



# 桃園縣政府教育局網路中心 網路解決說明

報告人：莊斯凱

# Outline

- ◆ 網路危機
- ◆ 防禦措施
- ◆ 管理問題
- ◆ 好康分享

# 網路危機

- ◆ 網路釣魚事件2006.08~12共13起
  - ◆ 網路釣魚事件2007.01共24起
  - ◆ 網路釣魚事件2007.02共5起
  - ◆ 網路釣魚事件2007.03共12起
  - ◆ 網路釣魚事件2007.04共3起
  - ◆ 網路釣魚事件2007.05➡還不知道有多少
- 
- ◆ 每日許許多多的攻擊事件，每1.5小時就有22k次的攻擊。

# 重複發生➡ 13所學校

校名	重複次數
楊光國中小	4
楊明國中	3
信義國小	3
瑞梅國小	3
笨港國小	3
巴峻國小	3
中壢國小	3
壽山國中	3
南崁國小	2
社子國小	2
羅浮國小	2
大崗國中	2
三坑國小	2

# 許許多多的網路攻擊

163.30.255.251 - Check Point SmartView Tracker - [fw.log : All Records\*]

File Edit View Query Navigate Tools Window Help

Log Active Audit

Log Queries

- Predefined
  - All Records
  - Fire Wall
  - VPN
  - FloodGate-1
  - SecureClient
  - SmartDefense
  - Account
  - SmartView Monitor
  - UA WebAccess
  - UA Server
  - Fire Wall GX
  - Voice over IP
  - IPv6
  - VPN Edge
  - Login Failures
  - Connectra
  - Integrity
  - Custom

No.	Date	Time	Origin	Service	Source	Destination	Rule	Curr. Rule ...	Rule Na...	S...
21915	15May2007	1:32:35	FW710-A	TCP	TYC_Squid_8080	222.213.245.254	TYC_proxy			1708
21927	15May2007	1:32:38	FW710-B	TCP	45312	222.215.119.136	user-30.s2.tyc.edu.tw			http
21939	15May2007	1:32:39	FW710-A	UDP	3850	64.79.141.53	TYC_ns2	75	75-Standard	domain
21951	15May2007	1:32:42	FW710-A	TCP	http	61.135.162.119	TYC_ftp	75	75-Standard	59981
21952	15May2007	1:32:43	FW710-A	TCP	http	61.135.162.119	TYC_ftp	75	75-Standard	60128
21956	15May2007	1:32:43	FW710-B	TCP	epmap	bzq-84-110-218-118...	FW710-B	10	10-Standard	35203
21961	15May2007	1:32:44	FW710-B	TCP	2108	219-87-152-215.stati...	foxyipic.com	75	75-Standard	35036
21971	15May2007	1:32:46	FW710-A	TCP	http	61.135.162.119	TYC_ftp	75	75-Standard	33694
21973	15May2007	1:32:47	FW710-A	TCP	http	61.135.162.119	TYC_ftp	75	75-Standard	34093
21981	15May2007	1:32:49	FW710-A	TCP	35938	222.215.119.136	163.30.1.58			http
21983	15May2007	1:32:49	FW710-B	TCP	10565	218.61.11.39	163.30.0.74			irc2
22014	15May2007	1:33:00	FW710-A	TCP	2108	219-87-152-215.stati...	222.178.185.5	75	75-Standard	25417
22018	15May2007	1:33:01	FW710-B	UDP	2425	ns5.ahhftt.net.cn	TYC_nsl	75	75-Standard	domain
22021	15May2007	1:33:02	FW710-A	UDP	7188	RisingTek_SIP	61-230-17-20.dyna...	75	75-Standard	sip_en
22024	15May2007	1:33:02	FW710-A	UDP	2425	d.dns.br	TYC_nsl	75	75-Standard	domain
22033	15May2007	1:33:05	FW710-A	TCP	epmap	bas2-windsor12-1128...	219-87-152-215.stati...	75	75-Standard	23706
22035	15May2007	1:33:05	FW710-A	TCP	9582	222.215.119.136	user-120.s2.tyc.edu.tw			http
22043	15May2007	1:33:06	FW710-B	TCP	TYC_Squid_8080	58.61.36.103	219-87-152-217.stati...	75	75-Standard	X11
22044	15May2007	1:33:06	FW710-B	TCP	TYC_Squid_8080	58.61.36.103	219-87-152-216.stati...	75	75-Standard	X11
22046	15May2007	1:33:06	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	219-87-152-213.stati...	75	75-Standard	X11
22047	15May2007	1:33:06	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	219-87-152-210.stati...	75	75-Standard	X11
22048	15May2007	1:33:06	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	Nokia-Cluster	10	10-Standard	X11
22049	15May2007	1:33:07	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	219.87.152.218	75	75-Standard	X11
22051	15May2007	1:33:07	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	FW710-A	10	10-Standard	X11
22052	15May2007	1:33:07	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	219.87.152.223	75	75-Standard	X11
22054	15May2007	1:33:07	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	219.87.152.209	75	75-Standard	X11
22055	15May2007	1:33:07	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	RisingTek_SIP	75	75-Standard	X11
22056	15May2007	1:33:07	FW710-A	TCP	TYC_Squid_8080	58.61.36.103	219-87-152-214.stati...	75	75-Standard	X11
22060	15May2007	1:33:08	FW710-B	TCP	55076	218.61.31.108	TYC_Mail			irc2
22063	15May2007	1:33:08	FW710-B	TCP	34161	221.231.140.73	163.30.3.68			http
22088	15May2007	1:33:13	FW710-A	UDP	2425	217.11.96.154	TYC_nsl	75	75-Standard	domain
22089	15May2007	1:33:13	FW710-A	TCP	39038	218.61.11.39	163.30.0.92			irc2

