# 臺灣學術網路(TANet)區域網路中心
# 臺北區網 1

# 『114 年度基礎維運與資安人員計畫』

113　　年　　12　　月

# 【目　　錄】

# 壹、計畫基本項目

## 一、計畫期程

114 年 1 月 1 日至 114 年 12 月 31 日

## 二、計畫執行單位

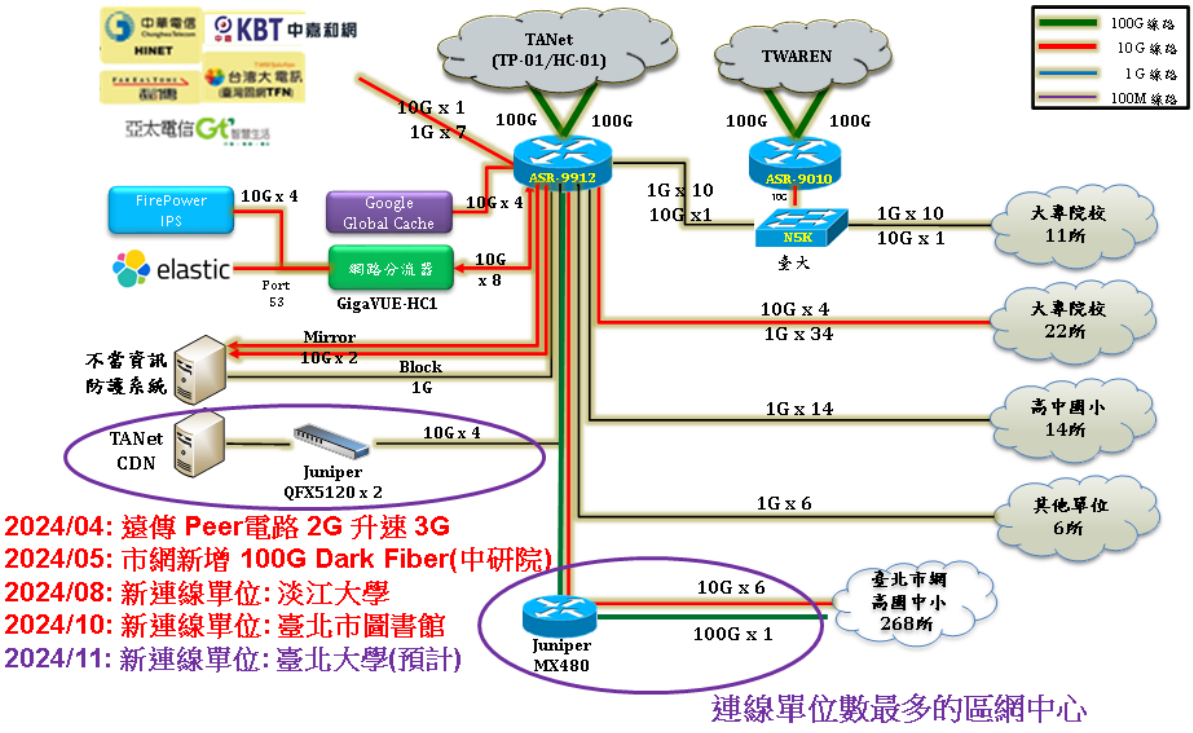
臺北區域網路中心 I—臺灣大學計算機及資訊網路中心

# 貳、計畫執行內容

## 一、基本維運

### (一)現況說明

1. 目前與臺大區網 Peering ISP 包含中華電信 10Gbps、遠傳電信 3Gbps、中嘉和網電信 1Gbps、亞太電信 1Gbps 及台灣固網 2Gbps 等五個 ISP，目前這些 ISP 都已接在區網 ASR 9K 骨幹路由器上，提供連線學校使用。

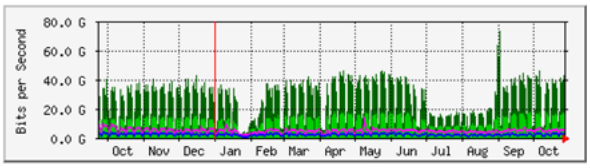



圖、臺大區網連線架構圖

2. 臺北市市網 IPv4 + IPv6 80Gbps 頻寬, 使用亞太電信 10Gbps x 2、中華電信 10Gbps x 2、東豐科技 10 Gbps x 2、中研院 Dark Fiber 100G
3. 提供區網連線學校 IP 網段查詢。
4. 參與 TWAREN 骨幹網路設備維運計劃。
5. 對連線學校(單位) 提供 WEB 及 DNS 服務狀態連線偵測情形詳細紀錄。
6. 今年新增三個連線單位 2024/08: 淡江大學 2024/10: 臺北市立圖書館 2024/12: 臺北大學
7. 連線單位數：54 所學校/單位。
8. 尚可供所屬連線學校申請分配之 IP ：0 個。
9. 人力狀況
   - 計中主任：周承復 主任
   - 網路組組長：謝宏昀教授
   - 網路管理負責人：游子興
   - 資安業務負責人：史詩妤
   - 編制內及約聘僱專職人員：8 名

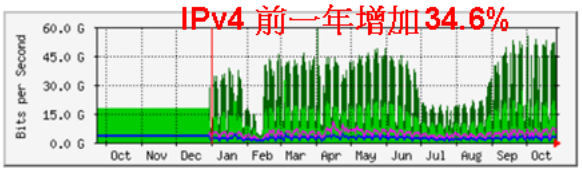
   協助處理各伺服器系統之例行維護、問題諮詢及統計監控使用狀況，Linux 伺服器系統維護、管理及統計使用者使用行為。撰寫網路管理應用相關文件，網路流量分析、監控及資料庫建立等。
10. Router 線路異動與路由管理。
11. 設置故障雙向測試系統，縮短故障排除時間，並提供 ISP 業者之聯絡資訊。
12. 提供各連線學校自行修改單位資料之網頁界面。
13. 推動各連線學校資源交流 (例如網路電話、IPv6、網路管理經驗分享) 。
14. 每年暑假期間固定舉辦網路技術之研討會。經由固定舉行研討會，期能將技術及網路科技與資訊安全等最新訊息達成全面性往下紮根，使區網連線單位能快速接收到最新資訊。
15. 流量統計 ipv4

`Yearly' Graph (1 Day Average) 2023



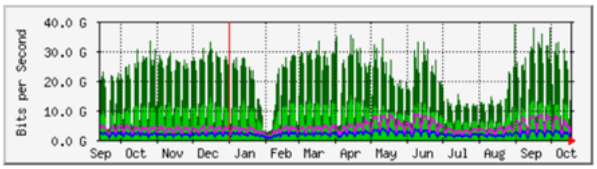

| | Max | Average | Current |
|---|---|---|---|
| InterNet => 北區區網 | 73.4 Gb/s (73.4%) | 10.1 Gb/s (10.1%) | 14.8 Gb/s (14.8%) |
| 北區區網 => InterNet | 13.1 Gb/s (13.1%) | 1958.7 Mb/s (2.0%) | 2298.1 Mb/s (2.3%) |

`Yearly' Graph (1 Day Average) 2024



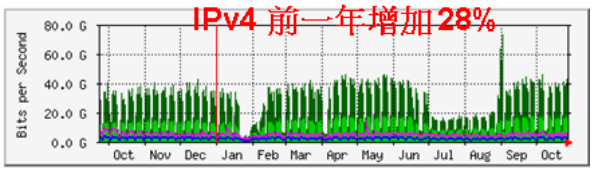

| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 59.6 Gb/s (59.6%) | 13.6 Gb/s (13.6%) | 7296.0 Mb/s (7.3%) |
| 北區區網 => 台北主節點 | 10.6 Gb/s (10.6%) | 2271.0 Mb/s (2.3%) | 1393.2 Mb/s (1.4%) |

`Yearly' Graph (1 Day Average) 2022



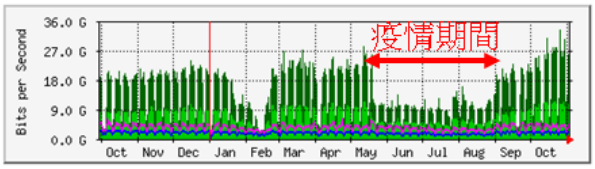

| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 39.0 Gb/s (39.0%) | 7882.8 Mb/s (7.9%) | 11.7 Gb/s (11.7%) |
| 北區區網 => 台北主節點 | 8786.5 Mb/s (8.8%) | 1862.4 Mb/s (1.9%) | 2506.5 Mb/s (2.5%) |

`Yearly' Graph (1 Day Average) 2023



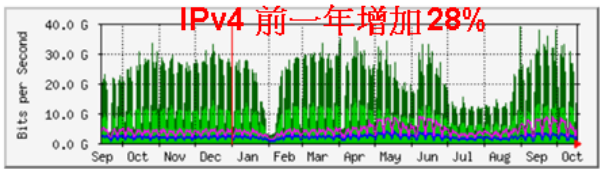

| | Max | Average | Current |
|---|---|---|---|
| InterNet => 北區區網 | 73.4 Gb/s (73.4%) | 10.1 Gb/s (10.1%) | 14.8 Gb/s (14.8%) |
| 北區區網 => InterNet | 13.1 Gb/s (13.1%) | 1958.7 Mb/s (2.0%) | 2298.1 Mb/s (2.3%) |

`Yearly' Graph (1 Day Average) 2021



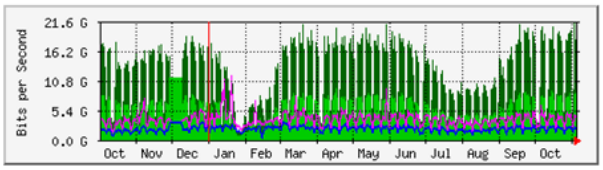

| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 33.2 Gb/s (33.2%) | 6115.1 Mb/s (6.1%) | 10.8 Gb/s (10.8%) |
| 北區區網 => 台北主節點 | 6075.9 Mb/s (6.1%) | 1676.6 Mb/s (1.7%) | 1825.1 Mb/s (1.8%) |

`Yearly' Graph (1 Day Average) 2022



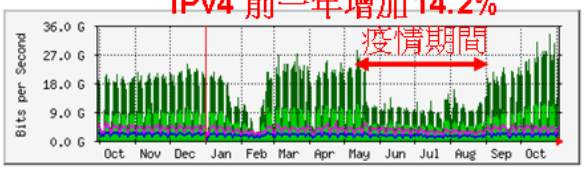

| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 39.0 Gb/s (39.0%) | 7882.8 Mb/s (7.9%) | 11.7 Gb/s (11.7%) |
| 北區區網 => 台北主節點 | 8786.5 Mb/s (8.8%) | 1862.4 Mb/s (1.9%) | 2506.5 Mb/s (2.5%) |

每年 圖表 (1 天 平均) 2020




| | 最大 | 平均 | 目前 |
|---|---|---|---|
| 台北主節點 => 北區區網 | 21.3 Gb/秒 (21.3%) | 5352.9 Mb/秒 (5.4%) | 8451.7 Mb/秒 (8.5%) |
| 北區區網 => 台北主節點 | 11.5 Gb/秒 (11.5%) | 1958.4 Mb/秒 (2.0%) | 2076.6 Mb/秒 (2.1%) |

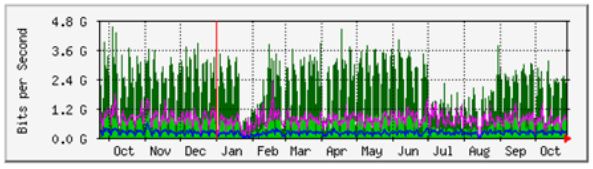
`Yearly' Graph (1 Day Average) 2021




| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 33.2 Gb/s (33.2%) | 6115.1 Mb/s (6.1%) | 10.8 Gb/s (10.8%) |
| 北區區網 => 台北主節點 | 6075.9 Mb/s (6.1%) | 1676.6 Mb/s (1.7%) | 1825.1 Mb/s (1.8%) |

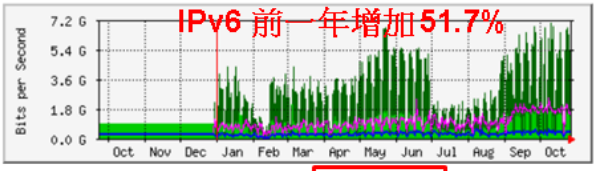
16. 流量統計 ipv6

`Yearly' Graph (1 Day Average) 2023

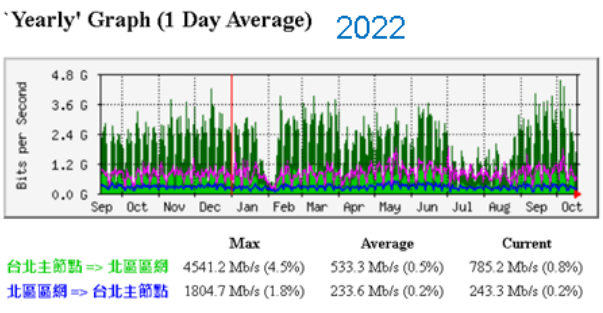


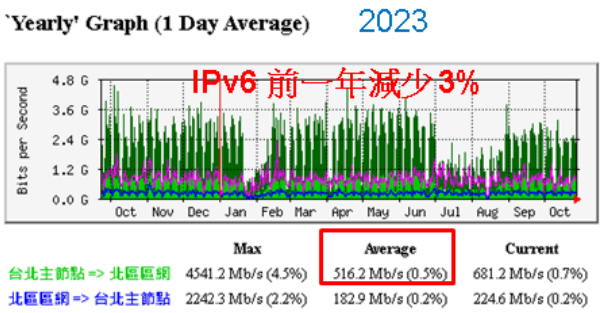

| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 4541.2 Mb/s (4.5%) | 516.2 Mb/s (0.5%) | 681.2 Mb/s (0.7%) |
| 北區區網 => 台北主節點 | 2242.3 Mb/s (2.2%) | 182.9 Mb/s (0.2%) | 224.6 Mb/s (0.2%) |

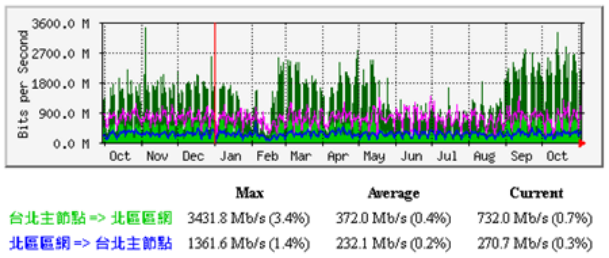
`Yearly' Graph (1 Day Average) 2024

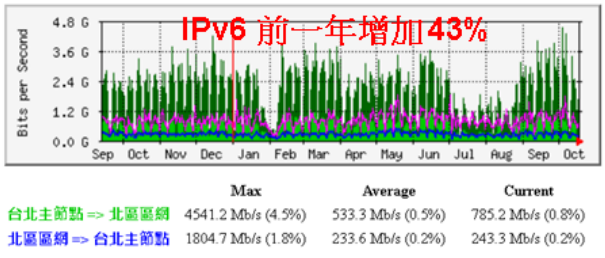


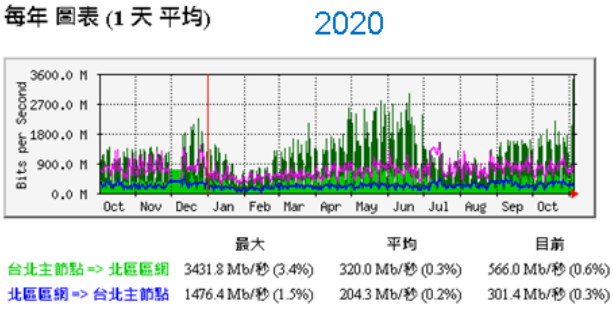

| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 7020.5 Mb/s (7.0%) | 783.3 Mb/s (0.8%) | 375.2 Mb/s (0.4%) |
| 北區區網 => 台北主節點 | 2399.8 Mb/s (2.4%) | 242.8 Mb/s (0.2%) | 277.9 Mb/s (0.3%) |

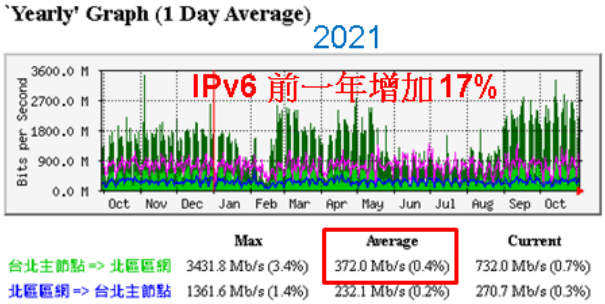


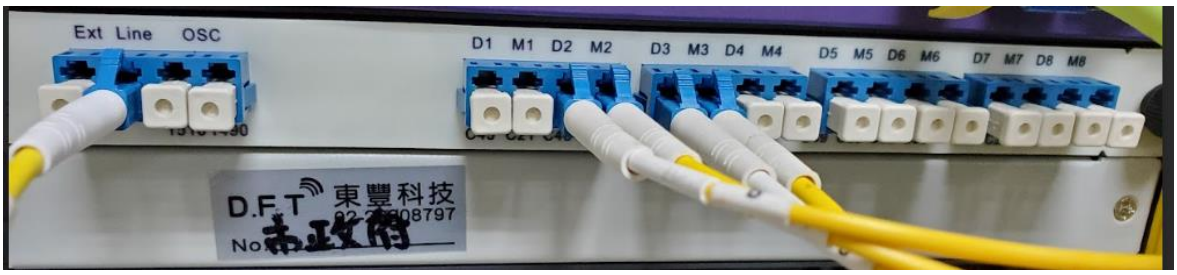



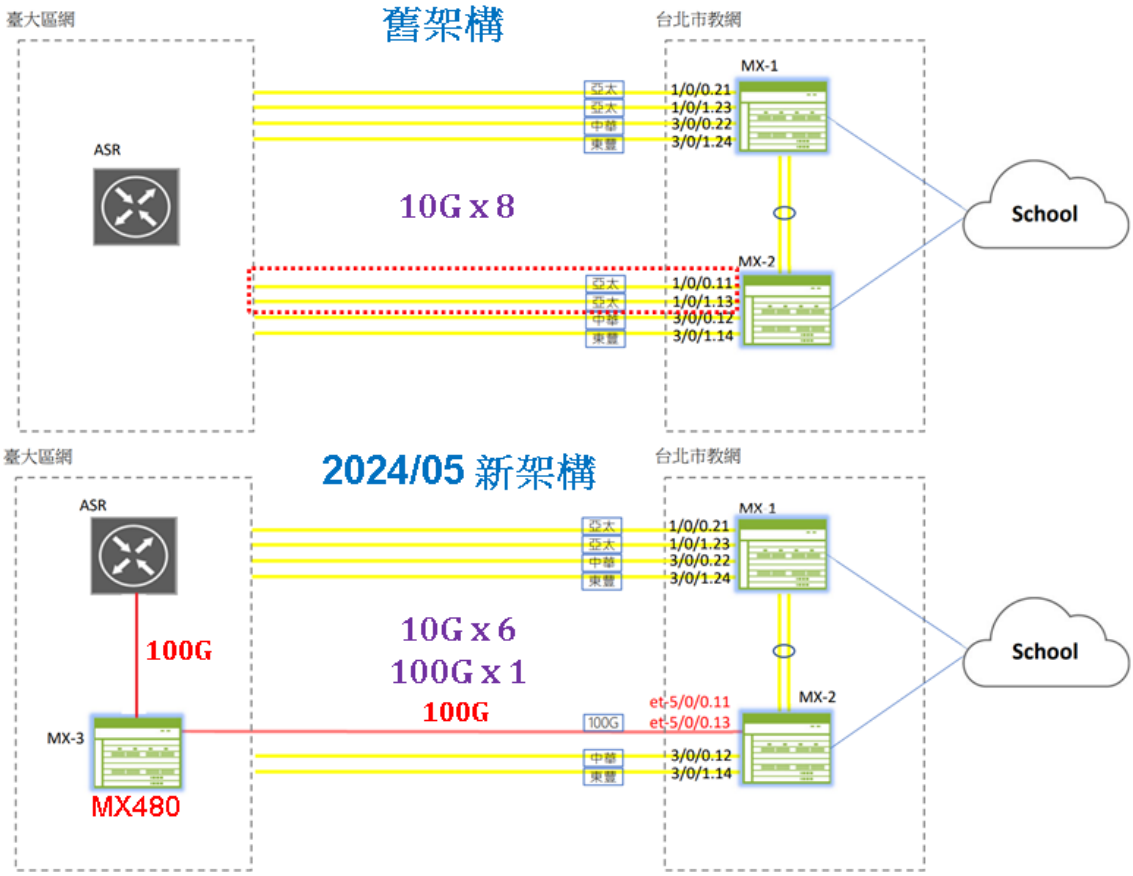

17. 臺北市網東豐科技線路

使用東豐科技 Single Dark Fiber，廠商提供一台 DWDM 8 Channels: Use 16 Waves 設備放置於電信機房




18. 臺北市網中研院 100G DarkFiber

經教育部協調，借用中研院所屬市網至台大 Dark Fiber 兩蕊光纖，使用 100G 頻寬直連，為配合目前 10Gx8 之 Equal Cost Multi Path 架構，100G 線路切成兩個 Vlan 使用




