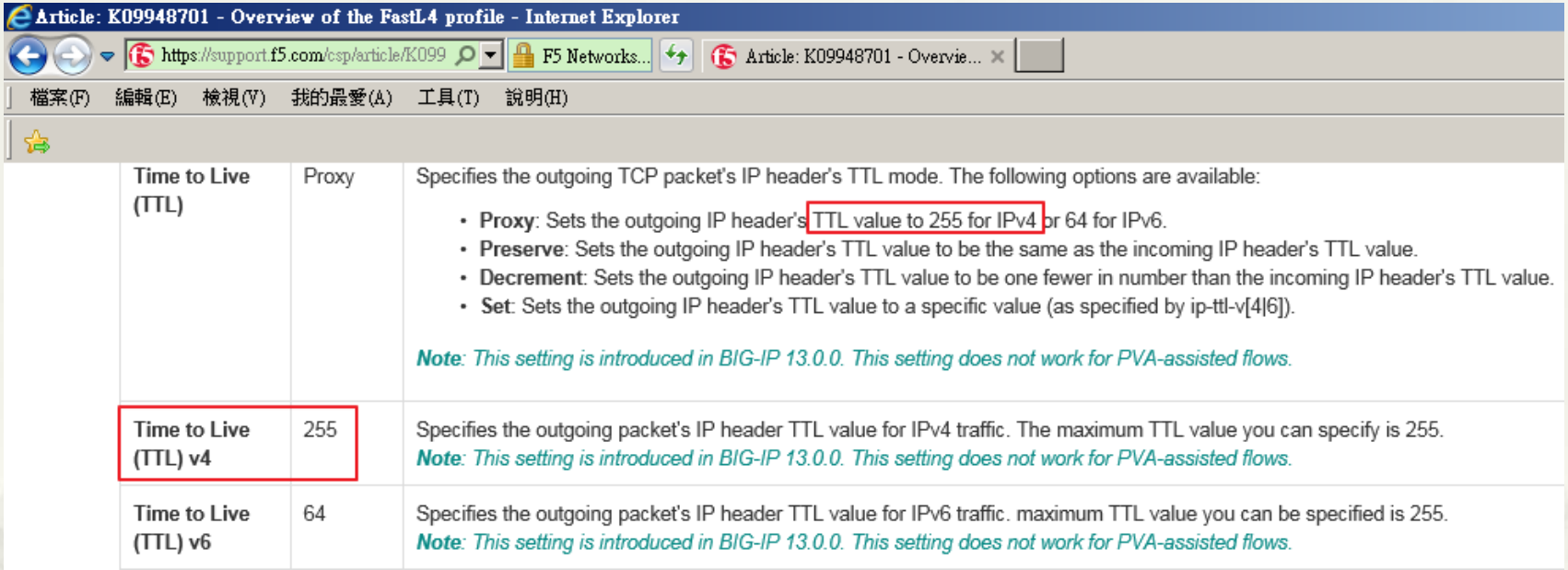


No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
64	1.720033	2	128	172.16.0.2	53549	140.112.114.80	3389	TCP	66	53549 → 3389 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
65	1.721081	2	123	140.112.114.80	3389	172.16.0.2	53549	TCP	66	3389 → 53549 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256
66	1.721135	2	128	172.16.0.2	53549	140.112.114.80	3389	TCP	54	53549 → 3389 [ACK] Seq=1 Ack=1 Win=65700 Len=0
353	3.595773	2	128	172.16.0.2	53549	140.112.114.80	3389	TCP	55	53549 → 3389 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=1

* Port 3389 正常(TTL=123)

* 140.112.114.80 為 Windows Server，TTL 初始值 128，但發出 Reset 封包 TTL=250，推測該設備 TTL 初始值為 255
  * 128-123=5 hops -> Windows Server
  * 255-250=5 hops -> 發出 Reset 設備

F5 Default TTL



Time to Live (TTL)	Proxy	Specifies the outgoing TCP packet's IP header's TTL mode. The following options are available: • **Proxy**: Sets the outgoing IP header's TTL value to 255 for IPv4 or 64 for IPv6. • **Preserve**: Sets the outgoing IP header's TTL value to be the same as the incoming IP header's TTL value. • **Decrement**: Sets the outgoing IP header's TTL value to be one fewer in number than the incoming IP header's TTL value. • **Set**: Sets the outgoing IP header's TTL value to a specific value (as specified by ip-ttl-v[4|6]). ***Note***: *This setting is introduced in BIG-IP 13.0.0. This setting does not work for PVA-assisted flows.*
Time to Live (TTL) v4	255	Specifies the outgoing packet's IP header TTL value for IPv4 traffic. The maximum TTL value you can specify is 255. ***Note***: *This setting is introduced in BIG-IP 13.0.0. This setting does not work for PVA-assisted flows.*
Time to Live (TTL) v6	64	Specifies the outgoing packet's IP header TTL value for IPv6 traffic. maximum TTL value you can be specified is 255. ***Note***: *This setting is introduced in BIG-IP 13.0.0. This setting does not work for PVA-assisted flows.*

F5 Rule 刪除
恢復正常

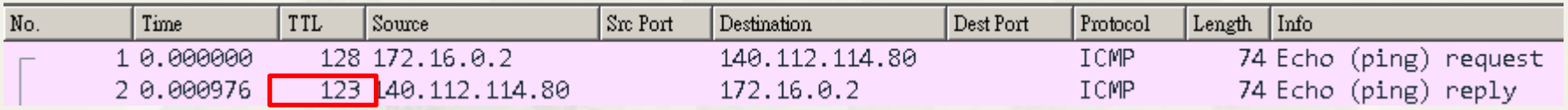
* 將 F5 Rule 刪除，Port 80 正常連線，TTL=123

ip.addr==140.112.114.80 Expression…

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
316	1.942571	4	128	172.16.0.2	53512	140.112.114.80	80	TCP	66	53512 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
317	1.943527	4	123	140.112.114.80	80	172.16.0.2	53512	TCP	66	80 → 53512 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
318	1.943584	4	128	172.16.0.2	53512	140.112.114.80	80	TCP	54	53512 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0

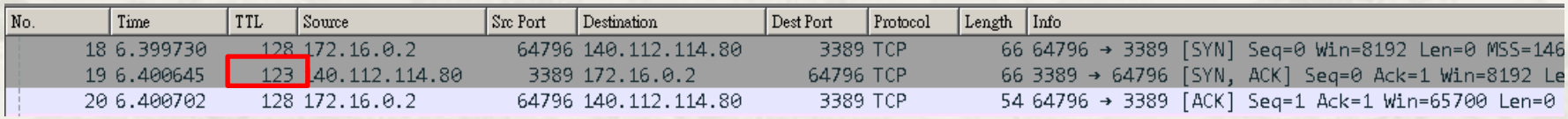
F5 Rule 設定正確後

- ping 140.112.114.80
  - TTL=123 Windows



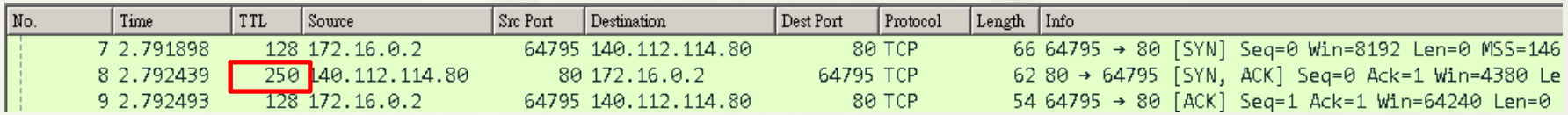
No.	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	128	172.16.0.2		140.112.114.80		ICMP	74	Echo (ping) request
2	0.000976	123	140.112.114.80		172.16.0.2		ICMP	74	Echo (ping) reply

- telnet 140.112.114.80 3389
  - TTL=123 Windows



No.	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
18	6.399730	128	172.16.0.2	64796	140.112.114.80	3389	TCP	66	64796 → 3389 [SYN] Seq=0 Win=8192 Len=0 MSS=146
19	6.400645	123	140.112.114.80	3389	172.16.0.2	64796	TCP	66	3389 → 64796 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le
20	6.400702	128	172.16.0.2	64796	140.112.114.80	3389	TCP	54	64796 → 3389 [ACK] Seq=1 Ack=1 Win=65700 Len=0

- telnet 140.112.114.80 80
  - TTL=250 F5



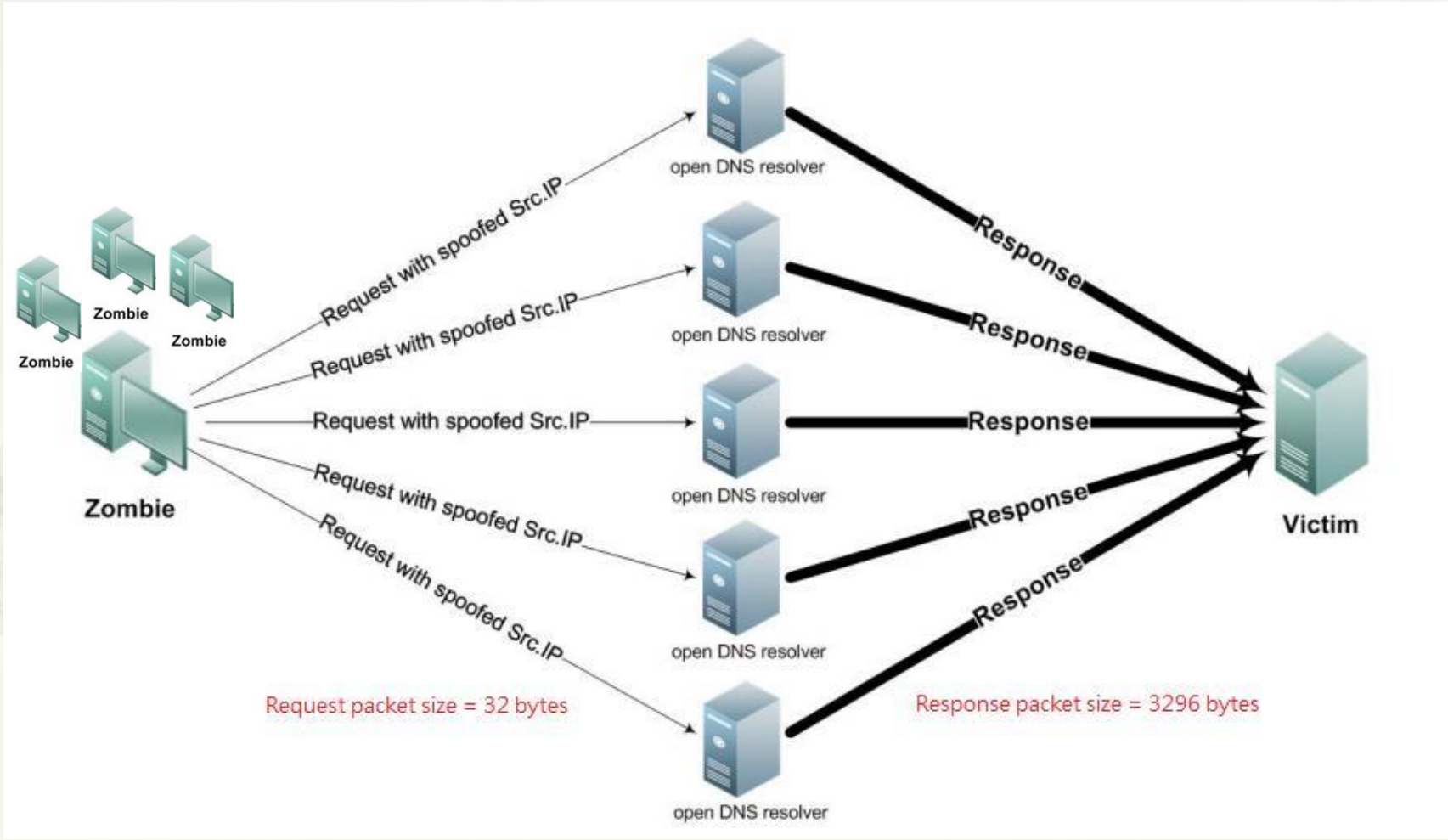
No.	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
7	2.791898	128	172.16.0.2	64795	140.112.114.80	80	TCP	66	64795 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146
8	2.792439	250	140.112.114.80	80	172.16.0.2	64795	TCP	62	80 → 64795 [SYN, ACK] Seq=0 Ack=1 Win=4380 Le
9	2.792493	128	172.16.0.2	64795	140.112.114.80	80	TCP	54	64795 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

