



# 桃園區網工作報告

呂芳發  
103年11月



# 大綱

- ☐ Tanet及TWAREN新骨幹計畫
- ☐ IPS Pa5060 問題解決
- ☐ 管理維運-異常流量偵測
- ☐ 資安防禦MiniSOC平台建置
- ☐ 建議

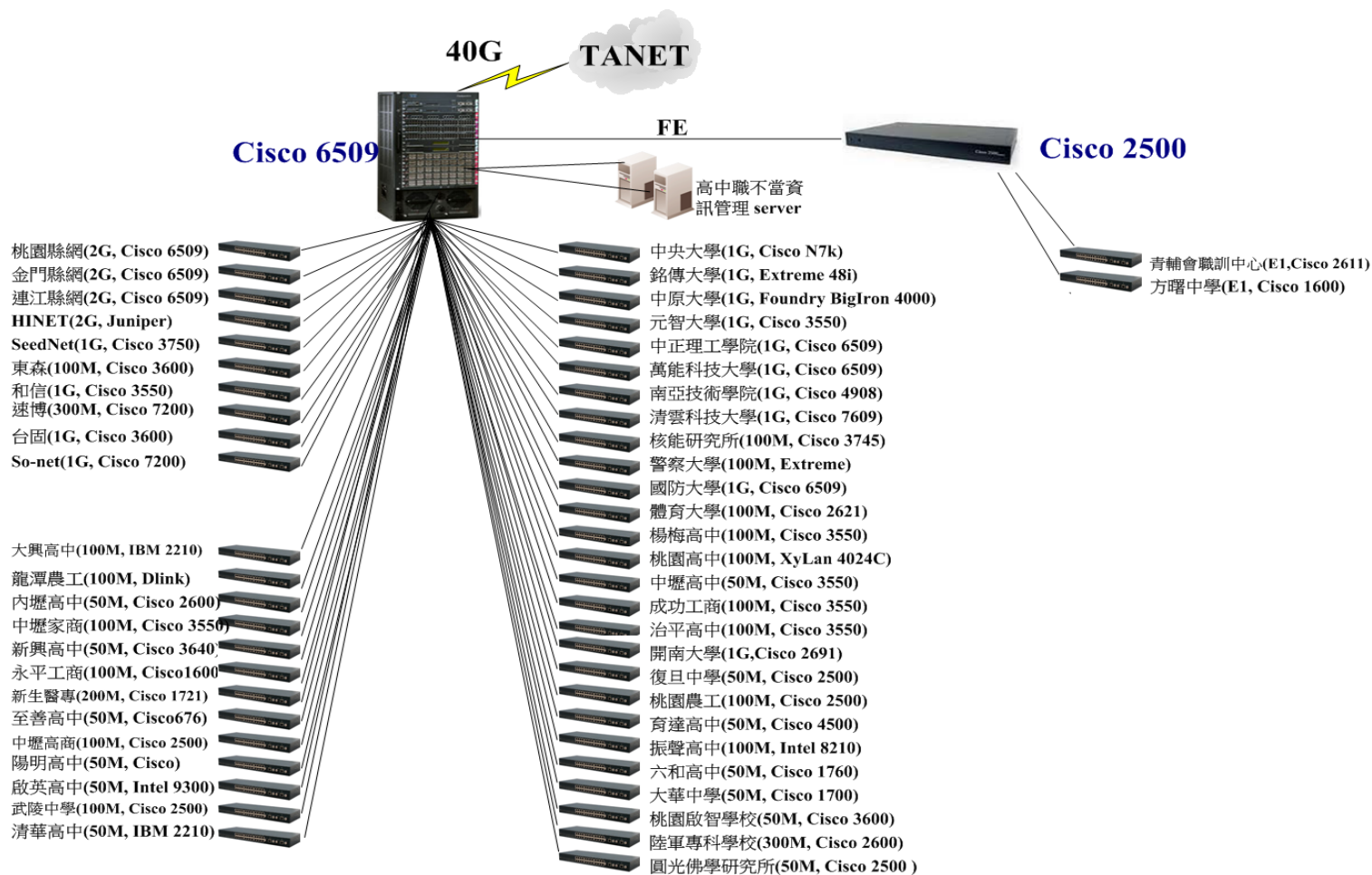


# Tanet及TWAREN新骨幹計畫

- ❑ Tanet及TWAREN骨幹頻寬各100G, 區網到Tanet 40G
- ❑ 分骨幹線路服務案及骨幹設備採購案, 都已公告, 年底前完成招標
- ❑ 明年初建置, 4月正式啟用

# Tanet區網新架構

## □ 骨幹頻寬100G, 區網到Tanet 40G





# Paloalto IPS問題

- ❑ 2014-05 設定超量攻擊 threshold
  - 當 Cpu Load (Data-plane) > 70% , 影響網路傳輸狀況
  - Dns, ssh, MS\_rdp (2012-12, 2013-03 調整threshold)
  - MySql, MsSql, Pop3 (2013-03-28)
- ❑ 2014-05 overload
  - Cpu Load (Manage-plane) 持續衝高
  - TANet Backbone ISIS routing 交換狀況不穩
  - Zone protection, ACL 阻擋 異常流量
- ❑ 2014-05 overload
  - Google 相關網站連線緩慢



