臺灣學術網路(TANet)區域網路中心
臺北區網 1

『112 年度基礎維運與資安人員計畫』

111　　年　　12　　月

【目　　錄】

壹、計畫基本項目

一、計畫期程

112 年 1 月 1 日至 112 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 2Gbps、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。

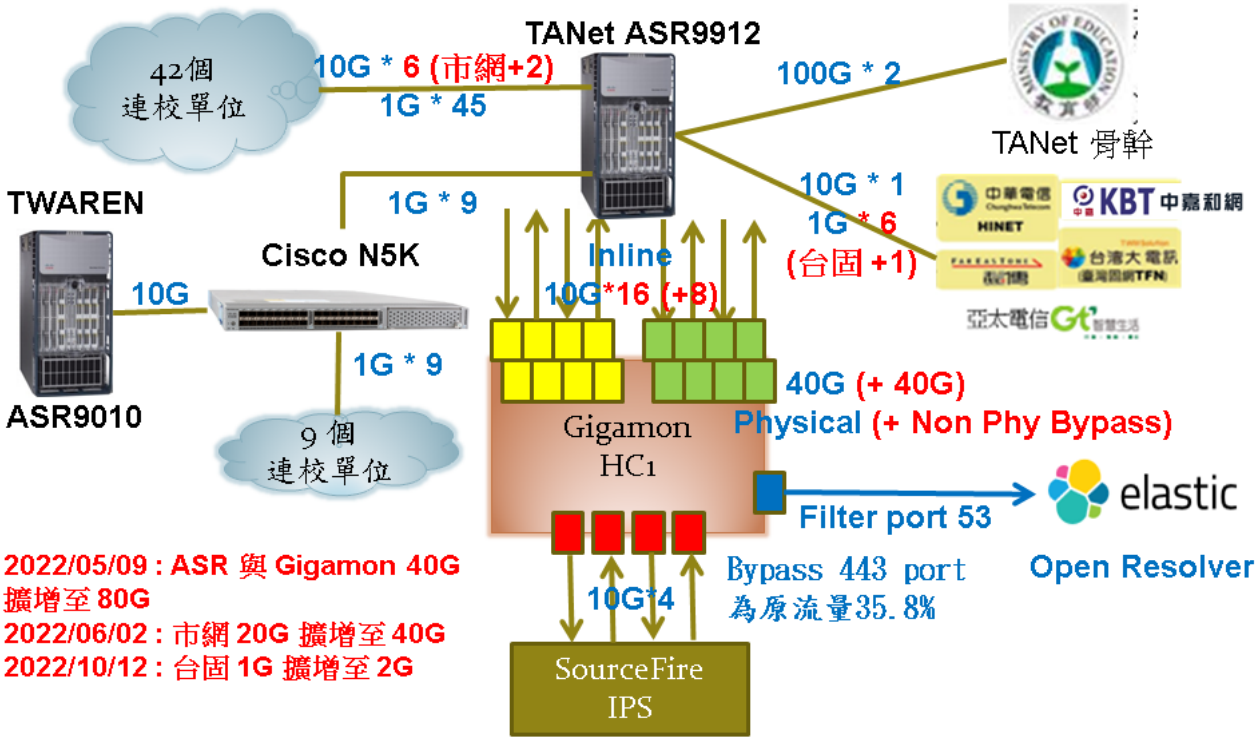
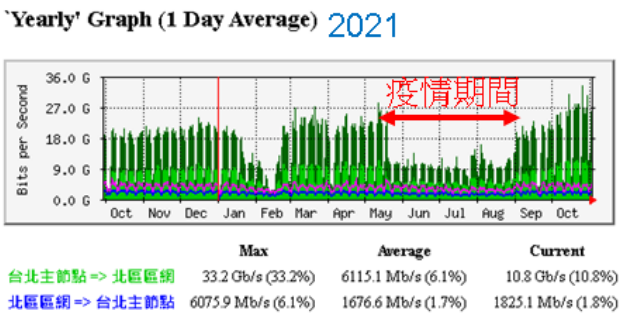
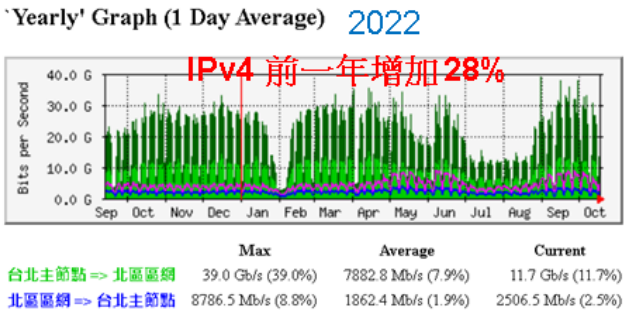


圖 1、臺大區網連線架構圖

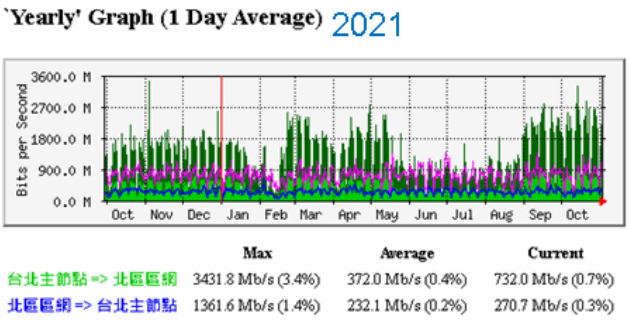
2. 臺北市市網 IPv4 + IPv6 使用亞太電信 10Gbps x 4 及中華電信 10Gbps x 2。
3. 提供區網連線學校 IP 網段查詢。
4. 參與 TWAREN 骨幹網路設備維運計劃。
5. 對連線學校(單位) 提供 WEB 及 DNS 服務狀態連線偵測情形詳細紀錄。
6. 連線單位數：51 所學校/單位。
7. 尚可供所屬連線學校申請分配之 IP ：0 個。
8. 人力狀況
   - 計中主任：莊永裕 主任
   - 網路組組長：謝宏昀教授
   - 網路管理負責人：游子興
   - 資安業務負責人：李墨軒
   - 編制內及約聘僱專職人員：8 名

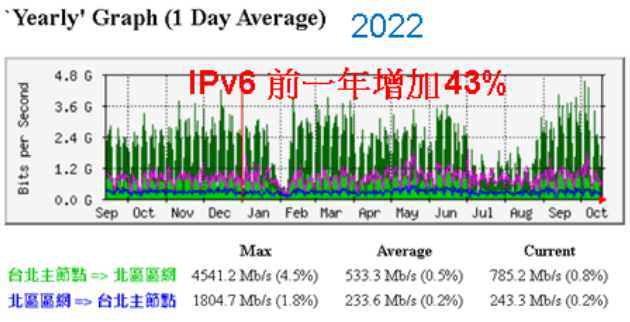
   協助處理各伺服器系統之例行維護、問題諮詢及統計監控使用狀況，Linux 伺服器系統維護、管理及統計使用者使用行為。撰寫網路管理應用相關文件，網路流量分析、監控及資料庫建立等。
9. Router 線路異動與路由管理。
10. 設置故障雙向測試系統，縮短故障排除時間，並提供 ISP 業者之聯絡資訊。
11. 提供各連線學校自行修改單位資料之網頁界面。
12. 推動各連線學校資源交流 (例如網路電話、IPv6、網路管理經驗分享) 。
13. 每年暑假期間固定舉辦網路技術之研討會。經由固定舉行研討會，期能將技術及網路科技與資訊安全等最新訊息達成全面性往下紮根，使區網連線單位能快速接收到最新資訊。
14.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