Ready

Track Logs: Read/Write

Total: 22097

# 內外交迫

SonicWALL - Administration for TYC034 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛

網址(1) https://10.12.19.18/main.html 移至

連結 元智Email 個人化的主頁 教育局信箱 VPN STATUS MGT

**SONICWALL** COMPREHENSIVE INTERNET SECURITY™

System  
Network  
SonicPoint  
Firewall  
VoIP  
VPN  
Users  
Hardware Failover  
Security Services  
Log

View  
Categories  
Syslog  
Automation  
Name Resolution  
Reports  
ViewPoint

Wizards  
Help  
Logout

Status: Ready

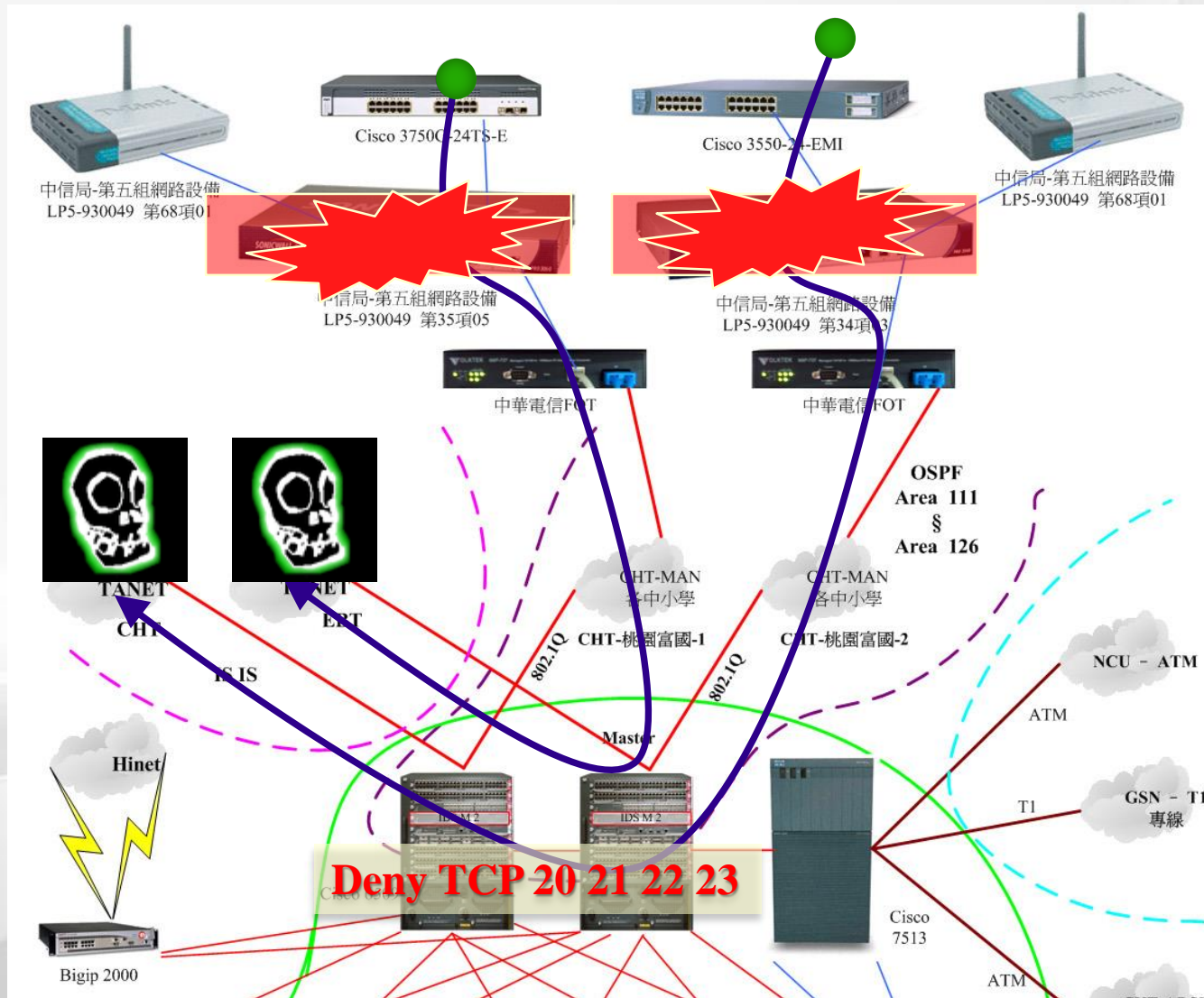
#	Time ▼	Priority	Category	Message	Source	Destination	Notes	Rule
1	05/15/2007 01:37:21.160	Notice	Network Access	UDP packet dropped	163.30.255.69, 20071, X1	10.12.19.18, 21254, X1	UDP Port: 21254	
2	05/15/2007 01:37:19.880	Info	Authenticated Access	WAN zone administrator login allowed	163.30.3.131, 0, X1 (admin)	10.12.19.18, 443, X1		
3	05/15/2007 01:16:33.768	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 3135, X0	163.28.4.23, 80, X1	MAC address: 00:11:93:a7:37:80	
4	05/15/2007 01:01:15.752	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 1417, X0	204.16.208.33, 137, X1	MAC address: 00:11:93:a7:37:80	