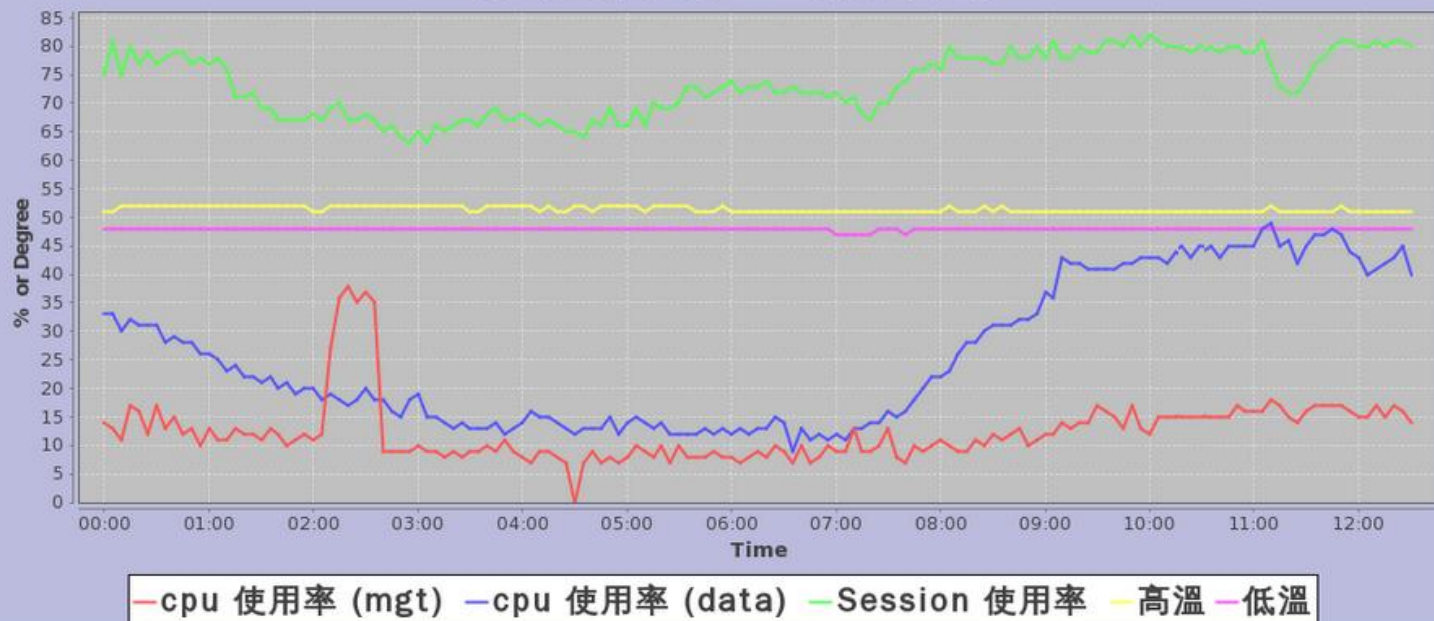
# Paloalto IPS load

Service Usage Statistics

區網 PaloAlto 5060 IPS

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2014-11-06)

系統運作溫度 不可過高, Session使用率 不可過高



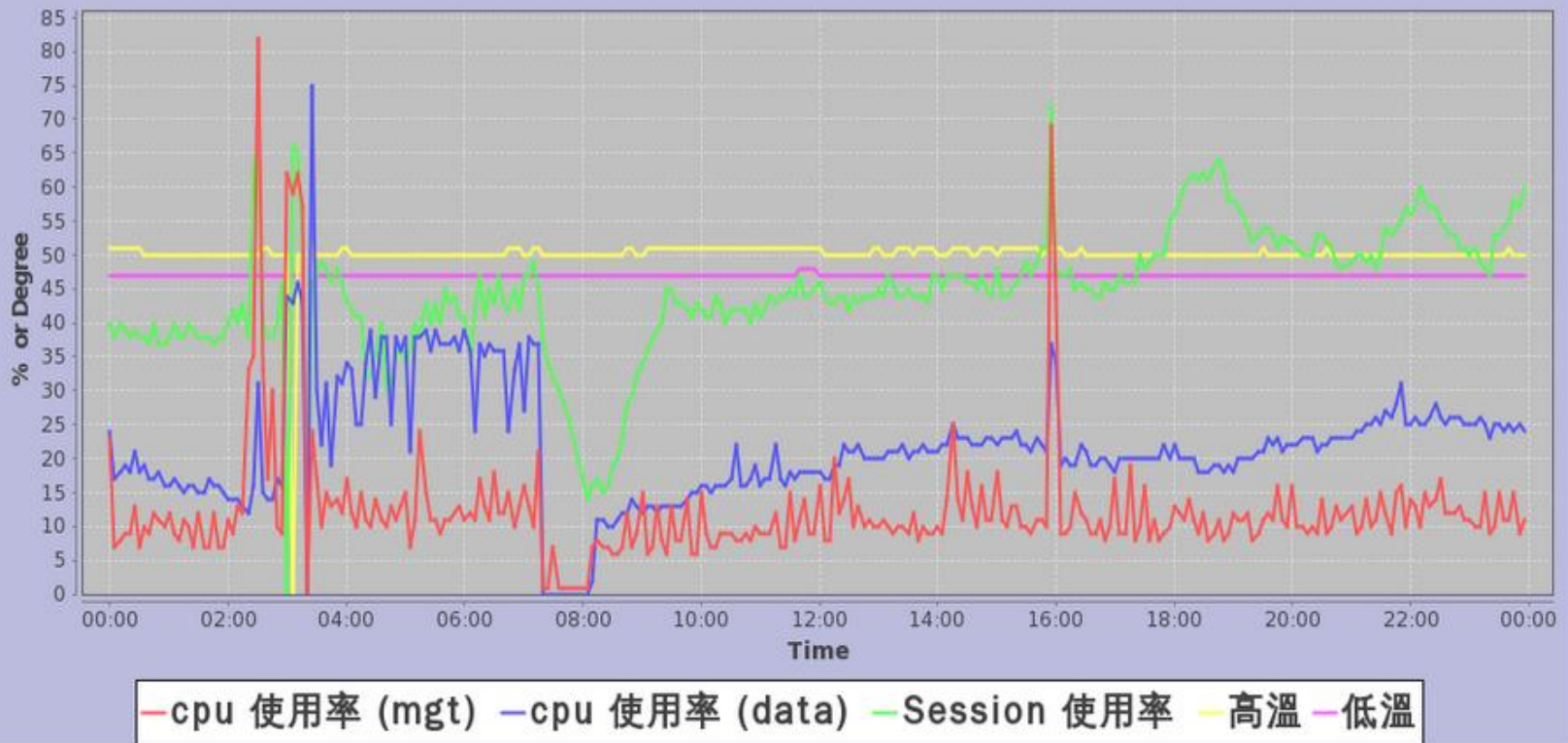




# Paloalto IPS load

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2014-10-05)

