108年度臺北區網Ⅰ
年度報告

- 單位：國立臺灣大學
- 計資中心主任：顏嗣鈞教授
- 網路組組長：謝宏昀教授
- 報告人：游子興
- Email：davisyou@ntu.edu.tw
- 電話：02-33665008

- 日期：2018/11/22

大綱

* 1.經費與人力
* 2.網路管理
* 3.資安服務
* 4.特色服務
* 5. 107年評審委員建議與回覆
* 6.未來目標與建議

1.1 區網經費

年度	教育部核定	實支總額	人事費繳回	達成率	扣除繳回達成率
105	1,579,088	1,367,903	87,140 (8、9月)	86.67%	91.7%
106	1,580,000	1,309,762	261,420 (1至6月)	82.90%	99.33%
107	1,720,000	1,577,987	51,040 (8月)	91.74%	95%
108	**1,720,000**	1,314,090 (11月)	0	97% (預估)	97% (預估)

* 因 105~107年因聘僱不到資安人員導致達成率偏低
* 108年度已無此現象

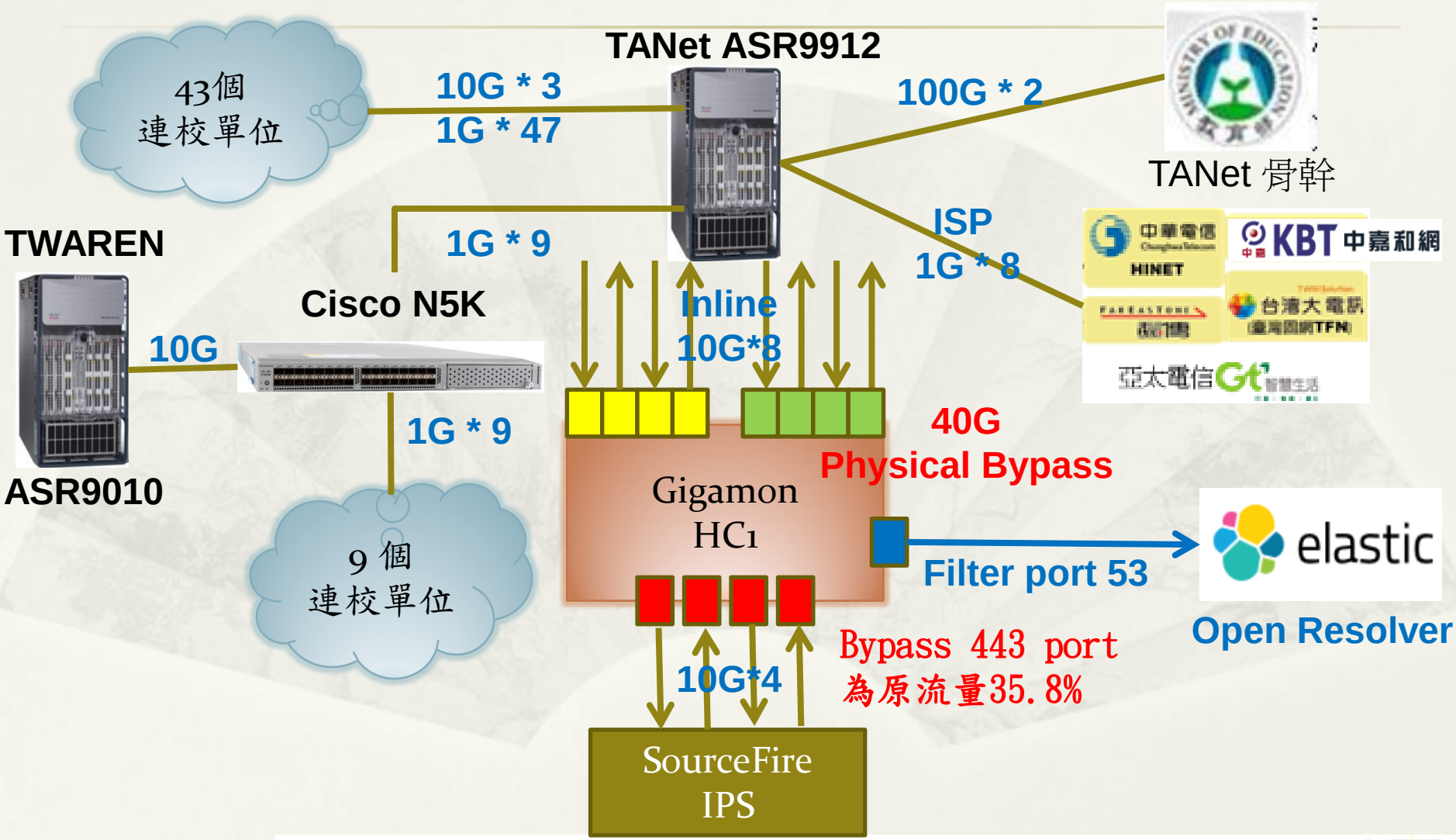
1.2 區網人力

- 計資中心主任：顏嗣鈞教授
  - E-mail：hcyen@ntu.edu.tw
  - 電話：(02) 33665001
- 網路組組長：謝宏昀教授
- 網路管理負責人：游子興
  - E-mail：davisyou@ntu.edu.tw
  - 電話：(02) 33665008
- 資安管理負責人：李墨軒
  - E-mail：molee@ntu.edu.tw
  - 電話：(02) 33665012
- 編制內專職及約聘僱人員8名，其中區網經費及資安經費各約聘2名

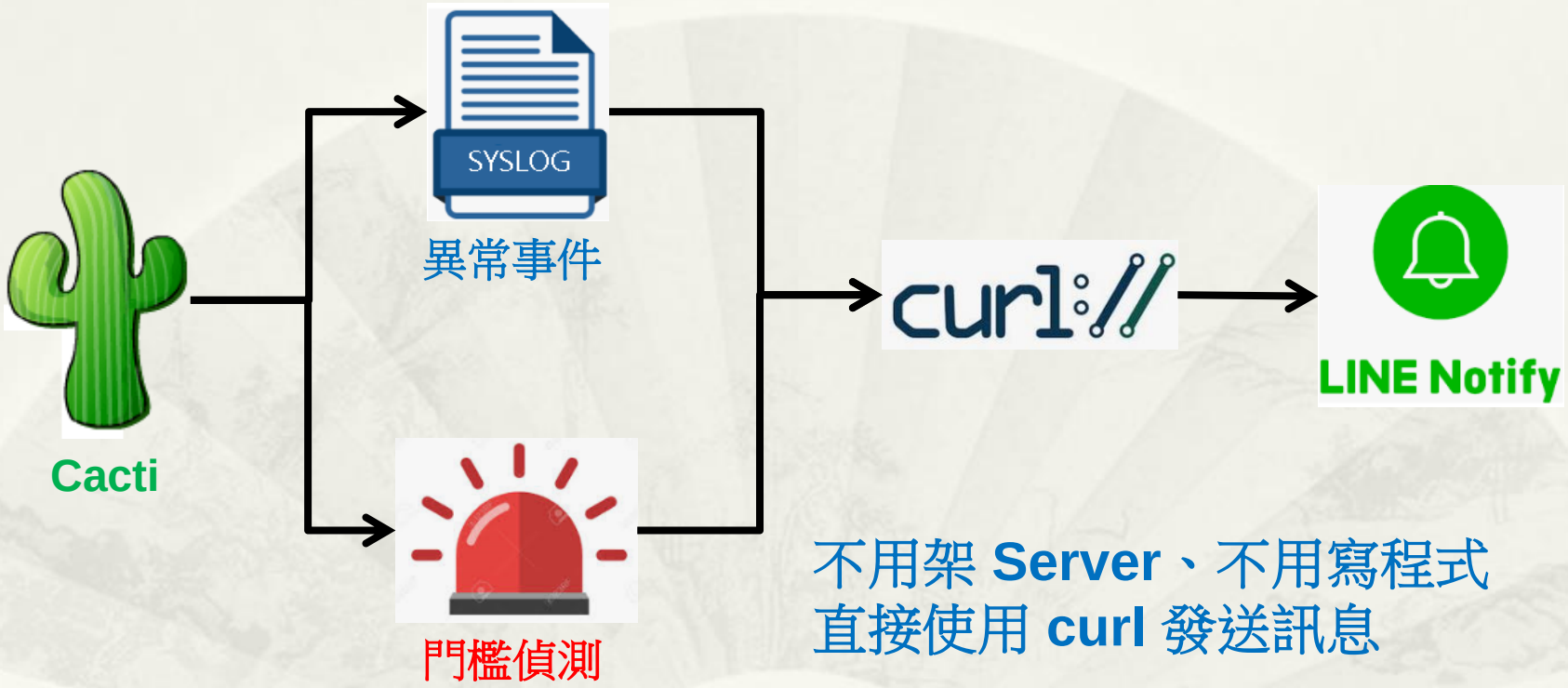
2.網路管理

* 1. 網路架構
* 2. Cacti 結合 Line Notify
* 3. 網路設備設定檔自動備份
* 4. 網管經驗分享
  * 資安設備阻擋封包分析
* 5. TANet 2019論文發表
  * 以校園網路連線大數據驗證六度分隔理論

2.1 網路架構


43個
連校單位
10G * 3
1G * 47
TANet ASR9912
100G * 2
TANet 骨幹
TWAREN
1G * 9
ISP
1G * 8
Cisco N5K
Inline
10G*8
10G
ASR9010
1G * 9
40G
Physical Bypass
Gigamon
HC1
9 個
連校單位
Filter port 53
elastic
Open Resolver
Bypass 443 port
為原流量35.8%
10G*4
SourceFire
IPS

2.2 Cacti 結合 Line Notify



不用架 **Server**、不用寫程式
直接使用 **curl** 發送訊息

107年評審委員建議:

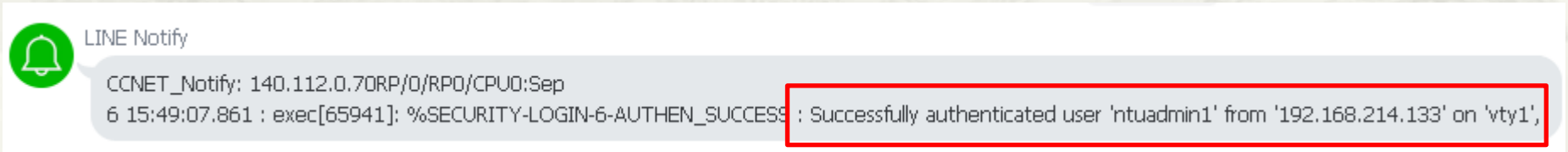
5.區網流量大幅成長，對於網管及資安服務應有配套規劃。

Cacti SYSLOG 異常事件

* 監控 ASR Router Log 異常事件

Alert Name**	Severity	Method	Threshold Count	Enabled	Match Type	Search String
Alert-AUTHEN_SUCCESS	Warning	Individual	N/A	Yes	Contains	AUTHEN_SUCCESS
Alert-LINEPROTO-5-UPDOWN	Warning	Individual	N/A	Yes	Contains	LINEPROTO-5-UPDOWN
Alert-LINK-3-UPDOWN	Warning	Individual	N/A	Yes	Contains	LINK-3-UPDOWN
Alert-LOGIN_SUCCESS	Warning	Individual	N/A	Yes	Contains	LOGIN_SUCCESS
logged command	Warning	Individual	N/A	Yes	Contains	logged command
OSPF-5-ADJCHG	Warning	Individual	N/A	Yes	Contains	OSPF-5-ADJCHG
OSPFv3-5-ADJCHG(ipv6)	Warning	Individual	N/A	Yes	Contains	OSPFv3-5-ADJCHG

事件: 有人成功登入 **Router**



Cacti SYSLOG Alert Action

Console > Syslog Alerts > (Edit) — Logged in as admin

- Create
- Management
- Device Tracking
- Tracking Tools
- Data Collection
- Templates
- Automation
- Presets
- Import/Export
- Syslog Settings
- Alert Rules
- Removal Rules
- Report Rules
- Configuration
- Utilities

Alert Details

Alert Name	Alert-LINK-3-UPDOWN
Severity	Warning
Reporting Method	Individual
Threshold	1
String Match Type	Contains
Syslog Message Match String	LINK-3-UPDOWN
Alert Enabled	Enabled
Re-Alert Cycle	Not Set
Alert Notes	

Alert Actions

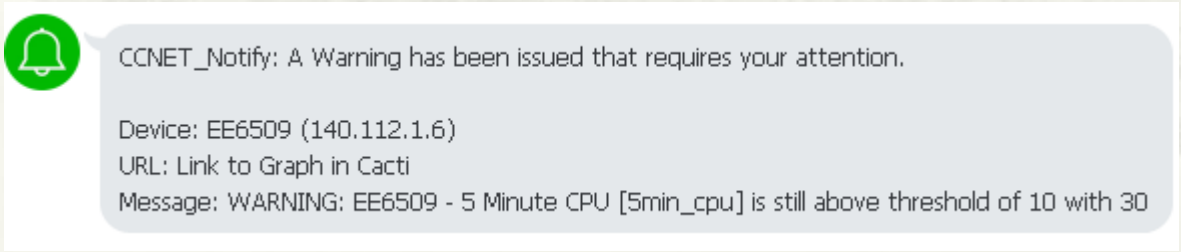
Open Ticket	No
Emails to Notify	davisyou@ntu.edu.tw
Alert Command	`/usr/share/cacti/cacti_line_syslog.sh '<HOSTNAME>' '<MESSAGE>'`

