



輔仁大學網路管理分享

輔仁大學 資訊中心 梁士杰





大綱

1. 資安運作
2. 網路管理
3. 其它分享



背景介紹

- 學生人數:25600人、教職員工人數:2500人
- 11個學院及附設神學院、大學部48個學系、進修學士班16個學系、二年制在職專班1系、碩士班47所、碩士在職專班23所、博士班11所。
- 資訊中心人數:網路與資源管理組:10人(網路:6、教學:4)、校務資訊開發組:20人。
- 學校及醫院資訊分治。

資安運作

- 資訊安全管理制度導入
- 弱掃工具
- 資安控管

資安運作

- 資訊安全管理制度導入
 - 2007年開始由教育部開始導入八校聯合的資安管理系統輔導，2009年通過ISO 27001:2005，驗證範圍為遠距教學(iCan3)與機房；2014年通過 ISO 27001:2013；2018年擴大驗證(增加選課系統與愛校建言系統)；2024年通過 ISO 27001:2022。
 - 計畫4年分階段全校導入資訊安全管理制度，另外教務處、學務處及人事室導入ISO27001第三方稽核。

資安運作

➤ 資安專章因應

2023年因應資安專章之要求：全校導入資訊安全管理系統(ISMS)。

1. 將原本僅限於資訊單位導入的範圍，擴大到全校導入。
2. 將導入範圍與欲進行第三方驗證的範圍重新規劃

	導入ISMS範圍	第三方驗證範圍
第一年	除了資訊中心既有4項核心業務之外。另外針對導入全校ISMS預作準備相關文件與系統設計。	持續針對資訊中心既有4項核心業務進行第三方驗證。
第二年	全校一級行政單位	持續針對資訊中心既有4項核心業務進行第三方驗證。
第三年	除了以上既有，增加：其他行政單位	除了以上既有，增加1項全校核心業務(教務系統)，共計5項核心業務。
第四年	除了以上既有，增加：教學單位，完成全校導入ISMS	除了以上既有，增加1項全校核心業務(人事系統)，共計6項核心業務。
第五年	持續維運與強化(資安管理制度暨委外驗證範圍)	除了以上既有，增加1項全校核心業務(學務系統)，共計7項核心業務。

資安運作

- 資安專章因應
 - 全校IP盤點系統:
 - a) 針對IP使用類型進行分類。
 - b) 未使用之IP於資安設備上使用ACL設定，使其無法連線。
 - 防護網頁遭竄:
 - a) 提供Windows及Linux網頁監控程式。
 - b) 針對主機管理者進行教育訓練。
 - 滲透測試
 - a) 對象為官網、選課系統及ISO驗證範圍內主機。
 - b) 委外給廠商。