19. 連線學校: 臺科大使用 2 蕊暗光纖達成頻寬 10G x 2

# 舊架構


* 10G SFP+ 通用/一般


* 需要一對光纖傳輸



## (二)提供優質網路連線與管理服務

繼續維持日常優良服務並作下列推廣：

1. 推動各連線學校資源交流 (例如 IPv6 應用服務及 VoIP 網路節費電話推廣)。
2. 鑑於網站入侵高居不下的統計比例，設置網頁弱點掃描機制。
3. 協助調查大專院校及高中職連線單位網路設備是否支援 IPv6。
4. 統計並整理網路異常事件處理過程，分享解決網管相關經驗於區網會議，包含如下主題：

   甲、 弱掃平台相關說明

   乙、 資安 Case Study 分享

   丙、 WAF 阻擋封包分析

丁、 DDoS 事件分析

戊、 BGP Hijacking 事件探討

己、 Shodan 簡介與應用

庚、 Openvas 簡介及應用實例

辛、 ipv6 推廣與建置

壬、 eduroam 推廣與建置

癸、 Line 群組加入

5. 將連線單位之流量、封包量、ping、packet lost% 整合顯示於一個畫面，可快速釐清網路異常問題。

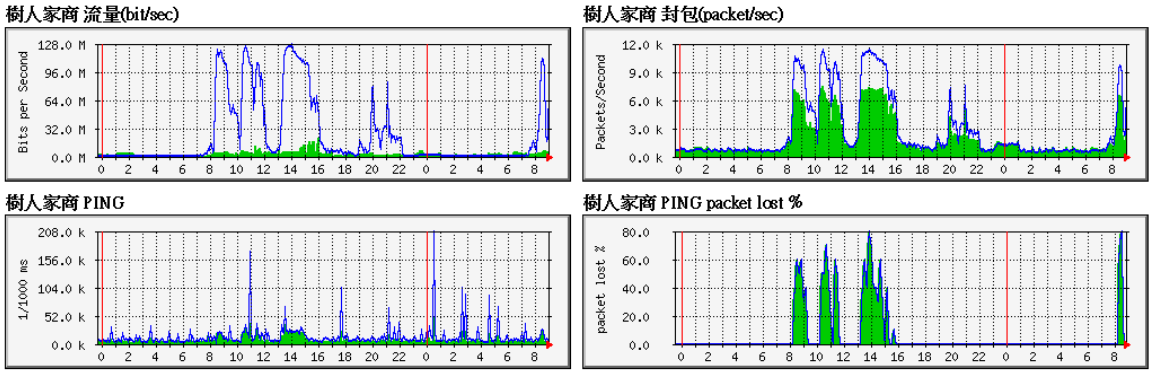



圖 2、連線單位 MRTG 網路監控圖

6. 將連線單位分類為大專院校、高中職、其他單位，更容易查找圖表資訊。

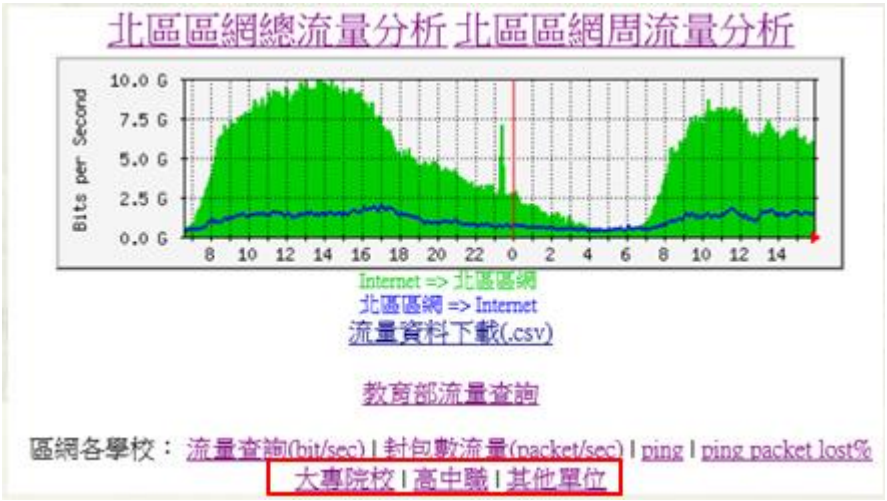
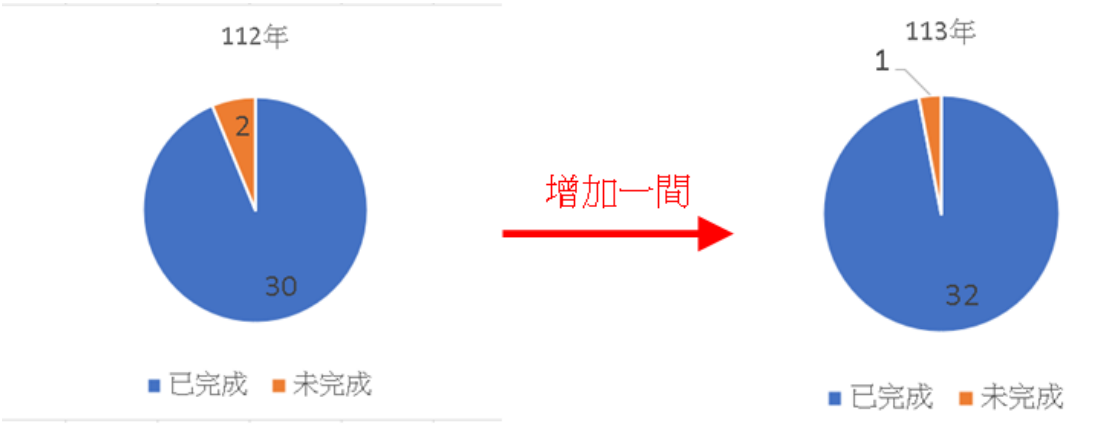



圖 3、連線單位監控圖表依照單位屬性分類

7. 使用 ELK Stack 記錄 TANet 區網 Router 之 Netflow 並提供 Src IP/Port、Dest IP/Port 等搜尋功能，並可依據封包數或流量查找 Top10 Src IP、Dest IP，若有網路異常流量發生，可快速釐清問題。
8. 使用 Cacti 收集 TANET 區網 Router Syslog 記錄並提供 Link Up/Down、Login Alerts 及 Config 指令修改通知。
9. 連線品質管理，使用 Ping Latency 監控 Yahoo/Google/Facebook/HiNet DNS 等常見之入口網站與服務。
10. 2024 年 IPv6 大專院校完成率: 大專院校: 33

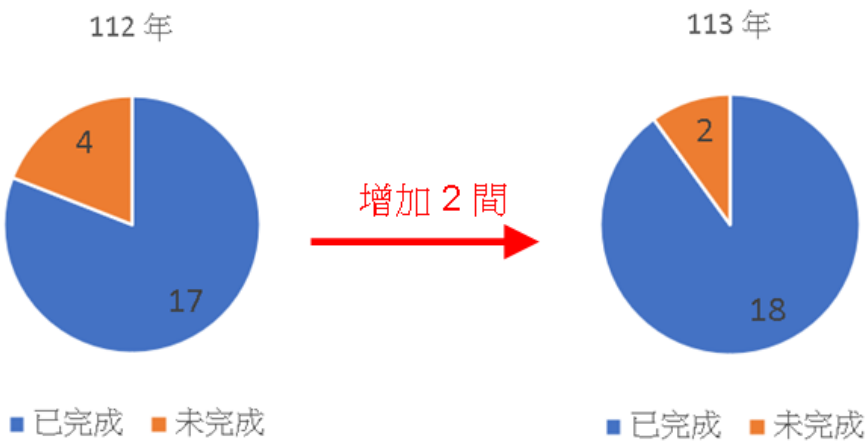



僅剩: 軍事情報局學校

有 ipv6 網段學校全部完成

尚無 ipv6 網段:軍事情報局學校

11. 2024 年 IPv6 高中職完成率: 高國中小及其他單位: 20




有 ipv6 網段學校全部完成

尚無 ipv6 網段:中華民國學生棒球運動聯盟、國家地震中心

12. ISP 線路統計

| 列標籤 | 計數 - 電信 |
|---|---|
| 中華電信 | 37 |
| 遠傳電信 | 6 |
| 台灣固網 | 5 |
| 亞太 | 4 |
| 臺灣智慧光網 | 1 |
| **總計** | **53** |

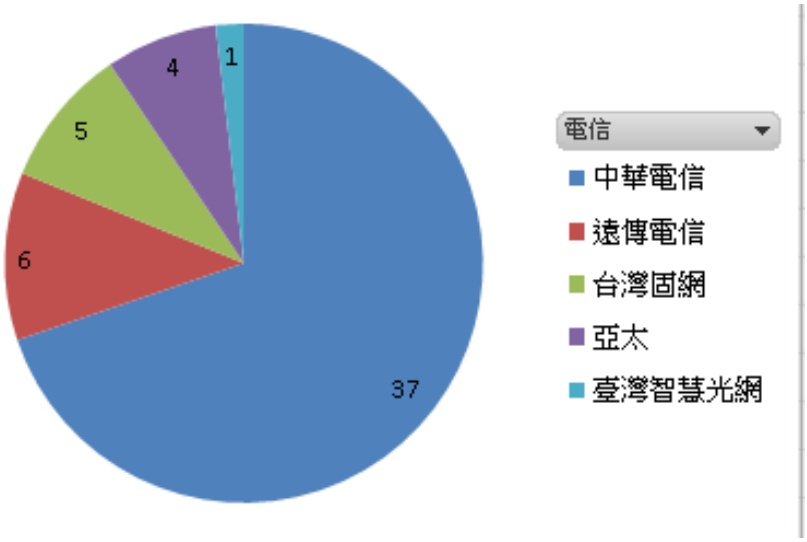



圖 4、連線單位 ISP 線路統計

13. 線路介面型態統計

| 列標籤 | 計數 - Type |
|---|---|
| 光纖 | 32 |
| 電UTP | 22 |
| 總計 | 54 |

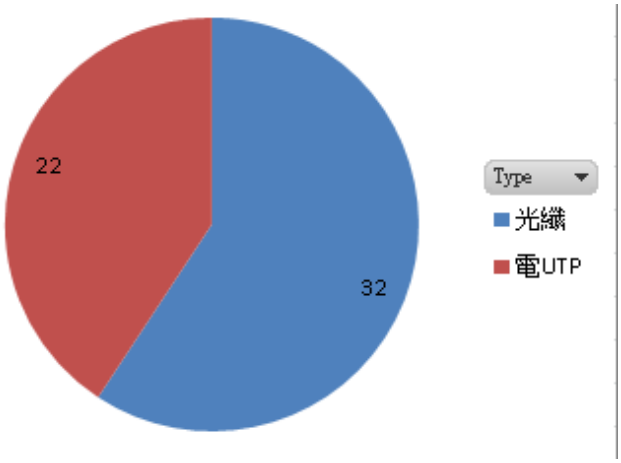



圖 5、連線單位使用介面統計

## (三)辦理資訊推廣活動

| 類別 | 研習課程 | 講師 | 出席人數 |
|---|---|---|---|
| 資安 | 駭客攻擊手法深入探討 | 中華資安 林峰正 | 91 |
| 雲端 | 檔案不再雜亂無章：使用 Google Workspace 打造超流暢工作流 (線上實做) | CloudMile 陳宏傑 | 80 |
| 系統 | Proxmox VE 入門實作課程 (LAB 實做) | 節省工具箱公司 技術總監 鄭郁霖 | 37 |
| 雲端 | Google Classroom 實際應用場景 (線上實做) | CloudMile 陳宏傑 | 48 |
| 雲端 | 解鎖工作效率新境界：Gemini for GWS 實戰應用 (線上實做) | CloudMile 鄭潯元 | 77 |
| 法規 | AI 著作權議題 | 胡中瑋律師 | 48 |
| 雲端 | 透過 AppScript Generative AI (Gemini API) 整理 Gmail 信件內容 (線上實做) | CloudMile 張家瑋 | 75 |
| 大數據 | Elasticsearch 上 AI 與 ML 的說明與運用 | 集先鋒 Anthony 陳俊佑 | 77 |

| | | | |
|---|---|---|---|
| 資安 | 深入探討特權帳號管理系統整合運用 | 鋐迪資訊　資深技術顧問 鍾迪 | 80 |
| 雲端 | 無痛連結 Google Workspace, REST APIs（初階） | CloudMile 陳智聰 | 71 |
| 雲端 | 無痛連結 Google Workspace, REST APIs（進階） | CloudMile 陳智聰 | 55 |
| 系統 | 以 Pure Storage 平台來加速擁抱 AI 的驅動力 | Pure Storage 蔣燚峰 | 53 |
| 資安 | 網站常見弱點檢測與修補(LAB 實做) | 高于凱 | 46 |
| 網路 | 網管工程師必修課程 -- 網路設備常見規格、常用工具與原理介紹 | 游子興、史詩妤 | 95 |
| 資安 | 常見的網站漏洞利用以及防禦介紹 (LAB 實做) | 中華資安 蕭子修 | 68 |
| 資安 | 滲透測試 LAB 實作練習 (LAB 實做) | 中華資安 蔡侑達 | 35 |
| 資安 | 常見網站弱點與修補方法 -- 以 WordPress 為例 | 陳思蘊、游子興 | 88 |

## (四) 區網服務 VM 主機群由 Vmware ESXi 移轉至 Proxmox Virtual Environment(PVE)

- 功能強大、友善硬體支援 Proxmox Virtual Environment(PVE)
  - Open Source Solution
    Linux Debian + QEMU/KVM + LXC(Linux Container)
  - 硬體相容性佳
    相容於 Linux Debian Kernel
    支援 Realtek 網卡
    支援 100Mbps 網卡
    支援舊型 PCI 介面網卡 (主流: PCI-E/PCI Express)
    PCI Passthrough 限制少
    支援 USB Mouse/Keyboad
    支援 USB Audio/Video (USB Camera)
- Vmware vCenter 能做到的 Proxmox VE 都支援
  - VM Clone
  - Full Clone
  - VM Template:

Link Clone

- Cluster 中控台

  不需安裝額外軟體 (vCenter Appliance)

  節省後續維運升級之困擾

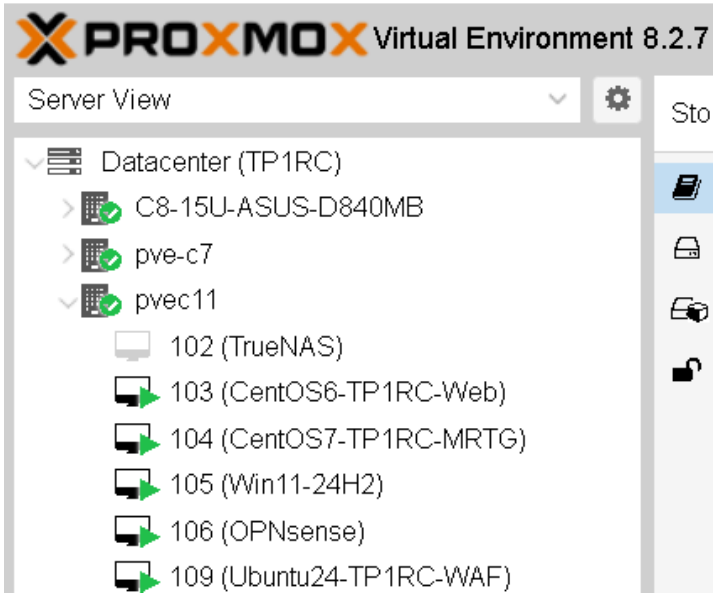
  每台 Node 皆可當成中控台

  避免 vCenter 當機或所在 Host 當機

- VM Migrate: (VMware vMotion)

  Node 主機搬移

  Storage 搬移




- HA 高可用性
- 不需額外付費，內建即支援

  Proxmox Backup Server

  增量備份、資料壓縮、重複資料刪除

  備份 VM Disk 內容檢視，不需還原即可取出檔案

  內建 Email Notification

## (五) TANet 400G 新世代骨幹網路建置規劃與支援

TANet 新世代 400G 骨幹已於 113 年 11 月決標並公告完成，得標廠商已經來機房現場進行場地勘查。

設備機櫃規劃如下圖黃底所示，預計使用三櫃的空間存放新設備。

| C13 | C12 | C11 | C10 | C9 | C8 | C7 | C6 | C5 | C4 | C3 | C2 | C1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| B13 | B12 | B11 | B10 | B9 | B8 | B7 | B6 | B5 | B4 | B3 | B2 | B1 |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| A13 | A12 | A11 | A10 | A9 | A8 | A7 | A6 | A5 | A4 | A3 | A2 | A1 |
| | TANet 400G 新世代網路 | | | | | | | | | | | |