5	05/15/2007 00:59:57.560	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 1417, X0	204.16.208.33, 137, X1	MAC address: 00:11:93:a7:37:80	
6	05/15/2007 00:53:05.848	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 1417, X0	58.19.183.42, 137, X1	MAC address: 00:11:93:a7:37:80	
7	05/15/2007 00:52:31.416	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 1417, X0	58.19.183.42, 137, X1	MAC address: 00:11:93:a7:37:80	
8	05/15/2007 00:51:46.096	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 1417, X0	58.19.183.42, 137, X1	MAC address: 00:11:93:a7:37:80	
9	05/15/2007 00:49:17.784	Notice	Network Access	UDP packet dropped	72.152.94.58, 63866, X1	163.30.57.38, 4672	UDP Port: 4672	
10	05/15/2007 00:48:33.704	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 1417, X0	202.97.238.199, 137, X1	MAC address: 00:11:93:a7:37:80	
11	05/15/2007 00:47:15.640	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.2.5, 1417, X0	202.97.238.199, 137, X1	MAC address: 00:11:93:a7:37:80	
12	05/15/2007 00:37:24.928	Alert	Intrusion Prevention	<a href="#">IP spoof dropped</a>	192.168.1.5, 137, X0	211.100.33.61, 137, X1	MAC address: 00:11:93:a7:37:80	
13	05/15/2007	Notice	Network Access	UDP packet dropped	163.30.255.69, 19498, X1	10.12.19.18, 21251, X1	UDP Port: 21251	