資安運作

➤ 資安專章因應

➤ 全校資訊資產盤點系統

- a) 先建立行政與教學單位資安窗口。
- b) 安排多次顧問現場講座，進行盤點系統講解與填寫。
- c) 進行各單位現場稽核，產出稽核報告與改善建議追蹤。

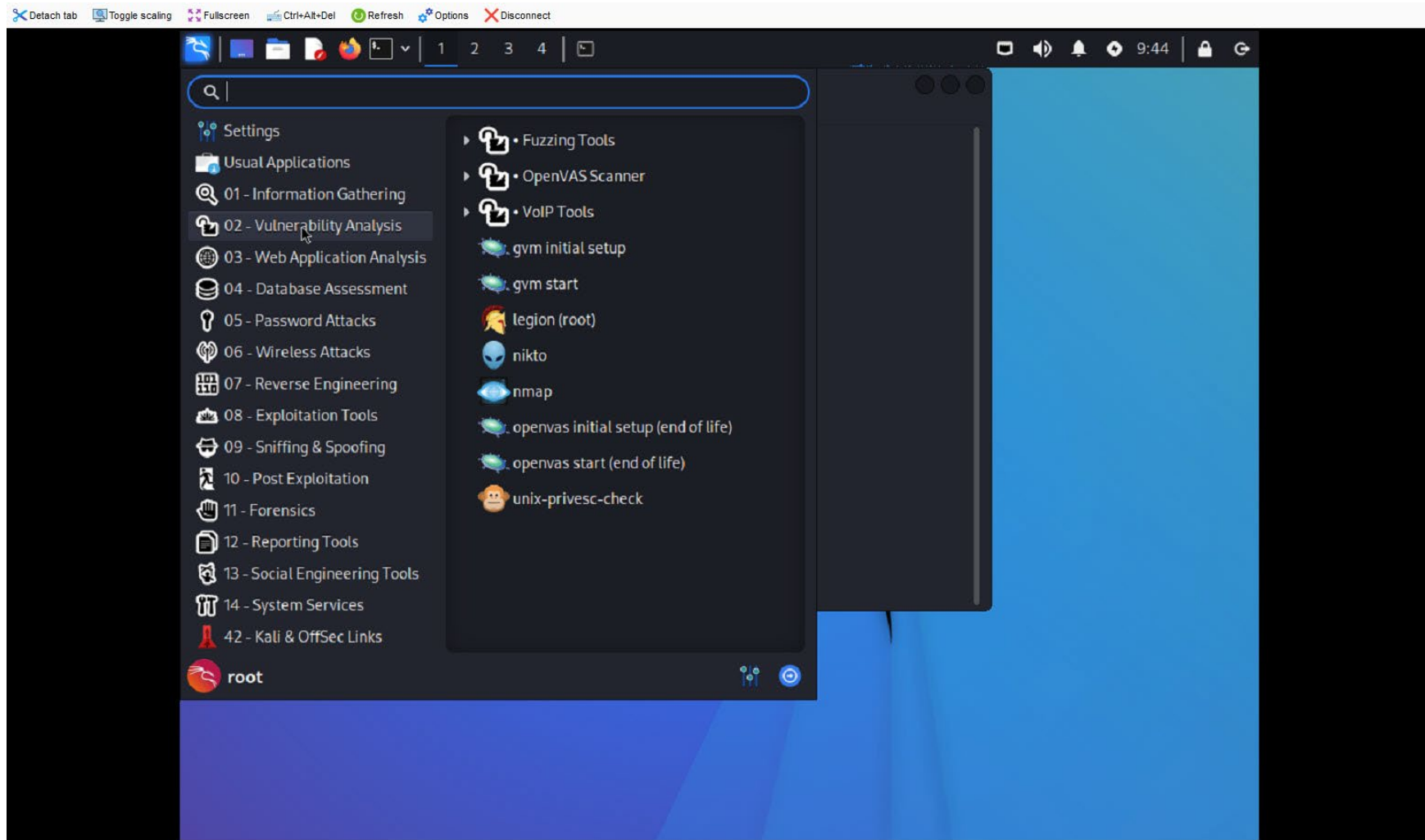
➤ 資安專責人員

- a) 以資安行政作業為主，非技術職。
- b) 協助舉辦資安教育訓練。
- c) 協助推動全校資訊安全管理制度。
- d) 建立輔大資通安全弱點通報系統(VANS)
- e) 協助推動教務處、人事室、學務處導入及通過ISO27001:2022。

