

107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

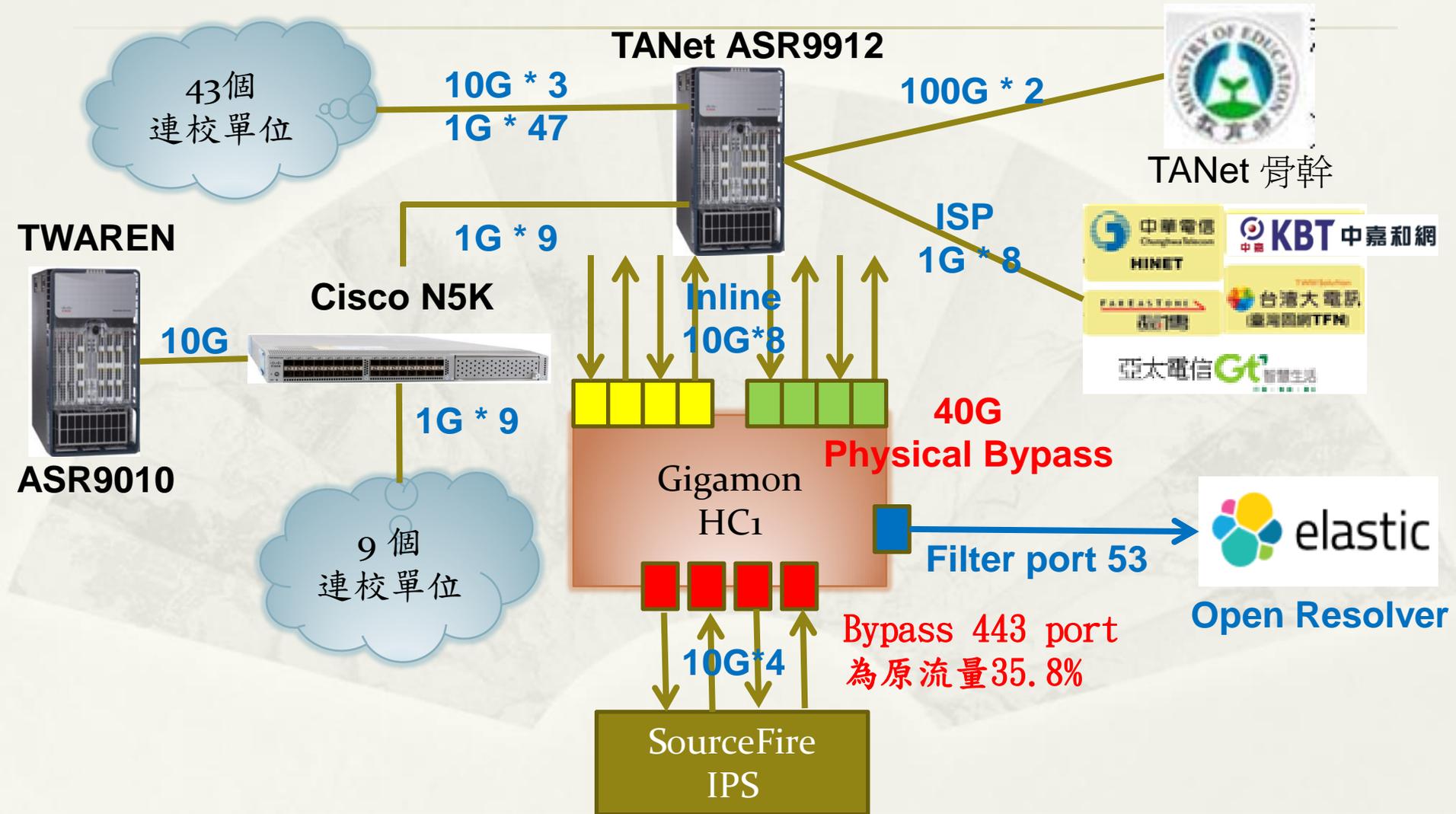
大綱

- * 1.區網人力與架構
- * 2.網路管理
- * 3.資安服務
- * 4.特色服務
- * 5.未來目標與建議

1. 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：謝宏昫教授
- * 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

1. 區網架構



2. 網路管理

- * 1. Cacti 建置符合 ISO27001 網管系統
- * 2. 提升網路服務品質
 - * Cacti-Plugin: MacTrack
- * 3. 連線單位技術支援
 - * 免費憑證安裝技術分享
 - * 如何隱藏 DNS 版本

2.1 Cacti 建置 ISO27001 網管系統

系統日誌 Review

* 監控 ASR Router Log 相關事件

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

寄件者: Cacti <Cacti@cactiusers.org>

寄件日期: 2017/11/16 (週四) 下午 09:26

收件者: 游子興

事件發生 email 通知
案例: 有人登入 Router

副本:

主旨: Event Alert - Alert-AUTHEN_SUCCESS

Hostname : 163.28.16.254

Date : 2017-11-16 21:25:16

Severity : Warning

Priority : 6

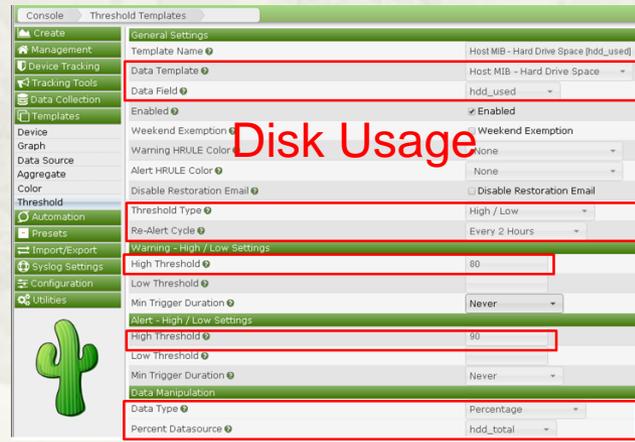
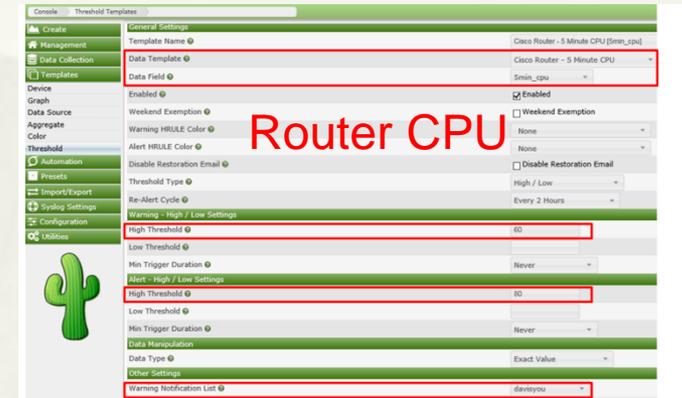
Message :

RP/0/RP0/CPU0:Nov 16 21:25:16.045 : exec[65944]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'ntuadmin1' from '192.168.214.133' on 'vty4'



設備狀態監控 Threshold

- * Router CPU : 80%
- * Interface Traffic Usage: 90%
- * Disk Usage: 80%
- * Interface Traffic Abnormal:
* Deviation 170%



Router CPU 80%

告警

Console Graphs Reporting Logs Syslog Thold Device Tracking

Console Thold Graph Logged in as admin

Thresholds Log Device Status

Threshold Log for [6 Months]

Search Enter a search term Site All Device Any Go Clear

Threshold All Status All Entries Default

All 8 Log Entries

Device	Time	Type	Event Description	Alert Value
Dept6509	2018-07-30 17:25:03	High / Low	NORMAL: Dept6509 - 5 Minute CPU [5min_cpu] Restored to Normal Threshold with Value 41	N/A
Dept6509	2018-07-30 17:20:03	High / Low	ALERT -> WARNING: Dept6509 - 5 Minute CPU [5min_cpu] Changed to Warning Threshold with Value 69	60
Dept6509	2018-07-30 17:15:15	High / Low	ALERT -> WARNING: Dept6509 - 5 Minute CPU [5min_cpu] Changed to Warning Threshold with Value 61	60
IM6509	2018-07-06 16:10:03	High / Low	NORMAL: IM6509 - 5 Minute CPU [5min_cpu] Restored to Normal Threshold with Value 17	N/A
Server6509	2018-07-06 16:10:03	High / Low	NORMAL: Server6509 - 5 Minute CPU [5min_cpu] Restored to Normal Threshold with Value 25	N/A
EE6509	2018-07-06 16:10:03	High / Low	Alert: Cacti <davisyou@gmail.com>	N/A
Dept6509	2018-07-06 16:10:03	High / Low	Alert: 游子典	N/A
www.tp1rc.edu.tw	2018-07-06 15:35:03	High / Low	Alert: 副本: with Value 30	N/A

Alert Alert2Warn

A warning has been issued that requires your attention.

Device: Dept6509 (140.112.1.10)
URL: [Link to Graph in Cacti](#)
Message: ALERT -> WARNING: Dept6509 - 5 Minute CPU [5min_cpu] Changed to Warning Threshold with Value 69

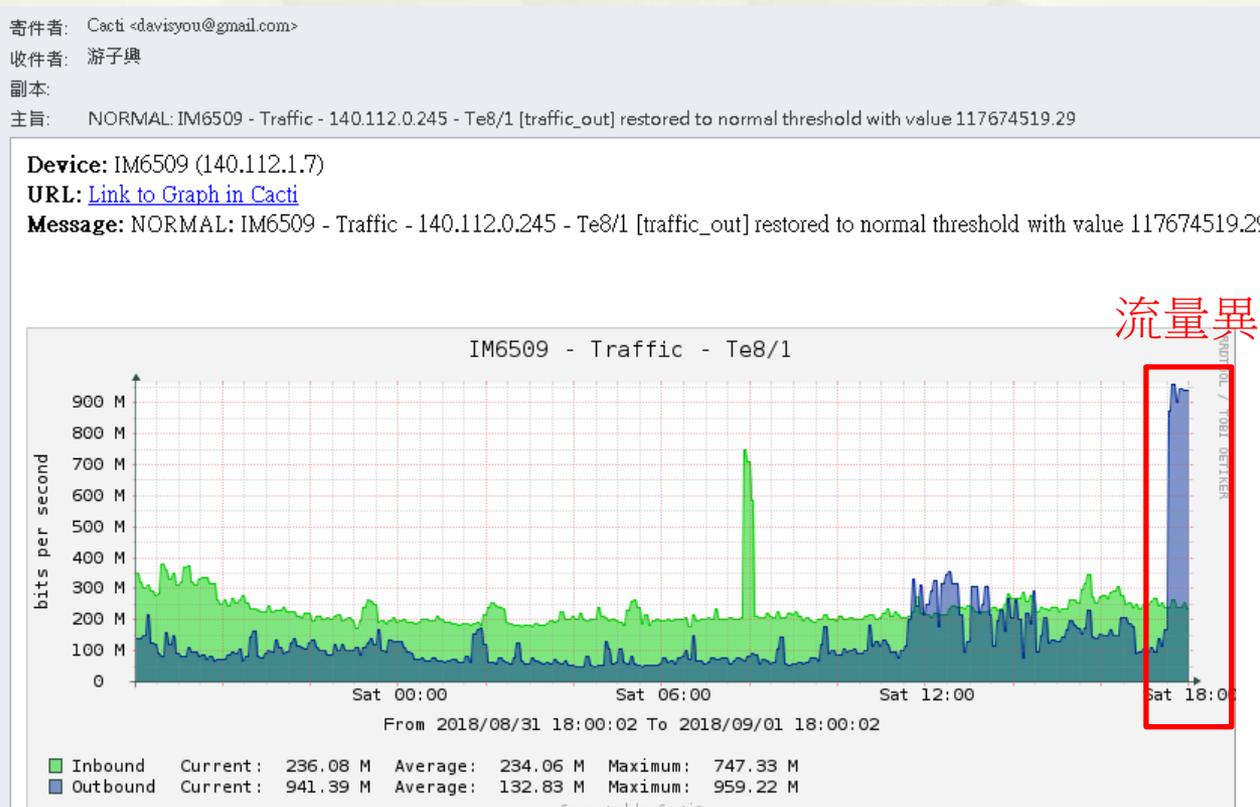
Dept6509 - CPU Usage

■ CPU Usage Current: 69 Average: 21 Maximum: 69
Generated by Cacti

CPU % 異常

Interface Traffic Abnormal 告警

- * 依據過去歷史統計資訊設定異常差異標準差



2.2 提升網路服務品質

Cacti-Plugin: MacTrack

- * 網管之限制與困境
 - * ARP Timeout: 4 hours(default)
 - * 電腦更換、重灌系統後忘記 IP
 - * IP 盜用、IP 使用狀況
 - * MAC address Timeout: 300 seconds(default)
 - * 無法快速找到 Gateway Router/Edge Switch
 - * 斷線太久追不到 Interface Port
 - * Interface Up/Down: syslog
 - * Up/Down 歷史記錄已被覆寫
- * 解決方案
 - * Cacti-Plugin: Device Tracking(MacTrack)

Cacti-Plugin: MacTrack ARP/IP View

Device Tracking IP Address Viewer Logged in as admin ▾

Sites | Devices | IP Ranges | **IP Address** | MAC Address | Interfaces | Dot1x | Graphs

Device Tracking - ARP/IP View

Search: Enter a search term 🔍 Site: N/A Device: All IP's: Default Go Clear Export

IP: Contains 140.112.3.
MAC:

Gateway 設備 使用者 IP MAC 設備廠牌

Switch Name	Switch Hostname	ED IP Address	ED MAC Address	Vendor Name	Port Number	Port Name
Server6509	140.112.1.16	140.112.3.1	00:90:E8:1A:8A:B8	Moxa Technologies Corp., Ltd.	163	VI304
Server6509	140.112.1.16	140.112.3.4	14:DA:E9:97:13:25	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.5	BC:EE:7B:DD:0B:7D	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.6	BC:EE:7B:DB:5D:75	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.16	00:50:56:BF:00:0A	Vmware, Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.20	00:02:B3:D3:FF:DF	Intel Corporation	163	VI304
Server6509	140.112.1.16	140.112.3.21	00:1B:21:2A:10:AA	Intel Corporate	163	VI304
Server6509	140.112.1.16	140.112.3.22	A4:EE:57:F5:88:D2	Seiko Epson Corporation	163	VI304
Server6509	140.112.1.16	140.112.3.23	AC:E2:D3:D7:EE:6A	Hewlett Packard	163	VI304
Server6509	140.112.1.16	140.112.3.25	00:25:64:E7:30:90	Dell Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.34	E0:CB:4E:7A:94:AA	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.35	54:04:A6:7F:D1:AD	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.57	10:78:D2:AA:F9:C0	Elitegroup Computer Systems Co.,ltd.	163	VI304
Server6509	140.112.1.16	140.112.3.58	00:26:18:83:39:45	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.61	14:DA:E9:97:D9:40	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.62	10:78:D2:C9:59:6F	Elitegroup Computer Systems Co.,ltd.	163	VI304
Server6509	140.112.1.16	140.112.3.63	30:85:A9:A4:40:26	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.64	E0:3F:49:E7:C2:87	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.67	C8:60:00:8D:DE:AA	Asustek Computer Inc.	163	VI304
Server6509	140.112.1.16	140.112.3.68	B0:6E:BF:5C:61:B7	Asustek Computer Inc.	163	VI304

Cacti-Plugin: MacTrack

* MAC to IP Report View

Sites Devices IP Ranges IP Address MAC Address Interfaces Dot1x Graphs

Device Tracking - MAC to IP Report View

Search Enter a search term Site N/A Device All MAC's 10 Go Clear Export

IP Matches 140.112.3.3 VLAN Name All Show All

MAC Authorized All

Portname

IP 相同, MAC 更換
更換設備? IP 盜用?

