110年度執行成效報告

國立中山大學圖書與資訊處

處長：賴威光 教授

報告人：王聖全、曹仲杰

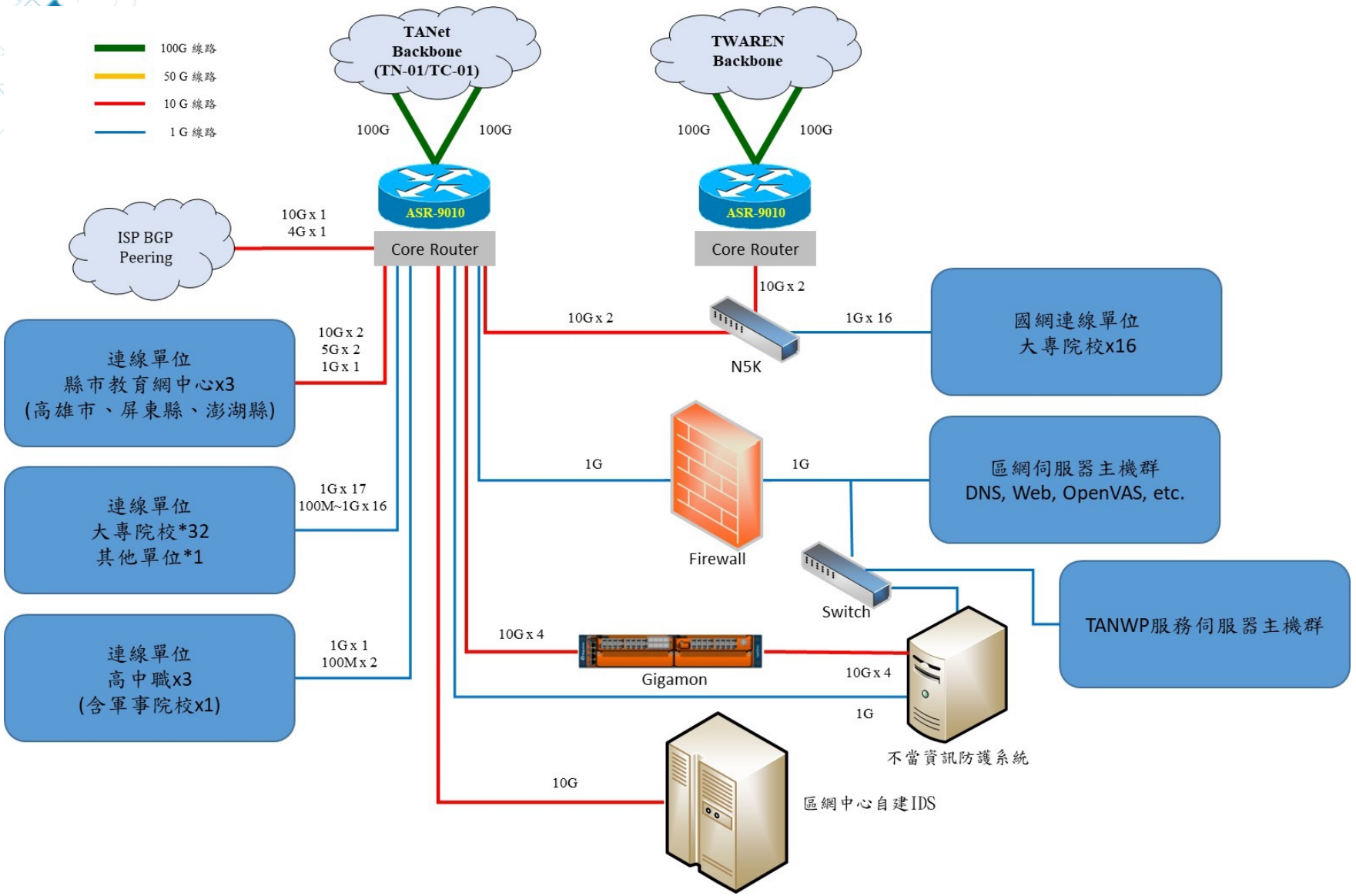
Agenda

- 網路中心基礎維運
- 網路及資安技術支援
- 創新特色服務
- 連線單位需求分析及滿意度調查
- 未來營運目標

網路中心基礎維運

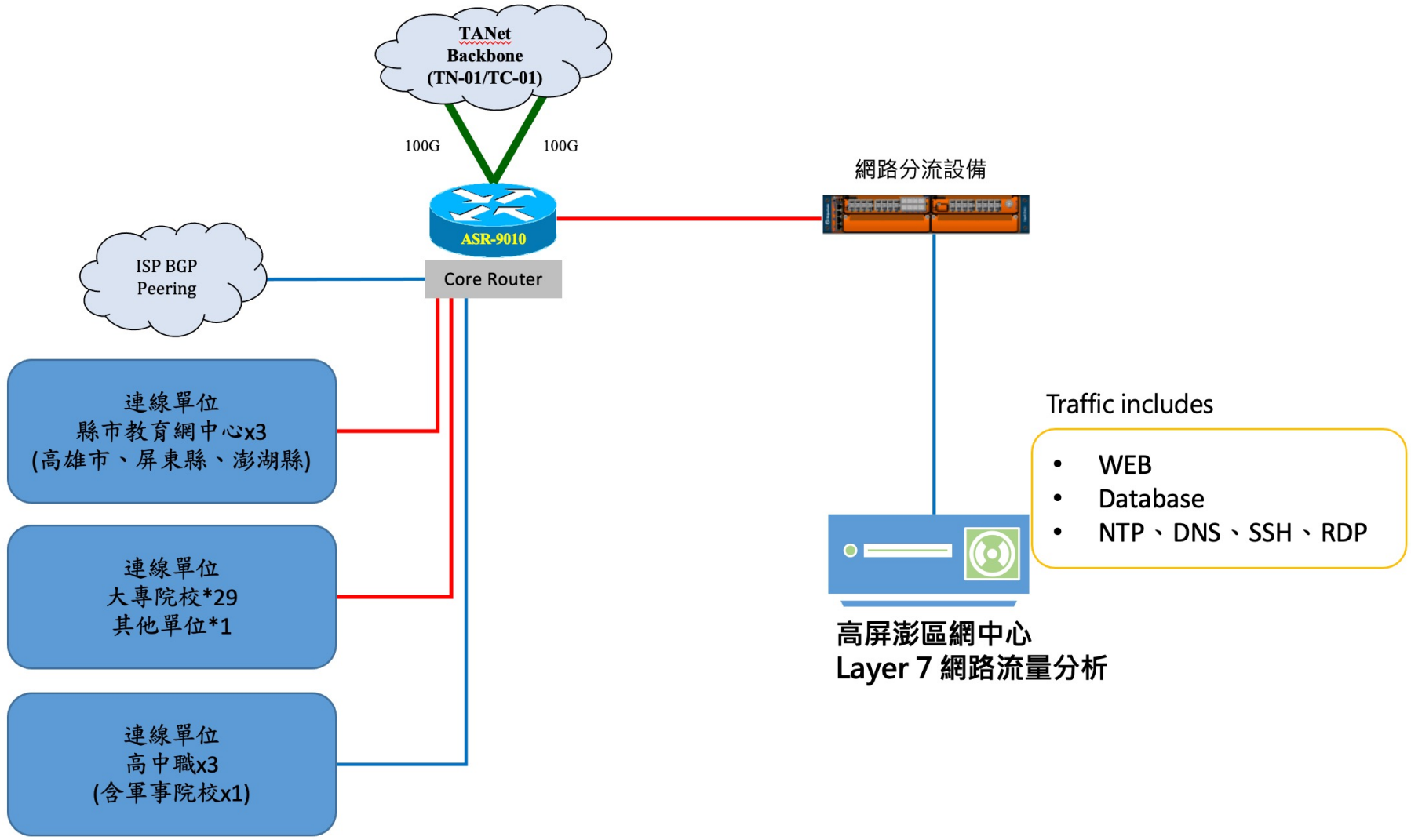
- 網路架構圖
- Layer 7網路流量分析系統
- 網路流量管理系統 (詳見高屏澎區網網站)
  - Cacti網管系統及weathermap plugin

高屏澎區網中心網路架構圖



Layer 7網路流量分析系統

Layer 7網路流量分析架構



連線單位異常流量分析

[Host 140.127.[redacted].94@101] Active Flows

SSH異常連線分析(來自國外的異常連線)

20 ▾ Hosts ▾ Status ▾ Severity ▾ Direction ▾ Applications ▾ Categories ▾ DSCP ▾ Host Pool

	Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes
	SSH	TCP	101	221.224.251.178 R :2123	140. 219.94 R :ssh	01:31	60	Client Server	0 bps	5.27 KB
	SSH	TCP	101	209.141.48.211 R :53028	140. 219.94 R :ssh	00:03	60	Client Server	0 bps	4.77 KB
	Unknown	TCP	101	193.163.125.91 R :58770	140. 219.94 R :25655	< 1 sec	110	Client Server	0 bps	122 Bytes
	SSH	TCP	101	193.112.27.122 R :49978	140. 219.94 R :ssh	< 1 sec	10	Client	0 bps	122 Bytes
	SSDP	UDP	101	157.230.58.45 R :24273	140. 219.94 R :32414	00:59		Client Server	4.20 kbit/s	407.8 KB
	Unknown	TCP	101	140. 219.94 R :51461	192.168.0.1 R :50963	00:09		Client	0 bps	234 Bytes
	MDNS	UDP	101	140. 219.94 R :mdns	73.142.79.211 R :80	21:20		Client Server	570.30 bit/s	106.56 KB
	Unknown	TCP	101	140. 219.94 R :32992	192.168.0.1 R :50963	00:09		Client	0 bps	234 Bytes
	Unknown	TCP	101	140. 219.94 R :57140	192.168.0.1 R :5431	00:09		Client	0 bps	234 Bytes
	Unknown	TCP	101	140. 219.94 R :57139	192.168.0.1 R :5431	00:09		Client	0 bps	234 Bytes
	Unknown	TCP	101	140. 219.94 R :58802	192.168.0.1 R :52151	00:09		Client	0 bps	234 Bytes
	SSH	TCP	101	140. 219.94 R :ssh	193.112.27.122 R :48440	00:51	60	Client Server	0 bps	6.22 KB