UPS 不斷電電池組，因台大計中機房空間有限，且建築物樓板承重有限，加上原先已於東西兩側自建不斷電電池組，因此就不需再加裝電池組。

電源的部分因為原機櫃即有安置電源，安培數足夠，但接頭的部分可能需要更換或調整。

目前時程預計於 114 年 Q2 建置完成，建議可先建置完成後，於暑假期間進行測試，並於九月開學前進行正式切換。

## 二、創新服務

### (一)建構主動式網路品質監控系統

1. 建構即時且自動化之網路品質監控系統，改善傳統被動式網路異常通知，建構化被動為主動之網路品質監控系統。


圖 6、網路品質監控系統概念圖

2. 建立主動網路偵測機制: 使用者端

   甲、提供網路速度測試工具: 網頁測速、Android/iPhone Speed Test App

   乙、網路簡易偵測工具: Ping Latency、Traceroute 出口路徑查詢

3. 建立主動網路偵測機制: 網路設備端

   甲、連線介面偵測: 頻寬使用狀況

   乙、網路設備偵測: Ping Latency、CPU 使用率

   丙、伺服器偵測: CPU 使用率、記憶體使用率、硬碟使用率

4. TCP-based 網路品質監控系統

   甲、監控方法: TCP

      i. RTT: TCP 3-way handshake

ii. Packet Lost: TCP Retrasmit & OutOfOrder

乙、優點

i. 被動式偵測(封包 Listening)，不佔用頻寬資源

ii. 可快速釐清 Intranet or Internet 緩慢或異常

iii. 不需佈建監控設備，節省電力與資源

iv. 準確性更高: 網路現成大量連線記錄提供量測結果

v. 可追溯過去之歷史統計記錄

丙、監控網路架構圖

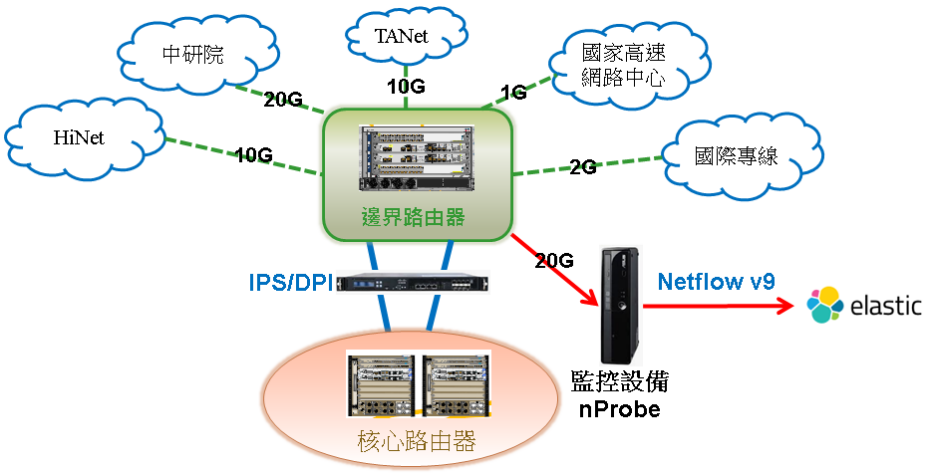



圖 7、監控網路架構圖

丁、Latency 24 Hrs 統計

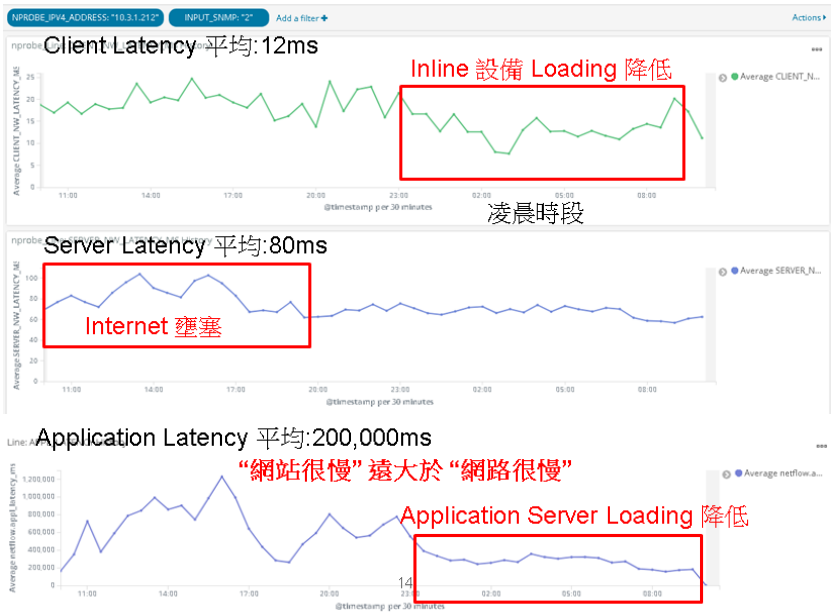



圖 8、Latency 24 Hrs 統計

戊、Latency 24 Hrs 各區網中心統計

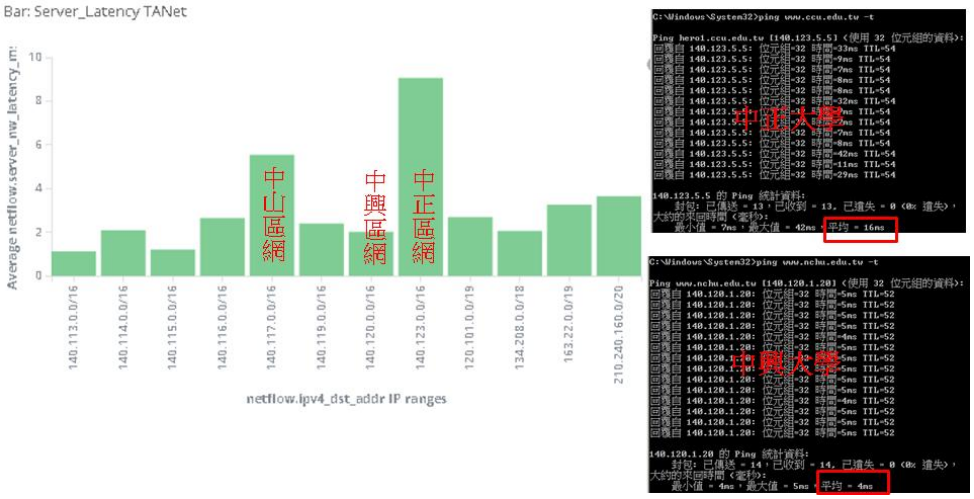



圖 9、Latency 24 Hrs 各區網中心統計

己、 辨識不同網段用途 Client 上網方式

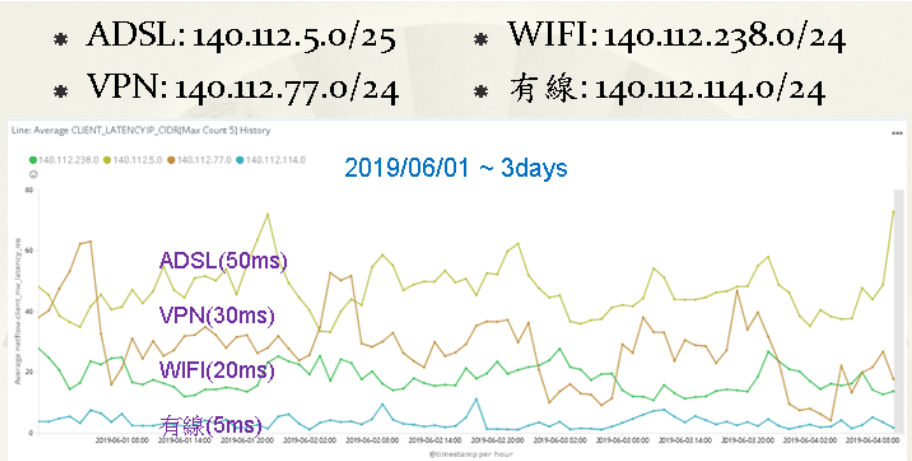



圖 10、辨識不同網段用途 Client 上網方式

庚、 辨識網段內連網設備 140.112.3.0/24 計中工作區

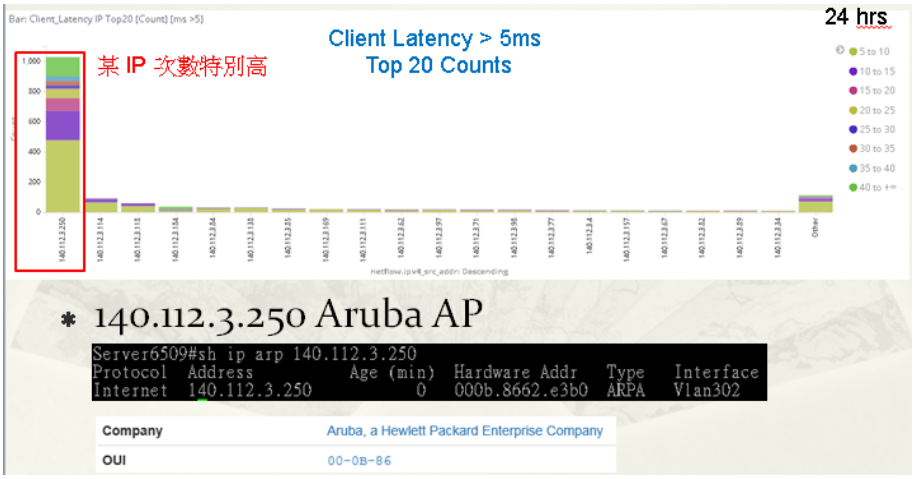



圖 11、辨識網段內連網設備

辛、 頻寬壅塞對 Client Latency 之影響--系所網路壅塞

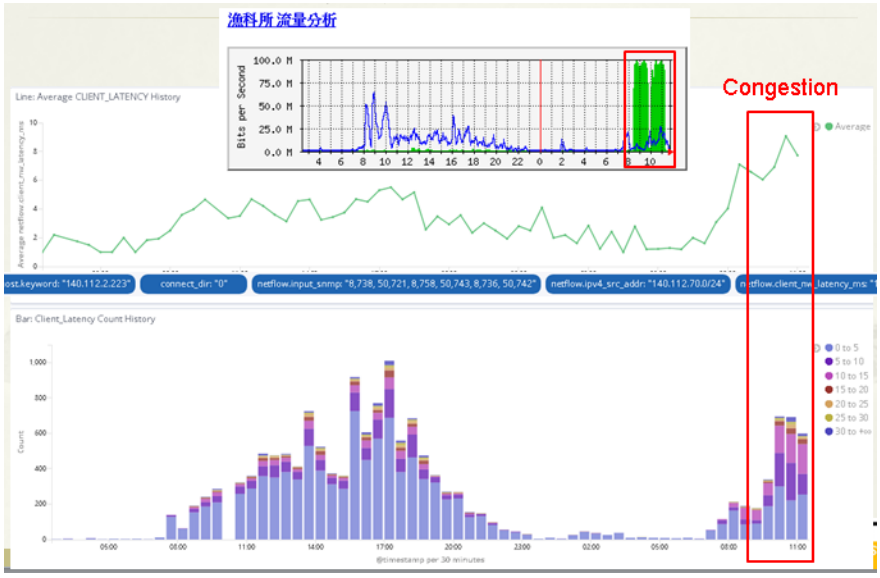



圖 12、頻寬壅塞對 Client Latency 之影響

壬、 頻寬壅塞對 Server Latency 之影響--國際頻寬壅塞

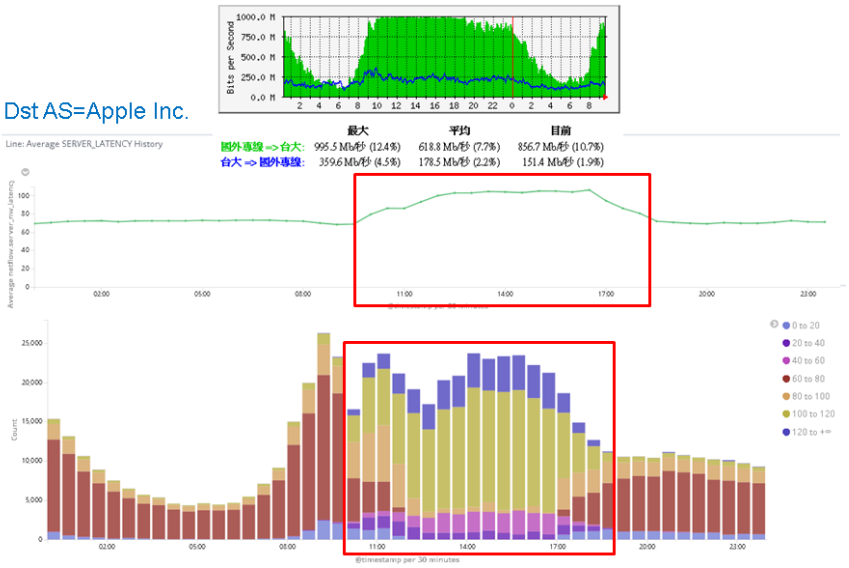



圖 13、頻寬壅塞對 Server Latency 之影響

## (二) IPv4 地理位置資料庫準確度分析

IP 地理位置將 IP 虛擬連線位址，對應於地球上一個實際地點，可用於分析網站連線之使用者分佈區域或駭客攻擊行為之來源國家等。IP 地理位置並無明確規範與定義，因此有許多商業公司在網路上販賣 IPv4 地理資料庫資訊。

此處提出三種方法驗證資料庫的正確性。

1. 使用 ISP 資訊驗證

在 2014 年國內某 ISP 與本校計資中心合作一個網路測速計畫，計畫目的在驗證臺灣六都城市之家用網路頻寬確實有達到 ISP 所宣稱之網路速度該計畫即使用 IP 地址來辨識參與測速之家用網路實際所在之城市地點。

| DB | 總筆數 (高雄) | Country 正確筆數 | City 正確筆數 | Country 正確率 | City 正確率 |
|---|---|---|---|---|---|
| dbip | 723 | 723 | 0 | 100% | 0% |
| geolite2 | 723 | 723 | 9 | 100% | 1.2% |
| ip2location | 723 | 723 | 430 | 100% | 59.4% |

2. 使用 Round Trip Time 驗證

在網際網路中封包從出發到目的節點來回所需的時間稱為 Round Trip Time，此 Round Trip Time 之計算基於物理限制，最短時間為”以光速行進來回所需的時間”。

舉例說明，使用 Google Map 量測台北到洛杉磯之直線距離約為 10,899 公里，而光線每秒行進之距離為 299,792 公里，因此以光速從台北到洛杉磯來回最短時間為 10,899 * 2/ 299,792= 72 ms。而網路封包同樣從台北到洛杉磯之網路傳輸使用海纜光纖，而海纜佈線通常無法直線抵達，加上途中經過許多網路設備有很多 Queuing 與 Forwarding 處理時間，由此可知網路封包從臺灣抵達美國本土之 Round Trip Time 絕對不可能小於 72 ms。

使用 Google 首頁網址 www.google.com，其所對應之 ipv4 位址 172.217.160.100。

接著以此 IP 分別至三家廠商提供之網頁版本位置資料庫查詢：

https://db-ip.com/172.217.160.100

https://www.maxmind.com/en/geoip2-precision-demo

https://www.ip2location.com/demo/172.217.160.100

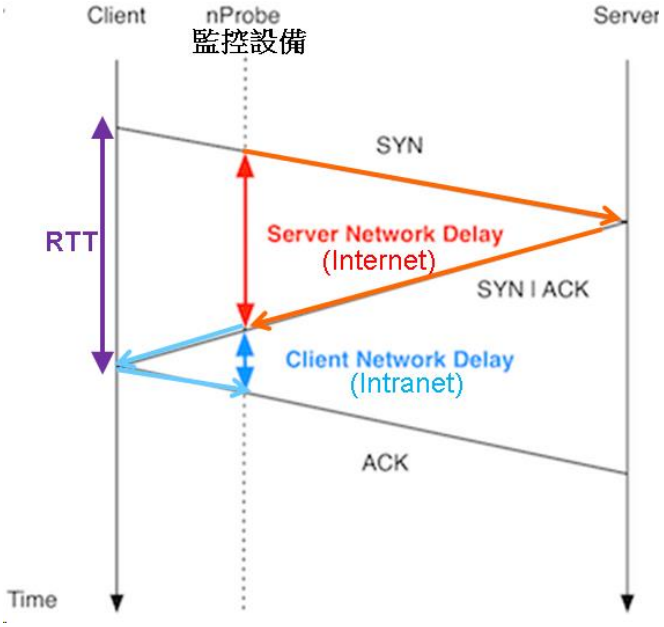
查詢結果僅有 DB-IP 資料庫顯示其地理位置在台灣，另兩家資料庫皆顯示位置在美國。

接著使用 ping 指令測試由台大校園至此 Google 首頁 IP 172.217.160.100 所需 Round Trip Time 需時 1 ms。


由實際網路封包測試僅有 1 ms 之結果來看，此 Google IP 實際地理位置應該在台灣而不可能在美國，以此範例可知僅有 DB-IP 資料庫為正確，另兩家資料庫提供之資訊為錯誤。

3. 使用大數據分析與實際量測來驗證

TCP Session 在建立之初，Client 與 Server 需透過 Three Way Handshake 交換訊息，若在 Client 與 Server 連線途中部署一台監測設備 nProbe，藉此量測 SYN 與 SYN/ACK 封包出現之時間差，即可得知此監測設備到 Server 連線來回之時間，此時間差可稱為 Server Delay Time。



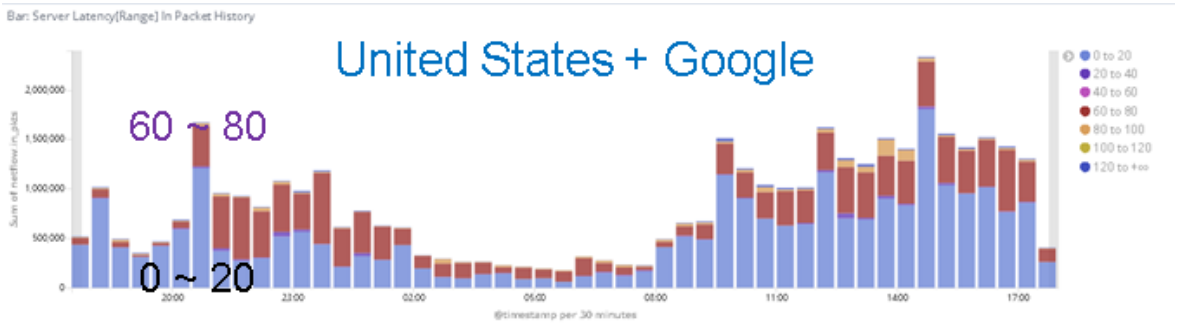

甲、 Country + ASN 平均值與其他 ASN 差異太大：大部分 IP，GeoIP DB 不正確

| Country | AS Org | ASN | Avg Delay(ms) |
|---|---|---|---|
| United States | Cloudflare Inc | 13,335 | 34.76 |
| United States | CloudRadium L.L.C | 33,330 | 74.453 |
| United States | Centrilogic, Inc. | 31,863 | 80.844 |
| United States | Centrilogic, Inc. | 19,693 | 102.462 |
| United States | Highwinds Network Group, Inc. | 20,446 | 26.249 |
| United States | Level 3 Communications, Inc. | 3,356 | 69.701 |
| United States | Level 3 Communications, Inc. | 3,549 | 78.526 |
| United States | Level 3 Communications, Inc. | 10,753 | 96.5 |
| United States | Sprint | 1,239 | 62.74 |
| United States | Unwired | 32,354 | 70.678 |
| United States | Fastly | 54,113 | 39.239 |
| United States | netDNA | 54,104 | 24.743 |
| United States | Massachusetts Institute of Techn | 3 | 82.457 |
| United States | Akamai International B.V. | 20,940 | 18.898 |
| United States | Akamai International B.V. | 33,905 | 83.675 |
| United States | Akamai International B.V. | 21,342 | 62 |
| United States | Akamai Technologies, Inc. | 35,994 | 13.896 |
| United States | Akamai Technologies, Inc. | 16,625 | 22.808 |
| United States | Dropbox, Inc. | 19,679 | 105.147 |

乙、 Country + ASN Deviation 過大：部分 IP ，GeoIP DB 不正確

| Country | AS Org | ASN | Avg Delay(ms) | Standard Deviation |
|---|---|---|---|---|
| United States | Apple Inc. | 714 | 76.21 | 965.279 |
| United States | Apple Inc. | 6,185 | 41.032 | 115.196 |
| United States | Amazon.com, Inc. | 16,509 | 1,192.79 | 6,257.81 |
| United States | Amazon.com, Inc. | 14,618 | 901.908 | 5,929.70 |
| United States | Microsoft Corporation | 8,075 | 79.898 | 268.647 |
| United States | Microsoft Corporation | 8,068 | 91.142 | 1,393.45 |
| United States | Microsoft Corporation | 3,598 | 75 | 85.436 |
| United States | Cloudflare Inc | 13,335 | 35 | 485.379 |
| United States | CloudRadium L.L.C | 33,330 | 74 | 181.358 |
| United States | Centrilogic, Inc. | 31,863 | 81 | 433.495 |
| United States | Centrilogic, Inc. | 19,693 | 102 | 109.72 |
| United States | Highwinds Network Group, Inc | 20,446 | 26 | 122.25 |
| United States | Level 3 Communications, Inc. | 3,356 | 70 | 330.522 |
| United States | Level 3 Communications, Inc. | 3,549 | 79 | 92.897 |
| United States | Level 3 Communications, Inc. | 10,753 | 97 | 99.5 |

丙、 Country + ASN 分佈比例異常：部分 IP ，GeoIP DB 不正確




## (三) Layer7 網路行為分析

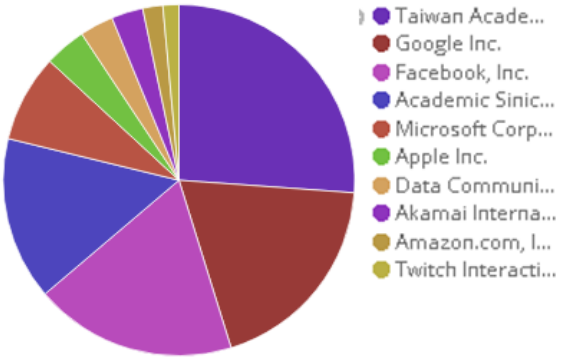
網管人員對於網路流量之分析，過去大都使用 MRTG 進行流量或封包數分析，但對於使用者上網行為一般常使用 UDP、TCP 加上 Port Number 進行分析，而此方法在現今網頁服務已成主流之情況下，分析結果已無特別意義。目前較有意義之呈現方法有 IP-Based + AS Number 及使用 nDPI 兩種方法來進行網路行為分析。

1. L7 網路分析使用 AS Number

在 Internet 上使用之 Public IP address 原則上都有該 IP 或網段所屬之識別號碼，稱為 Autonomous System Number(ASN)，ASN 是 BGP 路由協定用來交換路由資訊之重要資訊之一，藉由查詢 ASN 之擁有者或註冊者，可大略知道使用者之上網行為。

至於如何查詢 IP 所屬 ASN 有多種方法，針對單一或少數 IP 可查詢網路上免費提供之 Looking Glass Server 得知 ASN，至於需要批次查詢大量 IP 則建議使用 IP Geolocation 資料庫中所提供之 ASN 資訊，可自行在網路上搜尋 maxmind、ip2location 皆有提供此資料庫服務。

此方法還有個優點，就是適用於傳統 IP-Based 分析方法例如 netflow，統計網路流量中所有 IP 之 ASN 資訊後，可依據 ASN 流量大小進行排序，如下圖 19 所示，流量最高為臺灣學術網路，其他依序為 Google、Facebook 等。