完成 網際網路

# 防禦措施

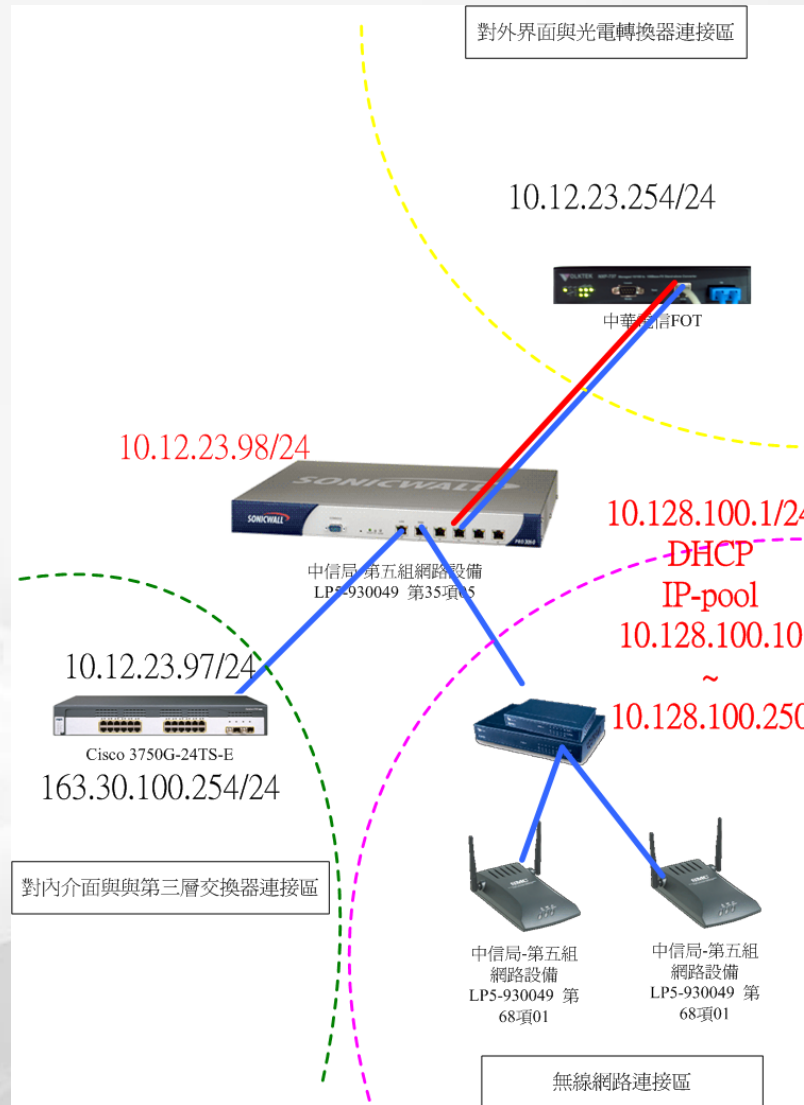
- ◆ 骨幹交換器
  - 封鎖TCP 20
  - 封鎖TCP 21
  - 封鎖TCP 22
  - 封鎖TCP 23
- ◆ 校園建置透通式防火牆
- ◆ 加強密碼設定的宣導