NTP流量觀察分析

NTP Active Flows　NTP流量分析

2.90 kbit/s | Total Bytes: 40 KB
0 bps | Total Throughput: 40.00 bit/s

20 ▾ Hosts ▾ Status ▾ Severity ▾ Direction ▾ Applications ▾ Categories ▾ DSCP ▾

	Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown
	NTP	UDP	101	213.152.187.3 R :35393	120. .136 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :58437	120. .90 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :58809	120. 3.67 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :52293	120. .174 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :37337	163. 35.86 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :49834	120. 25.217 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :48436	120. 5.30 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :49461	120. 3.233 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :38066	120. 7.15 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :34361	120. .163 R :ntp	< 1 sec		Client
	NTP	UDP	101	213.152.187.3 R :37176	120. .159 R :ntp	< 1 sec		Client

NTP DDoS分析 (1/3)

Active Flows [Host 140.[redacted].198@101]

100 Hosts Status Severity Direction Applications Categories IP Version Protocol VLAN

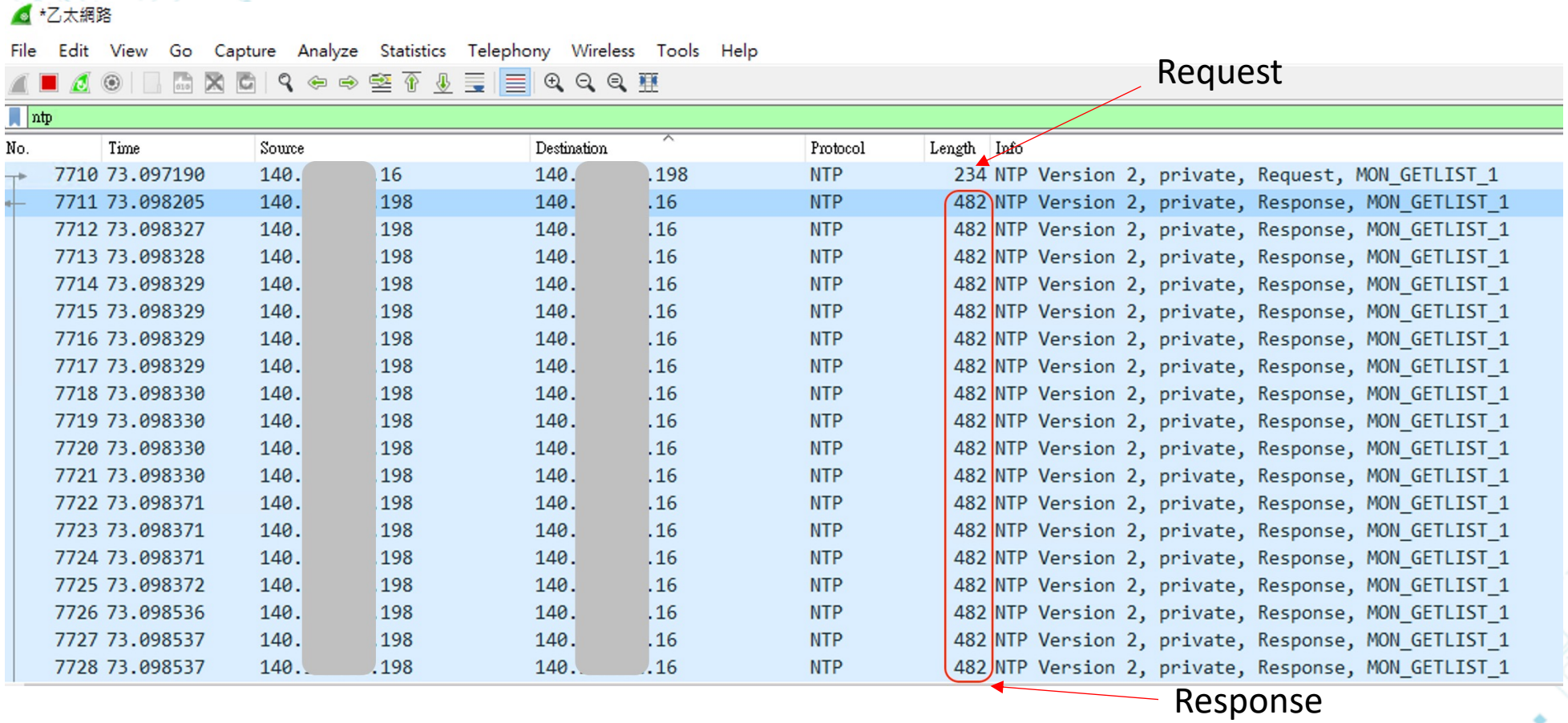
	Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
	NTP	UDP	101	69.174.140.59 :3074	140.[redacted].198 :ntp	17:15	10	Server	12.20 Mbit/s ↓	1.75 GB ↑	
	NTP.Cloudflare	UDP	101	172.67.217.27 :8443	140.[redacted].198 :ntp	04:04	10	Server	126.70 kbit/s —	716.94 MB —	
	NTP.Cloudflare	UDP	101	172.67.199.67 :8443	140.[redacted].198 :ntp	01:40	10	Server	1.40 Mbit/s —	186.66 MB —	
	NTP	UDP	101	124.142.16.72 :443	140.[redacted].198 :ntp	01:02	10	Server	26.40 Mbit/s —	230.08 MB —	
	NTP	UDP	101	16.162.13.137 :80	140.[redacted].198 :ntp	06:34	35	Client	17.00 kbit/s —	931.11 KB —	
	NTP	UDP	101	16.162.1.235 :80	140.[redacted].198 :ntp	06:40	35	Client	14.40 kbit/s —	728.5 KB —	
	NTP.Cloudflare	UDP	101	104.21.192.120 :8443	140.[redacted].198 :ntp	03:59	25	Client	3.30 kbit/s —	505.14 KB —	
	NTP	UDP	101	18.166.200.130 :80	140.[redacted].198 :ntp	06:42	40	Client	19.50 kbit/s —	1.14 MB —	
	NTP	UDP	101	116.203.186.178 :36083	140.[redacted].198 :ntp	02:42	10	Server	6.50 kbit/s —	190.08 KB —	

NTP DDoS分析 (2/3)

查看Server本身現有連線，連線數異常變高

remote address	port	local address	count	m	ver	rstr	avgint	lstint
163.28.129.228	37006	140.[redacted]198	6	7	2	0	22	0
45.200.9.137	13570	140.[redacted]198	123266	7	2	0	0	0
18.162.172.41	80	140.[redacted]198	192428	7	2	0	0	0
103.96.83.194	80	140.[redacted]198	104994	7	2	0	0	0
18.166.216.137	80	140.[redacted]198	203256	7	2	0	0	0
161.202.48.227	37015	140.[redacted]198	2007	7	2	0	0	0
69.174.140.59	3074	140.[redacted]198	275956	7	2	0	0	0
116.203.186.178	37148	140.[redacted]198	1376138	7	2	0	0	0
18.166.200.130	80	140.[redacted]198	219402	7	2	0	0	0
104.21.24.53	8443	140.[redacted]198	157190	7	2	0	0	0
18.162.179.6	80	140.[redacted]198	232811	7	2	0	21	0
18.162.67.171	80	140.[redacted]198	173288	7	2	0	0	0
18.166.39.177	80	140.[redacted]198	137616	7	2	0	0	8
16.162.54.24	80	140.[redacted]198	154370	7	2	0	0	16
16.162.1.235	80	140.[redacted]198	234209	7	2	0	0	25
185.153.133.157	80	140.[redacted]198	4735	7	2	0	0	45
104.21.192.121	8443	140.[redacted]198	226339	7	2	0	0	83
172.67.217.27	8443	140.[redacted]198	230490	7	2	0	0	100
16.162.13.137	80	140.[redacted]198	208740	7	2	0	0	200
104.21.192.120	8443	140.[redacted]198	210379	7	2	0	0	234
124.142.16.72	443	140.[redacted]198	51513	7	2	0	0	241

NTP DDoS分析 (3/3)



No.	Time	Source	Destination	Protocol	Length	Info
7710	73.097190	140. 16	140. .198	NTP	234	NTP Version 2, private, Request, MON_GETLIST_1
7711	73.098205	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7712	73.098327	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7713	73.098328	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7714	73.098329	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7715	73.098329	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7716	73.098329	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7717	73.098329	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7718	73.098330	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7719	73.098330	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7720	73.098330	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7721	73.098330	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7722	73.098371	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7723	73.098371	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7724	73.098371	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7725	73.098372	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7726	73.098536	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7727	73.098537	140. 198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1
7728	73.098537	140. .198	140. .16	NTP	482	NTP Version 2, private, Response, MON_GETLIST_1

請求封包大小只有234bytes，回應封包可放大至482*100 bytes (可達200倍放大)

Redis資料庫流量觀察分析

Redis流量分析

Recently Active Redis Flows

100 ▾ Hosts ▾ Status ▾ Severity ▾ Direction ▾ Applications ▾ Categories ▾ IP Version ▾

	Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown	A
	Redis	TCP	101	1.15.54.136 :8442	140. [redacted] 214 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 0 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 9 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 89 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 24 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 61 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 88 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 63 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 65 :6379	< 1 sec		Client	
	Redis	TCP	101	5.254.56.242 :24140	140. [redacted] 23 :6379	< 1 sec		Client	

