

桃園區網中心 第47次管理委員會

國立中央大學電算中心
100年11月15日



現況報告

- ☐ 表揚桃園區網中心-100年度TANet傑出貢獻人員之推薦人員
- ☐ 區網中心提供之資訊安全檢測狀況
- ☐ Ewavs網站弱點監測平台檢測數量
- ☐ 年度服務滿意調查
- ☐ 教育訓練及資安推廣課程
- ☐ 資安事件之處理原則



桃園區網中心傑出貢獻人員提名表揚

□ 桃園區網中心提名名單：

➤ 應用推廣類

- 中原大學 電子計算機中心 - 張耀仁 主任
- 長庚大學 資訊管理系 - 張錦特 教授
- 金門縣政府教育局網路中心 - 陳佳瓏 老師

➤ 管理維護類

- 桃園縣政府教育局網路中心 - 王良海 先生



資訊安全網站檢測

- 目前已經檢測完畢，將陸續發送Email信件通知申請之單位申請人。



Ewavs 網站弱點監測平台服務統計

□ Ewavs網站弱點監測平台檢測數量

年/月份	會員申請單月總計	申請檢測網站總計
2011年10月份	1件	10
2011年09月份	0件	11
2011年08月份	0件	2
2011年07月份	1件	6
2011年06月份	9件	12
2011年05月份	0件	9
2011年04月份	0件	0
2011年03月份	35件	14
2011年02月份	0件	6
2011年01月份	0件	7



年度服務滿意調查

☐ 年度滿意調查

<http://www.tyrc.ncu.edu.tw/year>

☐ 填寫時間：即日起至11月30日



教育訓練及資安推廣課程

□ 教育訓練課程

100/04/26-伺服器主機檢查系統之建置與使用

(中央大學-電算中心楊素秋 @新生醫專 -第45次區網會議)

100/06/11-100年度校園網路管理暨自由軟體應用研討會@連江縣教育網路中心

1. 軟體測試-(中央大學-資訊工程所 鄭永斌副教授)

2. Service Desk 與 MediaWiki共筆平台編輯課程(中央大學-電算中心 吳鏐美)

3. 教育單位網站弱點分析監測平台簡介(中央大學-電算中心 邱惠隆)

4. 伺服器主機檢查系統之建置與使用(中央大學-電算中心 楊素秋)

100/06/15-現代網路攻擊模式與網路安全使用手則

(石謂龍(HP TippingPoint資安技術顧問) @中央大學志希館-I210會議室)

100/06/29-系統備份使用自由軟體 (Bacula)

(邱健雄先生(自由軟體鑄造場專案經理)@中央大學志希館-I210會議室)

100/07/07-輕鬆建置Nagios網路監控主機

(黃俊宏(GNOME Asia Committee member) @中央大學志希館-I210會議室)

100/07/15-IPv6協定與應用服務介紹

(王士康先生(中華電信研究所 寬網室@中央大學志希館-I210會議室)



教育訓練及資安推廣課程

□ 教育訓練課程(續)

100/08/12-雲端電腦教室-自由軟體的實現模式

(蔡德明先生(鳥哥的Linux私房菜 作者)公司 營運長) @中央大學 志希館-I210會議室)

100/10/31-安心利用網路內容：從公眾授權概念談起

(OFFS 葛冬梅講師 -自由軟體鑄造廠 @國立中央大學 中正圖書館(舊圖)二樓 團體視聽室)

100年11月3日「TWNIC網路管理研習計畫」中央大學場-第一場

100年11月12日「TWNIC網路管理研習計畫」中央大學場-第二場

100年11月14日「TWNIC網路管理研習計畫」元智大學場-第三場(僅該校師生)

100年11月15日「TWNIC網路管理研習計畫」啟英高中場-第四場

100年11月30日「TWNIC網路管理研習計畫」清雲科大場-第五場(僅該校師生)