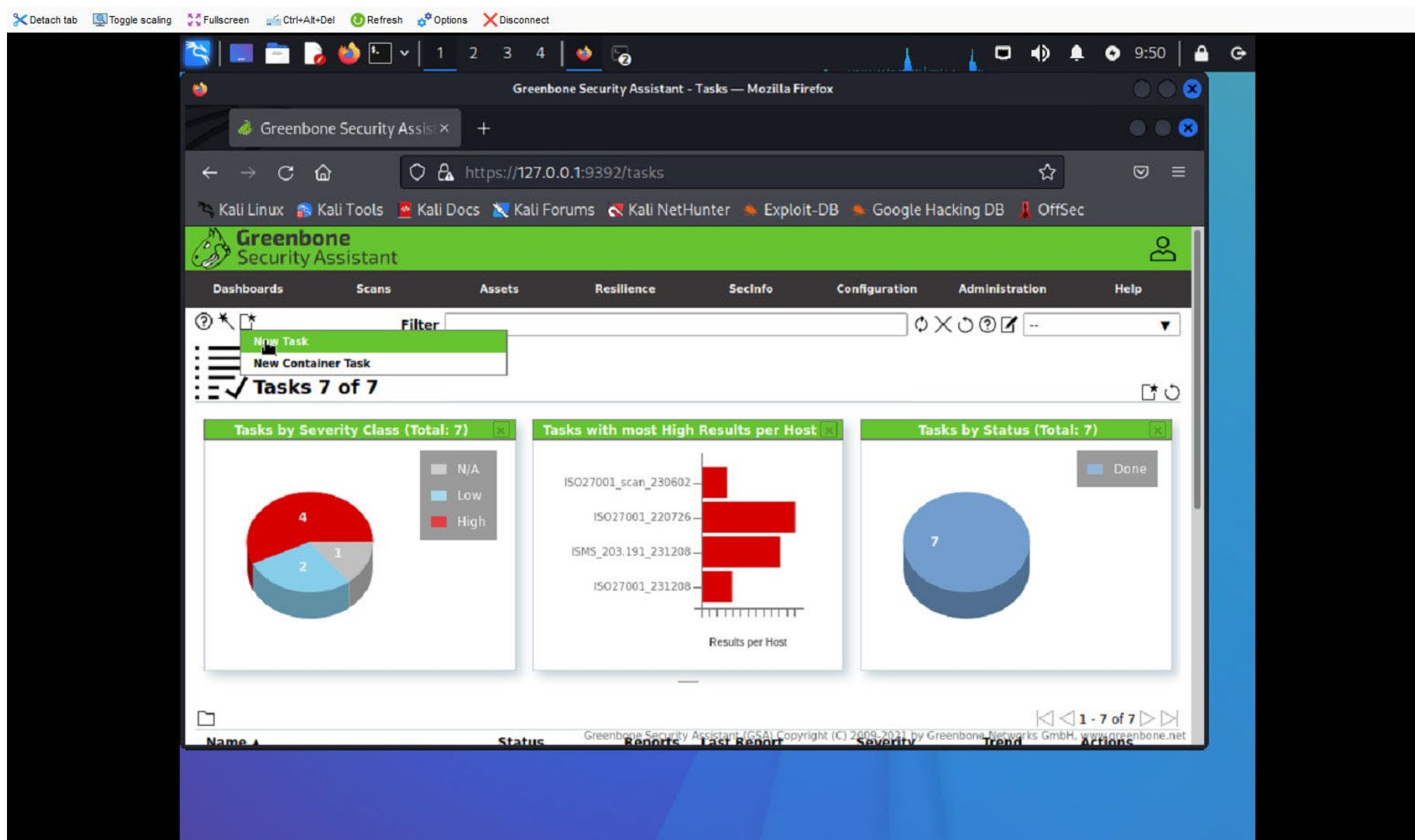
資安運作

- 弱掃工具GVM
 - 安裝Kali Linux
 - 安裝GVM
 - 安裝VNC:方便遠端操控

➤ 弱掃工具GVM



➤ 弱掃工具GVM



➤ 弱掃工具GVM

New Task

Name:

Comment:

Scan Targets:

Alerts:

Schedule: ☐ Once

Add results to Assets: ☒ Yes ☐ No

Apply Overrides: ☒ Yes ☐ No

Min QoD: %

Alterable Task: ☐ Yes ☒ No

Auto Delete Reports: ☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest reports

Scanner:

Scan Config:

Greenbone Security Assistant - Report Details — Mozilla Firefox

https://127.0.0.1:9392/report/cc2caa23-c953-42ec-bf25-68df00d1d99f

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

RepoMon, Oct 23, 2023
rt: 7:40 AM UTC

ID: cc2caa23-c953-42ec-bf25-68df00d1d99f Created: 2023 7:40 AM UTC Modified: 2023 8:12 AM UTC Owner: admin

Information	Results (1 of 26)	Hosts (1 of 1)	Ports (0 of 2)	Applications (1 of 1)	Operating Systems (1 of 1)	CVEs (0 of 0)	Closed CVEs (0 of 0)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)
-------------	-------------------	----------------	----------------	-----------------------	----------------------------	---------------	----------------------	---------------------------	-------------------------	---------------

Task Name: 140.136.246.70

Scan Time: Mon, Oct 23, 2023 7:40 AM UTC - Mon, Oct 23, 2023 8:12 AM UTC

Scan Duration: 0:31 h

Scan Status: Done

Hosts scanned: 1

Filter: apply_overrides=0 levels=hml min_qod=70

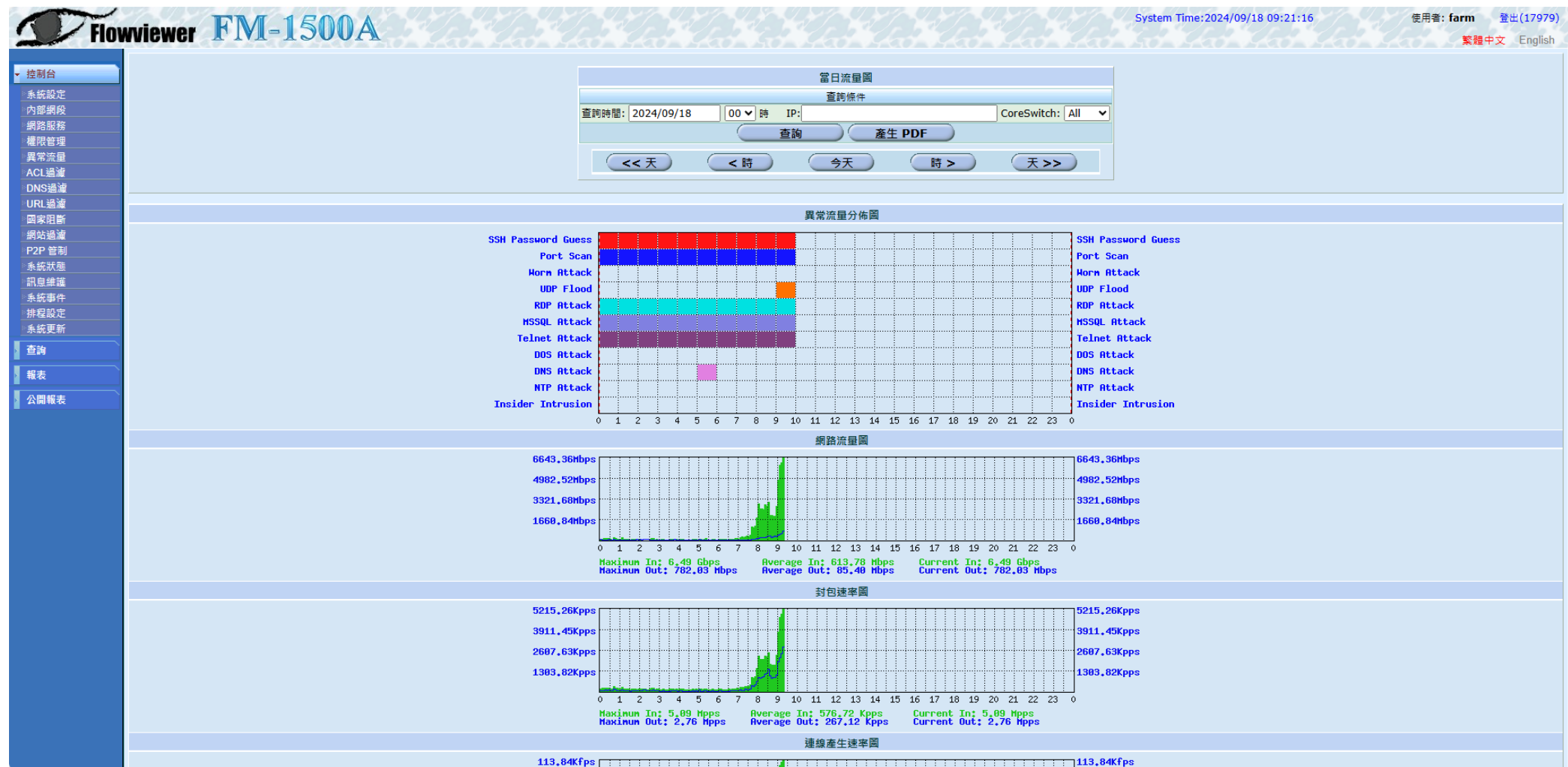
Timezone: Coordinated Universal Time (UTC)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