RDP遠端桌面流量觀察分析

RDP流量分析:來自大量的國外異常連線IP

Recently Active Flows [Host 140.[redacted].76@101]

100 Hosts Status Severity Direction Applications Categories IP Version

	Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown
	RDP	TCP	101	85.159.218.246 :57188	140.[redacted].76 :ms-wbt-server	00:04		Client Server
	RDP	TCP	101	175.125.93.120 :7323	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :20974	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :16608	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :57562	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :52646	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :48273	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :2955	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :34624	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :12240	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :43903	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :38986	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	175.125.93.120 :30257	140.[redacted].76 :ms-wbt-server	00:03		Client Server
	RDP	TCP	101	72.167.37.131 :60636	140.[redacted].76 :ms-wbt-server	00:02		Client Server

SNMP流量觀察分析

SNMP流量分析: Default string public

	SNMP	UDP	101	66.41.103.238 :3840	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :40192	140. .115 :snmp	00:01		Server
	SNMP	UDP	101	66.41.103.238 :15617	140. .115 :snmp	00:01		Server
	SNMP	UDP	101	66.41.103.238 :17409	140. .115 :snmp	00:01		Server
	SNMP	UDP	101	66.41.103.238 :20737	140. .115 :snmp	00:01		Server
	SNMP	UDP	101	66.41.103.238 :25089	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :49665	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :64513	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :26114	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :26626	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :44546	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :64258	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :13571	140. .115 :snmp	< 1 sec		Server
	SNMP	UDP	101	66.41.103.238 :50692	140. .115 :snmp	00:01		Server

Default string public 測試

```
g$ snmpwalk -c public 140. .115
SNMPv2-MIB::sysDescr.0 = STRING: ECS4210-28T
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.259.10.1.42.101
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (398024983) 46 days, 1:37:29.83
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 7
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (146) 0:00:01.46
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.3 = OID: IP-MIB::ipAddrEntry
SNMPv2-MIB::sysORID.4 = OID: IP-MIB::ipNetToMediaEntry
```

資安技術支援及服務

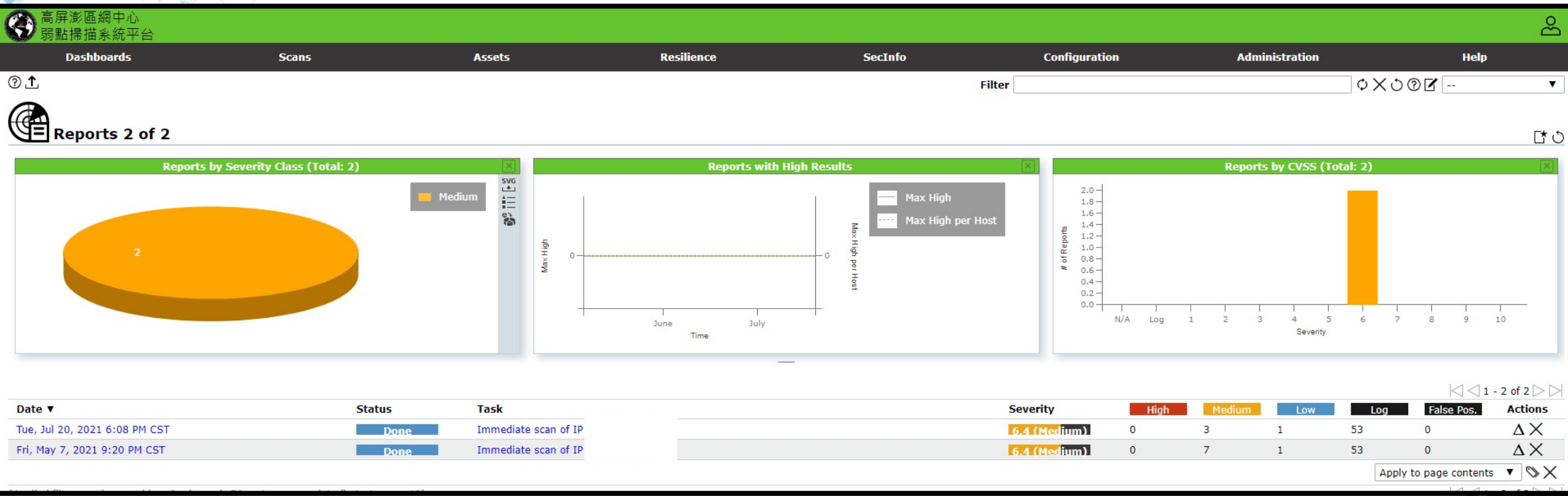
- 容器化主機弱點掃瞄工具
- DNS升級及資安健檢服務
- 資安通報事件處理時效
- 教育訓練辦理情形

連線單位資安技術支援

容器化弱點掃瞄工具OpenVAS11

- 取代過去外網掃描，掃描結果出現誤差。
- 採用分散佈建降低資安風險
- 彌補網站弱掃系統對伺服器弱點的不足。
- 由過去10版本引擎、提升為11版本引擎。
- 各單位自行建置後擁有帳號主控權。
- 容器化佈署，簡單及快速搭建，不受作業系統環境限制，核心系統環境由過去Ubuntu18.04提升為20.04，增加系統安全度。

主機弱點掃瞄工具主頁


高屏澎區網中心
弱點掃描系統平台
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Reports 2 of 2
Reports by Severity Class (Total: 2)
Medium
2
Reports with High Results
Max High
Max High per Host
Max High
Max High per Host
0
0
June
July
Time
Reports by CVSS (Total: 2)
# of Reports
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
N/A
Log
1
2
3
4
5
6
7
8
9
10
Severity
1 - 2 of 2
Date ▼
Status
Task
Severity
High
Medium
Low
Log
False Pos.
Actions
Tue, Jul 20, 2021 6:08 PM CST
Done
Immediate scan of IP
6.4 (Medium)
0
3
1
53
0
Fri, May 7, 2021 9:20 PM CST
Done
Immediate scan of IP
6.4 (Medium)
0
7
1
53
0
Apply to page contents

主機弱點掃瞄報告 (1/2)

Vulnerability	Severity	Location
CPE Inventory	0.0 (Log)	general/CPE-T
Hostname Determination Reporting	0.0 (Log)	general/tcp
CGI Scanning Consolidation	0.0 (Log)	80/tcp
Traceroute	0.0 (Log)	general/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	3389/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	3389/tcp
SSL/TLS: Report Medium Cipher Suites	0.0 (Log)	3389/tcp
SSL/TLS: Report Non Weak Cipher Suites	0.0 (Log)	3389/tcp
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites	0.0 (Log)	3389/tcp
SSL/TLS: Report Supported Cipher Suites	0.0 (Log)	3389/tcp
ICMP Timestamp Detection	0.0 (Log)	general/icmp
Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)	7.5 (High)	80/tcp
Apache Tomcat Privilege Escalation Vulnerability - Dec19 (Windows)	4.4 (Medium)	80/tcp
Apache Tomcat Session Fixation Vulnerability - Dec19 (Windows)	5.1 (Medium)	80/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80/tcp
Apache Tomcat Detection (Consolidation)	0.0 (Log)	general/tcp
jQuery Detection (HTTP)	0.0 (Log)	80/tcp
OS Detection Consolidation and Reporting	0.0 (Log)	general/tcp
HTTP Security Headers Detection	0.0 (Log)	80/tcp
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	135/tcp
Microsoft Remote Desktop Protocol Detection	0.0 (Log)	3389/tcp
DCE/RPC and MSRPC Services Enumeration	0.0 (Log)	135/tcp

主機弱點掃瞄報告 (2/2)

✓標的主機作業系統顯示

OS	Severity	Modified	Actions
	7.5 (High)	Mon, Jun 8, 2020 12:38 AM	
	10.0 (High)	Mon, Jun 8, 2020 12:45 AM	
	10.0 (High)	Mon, Jun 8, 2020 12:45 AM	
	10.0 (High)	Mon, Jun 8, 2020 1:20 AM	
	10.0 (High)	Mon, Jun 8, 2020 1:12 AM	
	10.0 (High)	Mon, Jun 8, 2020 12:45 AM	
	10.0 (High)	Mon, Jun 8, 2020 1:12 AM	
	5.0 (Medium)	Mon, Jun 8, 2020 12:45 AM	
	6.4 (Medium)	Wed, Apr 29, 2020 12:06 AM	
	4.8 (Medium)	Tue, Apr 28, 2020 5:15 PM	

DNS版本升級及資安健檢服務

- DNS Bind版本升級服務(9.10.4以上版本)
- DNS安全性設定服務及健檢
  - ACL設定
  - 限制來源查詢要求
  - Response Rate Limit (RRL)
  - Zone Transfer 限制
  - Minimal Any
  - Open DNS Resolver健檢
- 累積已協助九間連線單位夥伴完成升級及資安健檢服務
- 目前採用Layer 7流量分析系統，主動發現DNS潛在問題
- 服務申請網址：https://goo.gl/6PgWh4

資安通報事件處理時效

- 資安事件緊急通報處理之效率及通報率
  - **所屬之學校及單位1、2級資安事件處理**
    - 通報平均時間：0.06 小時
    - 應變處理平均時數：0.69 小時
    - 事件處理平均時數：1.41 小時
    - 通報完成率：100%
    - 事件完成率：100%
  - **所屬之學校及單位3、4級資安事件通報：無任何3、4級事件**
  - **資安事件通報審核平均時數：0.81 小時。**

22

教育訓練辦理情形

教育訓練辦理情形

時間	主題
4月29日	安全軟體發展生命週期(Secure Software Development Life Cycle)
7月16日	Keep Fighting！校園個資管理
7月30日	Keep Fighting！校園資安管理
11月4日	校園常見資安風險檢測與修補