Shell Script: `/usr/share/cacti/cacti_line_notify.sh <HOSTNAME> <MESSAGE>`

Line Notify Shell Script

- cacti_line_notify.sh
  - curl -v https://notify-api.line.me/api/notify \
  - -H 'Authorization: Bearer *Access_Token*' \
  - -F 'message='"$1" \
  - -F 'message='"$2“

事件: CPU Usage 異常

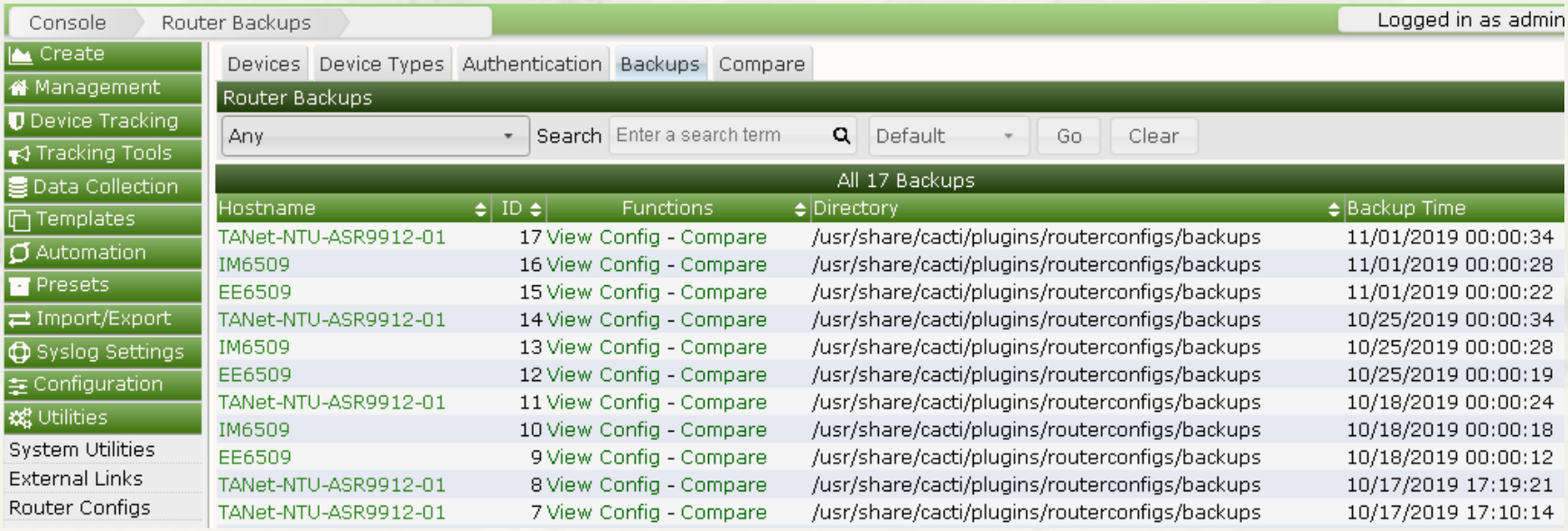


Cacti 結合 Line Notify
優點

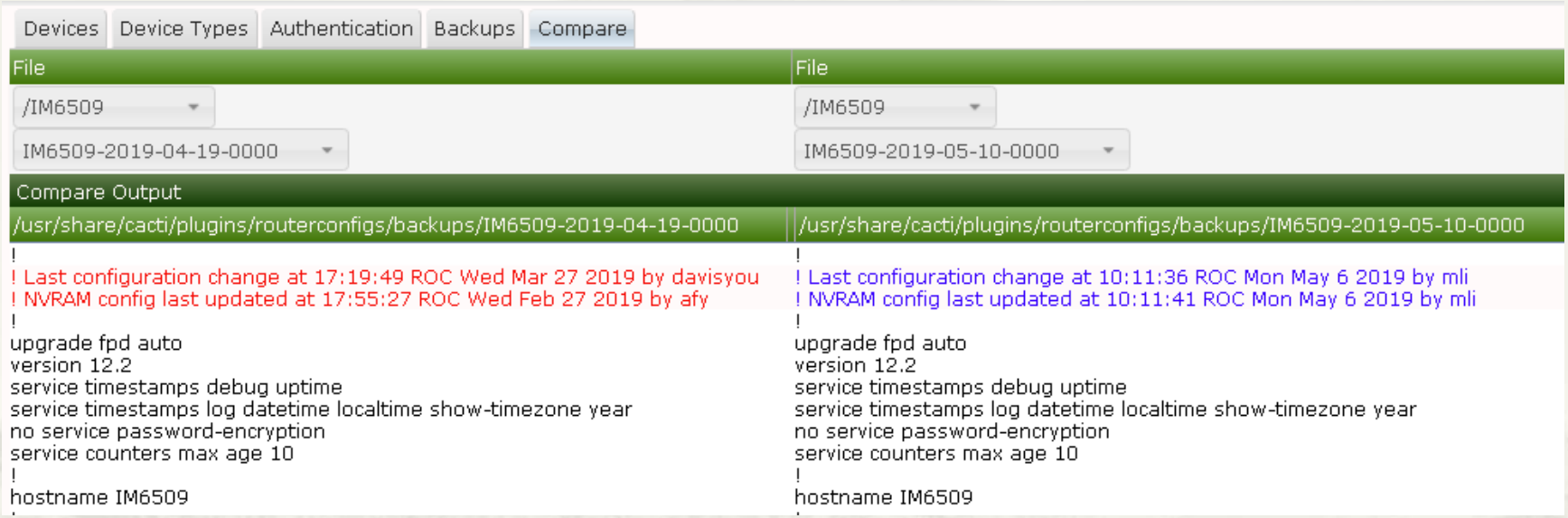
* 不需架設 Syslog Server
* 不需監控 Email Server 及 Parse 內容
* 不用寫程式(use curl only)
* 維護簡單且更即時

2.3 網路設備設定檔自動備份
Cacti Router Config

* 每週自動備份設定檔. (符合 ISO27001 要求)
* 支援 Telnet or SSH 連線設備
  * Support: Cisco ASR/IOS/CatOS/Nexus、 HP Comware



支援比較不同時間備份檔差異



2.4 網管經驗分享
資安設備阻擋封包分析

* 圖書館反應某資料庫網頁無法連線
* 封包側錄:

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

* 遠端桌面可正常連線
* 封包側錄:

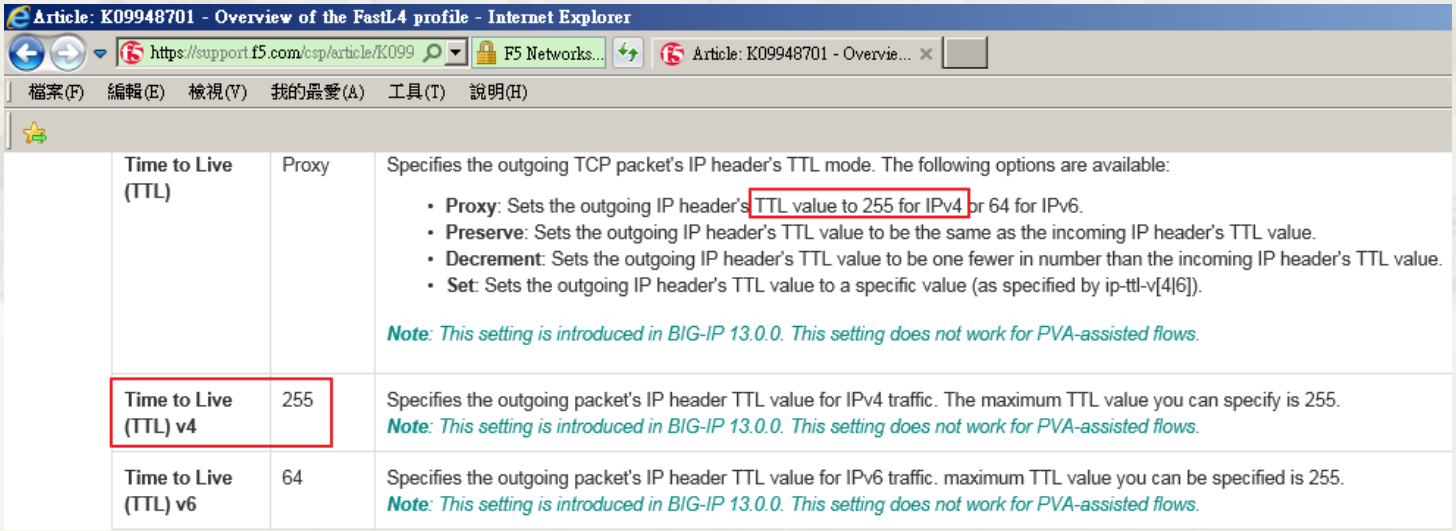
No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
64	1.720033	2	128	172.16.0.2	53549	140.112.114.80	3389	TCP	66	53549 → 3389 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
65	1.721081	2	123	140.112.114.80	3389	172.16.0.2	53549	TCP	66	3389 → 53549 [SYN, ACK] Seq=0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

* 兩者差異?

魔鬼藏在細節中

TTL 不同

- 該網頁為 Windows Server，TTL 初始值 128，但發出 Reset 封包 TTL=250，推測前端有一資安設備誤擋，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 修正後

* telnet 140.112.114.80 3389
  * TTL=123 → Windows

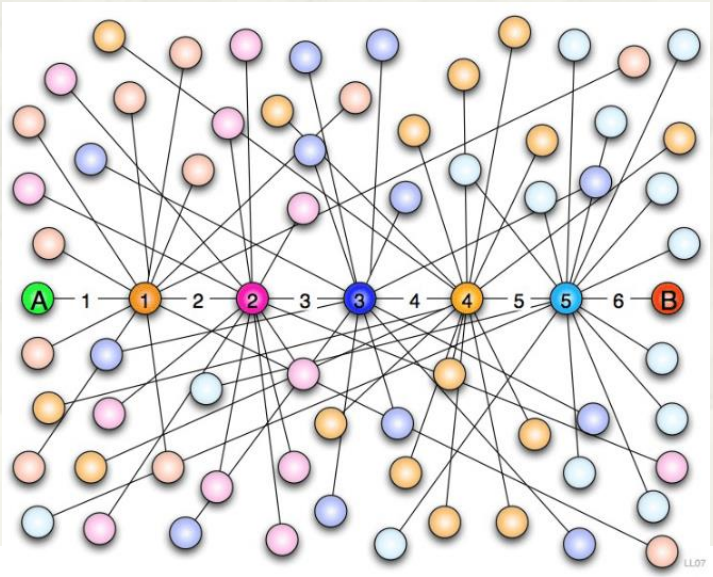
No.	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
18	6.399730	128	172.16.0.2	64796	140.112.114.80	3389	TCP	66	64796 → 3389 [SYN] Seq=0 Win=8192 Len=0 MSS=146
19	6.400645	123	140.112.114.80	3389	172.16.0.2	64796	TCP	66	3389 → 64796 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le
20	6.400702	128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

2.5 TANET2019論文發表

* 以校園網路連線大數據驗證六度分隔理論
  * 六度分隔理論所描述之現象，提出不同的驗證方法，並運用大數據資料統計校園網路連線資訊，包括IP 路由節點數(TTL Counts)與 BGP AS-Path 長度，來驗證六度分隔理論之正確性。



3.資安服務

* 1. 108年度資安事件統計
* 2.DDoS 攻擊方式分析
* 3.DDoS 攻擊案例分析

3.1 106~108年度資安事件統計

	106	107	108
1、2級資安事件處理			
通報平均時數	2.70小時	1.343 小時	0.586 小時
應變處理平均時數	0.05小時	0.026 小時	0.017 小時
事件處理平均時數	2.76小時	1.369 小時	0.602 小時
通報完成率	98.90%	99.86%	99.969%
事件完成率	99.91%	99.92%	99.627%
3、4級資安事件通報	無	無	無
資安事件通報審核平均時數	0.60小時	0.519小時	0.206小時
資料更新完整校數	72.92%	73.47%	81.633%

107年評審委員建議:

8. 對資安事件的通報處理效率應思考如何精進。

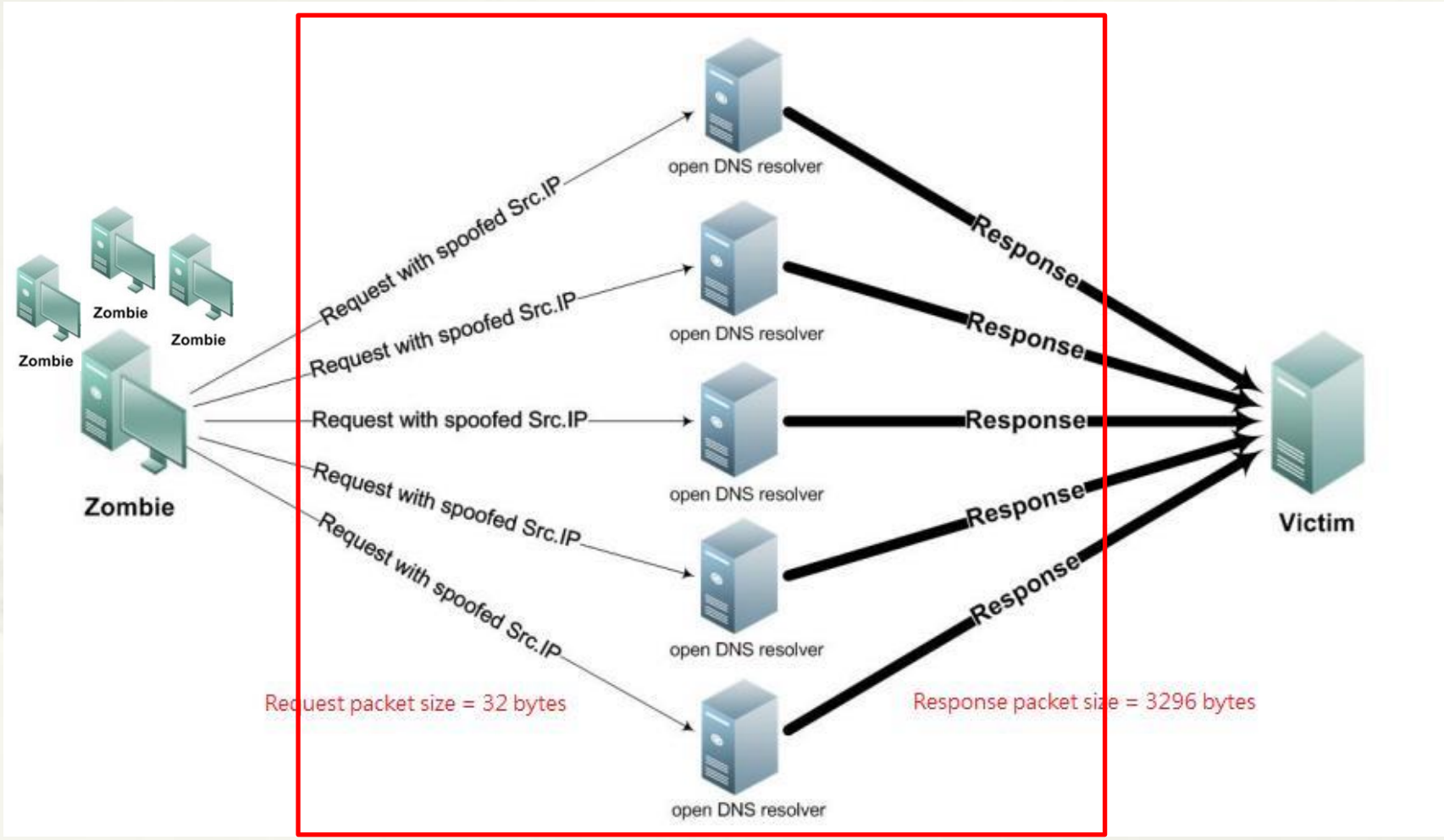
10. 資安通報及事件處理平均時數，建議仍需持續努力

3.2 DDoS 攻擊方式分析

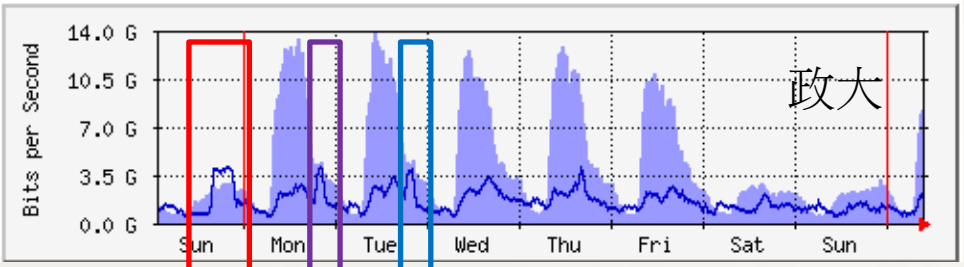
* 反射攻擊
  * 外對內: 遭受反射攻擊
  * 外對內 + 內對外: 內部有反射 Server 被利用於攻擊受害者
  * 內對外: 內部有 BOT 利用外部反射 Server 攻擊受害者
* 直接攻擊
  * 外對內: 遭受攻擊
  * 內對外: 內部有 BOT 攻擊受害者

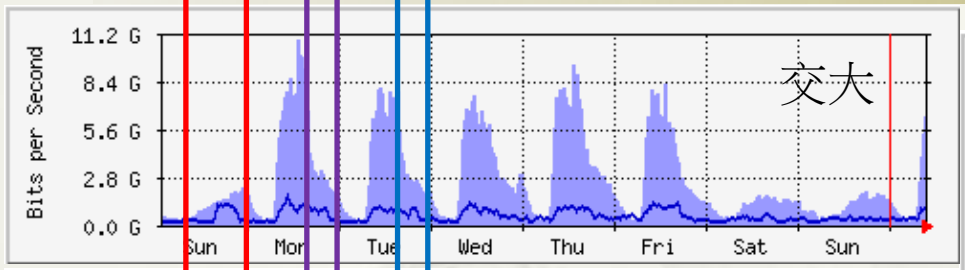
3.3 DDoS 攻擊案例分析

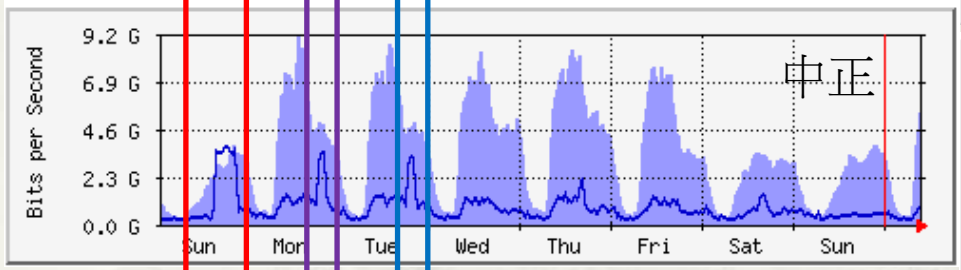
內部有反射 Server 被利用於攻擊受害者

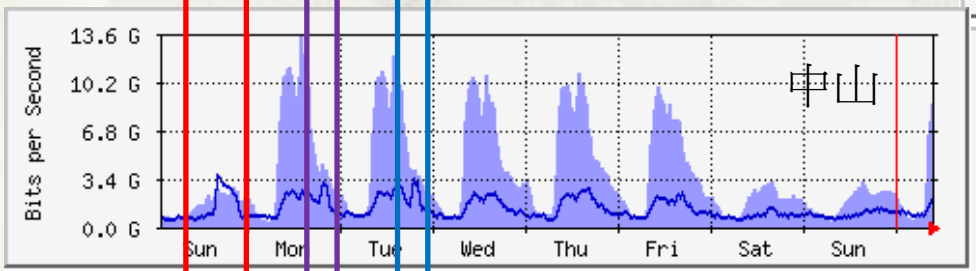


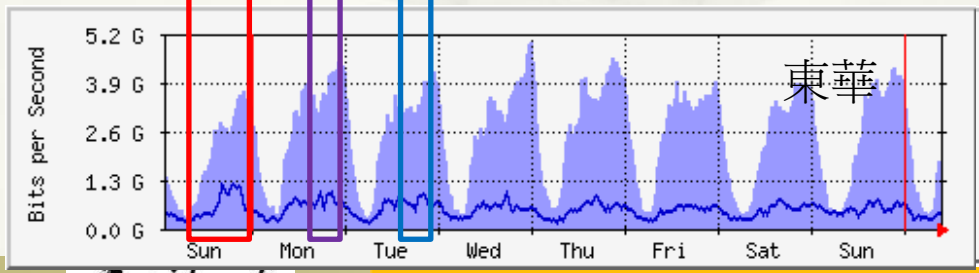
20190303~0305
各區網中心

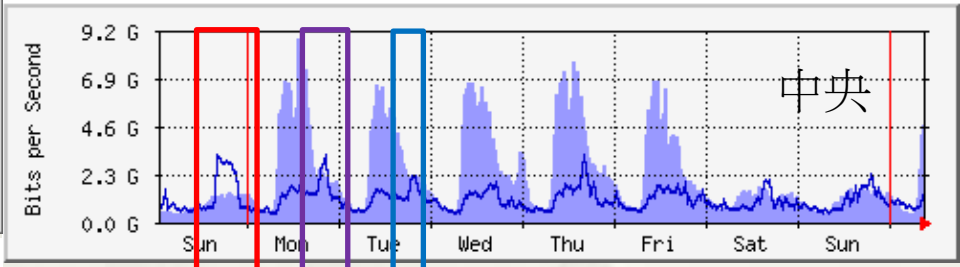


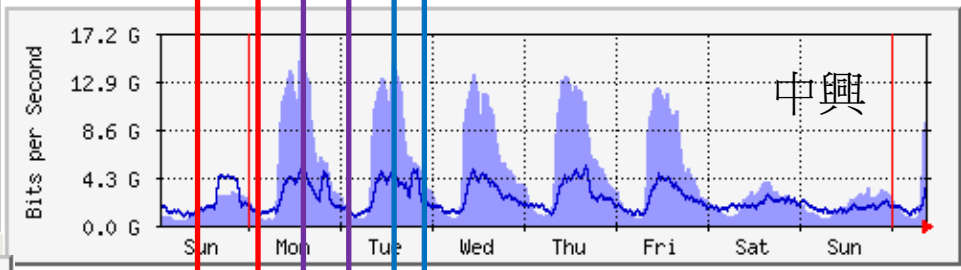


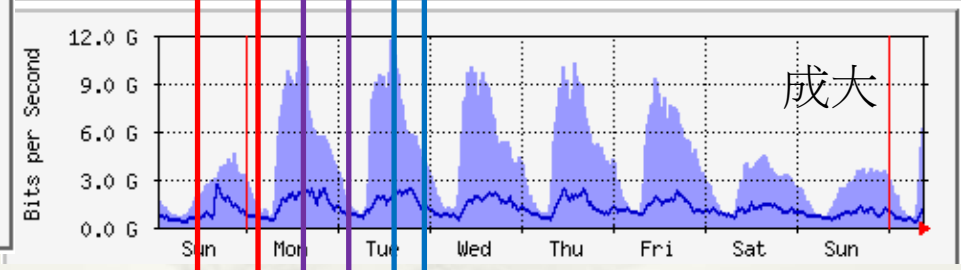


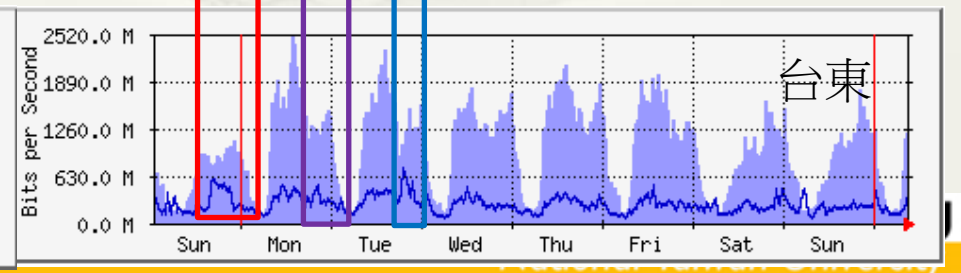






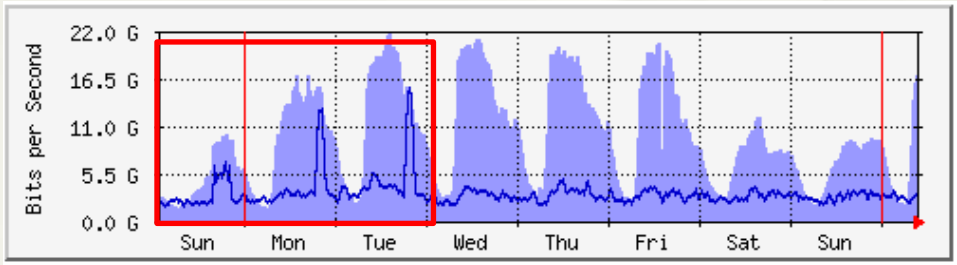






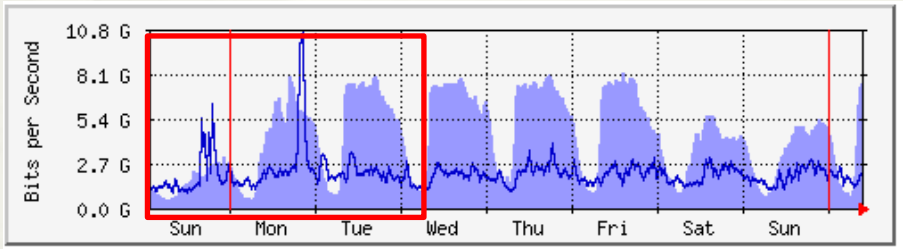
TANet DDoS 攻擊出口 Max 25~30 Gbps

TANet to Internet IPv4 [30G]



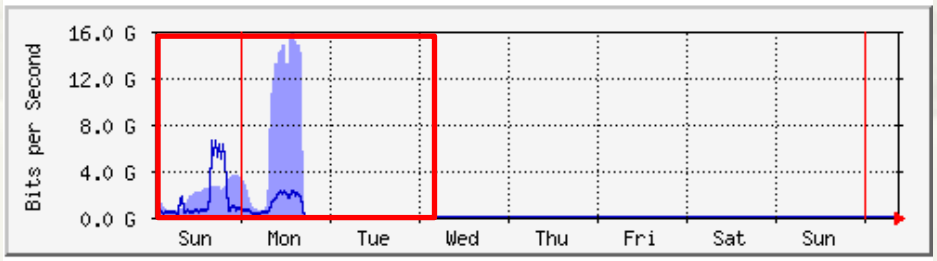
	最大	平均	目前
Internet ⇒ TANet	21.8 Gb/秒 (67.7%)	9419.5 Mb/秒 (29.2%)	16.9 Gb/秒 (52.4%)
TANet ⇒ Internet	15.2 Gb/秒 (47.2%)	3093.5 Mb/秒 (9.6%)	3132.5 Mb/秒 (9.7%)