# 防禦架構(1)





# 防禦架構(2)



# 密碼設定原則

- ◆ 混合字母與數字，大寫與小寫。
- ◆ 至少8個字母以上。
- ◆ 至少每三個月改一次密碼。
- ◆ 不要使用與自己有關的資訊，如親朋好友姓名、電話、卡號、身份證號、生日等。
- ◆ 不要重覆鍵盤字母，如aaaaa1111或qwertyui。
- ◆ 不要使用難記以至於需寫下來的密碼。
- ◆ 不要使用字典找得到的字。
- ◆ 不要使用電腦螢幕上任何出現的字。
- ◆ 不要將密碼給任何人，包括您的男女朋友、職務代理人、上司

# 管理問題

- ◆ FTP、SSH、TELNET使用需求
  - 修改標準的port
  - 限制存取的來源IP
- ◆ 使用VPN穿透
  - ◆ 架設PPTP的VPN服務
  - ◆ 教育局提供SSLVPN服務(公務帳號)
    - ◆ <https://sslvpn.tyc.edu.tw>
- ◆ 校園防火牆可由中心管理與派送ACL Rule
- ◆ 即時同步教育部的設限資料
  - ◆ <http://140.111.1.22/tanet/spam.html>

# SSLVPN

<https://sslvpn.tyc.edu.tw>



## 桃園縣政府教育局無線網路安全認證系統@SSL-VPN

請使用教師研習系統帳號密碼登入

歡迎使用桃園縣政府教育局無線網路認證系統

帳號

密碼

請選擇認證系統

桃園縣教育帳號(研習系統) ▼

登入

如果您是一般外來訪客，請連至[Guest](#)

下載NC安裝程式請點選[Network Connection 5.3](#)

本縣教育人員使用本無線網路認證機制

請選擇認證系統：**桃園縣教育帳號(研習系統)**

使用校園無線漫遊機制整合實驗與推廣計畫的使用者  
包含資策會、國家高速網路與計算中心之漫遊認證系統  
請選擇認證系統：**學術網路校園無線漫遊機制**

而本縣教育人員至其他各大學漫遊無線網路  
請使用公務帳號登入

帳號：帳號@ms.tyc.edu.tw

密碼：原研習系統密碼

# 防火牆中心端管理系統

SonicWALL GMS - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛

網址(D) https://sgms.tyc.edu.tw/sgms/auth 移至

連結 元智Email 個人化的主頁 教育局信箱 VPN STATUS MGT

Taoyuan County

- Bade City
- Chungli City
  - TYC115-hmjh
  - TYC116-lkjh
  - TYC117-cljh
  - TYC118-hnjh
  - TYC119-nljh
  - TYC120-tcjh
  - TYC121-dsjhs
  - TYC122-lsjh
  - TYC143-clps
  - TYC144-cpes
  - TYC145-simps
  - TYC146-blps
  - TYC147-cpps
  - TYC148-sjes
  - TYC149-hyes
  - TYC150-pzps
  - TYC151-ftes
  - TYC152-nlps
  - TYC153-dles
  - TYC154-sdes
  - TYC155-ccps
  - TYC156-zles
  - TYC157-lges
  - TYC158-ndes
  - TYC159-lses
  - TYC160-sgps
  - TYC161-hses
  - TYC162-jfes
  - TYC163-sres
  - TYC164-cves

Global Policies

- System
  - Status
  - Time
  - Administrator
  - Tools
  - Info
  - Settings
  - Schedules
  - Management
  - SNMP
- Network
- Firewall
- Log
- Diagnostics
- Website Blocking
- DHCP
- Users
- VPN
- Security Services
  - SonicPoint
- Wireless
- WGS
- Dialup
- Web Filters
- Register/Upgrades

Taoyuan County: Status (user: eric type: Administrators) Logout

Ready

Status Information for Global Node: Taoyuan County

SonicWALL	
SonicWALLs in the System	240
SonicWALLs that are Not Registered	240
SonicWALLs with VPN Upgrade	239
SonicWALLs that support MSSP	0
SonicWALLs with Global VPN Client Upgrade	0