創新特色服務

- 全國不當資訊防護系統
- 容器化網路裝置監控服務系統
- 2021 CCDS 全國大專校院資訊行政主管研討會

TANet青少年網路內容防護

防護計畫動機

- 強化臺灣學術網路的網路內容安全，保護學齡中使用者避免接觸不當資訊內容網站。

  依下列兩項法源作為防護原則：

  ➢**兒童及少年福利與權益保障法。**

  ➢**「臺灣學術網路(TANet)拒絕存取資訊之網站(頁)分類審議原則」。**

- 不當資訊內容之網站類型涵蓋類別：

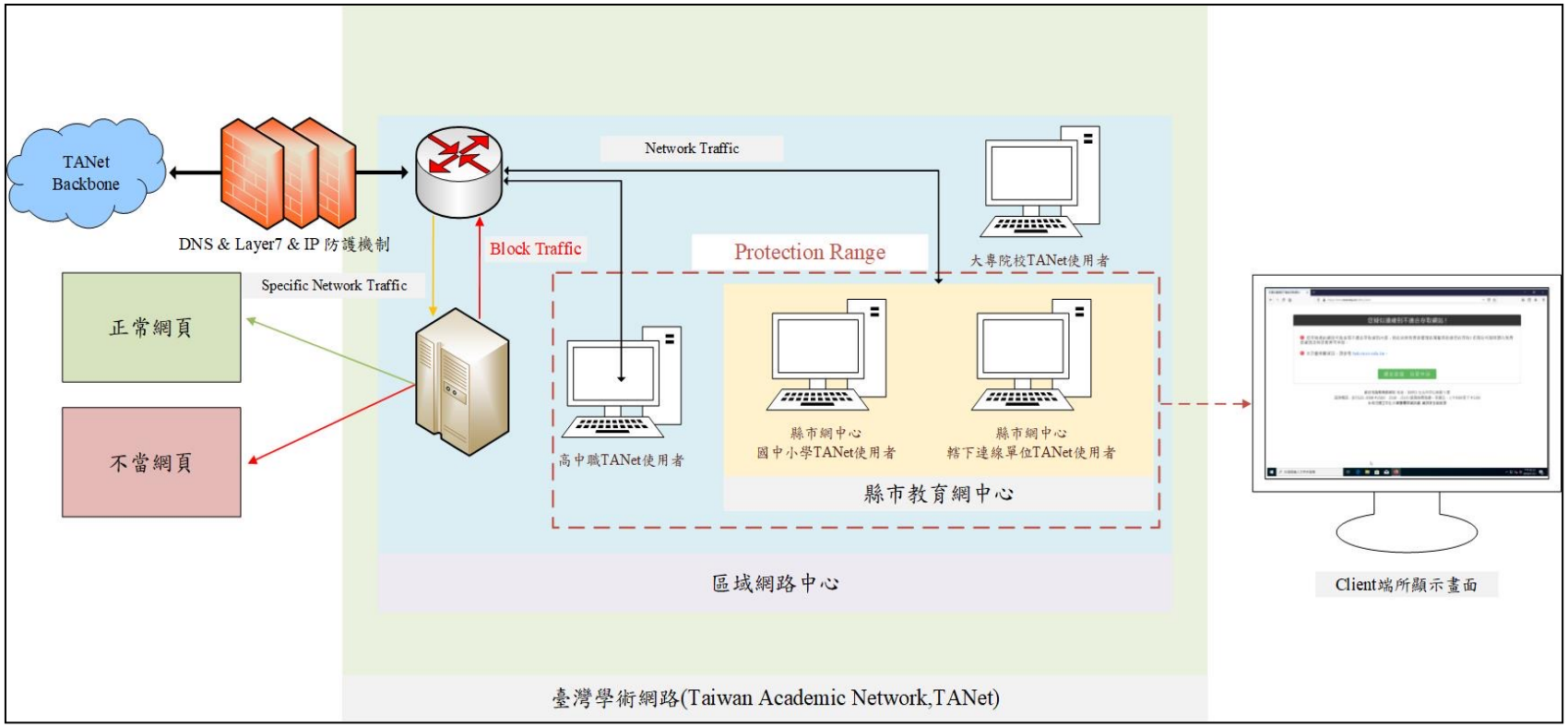
  ➢**110年度9月起五大類更新為六大類(色情、賭博、暴力恐怖、血腥、危險內容與其他有害行為)等。**

資料來源：http://twb.moe.edu.tw/index2.html

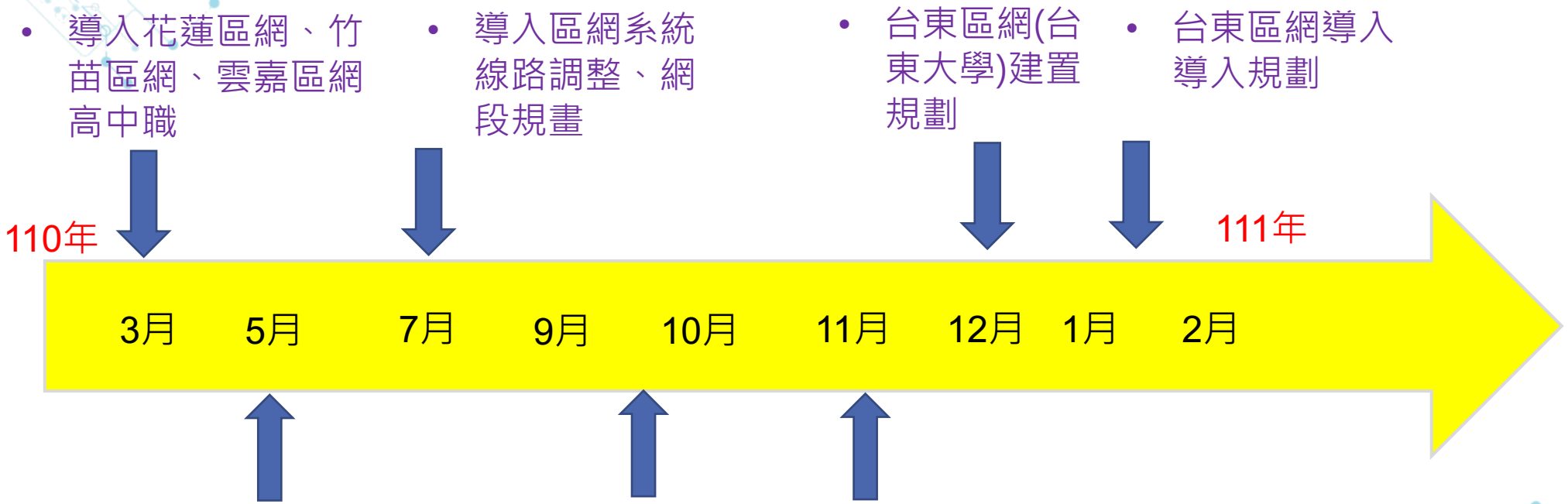
27

TANet青少年網路內容防護

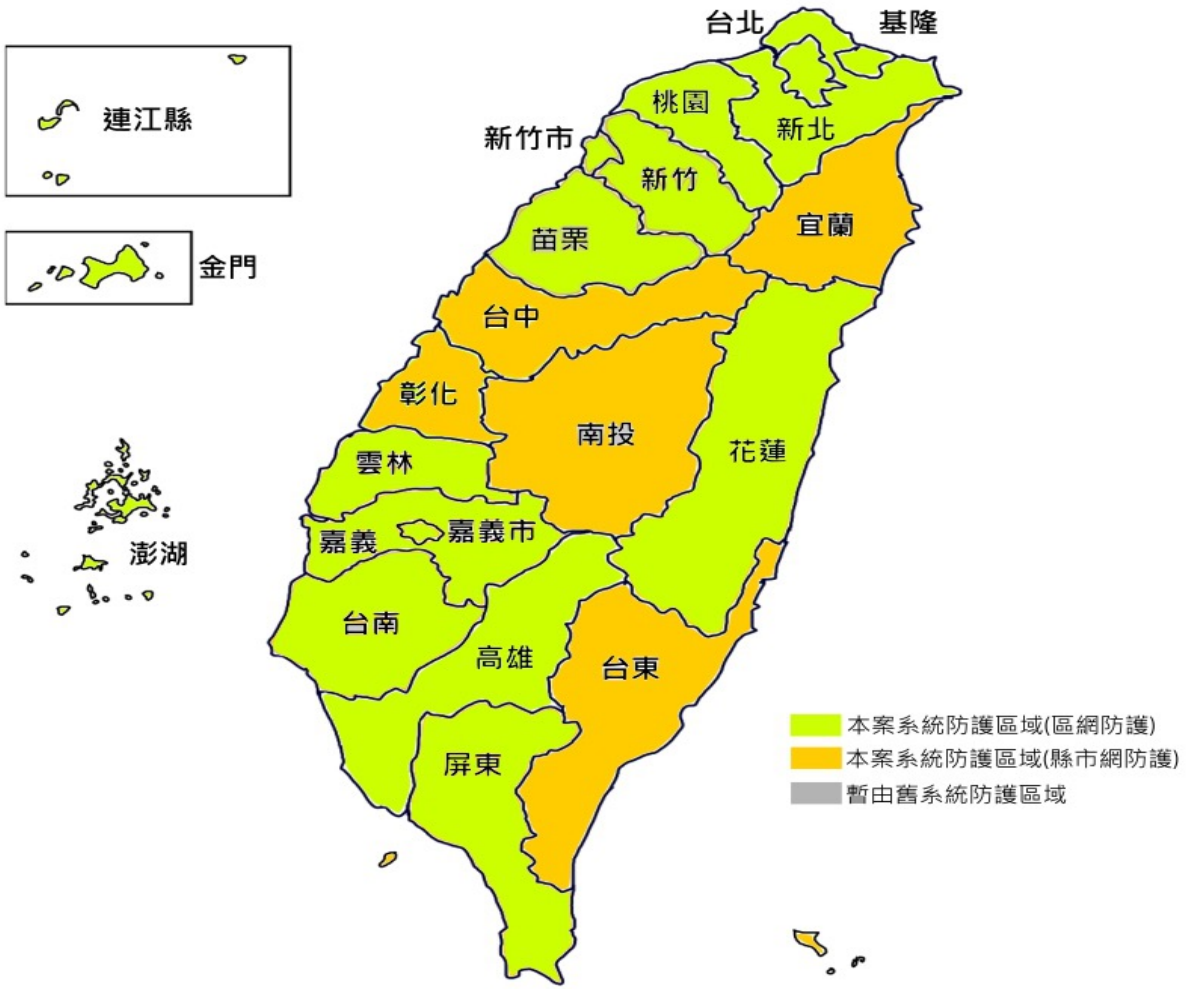
- 高屏澎區網中心自行開發
- 防護範圍含括全國各縣網中心之國中小學及各區網之高中職