DDoS 事件分析

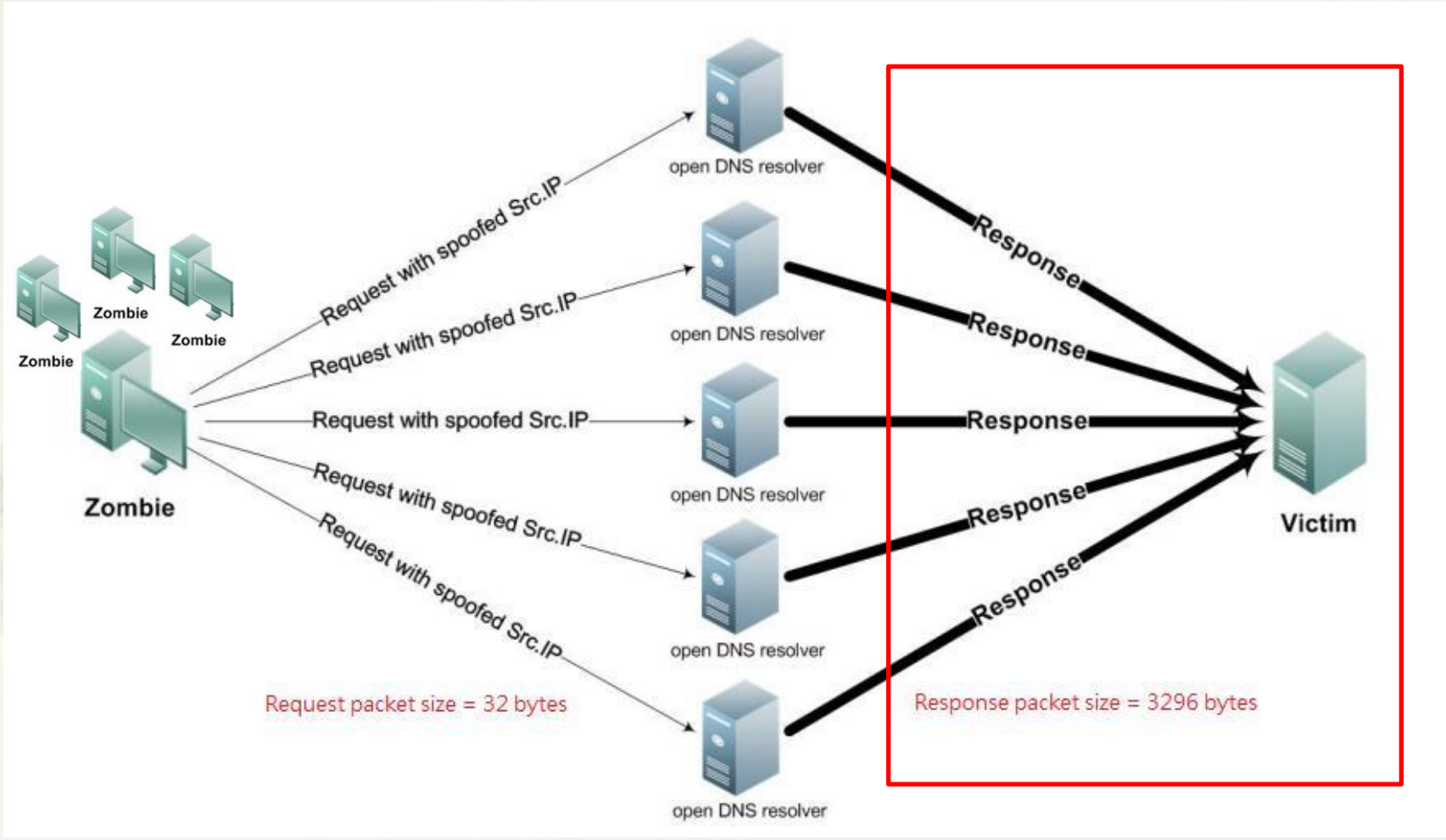
DDoS 攻擊方式

- 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

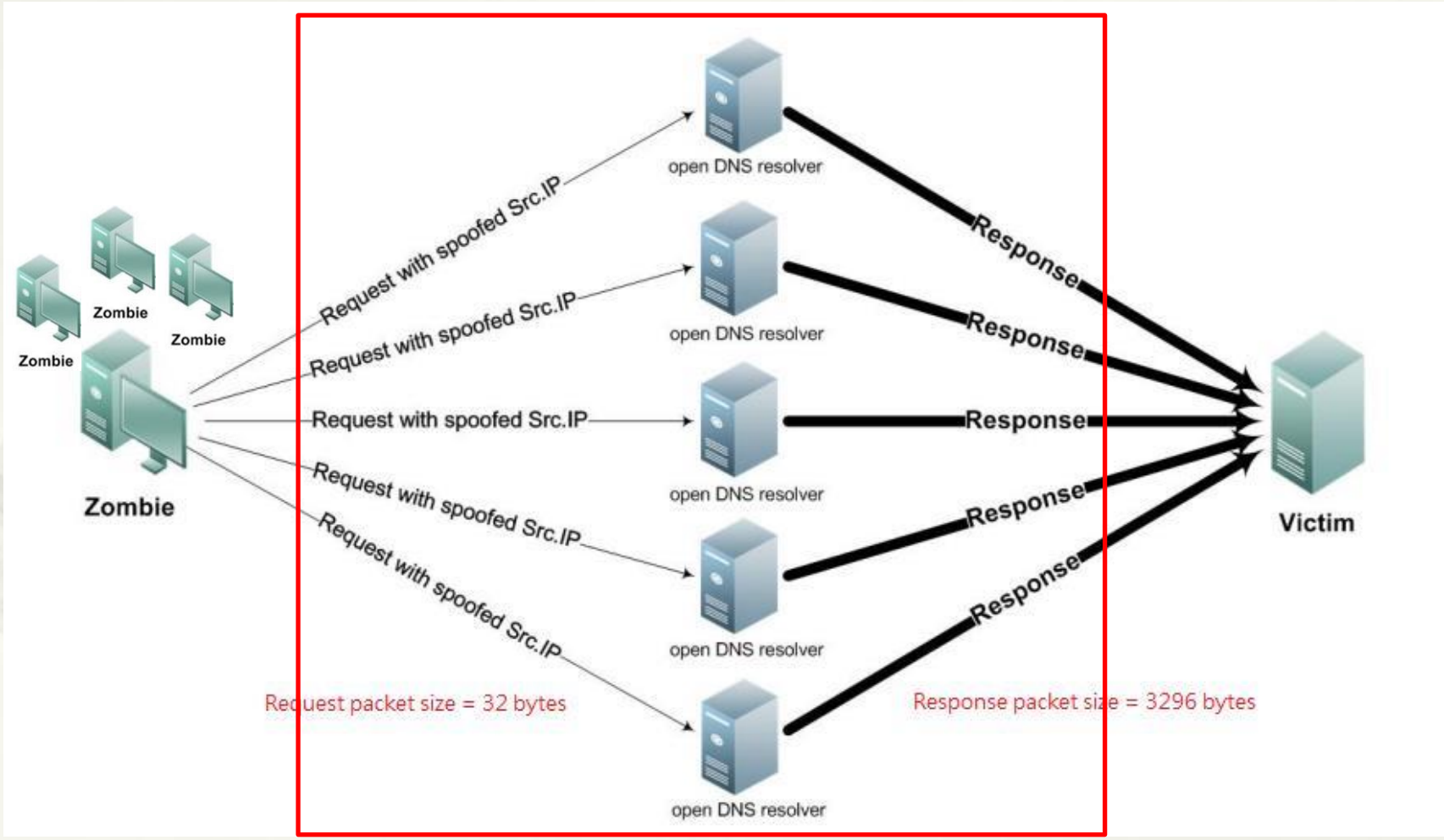
反射攻擊架構圖


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

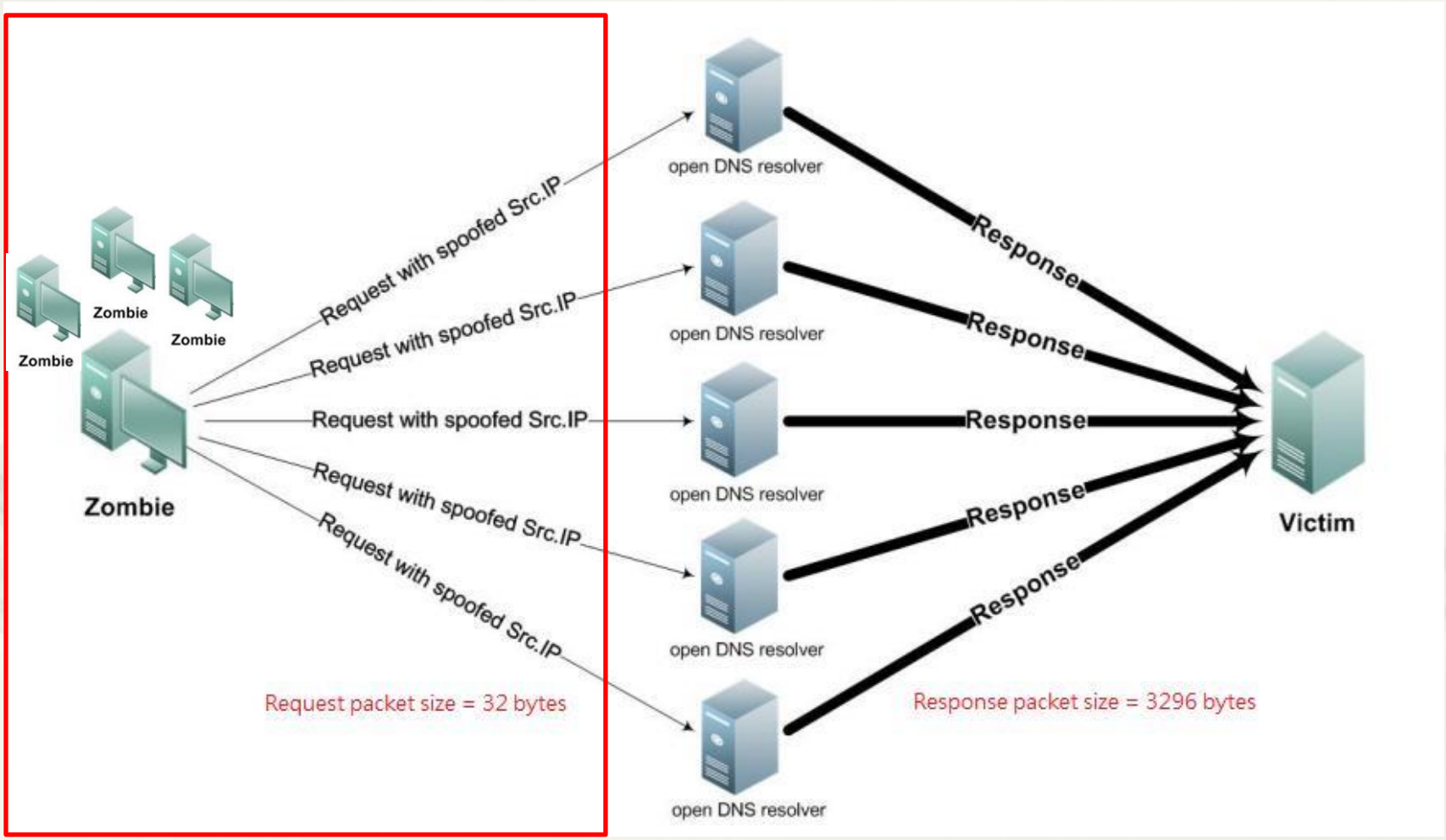
外對內: 遭受反射攻擊


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



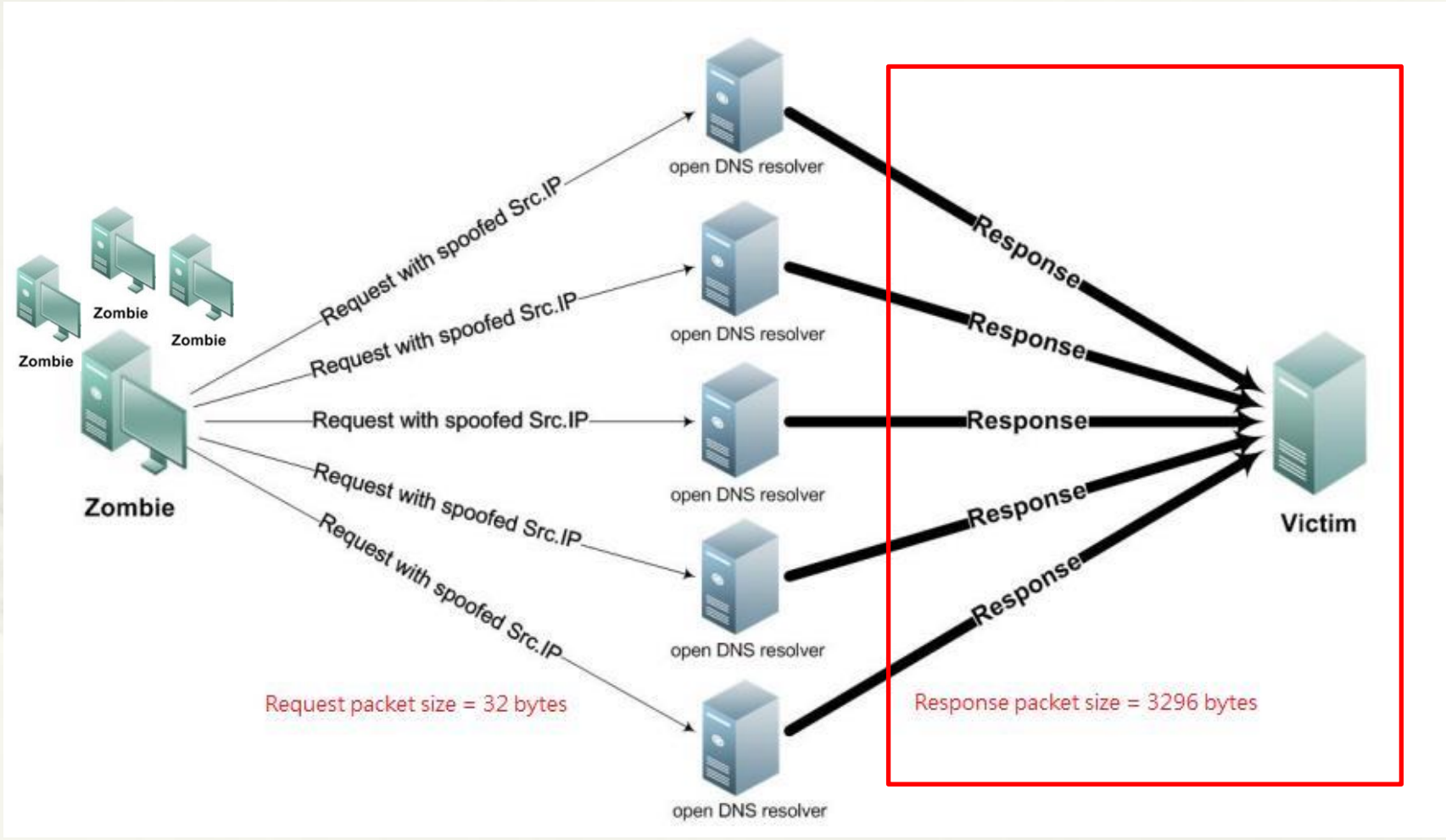
內對外: 內部有 **BOT** 利用外部反射 **Server** 攻擊受害者



反射攻擊類型

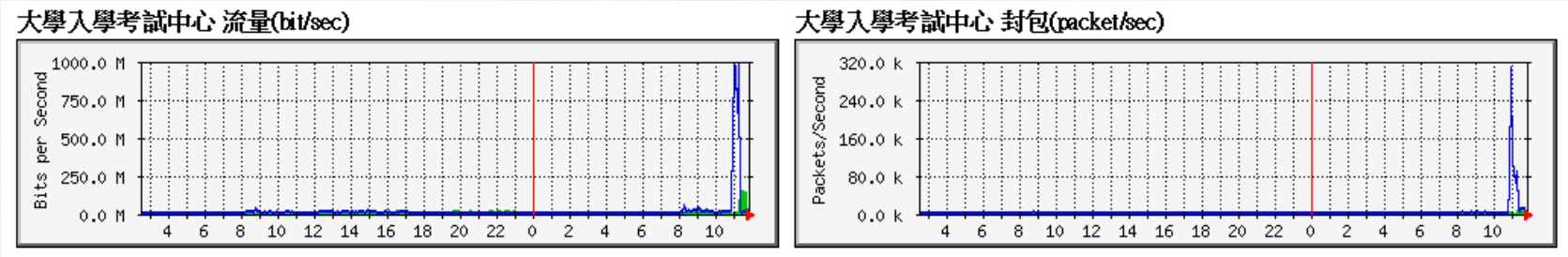
- Protocol: UDP
- 反射類型與 Port
  - DNS (Query Any Record): 53
  - RPC(Remote Procedure Call)/Port Mapper/NFS: 111
  - NTP (Mon List): 123
  - NetBIOS/SMB: 137
  - SNMP: 161
  - LDAP (CLDAP Query Root): 389
  - SSDP: 1900
  - Memcached: 11211