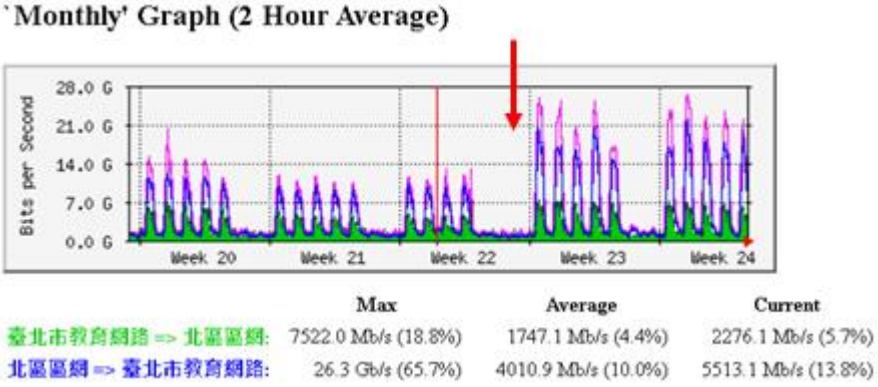
15. 流量統計 ipv6



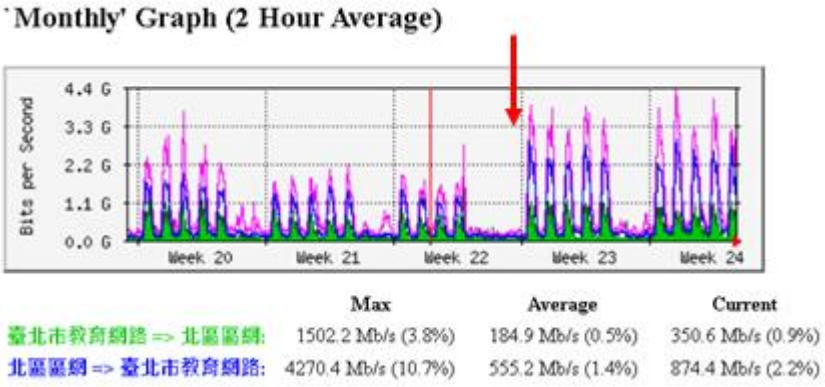


16. 臺北市網線路 20G 擴增至 40Gbps

臺北市網 ipv4



臺北市網 ipv6



(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。

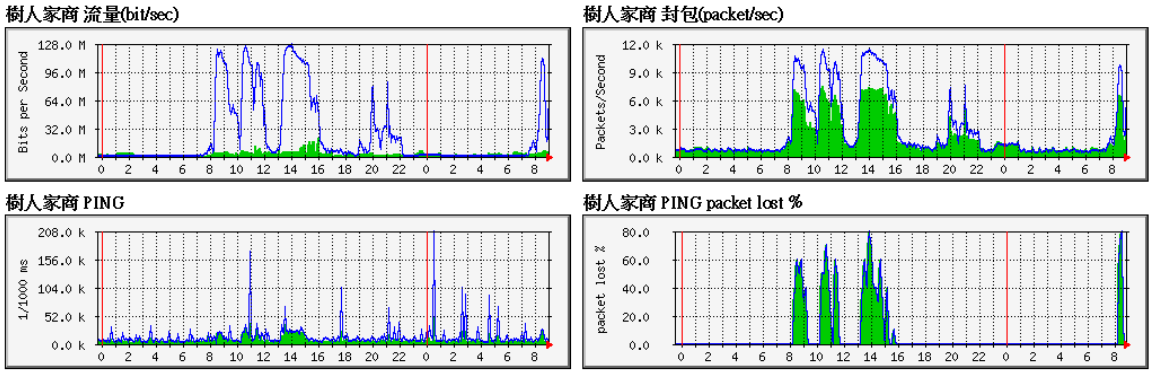


圖 2、連線單位 MRTG 網路監控圖

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。

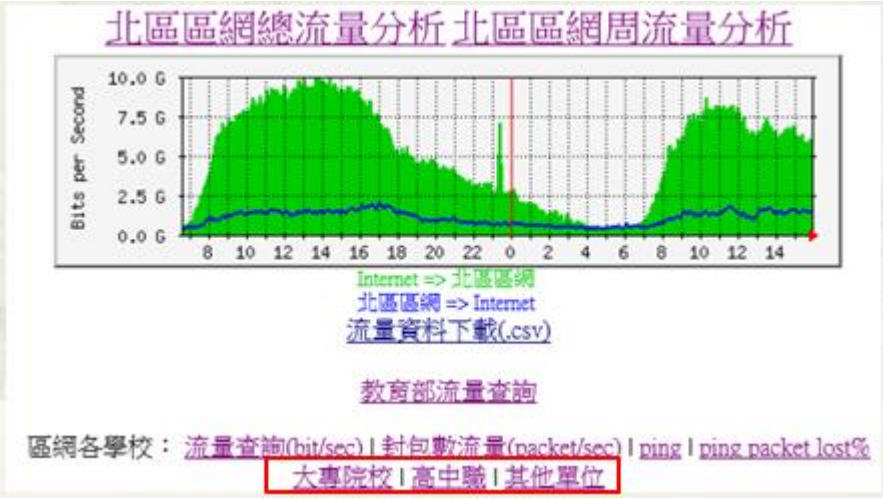
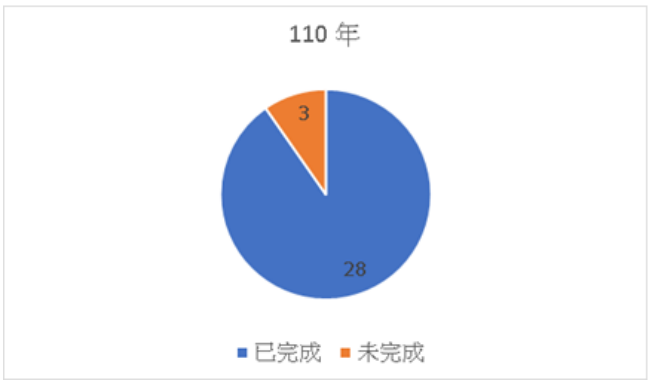


圖 3、連線單位監控圖表依照單位屬性分類

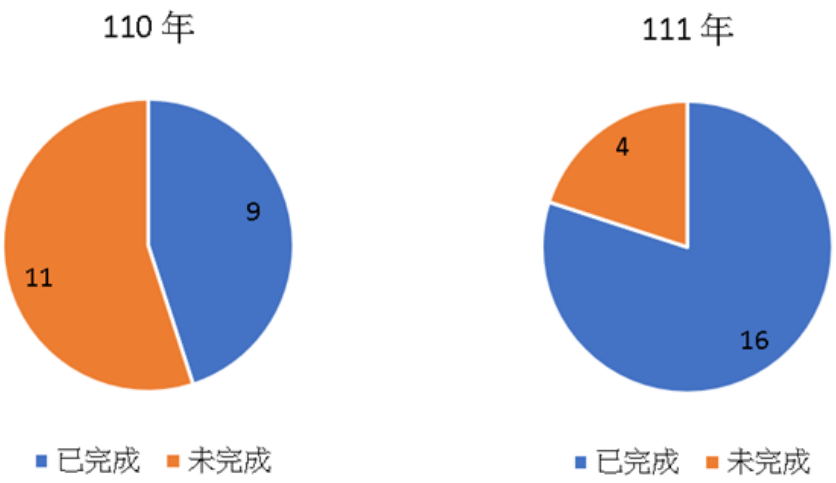
7. 使用 ELK Stack 記錄 TANet 區網 Router 之 Netflow 並提供 Src IP/Port、Dest IP/Port 等搜尋功能，並可依據封包數或流量查找 Top10 Src IP、Dest IP，若有網路異常流量發生，可快速釐清問題。
8. 使用 Cacti 收集 TANET 區網 Router Syslog 記錄並提供 Link Up/Down、Login Alerts 及 Config 指令修改通知。
9. 連線品質管理，使用 Ping Latency 監控 Yahoo/Google/Facebook/Hinet DNS 等常見之入口網站與服務。
10. 2022 年 IPv6 大專院校完成率: 大專院校: 31



有 ipv6 網段學校全部完成

尚無 ipv6 網段:軍事情報局學校、臺北基督學院

11. 2022 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:大學入學考試中心、中華民國學生棒球運動聯盟、高中體育總會、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**

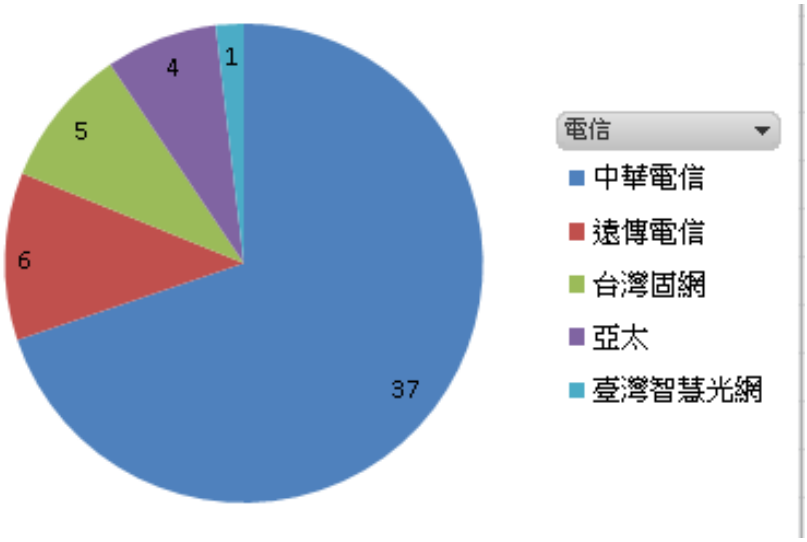


圖 4、連線單位 ISP 線路統計

13. 線路介面型態統計

列標籤	計數 - Type
光纖	32
電UTP	22
總計	54

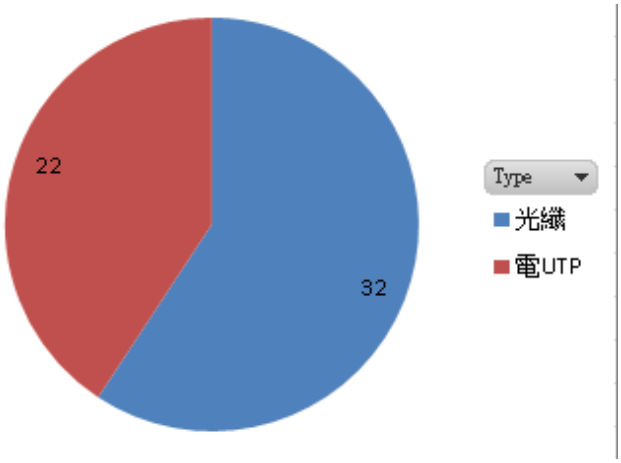


圖 5、連線單位使用介面統計

(三)辦理資訊推廣活動

場次	研習課程	上課地點	研習時數	報名人數
11101	Google Workspace for Education 與 Google Meet 實用技能運用 (含 Demo)	線上	2 小時	154
11102	運用零信任策略落實身份治理與單一簽入整合	線上	2 小時	90
11103	無痛連結 Google Workspace, REST APIs (含 Demo)（基礎）	線上	2 小時	125
11104	從資安到 AI，掌握 Google 全方位雲端生態 (含 Demo)	線上	2 小時	102
11105	校園智財權--著作權授權合約之實務運作	線上	2 小時	99

11106	ISO 27002 : 2022 資訊安全實務指導規範之新版初探	線上	2 小時	140
11107	開源網路設備監測系統	線上	2 小時	139
11108	疫情期間居家辦公 VPN 自動化管理、電子郵件攻防~實例探討	線上	2 小時	126
11109	無痛連結 Google Workspace, REST APIs (含實作)（進階）	線上	2 小時	125
11110	Google Workspace for Education 與 系統管理/雲端安全工作術 (含 Demo)	線上	2 小時	117
11111	Google Classroom 實際場景應用，打造高效線上課堂團隊	線上	2 小時	52