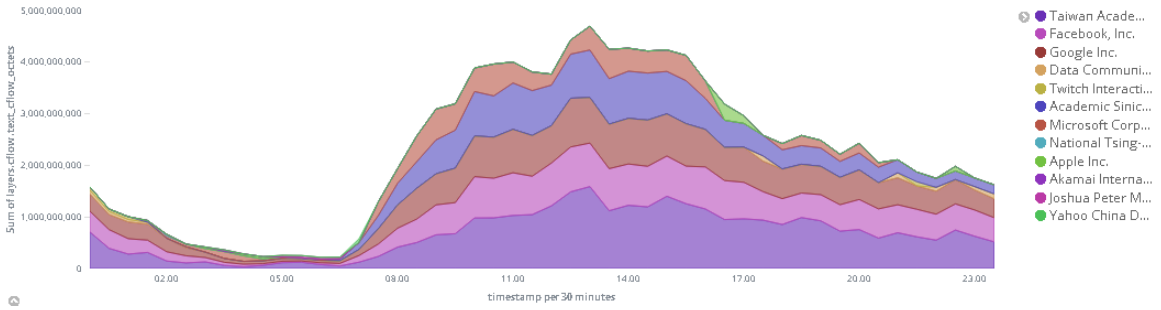
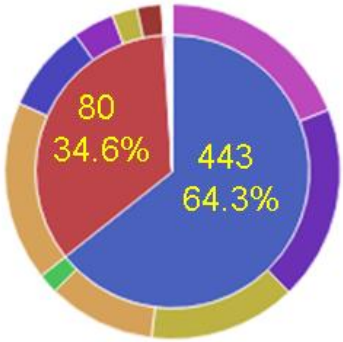



圖 19、 L7 網路分析 AS Number

使用 AS Number 分析上網行為的方法，還可結合 Port Number 進行分析，可進一步瞭解網路協定與上網服務之進一步關係。如下圖 20 所示，其中牽涉個人隱私的服務 Facebook 全部使用加密服務，而非加密的服務包含臺灣學術網路、微軟與蘋果等相關服務。




| port | Source ASN | % |
|---|---|---|
| 443 | Facebook, Inc. | 26% |
| 443 | Google Inc. | 25% |
| 443 | Academic Sinica Network | 19% |
| 443 | Taiwan Academic Network (TANet) Information Center | 14% |
| 443 | Data Communication Business Group | 3% |
| 80 | Taiwan Academic Network (TANet) Information Center | 50% |
| 80 | Microsoft Corporation | 25% |
| 80 | Apple Inc. | 11% |
| 80 | Academic Sinica Network | 8% |
| 80 | Akamai International B.V. | 6% |

圖 20、網路行為分析 Port Number + AS Number

2. L7 網路分析使用 DPI

若要明確分析使用者上網行為，就需要對 TCP/IP 之應用層或第七層協定(Payload)進行分析，此方法一般稱為 DPI(Deep Packet Inspection )分析。

目前市面上已有許多商業硬體設備可進行 DPI 分析，例如 P-Cube 及之後被 Cisco 併購成為 Cisco SCE Service Control Engine 系列、Procera 等。這些商業設備使用 Proprietary protocol pattern 來分析封包中的 payload 資訊，藉此來辨識不同的網路應用協定，新的應用協定需有新的 pattern，而舊的應用協定 pattern 也可能隨時更改，

此方法需倚賴廠商不斷的更新來維持正確之辨識率。因此這些設備需有維護合約才能持續更新，但若設備本身也進入 End of Life or End of Service，那就真的只能自求多福了。

區網目前使用一套 Open Source DPI Library 稱為 nDPI，程式使用 Portable C library (Win and Unix, 32/64 bit)，可自行在 https://github.com/ntop/nDPI 下載及編譯。nDPI 專案在 Github 一直有著非常高的活躍度，如下圖 21 所示，從 2015 年至今仍不斷進行更新，因此靠著網路社群集眾多人之力可得到長久不斷之更新。

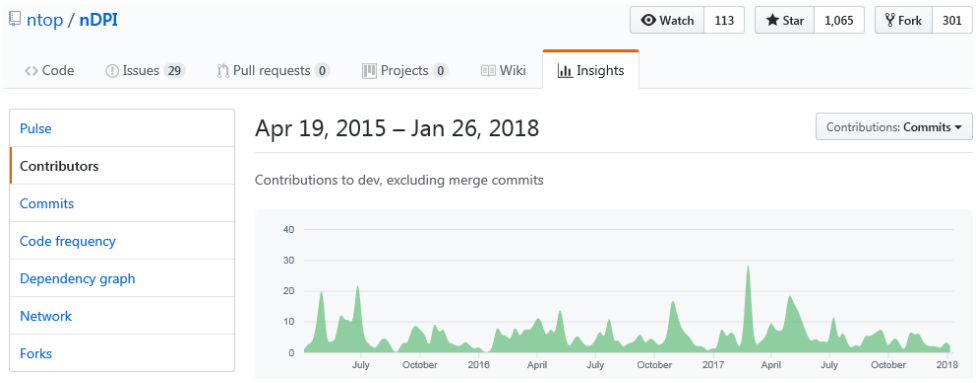



圖 21、 nDPI 於 Github 上之活躍度

目前 nDPI v2.3.0 已可辨識 239 以上之 protocols，支援之應用類別如下：

P2P (Skype, BitTorrent)
Messaging (Viber, Whatsapp, MSN, The Facebook)
Multimedia (YouTube, Last.gm, iTunes)
Conferencing (Webex, CitrixOnLine)
Streaming (Zattoo, Icecast, Shoutcast, Netflix)
Business (VNC, RDP, Citrix, *SQL)

佈建 nDPI 之網路架構圖如圖 22，將連線學校之網路流量 Mirror 至 nDPI reader，nDPI reader 產生 JSON 檔案後匯入 ELK Stack 進行統計與圖表繪製。

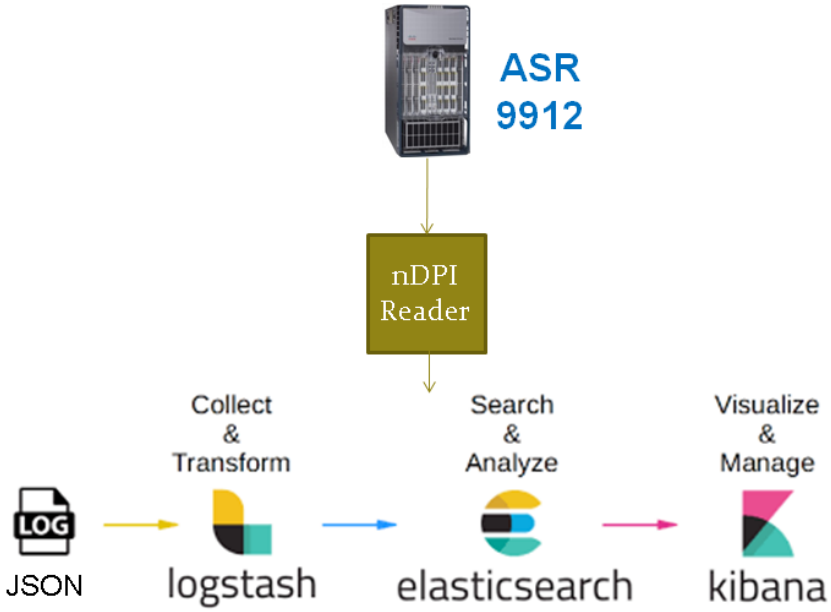



圖 22、 nDPI 佈建網路架構圖

Layer7 應用協定分析可顯示過去 24 小時 Top20 Layer7 應用協定如圖 23，另外提供過去 24 小時 Layer7 應用協定分佈之流量如圖 24，即時動態之圖表呈現於網址 http://www.tp1rc.edu.tw/layer7.html


圖 23、 Top20 Layer7 應用協定

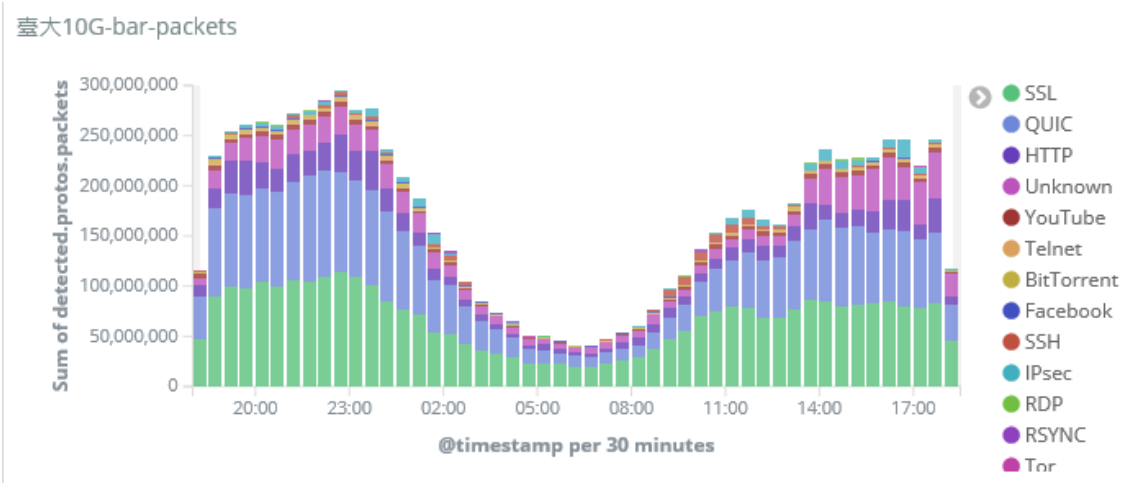



圖 24、過去 24 小時 Layer7 應用協定分佈流量圖

## (四) Line Bot 即時網頁內容搜尋系統

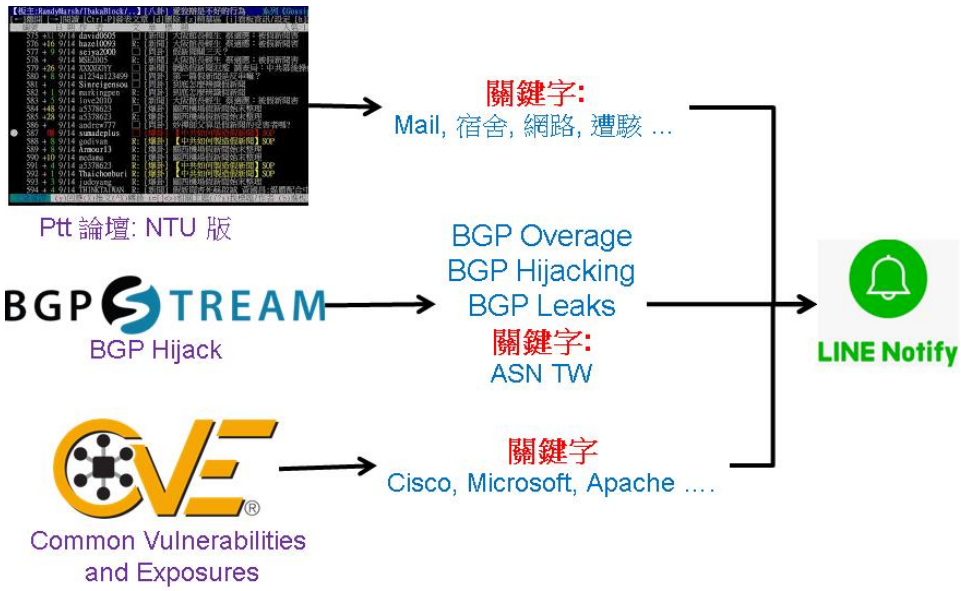



圖 25、Line Bot 即時網頁內容搜尋系統

1. ptt.cc 鄉民訊息~快速掌握

維持網路高可用性始終是網路管理之重要指標，但許多使用者對於網路異常卻不一定會循正常管道通報網管人員，而可能直接在社群網站或網路論壇 Post 文章進行抱怨與推文，此類訊息網管人員往往不容易掌握，或甚至後知後覺。因此開發一套 Line Bot 即時網頁內容搜尋系統，可搜尋事先定義好之關鍵字，例如:'信箱','

宿舍', '網路', '駭', 'ceiba', '掛', '壞' 等，當有文章標題符合這些關鍵字時，即可使用 Line Notify 即時通知網管人員，可快速掌握鄉民訊息並立即採取應映措施。下圖即是 2019 年 11 月計中 Email 信箱出問題及教務處 Ceiba 系統出問題時， ptt.cc 上之 Post 文章，即時使用 Line Notify 通知之畫面。

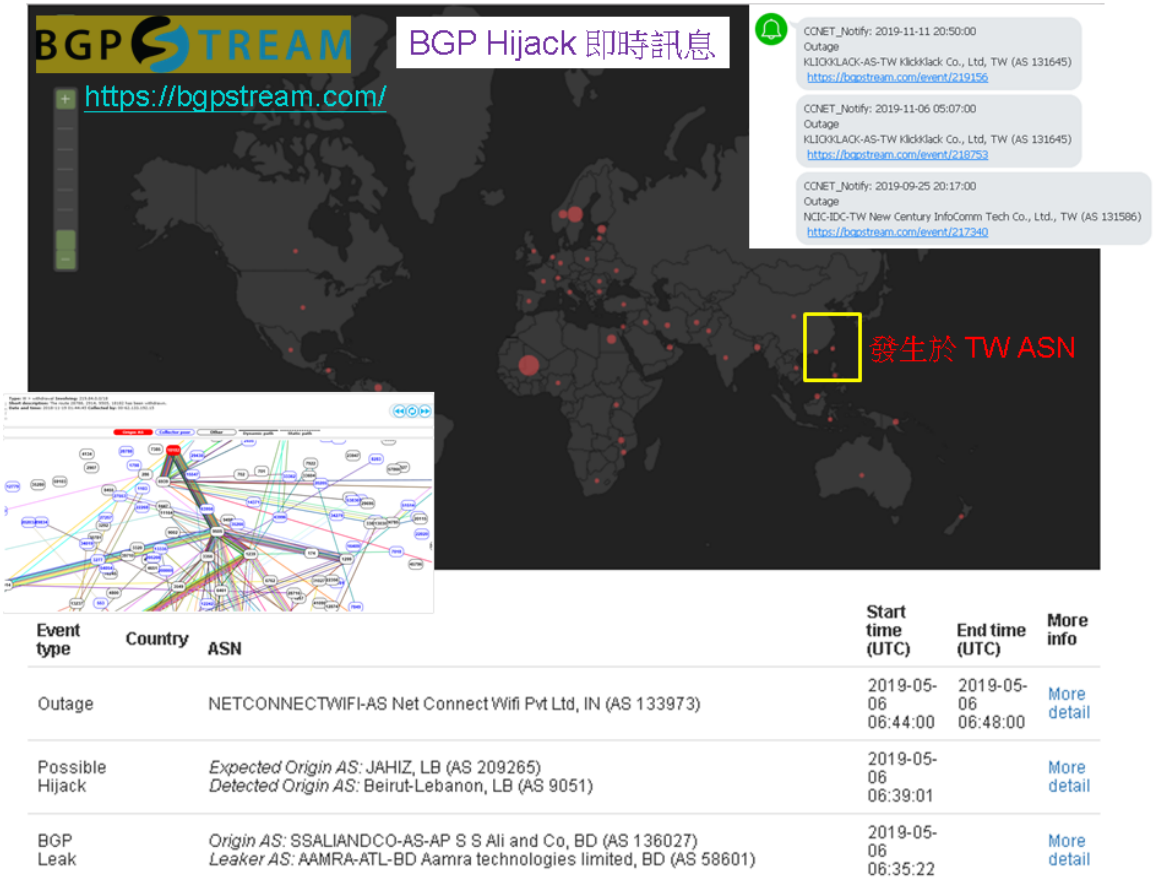

圖 26、ptt 鄉民訊息~快速掌握~

2. BGP Hijacking 即時訊息

BGP 路由協定為不同 Autonomous System(自治系統, 簡稱 AS) 彼此交換路由之方法，若有 BGP Hijacking 發生，影響的使用者至少數以萬計，因此網管人員應時時注意是否有自己或鄰近之 AS 有發生 BGP Hijacking 事件，https://bgpstream.com/ 在全世界各大 ISP 有佈建許多偵測 BGP AS Path 變化之監控設備，因此可即時偵測世界各地 BGP Hijacking 事件。

因此開發一套 Line Bot 即時網頁內容搜尋系統，可搜尋 https://bgpstream.com/ 註冊於台灣 TW 之 AS 若有 BGP Hijacking 發生，即可利用 Line Notify 即時通知網管人員。下圖即是顯時發生於 TW 之 AS 有 BGP Hijacking 發生時，可即時於 Line

Notify 上顯示。




| 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)<br>*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)<br>*Leaker AS:* AAMRA-ATL-BD Aamra technologies limited, BD (AS 58601) | 2019-05-06 06:35:22 | | More detail |

圖 27、BGP Hijacking 即時訊息

3. 資安漏洞~快速掌握~

各種作業系統、應用程式或甚至是網路設備之漏洞，一直是網管人員必須時時刻刻、戰戰兢兢面對的挑戰，目前對於所有已知漏洞威脅蒐集最即時也最完善的莫過於 CVE Database。因此開發一套 Line Bot 即時網頁內容搜尋系統，可搜尋 https://nvd.nist.gov/vuln/search 之已公佈 CVE 漏洞資訊，並以校內常見與使用之產品名稱如 Cisco, Microsoft, Apache 等進行過濾搜尋，即可利用 Line Notify 即時通知網管人員，可快速掌握產品漏洞訊息並立即採取應映措施。下圖即是顯時 Cisco FirePower 系列於 2019 年 11 月 發現之產品漏洞並即時顯示於 Line Notify。

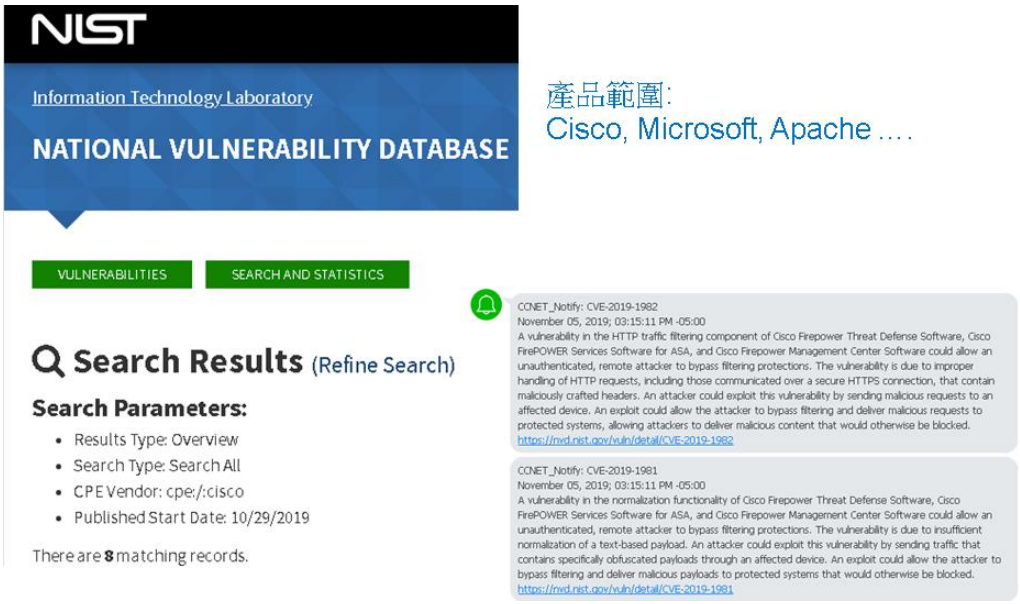



圖 28、資安漏洞~快速掌握

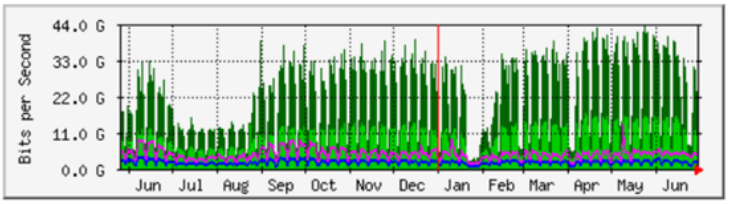
## (五) 使用大數據軟體 ELK Stack 分析學網史上最大規模 DDoS 攻擊事件