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%)

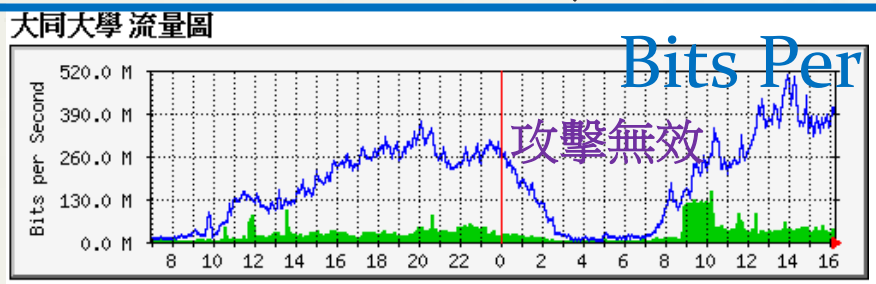
TPIX

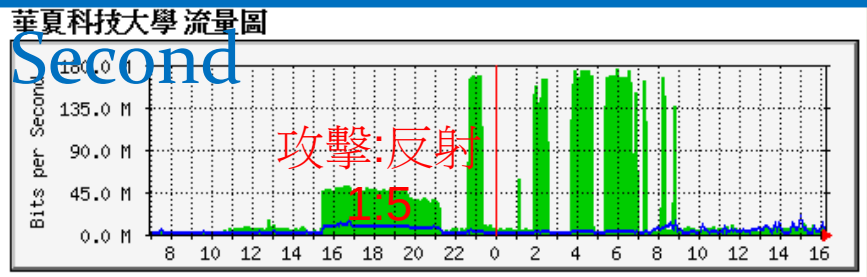


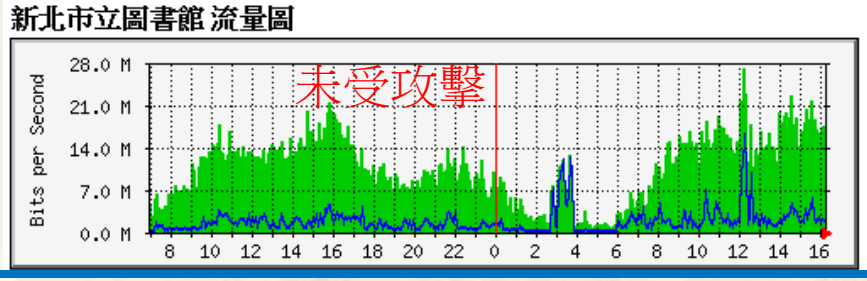
	最大	平均	目前
TPIX ⇒ 教育部 :	15.9 Gb/秒 (49.5%)	4318.9 Mb/秒 (13.4%)	0.0 b/秒 (0.0%)
教育部 ⇒ TPIX :	6513.3 Mb/秒 (20.2%)	1369.3 Mb/秒 (4.3%)	0.0 b/秒 (0.0%)

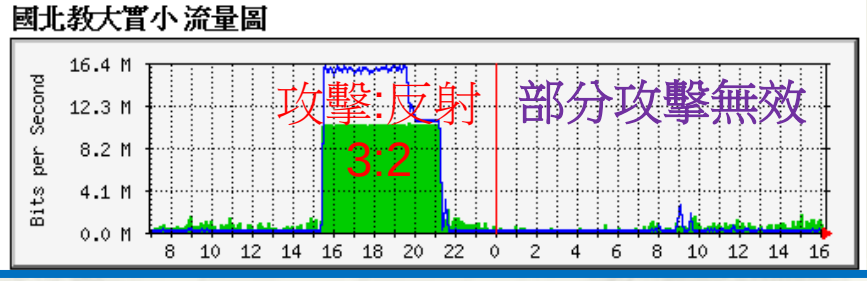
20190303
攻擊:反射 比例分析

Bits Per Second

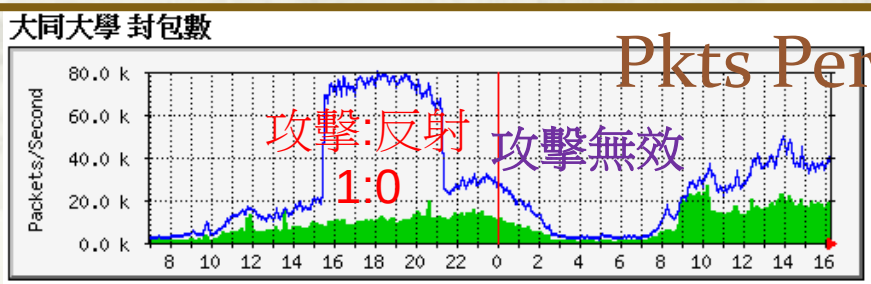


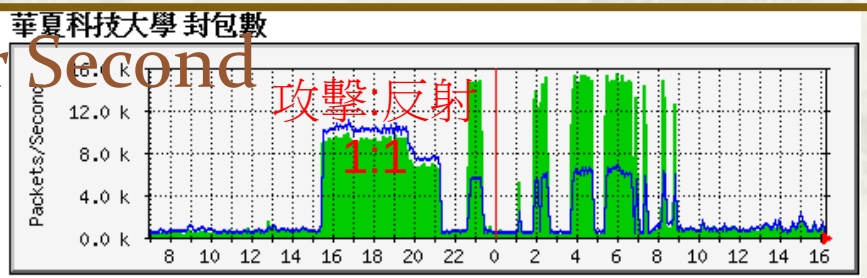


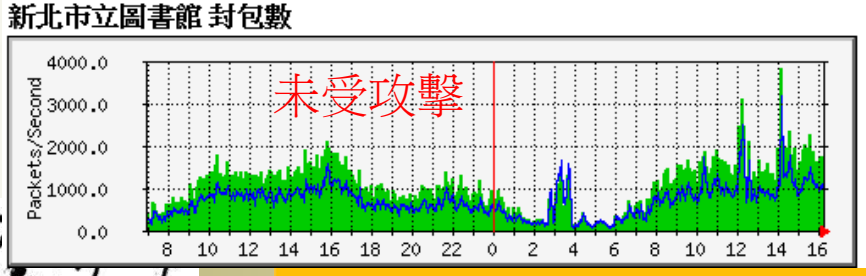


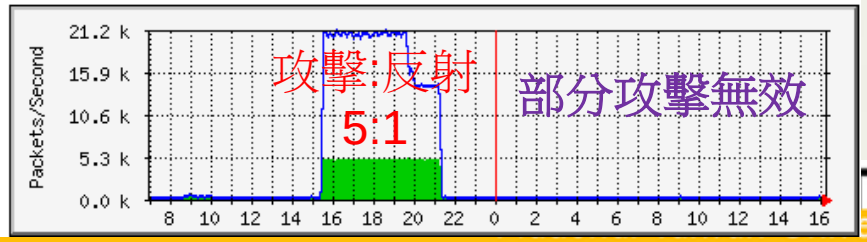


Pkts Per Second



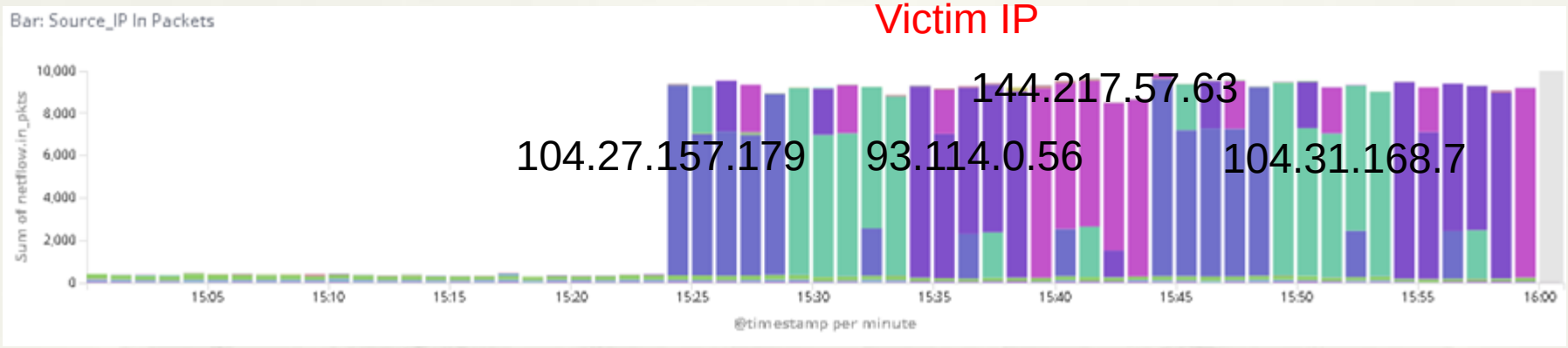


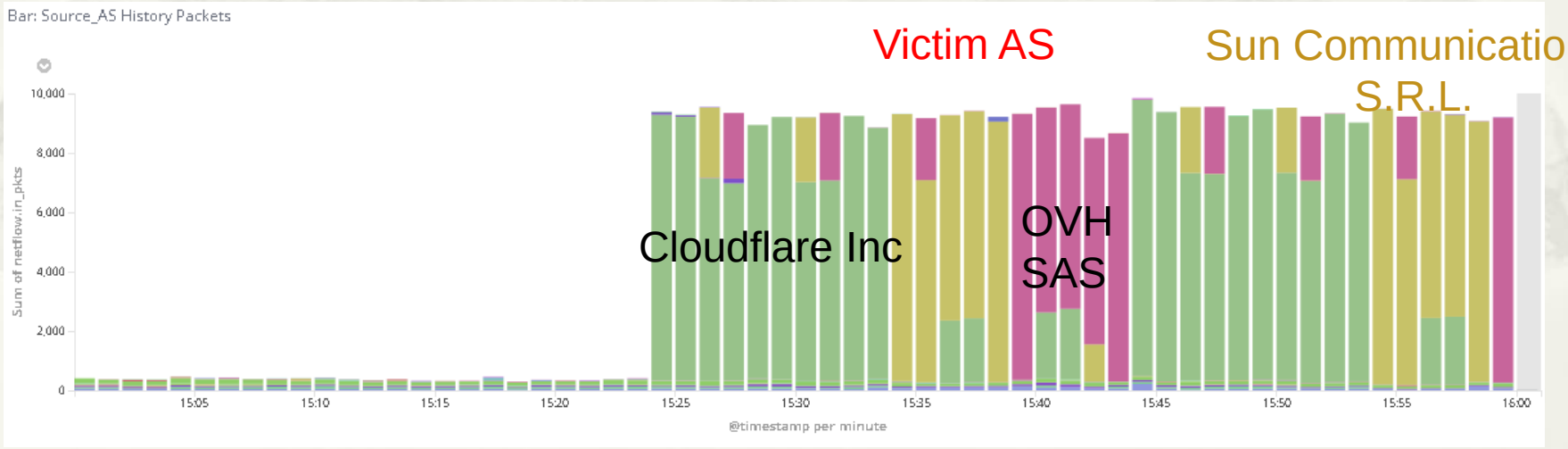




華夏科大
外對內 Port

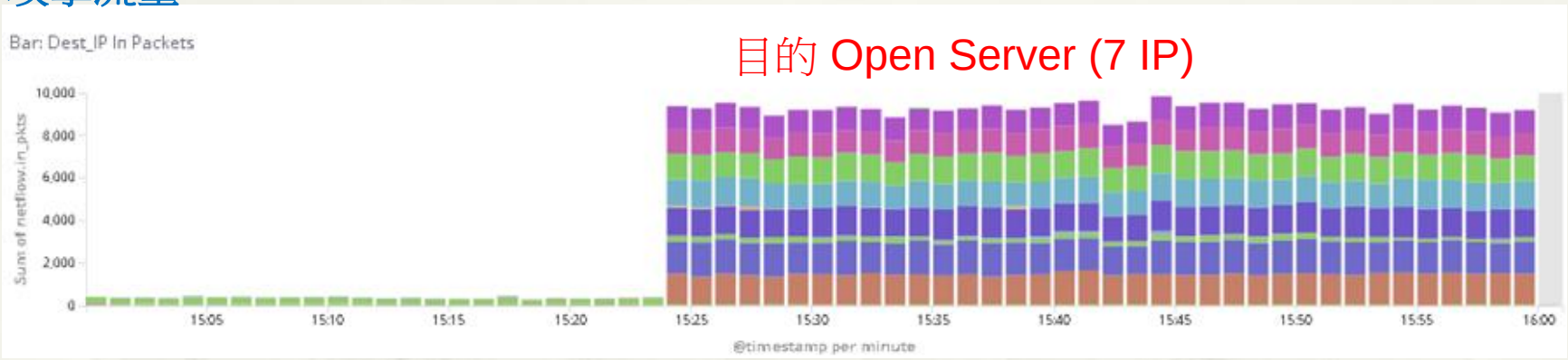
外對內
來源 IP/AS


Bar: Source_IP In Packets
Victim IP
144.217.57.63
104.27.157.179
93.114.0.56
104.31.168.7
Sum of netflow.in_pkts
10,000
8,000
6,000
4,000
2,000
0
15:05
15:10
15:15
15:20
15:25
15:30
15:35
15:40
15:45
15:50
15:55
16:00
@timestamp per minute