100年12月01日「TWNIC網路管理研習計畫」南亞技術學院場-第六場



教育訓練及資安推廣課程

□ 高中職資訊安全推廣

- 100年02月23日 - 治平中學(學生)
(南亞技術學院電算中心 林文彬老師 資訊安全簡述)
- 100年03月09日 - 清華中學(學生)
(核能研究所 鄭勝璋老師 - 資訊安全防護)
- 100年05月12日 - 治平中學(教職員)
(核能研究所 鄭勝璋老師-資訊安全防護)
- 100年10月18日 - 中壢高商資訊科 (網域及資安推廣)
- 100年10月26日 - 龍潭農工 (網域及資安推廣)
- 100年10月28日 - 泉僑中學資訊科 (網域及資安推廣)
- 100年10月31日 - 振聲中學資訊科 (網域及資安推廣)
- 100年11月04日 - 啟英高中資訊科 (網域及資安推廣)
- 100年11月09日 - 新生醫專資訊社(網域及資安推廣)
- 100年11月11日 - 中壢家商資訊科(網域及資安推廣)



資安事件之處理原則

- ❑ 若單位發生嚴重資安事件需要憲、警、調人員進入學校調查，請確認是否出具正式文件。
- ❑ 請主管單位視情況陪同及釐清事件責任歸屬，並請區縣市網路中心協助單位後續事件處理、跡證保存等鑑識事宜。
- ❑ 立即通報本部電算中心資安人員，可協助派遣鑑識人員協助單位進行數位鑑識以釐清責任歸屬。