資安運作

- Openvas:一套開放原始碼(Open Source)軟體的弱點掃描檢測工具，這個工具可以不斷從(NVT、SCAP、CERT)更新弱點測試資料庫。
- CVE:CVE是一個公開已知的網路安全性漏洞和暴露的清單。清單中的每一項都是基於在特定軟體產品中發現的特定漏洞或暴露，而不是基於一般類別或類型的漏洞或暴露。
- CVE清單將軟體漏洞分成了幾種類型，包括：
 - • Denial of Service (DoS)
 - • Code Execution
 - • Buffer Overflow
 - • Memory Corruption
 - • SQL Injection
 - • Cross-Site Scripting (XSS)
 - • Directory Traversal
 - • HTTP Response Splitting

➤ 使用異常行為攔阻設備



➤ ACL+國別



















































































































➤ 使用治科科技flowview進行IP與國別攔阻。

1. 依據攻擊來源統計，動態調整國別攔阻。



➤ ACL+國別

2. 設定ACL

ACL							
IP 群組							
新增 管理群組: campus_dns							
ACL設定							
#	來源IP	目的IP	通訊協定	來源埠	目的埠	動作	操作
1	Any		Any	Any		阻斷	     
2	中國[CN]		TCP	Any		阻斷	     
3	Any		TCP	Any		放行	     
4	Any		Any	Any		阻斷	     
5	Any		TCP	Any		放行	     
6	water_monitor_out		TCP	Any		放行	     
7	Any		TCP	Any		放行	     
8	Any		Any	any		單向阻斷	     
9	Any		Any	Any		雙向阻斷	     
10	Any		Any	Any		單向阻斷	     
11	Any		TCP	Any		阻斷	     
12	ga_monitor		Any	Any		阻斷	     
13	car_monitor		TCP	Any		阻斷	     
14	臺灣[TW] 中國[CN]		TCP	Any		放行	     
15	Any		TCP	Any		阻斷	     
16	Any		Any	Any		阻斷	     
17	臺灣[TW] 加拿大[CA] 澳門[MO] 香港[HK] 瑞士(中歐)[CH]		Any	Any		放行	     
18	Any		Any	Any		阻斷	     
19	Physics	日本[JP]	Any	Any		放行	     

➤ ACL+國別

2. 設定國別攔阻

阻斷來源國家					
新增					
#	來源國家	目的IP	備註	動作	
1	Any	Any		刪除	
2	北韓	Any		刪除	
3	Any	Any		刪除	
4	Any	Any		刪除	
5	Any	Any		刪除	
6	Any	Any		刪除	
7	Any	Any		刪除	
8	Any	Any		刪除	
9	Any	Any		刪除	
10	Any	Any		刪除	
11	Any	Any		刪除	
12	Any	Any		刪除	
13	Any	Any		刪除	
14	Any	Any		刪除	
15	Any	Any		刪除	
16	Any	Any		刪除	
17	Any	Any		刪除	
18	Any	Any		刪除	
19	俄羅斯聯邦	Any		刪除	
20	Any	Any		刪除	
21	Any	Any		刪除	
22	Any	Any		刪除	
23	Any	Any		刪除	
24	Any	Any		刪除	
25	Any	Any		刪除	
26	Any	Any		刪除	
27	喬治亞洲	Any		刪除	