上線時間

Actions	Switch Name	Switch Hostname	ED IP Address	ED MAC Address	Vendor Name	Port Number	Port Name	VLAN ID	VLAN Name	Last Scan Date
	Server6509	140.112.1.16	140.112.3.3	00:0C:29:83:B4:6A	Vmware, Inc.	Gi8/26		304	VLAN0304	2018-09-06 12:25:03
	Server6509	140.112.1.16	140.112.3.3	00:0C:29:83:B4:74	Vmware, Inc.	Gi8/26		304	VLAN0304	2018-09-06 16:30:04

All 2 MAC Addresses

* Network Interfaces View

Device Tracking View Interfaces

Sites Devices IP Ranges IP Address MAC Address Interfaces Dot1x Graphs

Device Tracking - Network Interfaces View

Site All Filters Up Interfaces Bandwidth >=70% Go Clear Export

Type All Device L2_R_library_3560 Interfaces Default

Search Enter a search term Show Totals

介面狀態
異動時間

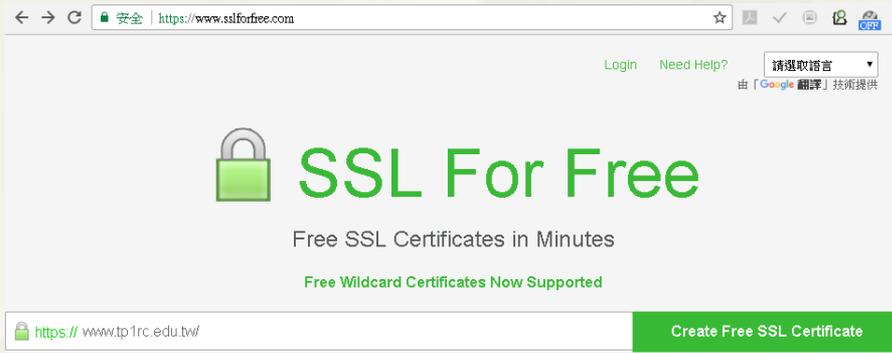
Actions	Hostname	Type	Name	Description	Alias	InBound	OutBound	In (B/S)	Out (B/S)	In Err Total	In Disc Total	UPproto Total	Out Err Total	Out Disc Total	Status	Last Change
	L2_R_library_3560	CISCO IOS	Fa0/6	FastEthernet0/6	## Farm ##	5.4 %	4.5 %	660.4 k	553.2 k	0	0	775	0	0	Up	Since Restart
	L2_R_library_3560	CISCO IOS	Fa0/7	FastEthernet0/7	Weather Control	0.1 %	0 %	15.87 k	37	0	0	0	0	0	Up	Since Restart
	L2_R_library_3560	CISCO IOS	Fa0/8	FastEthernet0/8	## Monitor System ##	12.7 %	0.5 %	1.510 m	59.32 k	0	0	0	0	0	Up	Since Restart
	L2_R_library_3560	CISCO IOS	Fa0/9	FastEthernet0/9	## Agron 75 ##	0.4 %	3.5 %	47.53 k	432.4 k	0	0	0	0	0	Up	Since Restart
	L2_R_library_3560	CISCO IOS	Fa0/19	FastEthernet0/19	## Coffee store ##	0 %	0.3 %	1.176 k	32.88 k	0	0	0	0	0	Up	Since Restart
	L2_R_library_3560	CISCO IOS	Fa0/4	FastEthernet0/4	## Lib_198 ##	2.2 %	20.8 %	272.1 k	2.483 m	0	0	112491	0	0	Up	39d:1h:58m
	L2_R_library_3560	CISCO IOS	Gi0/1	GigabitEthernet0/13750	## R_Library Lib_198 ##	3.1 %	2.1 %	3.682 m	2.489 m	0	0	0	0	0	Up	Since Restart
	L2_R_library_3560	CISCO IOS	Fa0/5	FastEthernet0/5	## Lib_198 ##	0.1 %	0.4 %	16.79 k	52.75 k	1	0	0	0	0	Up	39d:1h:58m

All 8 Interfaces

Scanning Rate: Every 4 Hours, Status: Idle, LastRuntime: 231.700000 seconds, Processes: 7 processes, Devices: 0, Next Run Time: 2018-09-12 22:55:04

2.3 連線單位技術支援 免費憑證安裝技術分享

* 免費憑證申請(90 days)



* 技術文件

» Home » 關於台北區網 » 網路品質管理

區網會議:

- ▶ 107年度北區區網委員會第一次會議
- 區網管理營運業務報告
- 資安Case Study分享
- 台師大雲端建置與各校區網路架構分享
- SSL憑證安裝與申請**

106年評審委員建議：
第 8 點 研創成果呈現於區網中心網頁。



2.3 連線單位技術支援 如何隱藏 DNS 版本

* 顯示DNS 版本可能暴露漏洞

學校名稱	FQDN	DNS server Ipv4	DNS server Ipv6	DNS server 版本
致理科技大學	dns.chihlee.edu.tw	140.131.77.1	2001:288:100f:1::2	BIND 9.6.-ESV-R3
	dns2.chihlee.edu.tw	140.131.77.33	2001:288:100f:1::3	BIND 9.6.-ESV-R3
	dns3.chihlee.edu.tw	211.22.7.173		停用
華夏科技大學	proxy1.hwh.edu.tw	140.131.39.205		bind 9.10.5-P3
	cc.hwh.edu.tw	140.131.39.200		bind 9.10.5-P3
	proxy2.hwh.edu.tw	140.131.39.206		bind 9.10.5-P3
	hwh.edu.tw	140.131.39.1		bind 9.10.5-P3
新北市立圖書館	dns.tphcc.gov.tw	203.64.154.1	2001:288:102c:1::2	Infoblox 7.3.13
國北教大實小	ntuees.tp.edu.tw	203.64.153.100		NTUEES DNS
樹人家商	dns.stgvs.ntpc.edu.tw	203.71.206.1		bind 9.3.4-p1.1
龍華科技大學	dns2.lhu.edu.tw	140.131.1.20		bind 9.9.9-P8
	dns.lhu.edu.tw	140.131.1.11		bind 9.9.9-P8
	dns3.lhu.edu.tw	218.32.30.125		bind 9.9.9-P8
東海高中	dns.thhs.ntpc.edu.tw	210.71.122.1		TIME OUT
開平中學	ns.kpvs.tp.edu.tw	61.219.31.96		9.3.6-P1-RedHat-9.3.6-20.P1.e15_8.6
	ns2.kpvs.tp.edu.tw	203.72.253.2		9.8.2xc1-RedHat-9.8.2-0.37.rc1.e16_7.5
光啟高中	dns.phsh.tyc.edu.tw	210.71.74.1		Bind 9.3.6-P1-RedHat-9.3.6-20.P1.e15_8.6,
南山高中	dns1.nssh.ntpc.edu.tw	203.71.175.1		bind 9.10.3
	dns.nssh.ntpc.edu.tw	203.71.175.1	2001:288:102f:2::1	bind 9.10.3
	dns2.nssh.ntpc.edu.tw	203.71.175.51		bind 9.10.3
台北護理健康大學	dns.ntunhs.edu.tw	140.131.85.210		9.3.6-P1-RedHat-9.3.6-25.P1.e15_11.6
	dns2.ntunhs.edu.tw	140.131.85.212		9.3.6-P1-RedHat-9.3.6-25.P1.e15_11.4
中華民國學生棒球運動聯盟	ns1.ctsbf.edu.tw	140.131.124.1		9.8.2xc1-RedHat-9.8.2-0.17.rc1.e16_4.4
臺灣藝術大學	sd1.ntua.edu.tw	140.131.21.1		Microsoft DNS 6.1.7601 (IDB15CD4)
	sd2.ntua.edu.tw	140.131.21.10		Microsoft DNS 6.1.7601 (IDB15CD4)

隱藏 DNS Server version

- * Linux

- * 修改 bind 設定檔

- ~# vi /etc/named.conf

- options {

- version "None of your business";

- * Windows

- * dnscmd /config /EnableVersionQuery o

```
D:\>nslookup -class=chaos -query=txt version.bind 163.28.16.46
伺服器: UnKnown
Address: 163.28.16.46

version.bind      text =
                  "None of your business"
version.bind      nameserver = version.bind
```

```
D:\>nslookup -class=chaos -query=txt version.bind 220.134.115.14
(root) nameserver = k.root-servers.net
(root) nameserver = l.root-servers.net
(root) nameserver = m.root-servers.net
(root) nameserver = a.root-servers.net
(root) nameserver = b.root-servers.net
(root) nameserver = c.root-servers.net
(root) nameserver = d.root-servers.net
(root) nameserver = e.root-servers.net
(root) nameserver = f.root-servers.net
(root) nameserver = g.root-servers.net
(root) nameserver = h.root-servers.net
(root) nameserver = i.root-servers.net
(root) nameserver = j.root-servers.net
k.root-servers.net      internet address = 193.0.14.129
l.root-servers.net      internet address = 199.7.83.42
m.root-servers.net      internet address = 202.12.27.33
伺服器: UnKnown
Address: 220.134.115.14

DNS request timed out.
        timeout was 2 seconds.
*** 對 UnKnown 的要求逾時
```

3. 資安服務

- * 1. 107年度資安事件統計
- * 2. DDoS 案例分析

3.1 107年度資安事件統計

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

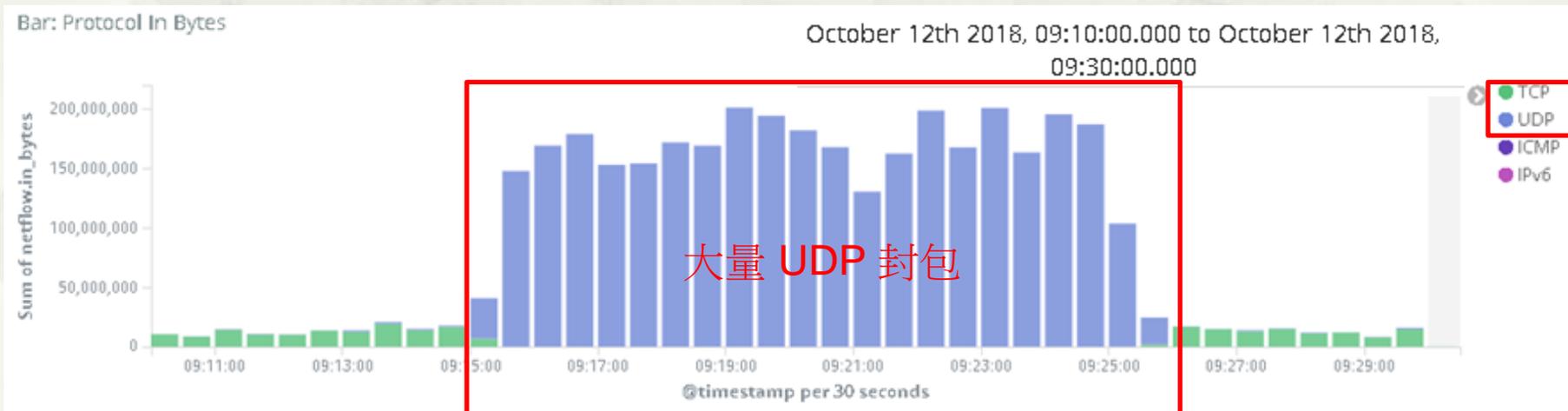
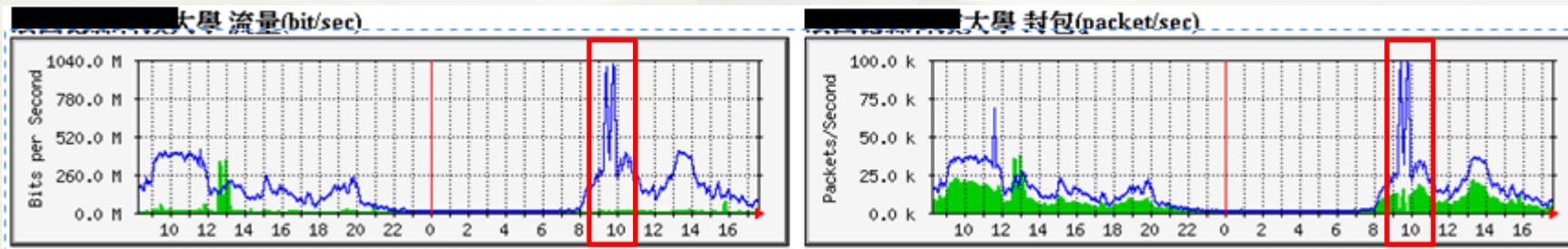
106年評審委員建議:

- 第 1 點 資安事件應變處理時數建議可逐步縮短
- 第 5 點 資安事件處理時效長，但仍請積極處理。

3.2 DDoS 案例分析

- * DDoS 攻擊方法
 - * 新型 LDAP 攻擊取代傳統 DNS、NTP 放大攻擊
- * DDoS 攻擊來源
 - * 過去使用 Internet Server(NTP, Open Resolver) 轉而利用現成雲端資源
- * 通報清洗機制建議