外對內: 遭受反射攻擊

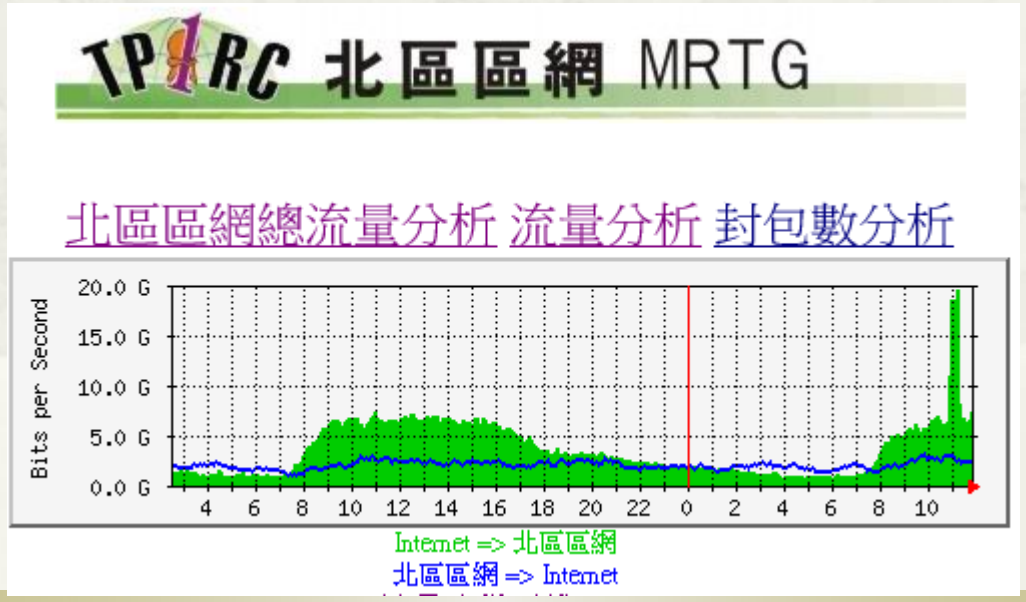

Zombie
Zombie
Zombie
Zombie
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
Request with spoofed Src.IP
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
Response
Response
Response
Response
Response
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