TANet青少年網路內容防護計畫



TANet青少年網路內容防護地圖



建置年度	區網	縣市網中心	設備種類
107年度	高屏澎區網	高雄市	皆以新設備建置
		屏東縣	
		澎湖縣	
108年度	臺北第一區網	台北市	
	臺北第二區網	新北市	
		基隆市	
	桃園區網	桃園市	
		金門縣	
		連江縣	
	台南區網	台南市	
109年度	竹苗區網	新竹縣	
		新竹市	
		苗栗縣	
	雲嘉區網	雲林縣	
		嘉義縣	
		嘉義市	
	花蓮區網	花蓮縣	
預計110年度建置	台中區網	台中市	尚為縣市舊設備
		彰化縣	
	南投區網	南投縣	
	宜蘭區網	宜蘭縣	
	台東區網	台東縣	

防護計畫特色


不當資訊防護系統特色
監控及資料庫派送
監測各區網運行狀況，資料庫更新可互相回傳。
DNS、Layer7、IP阻擋技術
設置三層防護機制，提升防護效果，全面隔絕不當資訊。
模擬自動瀏覽測試工具
模擬使用者瀏覽網站的方式，測試黑白名單的阻擋情形。
TANWP
虛擬化電腦伺服器
模擬防護環境、實測各項服務系統。
自主獲取黑名單來源
透過AI圖像辨識資料蒐集、搜尋引擎爬蟲、使用者建議回饋管道、iWIN提供資料，獲取資料庫來源。
數據報表系統
提供各區瀏覽次數、阻擋次數、阻擋比率及不當網域排名等資訊。

31

TANet青少年網路內容防護 (1/2)

- 各區網中心已建置單位數

區網中心	縣市網中心	高中職	國中	國小	其他單位
台北第一區網中心	台北市	14	0	2	0
台北第二區網中心	新北市 基隆縣	19	0	1	2
桃園區網中心	桃園市 金門縣 連江縣	17	0	0	0
竹苗區網中心	新竹縣 新竹市 苗栗縣	8	0	0	0

TANet青少年網路內容防護 (2/2)

- 各區網中心已建置單位數

區網中心	縣市網中心	高中職	國中	國小	其他單位
雲嘉區網中心	雲林縣 嘉義縣 嘉義市	8	0	0	0
台南區網中心	台南市	43	0	0	2
高屏澎區網中心	高雄市 屏東市 澎湖縣	3	0	0	0
花蓮區網中心	花蓮縣	10	0	0	1
台中區網中心	台中市 彰化縣	17	0	0	0

110年1至9月防護成效統計表 (1/4)

區域	縣市	110年1月至9月		
		總瀏覽次數	總阻擋次數	阻擋比率
台北第一區網	台北市網	42,981,660,747	46,821,044	0.11%
	台北第一區網高中職	1,891,994,525	90,848	0.00%
	台北第一區網全部	44,873,655,272	46,911,892	0.10%
台北第二區網	新北市網	25,793,033,624	4,248,094	0.02%
	基隆市網	3,660,439,038	117,627	0.00%
	台北第二區網高中職	874,825,187	115,358	0.01%
	台北第二區網全部	30,328,297,849	4,481,079	0.01%
桃園區網	桃園市網	17,467,421,783	53,544,381	0.31%
	金門縣網	2,772,268,810	68,546	0.00%
	連江縣網	775,703,520	24,808	0.00%
	桃園區網高中職	2,240,481,068	2,043,668	0.09%
	桃園區網全部	23,255,875,181	55,681,403	0.24%

110年防護成效統計表 (2/4)

區域	縣市	110年1月至9月		
		總瀏覽次數	總阻擋次數	阻擋比率
竹苗區網	新竹縣網	6,141,874,998	23,762,093	0.39%
	新竹市網	7,991,539,132	444,156	0.01%
	苗栗縣網	8,314,742,094	916,221	0.01%
	竹苗區網高中職	1,112,164,553	82,221	0.01%
	竹苗區網全部	23,560,320,777	25,204,691	0.11%
雲嘉區網	雲林縣網	14,888,508,450	3,868,100	0.03%
	嘉義縣網	3,639,583,601	242,405	0.01%
	嘉義市網	4,218,030,072	1,618,222	0.04%
	雲嘉區網高中職	546,632,329	49,860	0.01%
	雲嘉區網全部	23,292,754,452	5,778,587	0.02%

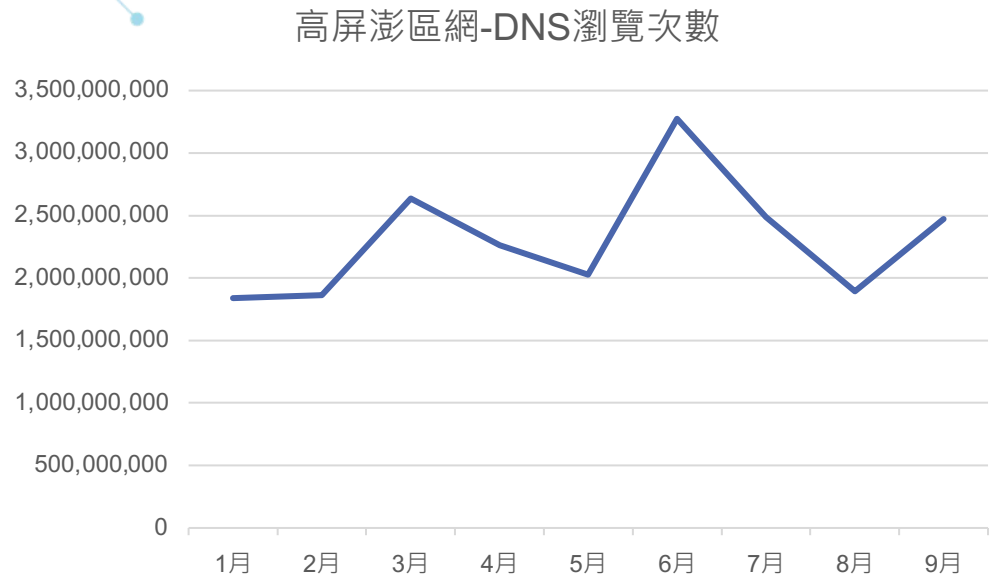
110年防護成效統計表 (3/4)

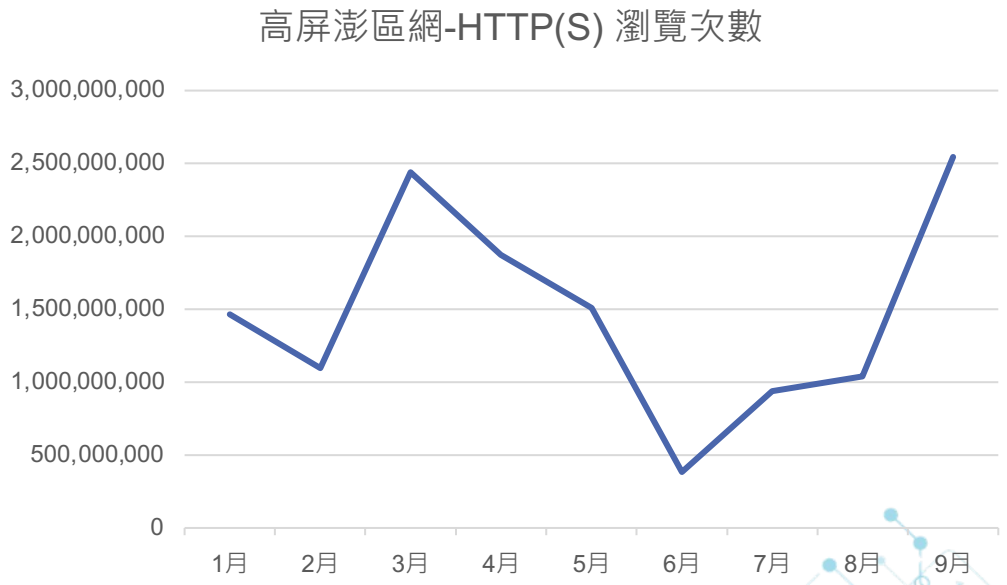
區域	縣市	110年1月至9月		
		總瀏覽次數	總阻擋次數	阻擋比率
台南區網	台南市網	14,102,137,395	7,434,900	0.05%
	台南區網高中職	3,602,666,273	5,217,291	0.14%
	台南區網全部	17,704,803,668	12,652,191	0.07%
高屏澎區網	高雄市網	21,876,495,138	4,998,426	0.02%
	屏東縣網	9,079,463,174	25,346,830	0.28%
	澎湖縣網	4,430,045,809	212,177	0.00%
	高屏澎區網高中職	204,417,095	1,738,727	0.85%
	高屏澎區網全部	35,590,421,216	32,296,160	0.09%
花蓮區網	花蓮縣網	3,338,656,265	359,083	0.01%
	花蓮區網高中職	496,845,010	67,010	0.01%
	花蓮區網全部	3,835,501,275	426,093	0.01%