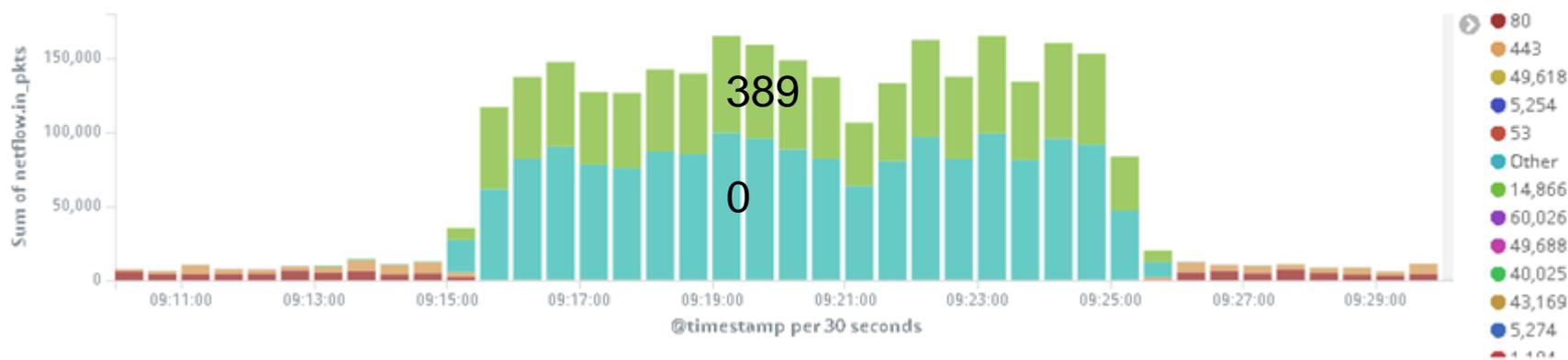
連線學校 DDoS 攻擊前後流量分析



攻擊來源與目的

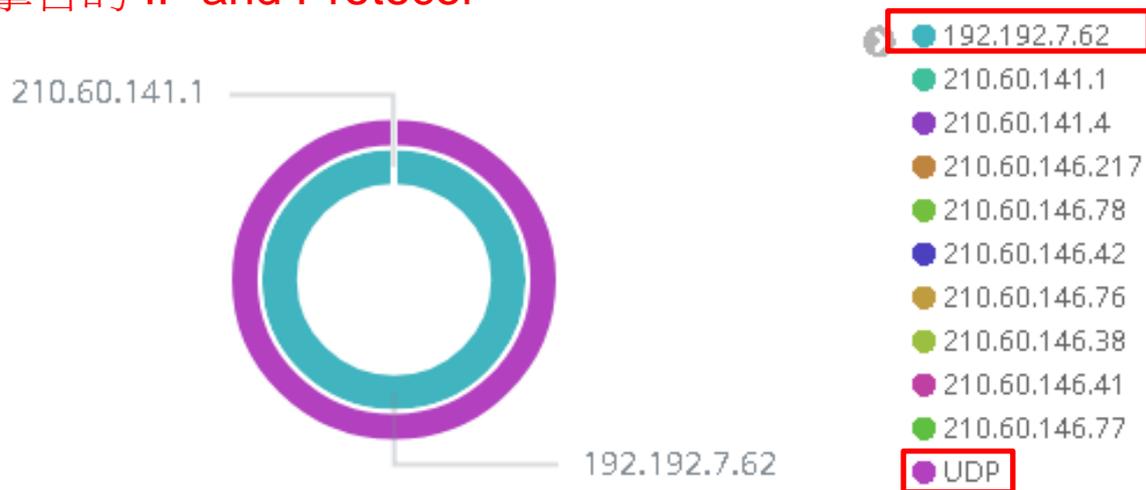
Bar: Source Port In Packets

攻擊來源 Port 389 (LDAP)



Pie: Dest_IP Protocol Top In Packets

攻擊目的 IP and Protocol



攻擊來源 Top ASN

* 攻擊來源: 各大雲端平台

Tag: Source_AS In Bytes



攻擊來源 Top ASN OVH SAS

Google OVH SAS

全部 地圖 圖片 新聞 影片 更多 設定 工具

約有 1,380,000 項結果 (搜尋時間 : 0.43 秒)

OVH: Cloud computing and dedicated servers
<https://www.ovh.com/world/> ▾ 翻譯這個網頁
Products and servicesEmailsVPSDedicated ServersSo you Start serversPublic CloudDedicated Cloud · **Hosting** Plans. Community & toolsOVH ManagerOVH ...
[Dedicated Hosting Servers](#) · [About](#) · [Report abuse \(abuse@ovh.net\)](#) · [VPS](#)
您已造訪這個網頁 2 次。上次造訪日期 : 2018/9/20

OVH: Web hosting, cloud computing and dedicated servers
<https://ovh.co.uk/> ▾ 翻譯這個網頁
OVH provides everything you need for a successful online project: web **hosting**, domain names, dedicated servers, CDN, cloud environments, Big Data...
[About](#) · [Abuse](#) · [Webmail](#) | [OVH](#) · [OVH News](#)

OVH - Wikipedia
<https://en.wikipedia.org/wiki/OVH> ▾ 翻譯這個網頁
Products, VPS, **Hosting**, Web **hosting**, DSL. Revenue, Increase 320 million € (2016). Website, www.ovh.com. OVH is a French cloud computing company that offers VPS, dedicated servers and other web ...
Headquarters: [Roubaix, France](#) **Industry:** Cloud computing, Hosting
Products: [VPS](#), [Hosting](#), [Web hosting](#), [DSL](#) **Revenue:** 320 million € (2016)
[Facts and figures](#) · [Wikileaks](#)
您已造訪這個網頁 2 次。上次造訪日期 : 2018/9/20

OVH
公司



創辦人 : Octave Klaba
創立於 : 1999 年 **法國巴黎**
收益 : 3.2 億歐元
子公司 : [OVH US LLC](#) · [OVH Limited](#)
核心成員 : [Octave Klaba](#) · [Henryk Klaba](#)
上級機構 : [Ovh Groupe](#)

攻擊來源 Top ASN OVH SAS

host.keyword: "192.192.60.112"

netflow.output_snmp: "159"

netflow.protocol.keyword: "UDP"

geoiip_src.as_org.keyword: "OVH SAS"

Map: Source_Location In Packets



攻擊來源 Top ASN Microsoft Corporation

host.keyword: "192.192.60.112"

netflow.output_snmp: "159"

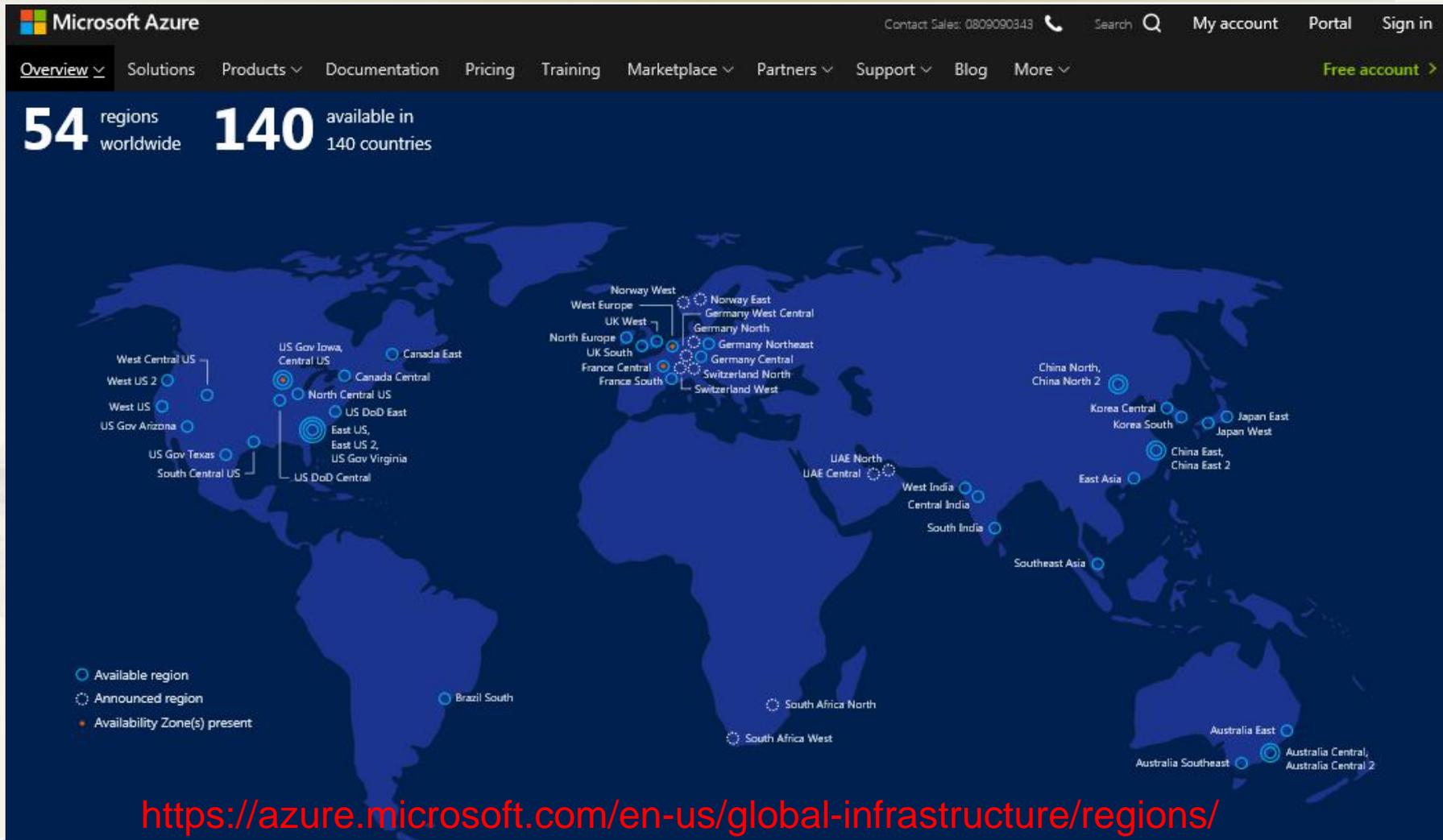
netflow.protocol.keyword: "UDP"

geoip_src.as_org.keyword: "Microsoft Corporation"

Map: Source_Location In Packets



Microsoft Azure regions



攻擊來源 Top ASN Amazon.com, Inc.

host.keyword: "192.192.60.112"

netflow.output_snmp: "159"

netflow.protocol.keyword: "UDP"

geoiip_src.as_org.keyword: "Amazon.com, Inc."

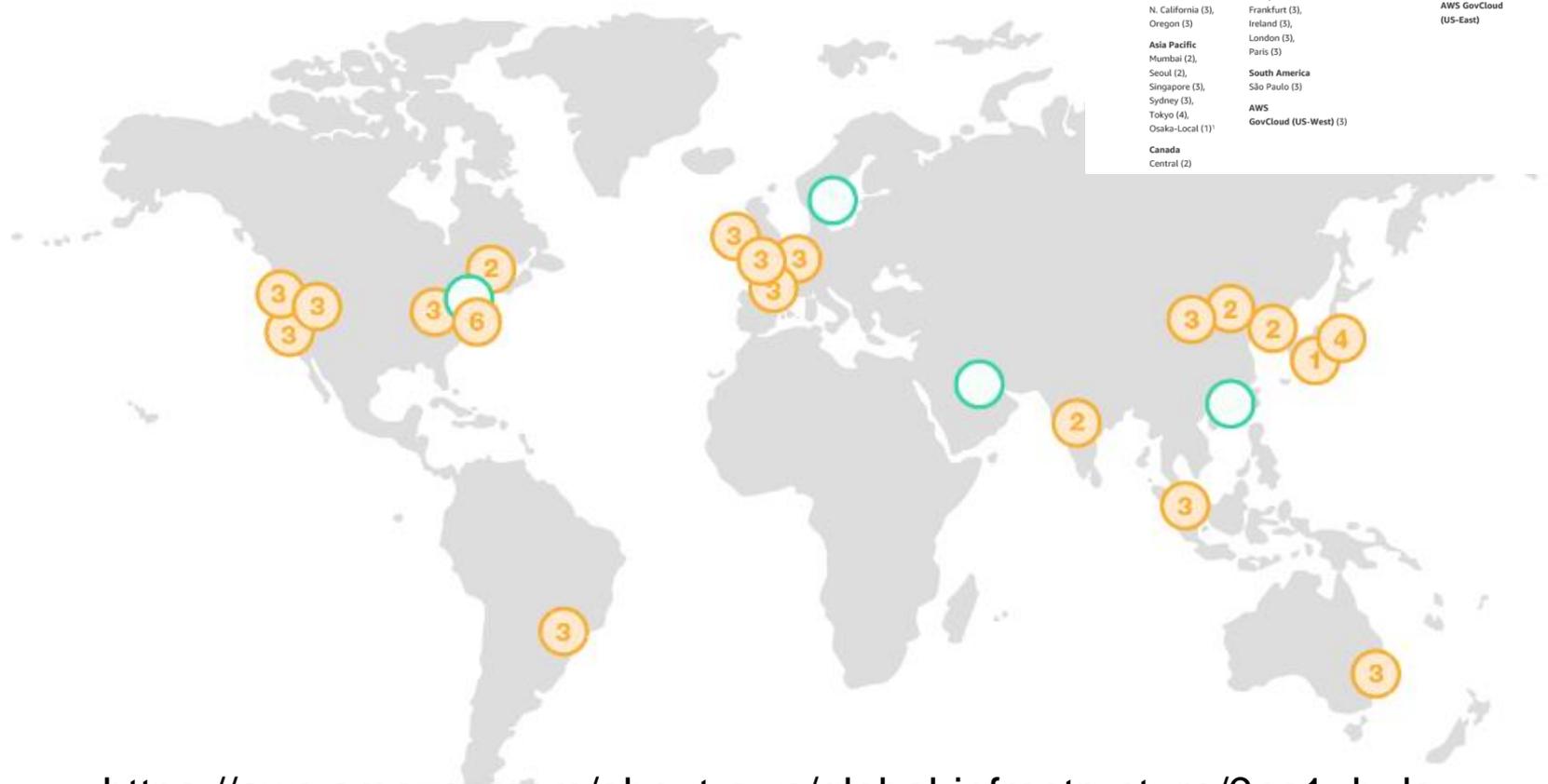
Map: Source_Location In Packets



AWS Global Infrastructure

Global Infrastructure

#	Region & Number of Availability Zones	New Region (coming soon)
	US East N. Virginia (6), Ohio (5)	Bahrain Hong Kong SAR, China Sweden AWS GovCloud (US-East)
	US West N. California (3), Oregon (3)	
	Europe Frankfurt (3), Ireland (3), London (3), Paris (3)	
	Asia Pacific Mumbai (2), Seoul (2), Singapore (3), Sydney (3), Tokyo (4), Osaka-Local (1) ¹	
	South America São Paulo (3)	
	AWS GovCloud (US-West) (3)	
	Canada Central (2)	



https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls

DDoS 案例分析

- * LDAP 是微軟 Active Directory 認證使用之通訊協議，因雲端租用使用者可能有遠端認證需求，又未限制來源IP，而被駭客利用作為放大攻擊。
- * DDoS 攻擊來源已從過去使用 Internet Server(NTP, Open Resolver) 轉而利用現成雲端資源。
- * 雲端資源主機多且對外流量大。
- * 雲端租用計費方式: 上傳流量不計費、僅計算下載流量
 - * 雲端公司也許不會主動告知流量異常(Money \$\$\$\$\$...)
 - * 租用雲端使用者誤以為網站變熱門，下載流量變高