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

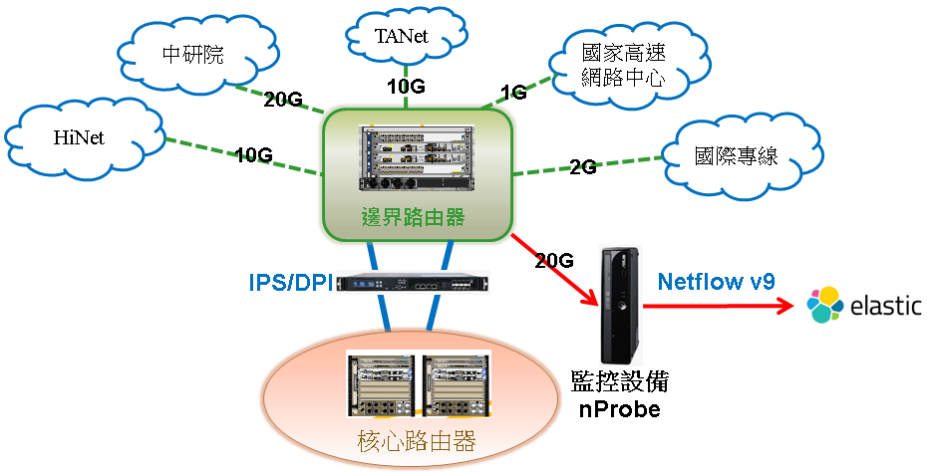


圖 7、監控網路架構圖

丁、Latency 24 Hrs 統計

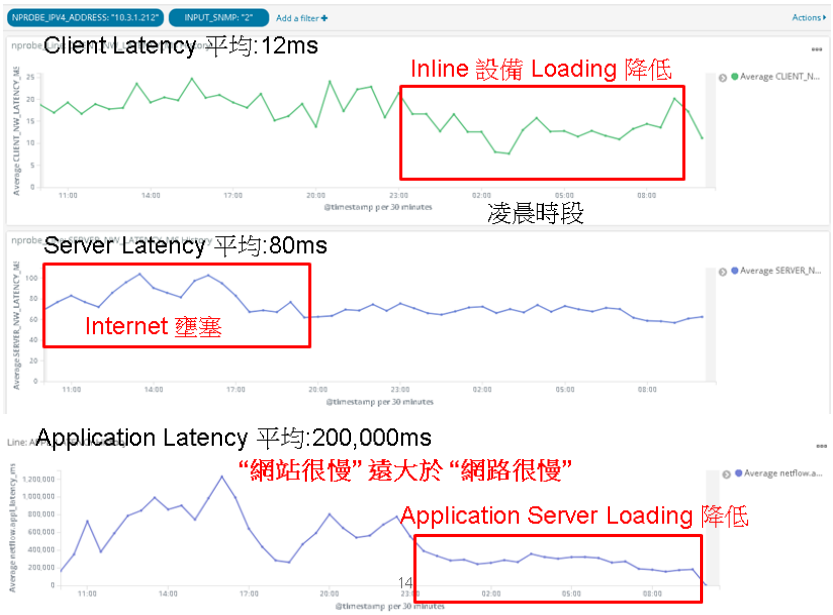


圖 8、Latency 24 Hrs 統計

戊、Latency 24 Hrs 各區網中心統計

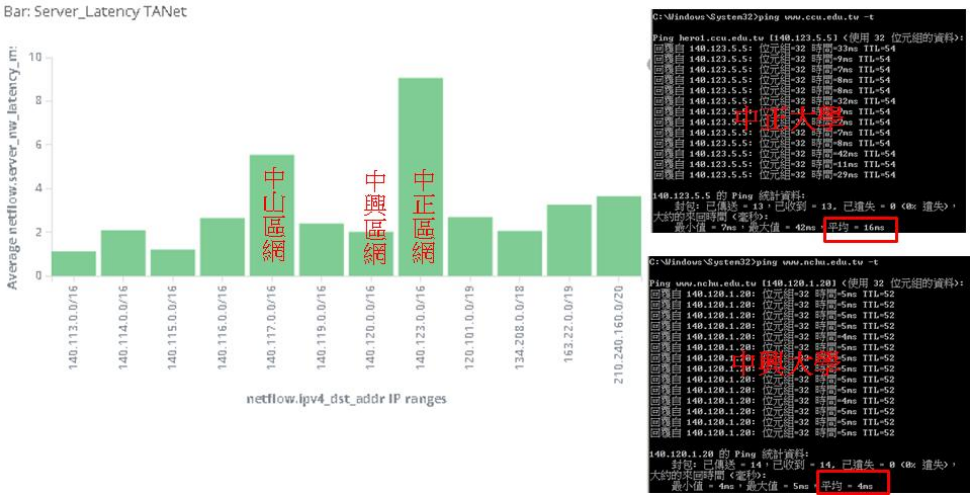


圖 9、Latency 24 Hrs 各區網中心統計

己、 辨識不同網段用途 Client 上網方式

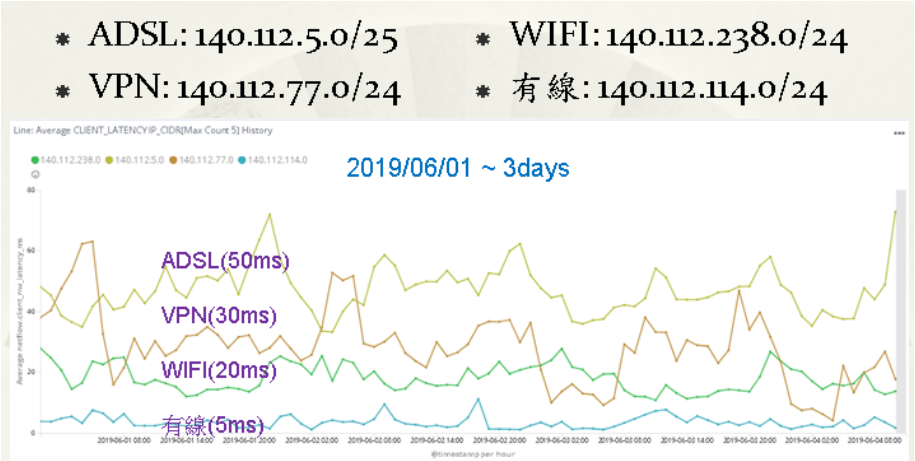


圖 10、辨識不同網段用途 Client 上網方式

庚、 辨識網段內連網設備 140.112.3.0/24 計中工作區

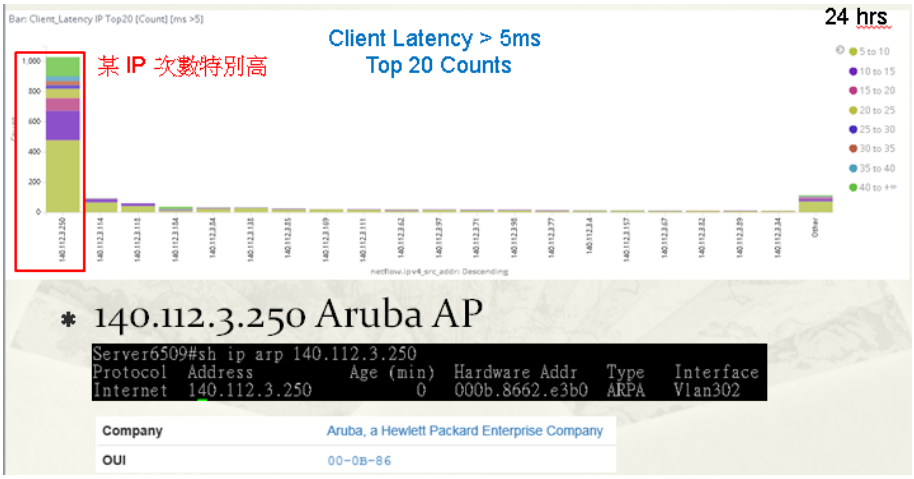


圖 11、辨識網段內連網設備

辛、 頻寬壅塞對 Client Latency 之影響--系所網路壅塞

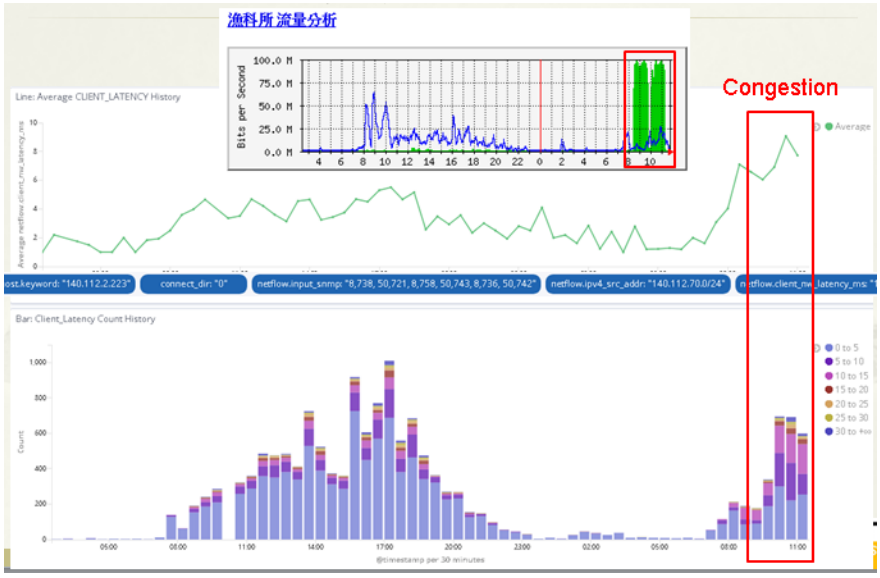


圖 12、頻寬壅塞對 Client Latency 之影響

壬、 頻寬壅塞對 Server Latency 之影響--國際頻寬壅塞

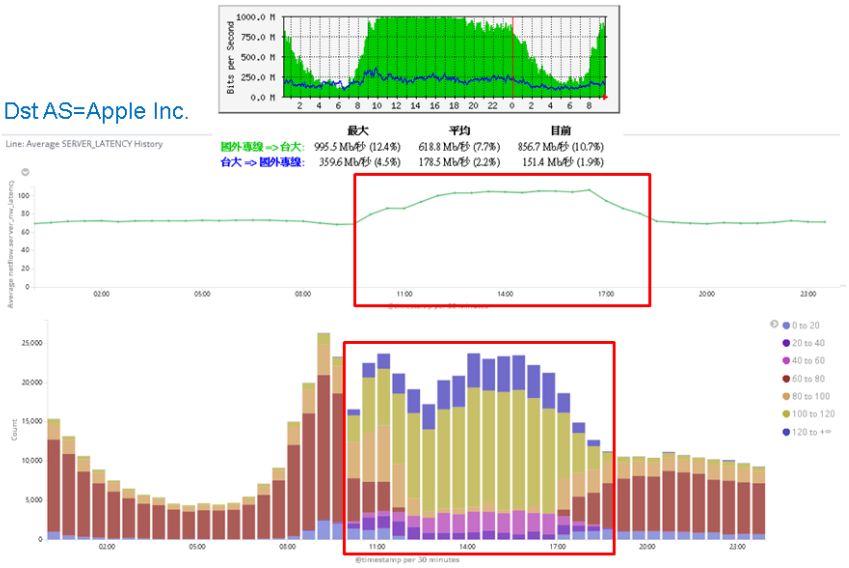


圖 13、頻寬壅塞對 Server Latency 之影響

(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

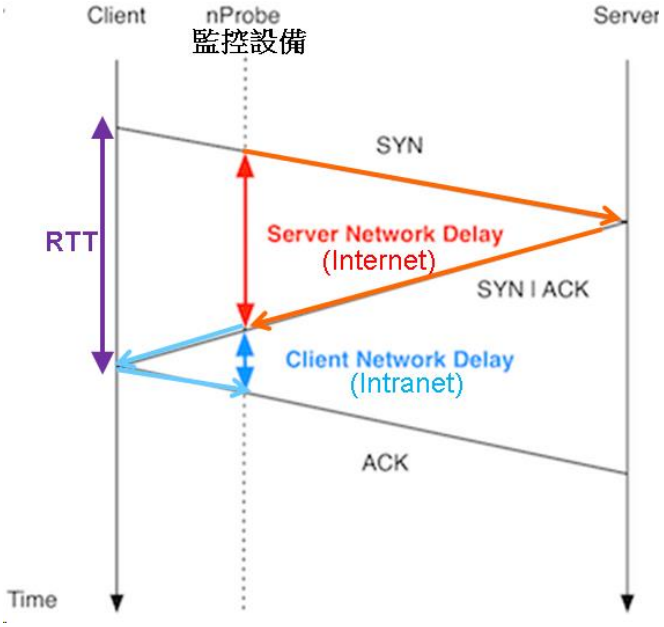
查詢結果僅有 DB-IP 資料庫顯示其地理位置在台灣，另兩家資料庫皆顯示位置在美國。

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。



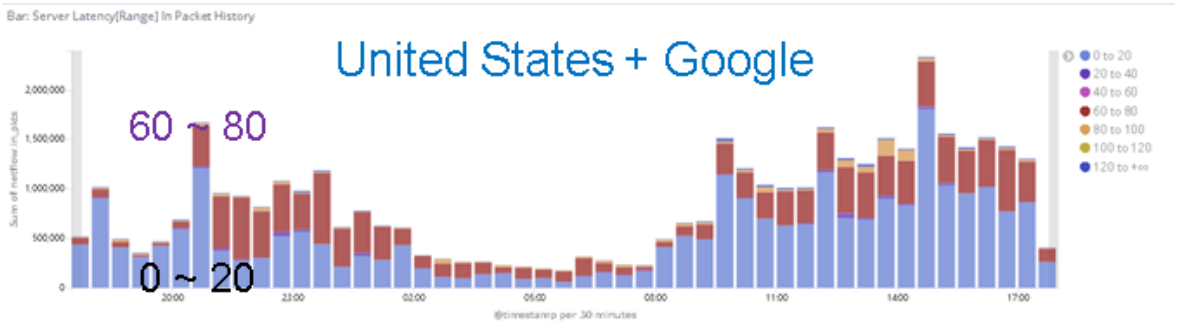
甲、 Country + ASN 平均值與其他 ASN 差異太大：大部分 IP，GeoIP DB 不正確