110年防護成效統計表 (4/4)

區域	縣市	110年1月至9月		
		總瀏覽次數	總阻擋次數	阻擋比率
其它完成新舊系統轉換之縣市網	臺中市網	25,664,487,915	108,244,838	0.42%
	彰化縣網	16,174,277,341	24,787,950	0.15%
	南投縣網	7,997,151,272	2,767,964	0.03%
	宜蘭縣網	9,061,349,922	898,696	0.01%
	臺東縣網	7,117,935,010	276,774	0.00%

110年1至9月高屏澎區網防護成效



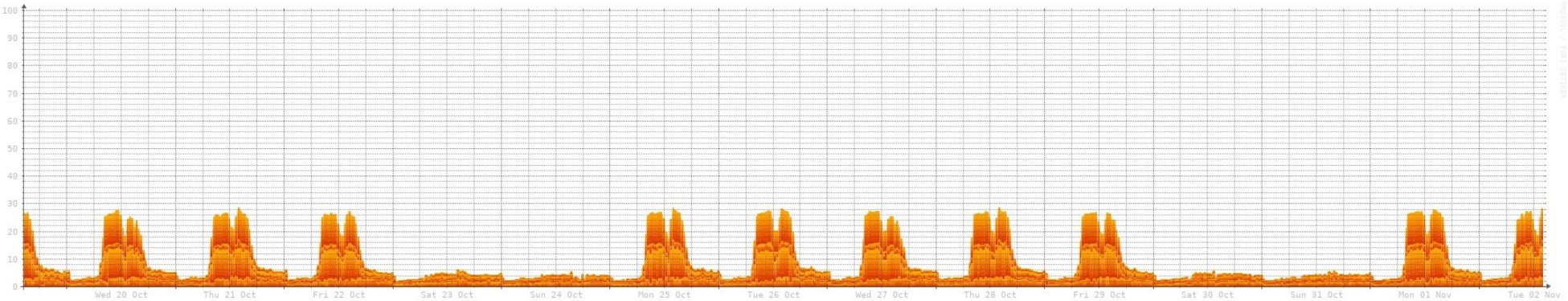


全國各區網中心-防護系統線上狀況

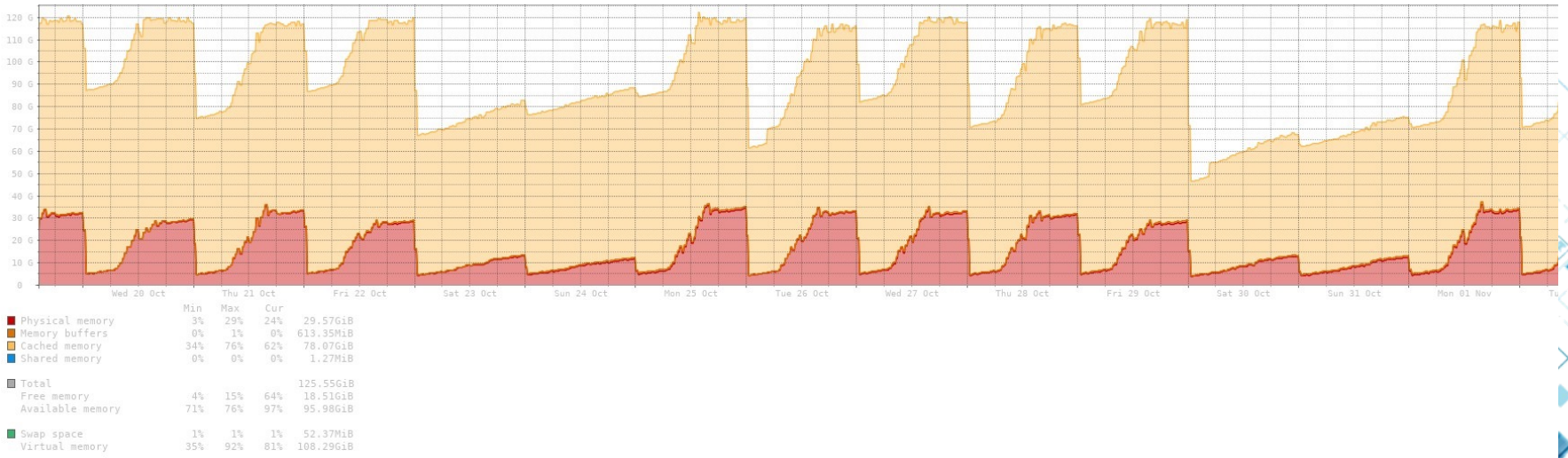
39

高屏澎區網中心-防護伺服器硬體狀況 (110/10/19-110/11/2)

CPU使用



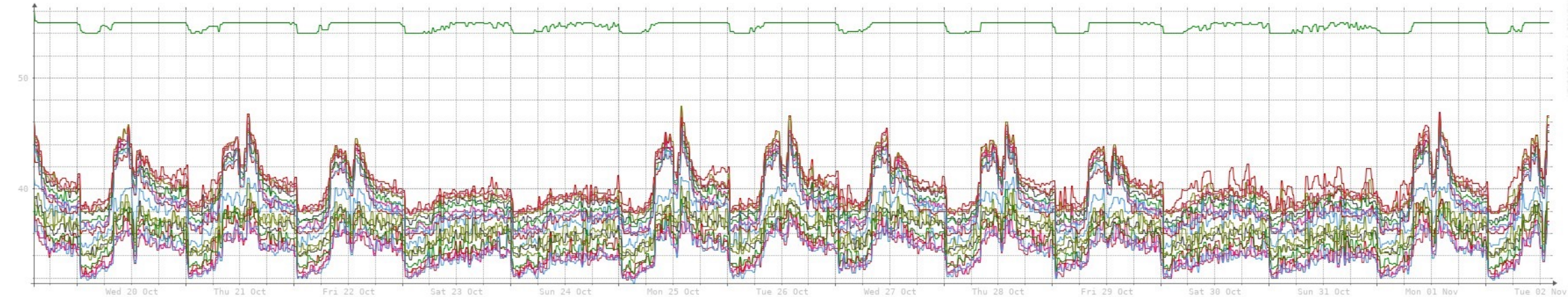
記憶體使用



40

高屏澎區網中心-防護伺服器硬體狀況

設備溫度狀況

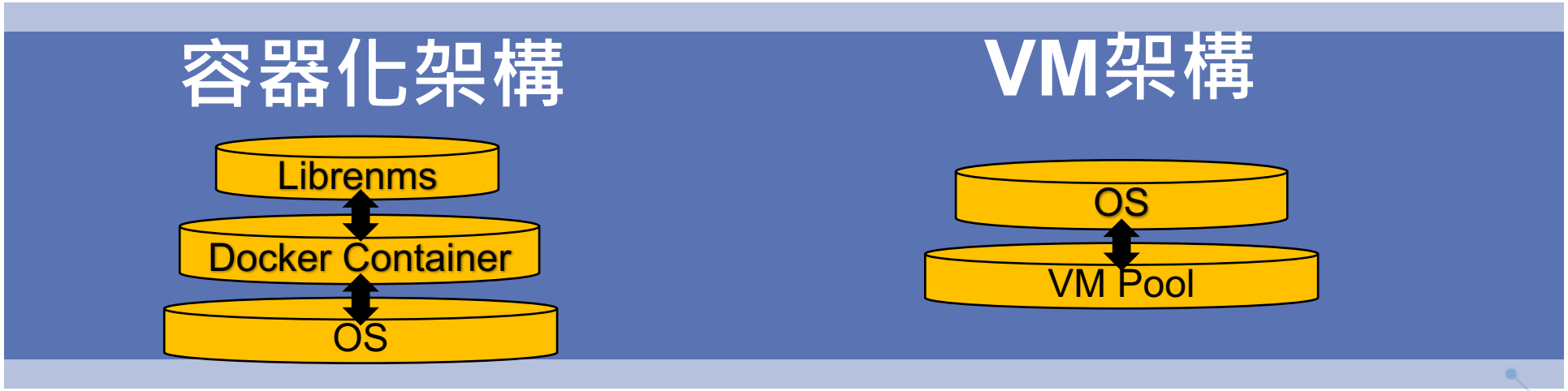


Degree C	Cur	Min	Max
Package id 1	46.6C	37.8C	47.3C
loc1	55.0C	54.0C	56.1C
Package id 0	40.3C	34.7C	41.1C
coreisa-0000	38.9C	34.0C	40.5C
coreisa-0000	37.1C	31.8C	38.1C
coreisa-0000	38.8C	33.6C	39.3C
coreisa-0000	37.1C	32.0C	38.1C
coreisa-0000	38.2C	32.2C	39.1C
coreisa-0000	38.9C	32.3C	39.9C
coreisa-0000	36.8C	31.5C	38.7C
coreisa-0000	38.8C	33.4C	40.1C
Core 0	45.8C	37.5C	46.2C
Core 1	45.3C	36.8C	45.9C
Core 2	45.1C	35.9C	45.9C
Core 3	44.3C	35.5C	45.6C
Core 4	45.1C	36.3C	45.6C
Core 5	45.5C	35.9C	45.7C
Core 6	46.4C	37.1C	47.5C
Core 7	45.7C	37.7C	46.7C