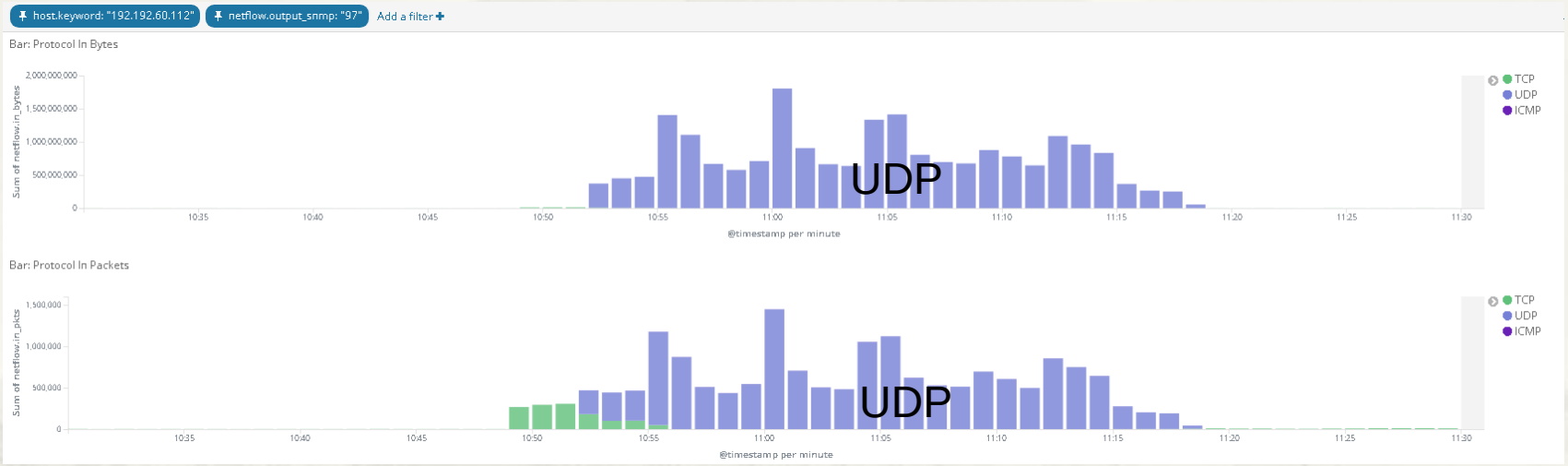


* 區網骨幹



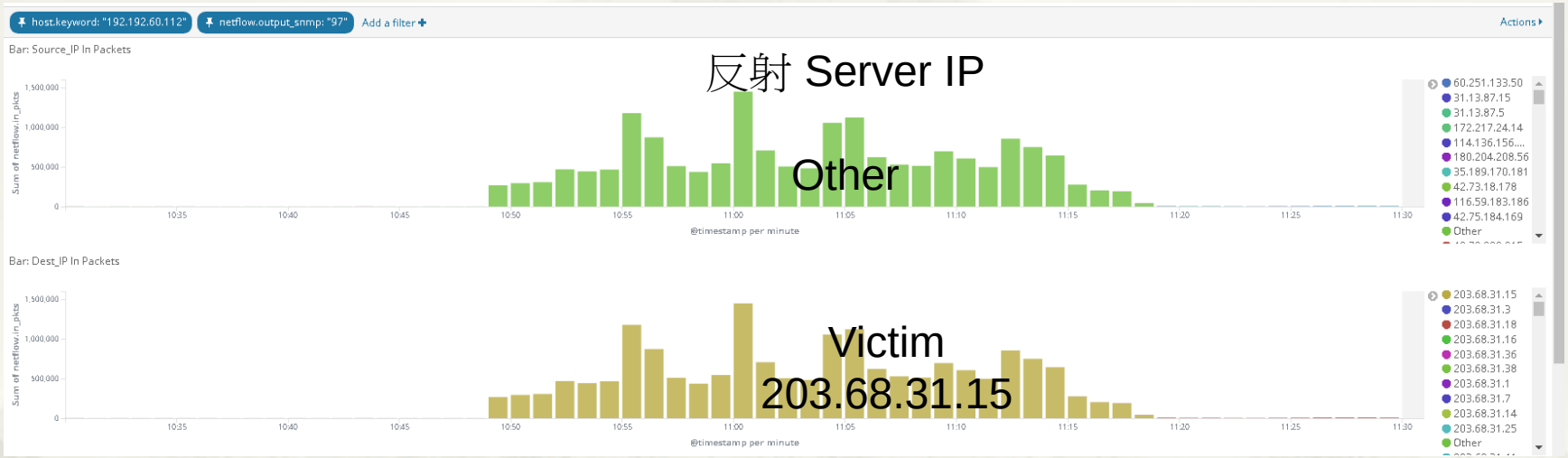
外對內: 遭受**DNS**反射攻擊

* Protocol: UDP

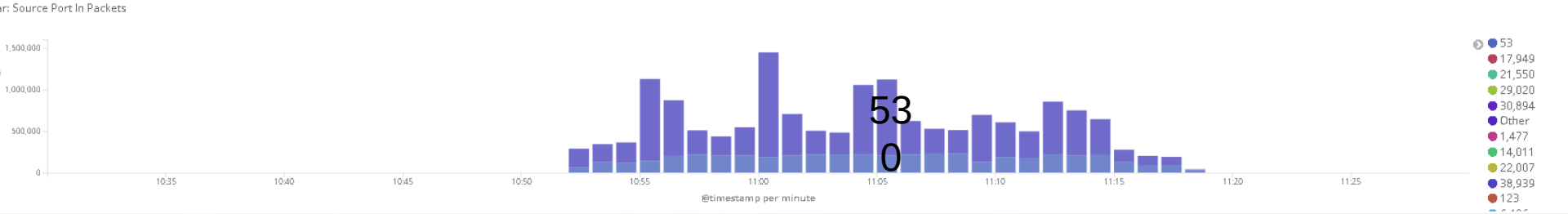


外對內: 遭受DNS反射攻擊

* Source IP & Dest IP

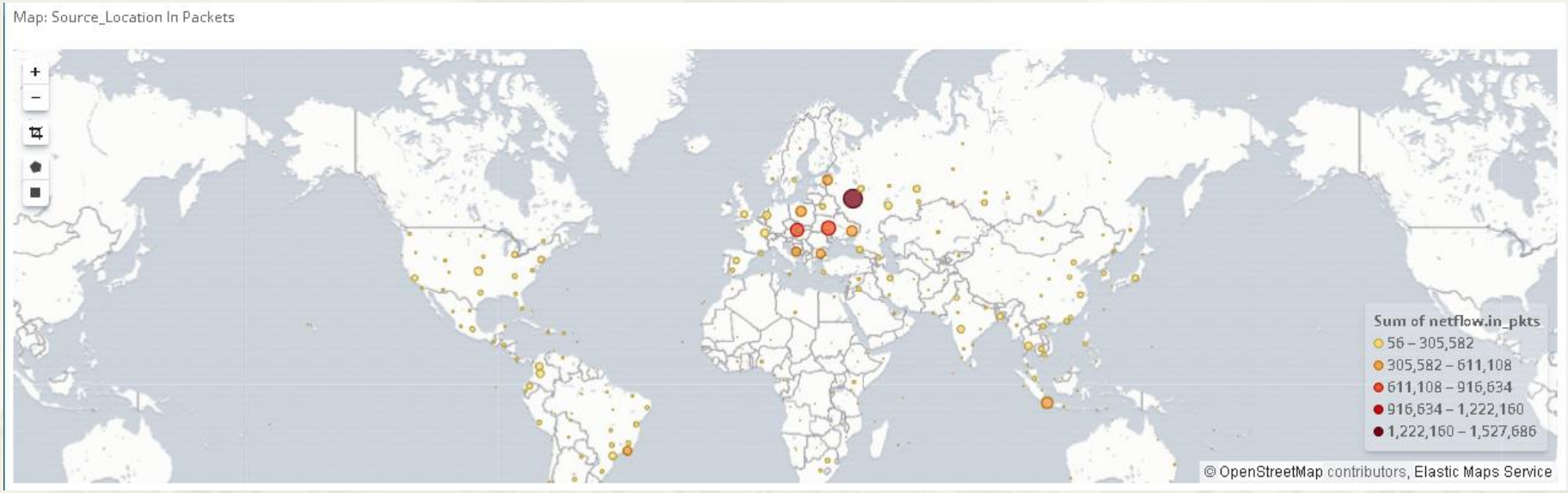


* Source Port

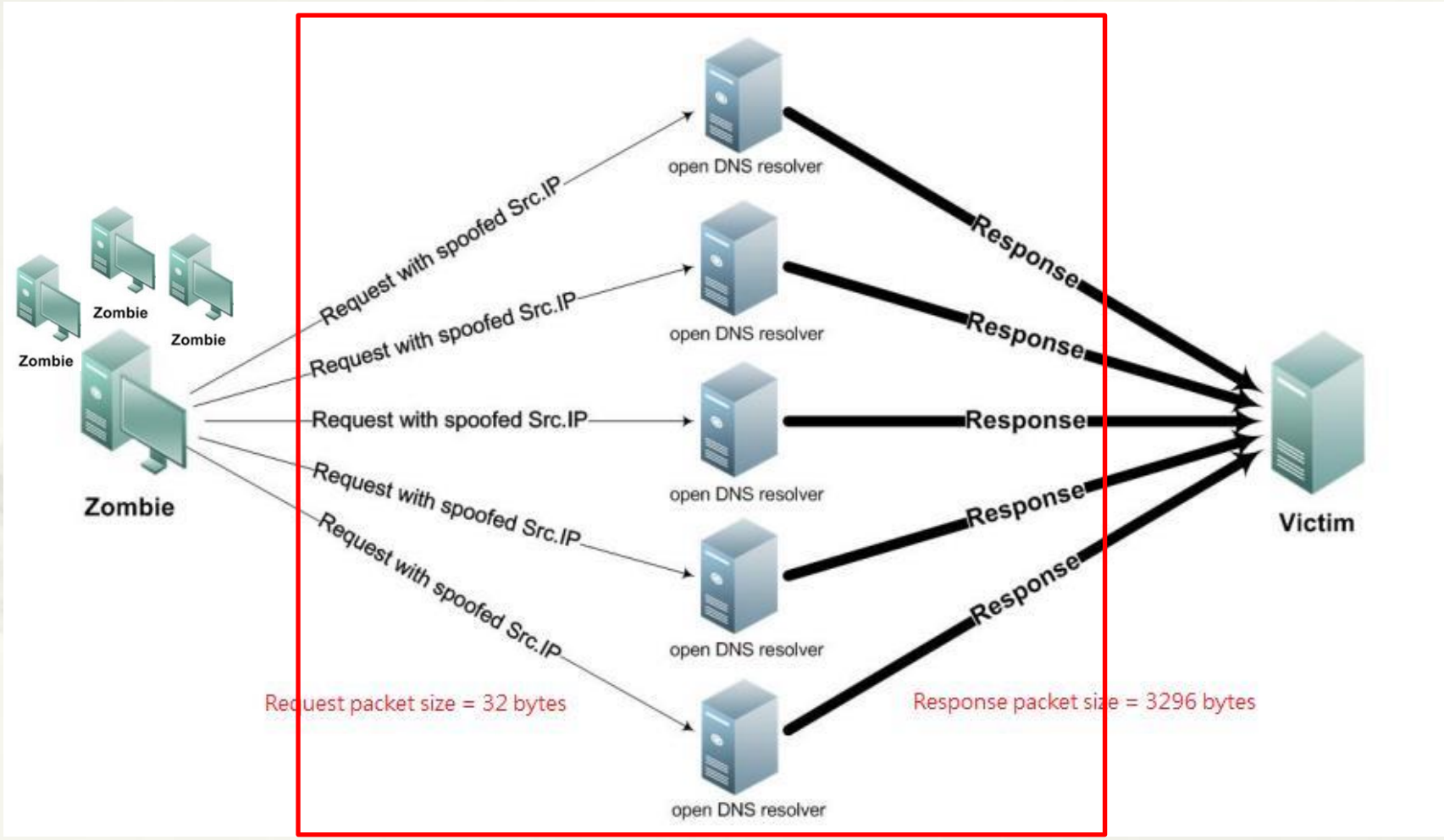


外對內: 遭受DNS反射攻擊

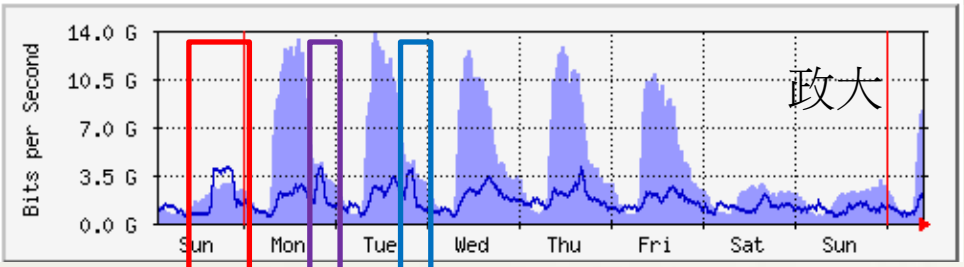
* 攻擊來源

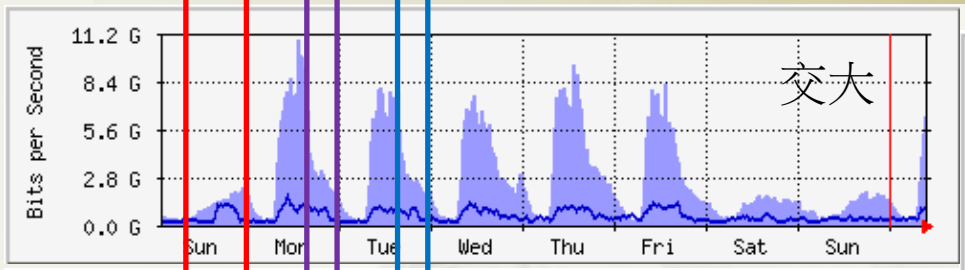


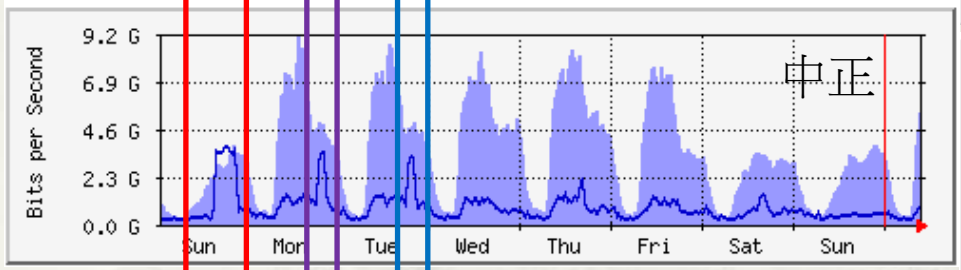
外對內 + 內對外
內部有反射 **Server** 被利用於攻擊受害者

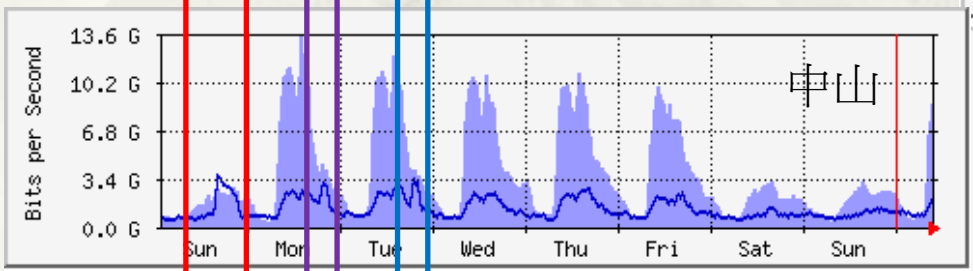


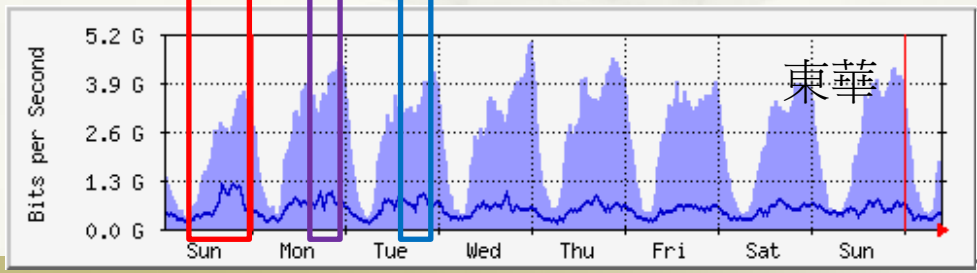
20190303~0305
各區網中心

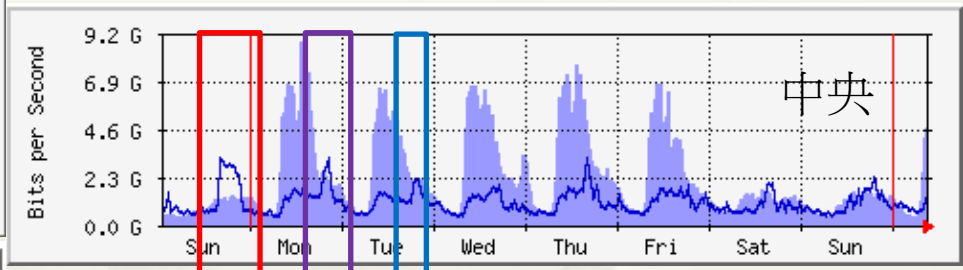


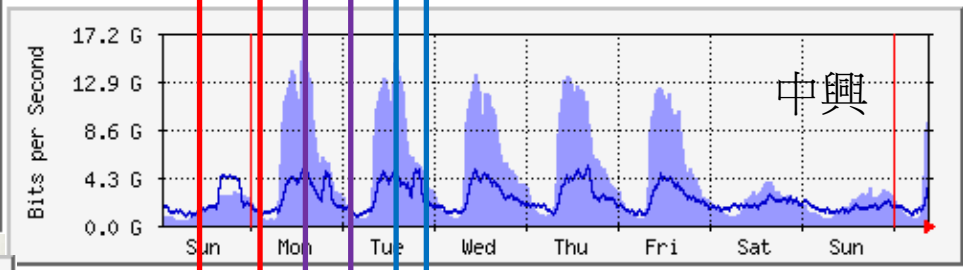


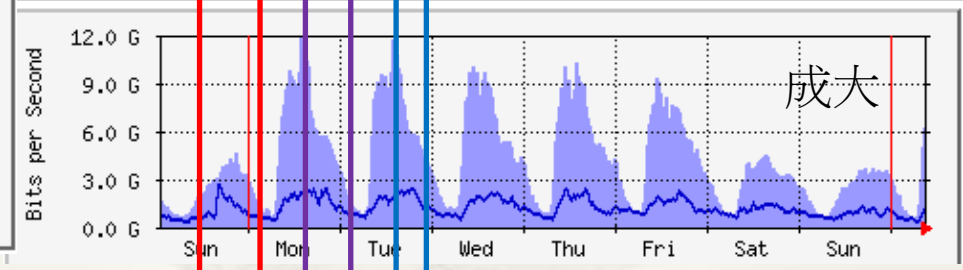


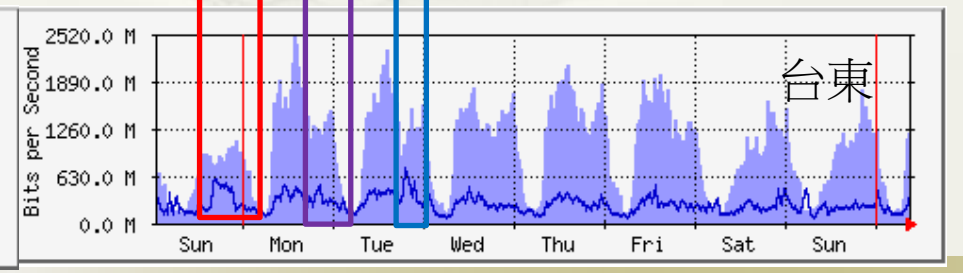






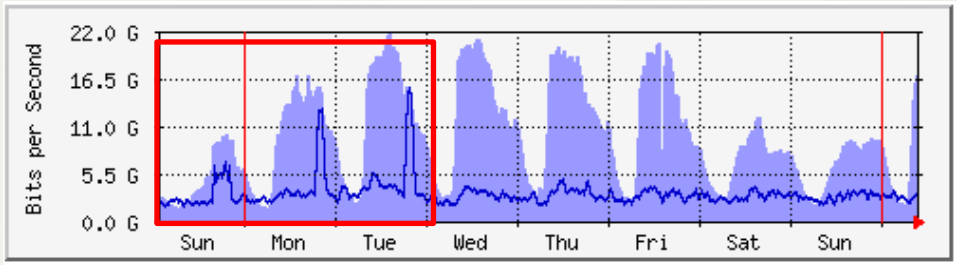






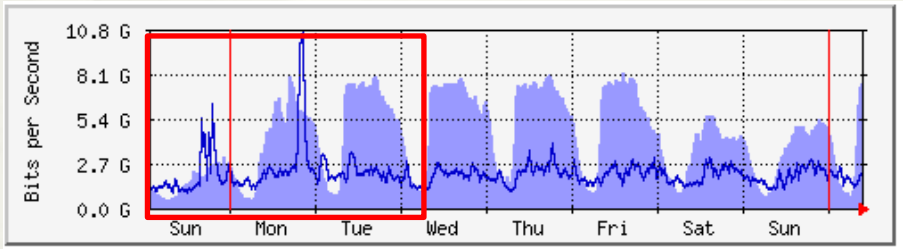
TANet DDoS 攻擊出口
Max 25~30 Gbps

TANet to Internet IPv4 [30G]



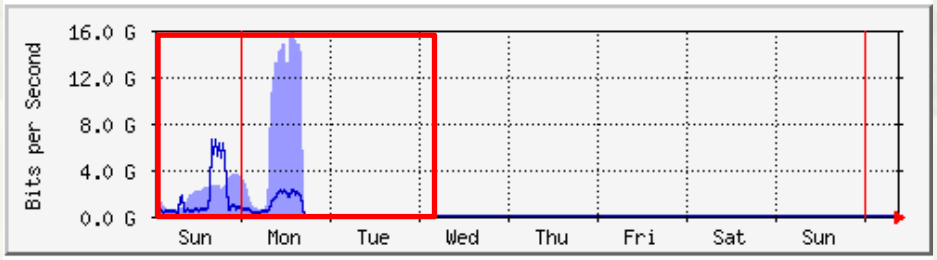
	最大	平均	目前
Internet ⇒ TANet	21.8 Gb/秒 (67.7%)	9419.5 Mb/秒 (29.2%)	16.9 Gb/秒 (52.4%)
TANet ⇒ Internet	15.2 Gb/秒 (47.2%)	3093.5 Mb/秒 (9.6%)	3132.5 Mb/秒 (9.7%)

CHIEF Transit Service



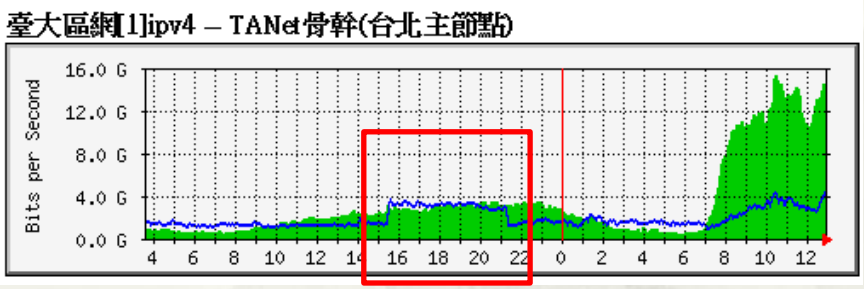
	最大	平均	目前
CHIEF ⇒ TANet	8180.1 Mb/秒 (76.2%)	4144.9 Mb/秒 (38.6%)	7496.5 Mb/秒 (69.8%)
TANet ⇒ CHIEF	10.6 Gb/秒 (98.3%)	2016.8 Mb/秒 (18.8%)	2007.1 Mb/秒 (18.7%)

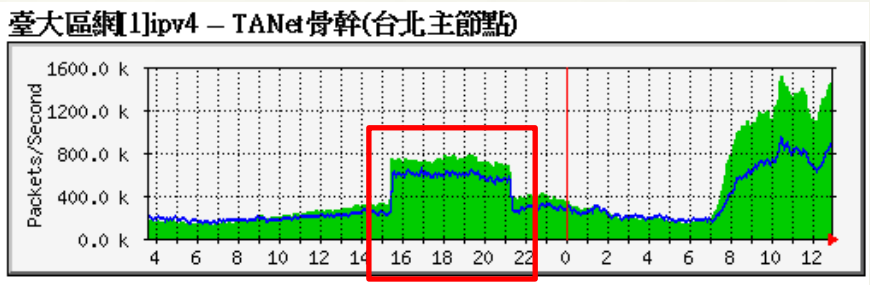
TPIX



	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



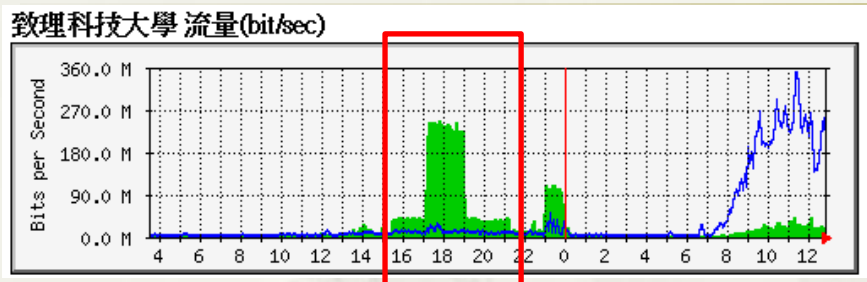


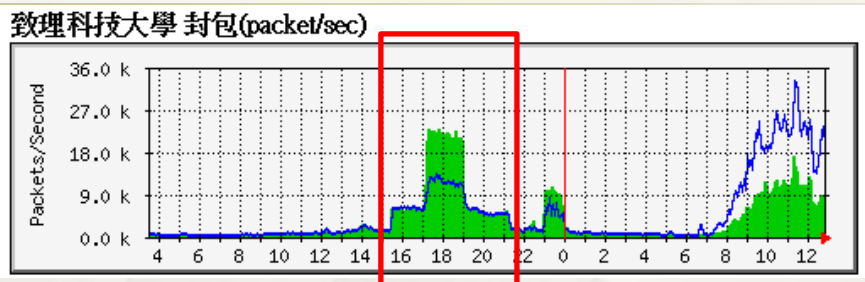
20190303 15:30~21:10

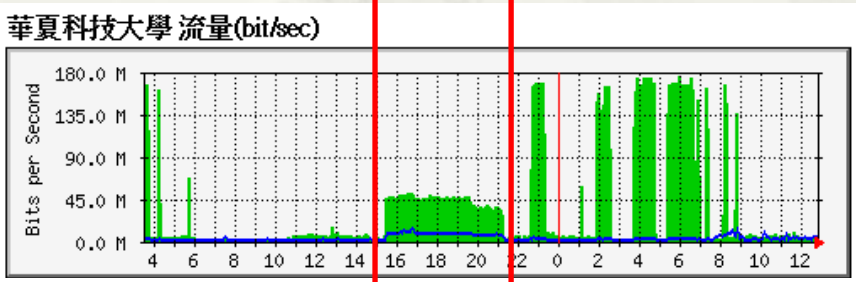
* TANet連線單位_反射攻擊_20190303_bps.mht
* TANet連線單位_反射攻擊_20190303_pps.mht
* TANet連線單位_反射攻擊_20190304_bps.mht
* TANet連線單位_反射攻擊_20190304_pps.mht
* TANet連線單位_反射攻擊_20190305_bps.mht
* TANet連線單位_反射攻擊_20190305_pps.mht