新增例外					
#	來源國家	來源IP	通訊協定	來源埠	動作
1	Any	Any	UDP	53	刪除
2	Any	Any	TCP	80,443,53	刪除
3	Any	Any	UDP	53	刪除
4	Any	Any	TCP	80,443,53	刪除
5	Any	Any	TCP	80,443	刪除
6	Any	Any	TCP	80,443,25	刪除

阻斷目的國家					
新增					
#	來源IP	目的國家	備註	動作	
1	Any	北韓		刪除	
2	Any	Any		刪除	
3	Any	Any		刪除	
4	Any	Any		刪除	
5	Any	Any		刪除	
6	Any	Any		刪除	
7	Any	Any		刪除	
8	Any	Any		刪除	
9	Any	Any		刪除	
10	Any	俄羅斯聯邦		刪除	
11	Any	Any		刪除	
12	Any	Any		刪除	
13	Any	喬治亞洲		刪除	

新增例外					
#	目的國家	目的IP	通訊協定	目的埠	動作

➤ 攔阻挖礦及P2P行為

套用 網站阻斷過濾設定

啟動阻斷網站功能: ☒ 是 ☐ 否

要阻斷的網站類型:		Hit Counts
<input type="checkbox"/> 影音		0
<input type="checkbox"/> 藥物		0
<input type="checkbox"/> 賭博		0
<input type="checkbox"/> 色情		0
<input type="checkbox"/> 暴力		68,936
<input checked="" type="checkbox"/> 挖礦		226,477

網站清單搜尋: 搜尋 清除

套用 P2P流量控制設定

P2P軟體流量監控方式: ☐ 不監看也不控管 ☒ 監看和控管 ☐ 只監看不控管

一天內偵測到P2P行為幾次後，中斷該用戶所有連線 (0 代表不使用此功能): 次

阻斷時間: 小時

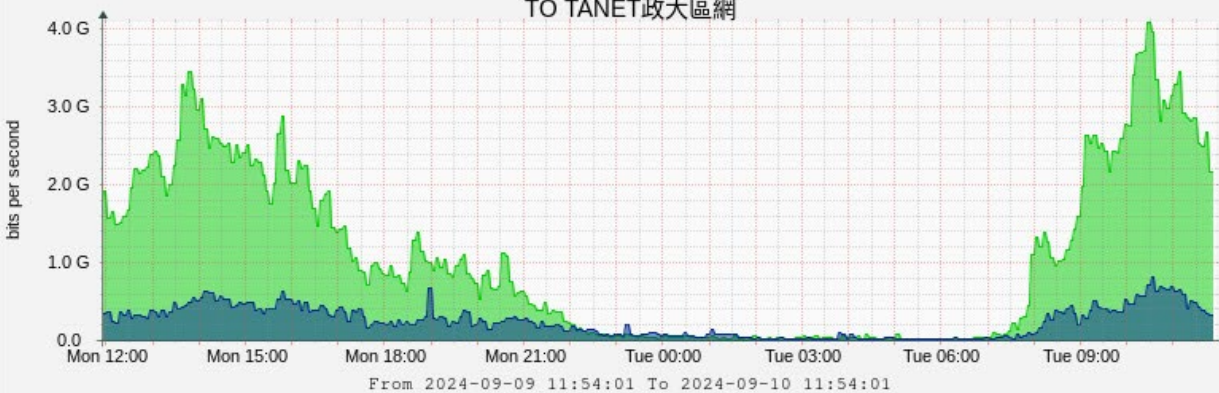
P2P類型	啟用	排程
eDonkey,eMule,Kademlia	<input checked="" type="checkbox"/>	Any Time ▼
KaZaA,FastTrack	<input checked="" type="checkbox"/>	Any Time ▼
Gnutella,Foxy	<input checked="" type="checkbox"/>	Any Time ▼
Direct Connect	<input checked="" type="checkbox"/>	Any Time ▼
BitTorrent	<input checked="" type="checkbox"/>	Any Time ▼
AppleJuice	<input checked="" type="checkbox"/>	Any Time ▼
WinMX	<input checked="" type="checkbox"/>	Any Time ▼
SoulSeek	<input checked="" type="checkbox"/>	Any Time ▼
Ares,AresLite	<input checked="" type="checkbox"/>	Any Time ▼
Xunlei,Thunder	<input checked="" type="checkbox"/>	Any Time ▼
PPStream,QQLive,feidian,POCO,QVOD	<input type="checkbox"/>	Any Time ▼
SIP(VoIP)	<input type="checkbox"/>	Any Time ▼
MSN	<input type="checkbox"/>	Any Time ▼
Yahoo Messenger	<input type="checkbox"/>	Any Time ▼
Facebook	<input type="checkbox"/>	Any Time ▼