雲端業務扮演火車頭，Azure強勢成長89%

雲端業務是這幾年推升微軟營收的強力引擎，原因是越來越多企業將工作資料轉移到雲端，以此降低資料儲存、軟體成本。根據市場研究公司Canalys的預估，公用雲端服務平台Azure在全市場占比達16%，是僅次於亞馬遜AWS的全球第二大雲端服務供應商。

通報清洗機制

報表查詢系統
Developed By TACERT

| 您好 登出

OID查詢 威脅名單 事件單列表 EWA列表 事件類型統計 轄下單位密碼更動情況 DDOS清洗系統

清洗IP*	192.192.7.62
DNS IP	
單位名稱*	██████████大學
通訊協定*	UDP
服務說明*	LDAP 例如:WEB FTP
通訊埠*	389 例如:80
申請理由	遭受DDoS 攻擊
	送出 (本系統僅適用於TANET部份地區)

上述資訊非能在發生攻擊時短時間得知
建議應建立南北 SOC 主動通知機制

4. 特色服務

- * 1. TCP-based 網路品質監控
- * 2. Line Bot 網路監控系統
- * 3. Layer 7 網路行為分析
- * 4. 高風險協定分析

4.1 TCP-BASED 網路品質監控

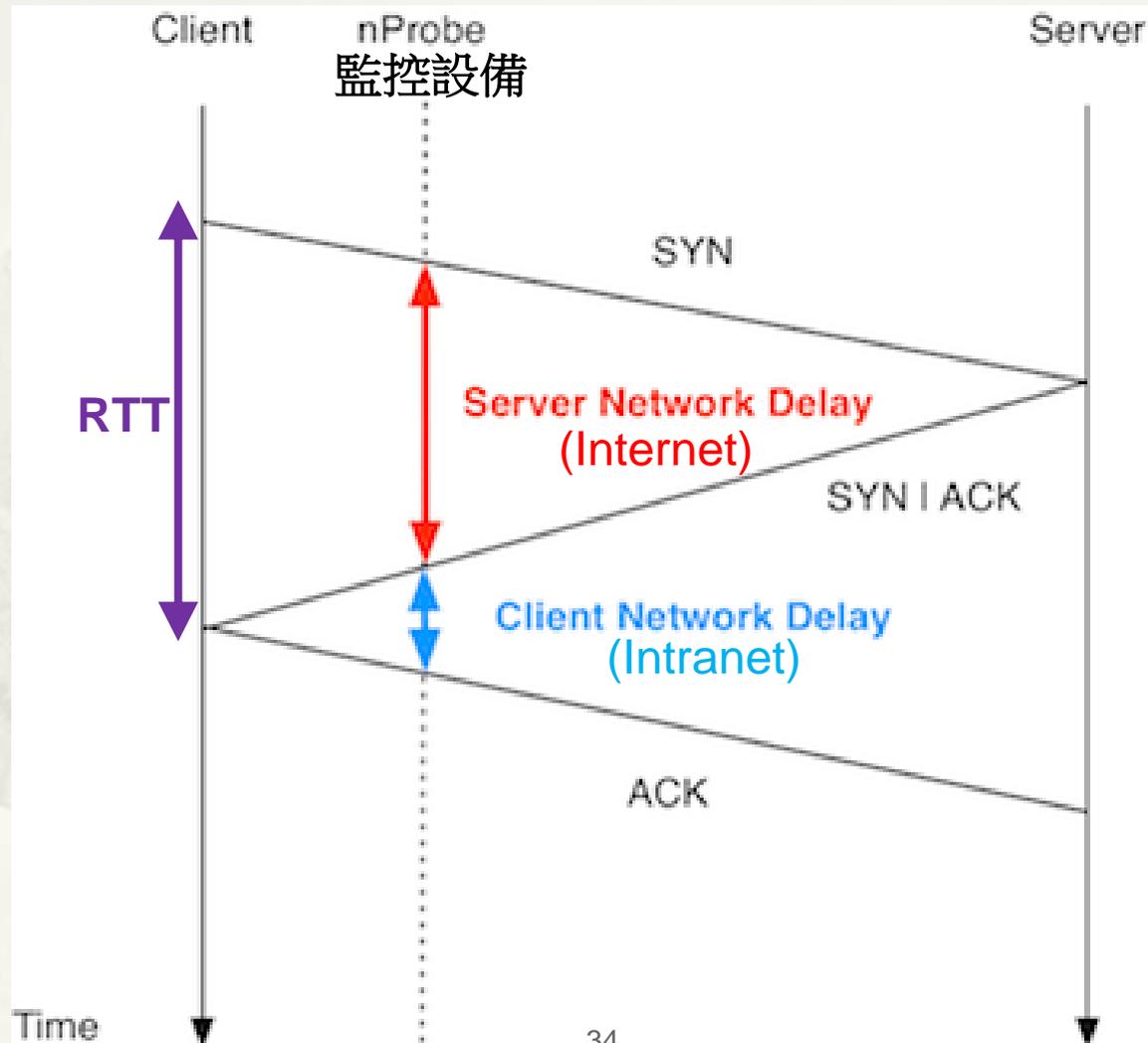
傳統網路品質監控

- * 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

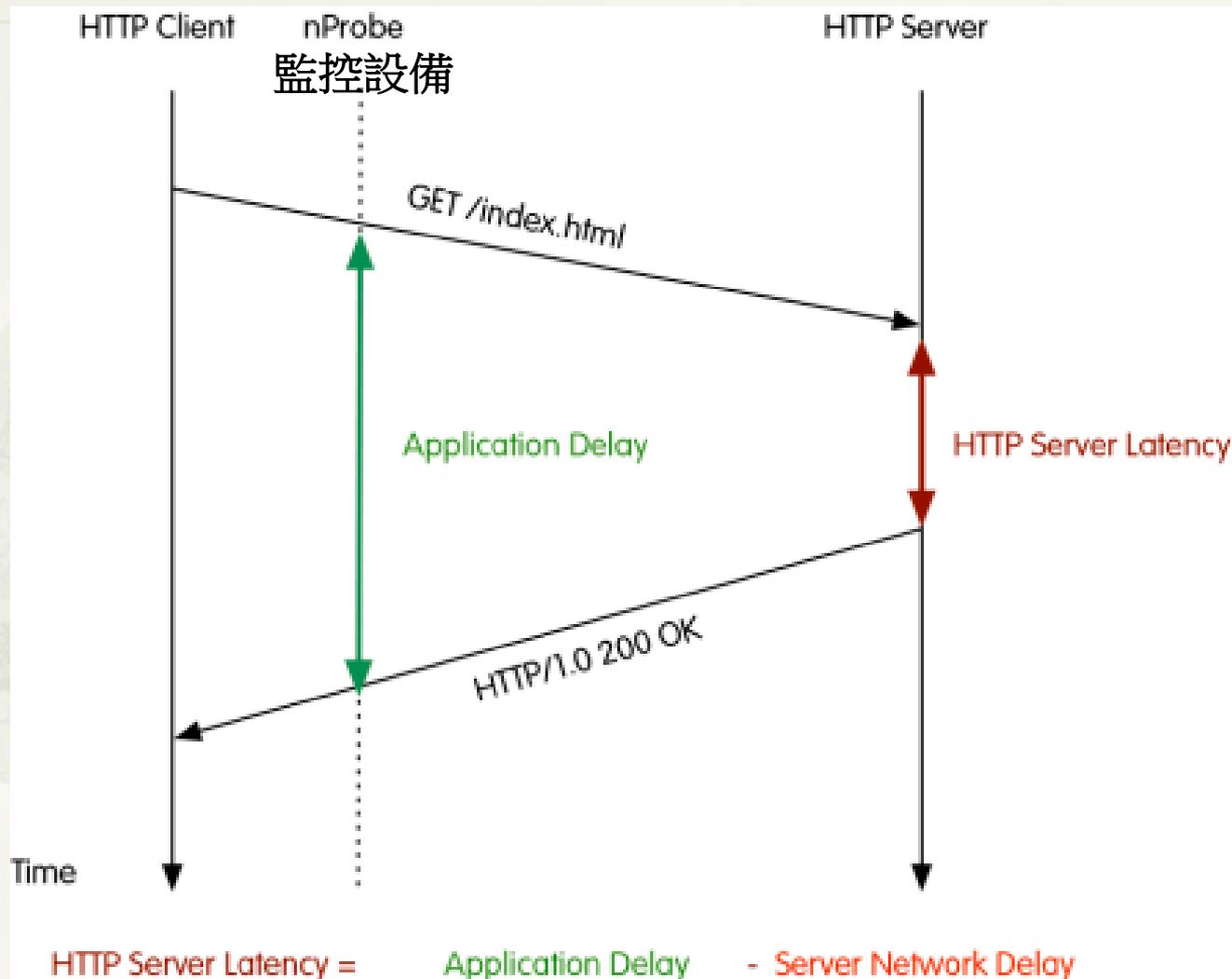
TCP-based 網路品質監控

- * 監控方法: TCP
 - * RTT: TCP 3-way handshake
 - * Packet Lost: TCP Retrasmit & OutOfOrder

Network Latency



Application Latency



監控設備

* 新一代 Router

* Cisco Application Visibility and Control Solution (Cisco AVC)

* Cisco ASR 1000

* Use Netflow V9/V10 自訂格式

* flow record name

collect connection delay network to-server sum

collect connection delay network to-client sum

collect connection delay application sum

collect connection client counter packets retransmitted

* Mirror/SPAN 到外部設備進行分析

* Cisco Flow Sensor

* nProbe (教育與研究機構免費)