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

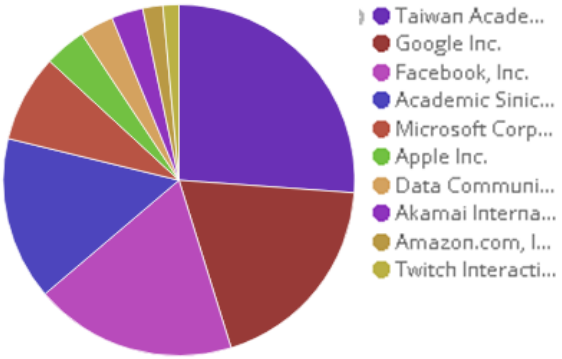
網管人員對於網路流量之分析，過去大都使用 MRTG 進行流量或封包數分析，但對於使用者上網行為一般常使用 UDP、TCP 加上 Port Number 進行分析，而此方法在現今網頁服務已成主流之情況下，分析結果已無特別意義。目前較有意義之呈現方法有 IP-Based + AS Number 及使用 nDPI 兩種方法來進行網路行為分析。

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。



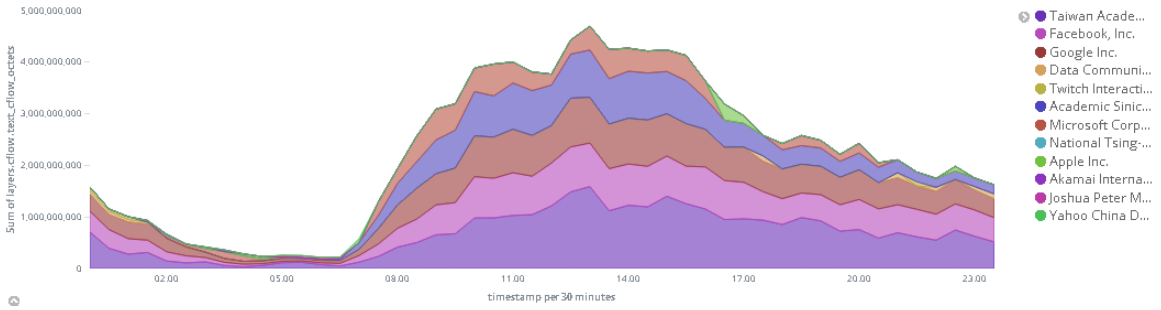
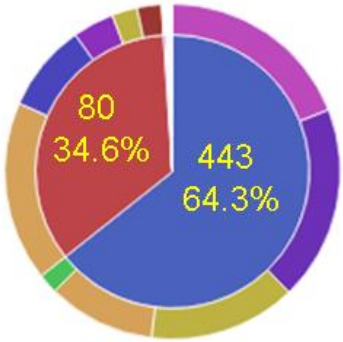


圖 19、 L7 網路分析 AS Number

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。

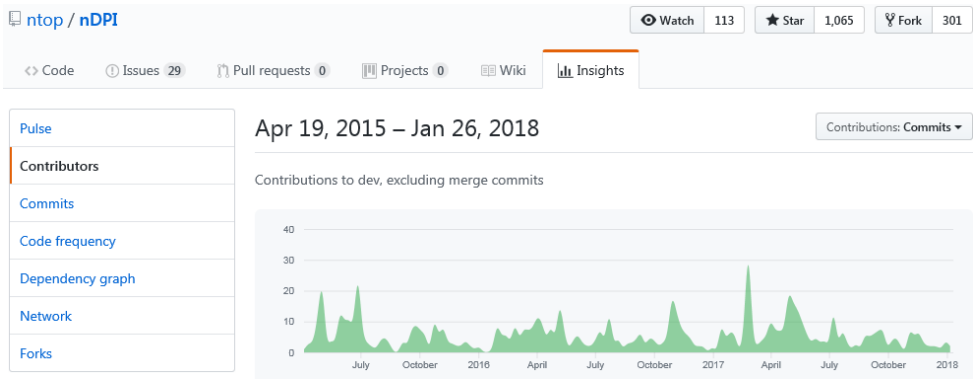


圖 21、 nDPI 於 Github 上之活躍度

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。

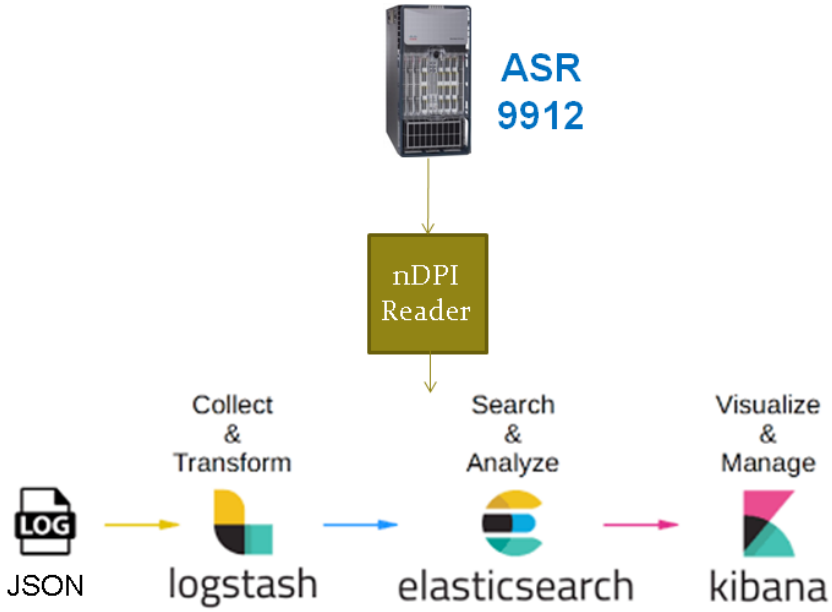


圖 22、 nDPI 佈建網路架構圖

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

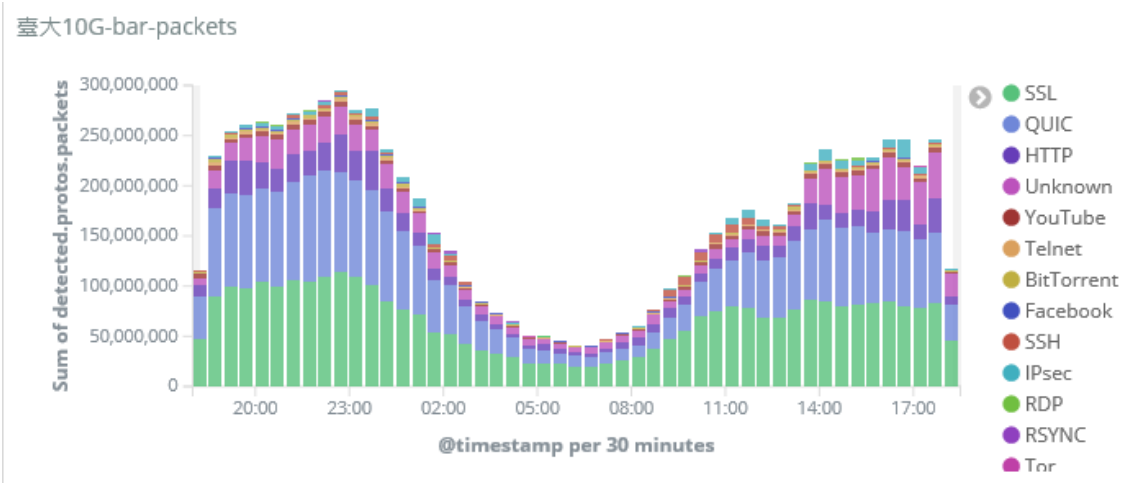


圖 24、過去 24 小時 Layer7 應用協定分佈流量圖

(四) Line Bot 即時網頁內容搜尋系統

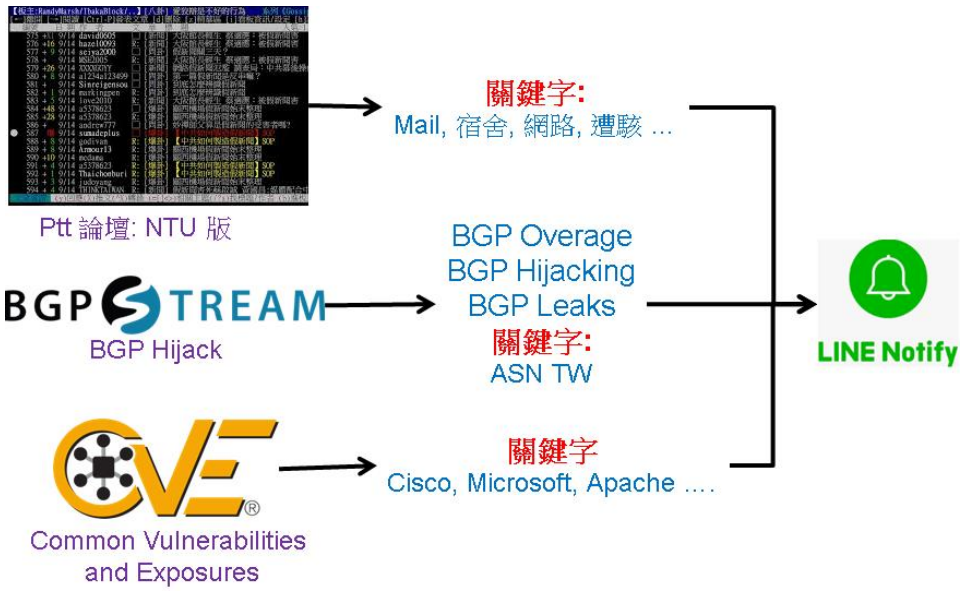


圖 25、Line Bot 即時網頁內容搜尋系統

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。

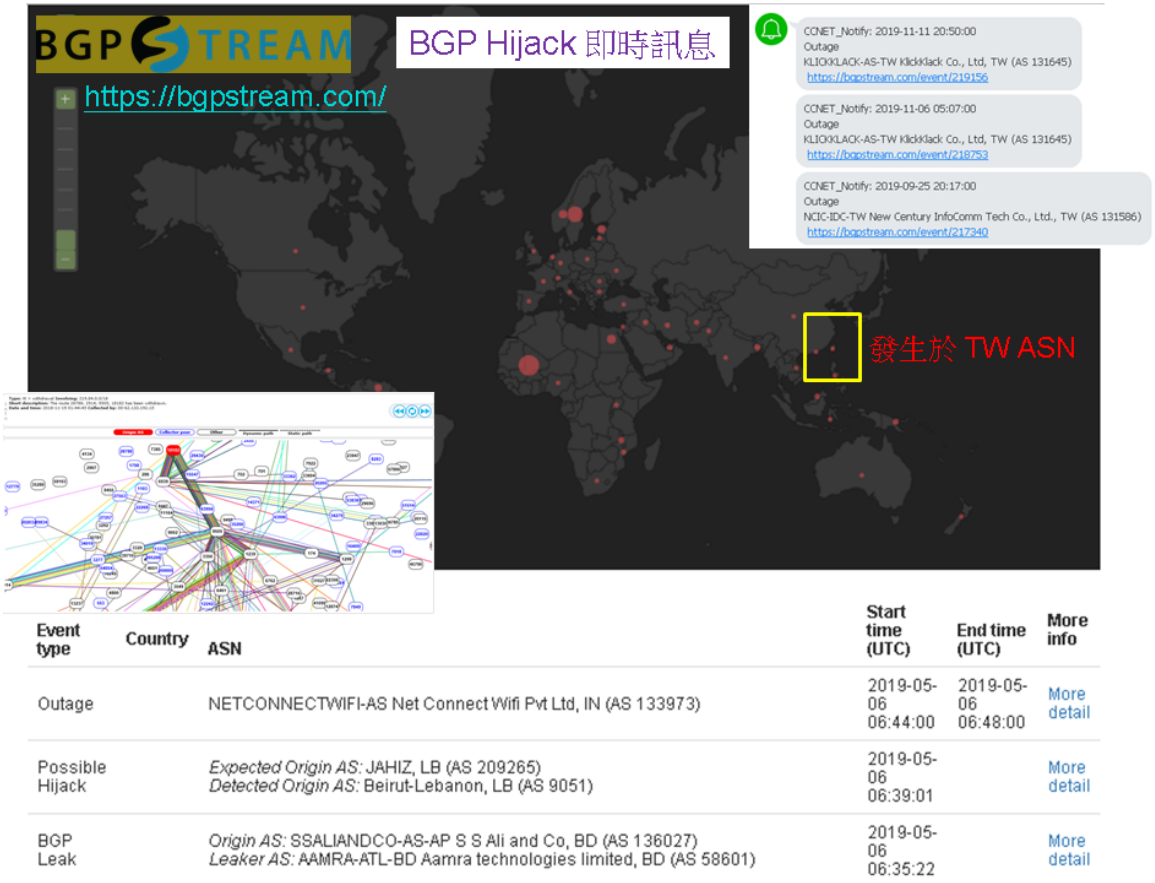
圖 26、ptt 鄉民訊息~快速掌握~

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) *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