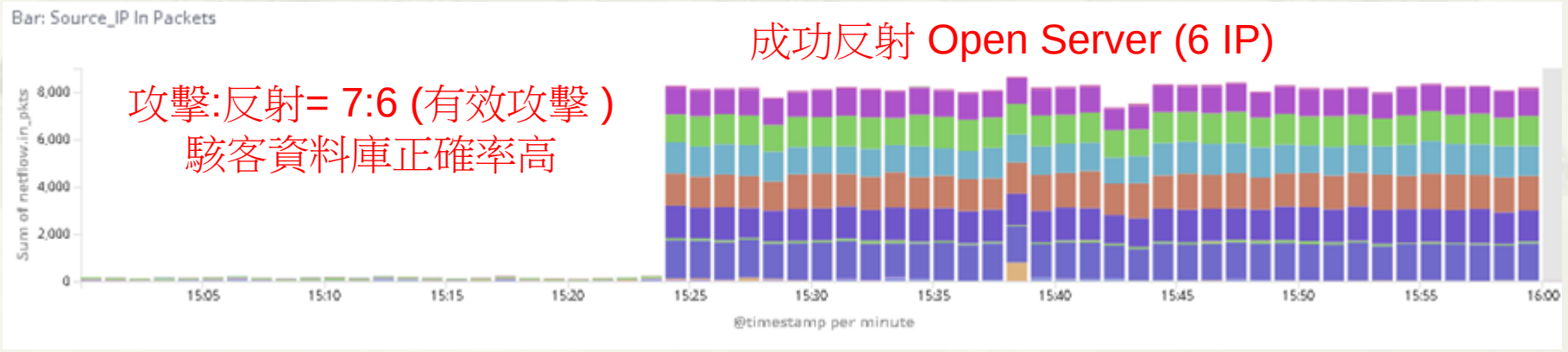

Bar: Source_AS History Packets
Victim AS
Sun Communications S.R.L.
Cloudflare Inc
OVH SAS
Sum of netflow.in_pkts
10,000
8,000
6,000
4,000
2,000
0
15:05
15:10
15:15
15:20
15:25
15:30
15:35
15:40
15:45
15:50
15:55
16:00
@timestamp per minute

攻擊 vs. 反射結果

攻擊流量



反射流量



完整文件請參考 http://www.tp1rc.edu.tw/e1.php
技術文件 -> DDoS 攻擊案例分析

4.特色服務

* 1.TCP-based 網路品質監控
* 2.Line Bot 網頁內容搜尋
  * ptt.cc 論壇校園版爬文
  * BGP Hijack
  * CVE 搜尋

107年評審委員建議:
5.區網流量大幅成長，對於網管及資安服務應有配套規劃。

4.1 TCP-BASED 網路品質監控

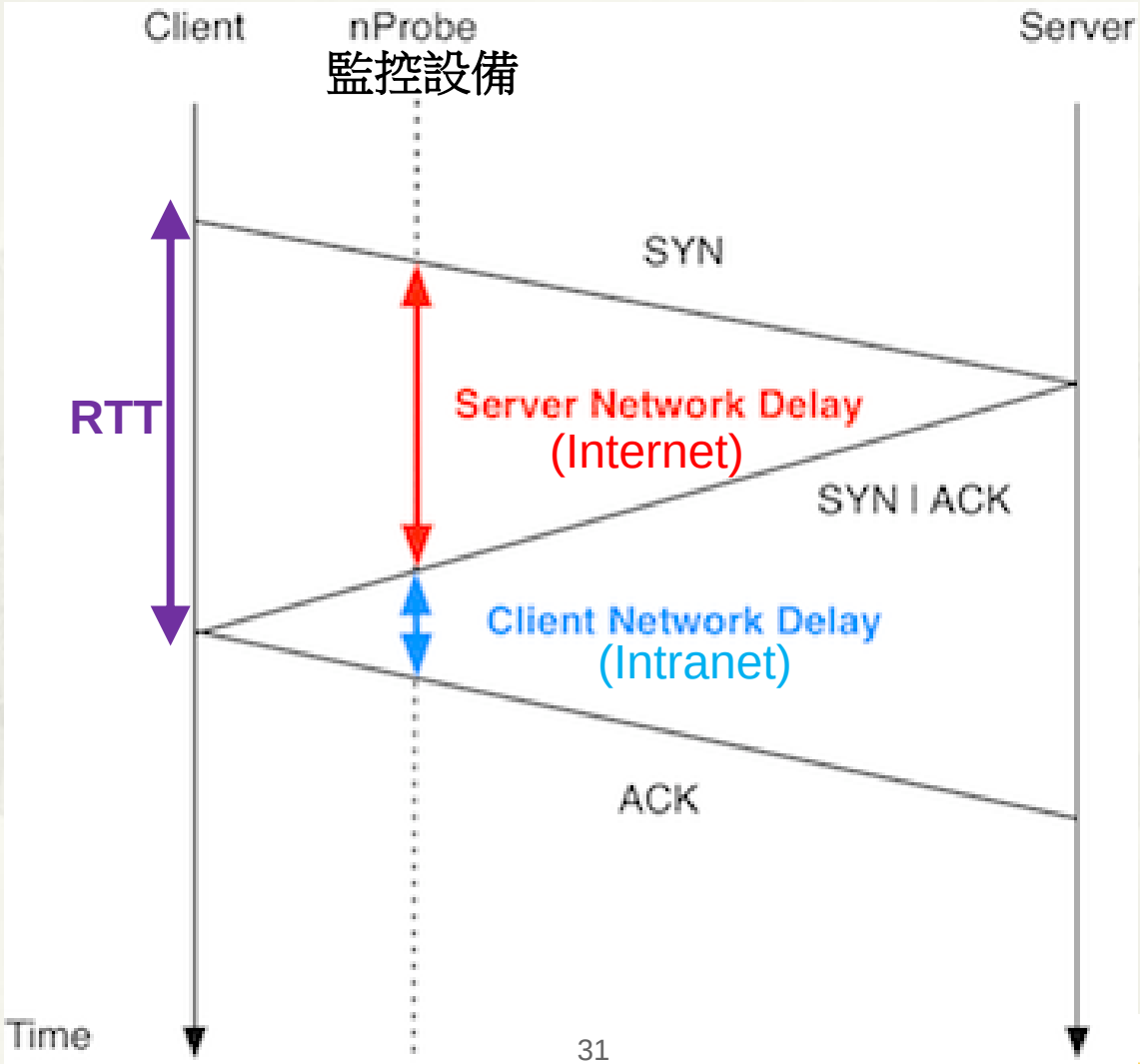
受邀於 TANet 100G 研討會-花蓮場 發表

完整文件請參考 http://www.tp1rc.edu.tw/e1.php
技術文件 -> TCP-based 網路品質監控

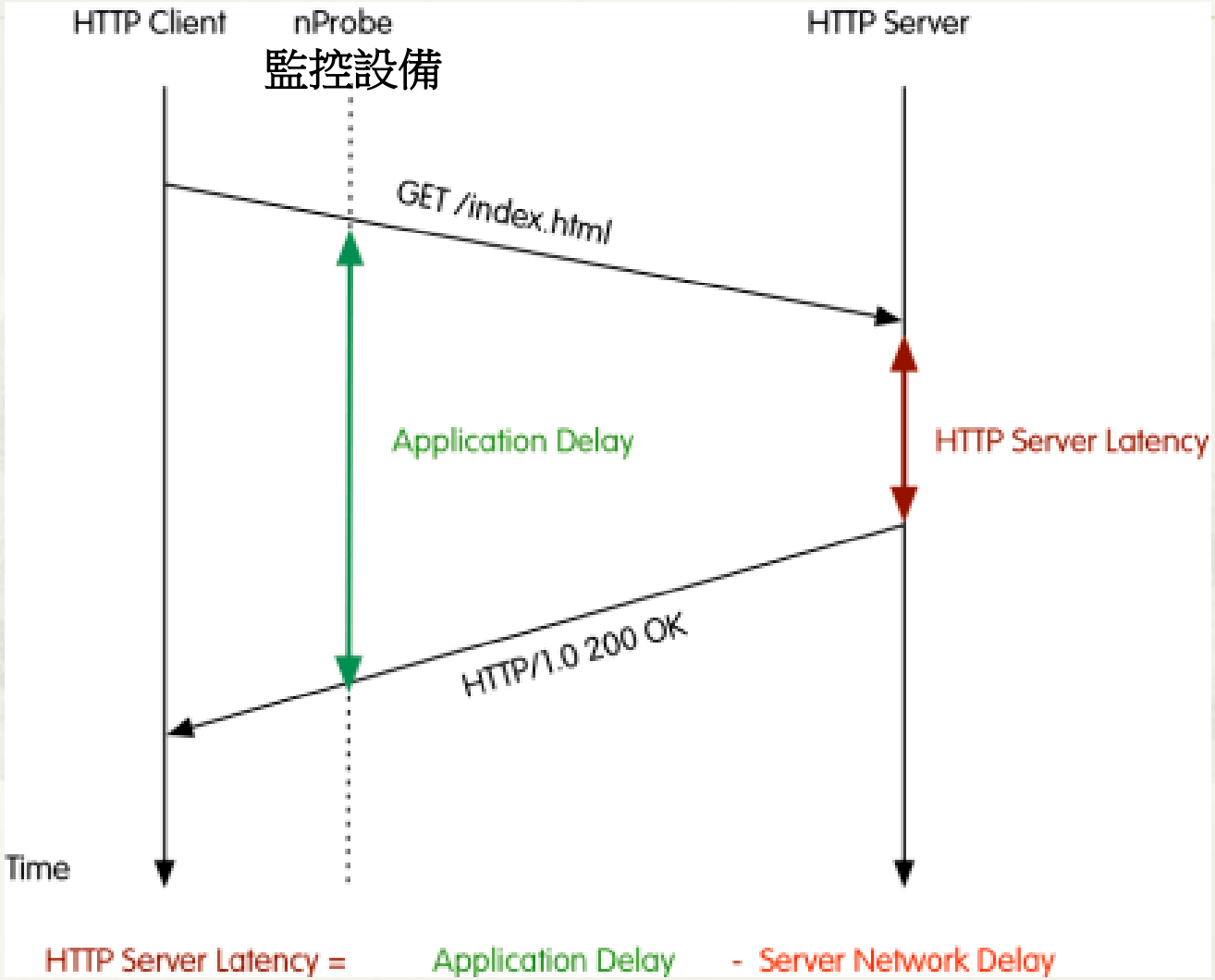
傳統網路品質監控

- 監控方法: ICMP Ping、TraceRoute
  - Round Trip Time(RTT)
  - Packet Lost
- 缺點與限制:
  - 需對方設備回應 ICMP Ping
  - 主動式偵測佔用頻寬資源
  - 無法大量佈建與監控:
    - 國網於所有區網中心與部分雲端佈建監控設備
  - 需有專用設備與軟體才能進行 24Hr 監控與統計