➤ 匯入威脅名單

DNS 黑名單 DNS 白名單 Import ODS					
新增		匯入資料	名稱搜尋:	搜尋	DNS 阻斷名單
套用					
#	Domain Name / URL		備註	動作	
1	*.rbeopp.com		SEX	修改 刪除	
2	*.91rb.net		SEX	修改 刪除	
3	*.rbe9966.com		SEX	修改 刪除	
4	*.rm2029.com		SEX	修改 刪除	
5	*.repe21.com		SEX	修改 刪除	
6	*.joinside.org		SEX	修改 刪除	
7	*.rbc007.com		SEX	修改 刪除	

- 連外線路提升為連政大區網10G，連是方電信4G
 - 1. 路由配置:走國內網段連政大區網、走國外網段連是方電信。
 - a) 往政大以靜態路由設定國內網段。
 - b) 往國外透過是方帶140.136.0.0/16發佈於國外網段。
 - 2. 流量顯示。
 - a) 架設Cacti呈現MRTG。

TO TANET政大區網

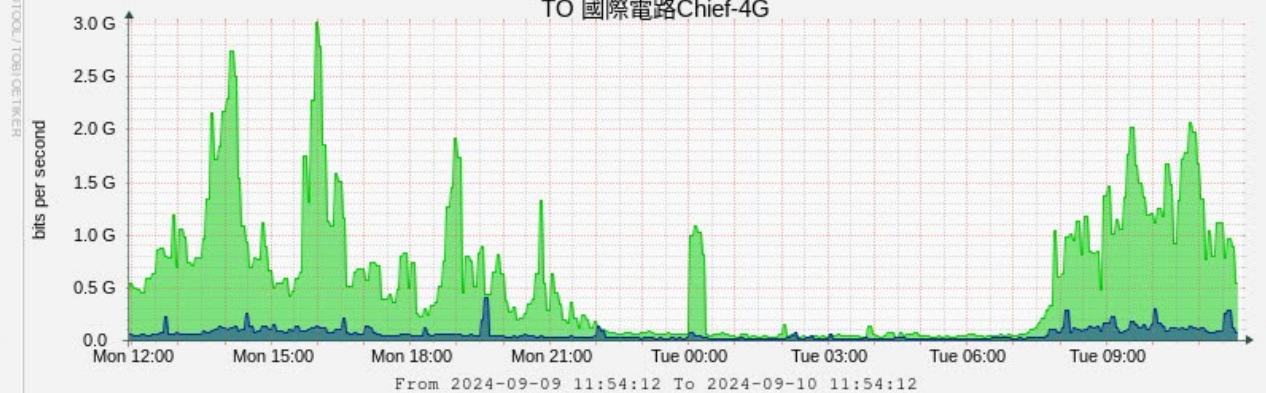


Inbound Current: 2.16 G Average: 1.07 G Maximum: 4.09 G
Outbound Current: 330.98 M Average: 239.42 M Maximum: 823.14 M

Generated by Cacti®

Daily (5 Minute Average)

TO 國際電路Chief-4G

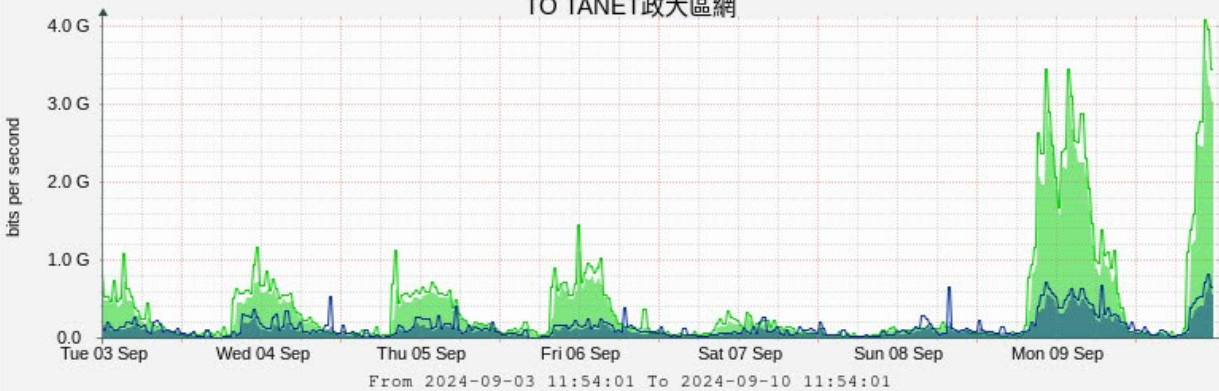


Inbound Current: 546.70 M Average: 583.73 M Maximum: 3.02 G
Outbound Current: 69.79 M Average: 65.13 M Maximum: 413.87 M

Generated by Cacti®

Daily (5 Minute Average)