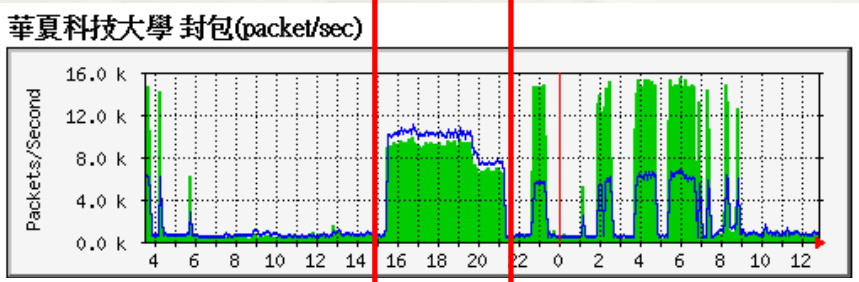
異常連線單位

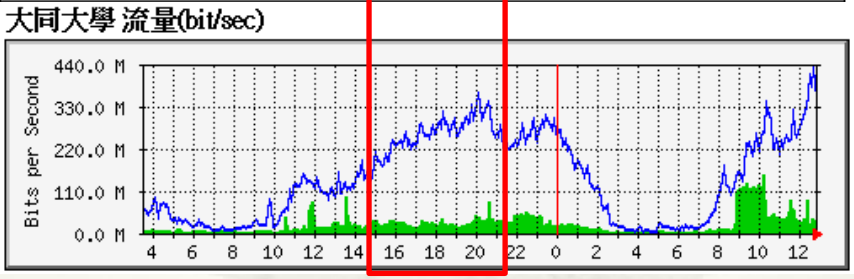
20190303

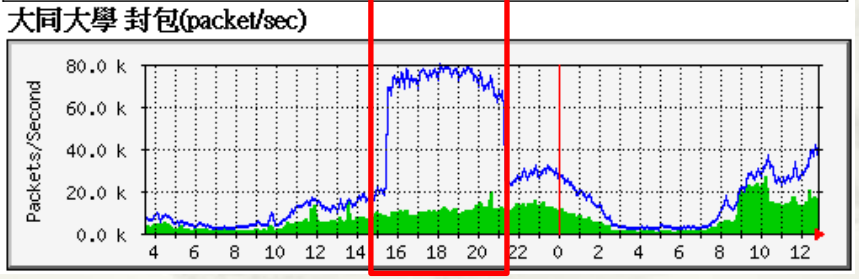


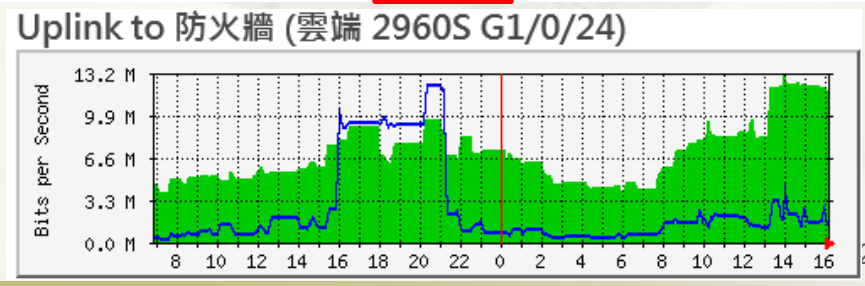






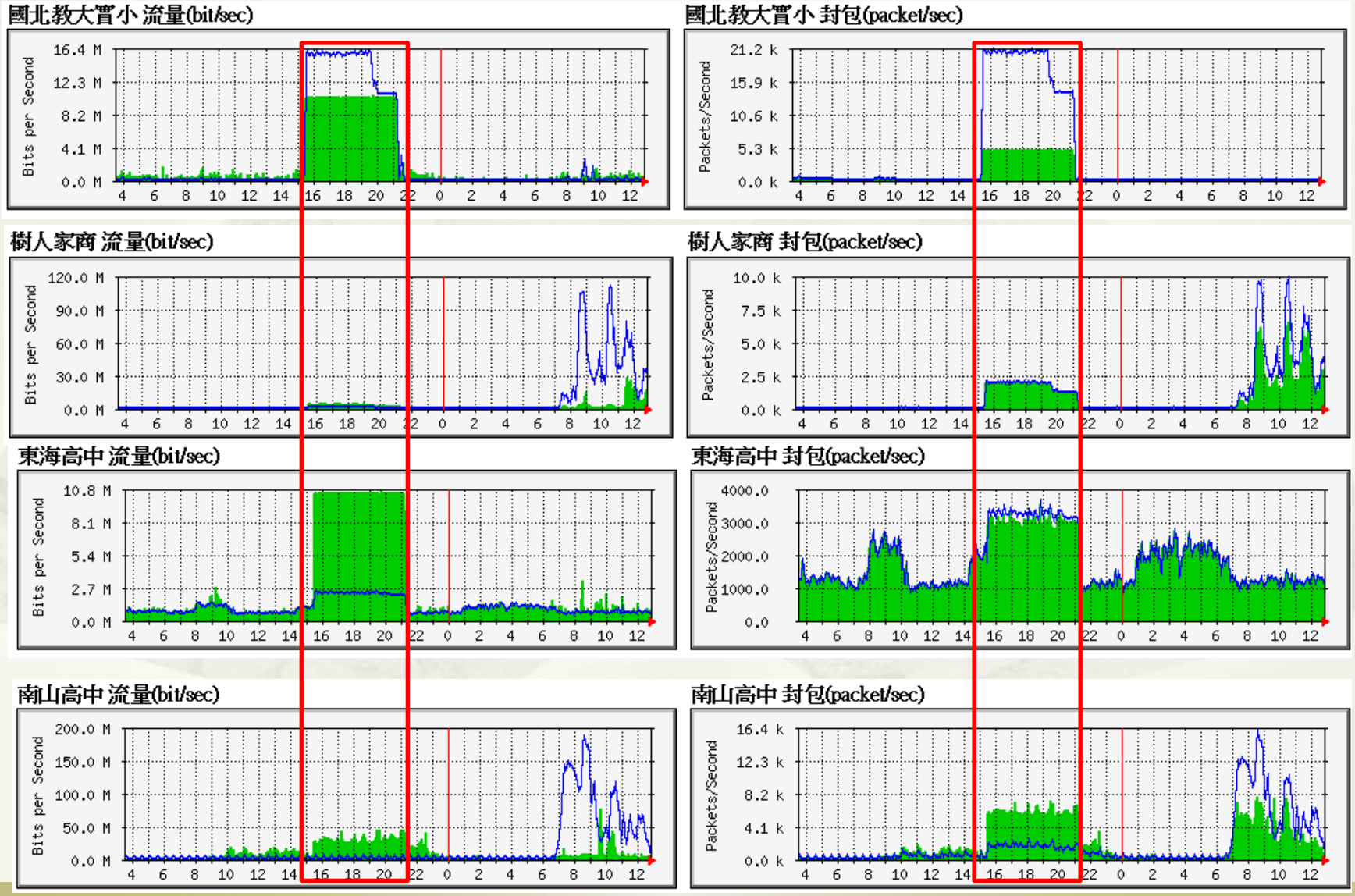






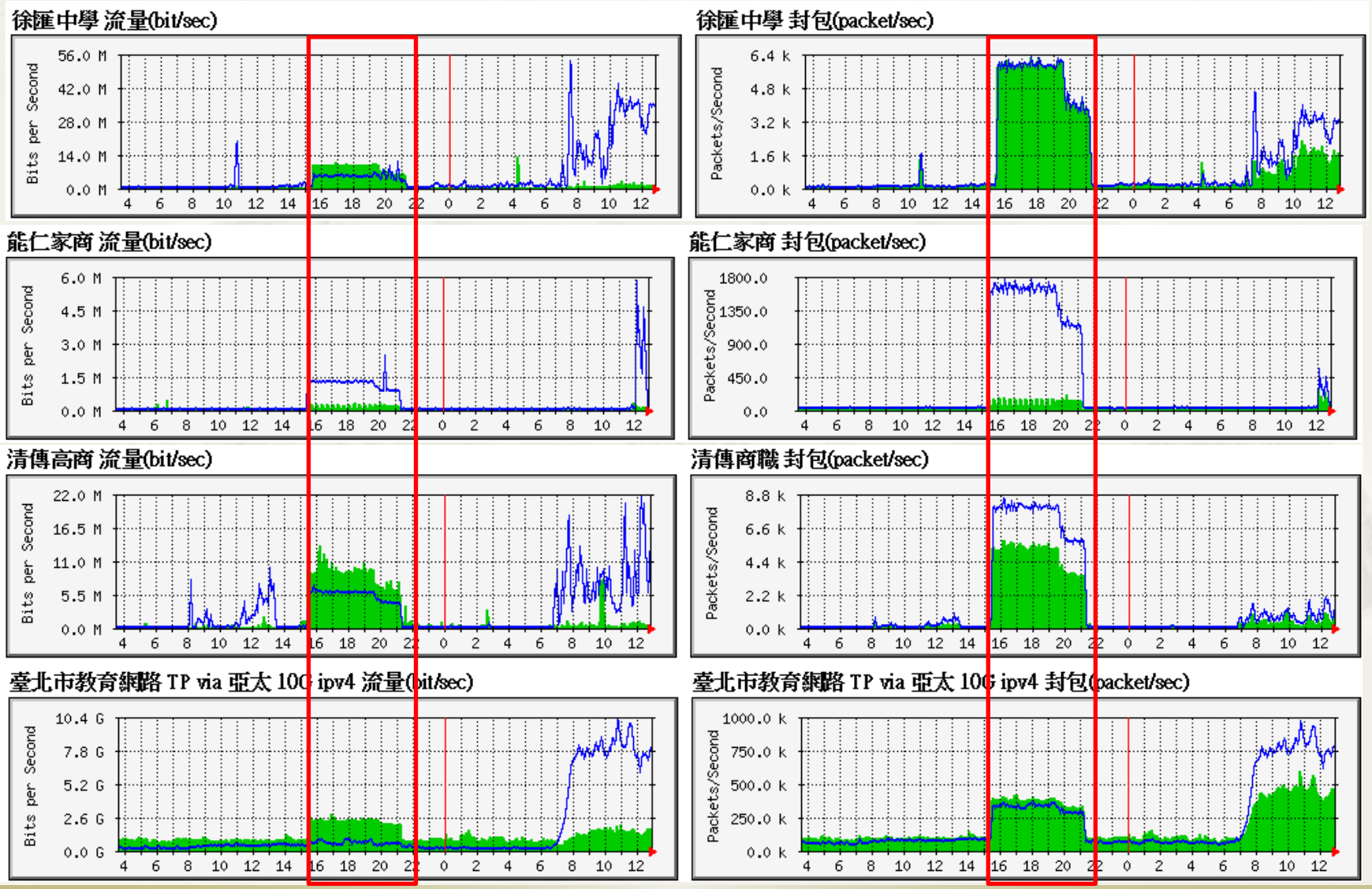
異常連線單位

20190303



異常連線單位

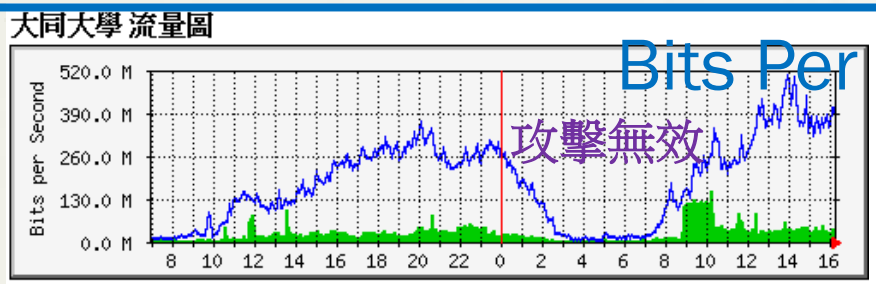
20190303

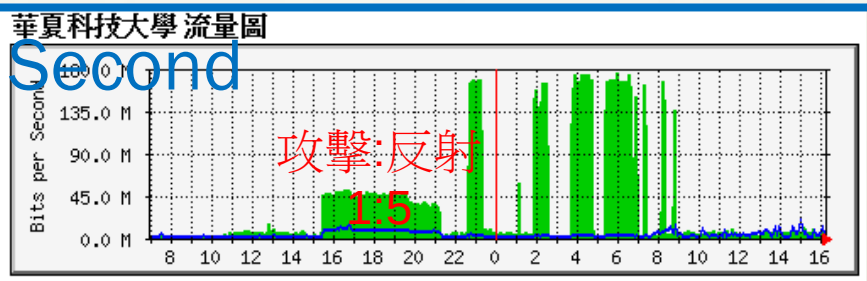


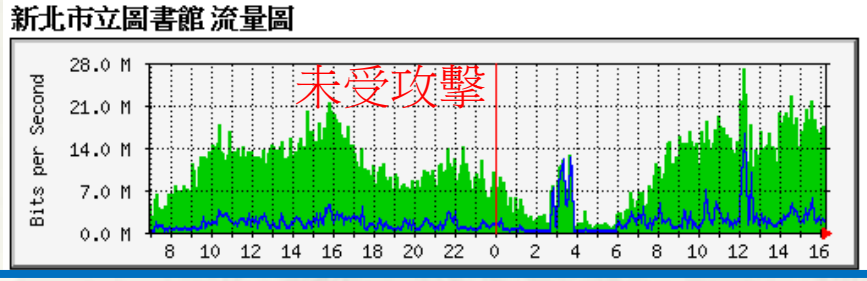
20190303