41

容器化網路裝置監控服務系統

容器化(container)網路裝置監控系統架構



容器化監測優勢

01

只需要安裝Docker
每台電腦都可以成為監測系統

不受OS環境限制

02

透過Docker雲端可設置上傳映像版本進行管理與備份效果，省去VM快照儲存容量消耗

雲端版本控制備份簡易

03

透過輕量化監測系統即時監測伺服器狀態與網路流量控管網路安全

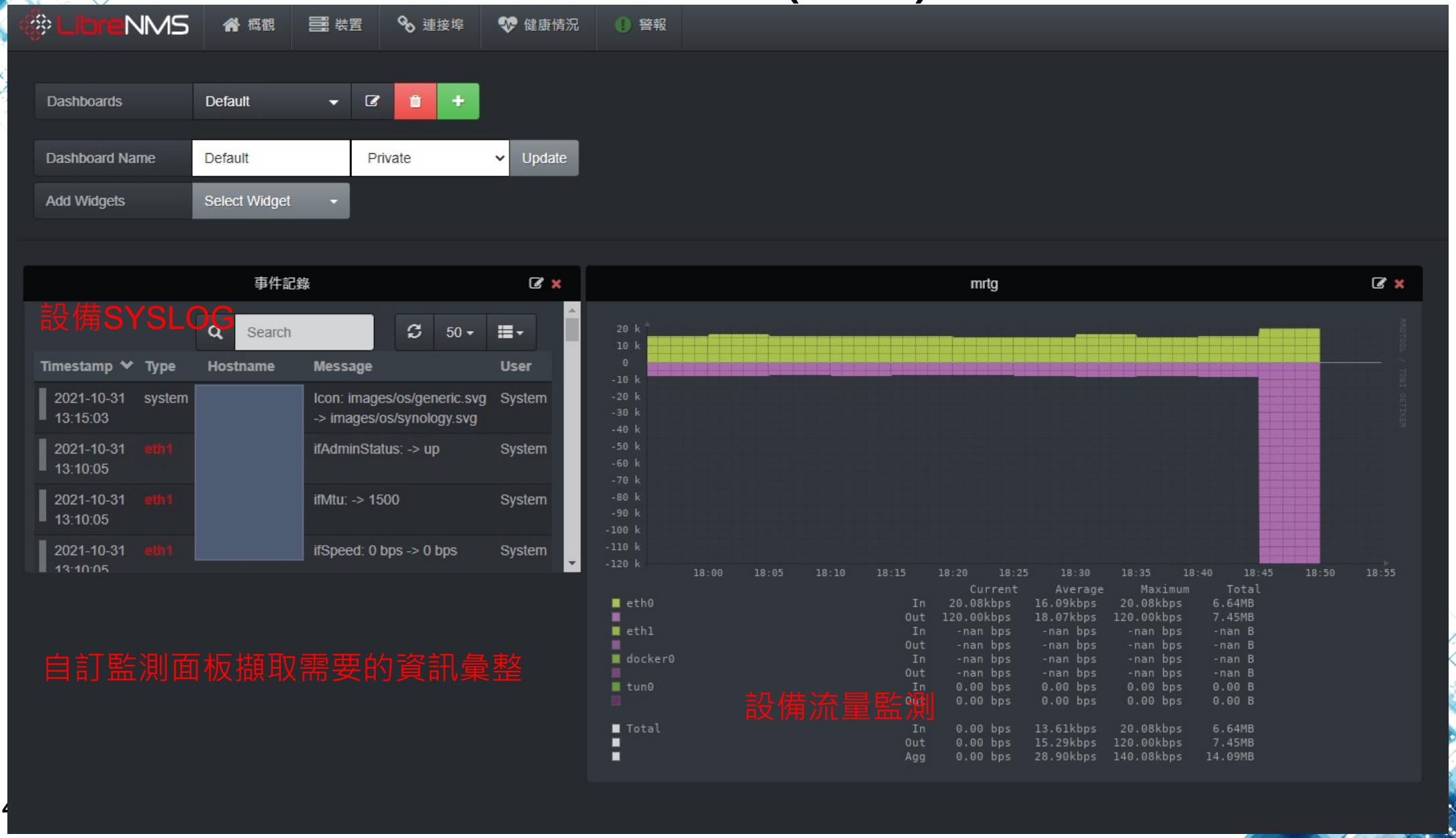
即時掌握伺服器狀態

04

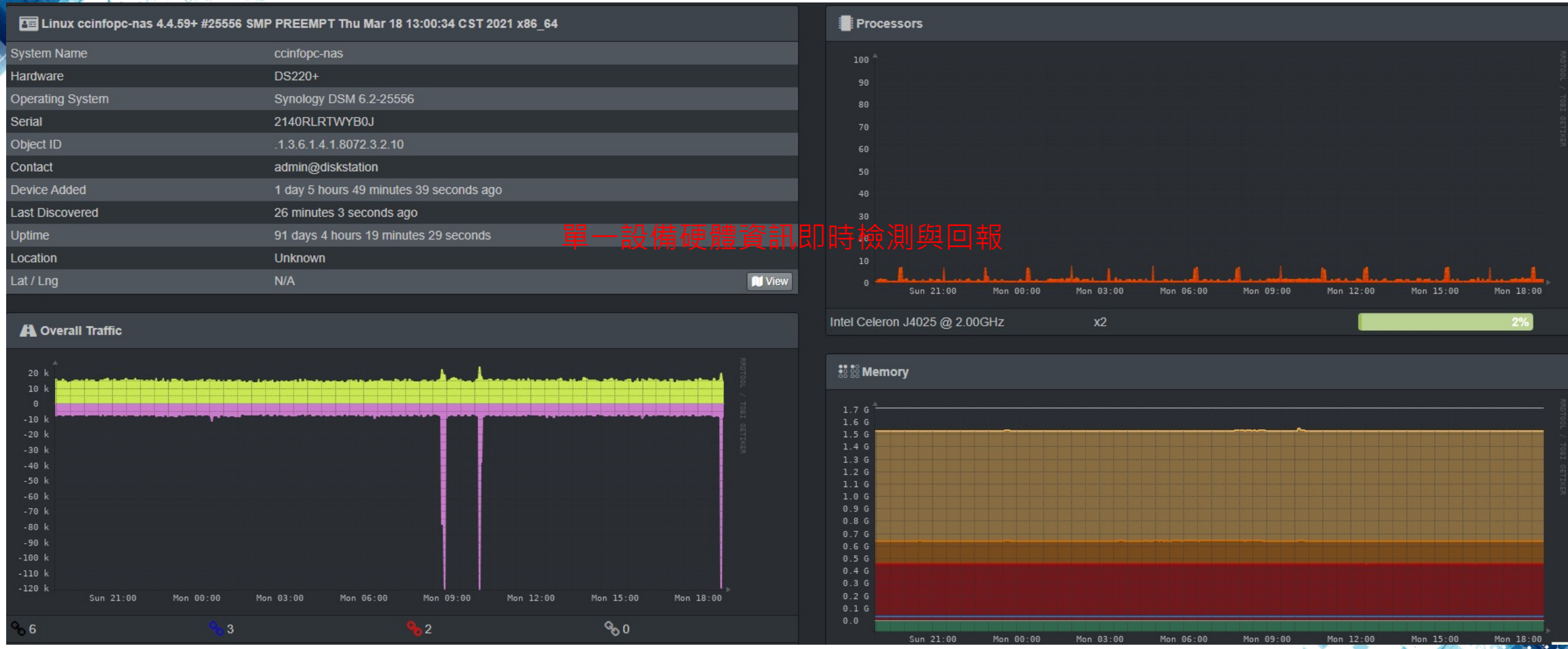
透過如Docker上傳版本號分享，快速支援轄下單位進行使用，幫助轄下單位有效管理網路裝置

易用易分享

監測實績展示 (1/2)


LibreNMS
概觀
裝置
連接埠
健康情況
警報
Dashboards
Default
Dashboard Name
Default
Private
Update
Add Widgets
Select Widget
事件記錄
設備SYSLOG
Search
50
Timestamp
Type
Hostname
Message
User
2021-10-31 13:15:03
system
Icon: images/os/generic.svg -> images/os/synology.svg
System
2021-10-31 13:10:05
eth1
ifAdminStatus: -> up
System
2021-10-31 13:10:05
eth1
ifMtu: -> 1500
System
2021-10-31 13:10:05
eth1
ifSpeed: 0 bps -> 0 bps
System
mrtg
20 k
10 k
0
-10 k
-20 k
-30 k
-40 k
-50 k
-60 k
-70 k
-80 k
-90 k
-100 k
-110 k
-120 k
18:00
18:05
18:10
18:15
18:20
18:25
18:30
18:35
18:40
18:45
18:50
18:55
Current
Average
Maximum
Total
eth0
In 20.08kbps 16.09kbps 20.08kbps 6.64MB
Out 120.00kbps 18.07kbps 120.00kbps 7.45MB
eth1
In -nan bps -nan bps -nan bps -nan B
Out -nan bps -nan bps -nan bps -nan B
docker0
In -nan bps -nan bps -nan bps -nan B
Out -nan bps -nan bps -nan bps -nan B
tun0
In 0.00 bps 0.00 bps 0.00 bps 0.00 B
Out 0.00 bps 0.00 bps 0.00 bps 0.00 B
Total
In 0.00 bps 13.61kbps 20.08kbps 6.64MB
Out 0.00 bps 15.29kbps 120.00kbps 7.45MB
Agg 0.00 bps 28.90kbps 140.08kbps 14.09MB
自訂監測面板擷取需要的資訊彙整
設備流量監測

監測實績展示 (2/2)



單一設備硬體資訊即時檢測與回報

110年全國大專校院資訊行政主管研討會

大會網站與主題


2021 CCDS 全國大專校院資訊行政主管研討會
研討會首頁
大會資訊
與會者資訊
防疫宣導與應變措施
合作夥伴
報名截止
CCDS
2021
10/
THU
28
FRI
29
國立中山大學
2021
智慧科技縱雲端
網路互聯守資安
CCDS 全國大專校院資訊行政主管研討會

活動介紹

大會資訊

會議日期

110年10月28日(四)～110年10月29日(五)