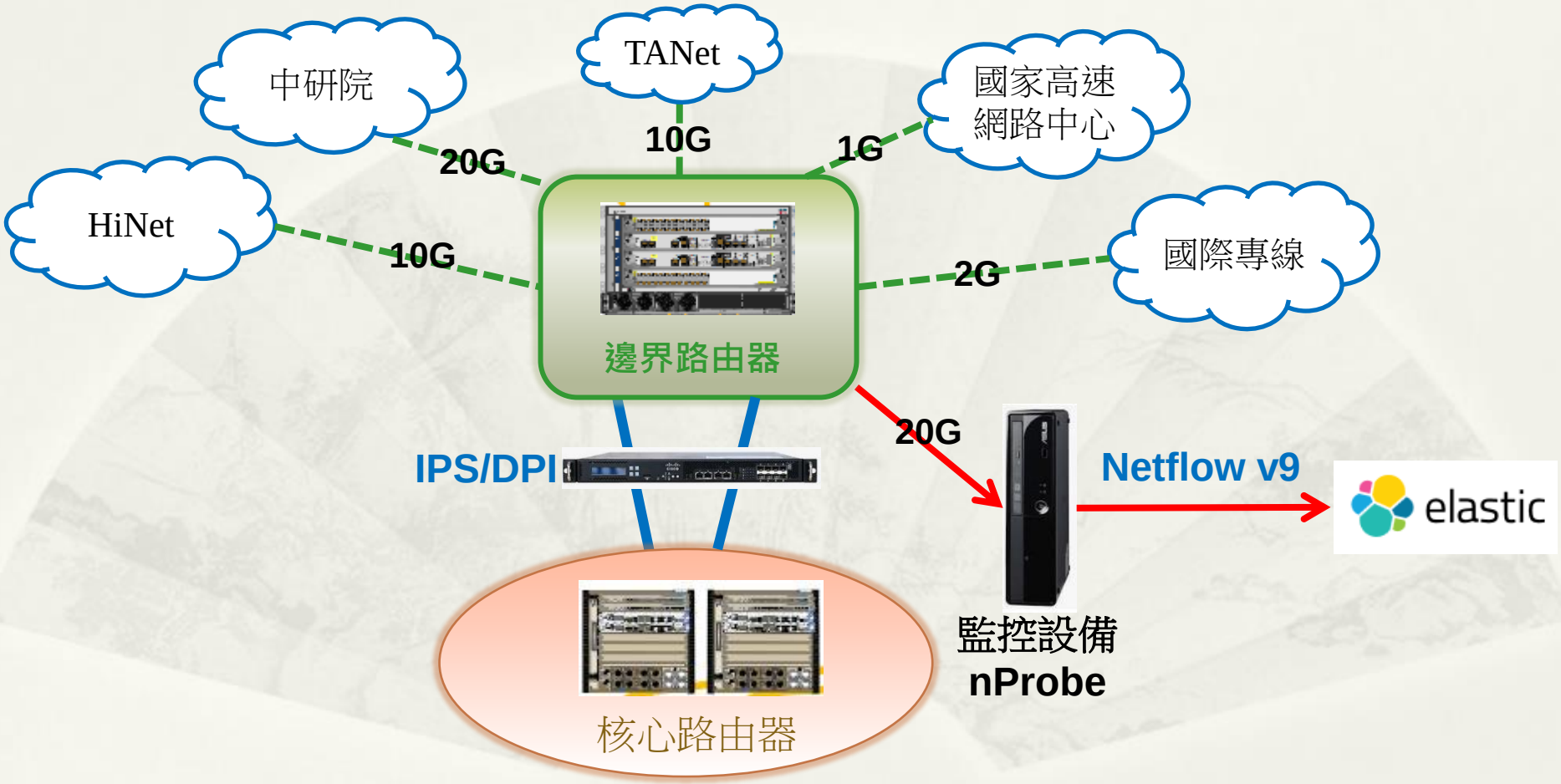
Network Latency
TCP 3-way handshake



Application Latency



TCP-based 網路品質監控
臺大網路架構圖

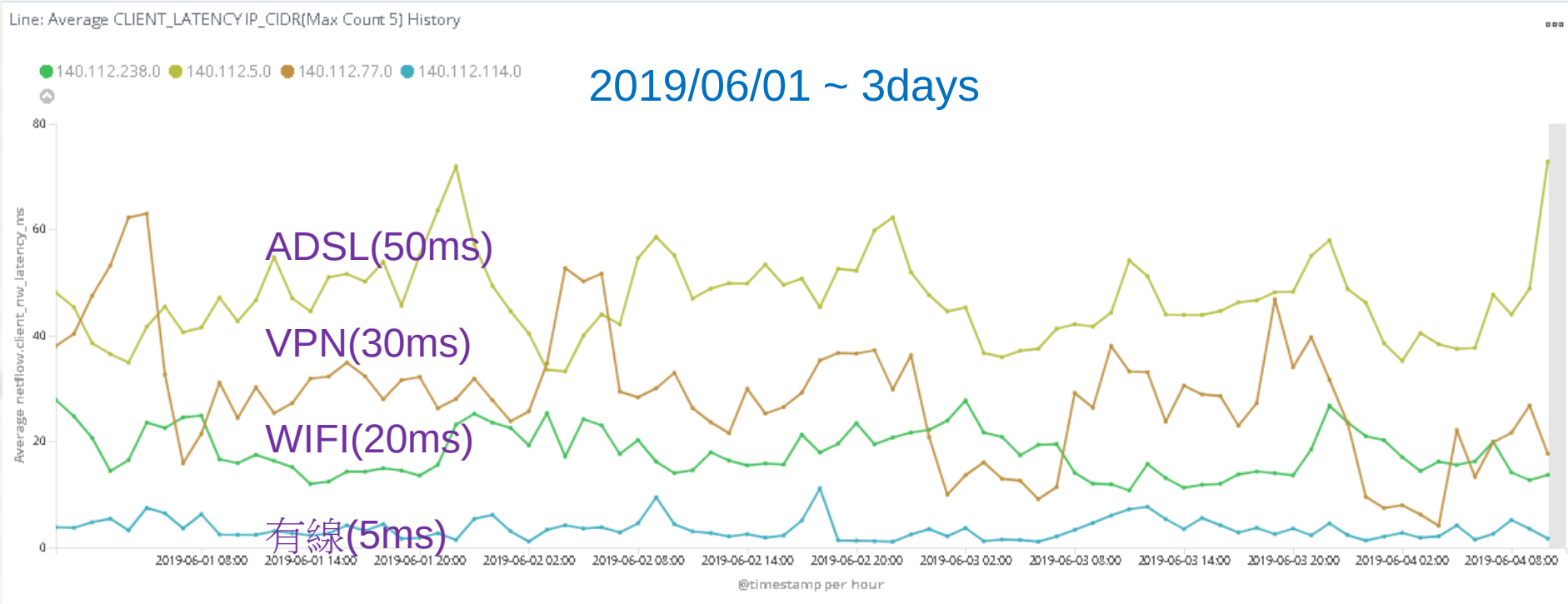


影響 Latency 原因

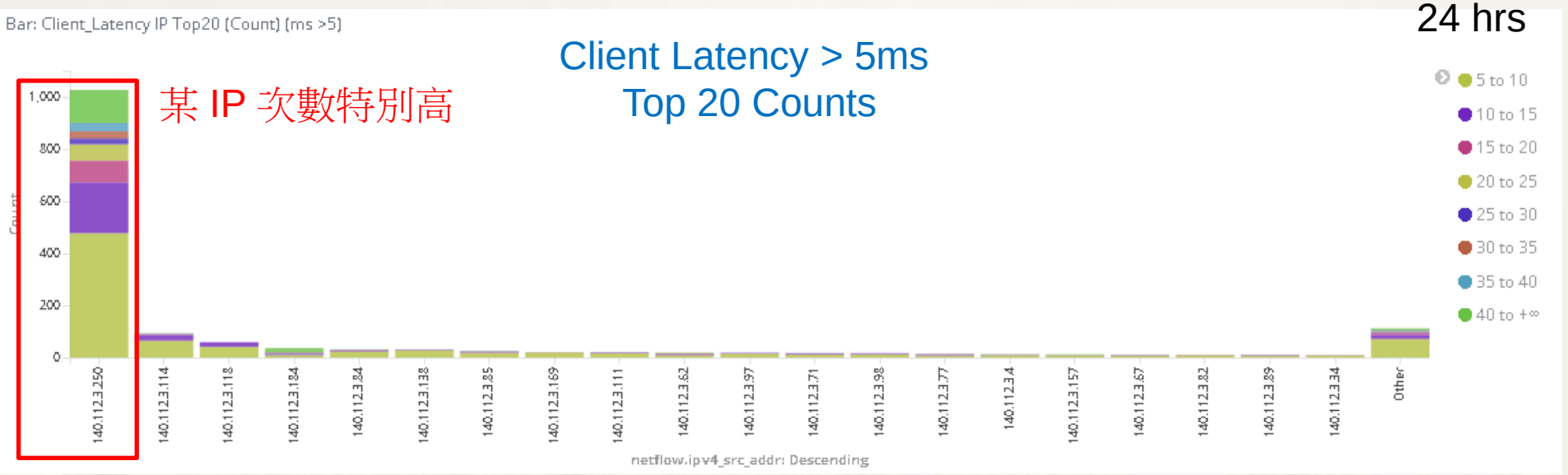
- Client 上網方式
  - 有線、WIFI、VPN、ADSL、4G (Client Latency)
- 實際距離
  - WIFI AP vs. 上網裝置 (Client Latency)
  - Client between Server (Server Latency)
- Network Congest 頻寬壅塞
  - WIFI Congest (Client Latency)
  - 骨幹 Congest (Client /Server Latency)
- 網路設備
  - Inline/Bypass (Client /Server Latency)
  - 設備 Loading (Client /Server Latency)
  - Server Loading (Application Latency)
- Server/網路設備 異常 (Server Latency)
- 封包大小(Server/Application Latency)

辨識不同網段用途
Client 上網方式

- ADSL: 140.112.5.0/25
- VPN: 140.112.77.0/24
- WIFI: 140.112.238.0/24
- 有線: 140.112.114.0/24



辨識網段內連網設備
140.112.3.0/24 計中工作區



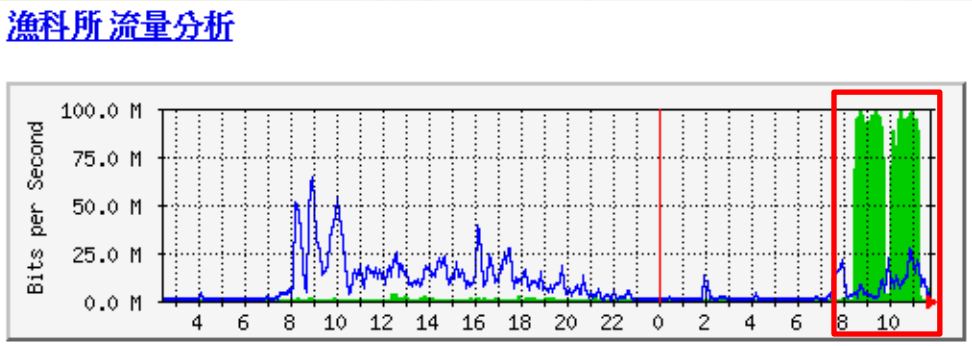
* 140.112.3.250 Aruba AP

```
Server6509#sh ip arp 140.112.3.250
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  140.112.3.250           0   000b.8662.e3b0  ARPA   Vlan302
```

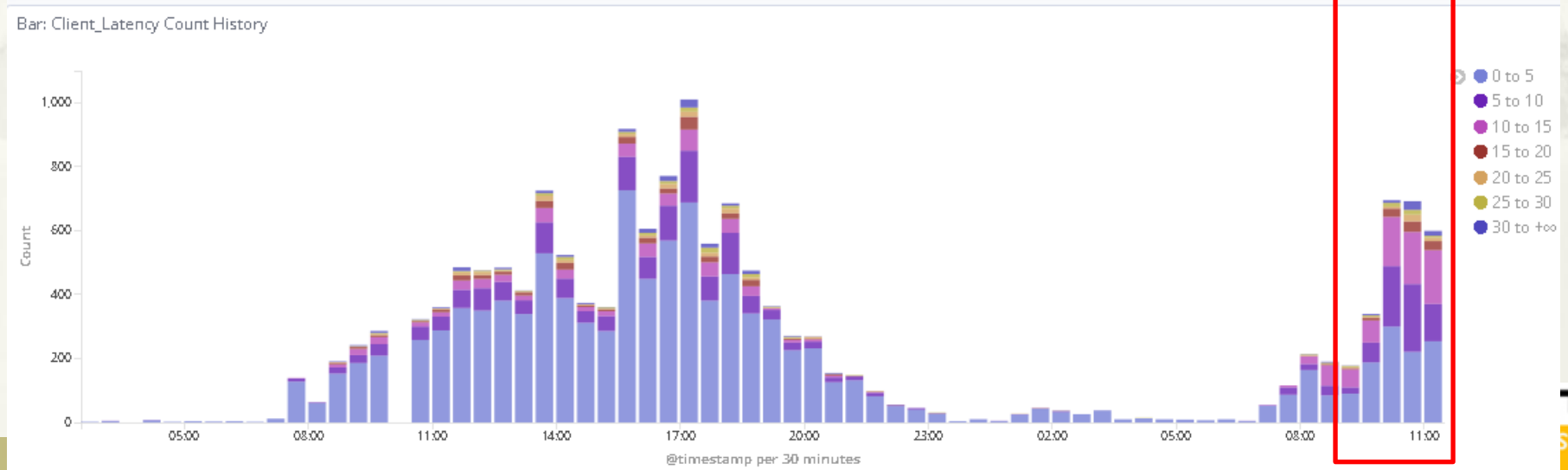
Company	Aruba, a Hewlett Packard Enterprise Company
OUI	00-0B-86