系統運作溫度 不可過高, Session使用率 不可過高



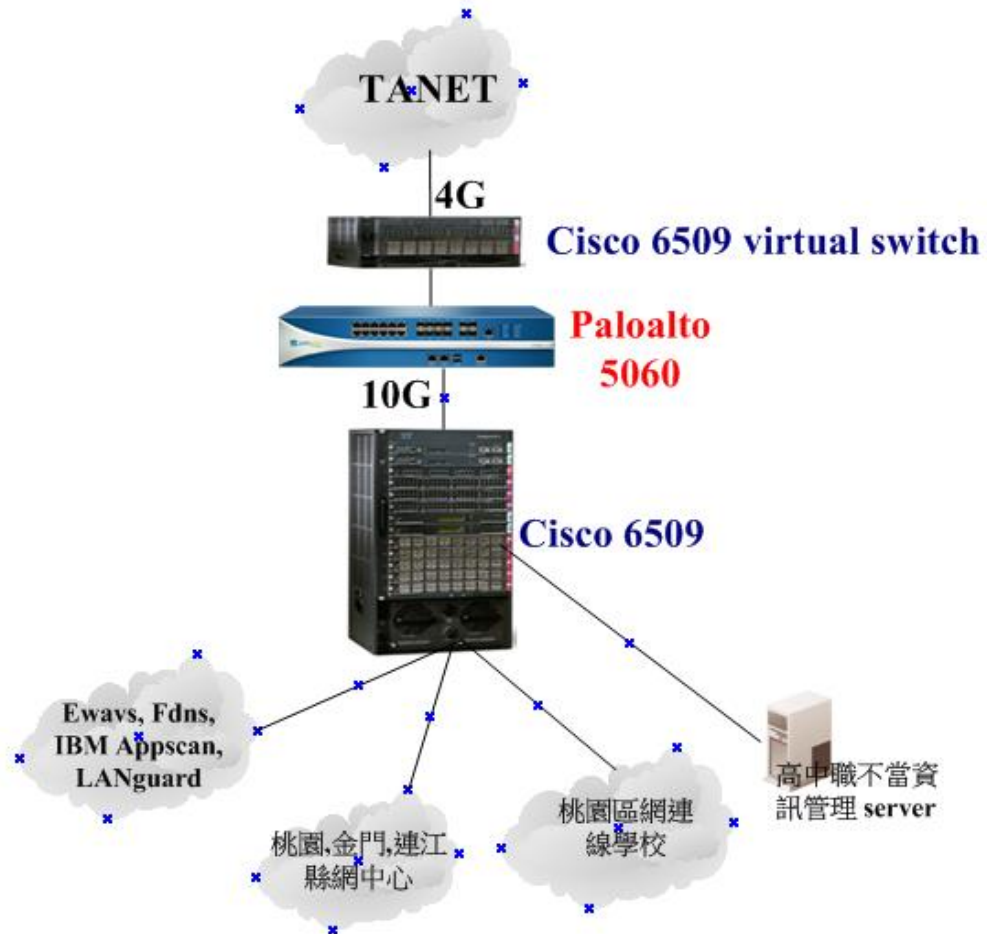


# IPS 及網路調整記錄

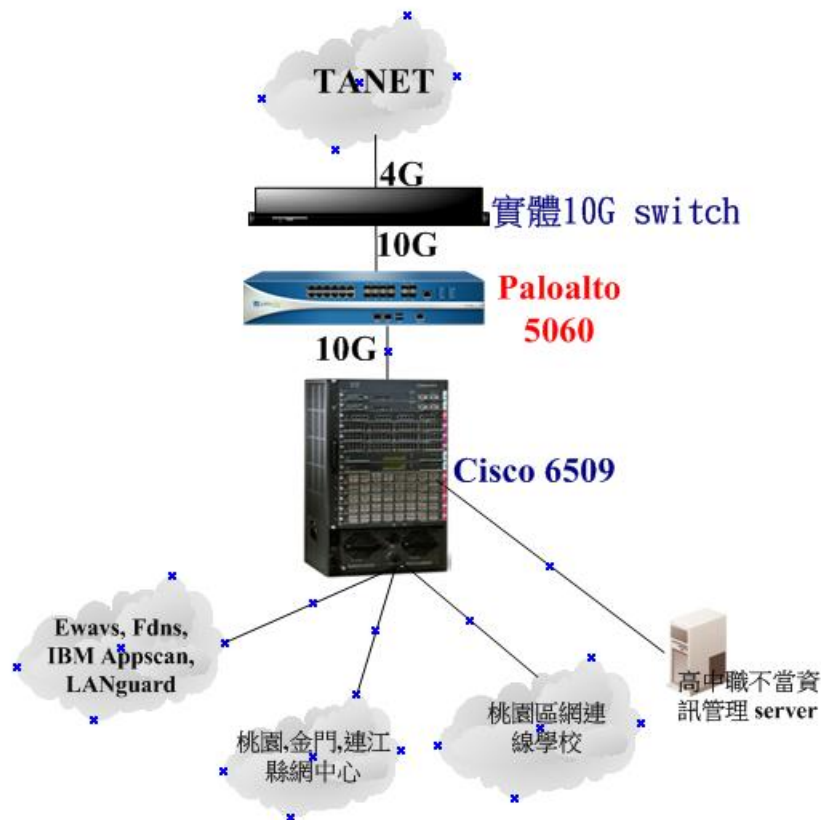
- ❑ 5/16桃園區網IPS設備(paloaloto 5060)受到攻擊, cpu 使用率滿載造成對外網路緩慢.
  - bypass IPS設備後,與IPS介接相關的介面會cache住資料,需手動清除相關cache資料才能回復正常.
- ❑ 5/29(星期四)12:20~14:20 Paloalto5060 IPS 更改設定後重新上線
  - 加入Zone Protection.
- ❑ 6/13(星期五)12:00~14:30 Paloalto5060 IPS 更換設備後重新上線.
  - cisco 6509 在做vlan forwarding 無法正常
- ❑ 6/19(星期四)12:00~14:30 Paloalto5060 IPS 更改設定後重新上線.
  - 為解決 cisco 6509 在做vlan forwarding 的問題,先在6509與骨幹網路之間先串接 1 部10G switch.
- ❑ 9/23元智大學告知到google,淘寶等網站非常緩慢,經檢查確認是中央大學管理學院網路送出大量異常封包,導致桃園區網6509 cpu load 滿載對外連線速度緩慢,先暫時將中央大學管理學院網路隔離,網路恢復正常.