* Inline 設備: Proprietary Report

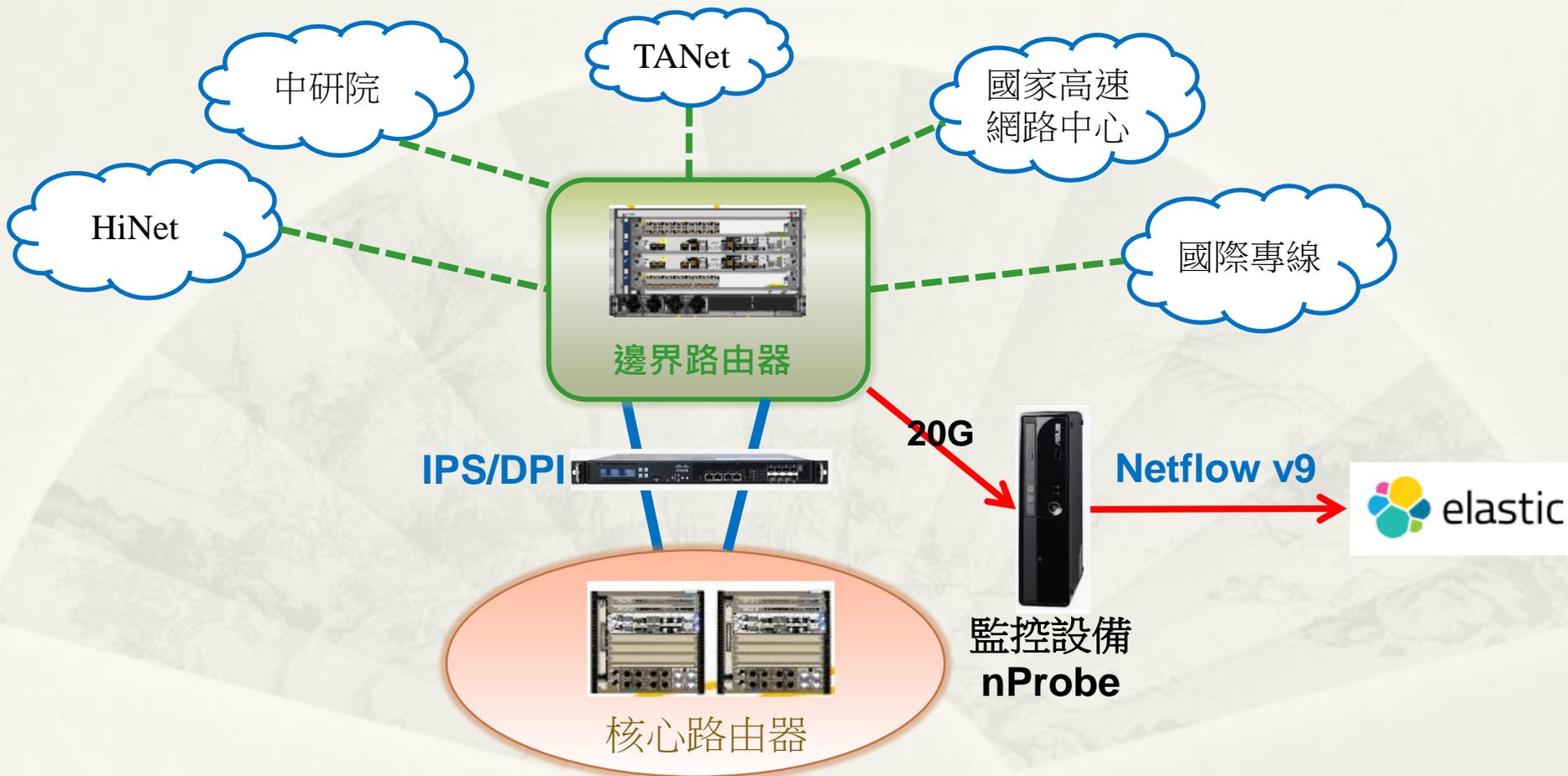
* 頻寬管理器/DPI 設備: Procera

TCP-based 網路品質監控

* 優點

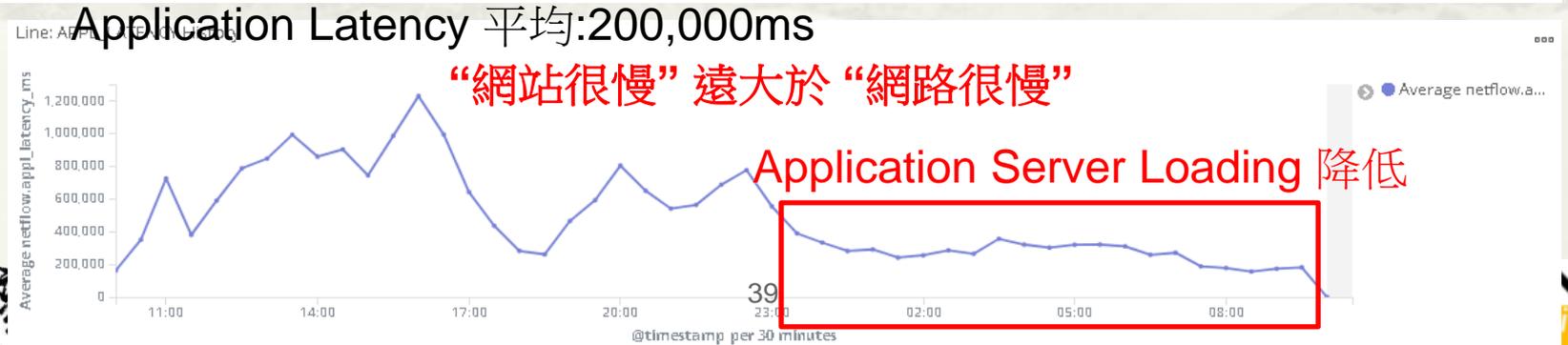
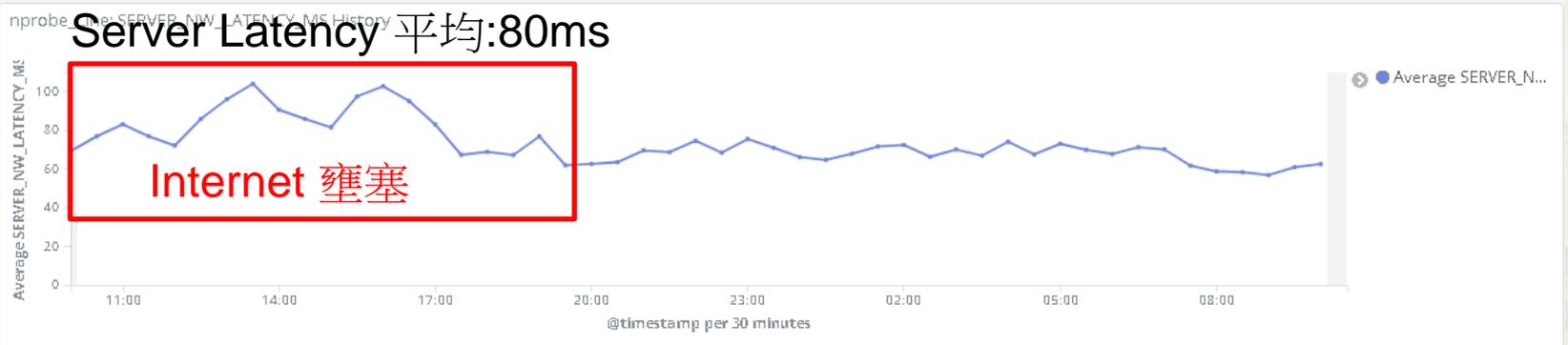
- * 被動式偵測(封包 Listening)，不佔用頻寬資源
- * 可快速釐清 Intranet or Internet 緩慢或異常
- * 不需佈建監控設備，節省電力與資源
- * 準確性更高: 網路現成大量連線記錄提供量測結果
- * 可追溯過去之歷史統計記錄

TCP-based 網路品質監控 臺大網路架構圖



Latency 24 Hrs 統計

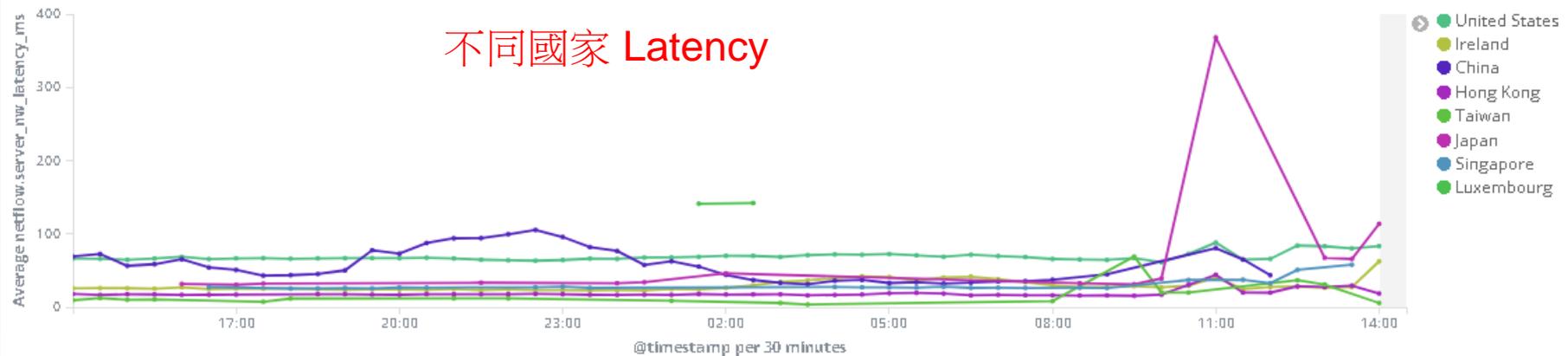
NPROBE_IPV4_ADDRESS: "10.3.1.212" INPUT_SNMP: "2" Add a filter + Actions ▶



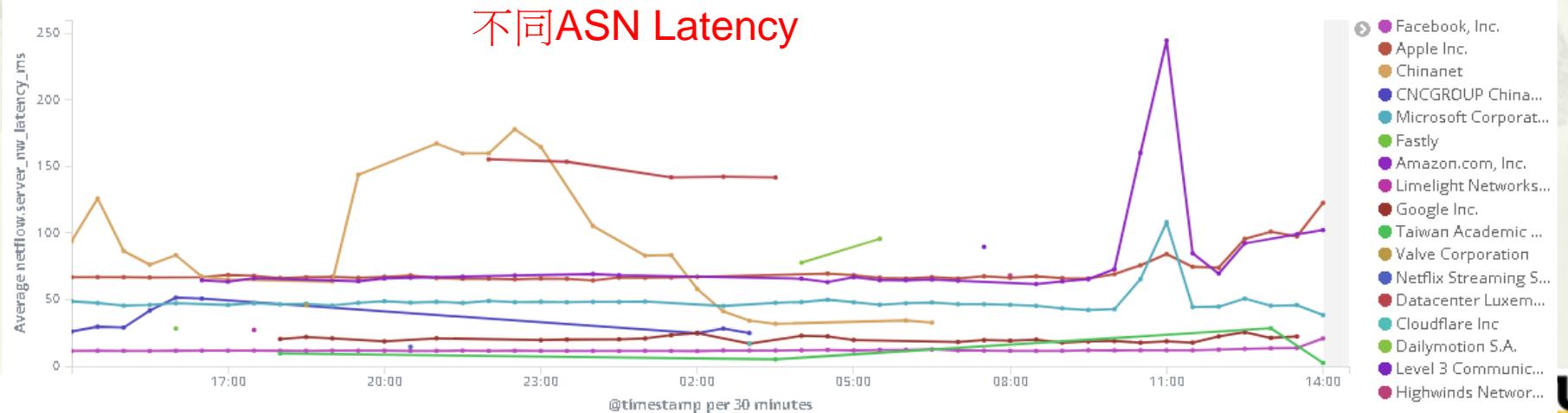
Latency 24 Hrs 統計

國家/ASN

Line: SERVER_LATENCY Dest_Country(Max PKT) History



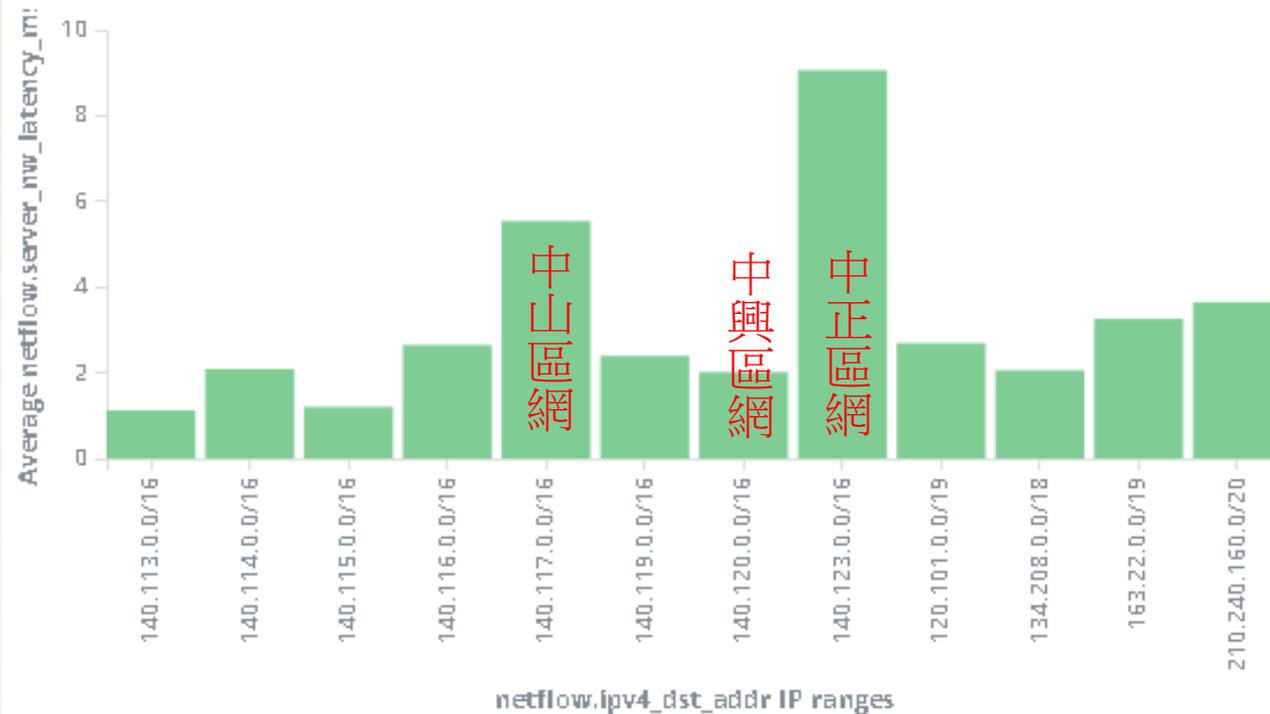
Line: SERVER_LATENCY Dest_AS(Max PKT) History



Latency 24 Hrs 統計

各區網中心

Bar: Server_Latency TANet



```
C:\Windows\System32>ping www.ccu.edu.tw -t

Ping hero1.ccu.edu.tw [140.123.5.5] <使用 32 位元組的資料>:
回覆自 140.123.5.5: 位元組=32 時間=33ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=9ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=8ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=8ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=32ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=42ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=11ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=29ms TTL=54

140.123.5.5 的 Ping 統計資料:
    封包: 已傳送 = 13, 已收到 = 13, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 7ms, 最大值 = 42ms, 平均 = 16ms
```

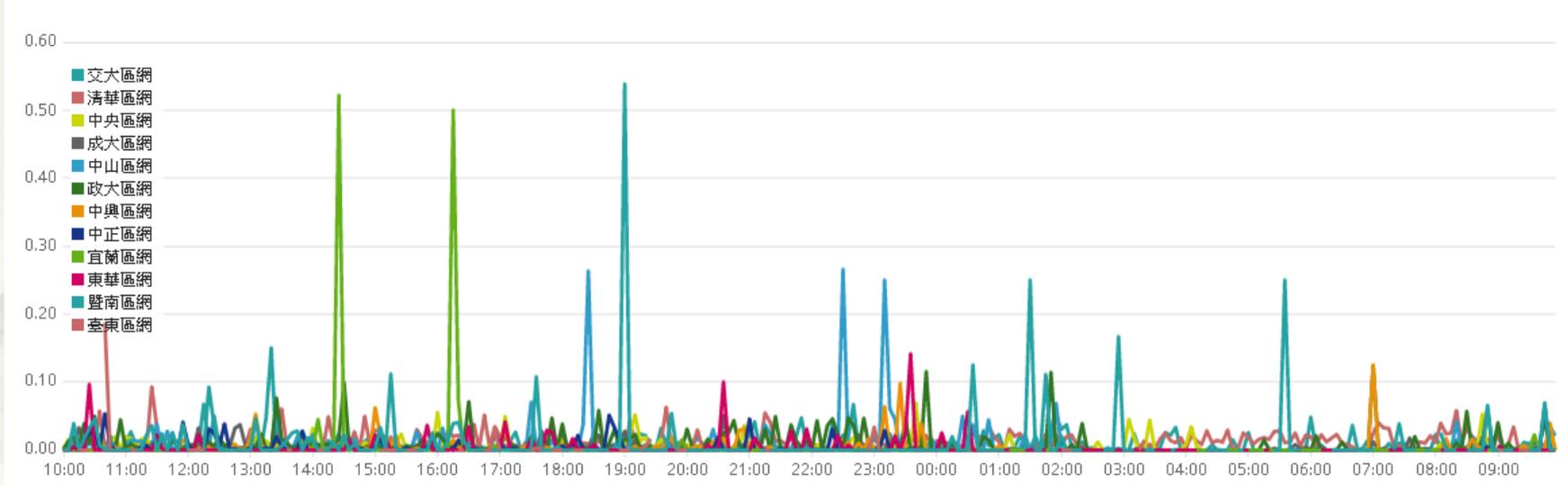
```
C:\Windows\System32>ping www.nchu.edu.tw -t

Ping www.nchu.edu.tw [140.120.1.20] <使用 32 位元組的資料>:
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=4ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=4ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52

140.120.1.20 的 Ping 統計資料:
    封包: 已傳送 = 14, 已收到 = 14, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 4ms, 最大值 = 5ms, 平均 = 4ms
```