頻寬壅塞對 Client Latency 之影響

系所網路壅塞

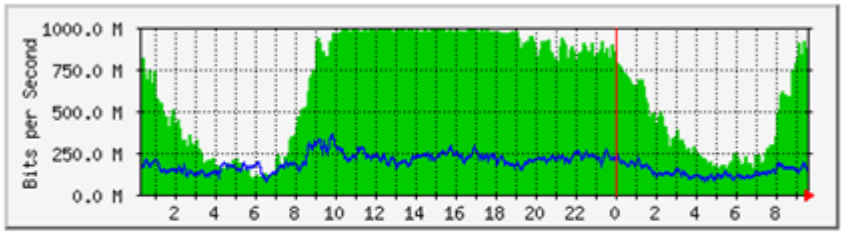


Congestion



頻寬壅塞對 Server Latency 之影響

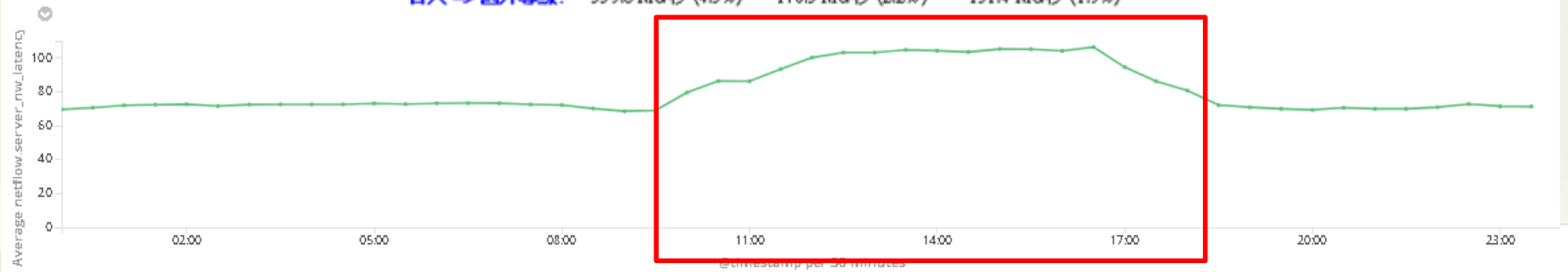
國際頻寬壅塞

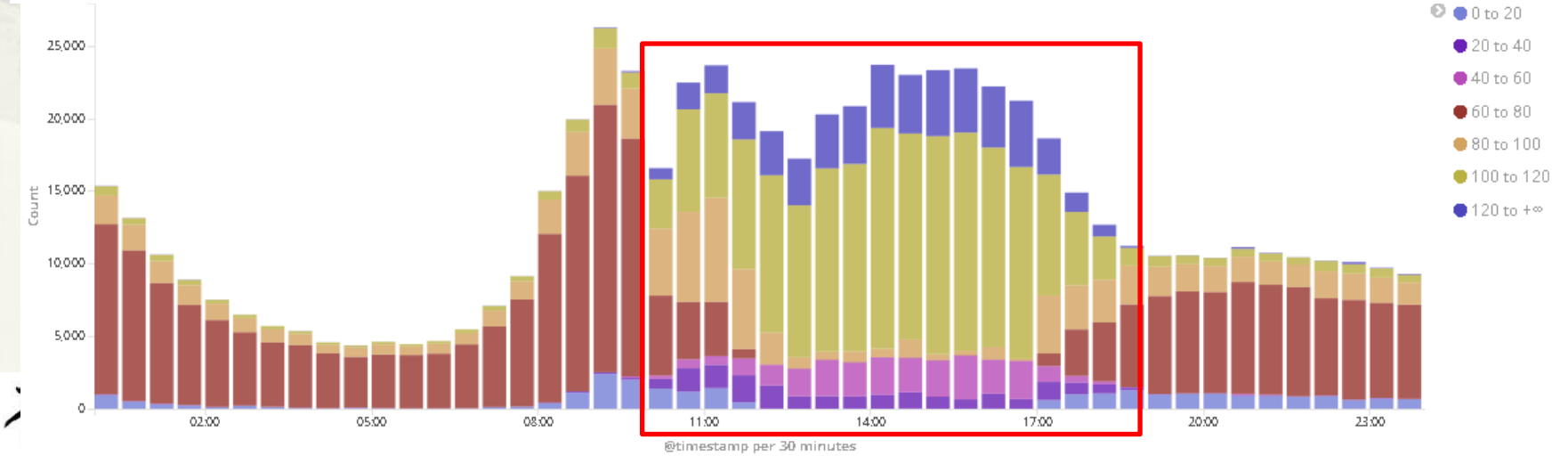


Dst AS=Apple Inc.

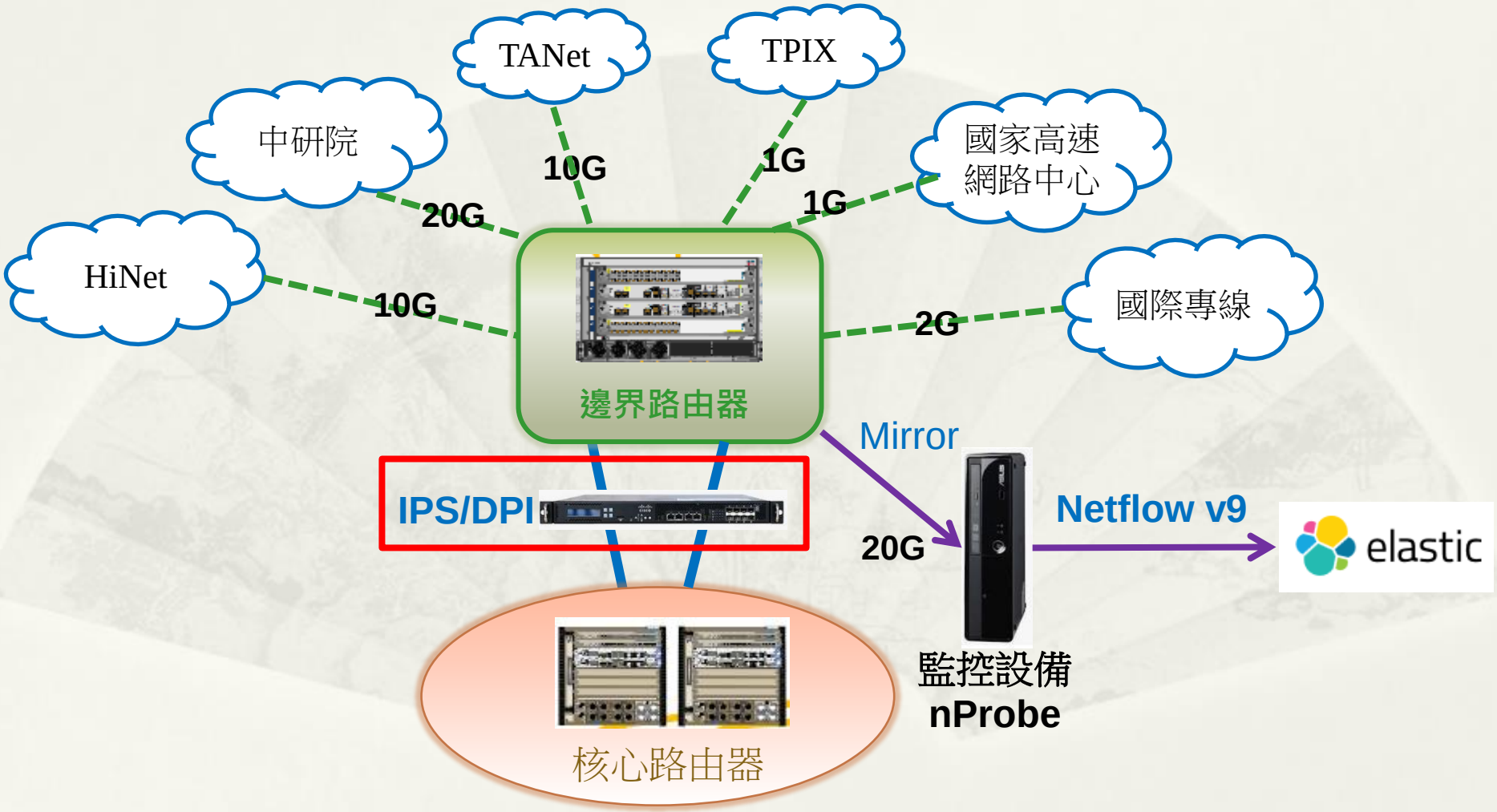
Line: Average SERVER_LATENCY History

	最大	平均	目前
國外專線 => 台大:	995.5 Mb/秒 (12.4%)	618.8 Mb/秒 (7.7%)	856.7 Mb/秒 (10.7%)
台大 => 國外專線:	359.6 Mb/秒 (4.5%)	178.5 Mb/秒 (2.2%)	151.4 Mb/秒 (1.9%)