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。

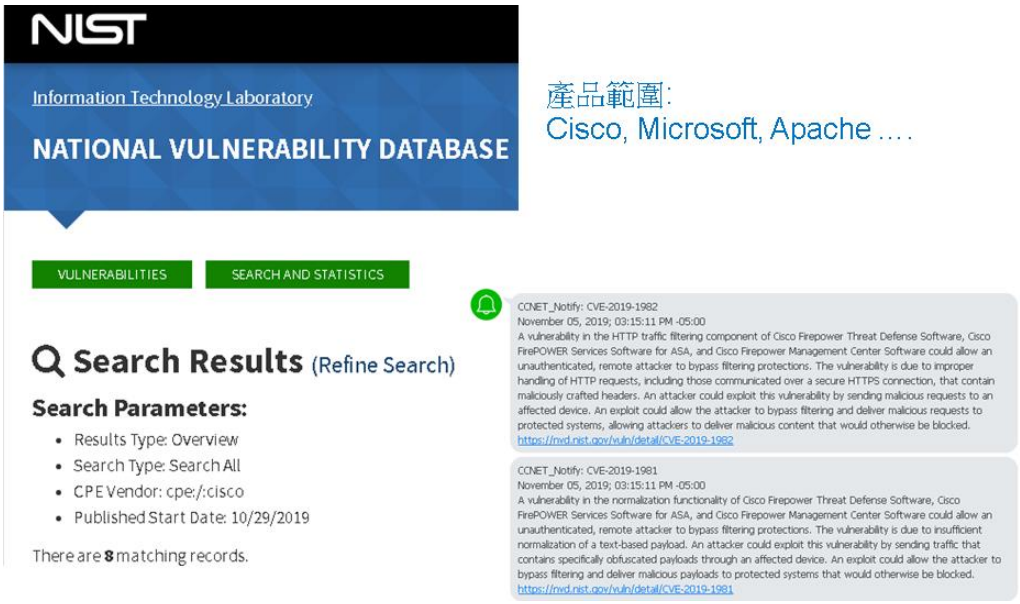


圖 28、資安漏洞~快速掌握

(五) 解決 DDoS 導流清洗時部份服務異常

1. 被導流清洗網段部分服務異常

   - BG Line: 無法登入
   - 部份國外網站連線異常，但 Ping/TraceRoute 卻都正常: Amazon, GitHub, Yahoo 日本, 日本首相官網 等

2. 測試結果

   - 非 DDoS 清洗設備造成: Bypass 設備依然如此
   - 於 Client or Server 設定 MTU ≦ 1492 即可正常連線

MTU	可否順利連線
1500	否
1493	否
1492	可
1000	可

3. Alternative Solution

- 調整本機網卡 MTU ≦ 1492
- 於 防火牆/Router 調整 TCP Maximum Segment Size (MSS) ≦ 1452
  - 防火牆 Pfsense: MSS clamping
  - Cisco Router: (config-if)# ip tcp adjust-mss 1360
- Client

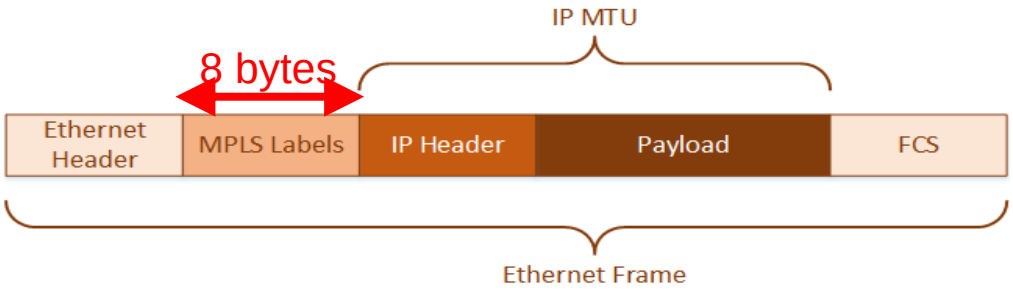
No.	Time	tcp.stream	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1850	10.679127	10	172.16.0.17	52333	163.28.16.200	3389	TCP	66	52333 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1852	10.680699	10	163.28.16.200	3389	172.16.0.17	52333	TCP	66	3389 → 52333 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1360 WS=1 SACK_PERM=1
1853	10.680751	10	172.16.0.17	52333	163.28.16.200	3389	TCP	54	52333 → 3389 [ACK] Seq=1 Ack=1 Win=262400 Len=0

- Server

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
771	3.196712	140.112.3.82	35276	163.28.16.200	3389	TCP	66	35276 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1360 WS=256 SACK_PERM=1
772	3.196843	163.28.16.200	3389	140.112.3.82	35276	TCP	66	3389 → 35276 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1
773	3.198009	140.112.3.82	35276	163.28.16.200	3389	TCP	60	35276 → 3389 [ACK] Seq=1 Ack=1 Win=262400 Len=0

4. 根因分析(推測)

- MPLS MTU: Adding two labels, of 4 bytes each, means that the packet with labels is 1508 bytes



- DDoS 導流方法為使用 MPLS 路由將異常流量經新竹主節點導入清洗機，推測為途中某節點未將 MTU 預設 1500 bytes 調整至 1508 bytes，導致部分封包中途被丟棄所致。