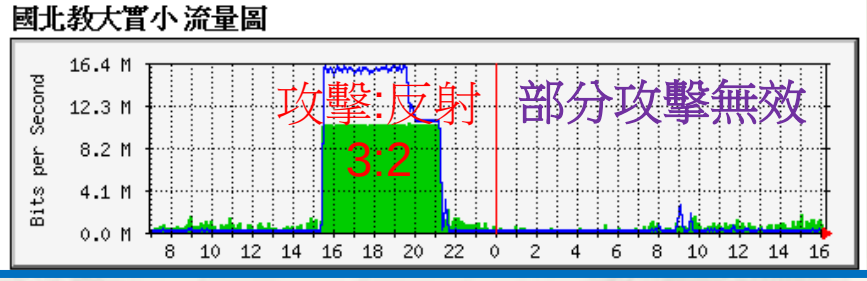
攻擊:反射 比例分析

Bits Per Second

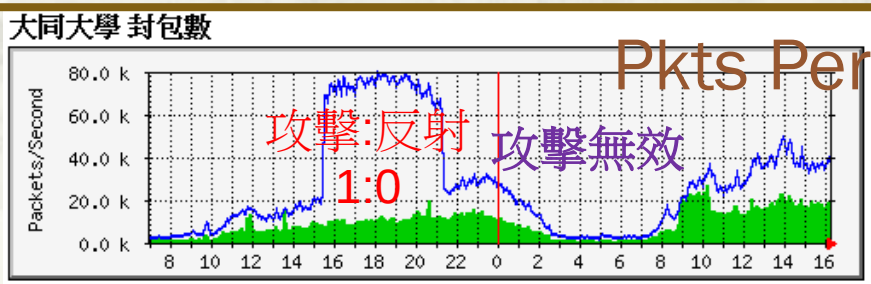


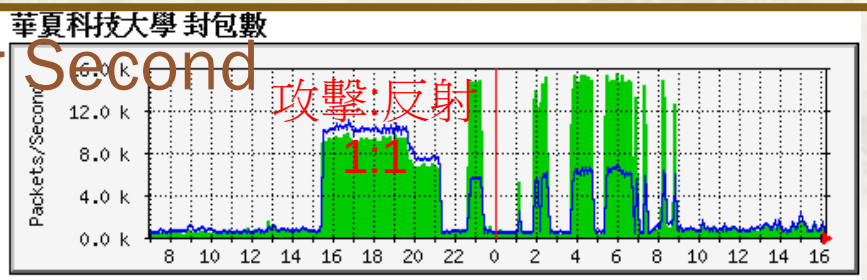


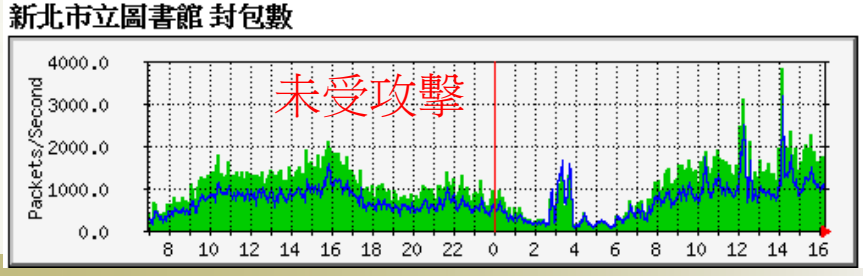


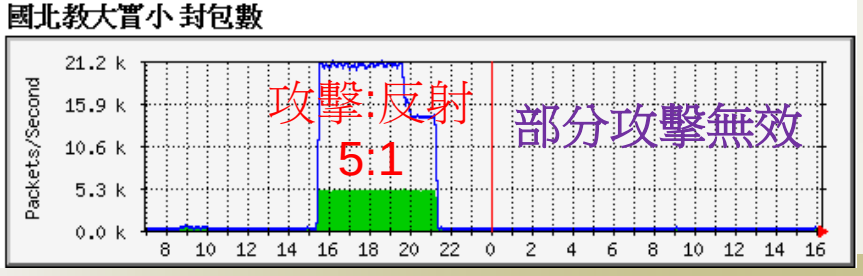


Pkts Per Second

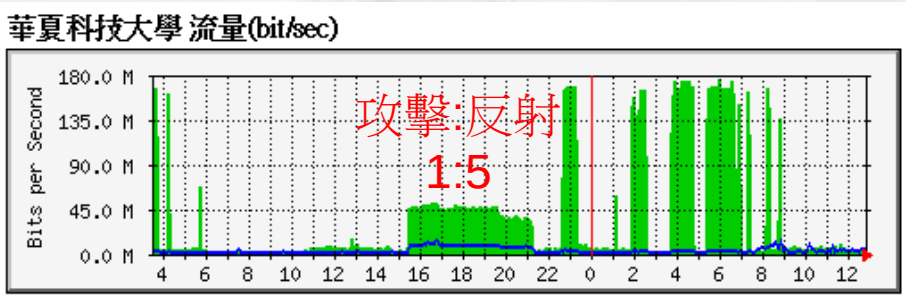


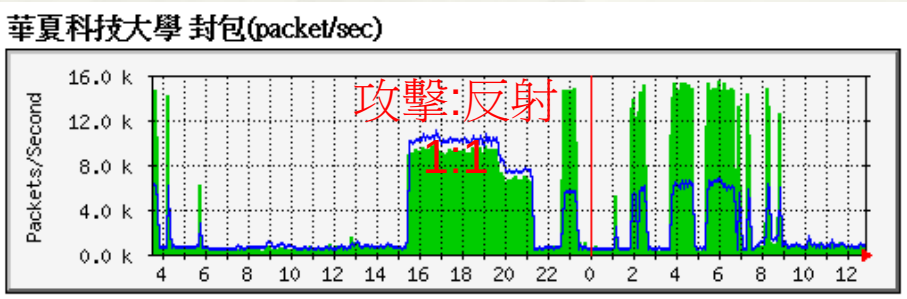




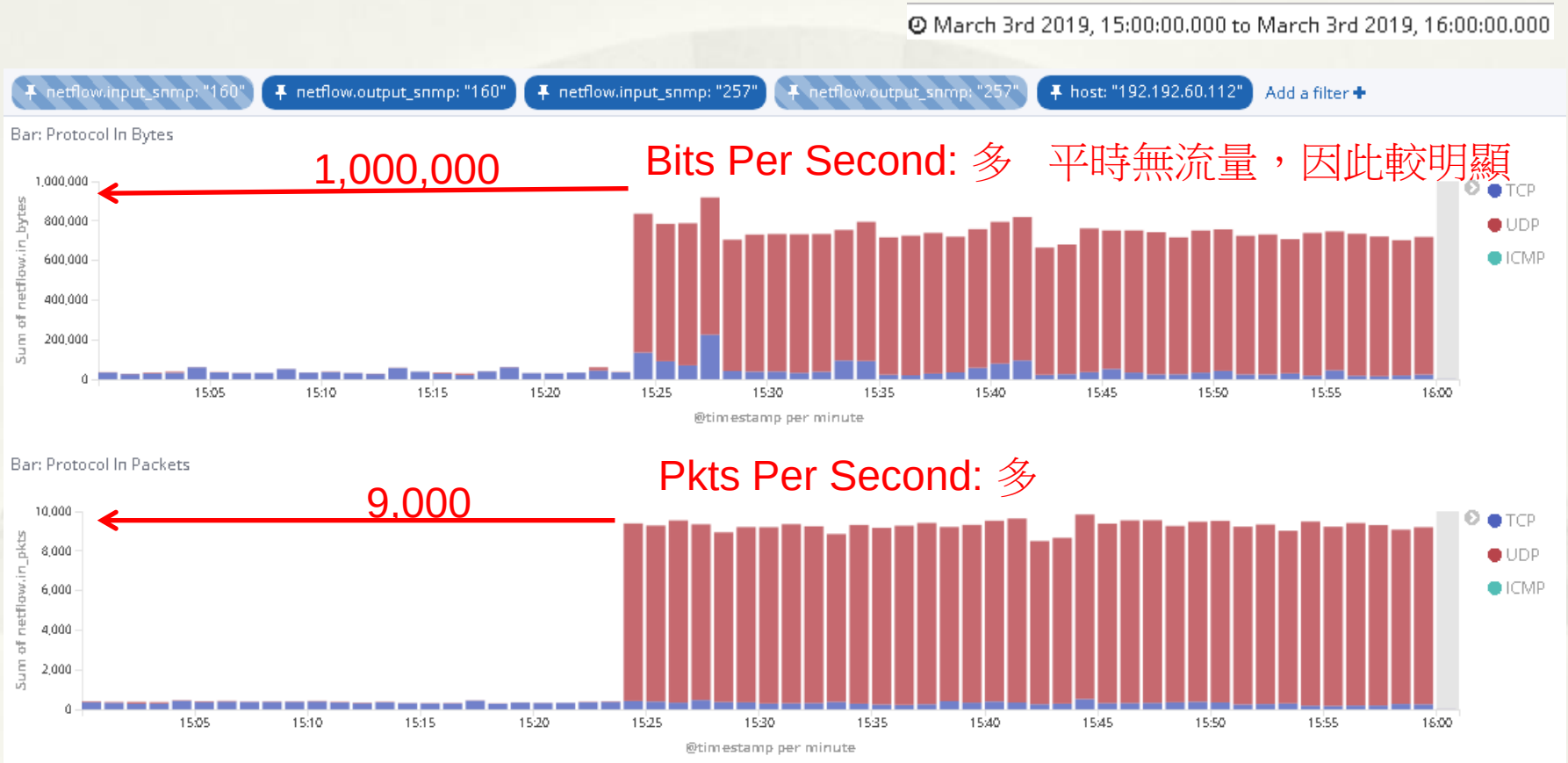


Case. 華夏科大 20190303
MRTG



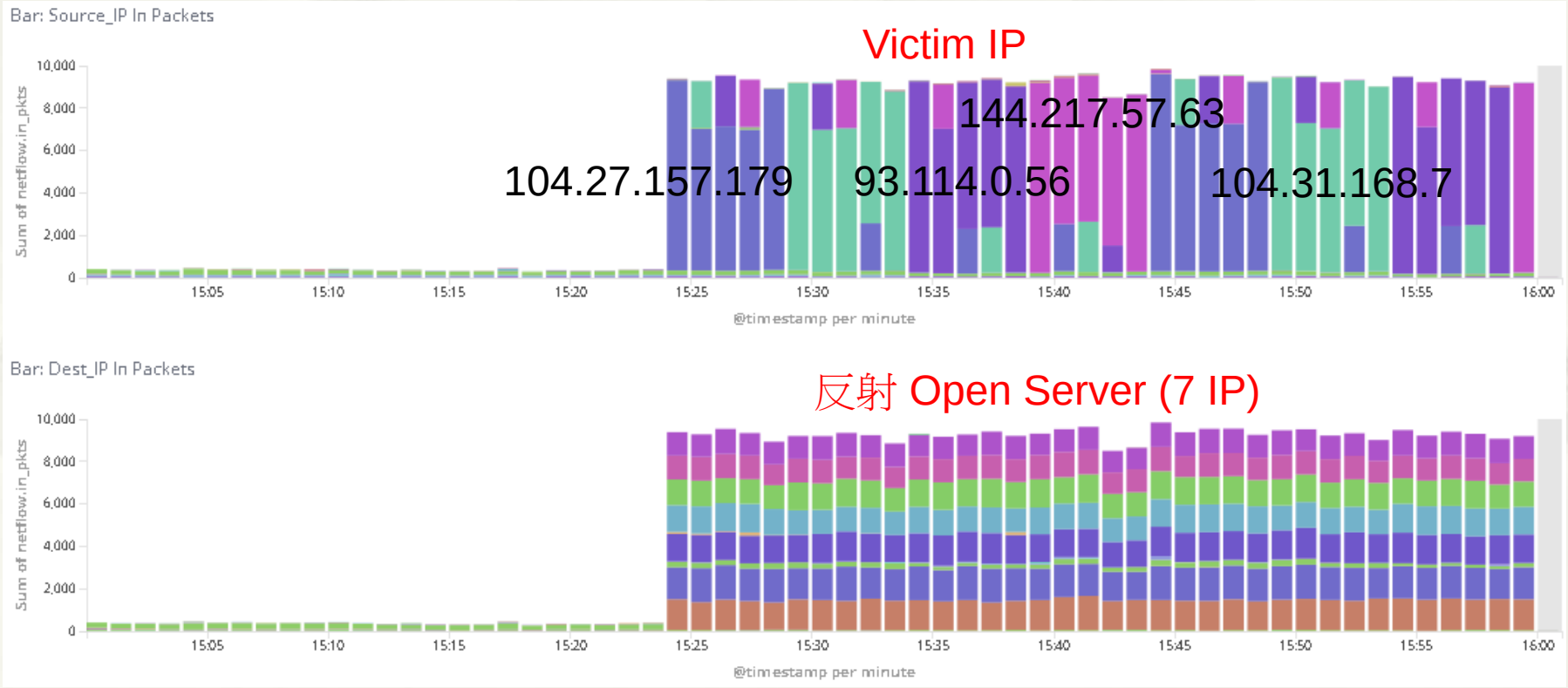