1. DDoS 攻擊

- 攻擊方法: SYN Flood
- 攻擊期間: 4/20 ~ 5/15 (幾乎每天都有)
- 持續時間: 5 分鐘~ 1 小時
- 攻擊來源: 3 Subnets(/24)
- 89.248.163.0/24、89.248.165.0/24、92.63.196.0/24
- 攻擊目的:
- TANet 全網段，/24 網段輪流: 每次 1 ~ 3 分鐘
- 攻擊目的 Port: Random

2. TANet 100G 臺北主節點 攻擊期間: 4/20 ~ 5/15

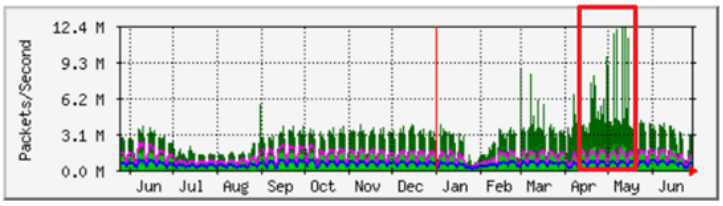
`Yearly' Graph (1 Day Average) 流量 bits per-second




流量圖
無法顯示異常

| | Max | Average | Current |
|---|---|---|---|
| 台北主節點 => 北區區網 | 43.8 Gb/s (43.8%) | 8850.3 Mb/s (8.9%) | 11.5 Gb/s (11.5%) |
| 北區區網 => 台北主節點 | 13.1 Gb/s (13.1%) | 1845.4 Mb/s (1.8%) | 2116.3 Mb/s (2.1%) |

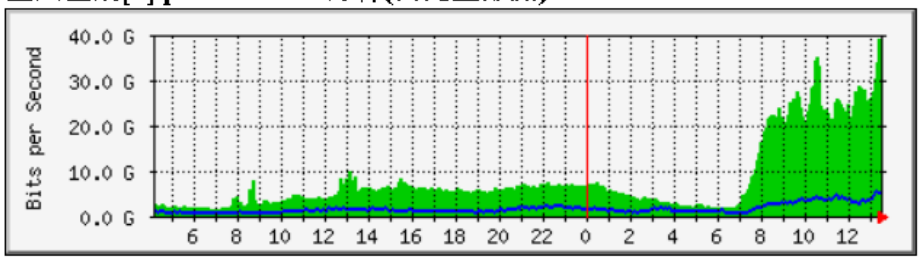
`Yearly' Graph (1 Day Average) 封包數 packets per-second



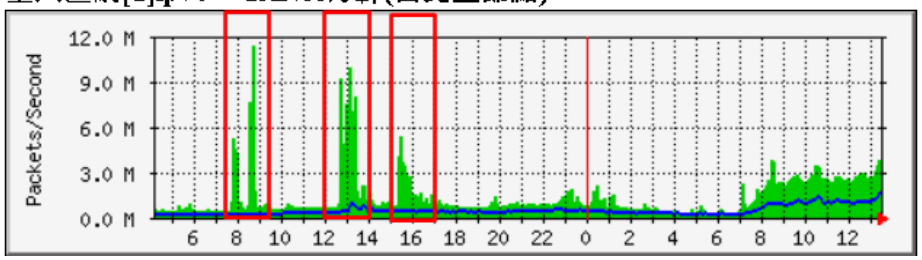

| | Max | Average | Current |
|---|---|---|---|
| In 封包數, Packets | 12.4 Mpkt/sec | 1043.3 kpkt/sec | 1132.8 kpkt/sec |
| Out 封包數, Packets | 2292.3 kpkt/sec | 488.3 kpkt/sec | 469.2 kpkt/sec |

3. 5/14 假日持續進行攻擊

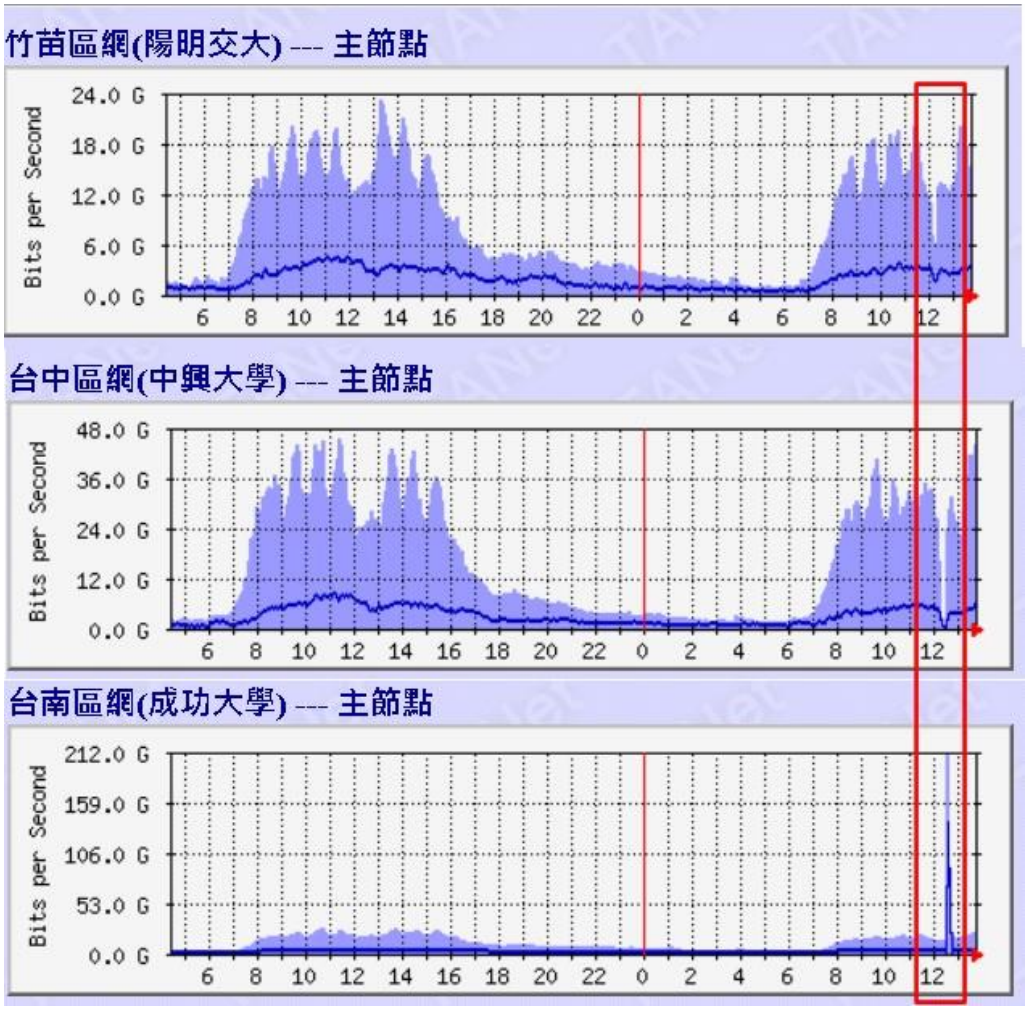
臺大區網[1]ipv4 -- TANet骨幹(台北主節點)




臺大區網[1]ipv4 -- TANet骨幹(台北主節點)

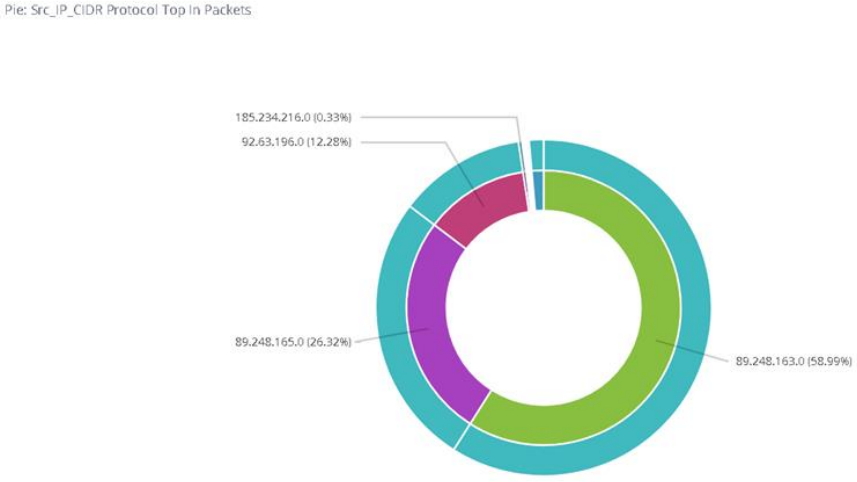



4. 其他區網同樣遭受攻擊

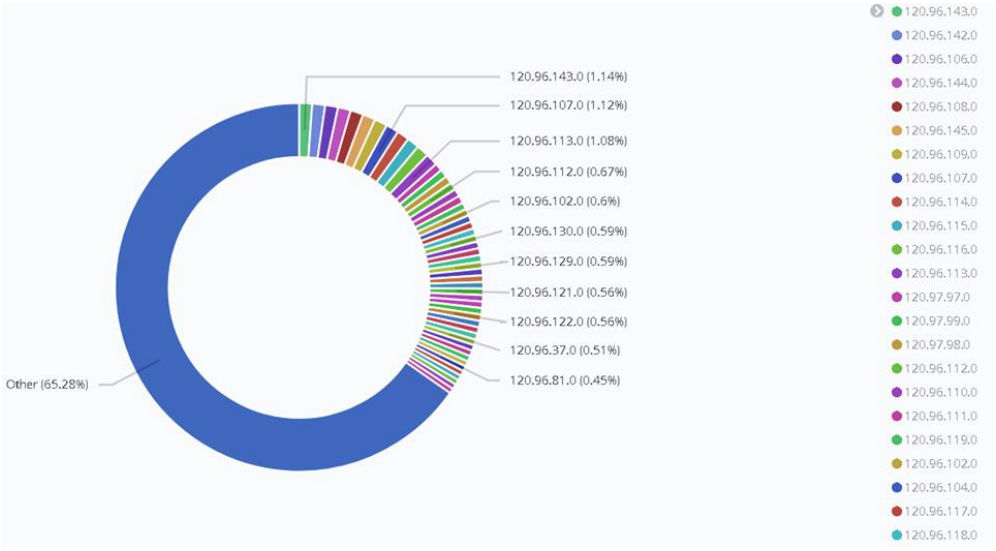



5. 分析攻擊來源 CIDR /24

- 89.248.163.0/24、89.248.165.0/24、92.63.196.0/24

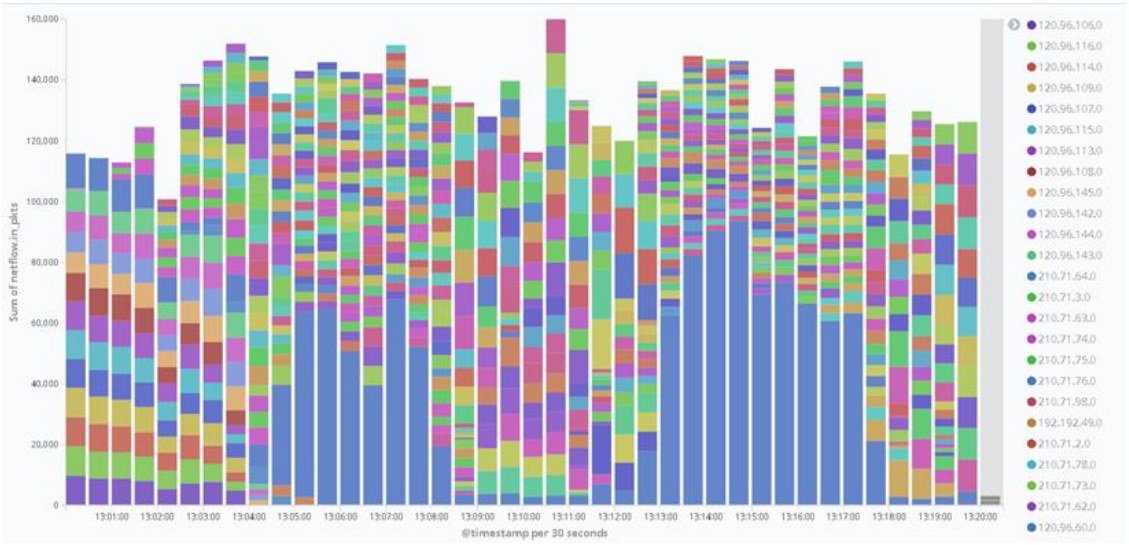



6. 分析攻擊目的 IP CIDR /24

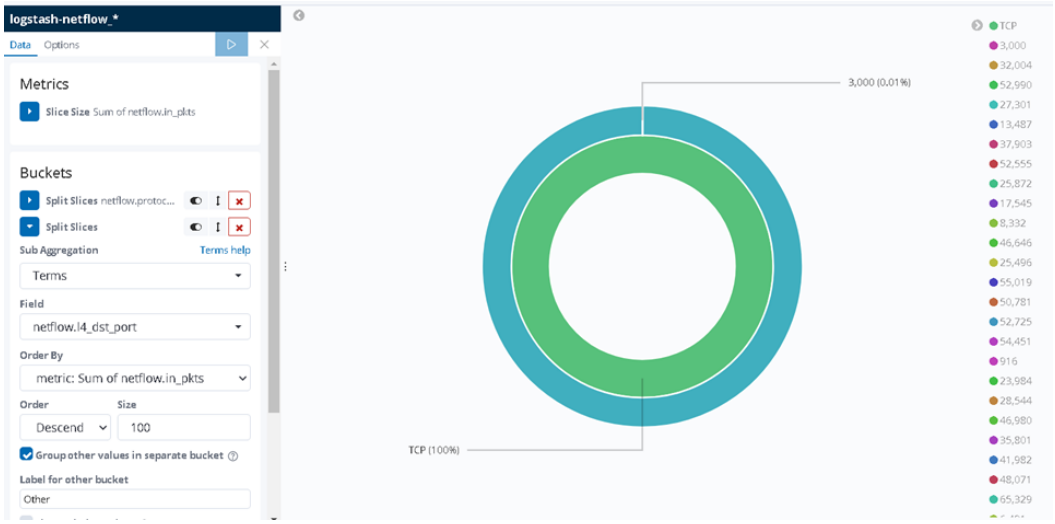



7. 分析攻擊目的 IP CIDR /24

Class C 網段輪流: 每次 1 ~ 3 分鐘




8. Dest Port Top100 (Random)




9. 阻擋方法

- DDoS 導流清洗(Out of Band)

將攻擊”來源 IP” 導入流量清洗

※過去皆是導流”目的 IP”

- Router 用 ACL 將攻擊來源 IP 封包 Drop

ACL 設定於區網端 100G 介面 In

ACL 設定於 TANet Border Router 介面 In

- Router 用 ACL 將攻擊來源 AS 所有 IP 網段封包 Drop

於 TANet Border Router 介面 In

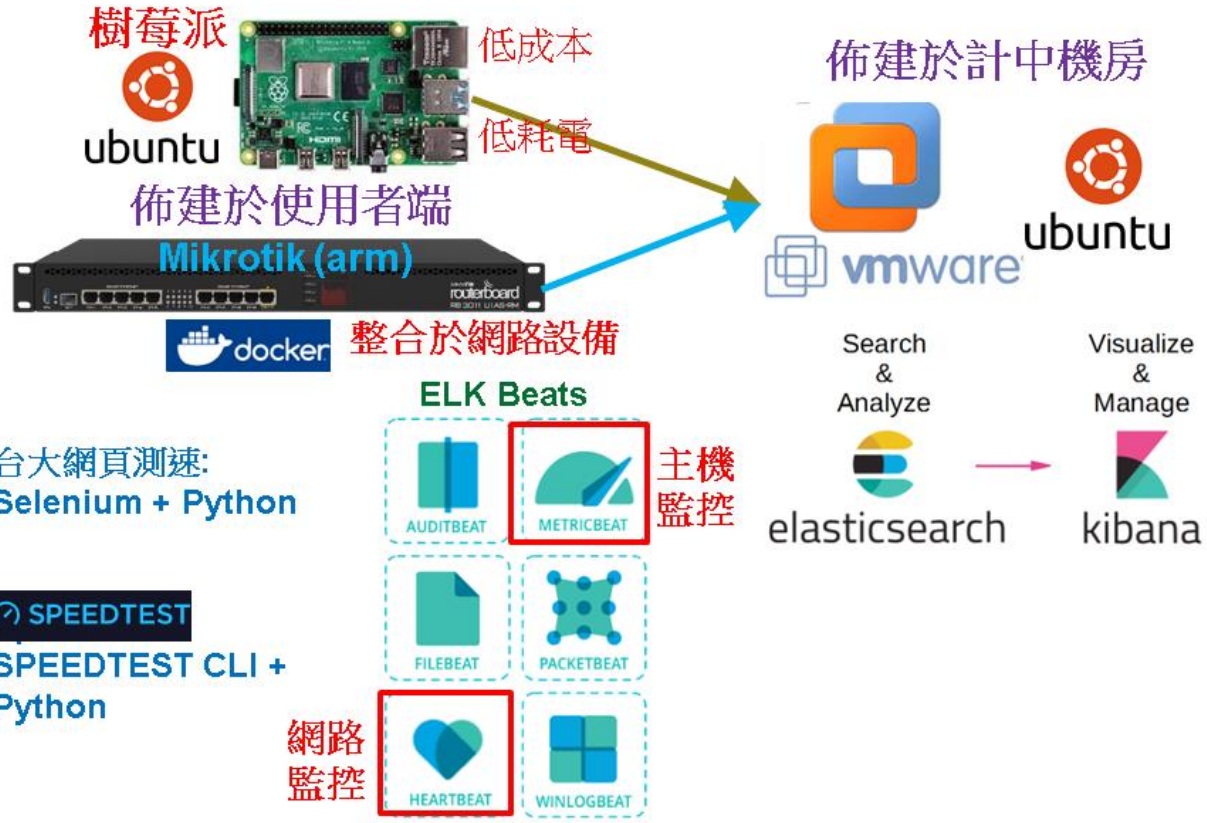
教育部駐點工程師採用此方式


## (六) 使用者端網路品質監控系統

1. 網管面臨挑戰

   - 使用者反應網路偶有異常斷線、網速過慢等情況
   - 骨幹網路監控無法呈現使用者情況
   - 以使用者角度長期記錄網路量測數據
     - ELK Heartbeat: ICMP ping、RTT 量測、HTTP GET/POST Delay Time
     - 網頁測速: Speed Test