# IPS架構圖(old)



# IPS架構圖 (current)



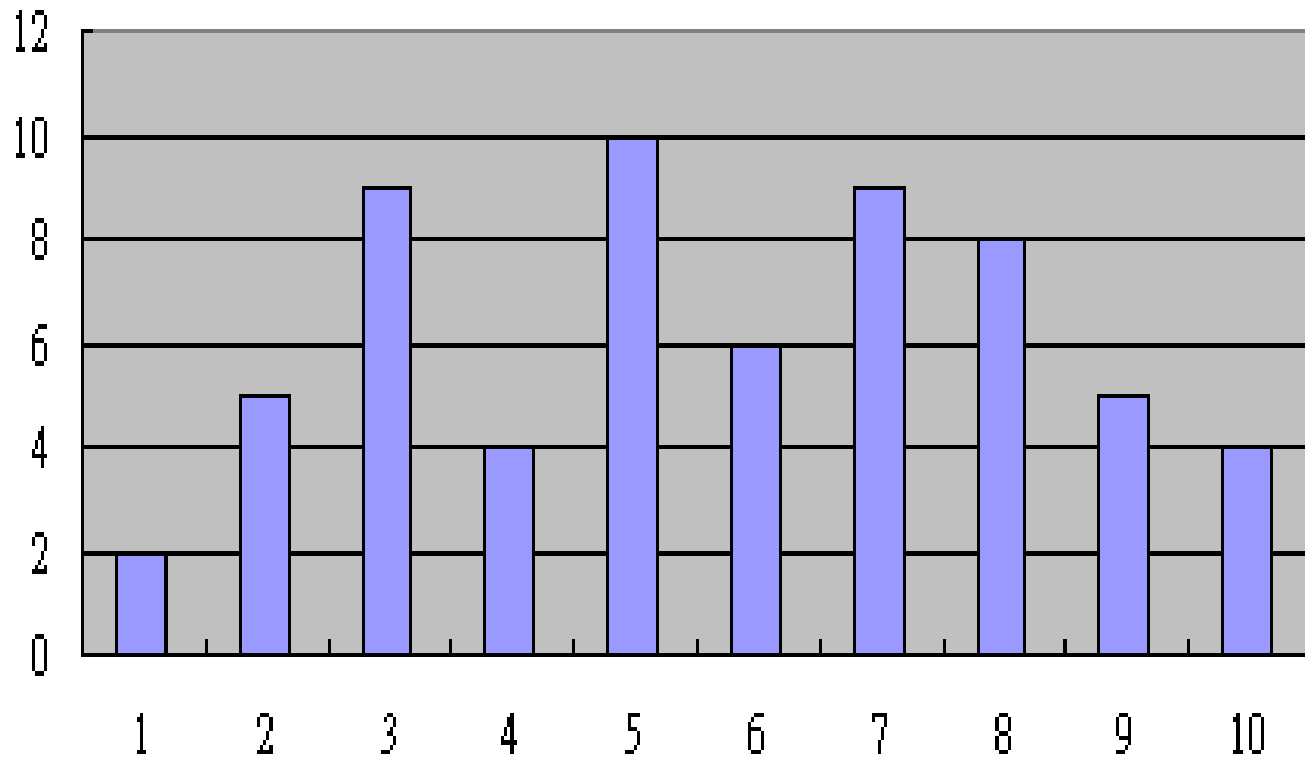


# 資安通報統計





# 智財權統計





# Cloud-based 異常流量偵測

## □ 桃園區網 FDNS (舊)

- • <http://hadoop5.tyc.edu.tw>
- -TopN 流量排行, Top 連結 排行
- -Top UDP 排行 (mysql DB)

## □ 桃園區網 FDNS (新)

- <http://hadoop.tyc.edu.tw/Fdns/>
- -Mongo DB Collections
- -SEARCH 功能





# Cloud-based 異常流量偵測

hadoop.tyc.edu.tw/ | x

hadoop.tyc.edu.tw/Fdns/

國立中央大學

## TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器主機檢查系統\]](#)

INCU (伺服器主機檢查系統) | INCU TopN 流量偵測

### TopN 流量

[TopN 流量排行](#)  
[TopN 流量 \(小時\)](#)

### UDP Flooding 流量監看

[UDP Flooding 流量](#)  
[Connection Flooding 流量](#)

### UDP 詳細流量

[UDP 流量排行](#)  
[Udp 流量 \(小時\)](#)  
[Udp 流量 \(10分鐘\)](#)

### Pscan 異常

[Pscan 異常流量排行](#)  
[Pscan 異常流量 \(小時\)](#)  
[Pscan 異常流量 \(10分鐘\)](#)

### TopP 封包量

[TopP 封包量排行](#)  
[TopP 封包量 \(小時\)](#)  
[TopP 封包量 \(10分鐘\)](#)

### TopC 連接量

[TopC 連接數量排行](#)  
[TopC 連接量 \(小時\)](#)  
[TopC 連接量 \(10分鐘\)](#)

### TCP 異常流量偵測

[密碼猜測 流量](#)  
[Pandora 流量 \(111.111.111.111\)](#)

#### TopN 流量排行

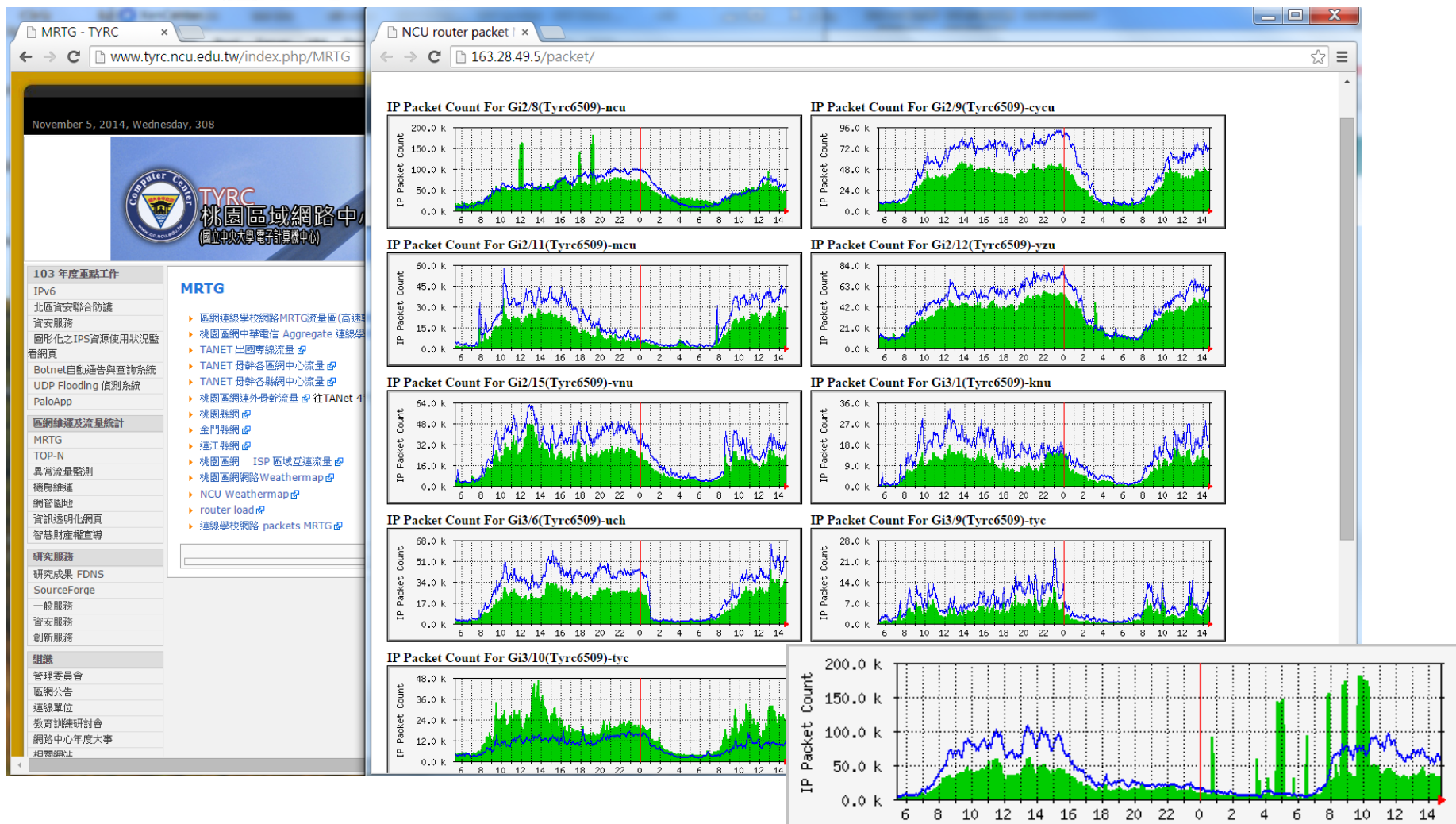
Keyword:

| Oid | IP 位址           | 總流量 (MB) | 輸入流量   | 輸出流量   | 輸入封包長度 | 輸出封包長度 | 持續時間(Hour) |
|-----|-----------------|----------|--------|--------|--------|--------|------------|
| 1   | 140.138.144.170 | 1024825  | 149362 | 875463 | 371    | 1427   | 20         |
| 16  | 120.96.83.24    | 291000   | 125    | 290875 | 53     | 1497   | 16         |
| 17  | 120.124.150.176 | 269399   | 263765 | 5634   | 1488   | 53     | 11         |
| 18  | 220.129.24.72   | 244987   | 1034   | 243953 | 46     | 1484   | 15         |
| 19  | 140.115.77.225  | 238341   | 0      | 238341 | 0      | 464    | 11         |
| 20  | 120.125.11.230  | 227549   | 193661 | 33888  | 1297   | 290    | 17         |
| 22  | 210.60.0.2      | 212373   | 199419 | 12954  | 1317   | 171    | 20         |
| 23  | 120.124.84.102  | 208581   | 201203 | 7378   | 1316   | 78     | 20         |
| 24  | 163.28.5.32     | 199115   | 4117   | 194998 | 51     | 1485   | 20         |
| 25  | 163.28.5.26     | 165303   | 3838   | 161465 | 56     | 1474   | 20         |
| 26  | 163.30.55.100   | 154978   | 0      | 154978 | 0      | 571    | 5          |
| 27  | 163.28.5.27     | 154780   | 4755   | 150025 | 68     | 1456   | 20         |
| 28  | 163.28.5.18     | 154770   | 3465   | 151305 | 53     | 1486   | 20         |
| 29  | 120.125.190.108 | 153149   | 1533   | 151616 | 52     | 1499   | 7          |
| 30  | 163.28.5.17     | 144475   | 3764   | 140711 | 57     | 1474   | 20         |
| 31  | 163.28.5.33     | 143874   | 4108   | 139766 | 62     | 1463   | 20         |
| 32  | 163.28.5.10     | 143814   | 3930   | 139884 | 58     | 1473   | 19         |
| 33  | 163.28.5.25     | 141303   | 3838   | 137465 | 62     | 1471   | 20         |
| 34  | 163.28.5.34     | 137893   | 3631   | 134262 | 57     | 1473   | 20         |

國立中央大學 電算中心



# 管理維運-異常流量偵測






# TANet桃園區網中心—Fdns

tyrc/tanet\_tyrc

← → ↻ 163.25.255.31/Fdns/ ☆ ≡



## TANet 桃園區網 TopN 流量監測

[連線學校 MRTG流量](#) | [IPv6 MRTG流量](#) | [Links連線狀態偵測](#) | [網管工具箱](#) | [伺服器主](#)

[連線器系統](#) | [INCU\(伺服器主\)連線器系統](#) | [INCU TopN 流量偵測](#)

### TopN 流量

[TopN 流量排行](#)  
[TopN 流量 \(小時\)](#)

### UDP Flooding 流量監看

[UDP Flooding 流量](#)  
[Connection Flooding 流量](#)

### UDP 詳細流量

[UDP 流量排行](#)  
[Udp 流量 \(小時\)](#)  
[Udp 流量 \(10分鐘\)](#)

### Pscan 異常

[Pscan 異常流量排行](#)  
[Pscan 異常流量 \(小時\)](#)  
[Pscan 異常流量 \(10分鐘\)](#)

### TopP 封包量

[TopP 封包量排行](#)  
[TopP 封包量 \(小時\)](#)  
[TopP 封包量 \(10分鐘\)](#)

### TopC 連接量

[TopC 連接數量排行](#)  
[TopC 連接量 \(小時\)](#)  
[TopC 連接量 \(10分鐘\)](#)

### TCP 異常流量偵測

[密碼猜測 流量](#)  
[Pandora 流量 \(111.111.111.111\)](#)

TopP 封包量排行 (10分鐘)

Keyword:


| IP 位址          | 輸入流量(MB) | 輸出流量 | 輸入連接數 | 輸出連接數  | 輸入封包長度 | 輸出封包長度 | 輸入封包量   | 輸出封包量    | 紀錄時間        |
|----------------|----------|------|-------|--------|--------|--------|---------|----------|-------------|
| 163.30.80.253@ | 2778     | 84   | 5248  | 9819   | 1442   | 58     | 1926337 | 1446433  | 11-05 10:10 |
| 163.30.20.45@  | 362      | 1403 | 190   | 340    | 545    | 696    | 664382  | 2013495  | 11-05 10:10 |
| 163.28.5.34@6  | 79       | 2989 | 7840  | 2674   | 56     | 1468   | 1409838 | 2035401  | 11-05 10:10 |
| 163.28.5.33@6  | 107      | 3280 | 20578 | 6333   | 56     | 1482   | 1908352 | 2212938  | 11-05 10:10 |
| 163.28.5.32@6  | 96       | 5187 | 8694  | 2758   | 48     | 1480   | 1970315 | 3504723  | 11-05 10:10 |
| 163.28.5.27@6  | 79       | 3010 | 10412 | 3286   | 56     | 1485   | 1424072 | 2026131  | 11-05 10:10 |
| 163.28.5.19@6  | 92       | 3521 | 17592 | 5678   | 64     | 1479   | 1434001 | 2380341  | 11-05 10:10 |
| 163.25.34.50@  | 8955     | 165  | 4683  | 12876  | 1493   | 56     | 5997934 | 2906944  | 11-05 10:10 |
| 163.25.155.16@ | 2283     | 106  | 9668  | 25915  | 1361   | 67     | 1677649 | 1563073  | 11-05 10:10 |
| 163.25.131.1@  | 0        | 3096 | 0     | 4      | 1079   | 45     | 0       | 67313754 | 11-05 10:10 |
| 140.138.144.17 | 288      | 8090 | 9230  | 16012  | 99     | 1427   | 2893735 | 5669059  | 11-05 10:10 |
| 140.135.66.45@ | 45       | 2506 | 179   | 252    | 46     | 832    | 982985  | 3011705  | 11-05 10:10 |
| 140.135.66.33@ | 87       | 165  | 7292  | 5825   | 49     | 92     | 1769441 | 1791415  | 11-05 10:10 |
| 140.115.145.1@ | 0        | 83   | 0     | 3      | 1308   | 50     | 0       | 1637976  | 11-05 10:10 |
| 140.109.66.227 | 0        | 340  | 0     | 1      | 46     | 46     | 0       | 7322707  | 11-05 10:10 |
| 120.125.11.23@ | 5647     | 681  | 63836 | 137281 | 1328   | 206    | 4249729 | 3292238  | 11-05 10:10 |
| 120.125.11.20@ | 2110     | 142  | 28238 | 58331  | 1353   | 120    | 1558867 | 1184039  | 11-05 10:10 |
| 120.124.84.36@ | 6244     | 222  | 12055 | 26654  | 1396   | 67     | 4470695 | 3321447  | 11-05 10:10 |
| 74.125.23.116@ | 1255     | 59   | 53    | 28     | 766    | 46     | 1637294 | 1284191  | 11-05 10:00 |