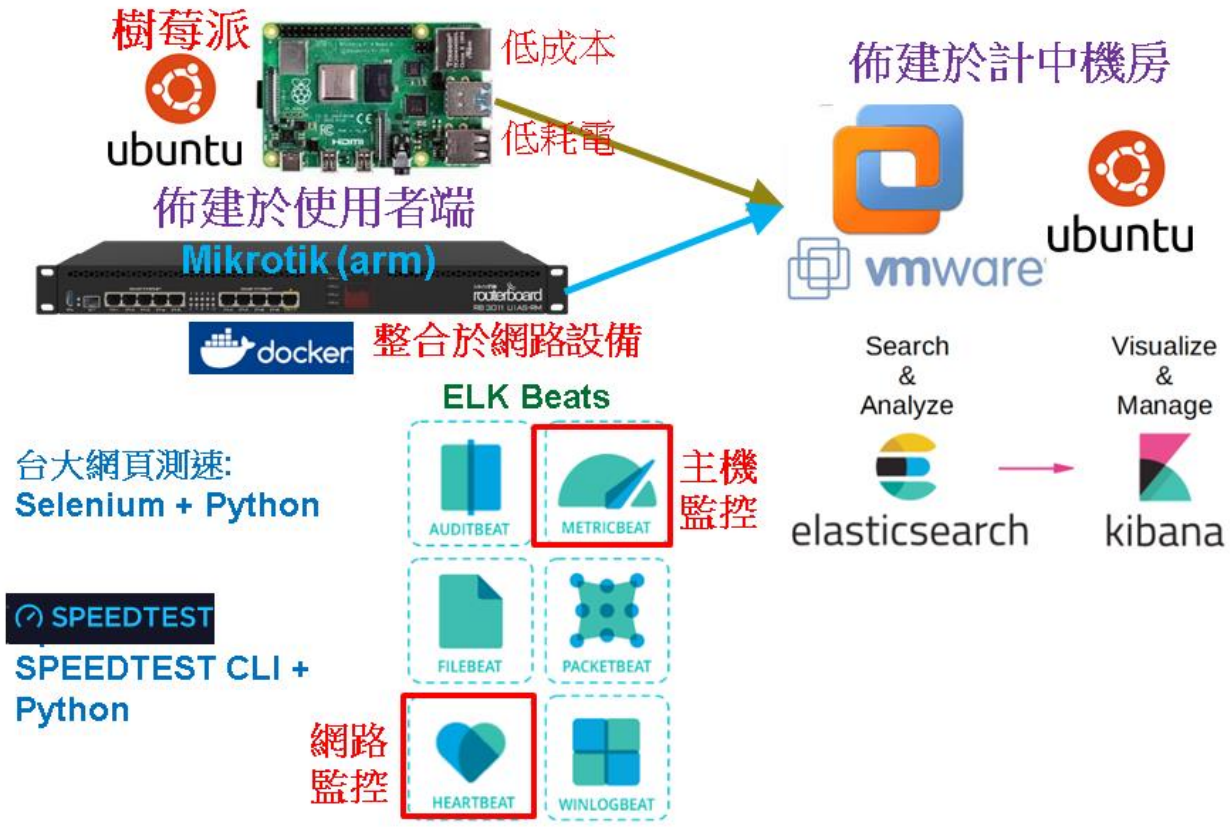
(六) 使用者端網路品質監控系統

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

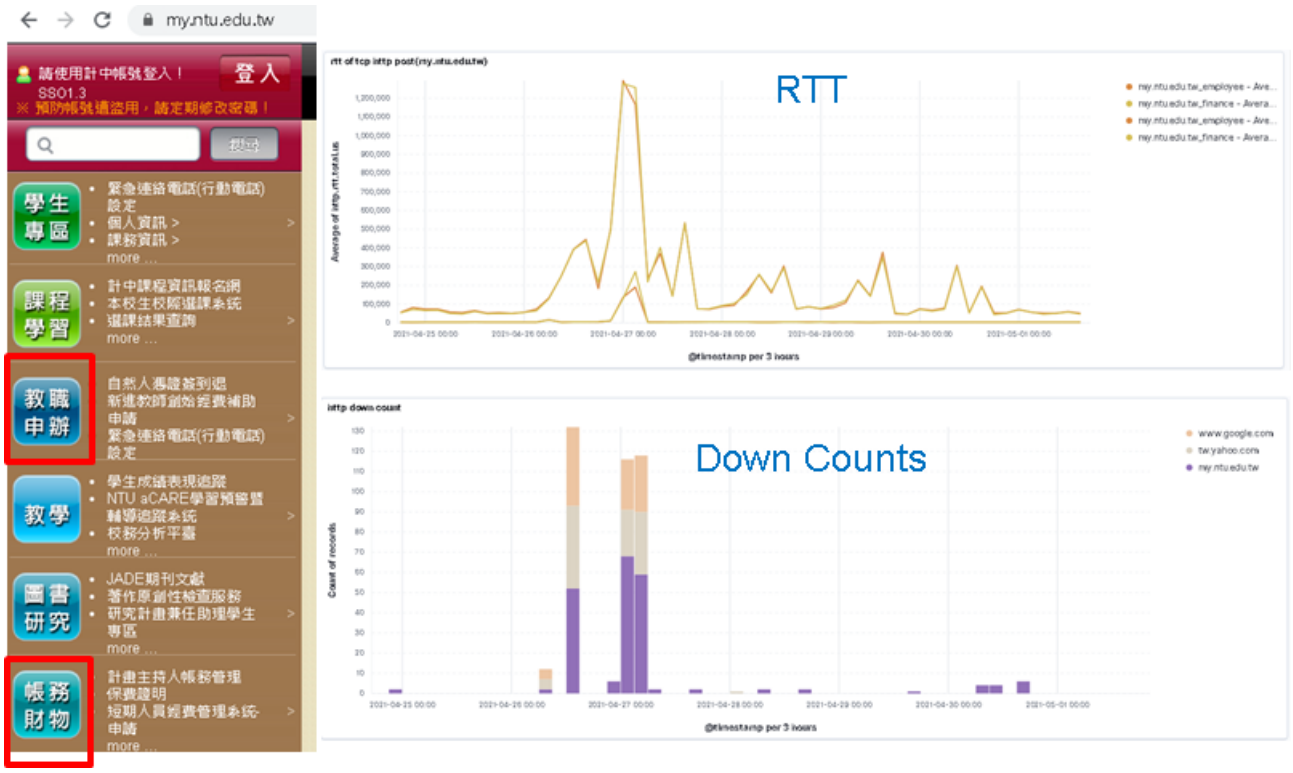
2. 建置架構圖



3. 使用樹莓派建置優點

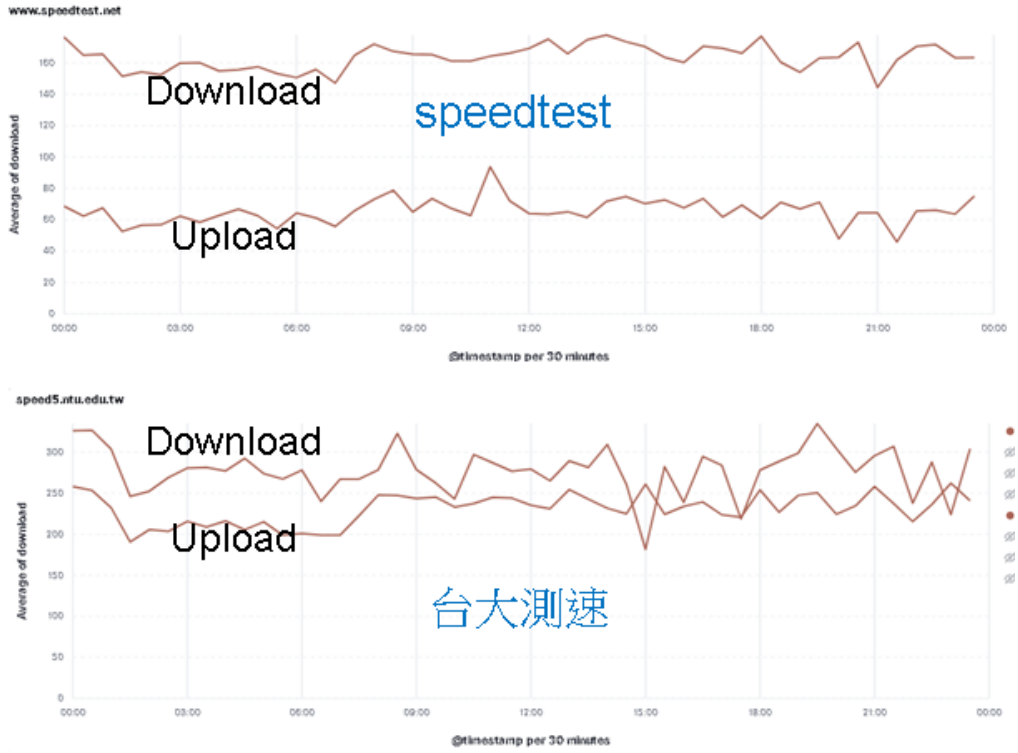
- 成本低 < $2000
- 低耗電 < 10Walt
- 體積小佈建容易
- 支援有線與無線網路監控

4. 校務系統監控

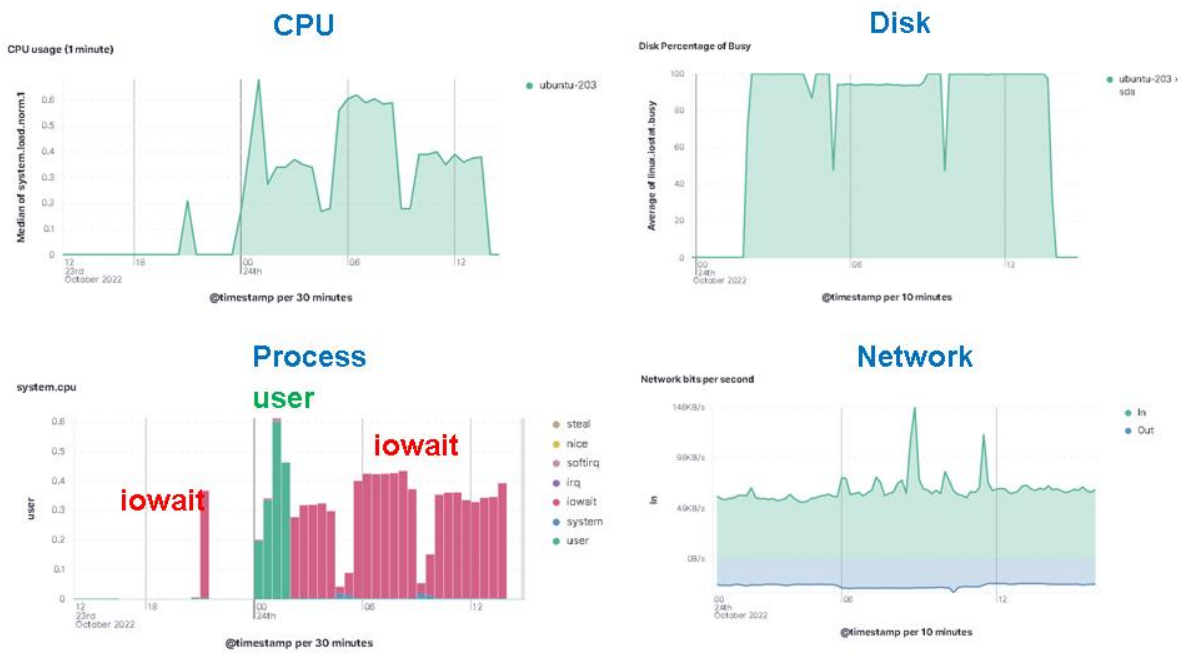


5. 網路測速

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



6. ELK Metricbeat 主機監控



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。

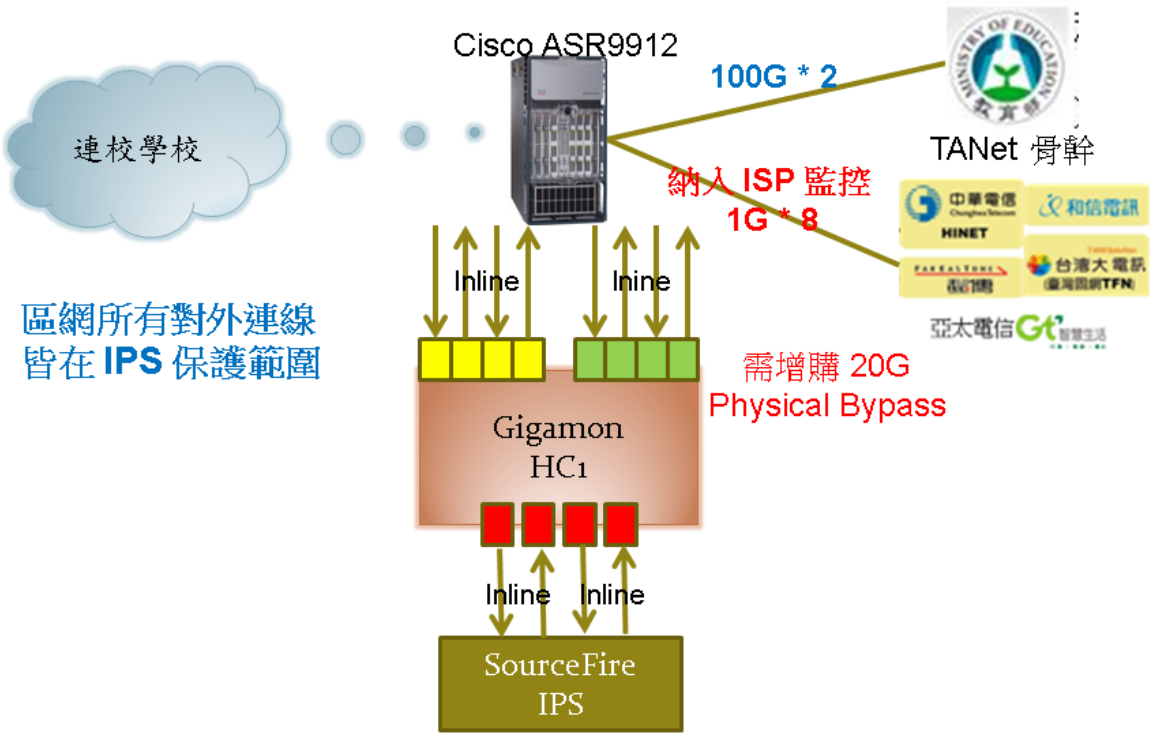


圖 29、Peer ISP 納入 IPS 偵測範圍

(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

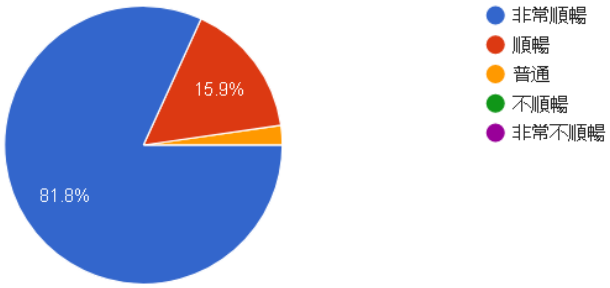
2. 滿意度調查共有 51 連線單位，收到 44 份回覆，回覆率 86%

3. 非常滿意佔八成以上

4. 節錄部分調查結果如下

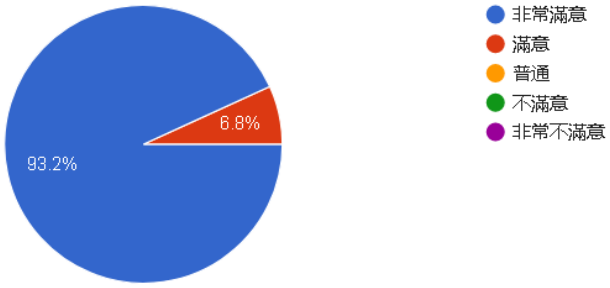
本年度 貴單位之網路連線服務，順暢與否?