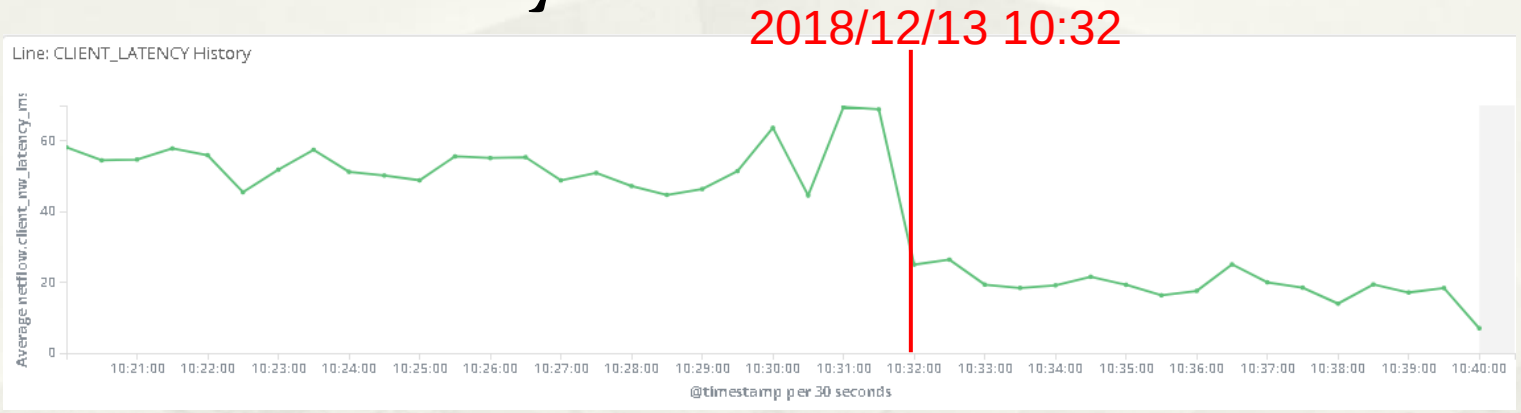


Inline 設備對 Latency 影響

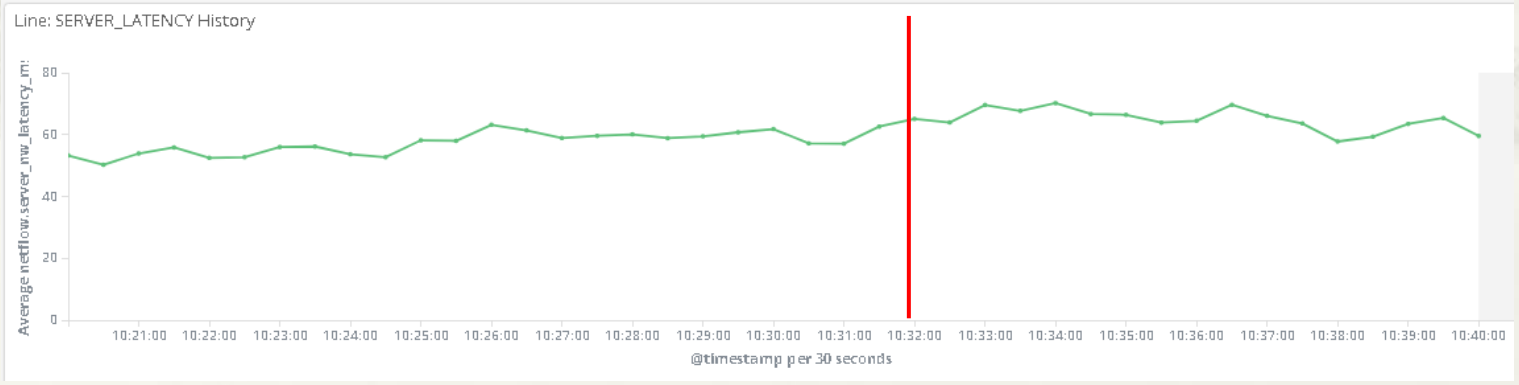


IPS Inline/Bypass vs. Latency

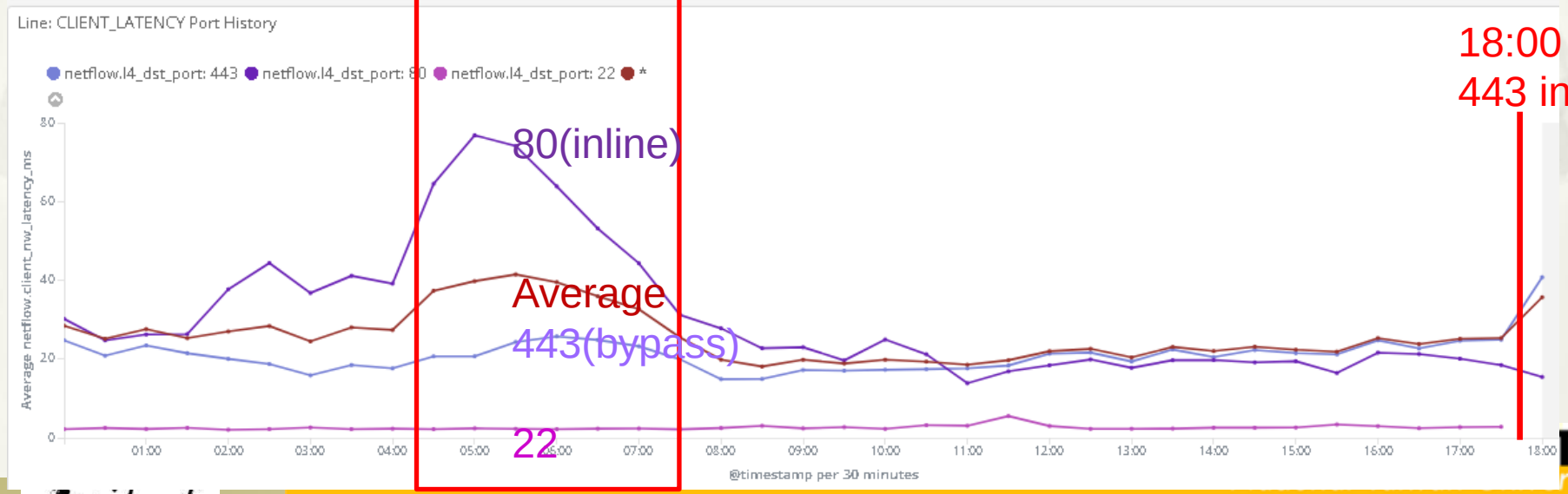
* Client Latency



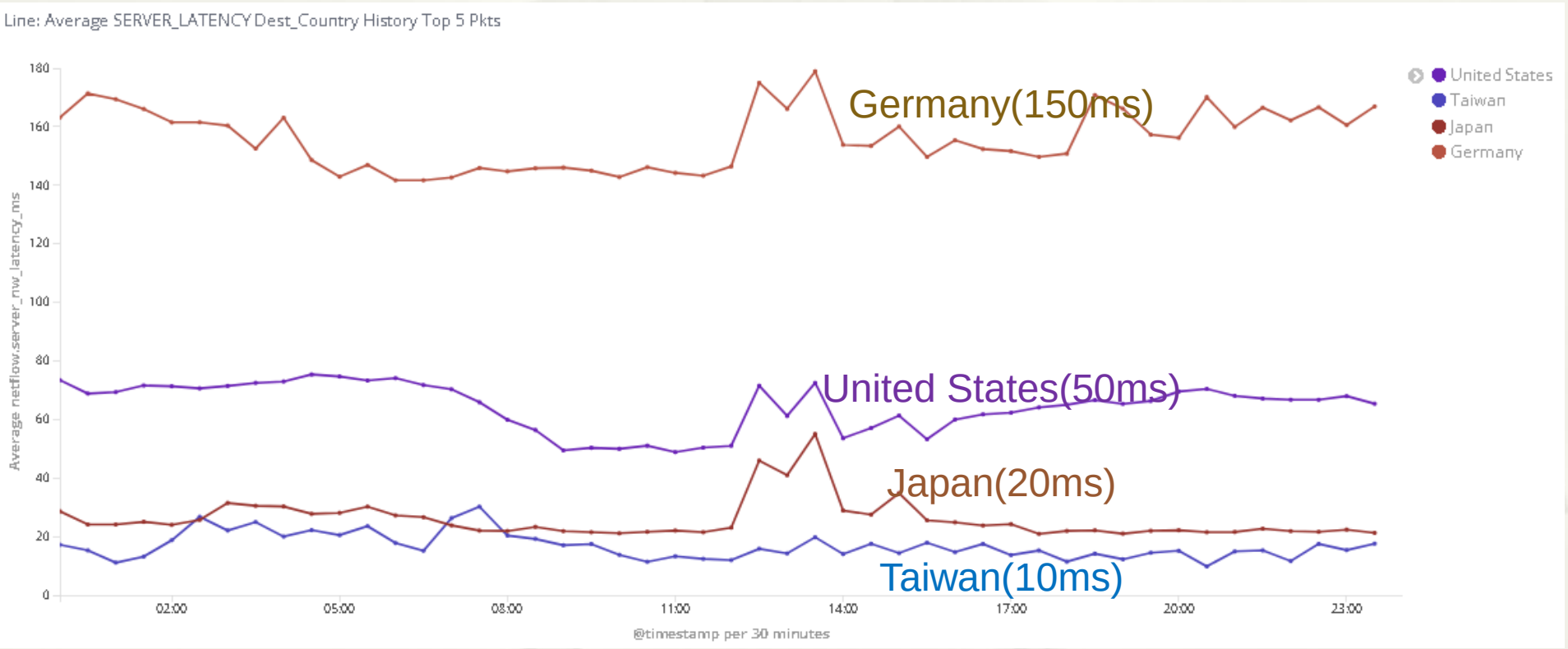
* Server Latency (無影響)



IPS Loading vs. Latency



實體距離影響 Server Latency
不同國家 24 Hrs



TCP-based 網路品質監控

* 優點
  * 利用使用者上網行為進行量測，提供大量數據
  * 被動式偵測(封包 Listening)，不佔用頻寬資源
  * 可快速釐清 Intranet or Internet 異常
  * 不需佈建監控設備，節省電力與資源
  * 可追溯過去之歷史統計記錄

4.2 LINE BOT 即時網頁內容搜尋

4.2 Cacti 結合 Line Notify 群組通知

Ptt 論壇: NTU 版

關鍵字:
Mail, 宿舍, 網路, 遭駭 …

BGP STREAM

BGP Hijack

BGP Overage
BGP Hijacking
BGP Leaks

關鍵字:
ASN TW

LINE Notify

CVE®

Common Vulnerabilities and Exposures

關鍵字
Cisco, Microsoft, Apache ….

107年評審委員建議:
5.區網流量大幅成長，網管及資安服務應有配套規劃。

庶民訊息~快速掌握~

ptt.cc 鄉民的正義

BGP Hijack 即時訊息

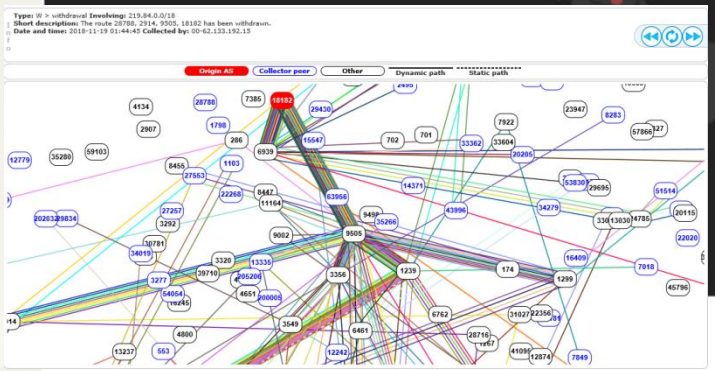
https://bgpstream.com/

CCNET_Notify: 2019-11-11 20:50:00
Outage
KLICKKLACK-AS-TW KlickKlack Co., Ltd, TW (AS 131645)
https://bgpstream.com/event/219156

CCNET_Notify: 2019-11-06 05:07:00
Outage
KLICKKLACK-AS-TW KlickKlack Co., Ltd, TW (AS 131645)
https://bgpstream.com/event/218753

CCNET_Notify: 2019-09-25 20:17:00
Outage
NCIC-IDC-TW New Century InfoComm Tech Co., Ltd., TW (AS 131586)
https://bgpstream.com/event/217340

發生於 TW ASN



Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Outage		NETCONNECTWIFI-AS Net Connect Wifi Pvt Ltd, IN (AS 133973)	2019-05-06 06:44:00	2019-05-06 06:48:00	More detail
Possible Hijack		*Expected Origin AS:* JAHIZ, LB (AS 209265) *Detected Origin AS:* Beirut-Lebanon, LB (AS 9051)	2019-05-06 06:39:01		More detail
BGP Leak		*Origin AS:* SSALIANDCO-AS-AP S S Ali and Co, BD (AS 136027) *Leaker AS:* AAMRA-ATL-BD Aamra technologies limited, BD (AS 58601)	2019-05-06 06:35:22		More detail

資安漏洞~快速掌握~
CVE Database

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

https://nvd.nist.gov/vuln/search

VULNERABILITIES | SEARCH AND STATISTICS

Search Results (Refine Search)

Search Parameters:

- Results Type: Overview
- Search Type: Search All
- CPE Vendor: cpe:/:cisco
- Published Start Date: 10/29/2019

There are **8** matching records.

產品範圍:
Cisco, Microsoft, Apache ….

CCNET_Notify: CVE-2019-1982
November 05, 2019; 03:15:11 PM -05:00
A vulnerability in the HTTP traffic filtering component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper handling of HTTP requests, including those communicated over a secure HTTPS connection, that contain maliciously crafted headers. An attacker could exploit this vulnerability by sending malicious requests to an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems, allowing attackers to deliver malicious content that would otherwise be blocked.
https://nvd.nist.gov/vuln/detail/CVE-2019-1982

CCNET_Notify: CVE-2019-1981
November 05, 2019; 03:15:11 PM -05:00
A vulnerability in the normalization functionality of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to insufficient normalization of a text-based payload. An attacker could exploit this vulnerability by sending traffic that contains specifically obfuscated payloads through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious payloads to protected systems that would otherwise be blocked.
https://nvd.nist.gov/vuln/detail/CVE-2019-1981

To Do List

* 首頁網站內容是否被竄改
* 校內網段攻擊/被攻擊
* Talos 黑名單搜尋
* Zero day
* RSS 訂閱
* 個人~暗黑應用
  * ptt 演場會門票版
    * ‘急售’,‘超低價‘,’破盤’

5. 107年評審委員建議與回覆

107年評審委員建議與回覆

委員建議	回覆
1. TCP Based 網路品質監控僅在台大校園網路，並位於區網建置，建請移至區網建置時，同時建立 SOP ，以考慮移植至其他區網和學校。同時評估以OPEN DATA 方式呈現。	因區網骨幹尖峰流量進出加總超過 25 Gbps 流量，已經超過一般市面上可購得 PCI-E based 網卡 10Gbps 之處理能力，因此暫時無法將監控系統移植於區網網路進行監控。目前預計將此技術舉辦相關技術研討會，請有興趣建置之連線單位可自行建置 TCP Based 網路品質監控系統。
2.考慮服務學校與區網配合，制定 DDOS 攻擊處理程序 SOP ，以縮短處理時間，更有效率解決問題。	目前北區A-SOC 已有自動偵測與email通知機制，可主動告知被攻擊之區網連線單位，及攻擊之來源與目的等相關資訊，並詢問是否進行封包清洗作業。
3.建立故障、 資安技術問題集，供使用學校查詢，可節省區網人員回覆問題的工作量。	在區網網站新設立技術文件專區 http://www.tp1rc.edu.tw/e1.php，將逐步整理相關資安及網路技術文件，可供網管人員參考與自行學習。

107年評審委員建議與回覆

委員建議	回覆
4.對區網中心維運計畫之網管及資安相關專案人員，建議應呈現其對應區網業務之績效，俾利後續能展現經費在此面上的運用效益。	依委員建議已經回覆於"108年度區域網路中心年終成果基礎資料彙整表"中第三項、請詳述本部補助貴區網中心網管及資安人力之服務績效。
5.對區網之網路流量由去年的 9.9G 成長至 21G 建議對應的網管及資安服務機制應有相關配套調整規劃。	Cacti Threshold 及 Syslog 異常偵測加上 Line Notify 自動通知功能，可加速處理效率。 使用"Line Bot 即時網頁內容搜尋"，可快速處理使用者抱怨及掌握資安訊息。
6.對區網中心所提供連線服務學校之 DDOS 清洗服務 建議依實際運作對照教育部所訂定之處理 SOP 提出相關修正建議以利各校能更有效率的因應 DDOS 資安事件的處置。	目前北區A-SOC 已有自動偵測與email通知機制，可主動告知被攻擊之區網連線單位，及攻擊之來源與目的等相關資訊，並詢問是否進行封包清洗作業。

107年評審委員建議與回覆

委員建議	回覆
7.對評估建議連線學校採用之免費憑證請瞭解其安全性。	Let's Encrypt由網際網路安全研究小組（縮寫ISRG）提供服務。旨在以自動化流程消除手動建立和安裝憑證的複雜流程，並推廣使全球資訊網伺服器加密服務，為安全網站提供免費的SSL/TLS憑證。主要贊助商包括電子前哨基金會、Mozilla基金會、Akamai以及思科。因此提供之憑證確實可靠且具安全性。
8.對資安事件的通報處理效率應思考如何精進。	108 年度資安通報平均時數 0.586 小時事件處理平均時數 0.602 小時，已經縮短至1 個小時內，相較去年有大幅進度。
9.建議爾後簡報資料請同步更新至網站以利委員審查。	今年若簡報有更改，將同步更新於區網網站與教育部 TANet NOC 網站。

107年評審委員建議與回覆

委員建議	回覆
10.資安通報平均通報時數及事件處理平均時數已較去年進步，但建議仍需持續努力，逐步縮短至1個小時內。另外聯絡資訊之資訊完整度：73.47% 亦可再加強。	108年度資安通報平均時數0.586小時事件處理平均時數0.602小時，已經縮短至1個小時內，資訊完整度也進步至81.633%。

6.未來目標與建議

* 6.1 未來目標
  * ipv4/ipv6 使用率統計
  * Layer2 同網段異常封包分析
  * DNS Log 異常偵測
* 6.2 其他建議

6.1 未來目標

- ipv4/ipv6 使用率統計
  - 藉由統計 ipv4 及 ipv6 之個別 ip 流量來計算連線單位之 ipv6 使用率
  - ipv6 上網支援程度分析
- Layer2 同網段異常封包分析
  - 分析同網段中之異常封包，例如: Broadcast、Multicast及 Unicast Flooding
  - 預計開發可辨識 Layer2 封包中異常之網路流量。

6.1 未來目標

* DNS Log 異常偵測
  * 資安事件中常出現因使用者查詢惡意 Domain Name 導致校內 DNS Server 觸發資安事件，但從 DNS Server 若開啟詳細 Log 可能影響 DNS 正常運作，且 Log 也無法詳實記錄 Quest and Reply 之詳細結果。
  * DNS 封包傳輸方式為明碼未加密，因此若能從封包中擷取出 DNS Quest and Reply 之詳細結果將有助於資安事件之調查。

6.2 其他建議

- 三年保固即將到期 2020/10
  - 分流器: Gigamon HC1
  - Netflow/Log 分析器: GenieATM
- eduroam
  - 技術小組會議: 明年區網連線學校 100%支援
  - 現況: 各區網中心 不相容?
    - 實測: 台大 eduroam 帳號在科技大樓、交大計中皆無法完成認證
  - 經費問題: 需 Wifi Controller 支援
    - 縣市網前瞻經費 100% 支援
    - 區網連線學校經費補助 ??

6.2 其他建議 (去年已提出)

* 建議各節點路由器加上IP 反解，網管才能瞭解網路路徑

```
C:\Users\Administrator>tracert line.me

在上限 30 個躍點上
追蹤 line.me [203.104.138.138] 的路由:

  1    <1 ms    <1 ms    <1 ms  192.168.20.1
  2     1 ms    <1 ms    <1 ms  nep17-254.tp1rc.edu.tw [163.28.17.254]
  3     2 ms     1 ms     1 ms  192.192.61.82
  4     3 ms     3 ms     3 ms  192.192.61.185
  5     1 ms     1 ms     1 ms  192.192.61.194
  6    53 ms    53 ms    52 ms  202.169.174.154
  7     *        *        *     要求等候逾時。
  8     *        *        *     要求等候逾時。
  9  ^C
```

* TANet NOC 網頁憑證錯誤

簡報完畢
謝謝