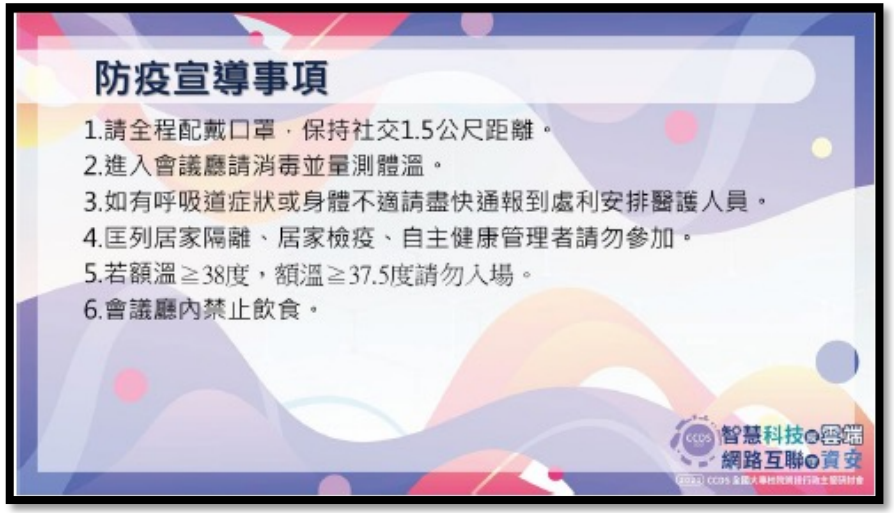
活動地點

第一天：中山大學國研大樓2F-光中廳
中山大學國研大樓1F-華立廳

第二天：中山大學國研大樓2F-光中廳
中山大學國研大樓1F-華立廳

與會人數:146人

活動特色 (1/2)



防疫計畫高雄市教育局審核通過

國立中山大學國研大樓IR1001
場所代碼：1053 5504 1452 498

國立中山大學國研大樓IR1002
場所代碼：1718 4694 2507 262

國立中山大學國研大樓光中廳
場所代碼：1838 2361 0859 802

國立中山大學國研大樓1F入口
場所代碼：1637 6644 9587 949

國立中山大學國研大樓華立廳
場所代碼：1880 4155 0985 318

會議廳獨立分流實名制

活動特色 (2/2)

YouTube

現場直播分流容留人數

減少室內活動戶外散策參訪
聘用專業導遊帶領

專題演講陣容

A.數位學習未來規劃與資訊安全
教育部資訊及科技教育司 郭伯臣司長

B.人工智慧最有希望的機會和最緊迫的危險
國立台北商業大學 張瑞雄校長

C.邁向智慧政府新未來
行政院人事行政總處 蘇俊榮副人事長

D.大專校院以全機關為範圍導入ISMS應優先落實的執行策略
國立中興大學計算機中心 陳育毅主任

E.準備好面對無孔不入的網路攻擊嗎?淺談教育部資安防護體系
國立中山大學資訊與管理學系 陳嘉玫教授

F.「關懷、生態、永續」：從知識走向行動，從在地走向全球
國立東華大學 趙涵捷校長

科技新知分享陣容

主持人:
交通部公路總局
資訊室王東琪主任

主持人:
國家衛生研究院資訊中心
莊育秀主任

主持人:
國家高速網路與計算機中心
史曉斌主任

主持人:
國家高速網路與計算機中心
劉德隆博士

主持人:
國家衛生研究院資訊中心
林瑞龍副技術師

主持人:
國立台東大學資訊工程學系
張耀中系主任

資訊新知分享陣容

2021大專校院資訊單位組織及經費合理性調查研究報告

主講人:
中國文化大學資訊處 王舒民資訊長

主持人:
ISAC中華民國大專校院資訊服務協會 黃明達榮譽理事長

活動花絮 (1/4)


開幕致詞
國立中山大學
鄭英耀 校長
智慧科技x雲端 網路互聯x資安
CCDS2021 全國大專校院資訊行政主管研討會
10/28 THU ▸ 29 FRI
2021
國立中山大學


教育體系資安事件案例(1/7)
• 事件說明
• 國立OO高中受本部OO機關委辦OO課程平臺，因該校委外廠商系統設計漏洞，致使登入後即可取得管理者權限，造成大量個資外洩
• 發生原因
• 委外廠商系統權限設計控管不完善，使用者僅需在網址列後方加上頁面名稱即可存取管理頁面
• 建議改善事項
• 須落實委外廠商資安監督責任，包含其開發測試是否遵守SSDLC、針對可能發生資安或個資風險通報等
• 資訊系統委外應會請資訊技術人員(如計中等單位)協助評估廠商能力、確認資安應辦事項等

活動花絮 (2/4)


CCDS 2021
智慧科技x雲端
網路互聯x資安
CCDS2021 全國大專校院資訊行政主管研討會
10/28 THU ▸ 29 FRI 2021
國立中山大學


Background
有些人擔心人工智慧會讓我們感到自卑，但是，任何一個頭腦正常的人每次看到花朵都應該會有自卑感。
Alan Kay (Turing Award 2003, OO先驅)
Father of personal computers
Alan Kay
智慧科技x雲端
網路互聯x資安
CCDS2021 全國大專校院資訊行政主管研討會
2021 國立中山大學
10 THU 28 ▸ 29 FRI

活動花絮 (3/4)


Linking the Government to the Future
邁向智慧政府新未來
行政院人事行政總處 政務副人事長 蘇俊榮
智慧科技 雲端 網路互聯 資安
CCDS2021 全國大專校院資訊行政主管研討會
2021 國立中山大學
10/28 THU ▸ 29 FRI

活動花絮 (4/4)


資科司綜合座談
教育部資訊及科技教育司
李月碧 高級管理師
裴善成 科長
智慧科技縱雲端網路互聯守資安
CCDS2021 全國大專校院資訊行政主管研討會
2021 國立中山大學
10/28 THU ▸ 29 FRI


資科司綜合座談
教育部資訊及科技教育司
李月碧 高級管理師
裴善成 科長

連線單位需求分析及滿意度調查

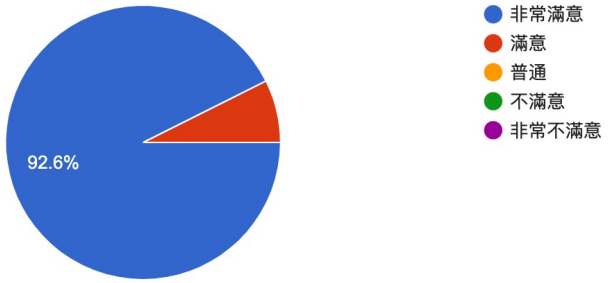
- 區網服務滿意度問卷調查
- 連線單位需求分析

服務滿意度問卷調查結果

➢ 今年服務人員熱忱及親和力非常滿意度達92.6% (前年度90%)

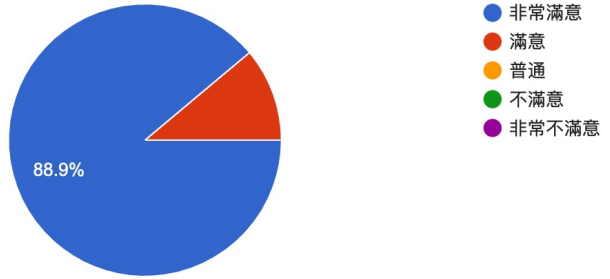
2 . 本年度區網中心對　貴校(單位)之網路連線服務，您認為是否滿意?

27 則回應



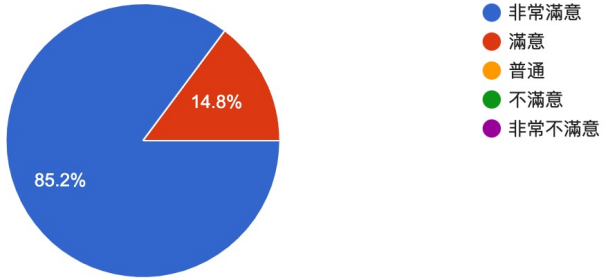
3. 本年度貴校(單位)如有網路管理或連線的技術諮詢時，區網中心的協助是否符合您的需求?

27 則回應



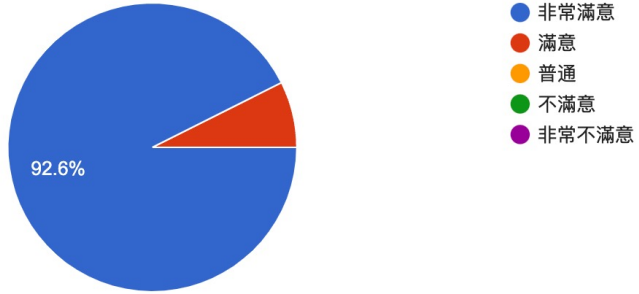
5. 資通安全事件的通報應變的協助處理:

27 則回應



10. 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? ?

27 則回應



連線單位需求分析(問卷調查)

- Google Meet 連線不穩定問題
  - 協助連線單位排除網路連線問題
- 使用者遇到一些行動網路無法連線學校網站的問題
  - 與ISP業者聯絡，協助連線單位排除網路連線問題
- 漏洞資安防護
  - 提供防護建議與情資給連線單位
  - 資安防護公告於區網網站上
- 建議爭取南部舉辦大型資安培訓課程，增加南部人才
  - 與外單位爭取合作辦理資安培訓課程

未來營運目標

110年度預計推動之重點工作(1/2)

- 容器化系統精進整合
  - 至少提供一種以上容器化系統 (如syslog導入等系統)
- 資安健檢服務推動
  - 擬使用如SHODAN弱點平台協助連線單位做資安健檢。
- Layer 7 流量分析服務
  - 今年已分析3所連線單位學校流量，明年至少分析3所以上連線單位
- 不當資訊系統防護
  - 現已導入8個區網中心，明年預計導入至少10個區網中心

110年度預計推動之重點工作(2/2)

- 網路管理
  - 推廣至少一種以上網路管理相關工具，幫助連線單位提升網管能力
- 技術交流
  - 至少辦理4場以上技術交流研討會

敬請　委員指教

謝謝!!