Case. 華夏科大 20190303
外對內 Protocol

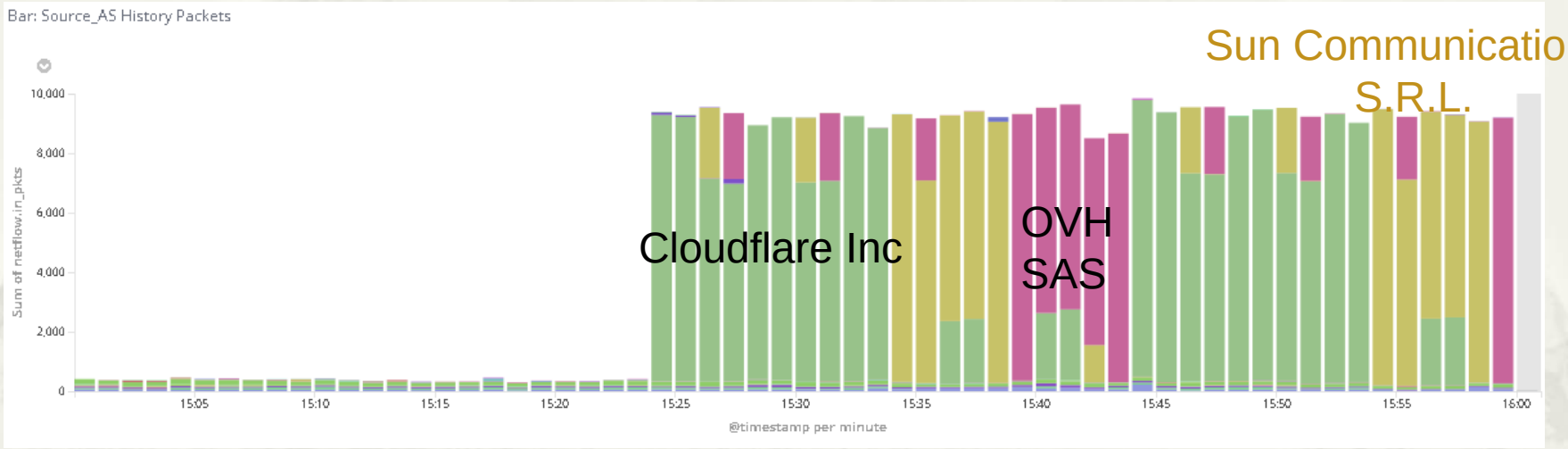


Case. 華夏科大 20190303
外對內 Port

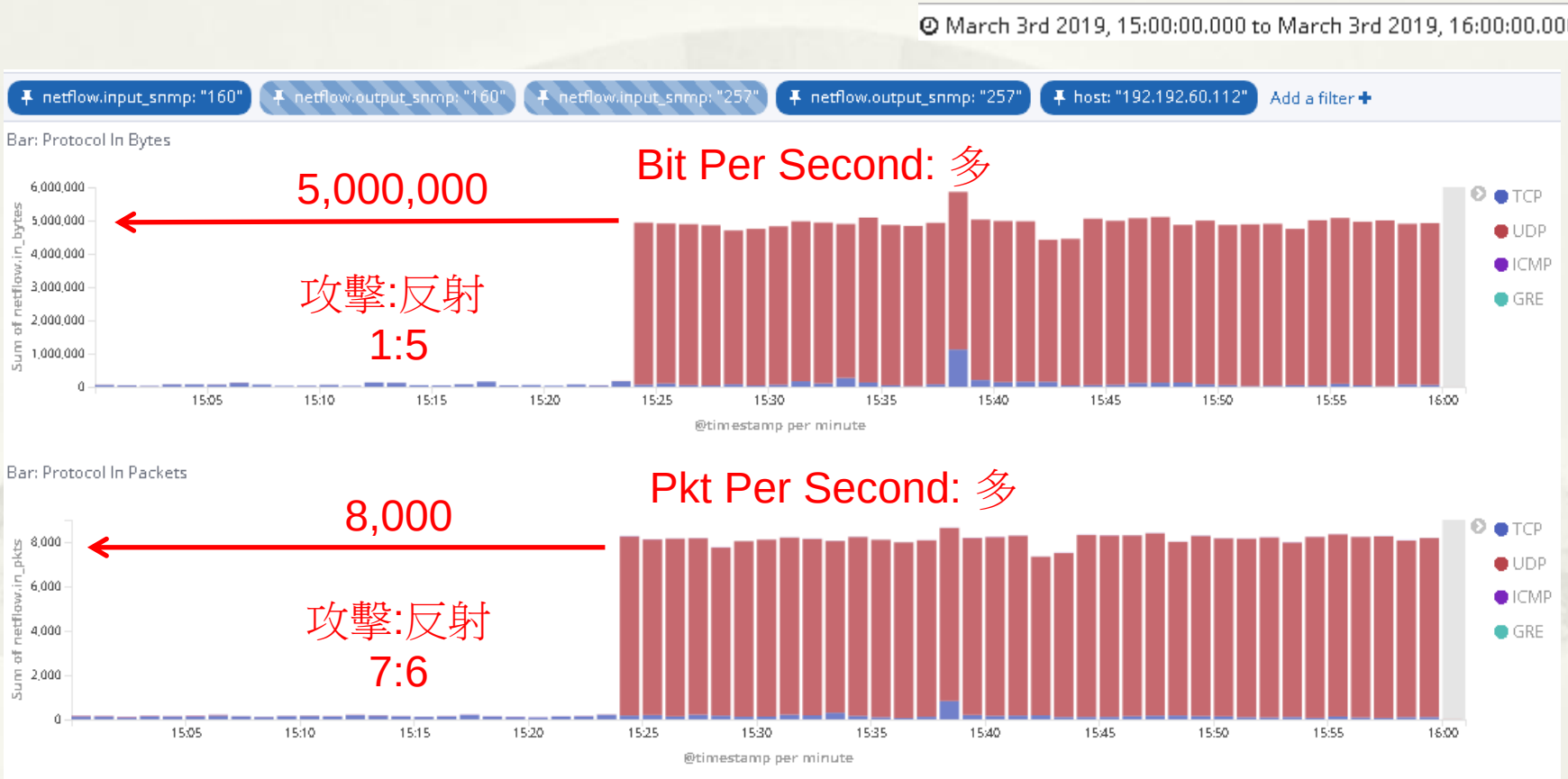
Case. 華夏科大 20190303
外對內 IP



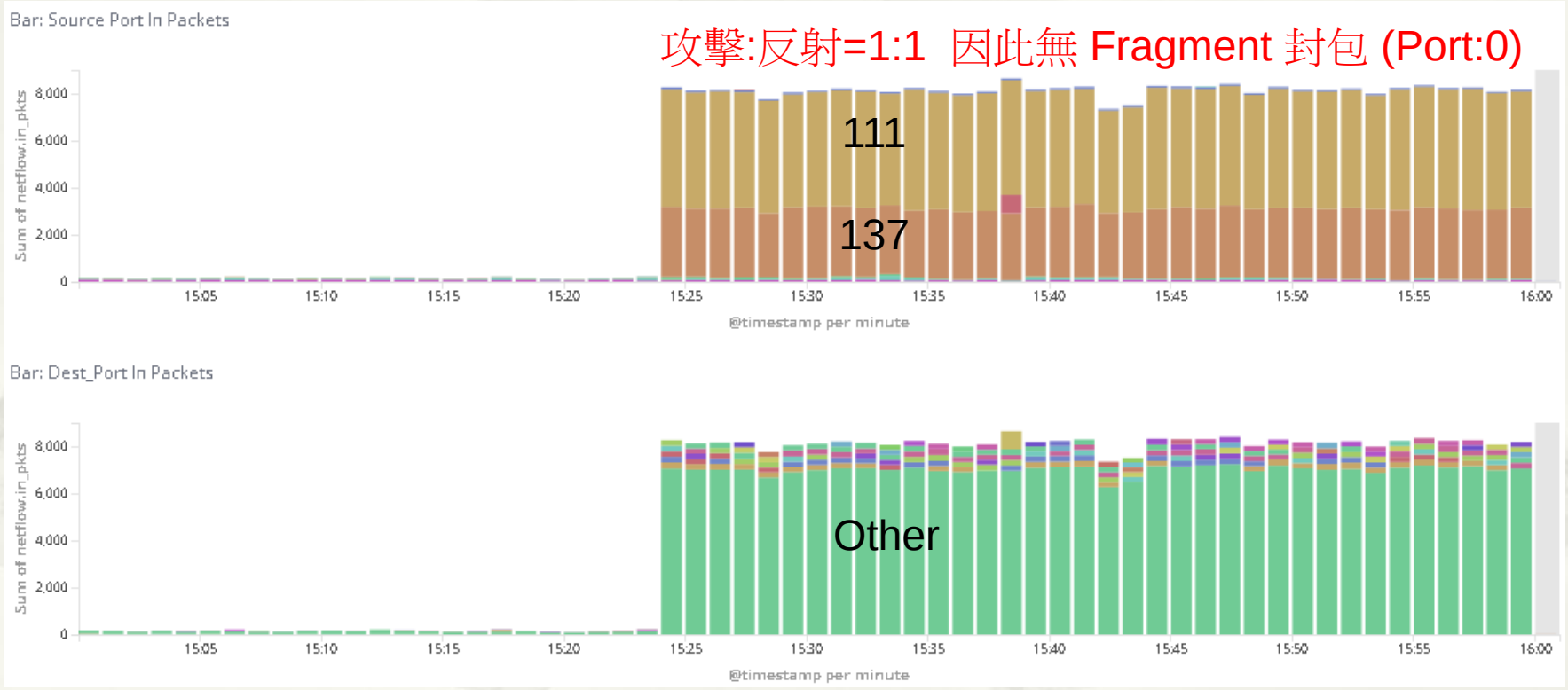
Case. 華夏科大 20190303
外對內 AS



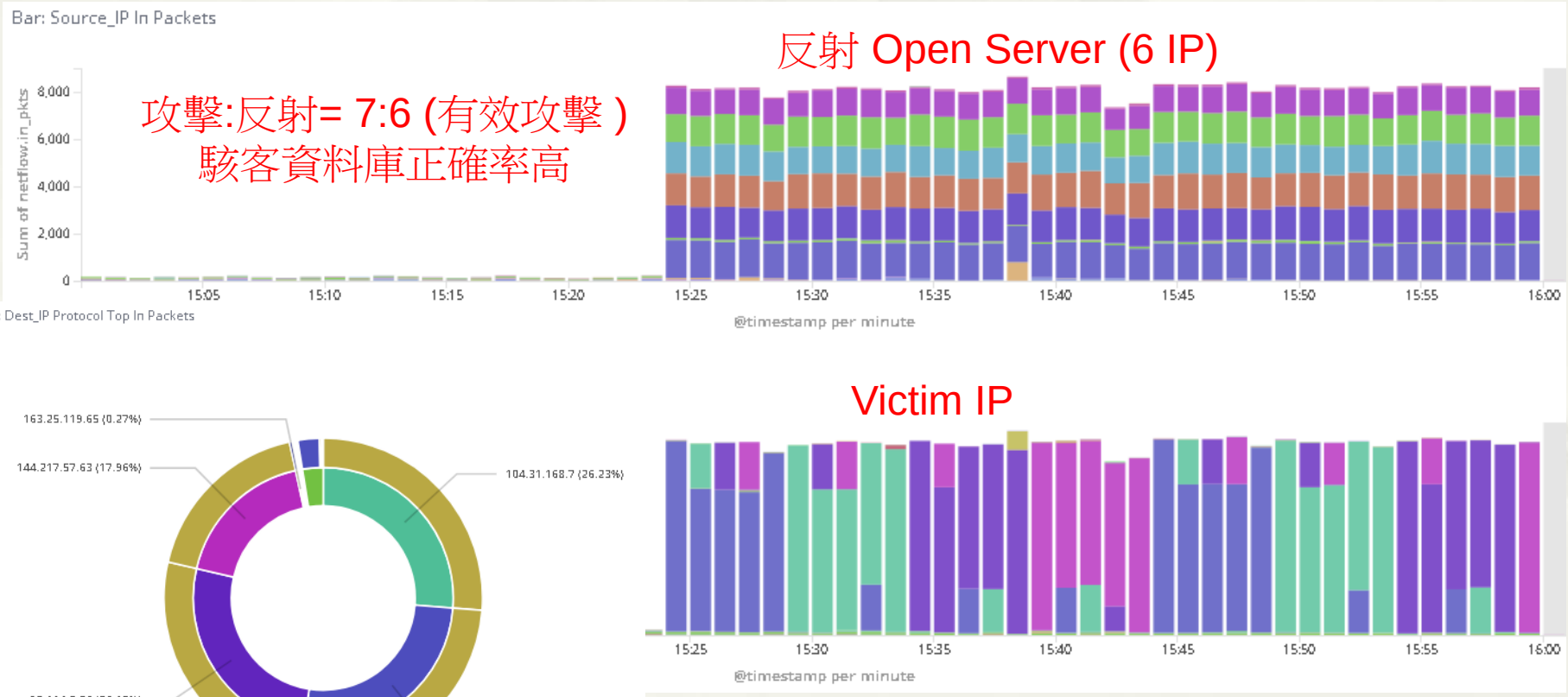
Case. 華夏科大 20190303
內對外 Protocol



Case. 華夏科大 20190303 內對外 Port

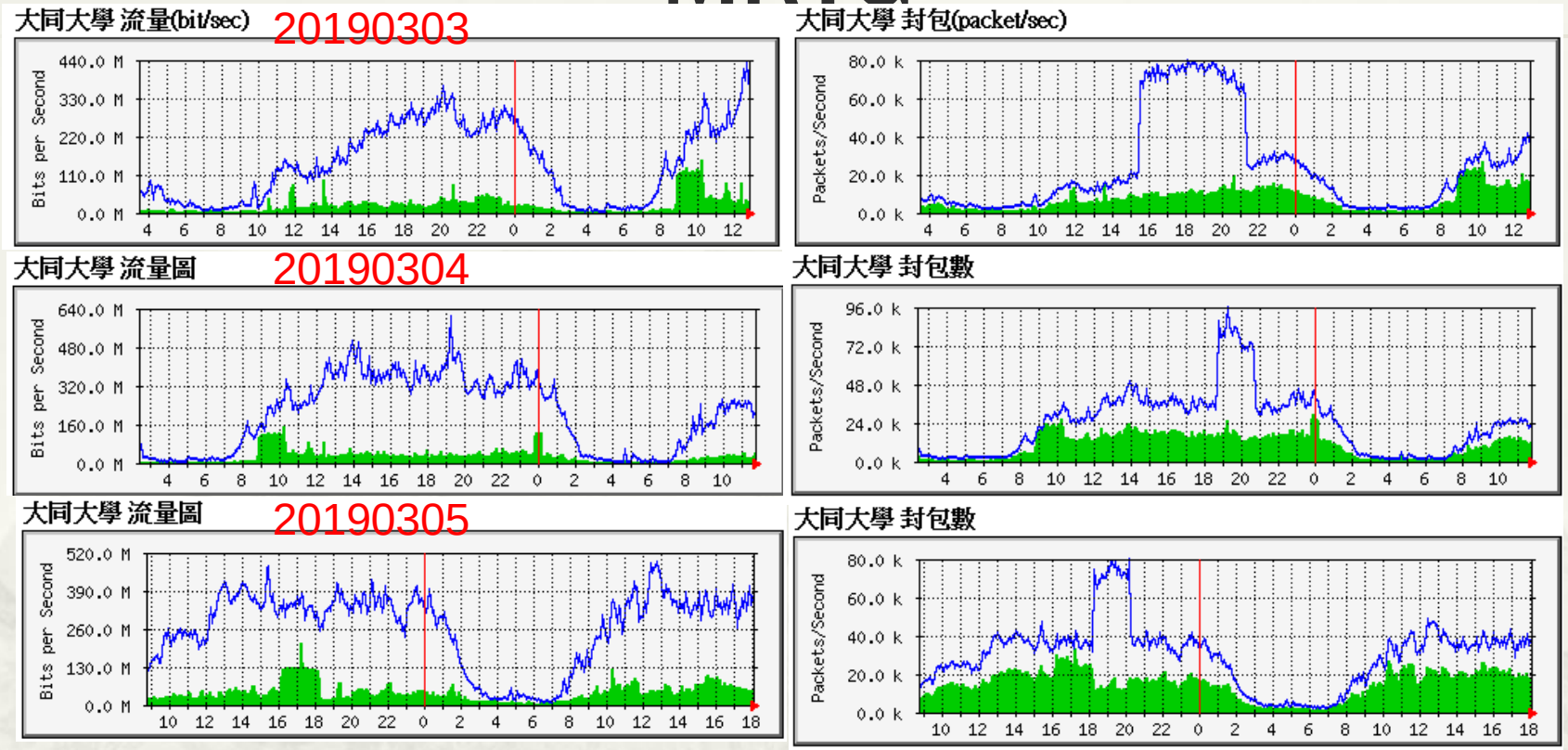


Case. 華夏科大 20190303 內對外 IP



Case.大同大學 (無效反射)