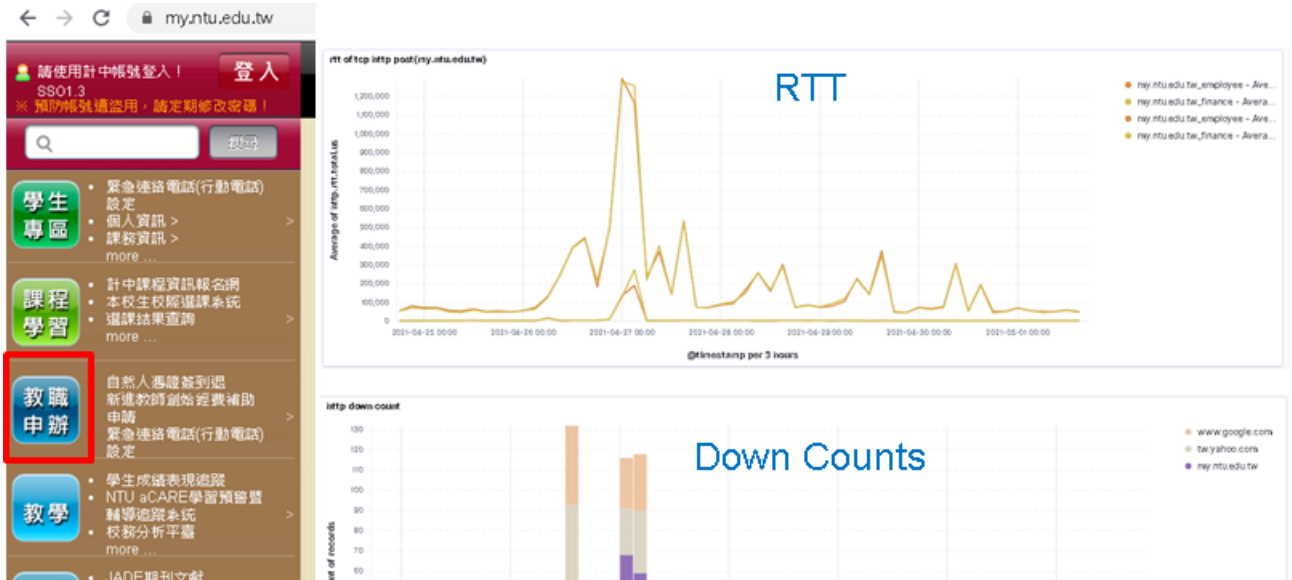
2. 建置架構圖




3. 使用樹莓派建置優點

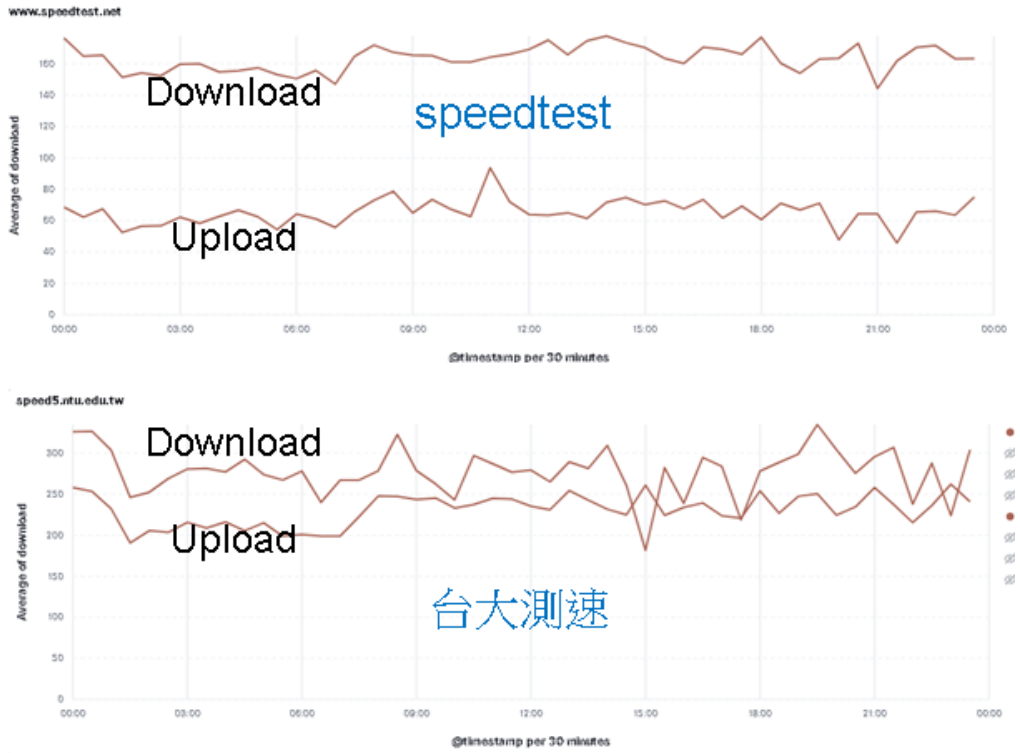
- 成本低 < $2000
- 低耗電 < 10Walt
- 體積小佈建容易
- 支援有線與無線網路監控

4. 校務系統監控

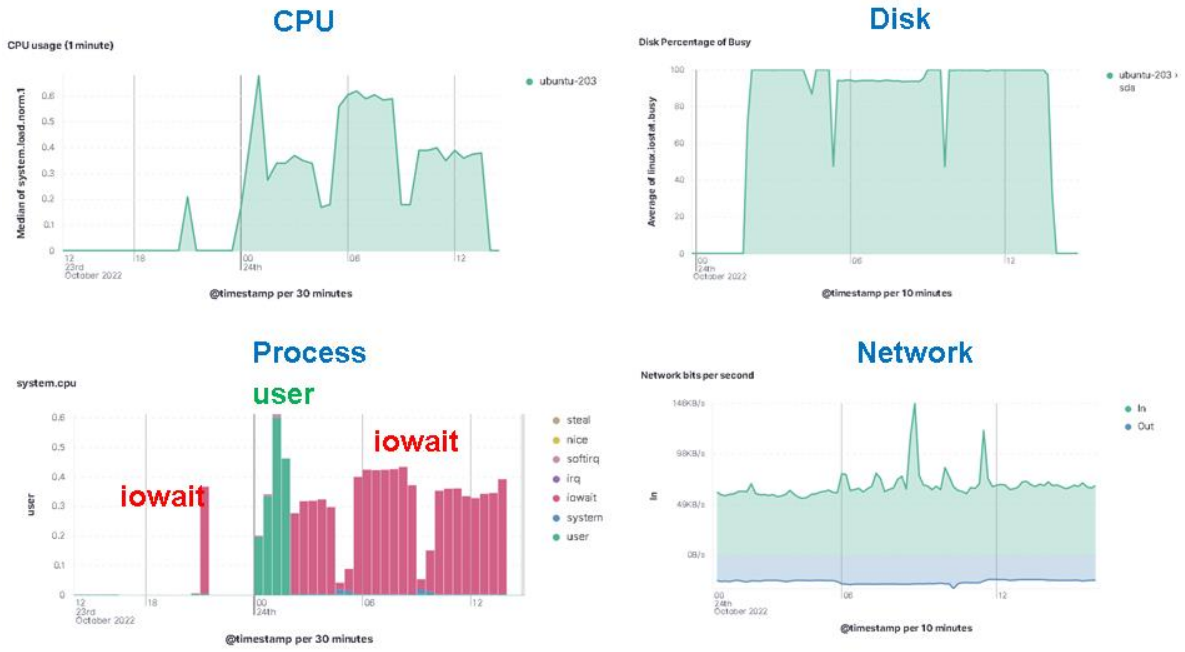


5. 網路測速

- speedtest http://www. speedtest.net
- 台大測速 http://speed5.ntu.edu.tw/

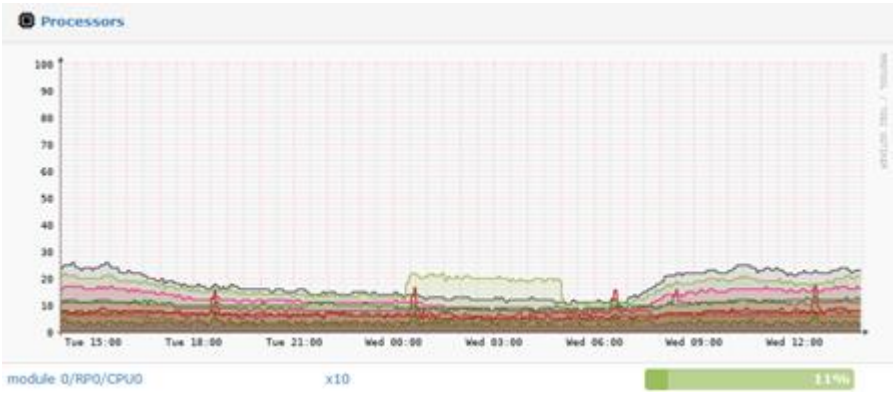



6. ELK Metricbeat 主機監控



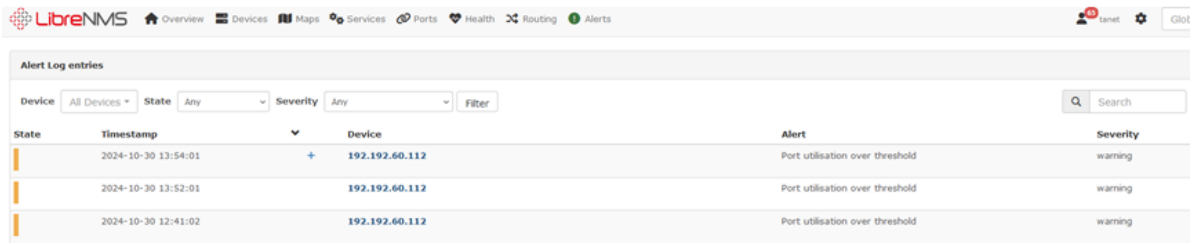

## (七) 架設 LibreNMS 提供區網連線單位網路品質監控

- LibreNMS 透過 SNMP 蒐集區網 ASR 相關資訊
- 架設告警系統以即時偵測設備狀況與流量
- 建立即時流量圖表
- SNMP 蒐集區網 Router 資訊，以即時監測設備狀態與告警

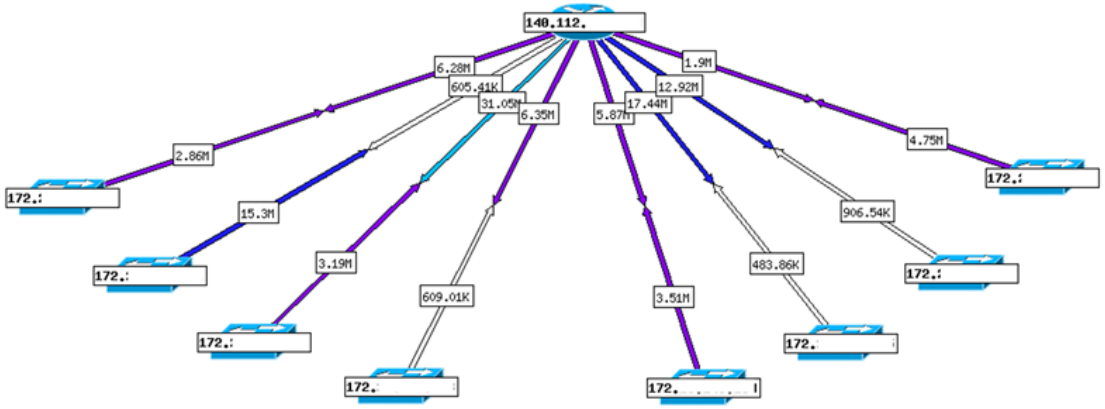




- LibreNMS 自動告警機制，建立斷線、流量異常等信件、Line 告警


- LibreNMS 可透過 WeatherMap 建立連線即時流量圖。預計後續架起該功能，以供查看。




## (八) Open Source WAF 從區網網站推廣至其他單位

■ 系所網站面臨問題

網站 OS、Web Server、動態程式，版本老舊無法升級，需重新安裝、程式重新改寫

原網站開發人員離職、無維護廠商

經費不足

■ 快速導入 WAF 防護機制

◆維持原網頁主機實體環境與 IP 網路架構

阻擋校外直接連線網頁主機( IPS 封鎖)，僅限校內存取

不需將網頁主機搬移至計中 VM 租賃區

計中 VM 租賃區規定: 主機弱掃、網站弱掃、原碼掃描、EDR(CrowdStrike)

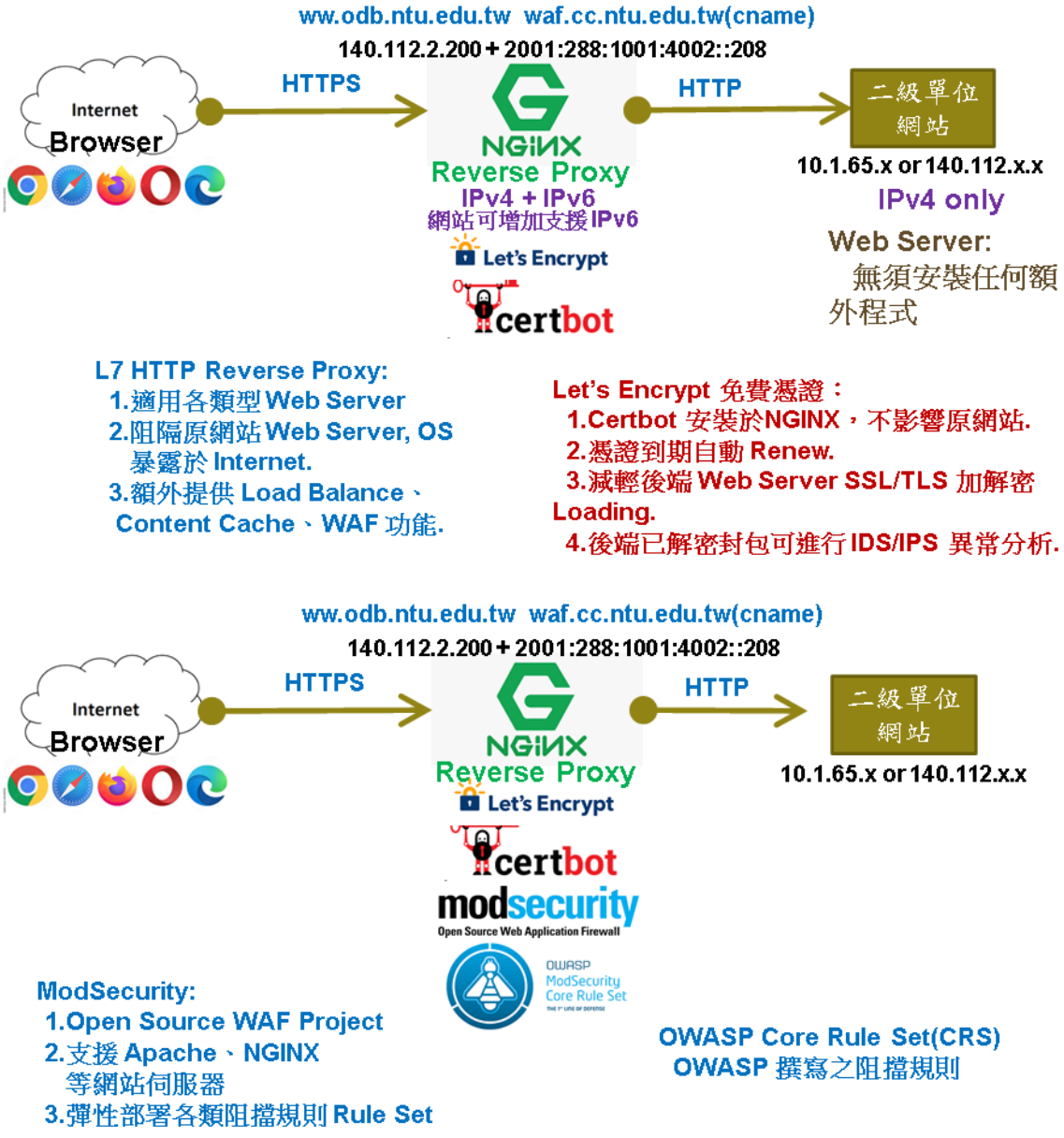
◆在校內可直接連線網頁後台、SSH、RDP

網頁管理後台不需通過 WAF 檢測，減少 WAF 規則誤擋

減輕 WAF 規則設定

不需在 WAF 設定 Port Forward for SSH, RDP

■ Open Source WAF 網頁防護架構




■ DNS 設定方法

原網站使用 DNS Alias Name 指向 waf.cc.ntu.edu.tw

www.odb.ntu.edu.tw IN CNAME waf.cc.ntu.edu.tw

設定 waf.cc.ntu.edu.tw 之 A Record 記錄

waf.cc.ntu.edu.tw IN A 140.112.2.x

原網站 IP

維持 140.112.x.x (IPS 封鎖，僅限校內存取)

改成 10.1.x.x

■ AppScan 掃描結果比較

* 原網站


| 問題類型 | | 問題數目 |
|---|---|---|
| 重 | 有漏洞的元件 | 144 |
| 高 | API 不當資產管理 | 2 |
| 高 | 發現不存在網域的鏈結 | 1 |
| 高 | 盲目的 LDAP 注入 | 3 |
| 中 | CORS 原則是依據任意原始標頭所設定 | 1 |
| 中 | Microsoft Windows MHTML 跨網站 Scripting | 1 |
| 中 | SameSite 屬性不安全、不適當或遺漏的 Cookie | 1 |
| 中 | 不安全的第三方鏈結 (target="_blank") | 47 |
| 中 | 偵測到 SHA-1 密碼組合 | 1 |
| 中 | 啟用 TRACE 與 TRACK HTTP 方法 | 1 |
| 中 | 找到目錄清單型樣 | 2 |
| 中 | 機密性標頭上的 ADNS 盲目 SSRF | 12 |
| 中 | 檢查是否有 SRI（子資源完整性）支援 | 15 |
| 中 | 目錄清單 | 2 |

* 導入 WAF 後

| 問題類型 | | 問題數目 |
|---|---|---|
| 重 | 有漏洞的元件 | 80 |
| 中 | 偵測到 SHA-1 密碼組合 | 1 |
| 中 | 檢查是否有 SRI（子資源完整性）支援 | 7 |

■ WordPress xmlrpc 程式 POST listMethod (成功阻擋)

Request

Pretty Raw Hex

```
1 POST /xmlrpc.php HTTP/1.1
2 Host: pc4.buda.idv.tw
3 Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
15 Priority: u=0, i
16 Connection: close
17 Content-Length: 95
18
19 <methodCall>
20   <methodName>
       system.listMethods
     </methodName>
21   <params>
22   </params>
23 </methodCall>
24
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 403 Forbidden
2 Server: nginx/1.24.0 (Ubuntu)
3 Date: Tue, 11 Jun 2024 09:14:24 GMT
4 Content-Type: text/html
5 Connection: close
6 Content-Length: 564
7
8 <html>
9   <head>
      <title>
        403 Forbidden
      </title>
    </head>
10  <body>
11    <center>
        <h1>
          403 Forbidden
        </h1>
      </center>
12    <hr>
      <center>
        nginx/1.24.0 (Ubuntu)
      </center>
13  </body>
14 </html>
15 <!-- a padding to disable MSIE and Chrome friendly error page -->
16 <!-- a padding to disable MSIE and Chrome friendly error page -->
17 <!-- a padding to disable MSIE and Chrome friendly error page -->
18 <!-- a padding to disable MSIE and Chrome friendly error page -->
19 <!-- a padding to disable MSIE and Chrome friendly error page -->
20 <!-- a padding to disable MSIE and Chrome friendly error page -->
21
```

■ Outbound Rules Test Directory Transversal

* https://ghp.ntu.edu.tw/icons/small/

**Index of /icons/small**

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| back.gif | 2004-11-21 04:16 | 129 | |
| back.png | 2007-08-28 18:53 | 181 | |
| binary.gif | 2004-11-21 04:16 | 134 | |
| binary.png | 2007-08-28 18:53 | 172 | |


messages: [Array]
[0]: [Object]
message: "Directory Listing"
details: [Object]
match: "Matched \"Operator `Rx' with parameter `(?:<(?:TITLE>Index of.*?<H|title>Index of.*?<h)1>Index of|>\\[To Parent Directory\\]</[Aa]><br>)' ag
reference: "o73,66v824,14299"
ruleId: "950130"
file: "/usr/share/modsecurity-crs/rules/RESPONSE-950-DATA-LEAKAGES.conf"
lineNumber: "35"
data: "Matched Data: <title>Index of /icons/small</title>\n </head>\n <body>\n<h1>Index of found within RESPONSE_BODY"
severity: "3"
ver: "OWASP_CRS/4.4.0-dev"
rev: ""
tags: [Array]
maturity: "0"
accuracy: "0"


3:ERROR Score:4


[1]: [Object]
message: "Outbound Anomaly Score Exceeded (Total Score: 4)"
details: [Object]
match: "Matched \"Operator `Ge' with parameter `4' against variable `TX:BLOCKING_OUTBOUND_ANOMALY_SCORE' (Value: `4' )"
reference: ""
ruleId: "959100"
file: "/usr/share/modsecurity-crs/rules/RESPONSE-959-BLOCKING-EVALUATION.conf"
lineNumber: "232"
data: ""
severity: "0"
ver: "OWASP_CRS/4.4.0-dev"
rev: ""
tags: [Array]
maturity: "0"
accuracy: "0"

## 三、強化與連線單位溝通及資安防護

### (一)工作內容

1. 因應個資法的實施，各校對於自己是否會無意中於網站洩漏個資而感到憂心，手動檢查也怕有所遺漏且浪費時間。現提供連線學校提供網站防洩漏個資偵測服務，使用掃描平台檢測目標網站，並將可能洩漏的風險輸出報告提供給使用者作為修正佐證。
2. 鑑於連線學校的網站多半為數位老師交接完成或架設已久從未檢查更新，常導致網站暴露許多可被利用的弱點，導致使用者會因為瀏覽網頁受害。現提供連線學校提供新版網站弱點掃描服務，使用掃描平台檢測目標網站，並將存在的弱點及可能產生的攻擊輸出報告提供給使用者作為修正佐證。
3. 由於區網底下連線學校眾多，各校也會自行架設 DNS server 提供服務，但因對設定不熟悉，便很容易成為公開的 DNS server 導致被利用來進行攻擊。現提供連線學校提供 DNS server 檢測，針對 Recursion、Transfer 及反解-完整性做檢查，並提供修正說明讓管理者可以依序操作修正設定。
4. 透過分流交換器流量分析功能，主動偵測區網連線單位內發生異常服務之主機，應可減少資安事件之發生。
5. 透過分流交換器篩選過濾網路流量，將加密封包過濾後，可大幅降低資安設備 IPS 之負載。
6. 所有區網對外流量，TANet 骨幹與 Peer ISP 共五家 8 條電路皆納入 IPS 偵測範圍，可保護區網轄下所有連線單位。
7. 區網 Peering ISP 電路包含中華電信、遠傳電信、臺灣固網、亞太電信、中嘉和網電信皆納入 IPS 偵測範圍，如圖 29 所示。