TO TANET政大區網

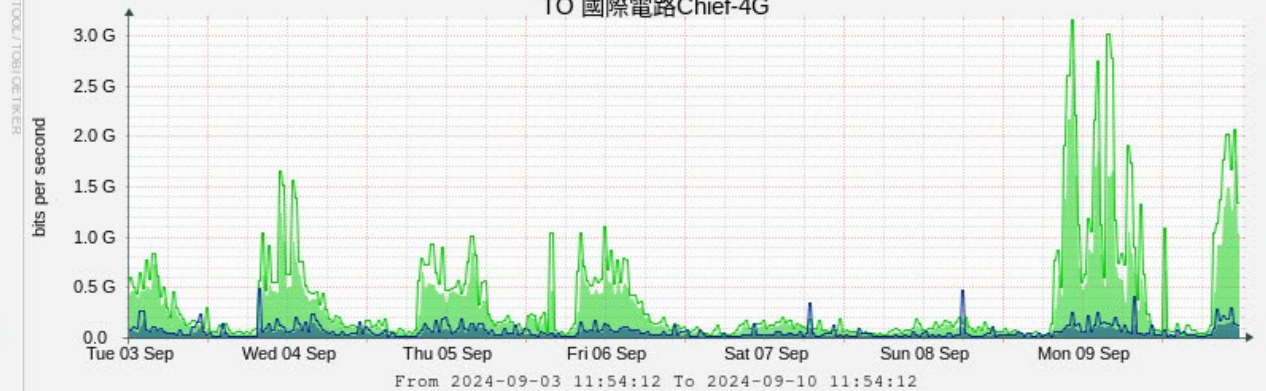


Inbound Current: 3.04 G Average: 353.97 M Maximum: 3.56 G
Outbound Current: 552.70 M Average: 101.00 M Maximum: 698.05 M

Generated by Cacti®

Weekly (30 Minute Average)

TO 國際電路Chief-4G



Inbound Current: 1.03 G Average: 272.60 M Maximum: 2.77 G
Outbound Current: 94.22 M Average: 42.02 M Maximum: 172.47 M

Generated by Cacti®

Weekly (30 Minute Average)

➤ 頻寬管理

1. 星期一~五 9:00~18:00 有線IP及無線帳號1天上下載共16G，超過則降速為512K。
2. 代管主機網段，1天上下載共20G。
3. P2P攔阻。

網路管理

➤ 網路工具

➤ 路由路徑:

a) <https://ping.pe>

b) <https://www.itdog.cn/>

➤ 針對特定國別IP進行攔阻或允許

a) iptables+xtables-addons

作法:參考<https://gist.github.com/netrunn3r/d5d9eddde86a7ad7cd31a7d8e5d747c4>

➤ 進行來回測試

- 1) 用ping.pe相關網站測試回來品質。
- 2) 從校內用traceroute or tracert測試到目的端IP之品質。

140.119.168.10

Go

Help

Settings

Query: ping 140.119.168.10, interval: 5s, dense mode: no

Probing 140.119.168.10 - APNIC /12 AS1659 ERX-TANET-ASN1 - Taiwan, Taipei City, Taipei [college] MAP

Geo	ISP	Loss	Sent	Last	Avg	Best	Worst	StDev	MTR	Chart
Canada, BC, Vancouver	Telus	0%	30	208.47	209.31	208.29	213.54	0.95	show	
Canada, BC, Vancouver	Shaw	0%	30	216.09	207.63	191.82	293.62	24.55	show	
USA, CA, Fremont	Hurricane	0%	30	130.93	130.68	130.09	131.44	0.37	show	
USA, CA, Fremont	IT7 FMT2	0%	30	130.02	130.2	129.58	130.78	0.35	show	
USA, CA, Fremont	Linode	0%	30	139.41	139.79	139.25	140.63	0.31	show	
USA, CA, San Francisco	Digital Ocean	0%	30	164.08	164.11	163.32	166.63	0.68	show	
USA, CA, Santa Clara	Hurricane	0%	30	130.01	131.87	129.9	142	2.67	show	
USA, CA, Los Angeles	Cogent	0%	30	135.78	135.83	135.13	138.21	0.71	show	
USA, CA, Los Angeles	Hurricane	0%	30	134.07	134.15	133.55	134.8	0.34	show	
USA, CA, Los Angeles	DMIT	0%	30	158.63	158.84	158.32	159.41	0.3	show	
USA, CA, Los Angeles	Vultr	0%	30	160.4	160.05	159.11	166.87	1.31	show	
USA, CA, Los Angeles	RamNode	0%	30	136.21	136.11	135.52	137.15	0.42	show	
USA, CA, Los Angeles	NetActuate	0%	30	132.93	132.85	132.16	134.1	0.42	show	
USA, WA, Seattle	Cogent	0%	30	159.61	160.3	159.28	164.53	0.97	show	
USA, WA, Seattle	Google	0%	30	125.17	124.87	124.3	125.5	0.34	show	
USA, WA, Seattle	RamNode	0%	30	178.8	179.57	178.27	193.18	2.83	show	
USA, CO, Denver	Cogent	0%	30	192.7	193.4	191.46	197.47	1.48	show	
USA, CO, Denver	NetActuate	0%	30	192.47	192.67	192.21	193.28	0.3	show	
USA, TX, Dallas	Softlayer	0%	30	184.66	181.37	179	185.06	2.11	show	
USA, TX, Dallas	NetActuate	0%	30	163.69	163.57	163.02	164.37	0.4	show	
USA, IL, Chicago	Cogent	0%	30	183.01	183.71	181.84	189.88	1.55	show	
USA, IL, Chicago	NetActuate	0%	30	183.13	183.45	182.79	184.41	0.4	show	
USA, GA, Atlanta	RamNode	0%	30	204.06	205.39	203.45	219.92	3.47	show	
USA, FL, Miami	Cogent	0%	30	199.08	199.4	197.99	203.27	1.35	show	
USA, VA, Ashburn	NetActuate	0%	30	195.13	195.34	194.75	196.98	0.44	show	
USA, NY, New York	Cogent	0%	30	219.15	219.01	218.17	222.46	0.96	show	