44 則回應



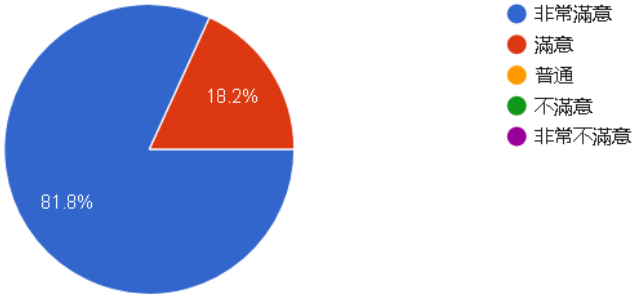
本年度 貴單位如有網路管理或連線問題時，區網中心的協助是否有順利排除障礙?

44 則回應



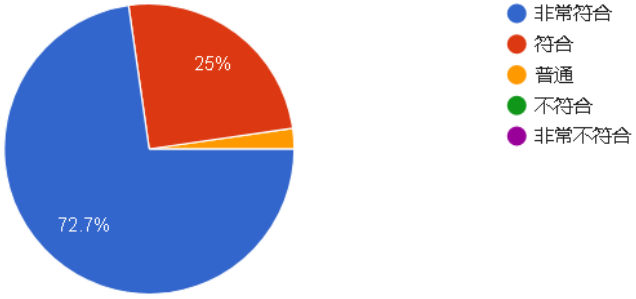
資通安全事件的通報應變的協助處理：

44 則回應



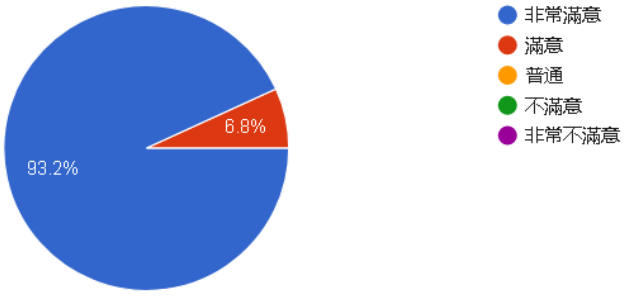
對區網所舉辦之教育訓練或研習課程，是否能符合　貴單位實務運作上的需求?

44 則回應



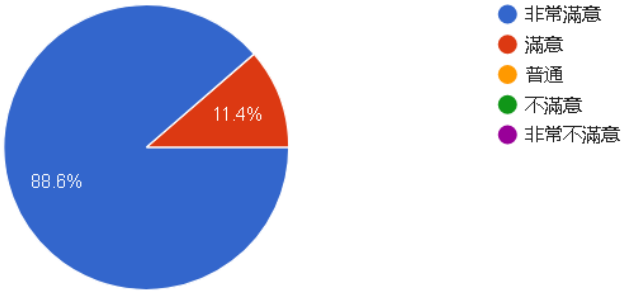
貴單位對於區網中心服務人員之熱忱及親和力的滿意度?

44 則回應



貴單位對於區網中心綜合整體服務的表現

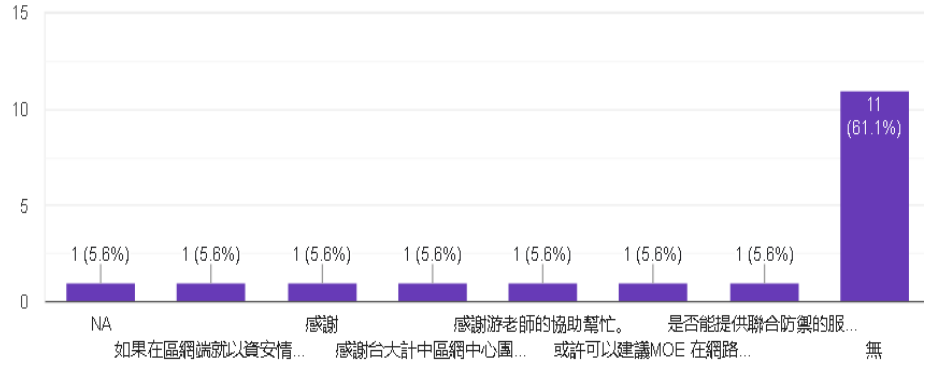
44 則回應



對區域網路中心在網路維運管理的建議

複製

18 則回應



對區網所舉辦之教育訓練或研習課程建議

18 則回應

NA

希望每個月都可以有新的課程

教育訓練的研習條,若有參訓者姓名,比較能當資安驗證教育訓練時數佐證,謝謝

網路硬體&未來發展趨勢

無.只有感謝!!

線上課程分享，讓白天忙碌的同仁可以找時間參與

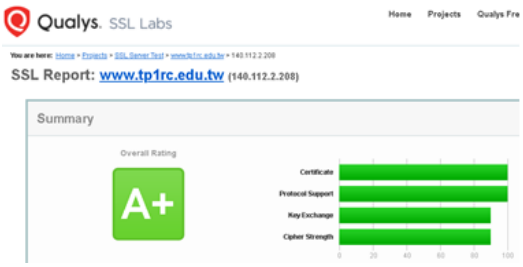
或許可以增加實戰案例探討，增加新進夥伴快速進入狀況

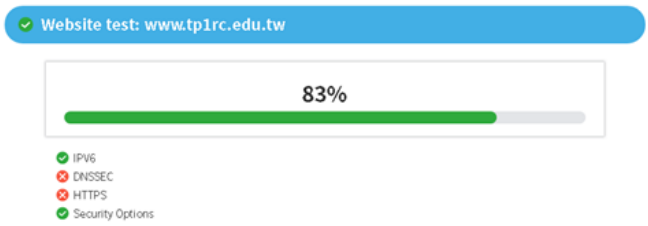
已經很努力以多元化方式協助夥伴，若能以資安實例探討更能提升新進夥伴實戰經驗

希望能持續辦理本年度研習課程。

(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

1. 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
2. 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

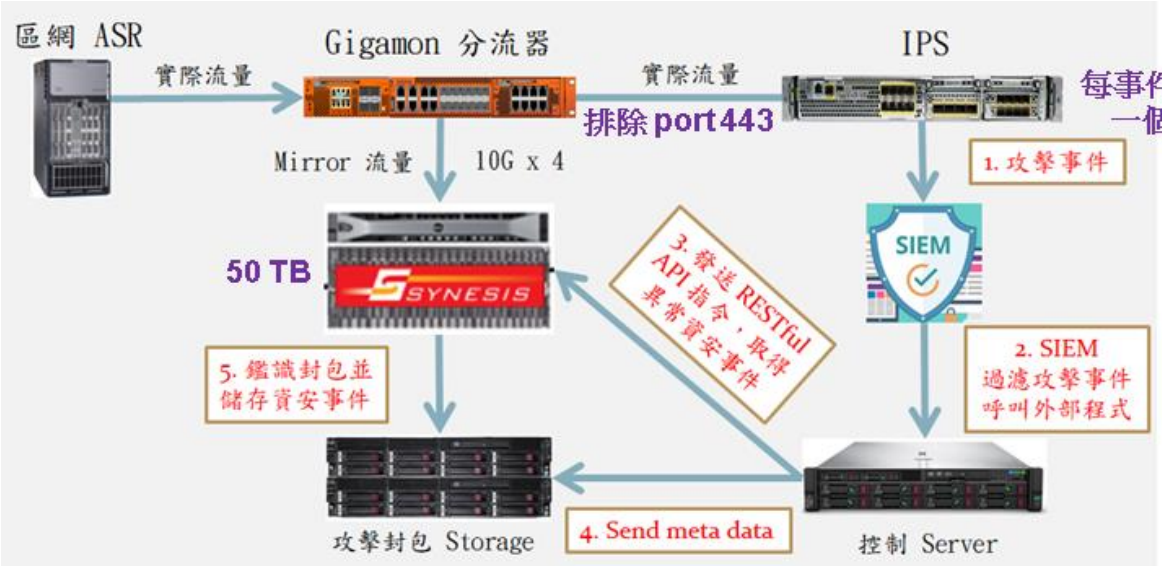
1. 於區網課程及網管會議分享
3. 資安檢核 GCB 導入案例分享
   - 技服 GCB 之規則及如何找出排除項，並使用微軟提供之免費工具 LGPO、Policy Analyzer 進行導入與檢核，提出三種不同的導入方法供使用者參考。
4. 資安檢核 GCB 排除項參考文件
   - 臺大計資中心導入技服 GCB 規則之排除項目，增加”風險等級”欄位以供參考。
5. 參考區網技術文件
   - https://www.tp1rc.edu.tw/e1.php

2. GCB 排除項來源
6. 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
7. 技服 GCB 網站 FAQ
8. 其他學校導入經驗 (智慧財產權)
9. 自行測試及使用者回饋

3. 應建立更接地氣的 GCB 規範
10. 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。
11. 取其 GCB 精神，而非規則細項
12. 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) 實習場域計畫 與北區 A-SOC 合作

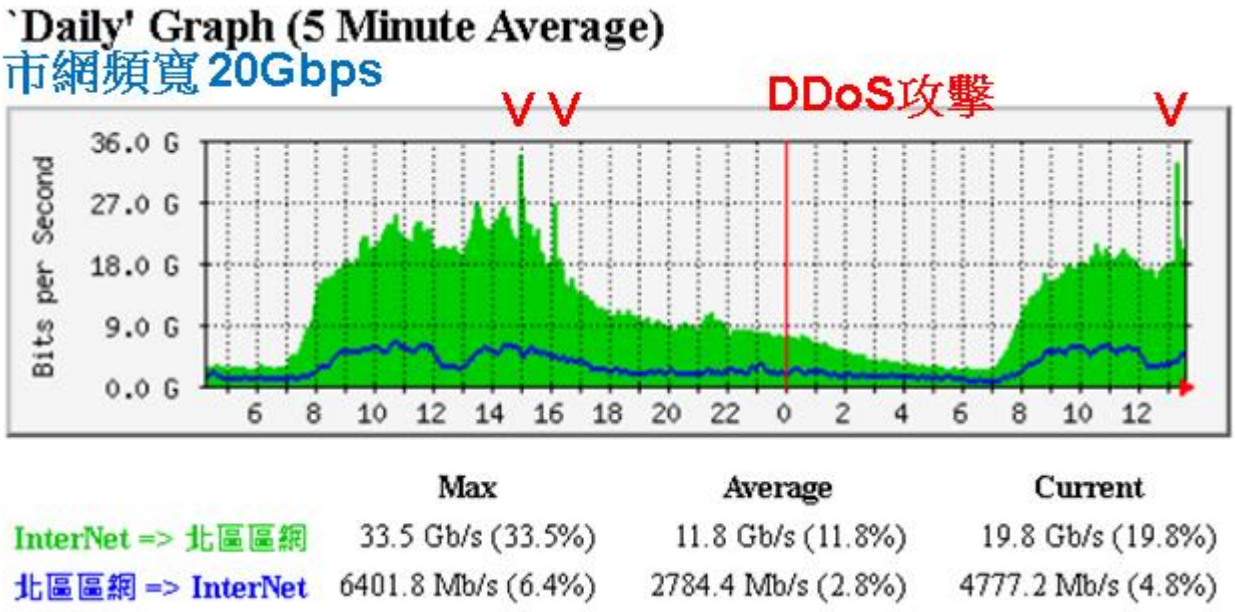


1. 資安事件封包分析、降低誤判率
   - IPS 設備僅能保留觸發事件規則之唯一封包
   - 若有完整事件封包檔，可進一步分析觸發主機資訊
     - OS Fingerprint、HTTP Agent、Web Server App/Version、加密憑證資訊.
   - 降低誤報率: 例. Apache 事件單不應開給 Windows IIS 伺服器
2. 豐富開單訊息: 挖礦事件為例