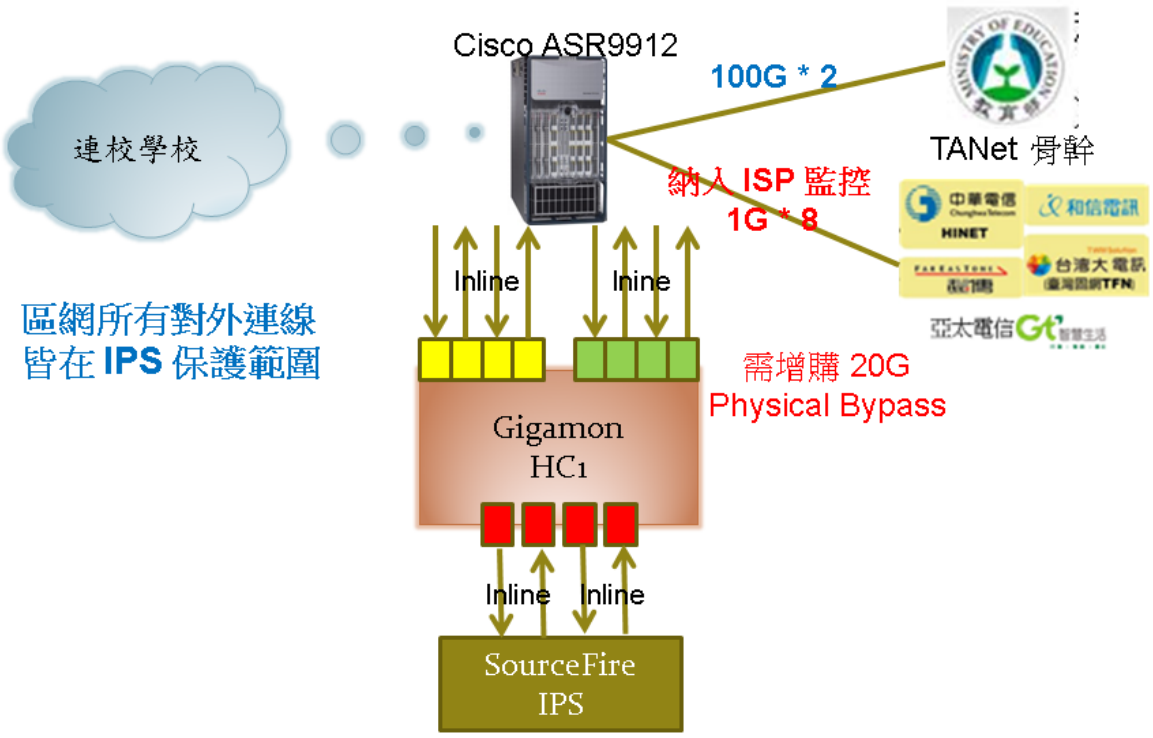



圖 29、Peer ISP 納入 IPS 偵測範圍

## (二)預期效益

1. 協助連線學校異常主機查找惡意程式，預計達成連線學校授與服務數之 100%。
2. 協助連線學校偵測是否於網站洩漏個資，預計達成連線學校授與服務數之 100%。
3. 協助連線學校偵測是否網站有弱點，預計達成連線學校授與服務數之 100%。
4. 協助連線學校偵測 DNS server 是否設定正確，預計達成連線學校諮詢數之 100%。

## (三)連線單位滿意度調查與結果

1. 題目:6 項選擇、2 項簡答

   甲、 本年度貴校(單位)之網路連線服務，您認為順暢度為何？

   乙、 本年度貴校(單位)如有網路管理或連線的技術諮詢時，區網中心的協助是否符合您的需求？

   丙、 資通安全事件的通報應變的協助處理？

   丁、 對區網所舉辦之教育訓練或研討(習)課程，是否能符合貴校(單位)實務運作上的需求?

戊、 貴校(單位)對於區網中心服務人員之熱忱及親和力的滿意度？

己、 貴校(單位)對於區網中心綜合整體服務的表現？

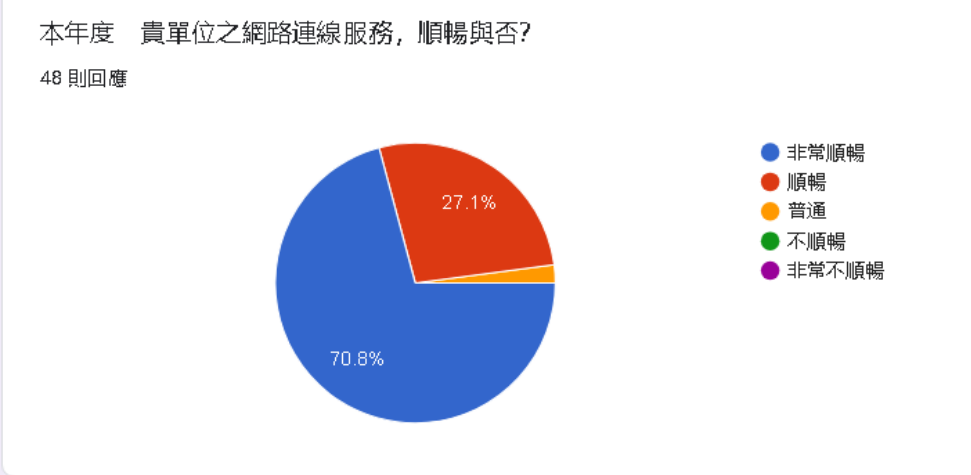
庚、 對區域網路中心在網路維運管理的建議

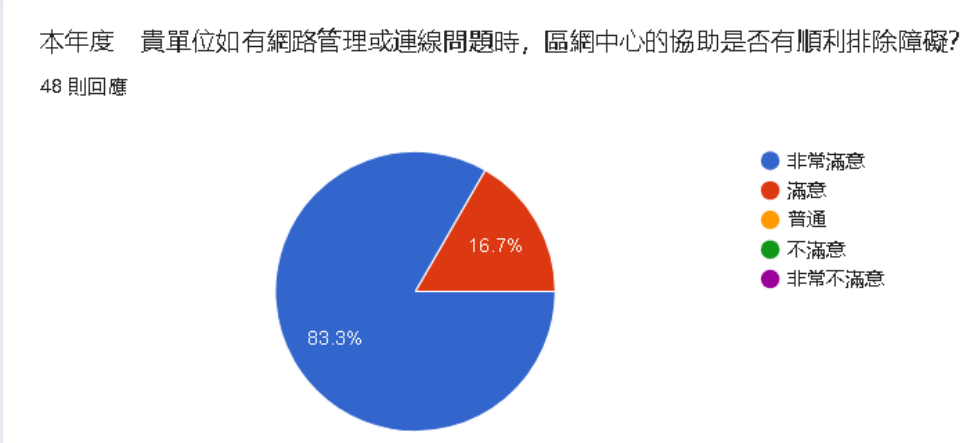
辛、 對區網所舉辦之教育訓練或研討(習)課程建議

2. 滿意度調查共有 54 連線單位，收到 48 份回覆，回覆率 89%

3. 非常滿意佔九成以上

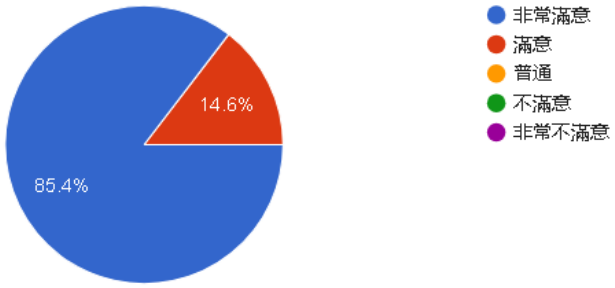
4. 節錄部分調查結果如下



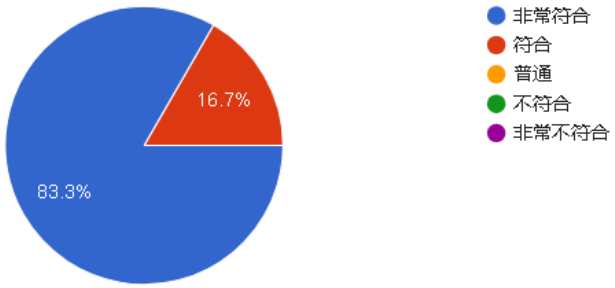
資通安全事件的通報應變的協助處理：

48 則回應



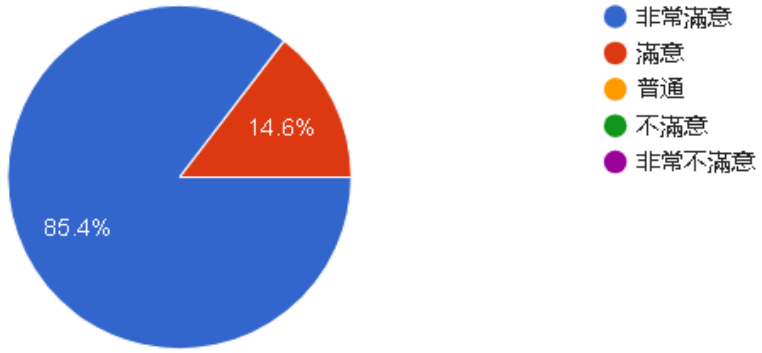

對區網所舉辦之教育訓練或研習課程，是否能符合　貴單位實務運作上的需求?

48 則回應



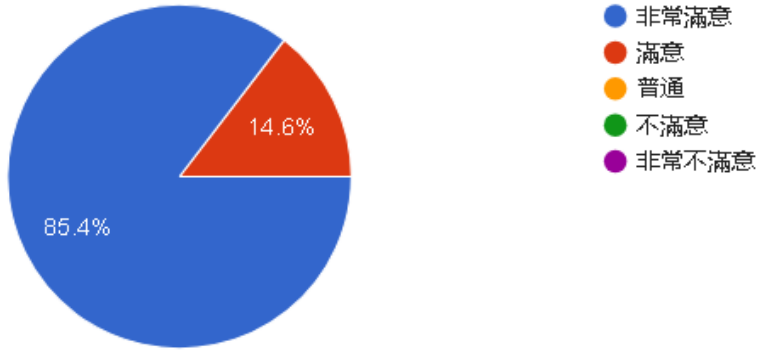
貴單位對於區網中心服務人員之熱忱及親和力的滿意度?

48 則回應




貴單位對於區網中心綜合整體服務的表現

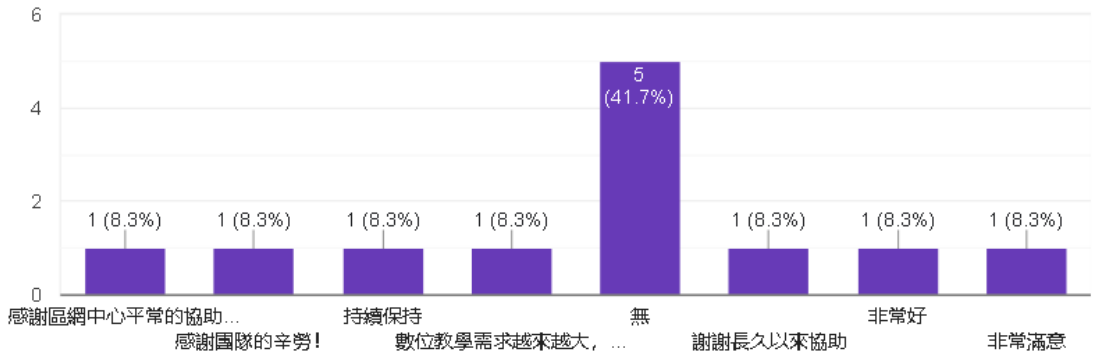
48 則回應




對區域網路中心在網路維運管理的建議

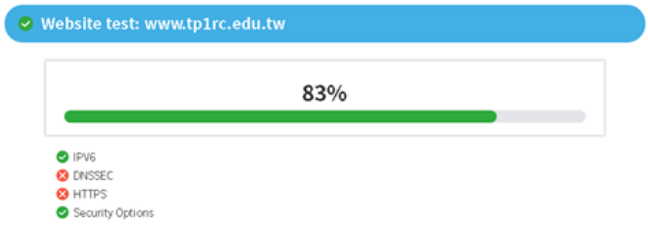
複製圖表

12 則回應



## (四) 連線單位 HTTPS 檢測支援

1. 臺北區網 I 檢測結果


2. 於區網課程及網管會議分享

- HTTPS 免費憑證安裝 Let's Encrypt
  - Certbot: Command Line 自動化安裝工具
  - SSL For Free : 網頁申請
- HTTPS Certificate Chain 常見問題與解決方法
  - 參考區網技術文件
  - https://www.tp1rc.edu.tw/e1.php

## (五) 教育體系資安檢核 GCB

1. 於區網課程及網管會議分享

- 資安檢核 GCB 導入案例分享
  - 技服 GCB 之規則及如何找出排除項，並使用微軟提供之免費工具 LGPO、Policy Analyzer 進行導入與檢核，提出三種不同的導入方法供使用者參考。
- 資安檢核 GCB 排除項參考文件
  - 臺大計資中心導入技服 GCB 規則之排除項目，增加”風險等級”欄位以供參考。
- 參考區網技術文件
  - https://www.tp1rc.edu.tw/e1.php

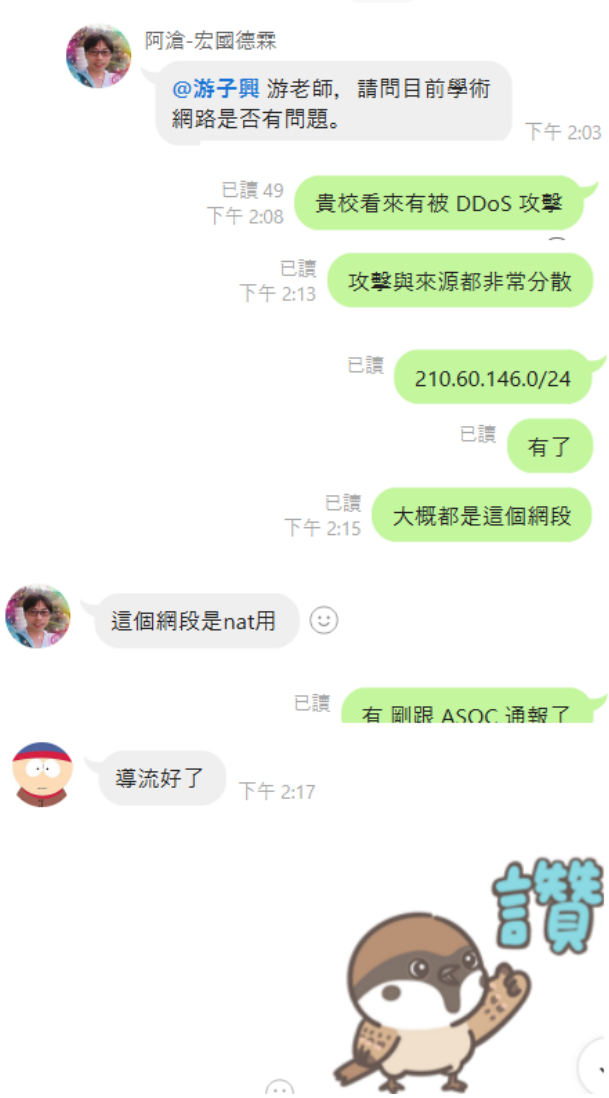
2. GCB 排除項來源

- 技服 GCB 規則 Review
  - 顯而易見、難以達成
  - 造成使用者不便且低風險等級
- 技服 GCB 網站 FAQ
- 其他學校導入經驗 (智慧財產權)
- 自行測試及使用者回饋

3. 應建立更接地氣的 GCB 規範

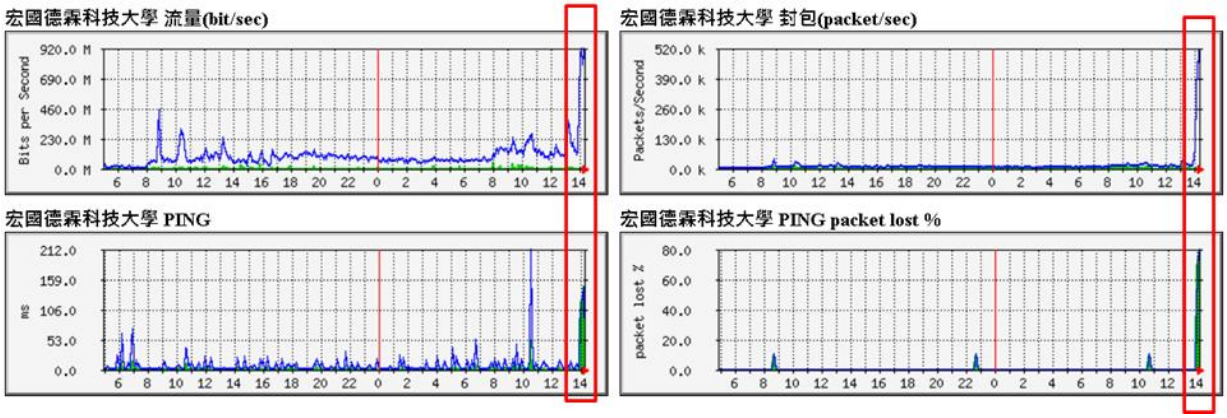
- 建議技服 GCB 規則可增加”風險等級:高/中/低”欄位可供參考
  - 應區分不同工作角色(行政人員、程式設計師、網管人員等)，訂立多套 GCB 規則範本
  - 若所有電腦不區分工作角色都套用相同規則，導致排除項非常多，可能造成資安破口。
- 取其 GCB 精神，而非規則細項
- 可先從計中管理設備做起
  - Cisco Config Template: 套用統一設定檔範本(Login, NTP, SSH, SNMP, ACL 等)

## (六) 快速緩解連線學校 DDoS 攻擊事件

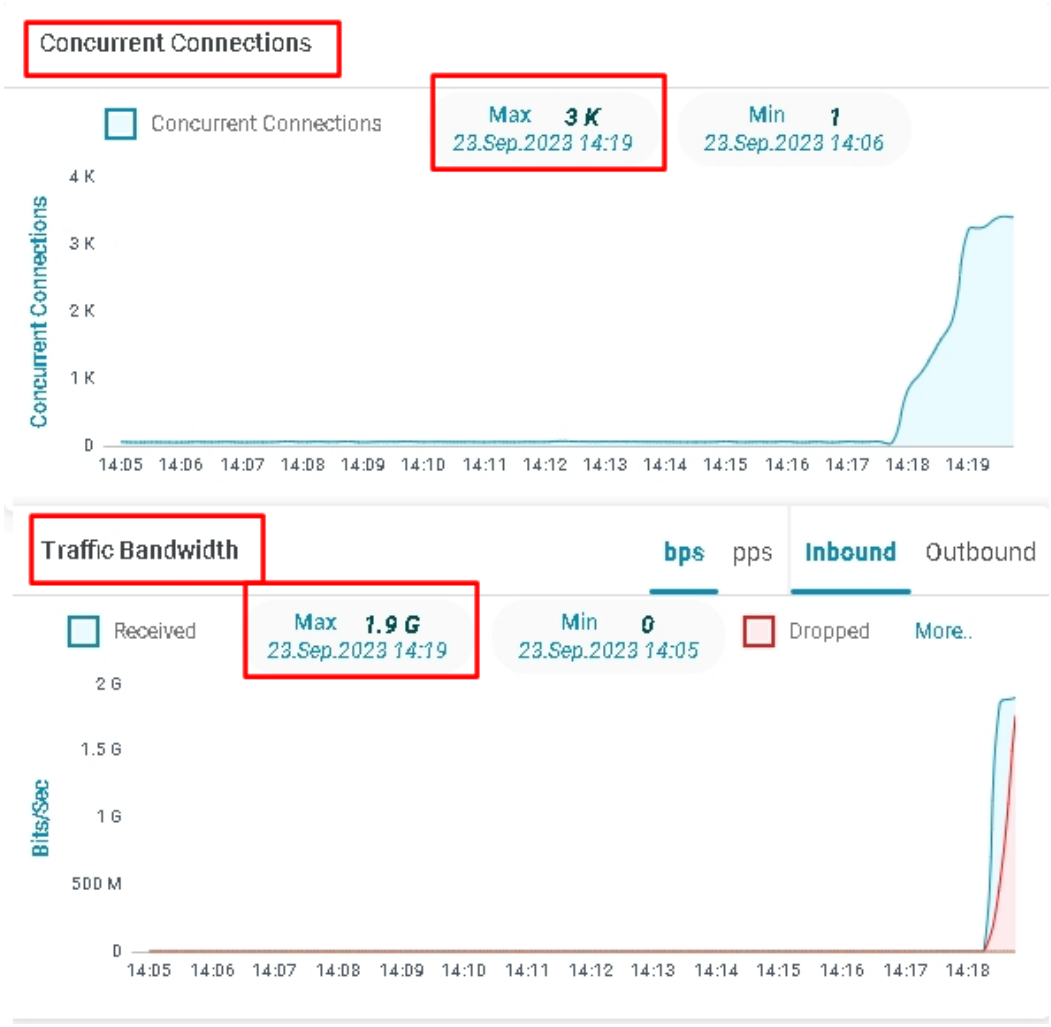



- 14:03 通報網路發生異常
- 14:08 回覆遭受 DDoS 攻擊，使用 ELK Stake 分析
- 14:13 完成 DDoS 來源與攻擊目標分析，通知 A-SOC
- 14:17 A-SOC 完成導流清洗