Management	
SonicWALLs that are Down	16
SonicWALLs that are Unacquired	1
SonicWALLs with Pending Tasks	15
SonicWALLs managed using	
Existing Tunnel/LAN	0
Management Tunnel	0
HTTPS	240
SonicWALLs with DHCP Server Enabled	239
SonicWALLs currently on Dialup	0

Subscription	
Anti-Virus	0
Content Filter List/Service	0
Extended Warranty	0
Gateway Anti-Virus	0
Intrusion Prevention Service	0

SonicWALL Models	
PRO 2040 Enhanced	208
PRO 3060 Enhanced	31
Unknown	1

SONICWALL

Monitor Reports Panel Console

SonicWALL Global Management System Standard Edition

W: SGF6Z7EQ

網際網路

# 即時同步教育部的設限資料

## 桃園縣教育網路中心 - 網路管理控制台

各類網路事件處理

流量資訊

線路與機房狀況

其他

## 中毒或是對外攻擊IP處理

教育部封鎖的IP

IP address	網域	校名	教育部定義事件	教育部登錄時間	教育局狀態	教育局定義事件	動作
------------	----	----	---------	---------	-------	---------	----

為求最佳效果，請用 1024\*768 ，IE 5.5以上版本觀看本網頁  
程式設計:莊斯凱 Eric Chuang

# 好康分享

<http://www.wifly.com.tw/sp/wiflynet/iii-students/iii-students.html>



**I am** 因為無限大夢想而偉大！ 史上最大無限夢想漫遊網

CONNECT EVERY GREAT DREAMER

WIFLY與經濟部工業局行動台灣應用推動計畫合作「行動台灣漫遊無限，校園漫遊上網專案」，  
只要以自己學校的無線上網帳號密碼，透過漫遊認證交換中心的認證登入WIFLY網路，  
隨時隨地打開電腦觀世界、讀財經、寫報告、聽音樂、玩遊戲、看賽事…。  
隨時隨地連結無線，遨遊史上最大無限夢想漫遊網！

**注意事項：**

- 1.本活動參加對象，僅限與漫遊認證交換中心直接接洽之學校或縣市教育網路中心轄下連線單位之教職員生，詳細清單請見 [合作學校清單](#)
- 2.本無線上網服務由WIFLY與漫遊認證交換中心合作提供，每次連線20分鐘後自動斷線，唯使用者仍可不限次數重複登入使用。
- 3.具備學生身份的使用者，亦可透過本活動以優惠價申辦WIFLY學生專案，享受不限登入次數及上網時數的無線上網。（申辦學生優惠專案須隨附本人有效學生證明）
- 4.活動期間自96年3月1日起，本活動主辦單位保留隨時修改服務內容或終止服務之權利。

指導單位：經濟部工業局行動台灣應用推動計畫辦公室  
執行單位：財團法人資訊工業策進會、漫遊認證交換中心、安源資訊

**學生專案費率表**

費用	★	加贈禮
NT: 299 / 月繳		ezPeer+ free trial 14 days
NT: 3000 / 年繳		ezPeer+ free trial 30 days

[申請表單連結](#) [ezPeer+試用券下載](#)

[申辦地點](#)

[直接前往 WIFLY](#)

WIFLY無線上網服務覆蓋範圍：戶外及特定室內上網區域—臺北市7-ELEVEN、Starbucks星巴克咖啡特定門市；臺北市縣捷運站、臺北市區戶外道路、臺北市七大商業區域（包含周邊巷道）、臺北市行政大樓、臺北市立圖書館、臺北市立聯合醫院、臺北小巨蛋、臺北市立美術館…；連鎖店家—IS Coffee 伊是咖啡、漢堡王、羅多倫咖啡、LAVAZZA CAFE 老咖啡、古典玫瑰園、新都里餐廳、紐約紐約展覽購物中心、中興百貨…；上網熱點陸續增建中，詳細店家數、熱點區域及地址，請至網站[www.wifly.com.tw](http://www.wifly.com.tw)查詢。

客服專線：0809010008 網址：[www.wifly.com.tw](http://www.wifly.com.tw)

 wifly.com.tw





謝謝指導