MRTG

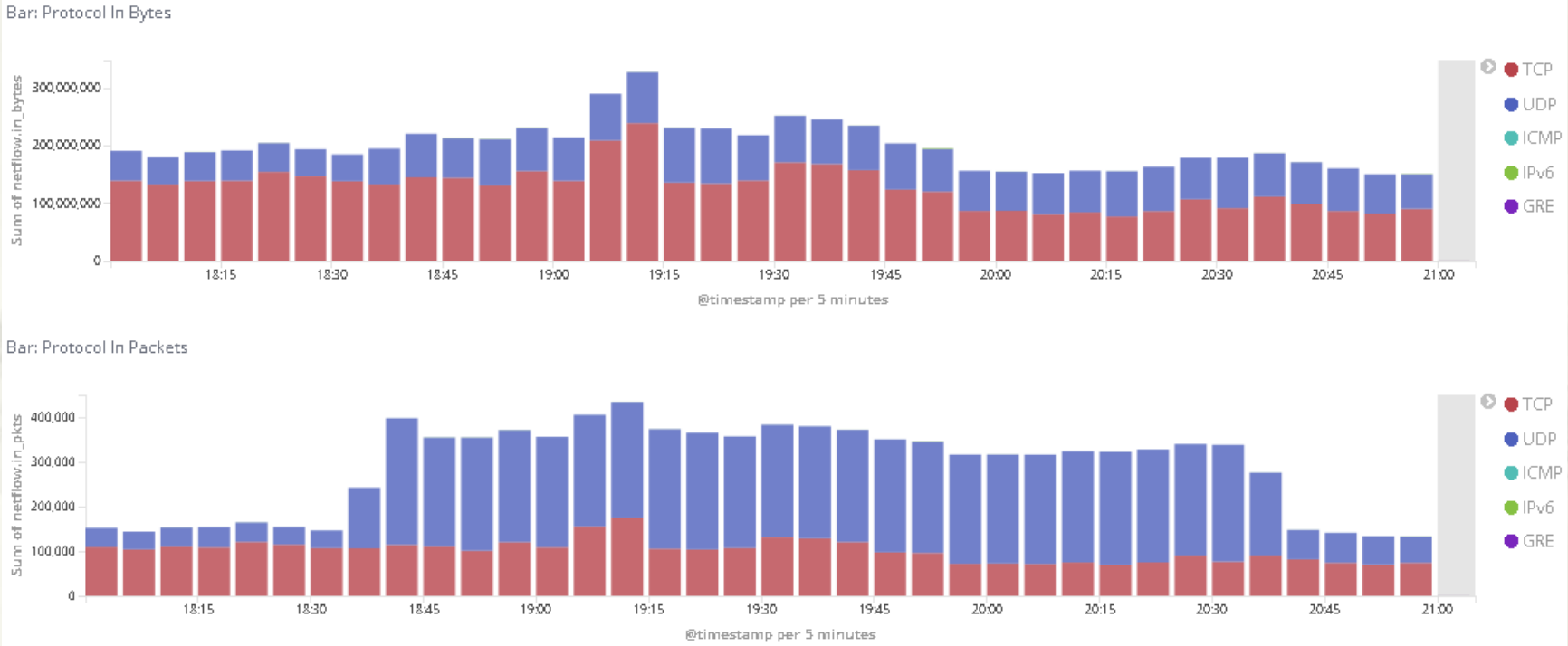


* 無效的反射攻擊，可能原因:
  * 反射 Open Server 無效
  * 校內有 DDoS 設備: A10 3030S (Inline)

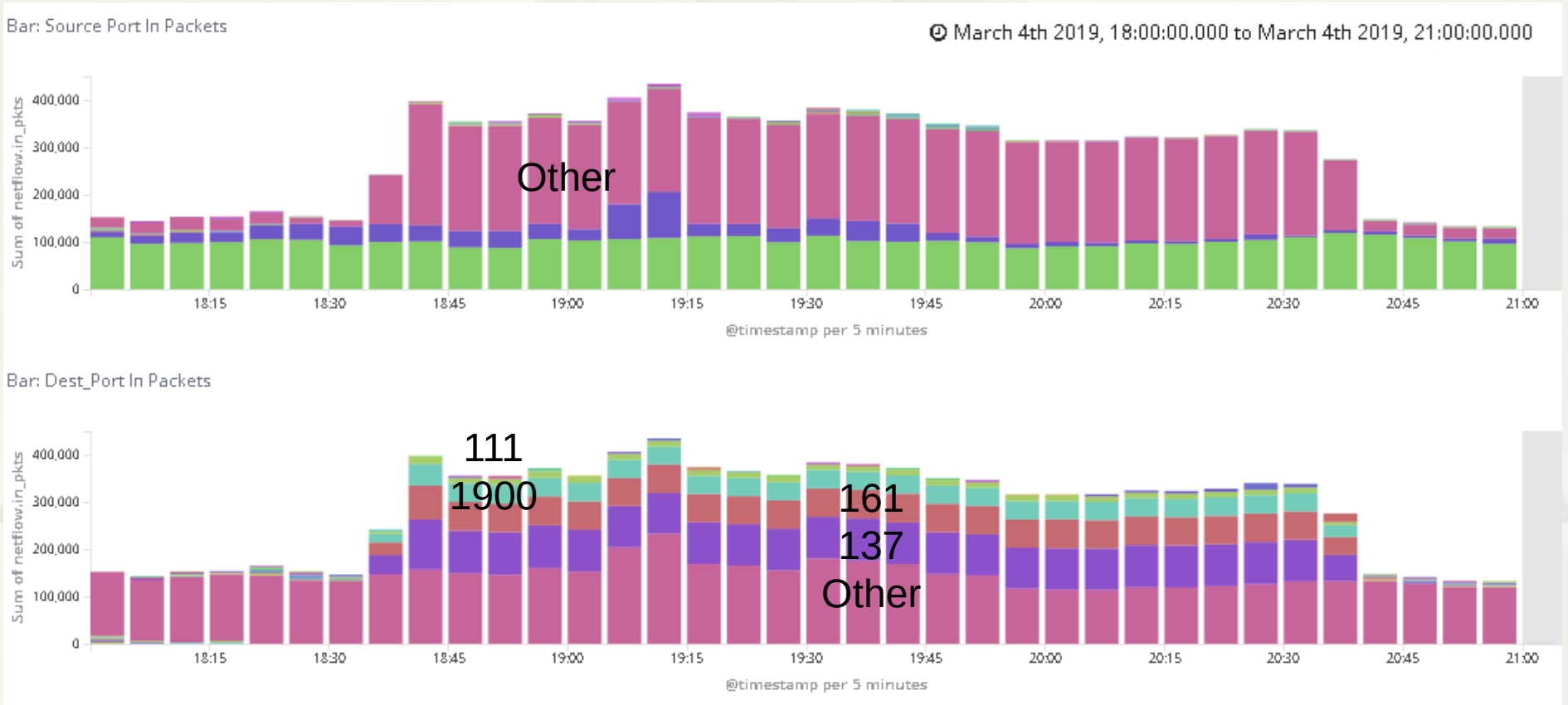
Case.大同大學20190304
外對內 Protocol

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

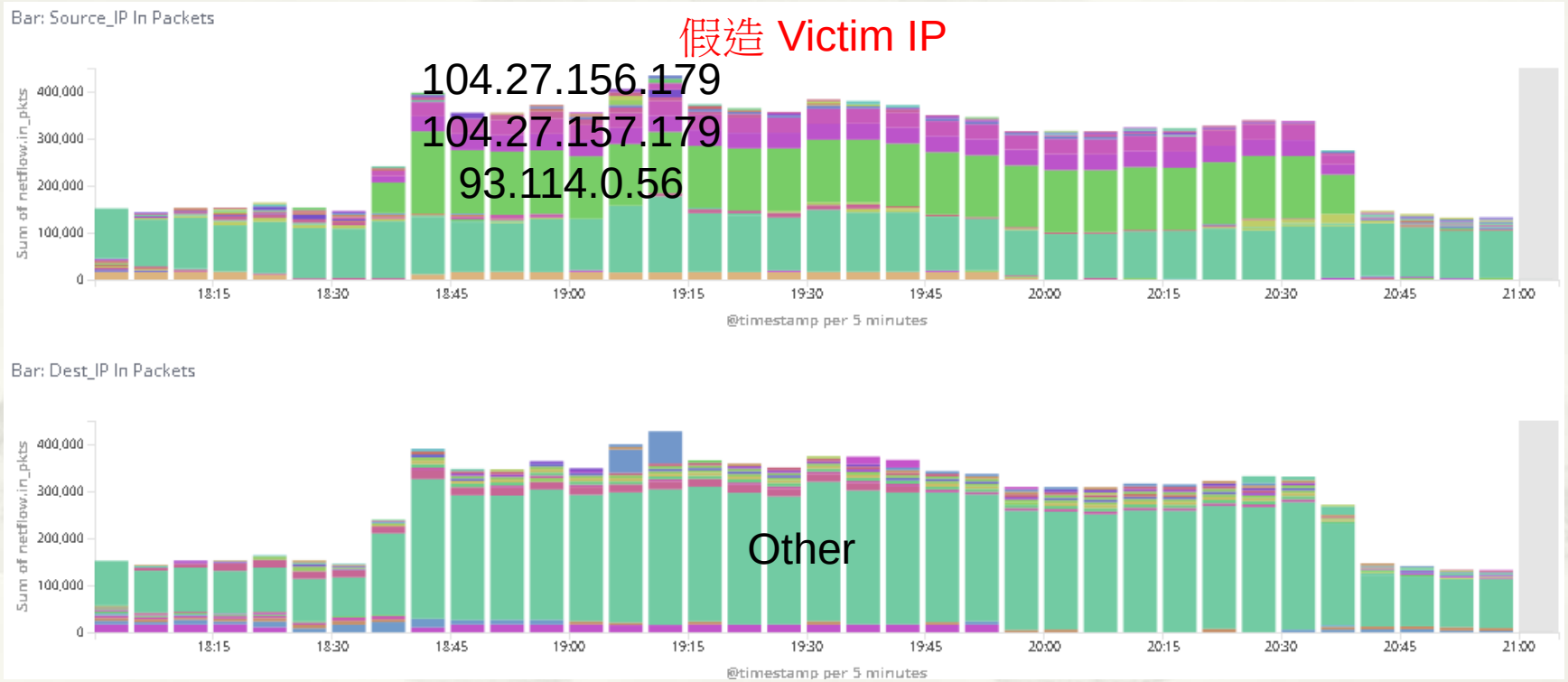
host.keyword: "192.192.60.112" | netflow.l4_dst_port: "161" | netflow.output_snmp: "49" | Add a filter +



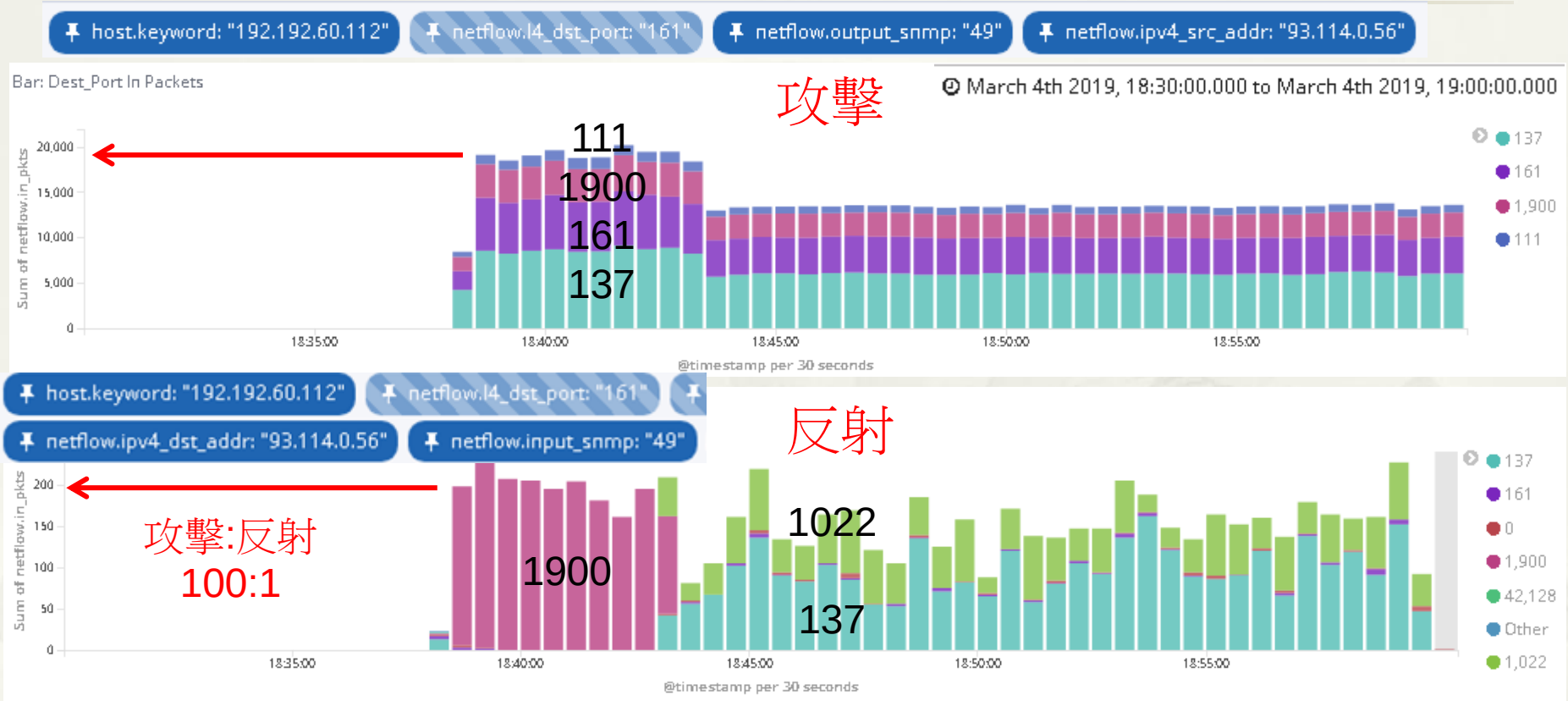
Case.大同大學20190304
外對內 Port



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)

工商服務

108年度課程(已確認)

分類	課程	時間	目前安排
資安	7/9	下午	網站安全程式開發 敦陽翁御舜
區塊鏈	7/11	下午	比特幣的過去、現在與未來 銘傳大學陳伯韋
資安	7/16	下午	駭客攻擊手法新趨勢 敦陽翁御舜
網管	7/18	下午	Great Firewall 的演進 銘傳大學陳伯韋
資安	7/25	上午	惡意攻擊之網路分析實作 劉得民老師
資安	7/25	下午	惡意攻擊之網路分析實作 劉得民老師
資安	8/1	下午	趨勢科技 X-Gen機器學習實驗室核心技術部門經理 張佳彥
SDN	8/5	下午	中華電信 SDN/NFV(軟體定義網路/網路功能虛擬化)之發展現況與應用實例 朱煜煌博士
論文	8/27	下午	國網:以 BDTS 進行長時間惡意網域 IP 變換行為偵測 張成睿
資安	9/4	下午	資策會:資安威脅情資掌握與案例分析 黃馨瑩博士

台灣智慧光網
電路優惠價格

業務部 熊佳義
james.hsiung@taifo.com.tw
0988-316-922
TEL: 886-2-7716-2666 ext.8827

台灣智慧光網
電信光纖(點對點)-產品說明

「電信光纖」產品說明：

以乙太網路（L2 Ethernet）之連接，提供高品質、高穩定度且彈性之充足頻寬；並以Switch為接取設備，提供備援路由，依照企業客戶的需求「端點對端點」的第二層可滿足對網路需求度高的客戶。

項目	Taifo	
頻寬	一次性 安裝設定費	電 信 光 纖 點對點專線月租費
100 Mbps	$1,500	$5,000
300 Mbps	$1,500	$10,000
500 Mbps	$1,500	$18,000
1Gbps	$1,500	$30,000

PS:

1. 此專案優惠價，限連接TANet 區網申請。
2. 需簽約二年 。

Confidential, Internal Circulating only

台灣智慧光網
專業型光纖上網服務

產品說明：

提供客戶高速、價廉的光纖上網連接；提供Cost Down的最佳選擇。

台北光纖上網	一 次 性 安裝設定費	電路＋連線 月 租 優 惠
300M/300M 3 IP	**Free**	**$1,672**
300M/300M 6 IP	**Free**	**$1,812**

PS:

1. **此專案優惠價，限TANet學術校區申請。**
2. **需簽約二年 。**

Confidential, Internal Circulating only

簡報完畢
謝謝