Retransmit %比例 24 Hrs 統計 各區網中心

Timelion: Retransmit_Out % TANet



RTT、Packet Lost 分析

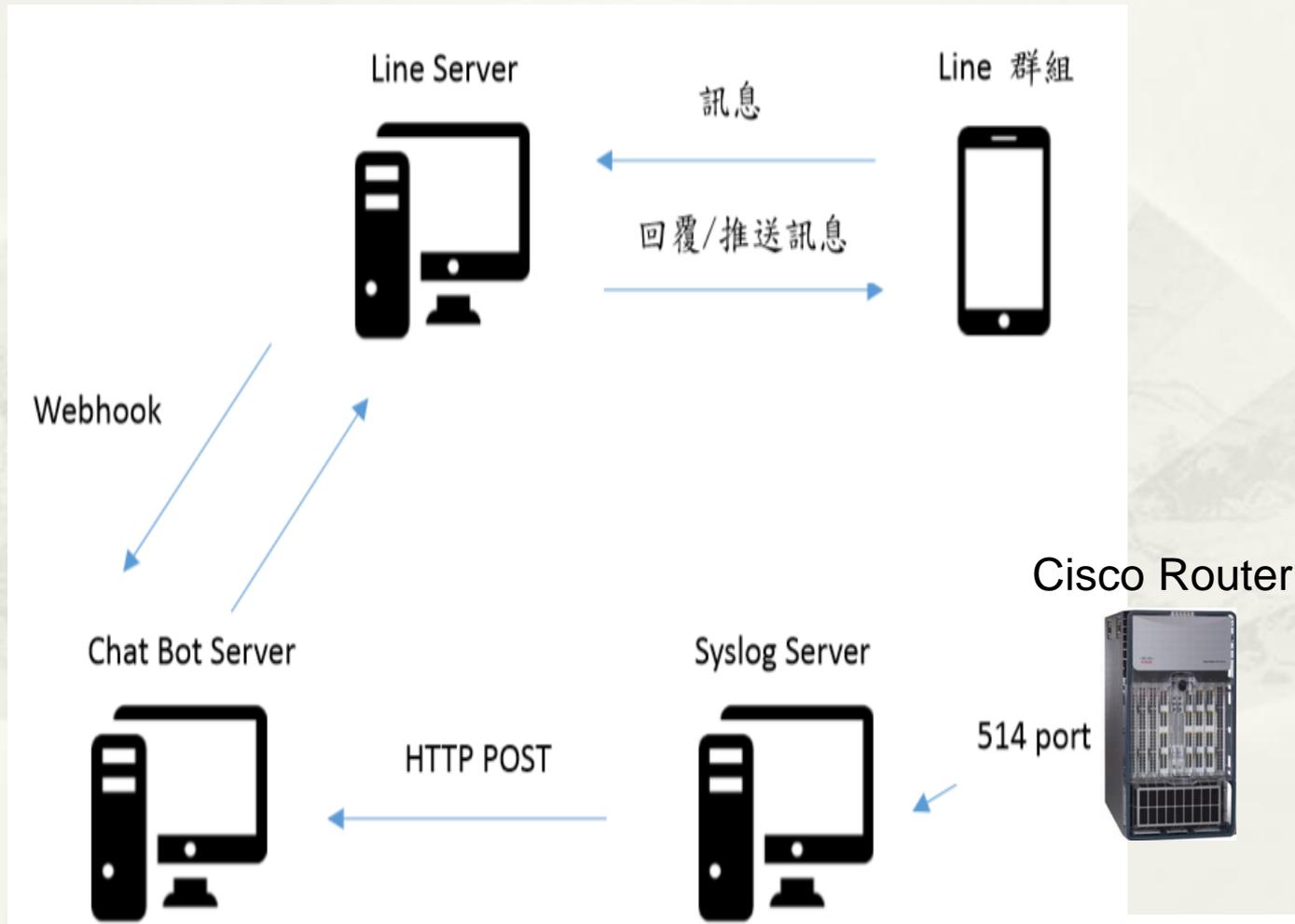
- * 影響 RTT 高低
 - * Inline 設備之有、無
 - * Inline 設備之 Loading 高、低
 - * 經過之 Node 節點數
 - * 網路設備 Loading
- * 影響 Packet Lost
 - * 頻寬壅塞
 - * 實體線路不良
 - * Inline 設備 Drop
 - * Server 異常
 - * 對方資安設備 Drop

4.2 LINE BOT 網路監控系統

Line Bot 網路監控系統

- * 即時訊息通知
 - * 接收網路設備 Syslog 並將異常及高風險事件通知於群組中。
- * 指令式 AI 對話
 - * 依據事先定義之指令，主動撈取相關網路監控圖表顯示於群組中。

Line Bot + Syslog Server 架構



Cisco Router Syslog Events

- * 線路異常
 - * LINK-3-UPDOWN
 - * LINEPROTO-5-UPDOWN
- * 路由協定異常
 - * OSPF-5-ADJCHG
 - * OSPFv3-5-ADJCHG -- ipv6
- * 帳號登入
 - * LOGIN_SUCCESS
 - * AUTHEN_SUCCESS – Cisco ASR
- * Config 指令修改
 - * logged command
 - * -CONFIG -- Cisco ASR

即時訊息通知

* 帳號登入 event



ntu_trial

Source - ip: 140.112.0.70: message: RP/0/RP0/CPU0:Jun 19 16:48:57.166 : exec[65592]:
%SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'ntuadmin1' from
'192.168.214.133' on 'vty0'

4:48 PM

* 線路異常 event



ntu_trial

Source - ip: 140.112.0.70: message: LC/0/9/CPU0:Jun 19 17:03:21.937 :
ifmgr[216]: %PKT_INFRA-LINK-3-UPDOWN : Interface GigabitEthernet0/9/1/9,
changed state to Down

Source - ip: 140.112.0.70: message: LC/0/9/CPU0:Jun 19 17:03:21.937 :
ifmgr[216]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol on Interface
GigabitEthernet0/9/1/9, changed state to Down

Source - ip: 140.112.0.70: message: LC/0/9/CPU0:Jun 19 17:03:25.697 :
ifmgr[216]: %PKT_INFRA-LINK-3-UPDOWN : Interface GigabitEthernet0/9/1/9,
changed state to Up

Source - ip: 140.112.0.70: message: LC/0/9/CPU0:Jun 19 17:03:25.698 :
ifmgr[216]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol on Interface
GigabitEthernet0/9/1/9, changed state to Up

5:03 PM

指令式 AI 對話

* 可用 !MRTG <連線單位> 顯示流量圖及連結

The screenshot shows a chat interface with the following messages:

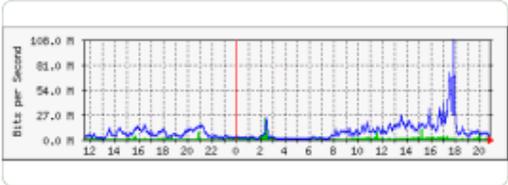
- ntu_trial** (8:29 PM): 可用指令表:
!help
!mrtg <部門>
- Jun 8(Fri)** (Date separator)
- Read 2** (4:46 PM) **!mrtg 女八舍**
- ntu_trial** (4:46 PM): [MRTG Traffic Graph for '女八舍']
The graph shows 'Bits per Second' on the y-axis (0.0 to 100.0) and time on the x-axis (8 to 16). It features a blue line for total traffic and a green line for download traffic. A red vertical line is present at approximately 22:00.
- ntu_trial** (4:46 PM): MRTG 詳細流量: <http://ws5.cc.ntu.edu.tw/cgi-bin/glance.pl?flow/dorm/f8>

指令式 AI 對話

劉冠宏
!mrtg 會計 8:54 PM

ntu_trial
是否在找:
文學院(會議室、研究大樓、中文系所)
社會系
管院計中
會計系所 8:54 PM

劉冠宏
!mrtg 會計系所 8:54 PM

ntu_trial
 8:54 PM
Download | Forward | Timeline | Keep

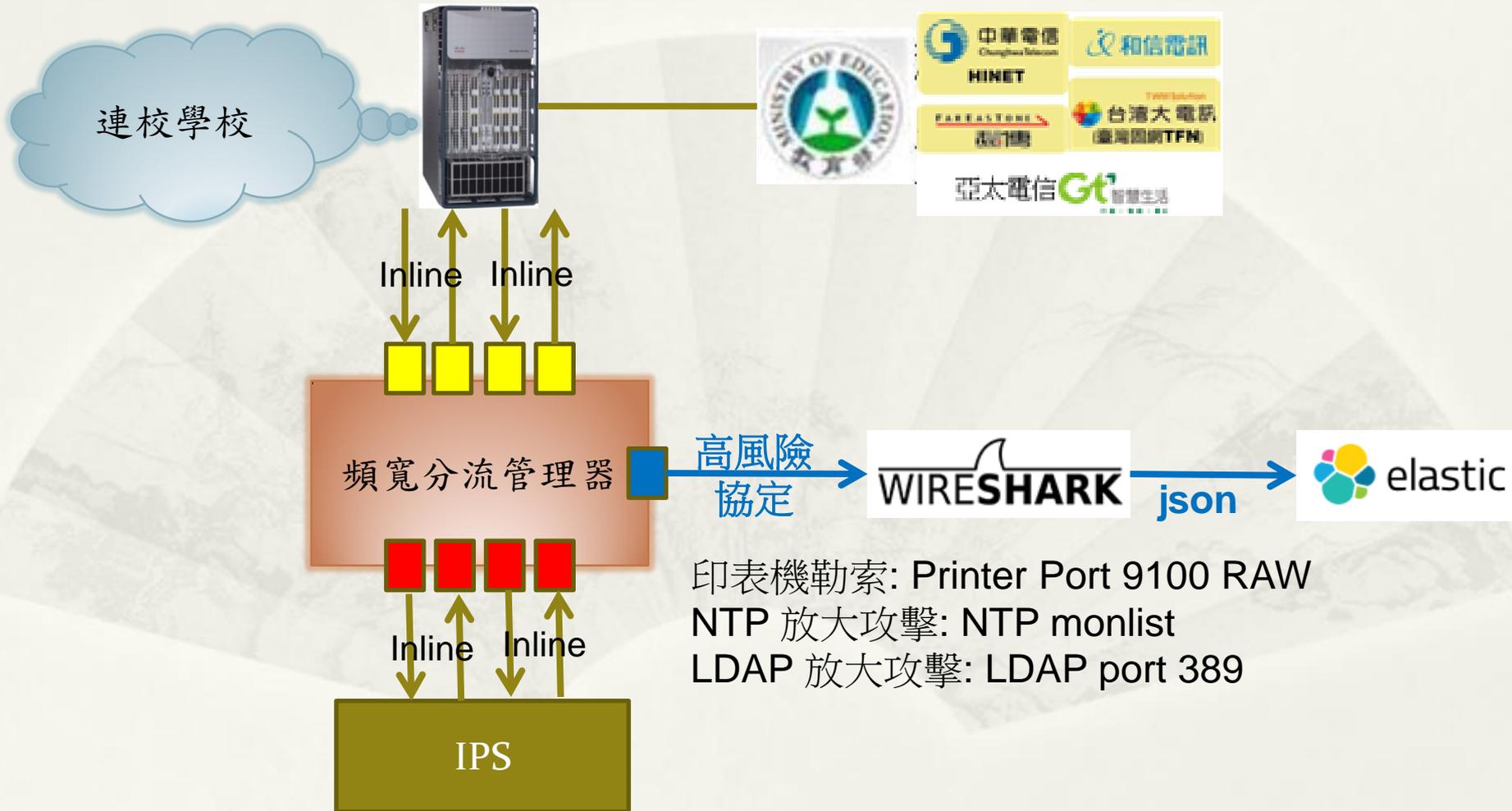
ntu_trial
MRTG 詳細流量: <http://ws5.cc.ntu.edu.tw/cgi-bin/glance.pl?flow/management/accounting> 8:54 PM

4.3 高風險協定分析

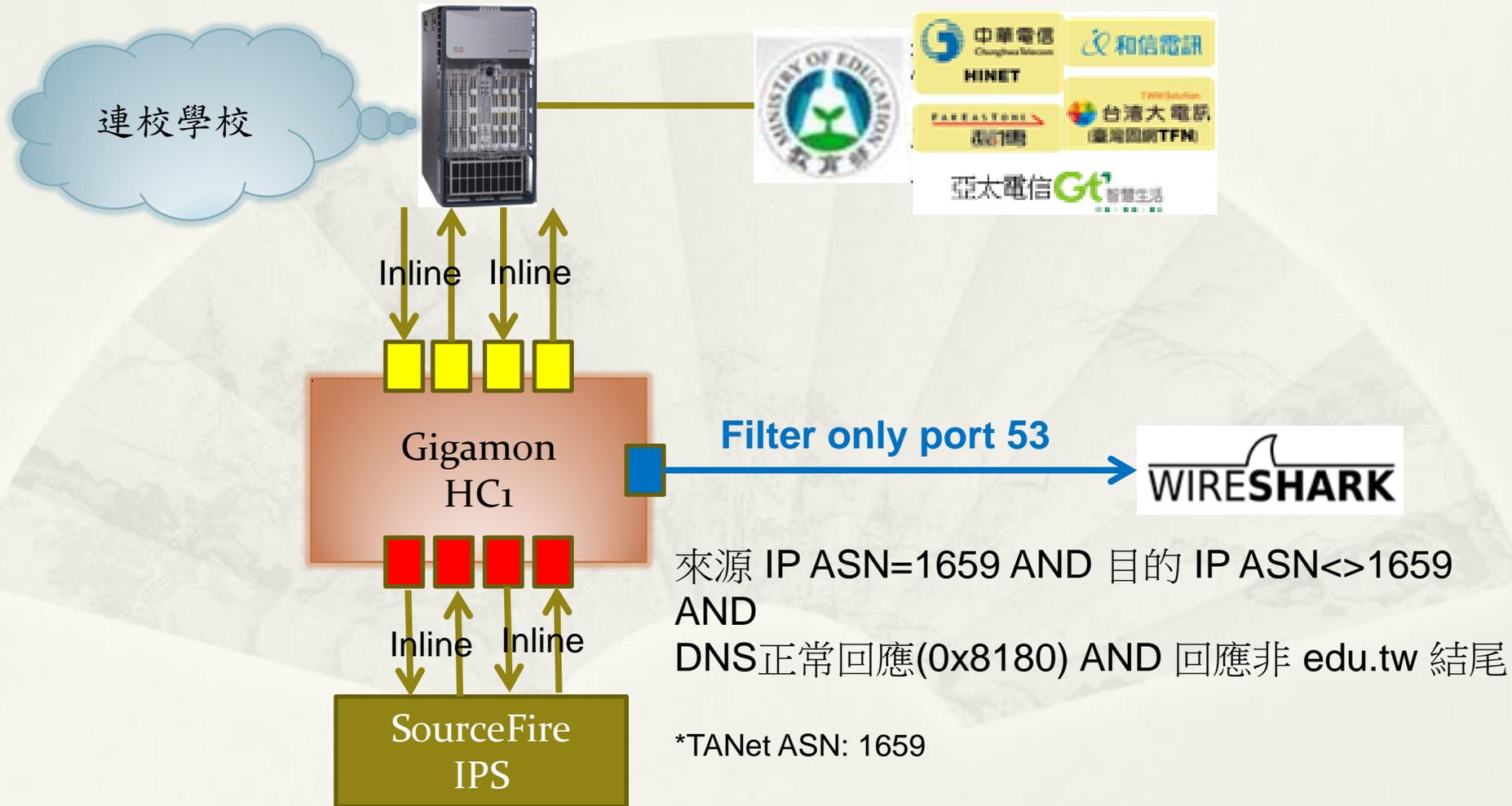
TANET2018論文

因應高速頻寬與加密流量之校園網路實驗與規劃

高風險協定偵測架構



Open Resolver DNS 偵測



高風險協定偵測

DDoS攻擊		
Port	用途	潛在風險
19	chargen	DDoS 攻擊
53	DNS	DNS 放大攻擊
123	NTP 校時	NTP monlist 放大攻擊
389	LDAP	LDAP 放大攻擊
1900	SSDP	SSDP 放大攻擊
11211	Memory Cache	Memory Cache 放大攻擊