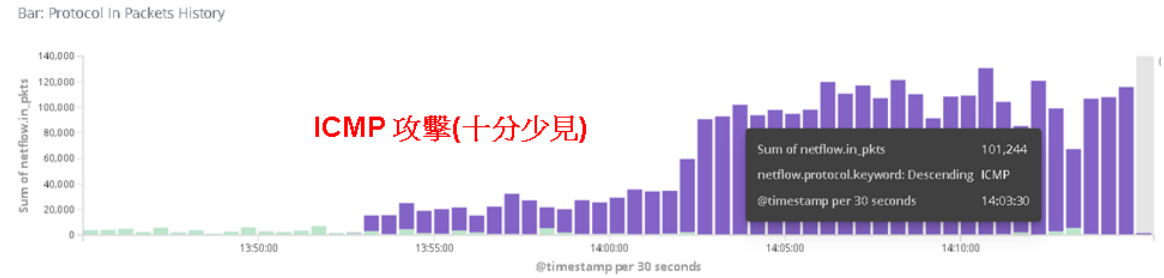
1. 收到告警、ELK 分析、進行導流僅花費 9 分鐘時間
2. MRTG 流量與封包圖

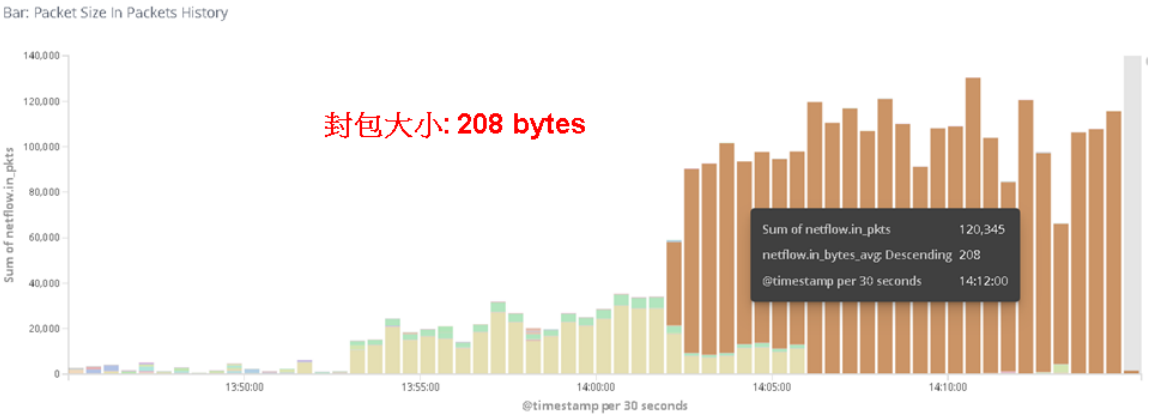


3. DDoS 流量清洗

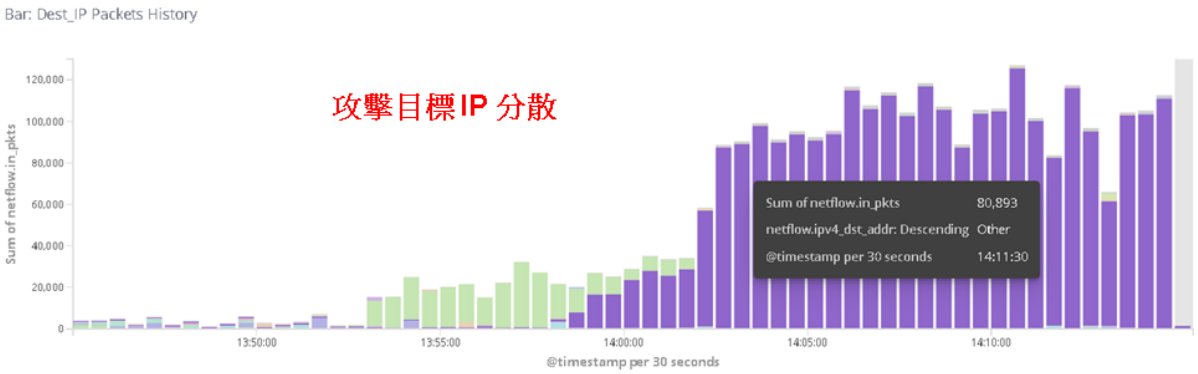



4. 攻擊協定 與 Packet Size

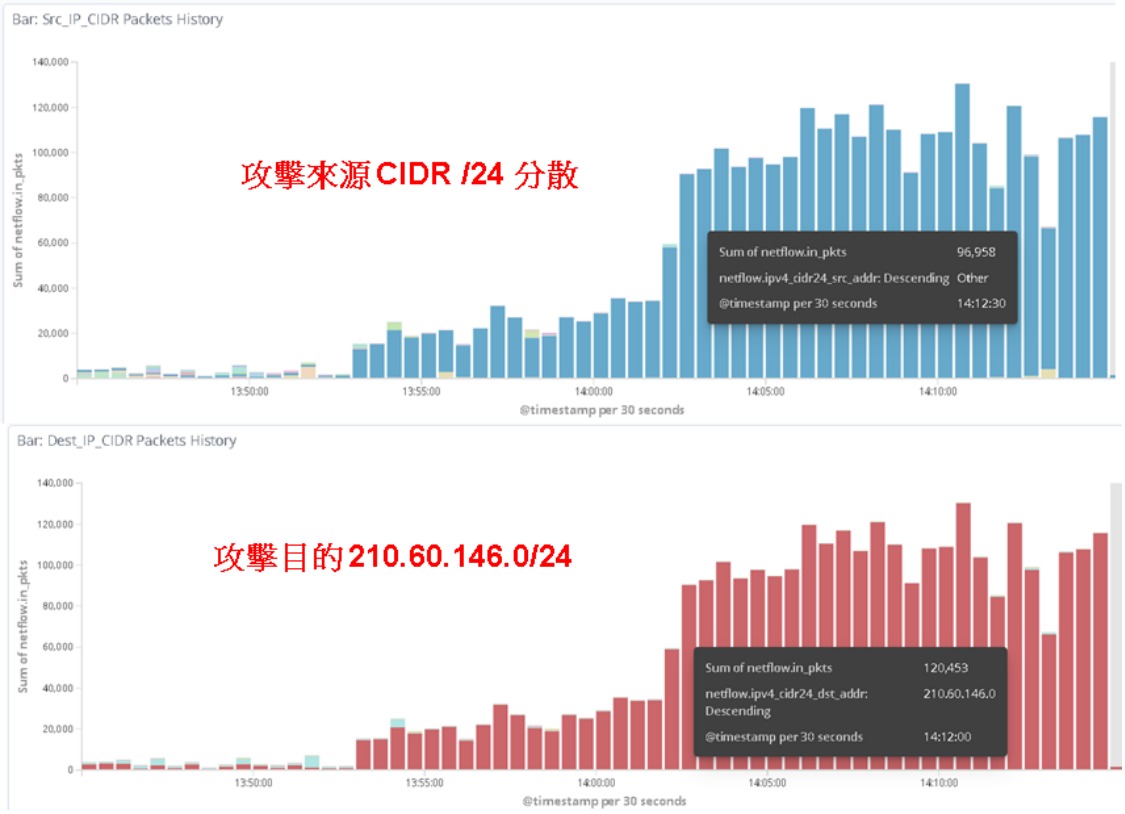


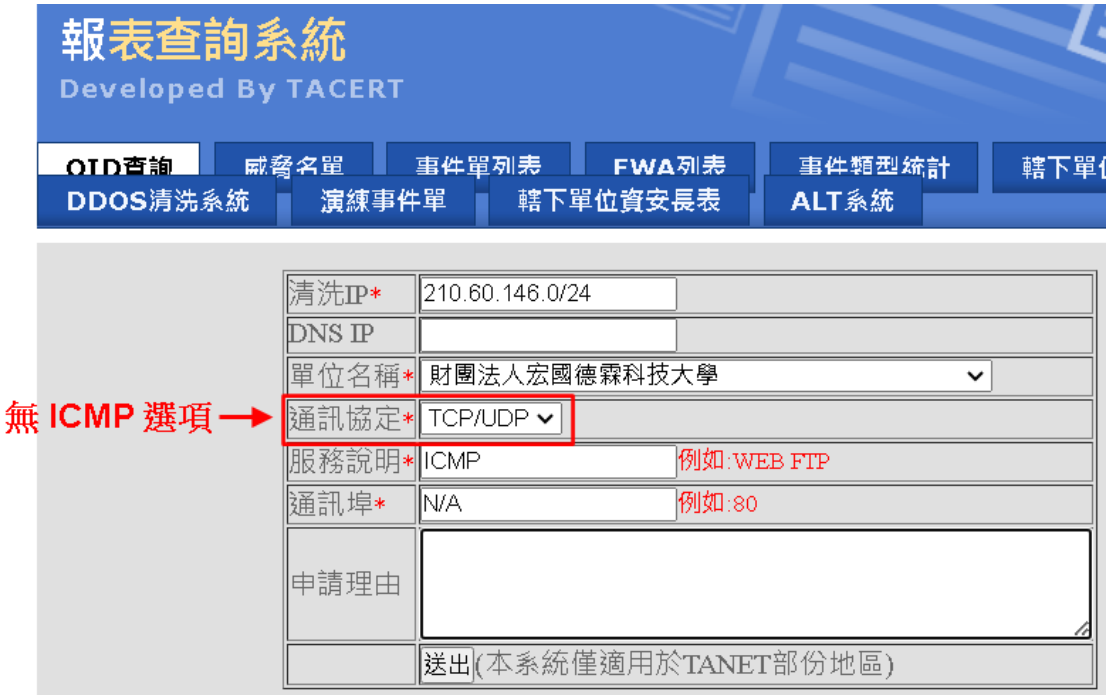

5. 攻擊來源與目的


6. 攻擊來源與目的




7. DDoS 通報(事後補填)



## (七) 新增連線單位中央氣象局之 IPv4 網段分配規則

1. 2023/01 新增連線單位: 中央氣象局(原接教育部科技大樓)
   - 原 IPv4 網段: 192.83.177.0/24、192.83.178.0/24
   - 上述可否使用 192.83.177.0/23 表示?
2. 問題釐清: 192.83.177.0/23 網段表示法是否有誤?
   - 於路由器上模擬設定 Static Route:
   - (config)# ip route 192.83.177.0 255.255.254.0 192.192.7.234
   - 出現錯誤訊息: "%Inconsistent address and mask"
   - 路由器允許之正確 Static Route:
     - # ip route 192.83.176.0 255.255.254.0 192.192.7.234
     - # ip route 192.83.178.0 255.255.254.0 192.192.7.234
3. 根因分析:
   - 192.83.177.0/23 非正確網段表示
   - /23 僅允許網段第三段為偶數。
4. 結論：
   - 非任意連續兩筆 /24 皆可合併成 /23
   - 中央氣象局 Static Route 需使用兩筆 /24 表示
     - # ip route 192.83.177.0 255.255.255.0 192.192.7.234
     - # ip route 192.83.178.0 255.255.255.0 192.192.7.234
   - Root Cause: 最初 IP 子網段分配不適當
   - 較佳之兩筆 /24 子網段分配
   - Case1: 192.83.176.0/23
     - 192.83.176.0/24、192.83.177.0/24(中央氣象局)
   - Case2: 192.83.178.0/23
     - 192.83.178.0/24(中央氣象局)、192.83.179.0/244
5. 補充資訊:
   - Network/Host/Broadcast Address:
   - 以 192.168.0.0/24 為例
   - Network Address (First): 192.168.0.0

- Host Address (頭尾去掉): 192.168.0.1 ~ 254
- Broadcast Address (Last): 1921.168.0.255

- Host Address: For 介面 IP 使用
  - (config)# int e0/0
  - (config-if)# ip address 192.168.0.1 255.255.255.0 --> Good
  - (config-if)# ip address 192.168.0.0 255.255.255.0 --> Fail, Bad mask /24 for address 192.168.0.0

- Network Address: For 路由網段使用
- /24
  - (config)# ip route 192.168.0.0 255.255.255.0 10.0.0.1 --> Good
  - (config)# ip route 192.168.0.1 255.255.255.0 10.0.0.1 --> Fail, %Inconsistent address and mask

- /23
  - (config)# ip route 192.168.0.0 255.255.254.0 10.0.0.1 --> Good
  - (config)# ip route 192.168.2.0 255.255.254.0 10.0.0.1 --> Good
  - (config)# ip route 192.168.1.0 255.255.254.0 10.0.0.1 --> Fail, %Inconsistent address and mask
- IP 第三段需為偶數

## (八) 連線單位北醫雙和新校區之 IPv4 網段分割最佳解法

1. 需求: 由現有網段切出四個 Class C 網段給新校區使用
   - 北醫現有網段:
     - 203.64.48.0/22 (203.64.48.0~203.64.51.255)
     - 203.71.84.0/22 (203.71.84.0~203.87.255)
     - 203.71.88.0/21 (203.71.88.0~203.71.95.255)
     - 120.97.32.0/19 (120.97.32.0~120.97.63.255)
     - 120.97.64.0/20 (120.97.64.0~120.97.79.255)
   - 如何選擇四個 Class C 網段?

2. 北醫回覆由 120.97.32.0/19 切出四個網段
   - 120.97.34.0/24、120.97.35.0/24、120.97.36.0/24、120.97.37.0/24
   - 原因(推測): 選擇最大網段切成小網段
   - 缺點 1: 四個網段無法由一筆路由表示
     - 120.97.34.0/22 非正常網段表示方式
     - (config)# ip route 120.97.34.0 255.255.252.0 10.0.0.1
     - %Inconsistent address and mask
     - 非任意連續四筆 /24 皆可合併成 /22 (需為 4 的倍數 )
     - 需使用兩筆網段表示：
     - 120.97.34.0/23、120.97.36.0/23
   - 缺點 2: 網段碎片化
     - 原網段: 120.97.32.0/19，切割後需用六個網段表示
     - 120.97.32.0/23
     - 120.97.34.0/23　北醫雙和校區
     - 120.97.36.0/23　北醫雙和校區
     - 120.97.38.0/23
     - 120.97.40.0/21
     - 120.97.48.0/20
     - 區網端 Static Route 由 1 筆變成 6 筆
     - 影響 EBGP 放給區網與 ISP Peering 路由
3. 如何選擇四個 Class C 網段較佳解法
   - 四個 Class C 網段，等同 /22
   - 優先使用目前 /22 網段
     - 203.64.48.0/22
     - 203.71.84.0/22
   - 應先考慮由較小的網段來切
   - 不要從中間切, 應從最前或最後來切網段.
4. 最後決定使用此網段切出四個 Class C
   - 120.97.64.0/20 (120.97.64.0 ~ 120.97.79.255)
   - 切成三個子網段:
     - 120.97.64.0/22 (120.97.64.0 ~ 120.97.67.255) --> 雙和校區(4 Class C)

- 120.97.68.0/22 (120.97.68.0 ~ 120.97.71.255)
- 120.97.72.0/21 (120.97.72.0 ~ 120.97.79.255)

## 四、114 年度工作目標與效益

### (一)工作目標

1. 定期召開管理委員會等並提供相關會議資料及下載。
2. 提供連線單位網路相關諮詢服務。
3. 持續提供穩定不斷線之優質服務為本區網中心工作目標。
4. 提供各式網路備援方案以提升各連線單位之網路可用率。
5. 網路品質監控預計全面導入 Cacti 監控系統，並於網管會議或暑期教育訓練課程中分享建置經驗。
6. 針對連線單位 DNS Server 若使用版本過於老舊，將輔導升級或直接安裝新版本，預計於網管會議與暑期教育訓練課程進行宣導。
7. 為節省電力資源與有效運用電腦資源，建構區網雲端虛擬伺服器:

   甲、區網網頁備份主機

   乙、網路品質偵測主機

   i. 線路品質偵測

   ii. Netflow 記錄與搜尋

   iii. Syslog 記錄與 Alert 通知

   丙、區網連線學校測試主機

   i. 可綁定連線學校提供特定網段 IP，做連線測試，可快速釐清為 Source IP 或電路問題

   ii. 提供 JPerf 測速 Server 主機服務
8. 持續整理網路異常事件處理過程，針對異常狀況擬定處理對策 SOP，並在區網會議提供經驗分享。
9. 針對目前尚未使用 ipv6 之連線單位，主動聯繫並輔導協助其上線，若是設備老舊不支援，則提供 Open Source Router 軟體例如 pfsense，提供技術支援與相關設定範本。

10. 將區網資安設備導入支援 IPv6 ，例如 DDoS 設備、IPS 入侵偵測系統。
11. 臺大計資中心所有重要服務皆導入 ISO27001-2013 版。
12. 建置 TCP-based 網路品質監控系統於區網中心，可提供連線學校網路連線品質 RTT、Packet Lost 數據參考，也可 24 小時監控 Internet 各種服務之網路品質。
13. 針對目前已經超過流量 50%之加密流量，預計進行加解密封包之 POC 設備測試。測試之架構分為外對內之網頁伺服器防護架構，及內對外高風險使用者之憑證安裝與解密。
14. 使用區網連線學校基礎資料更新情況進行評核與審查。

## (二)預期效益

1. 網路妥適率: 99.99%以上
2. 區網網管會議出席率: 90%以上
3. 大專院校 ipv6 使用率: 100%
4. 高國中小 ipv6 使用率: 80%以上
5. 區網網路與資安課程: 10 場以上
6. 區網課程上機實做課程: 佔 50%以上
7. 技術文件分享: 完成 3 份以上網路資安文件
8. 使用區網連線學校基礎資料更新情況進行評核與審查：每年至少完成 3 個單位評核與審查
9. HTTPS 網站自動檢核程式： check.twnic.tw (Selenium)
10. Google 表單增加發信回覆等功能。
11. 提升網路效率及其附加價值，例如：推動連線學校網路電話的普及率，建立網路通訊平臺，以節省國家經費。
12. 為有效推動 IPv6，完成 IPv6 測試網站與 IPv6 DNS 反解服務，區網提供之伺服器 100% 皆有 IPv6 之網址與 IPv6 DNS 反解位址。
13. 使用 Netflow 分析已導入 IPv6 連線單位之 IPv6 使用量，及 IPv6 位址之使用率分析。
14. 協助連線學校網路應用頻寬管理、P2P 網路應用管理及網路應用分析，預計達成連線學校授與服務數之 100%。

15. 檢測連線學校 DNS 版本與服務，針對若使用過舊版本與設定異常造成 Open Resolver 提出告警並通知該連線單位進行改善。
16. 透過網路品質偵測系統提供網路異常訊息，可即時通知連線學校網管相關人員。
17. 依據區網 Router 提供之 Netflow 記錄，可提供各時段之 ip 連線記錄，並可加快網路發生異常後之處理速度，預計所有區網對外連線 100%皆啟用 Netflow 記錄。
18. 針對 Netflow 記錄進行即時監控，及早發現網路異常活動，可確保網路頻寬有效被運用。
19. 推廣虛擬雲端計畫，提供虛擬主機租賃服務，可將高國中小之學校資訊設備轉換為雲端虛擬主機，可節省機房硬體設施如空調、不斷電系統之投資並節省電力。
20. IP 全球地址資料庫之應用實例：帳號盜用分析、網路頻寬使用分析等。
21. 針對網路異常使用 TCP-based 網路品質監控系統，可快速判斷為內部網路或 Internet 服務異常，並進一步提供解決方法。
22. 針對加密流量提供具體可行的分析方法。