國立中央大學 電算中心



# TANet桃園區網中心—Fdns

← → ↻ 163.25.255.31/Fdns/ ☆ ☰



## TANet 桃園區網 TopN 流量監測

[連線學校 MRTG流量1](#) [IPv6 MRTG流量1](#) [Links 連線狀態偵測](#) [網管工具箱](#) [伺服器](#)

[連線學校 MRTG流量1](#) [IPv6 MRTG流量1](#) [Links 連線狀態偵測](#) [網管工具箱](#) [伺服器](#)

TopN 流量

TopN 流量排行

TopN 流量 (小時)

UDP Flooding 流量監看

UDP Flooding 流量

Connection Flooding 流量

UDP 詳細流量

UDP 流量排行

Udp 流量 (小時)

Udp 流量 (10分鐘)

Pscan 異常

Pscan 異常流量排行

Pscan 異常流量 (小時)

Pscan 異常流量 (10分鐘)

TopP 封包量

TopP 封包量排行

TopP 封包量 (小時)

TopP 封包量 (10分鐘)

TopC 連接量

TopC 連接數量排行

TopC 連接量 (小時)

TopC 連接量 (10分鐘)

TCP 異常流量偵測

密碼猜測 流量

Pandora 流量 (111.111.111.111)

TopP 封包量排行 (10分鐘)

Keyword: 163.25.131.1

| IP 位址           | 輸入流量(MB) | 輸出流量 | 輸入連接數 | 輸出連接數 | 輸入封包長度 | 輸出封包長度 | 輸入封包量    | 輸出封包量       | 紀錄時間 |
|-----------------|----------|------|-------|-------|--------|--------|----------|-------------|------|
| 163.25.131.1@ 0 | 2964     | 0    | 3     | 1210  | 46     | 0      | 64449728 | 11-05 10:20 |      |
| 163.25.131.1@ 0 | 3096     | 0    | 4     | 1079  | 45     | 0      | 67313754 | 11-05 10:10 |      |
| 163.25.131.1@ 0 | 1548     | 0    | 1     | 72    | 46     | 0      | 33652216 | 11-05 10:00 |      |
| 163.25.131.1@ 0 | 4569     | 0    | 6     | 1122  | 45     | 0      | 99342302 | 11-05 09:50 |      |
| 163.25.131.1@ 0 | 3099     | 0    | 3     | 1460  | 45     | 0      | 67380932 | 11-05 09:40 |      |
| 163.25.131.1@ 0 | 2970     | 0    | 4     | 1376  | 45     | 0      | 64579286 | 11-05 09:00 |      |
| 163.25.131.1@ 0 | 3108     | 0    | 2     | 1301  | 46     | 0      | 67584651 | 11-05 08:50 |      |
| 163.25.131.1@ 0 | 1552     | 0    | 1     | 947   | 46     | 0      | 33754741 | 11-05 08:40 |      |
| 163.25.131.1@ 0 | 195      | 0    | 2     | 1299  | 46     | 0      | 4255102  | 11-05 08:10 |      |
| 163.25.131.1@ 0 | 3818     | 0    | 6     | 1291  | 45     | 0      | 83007897 | 11-05 07:50 |      |
| 163.25.131.1@ 0 | 2693     | 0    | 4     | 1019  | 1282   | 0      | 2099721  | 11-05 07:40 |      |
| 163.25.131.1@ 0 | 2117     | 0    | 1     | 1359  | 1152   | 0      | 1837371  | 11-05 07:30 |      |
| 163.25.131.1@ 0 | 381      | 0    | 2     | 206   | 46     | 0      | 8300202  | 11-05 05:40 |      |
| 163.25.131.1@ 0 | 4041     | 0    | 11    | 194   | 93     | 0      | 43357039 | 11-05 05:10 |      |
| 163.25.131.1@ 0 | 4265     | 0    | 5     | 165   | 49     | 0      | 85618606 | 11-05 05:00 |      |
| 163.25.131.1@ 0 | 3848     | 0    | 5     | 99    | 46     | 0      | 83670507 | 11-05 04:50 |      |
| 163.25.131.1@ 0 | 1895     | 0    | 2     | 68    | 46     | 0      | 41200737 | 11-05 04:40 |      |
| 163.25.131.1@ 0 | 490      | 0    | 3     | 60    | 45     | 0      | 10657303 | 11-05 04:10 |      |
| 163.25.131.1@ 0 | 649      | 0    | 3     | 320   | 96     | 0      | 6743434  | 11-05 03:40 |      |