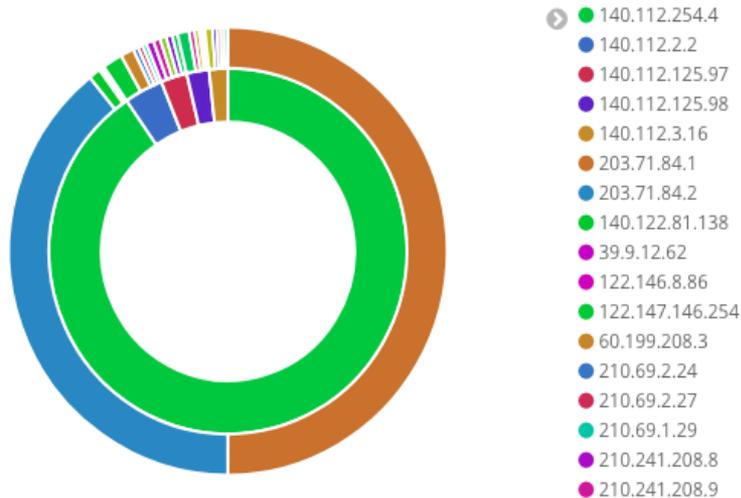
高風險協定偵測

不宜對 Internet 開放

Port	用途	潛在風險
445	網路芳鄰	WannaCry, Conficker
1433	MS sql Server	資訊洩漏
3306	Mysql Server	資訊洩漏
9100	Printer RAW	印表機勒索

Open DNS Resolver 調查

DNS open resolver server and client ip



DNS open resolver server ip

ip: Descending ↕	Count ↕
140.112.254.4	15,189
140.112.2.2	589
140.112.125.97	397
140.112.125.98	340
140.112.3.16	283
140.112.172.16	124
140.112.172.10	101
140.112.90.15	23
140.112.66.8	12

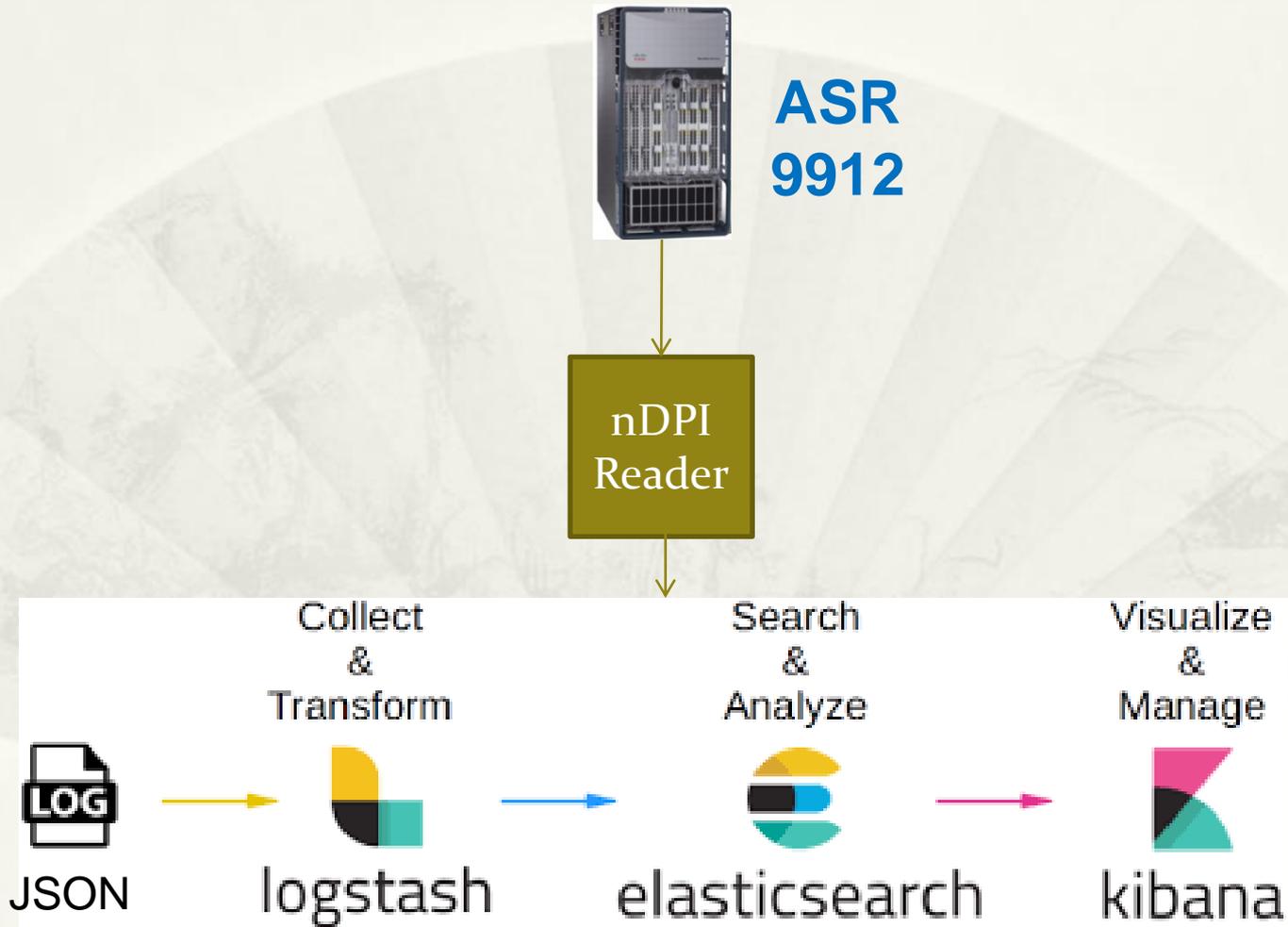
- * 無線 AP 分享器
 - * Ruckus 7372, D-Link DIR-513A
- * Windows 2008 R2 DNS 初始設定

4.4 Layer7 流量分析

nDPI

- * Open Source DPI Library
 - * <https://github.com/ntop/nDPI>
 - * 網路社群力量大
- * v2.3.0 Supported protocols 239+
 - * P2P (Skype, BitTorrent)
 - * Messaging (Viber, Whatsapp, MSN, The Facebook)
 - * Multimedia (YouTube, Last.fm, iTunes)
 - * Conferencing (Webex, CitrixOnline)
 - * Streaming (Zattoo, Icecast, Shoutcast, Netflix)
 - * Business (VNC, RDP, Citrix, *SQL)

Export JSON file to ELK Stack



臺大區網

網路品質管理 -> Layer7 流量分析

* <http://www.tp1rc.edu.tw/layer7.html>

Tag: Application_Name Bytes



106年評審委員建議:

第 8 點 研創成果呈現於區網中心網頁。

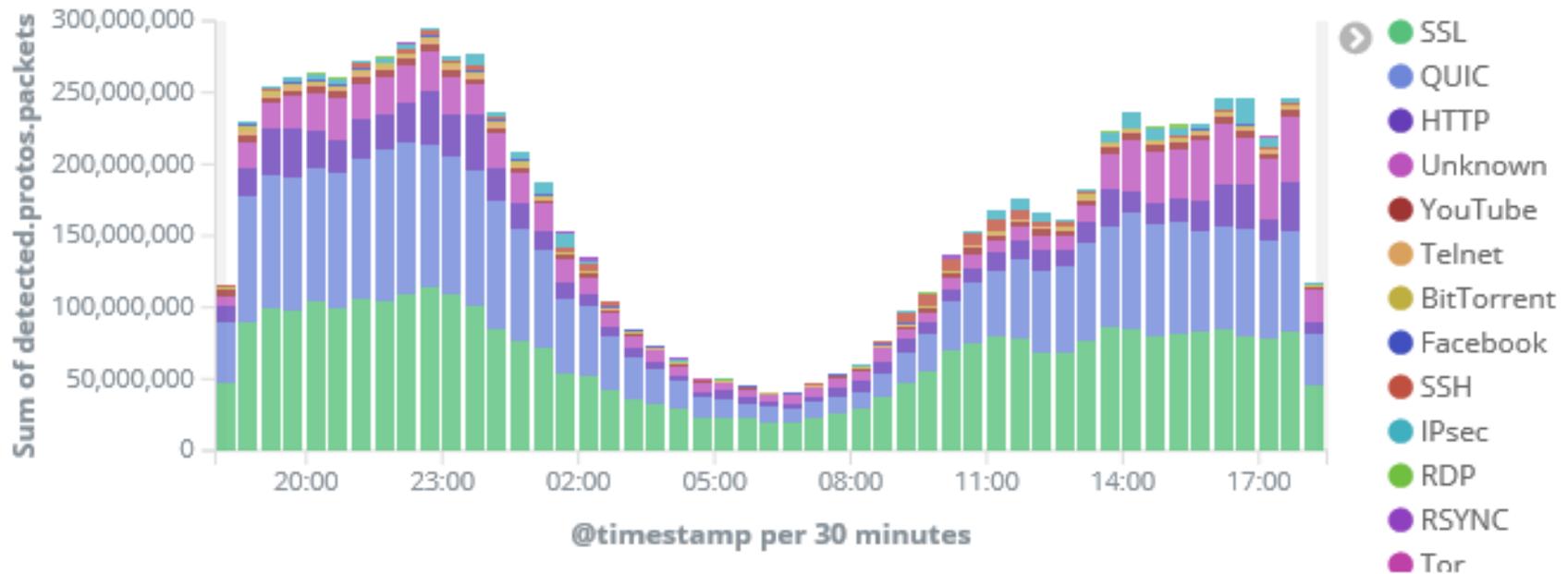
第 9 點 創新網路管理服務，呈現於區網中心網頁。

臺大區網

網路品質管理 -> Layer7 流量分析

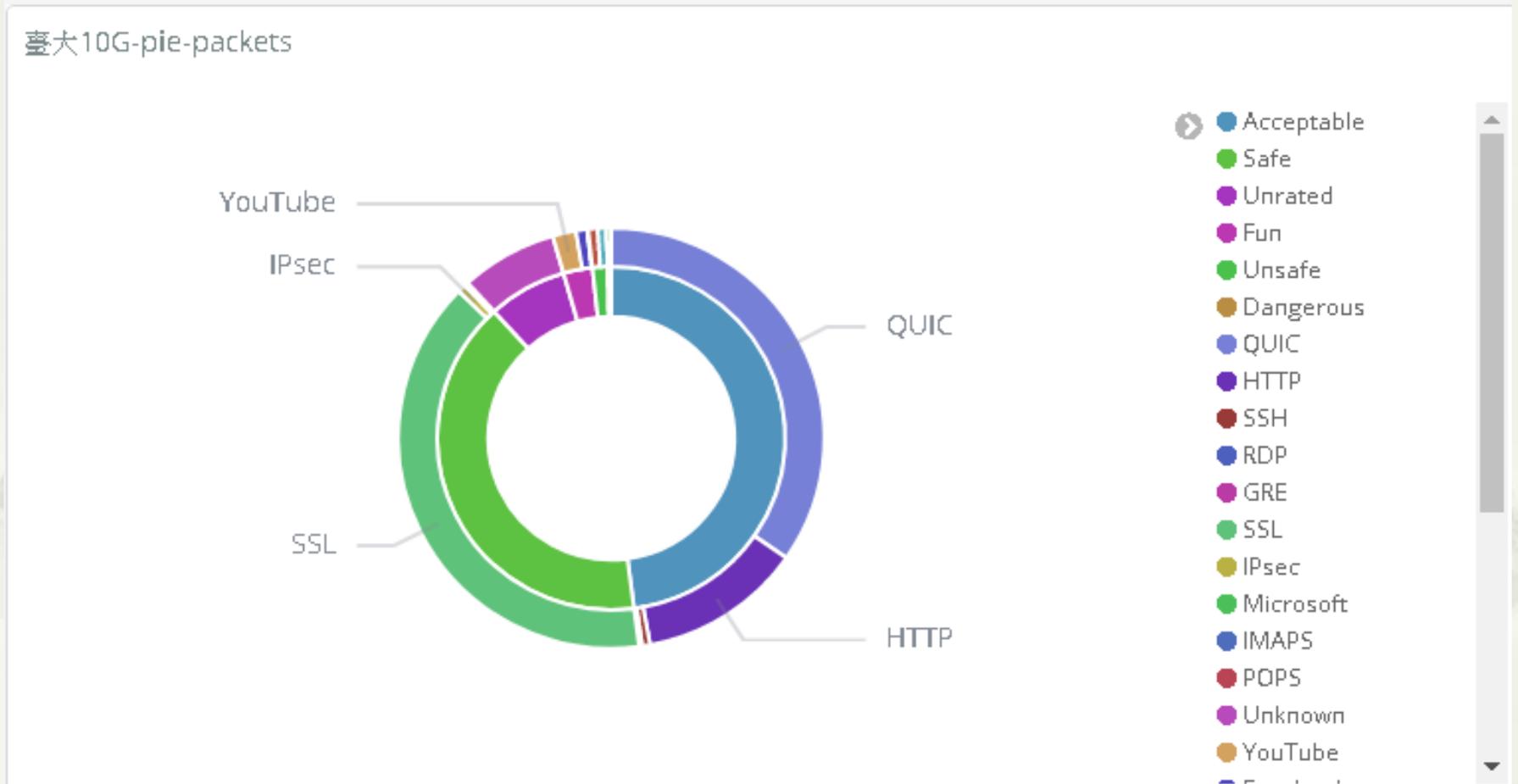
* <http://www.tp1rc.edu.tw/layer7.html>

臺大10G-bar-packets



臺大區網

網路品質管理 -> Layer7 流量分析



5. 未來目標與建議

* 未來目標與規劃

- * TCP-based 網路品質監控導入於區網骨幹

- * 加密流量分析

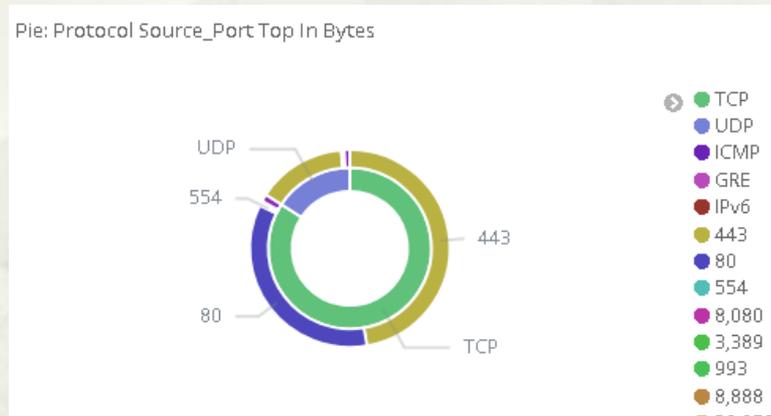
 - * 加解密設備 POC

 - * TANET2018 投稿論文

 - * 加密流量行為異常分析

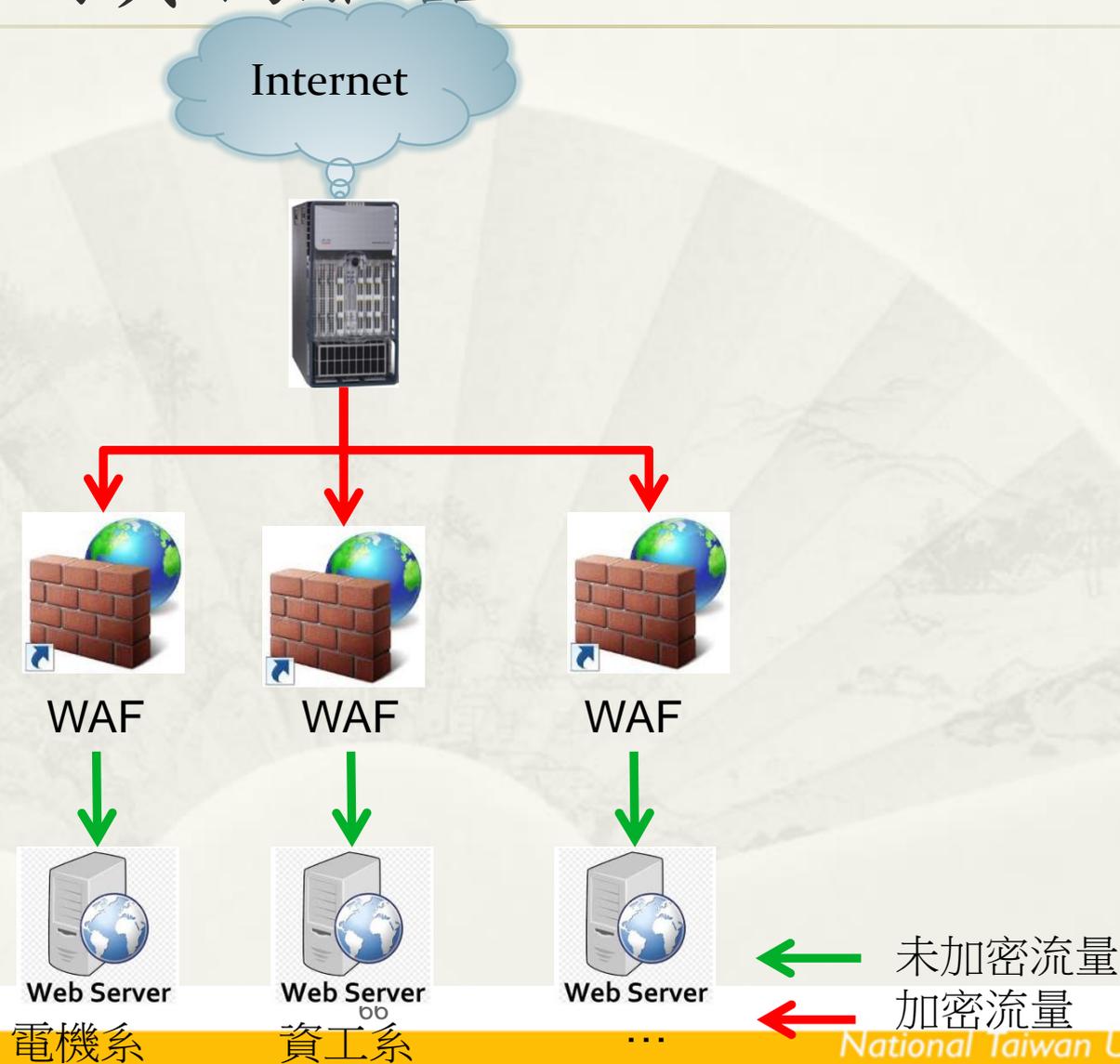
加密流量分析

- * 加密流量比例快速增加困難與解決方法
 - * 區網骨幹加密流量已達 50%

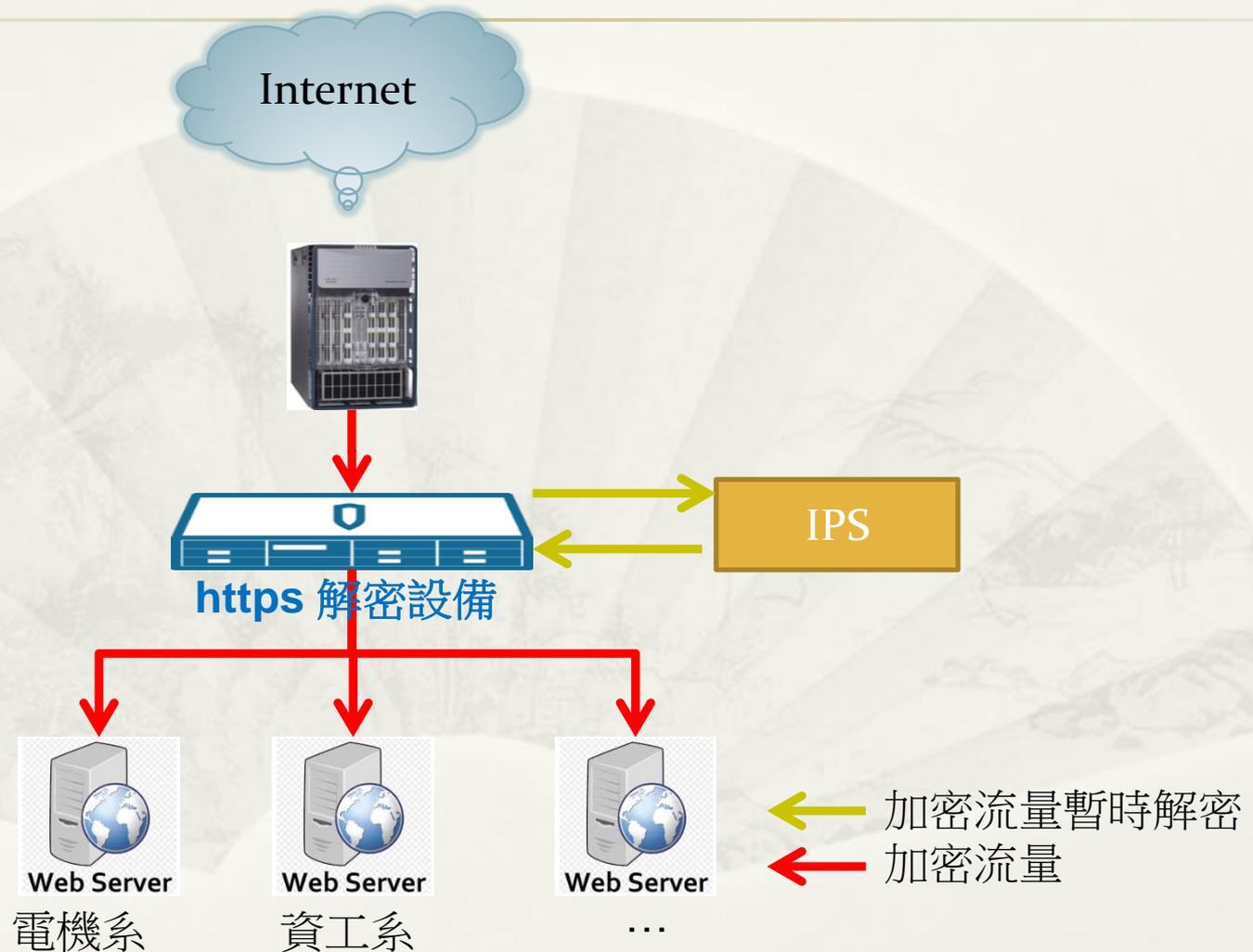


- * 加密流量無法辨識，原資安防護設備失效
 - * 解決方案
 - * 外對內防護 -> 解密設備 + 網頁憑證
 - * 內對外防護 -> 解密設備 + 根憑證安裝

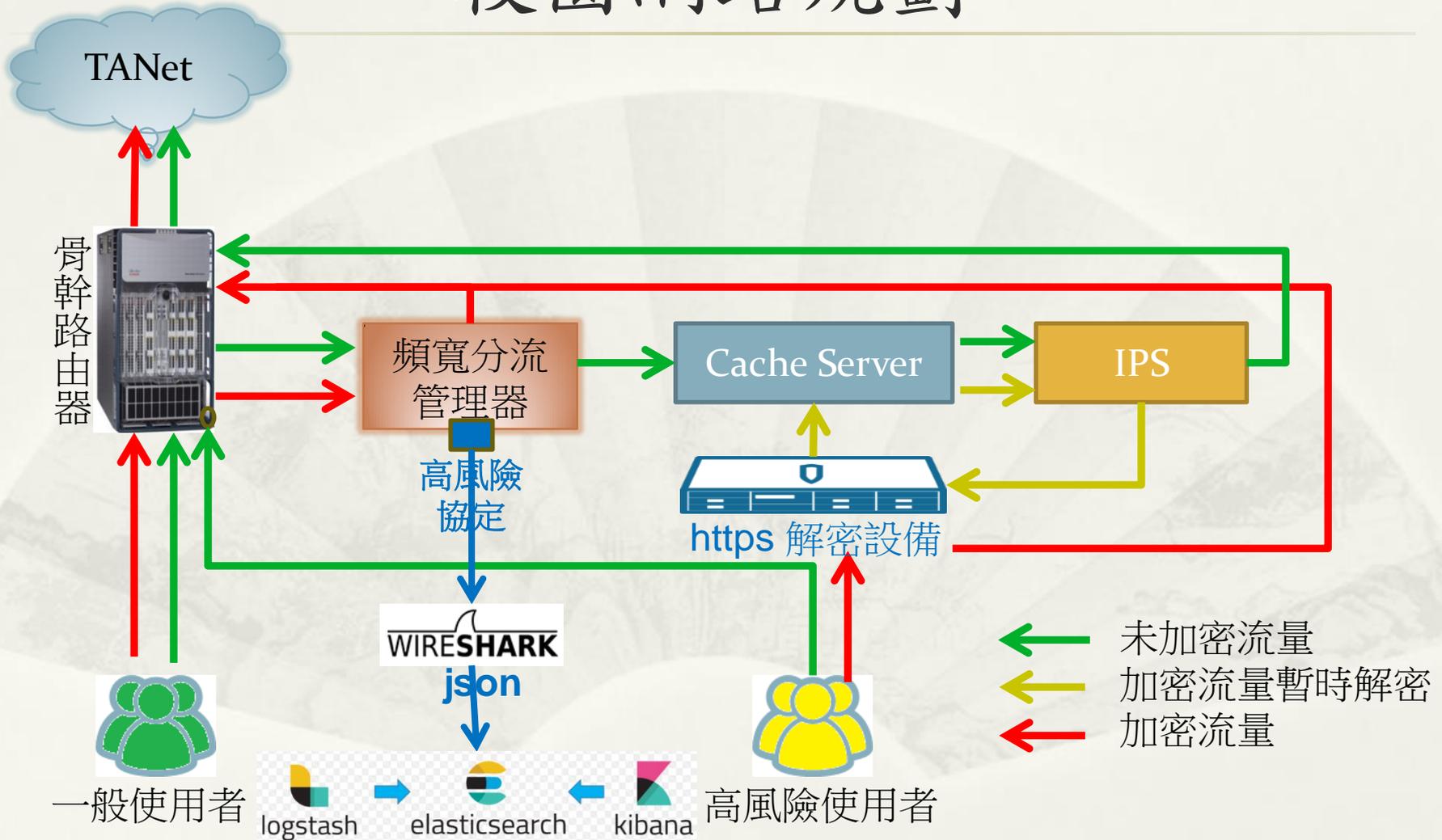
傳統外對內防護 網頁伺服器-WAF



網頁伺服器防護架構-解密設備



內對外防護 校園網路規劃



106年評審委員建議與回覆

委員建議	回覆
<p>1.資安事件處理之應變處理平均時數為2.7小時，事件處理平均時數為2.76小時，建議可逐步將其縮短至1小時內。同時來在教育部之資料有關資料，更新完整度為51.02%，建議可改善之。</p>	<p>資安事件應變與處理時數與去年比較皆有改善。 更新完整度也提高至73%。</p>
<p>2.11/16 凌晨區網斷線近3小時，雖可由台大之網路備援區網網頁達到公告訊息，此雖屬廠商施工不當所影響，但應思考爾後之應變措施，以使各連線單位之網路能順暢運作。</p>	<p>已建議區網連線臺北主節點與新竹主節點之 Dark Fiber 電路租用應由兩家不同 ISP 承包。</p>
<p>3.目前區網之網站網址為 http://www.ntu.tpirc.edu.tw/建議可調整為 http://www.tpirc.edu.tw/ 以使各區網網站之網址一致，便使用者使用。同時可思考從使用者角度之需要來提供相關資訊。</p>	<p>已將區網網址統一更改為 http://www.tpirc.edu.tw/</p>

106年評審委員建議與回覆

委員建議	回覆
4.請持續推動各連線單位升級DNS Server及校園網路導入IPv6/IPv4雙協定，以因應未來網路之發展。建議可了解其困難協助解決之。	已在2017年網管會議宣傳與說明IPv6雙協定之設定方法與路由設定。
5.資安事件處理時效較長，要精進不易，但仍請積極處理。	資安事件應變與處理時數與去年比較皆有改善。
6.工作量大又繁雜，所面對的事件經驗也最豐富，建議思考相關知識經驗該如何分享加值。	於區網會議上分享相關網管經驗與知識，定期於TANET研討會發表相關研究論文。
7.建議將區網人力完整呈現於區網中心網頁。	已更新網頁相關資訊
8.建議將區網中心研創成果呈現於區網中心網頁。	已將Layer7 流量分析成果呈現於網頁中 http://www.tpirc.edu.tw/layer7.html

106年評審委員建議與回覆

委員建議	回覆
9.建議將區網中心提供之各式服務，包含創新網路管理服務，呈現於區網中心網頁。	在區網網頁之網路品質管理呈現創新網路管理服務： http://www.tpirc.edu.tw/b1.php
10.建議持續強化網路連線資訊透明化，如：網路流量、線路頻寬等，在不違反資訊安全原則考量下，呈現於區域網路中心網頁。	所有區網連線單位之頻寬使用狀況皆提供MRTG 或 Cacti 圖表呈現於網頁中 http://www.tpirc.edu.tw/mrtg/ http://www.tpirc.edu.tw/cacti.html
11.建議持續推動連線單位IPv6支援能力，並將結果呈現於區網中心網頁。	已在2017年網管會議宣傳與說明IPv6雙協定之設定方法與路由設定。
12.建議將區網中心辦理之教育訓練成果以數位影音方式留存，以利資訊分享。	因教育訓練有部分課程為資安案例與攻防，部分資料敏感不便公開。預計先從網路管理或法規訓練等教育訓練開始著手。

其他建議

- * 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.tplrc.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



其他建議

- * 連線學校反應無法連線網站
 - * ntustbim.weebly.com
 - * u.camdemy.com
 - * slideplayer.com
 - * knowledge.exlibrisgroup.com
- * 回覆因該網站之前有侵權行為在台北主節點路由器進行 ACL 封鎖
- * 建議封鎖網址應公布於網站可供查詢



簡報完畢
謝謝