3. Open Data 特色封包資料集

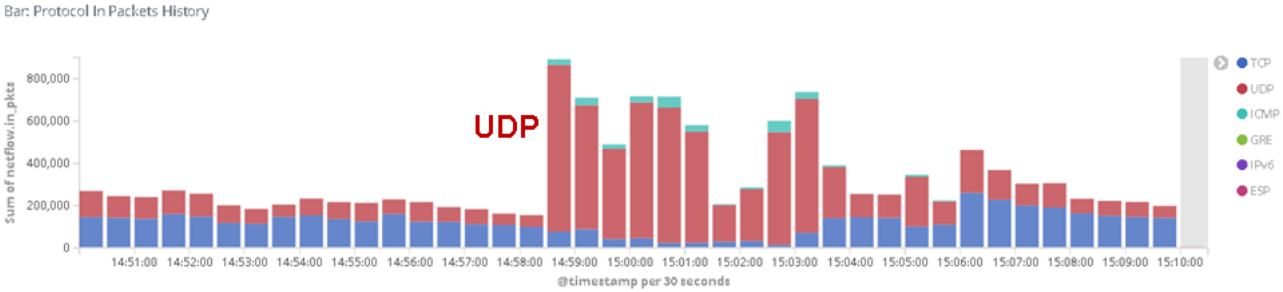
- 建立去識別化之 DNS 放大攻擊封包資料集
- 已運用於 111 年台大資安課程實做 Lab
  - 辨識攻擊類型、計算放大倍率、辨識攻擊封包與反射封包

(七) 市網 DDoS 攻擊事件

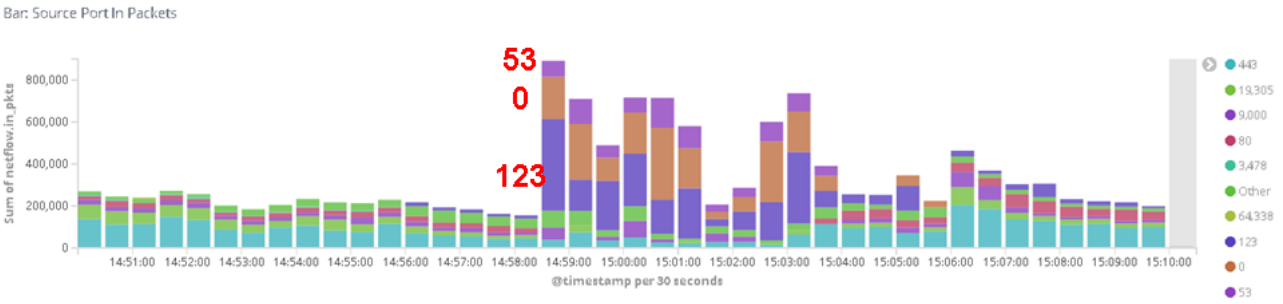


1. DDoS 事件發生時間
   - 2022/04/01 14:00~14:30
   - 2022/04/28 15:00~15:05
   - 2022/05/09 09:30 10:00 14:00 2022/05/10 09:50
   - 2022/05/13 14:20 17:00
2. 攻擊來源分析

* Protocol: UDP

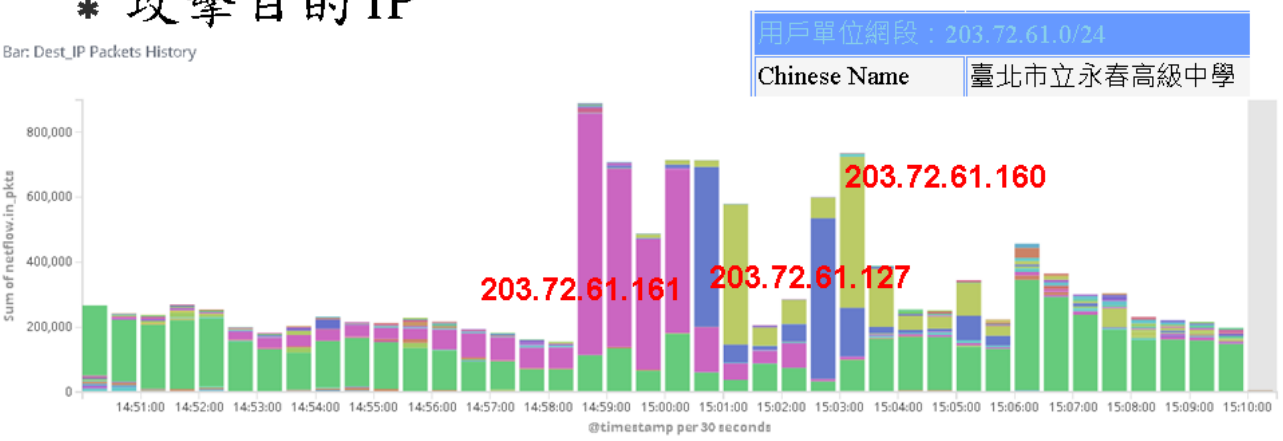


* Source Port: DNS, NTP 放大攻擊



3. 攻擊目標分析

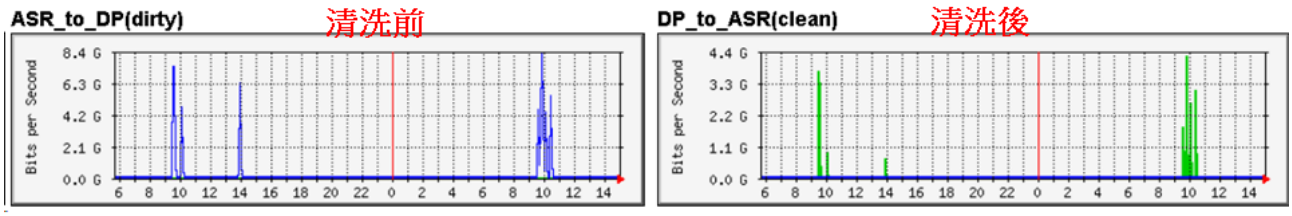
* 攻擊目的IP



* 每次不盡相同

4. 攻擊緩解方法

* 北區 ASOC 流量清洗



* ASR 至 Gigamon 分流器頻寬:40G 擴增至 80G
* 暫時移除 ASR 與主節點 BGP 之 BFD 設定

四、112 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。

(二)預期效益

1. 網路妥適率: 99.9%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: 85%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. 推廣無線漫遊認證: 建置於 2 個單位以上
9. 推廣網路品質監控系統: 建置於 3 個單位以上

10. HTTPS 網站自動檢核程式： check.twnic.tw (Selenium)
11. Google 表單增加發信回覆等功能。
12. 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。
13. 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。
14. 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。
15. 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%。
16. 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。
17. 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。
18. 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。
19. 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。
20. 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。
21. 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。
22. 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。
23. 針對加密流量提供具體可行的分析方法。

參、經費需求

□申請表

教育部補(捐)助計畫項目經費表(非民間團體) □核定表

申請單位: 國立臺灣大學	計畫名稱：臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫
計畫期程： 112 年 1 月 1 日至 112 年 12 月 31 日	
計畫經費總額：1,792,000 元，向本部申請補助金額：1,792,000 元，自籌款： 0 元	
擬向其他機關與民間團體申請補助：▓無□有 （請註明其他機關與民間團體申請補助經費之項目及金額） 教育部： 元，補助項目及金額： XXXX 部：.....元，補助項目及金額：	

補(捐)助項目	申請金額 (元)	核定計畫金額 (教育部填列) (元)	核定補助金額 (教育部填列) (元)	說明
人事費	1,400,545			1.聘任兼任計畫主持人 0 人、兼任協同主持人 0 人、專任行政助理 2 人(碩士 4 級 1 人含特殊薪酬加給、學士 9 級 1 人)、兼任行政助理 0 人，本計畫人員共 2 人。 2.所編費用含薪資、法定保險費用、勞退金、年終獎金及其補充保費。 3.補(捐)助款不得編列加班費及應休未休特別工資。 4.未依學經歷(職級)或期程聘用人員，致補(捐)助剩餘款不得流用。 5.所聘任之專任行政助理，為延攬聘任稀少性、技術性人員，若該員通過本校特殊性等助理申請審核，於補助計劃預算內給予加計資訊專業加給。
業務費	361,455			1.講座鐘點費(含補充保費)、工讀費、交通費、膳宿費等依講座鐘

				點費支給規定、二代健保規定、臨時人員薪資規範及國內出差旅費報支要點，訂有固定標準給付對象之費用。 2.依國內出差旅費報支要點之相關費用 。 3.辦理業務所需含維護運作費(辦公室電信費、水費、電費)，設備維護費，電腦、通訊、周邊設備之介面、零件，及專業證照、教育訓練費等，依「教育部補助臺灣學術網路區域網路中心管理作業要點」編列。 4.雜支費用(凡前項費用未列之辦公事務費用屬之。如文具用品、紙張、資料夾、郵資等，單價未達 1 萬元或耐用年限未達 2 年)依規定編列。
設備及投資	30,000			1.資訊軟硬體設備：電腦、網路交換器…等資訊設備(單價 1 萬元以上且耐用年限超過 2 年)。 2.個人電腦(含作業系統及螢幕)、筆記型電腦單價上限 3 萬元。
合　計	1,792,000			
承辦 單位	主(會)計 單位	首長		教育部 承辦人　　教育部 單位主管

補(捐)助方式：
□全額補(捐)助
□部分補(捐)助
指定項目補(捐)助□是□否
【補(捐)助比率　　%】

地方政府經費辦理方式：
□納入預算
□代收代付
□非屬地方政府

餘款繳回方式：
□繳回
□依本部補(捐)助及委辦經費核撥結報作業要點辦理
彈性經費額度:
□無彈性經費
□計畫金額 2%，計_____元(上限為 2 萬 5,000 元)

備註：
一、本表適用政府機關(構)、公私立學校、特種基金及行政法人。
二、各計畫執行單位應事先擬訂經費支用項目，並於本表說明欄詳實敘明。
三、各執行單位經費動支應依中央政府各項經費支用規定、本部各計畫補(捐)助要點及本要點經費

編列基準表規定辦理。

四、上述中央政府經費支用規定，得逕於「行政院主計總處網站-友善經費報支專區-內審規定」查詢參考。

五、非指定項目補(捐)助，說明欄位新增支用項目，得由執行單位循內部行政程序自行辦理。

六、同一計畫向本部及其他機關申請補(捐)助時，應於計畫項目經費申請表內，詳列向本部及其他機關申請補助之項目及金額，如有隱匿不實或造假情事，本部應撤銷該補(捐)助案件，並收回已撥付款項。

七、補(捐)助計畫除依本要點第 4 點規定之情形外，以不補(捐)助人事費、加班費、內部場地使用費及行政管理費為原則。

八、申請補(捐)助經費，其計畫執行涉及須依「政府機關政策文宣規劃執行注意事項」、預算法第 62 條之 1 及其執行原則等相關規定辦理者，應明確標示其為「廣告」，且揭示贊助機關（教育部）名稱，並不得以置入性行銷方式進行。

※依公職人員利益衝突迴避法第 14 條第 2 項前段規定，公職人員或其關係人申請補助或交易行為前，應主動據實表明身分關係。又依同法第 18 條第 3 項規定，違者處新臺幣 5 萬元以上 50 萬元以下罰鍰，並得按次處罰。

※申請補助者如符須表明身分者，請至本部政風處網站(https://pse.is/EYW3R)下載「公職人員及關係人身分關係揭露表」填列，相關規定如有疑義，請洽本部各計畫主政單位或政風處。