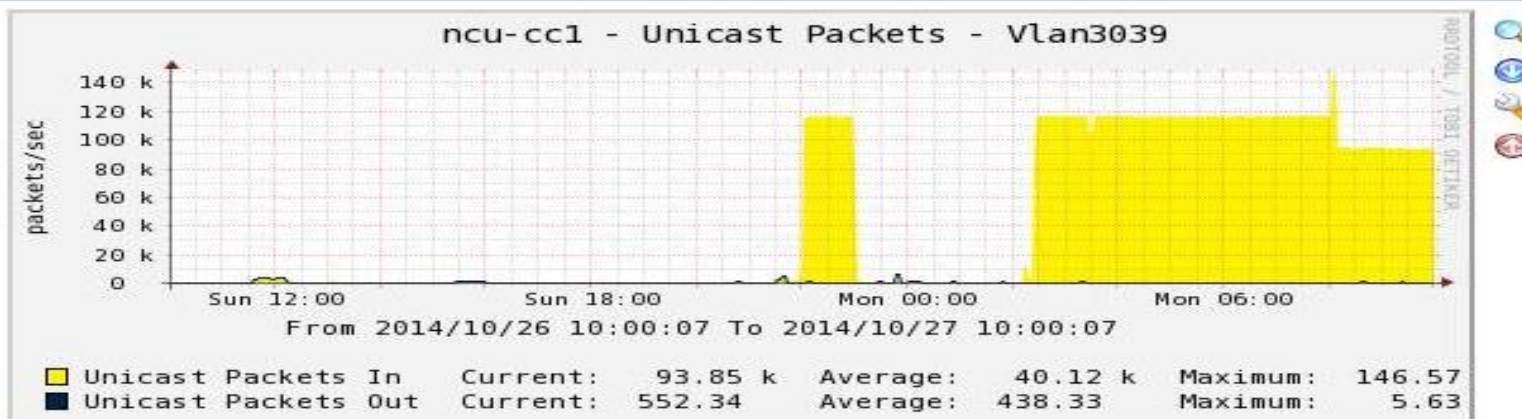
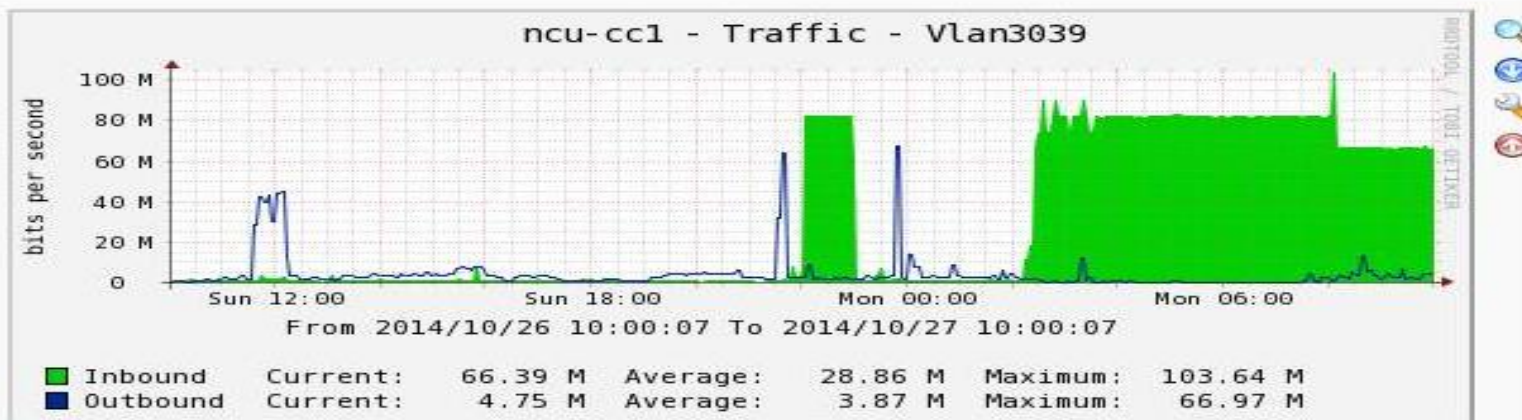
國立中央大學 電算中心





# 異常packet流量

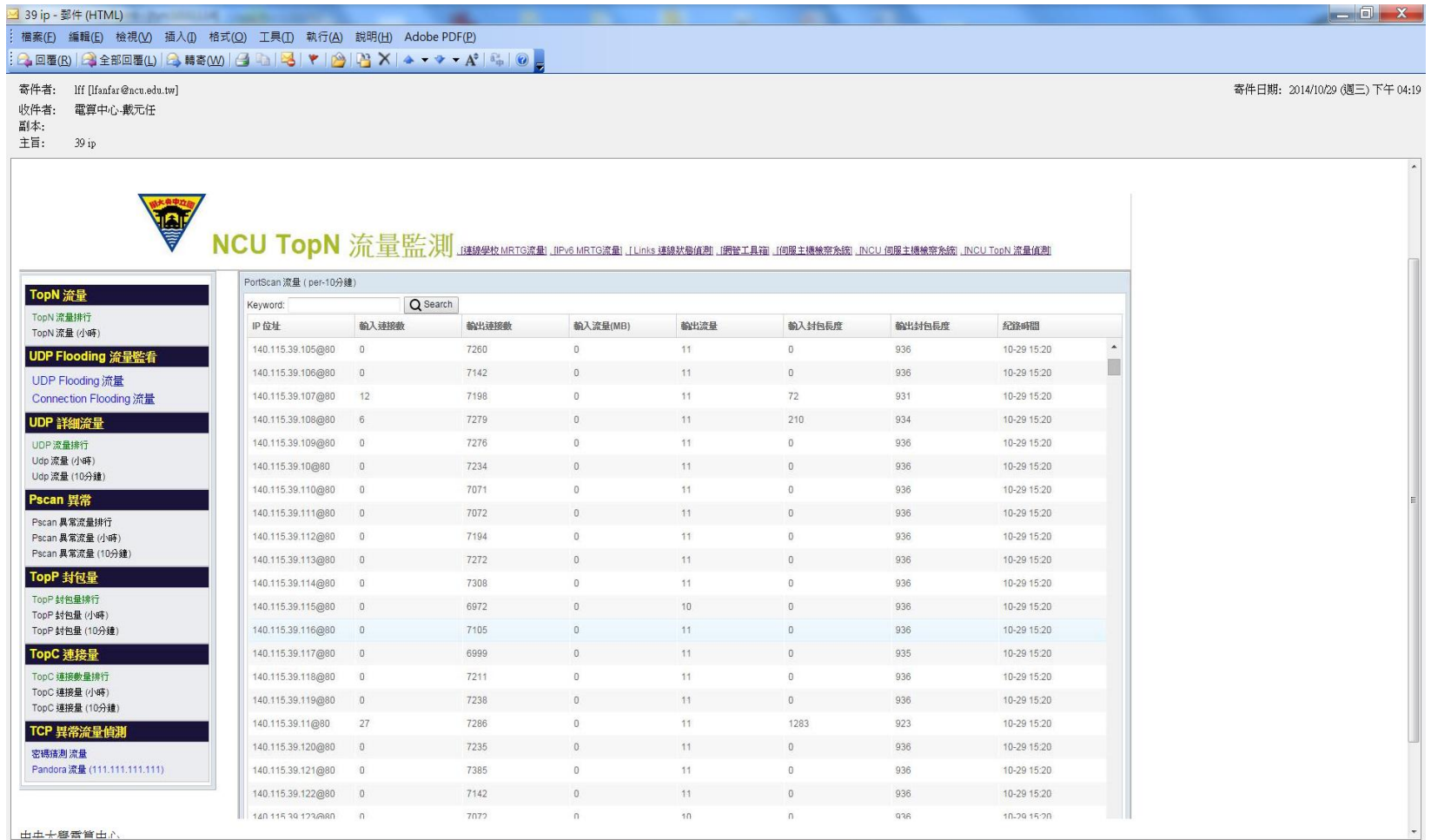
Mrtg:







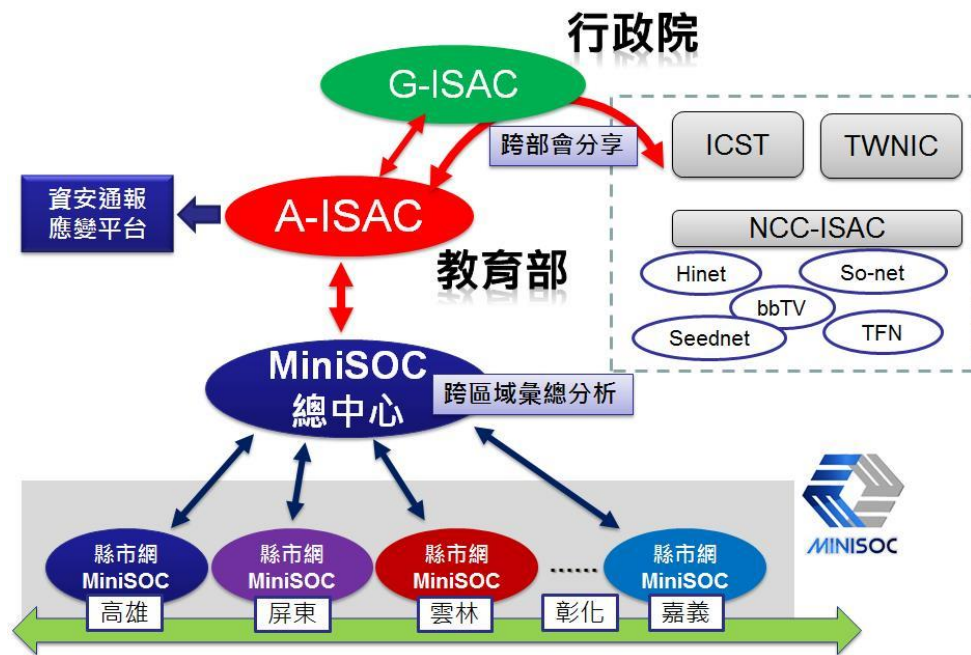
# 異常packet流量(假冒ip)



Cisco router : ip verify unicast source reachable-via rx

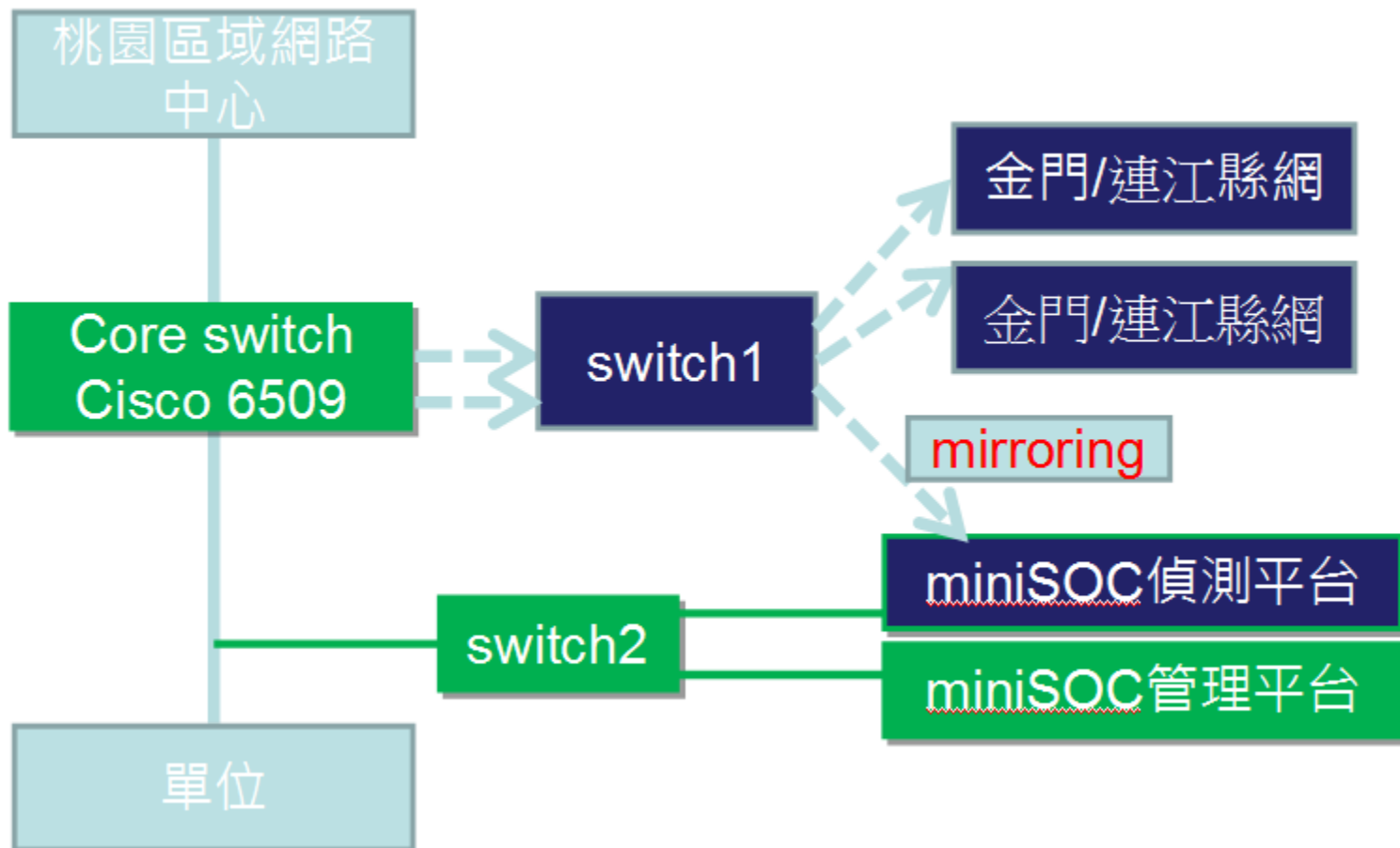
# 資安防禦MiniSOC平台建置

- 本計畫將依教育部資科司之規畫，完成金門縣及連江縣網中心MiniSOC之佈建。
- 進行不同區域之資安事件分析，並將這些深層分析結果透過MiniSOC與其分享模組機制落實協同防禦的目標。





# 資安防禦MiniSOC平台建置





# 建議

---

□ 對Tanet 及教育部的建議

➤ [center25@cc.ncu.edu.tw](mailto:center25@cc.ncu.edu.tw)



# Computer Center, National Central University.



***Thank You!***