140.136.239.254

Go

Help

Settings

Query: ping 140.136.239.254, interval: 5s, dense mode: no

Probing 140.136.239.254 - APNIC /17 AS38845 FUJEN-AS-TW Fu Jen - Taiwan, New Taipei City, New Taipei City [college] MAP

Geo	ISP	Loss	Sent	Last	Avg	Best	Worst	StDev	MTR	Chart
Canada, BC, Vancouver	Telus	0%	41	330.37	330.9	329.75	335.87	1.12	show	<div></div>
Canada, BC, Vancouver	Shaw	0%	41	147.68	153.21	140.36	287.87	29.25	show	<div></div>
USA, CA, Fremont	Hurricane	0%	41	156.22	155.84	154.86	163.99	1.35	show	<div></div>
USA, CA, Fremont	IT7 FMT2	0%	41	154.24	154.5	153.53	161.28	1.14	show	<div></div>
USA, CA, Fremont	Linode	0%	41	265.16	265.72	265.16	266.37	0.3	show	<div></div>
USA, CA, San Francisco	Digital Ocean	0%	41	263.67	263.51	262.93	265.7	0.48	show	<div></div>
USA, CA, Santa Clara	Hurricane	0%	41	155.96	157.01	155.65	164.48	1.56	show	<div></div>
USA, CA, Los Angeles	Cogent	0%	41	384.36	385.24	384.36	391.92	1.15	show	<div></div>
USA, CA, Los Angeles	Hurricane	0%	41	156.08	155.66	155.12	157.69	0.51	show	<div></div>
USA, CA, Los Angeles	DMIT	0%	41	249.01	249.17	248.47	249.91	0.34	show	<div></div>
USA, CA, Los Angeles	Vultr	0%	41	303.58	303.51	302.86	304.91	0.42	show	<div></div>
USA, CA, Los Angeles	RamNode	0%	41	242.18	242.43	241.8	243.04	0.32	show	<div></div>
USA, CA, Los Angeles	NetActuate	0%	41	304.3	304.65	304.01	305.42	0.32	show	<div></div>
USA, WA, Seattle	Cogent	0%	41	177.85	178.06	177.1	182.33	0.85	show	<div></div>
USA, WA, Seattle	Google	0%	41	132.95	133.09	132.33	133.71	0.3	show	<div></div>
USA, WA, Seattle	RamNode	0%	41	323.85	323.78	323.04	325.52	0.51	show	<div></div>
USA, CO, Denver	Cogent	0%	41	200.43	202.6	199.78	228.95	4.6	show	<div></div>
USA, CO, Denver	NetActuate	0%	41	285.66	285.79	284.98	286.76	0.33	show	<div></div>
USA, TX, Dallas	Softlayer	0%	41	211.17	211.03	210.34	215.95	0.91	show	<div></div>
USA, TX, Dallas	NetActuate	0%	41	280.4	279.73	279.04	282.3	0.53	show	<div></div>
USA, IL, Chicago	Cogent	0%	41	259.75	260.14	258.63	265.64	1.26	show	<div></div>
USA, IL, Chicago	NetActuate	0%	41	265.3	265.92	265.3	266.66	0.4	show	<div></div>
USA, GA, Atlanta	RamNode	0%	41	320.71	321.23	319.28	356.16	5.67	show	<div></div>
USA, FL, Miami	Cogent	0%	41	432.91	434.1	432.22	442.62	2.41	show	<div></div>
USA, VA, Ashburn	NetActuate	0%	41	254.94	254.6	253.91	255.49	0.42	show	<div></div>
USA, NY, New York	Cogent	0%	41	448.89	449.07	448.13	452.1	0.79	show	<div></div>



FUJEN CATHOLIC
UNIVERSITY



謝謝聆聽