北區 **A-SOC** 進度及資安通報演練

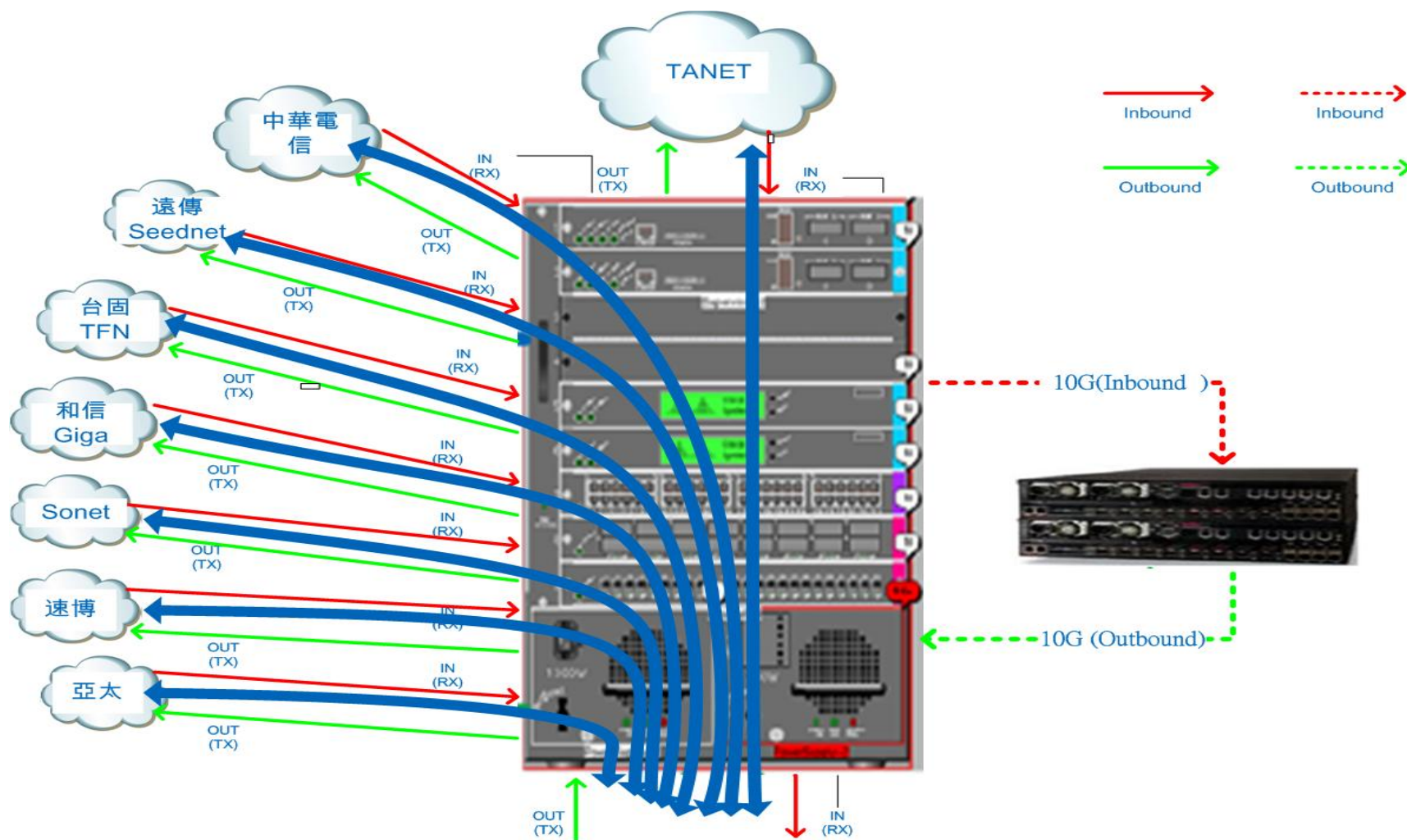
國立中央大學電算中心
100年11月15日



報告大綱

- ☐ 北區A-SOC系統運作進度
- ☐ 資安通報演練

桃園區網IPS規劃架構



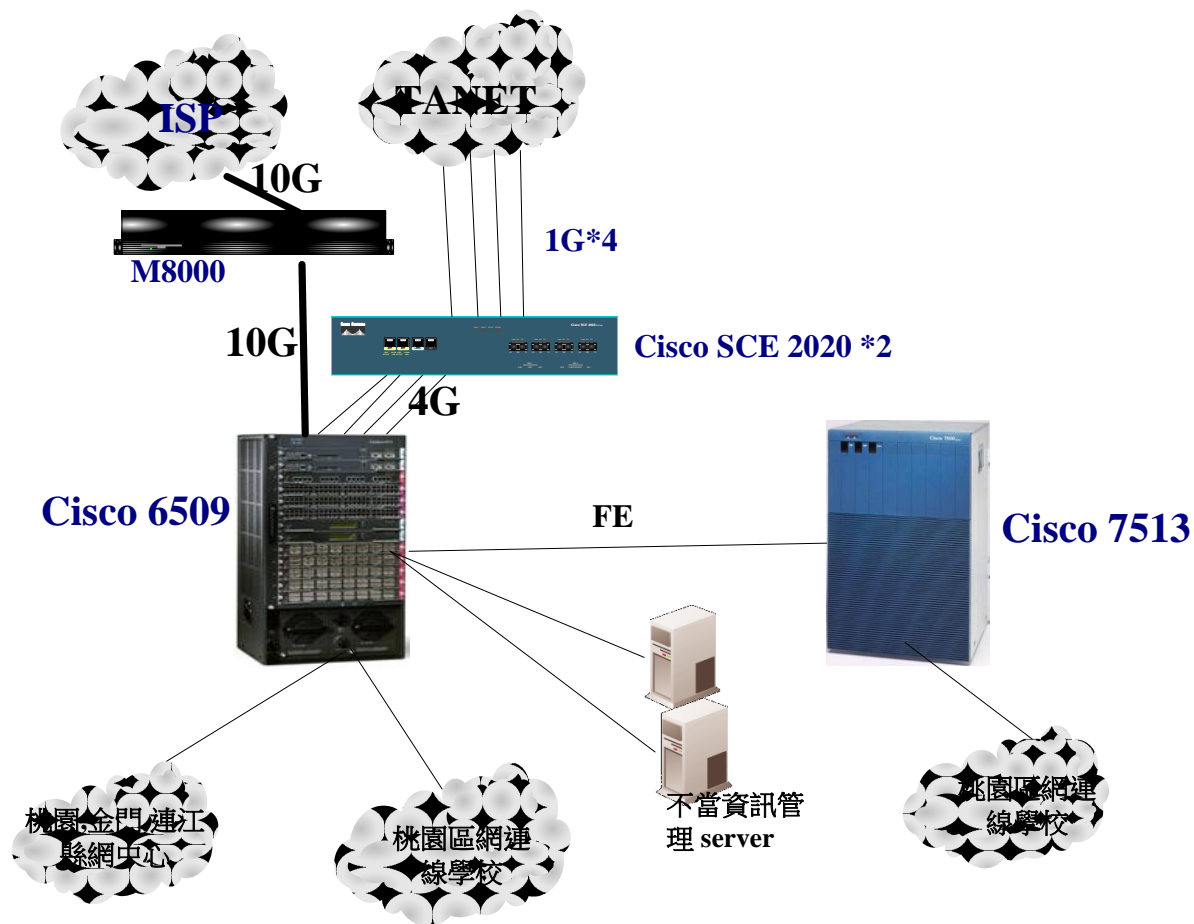


問題

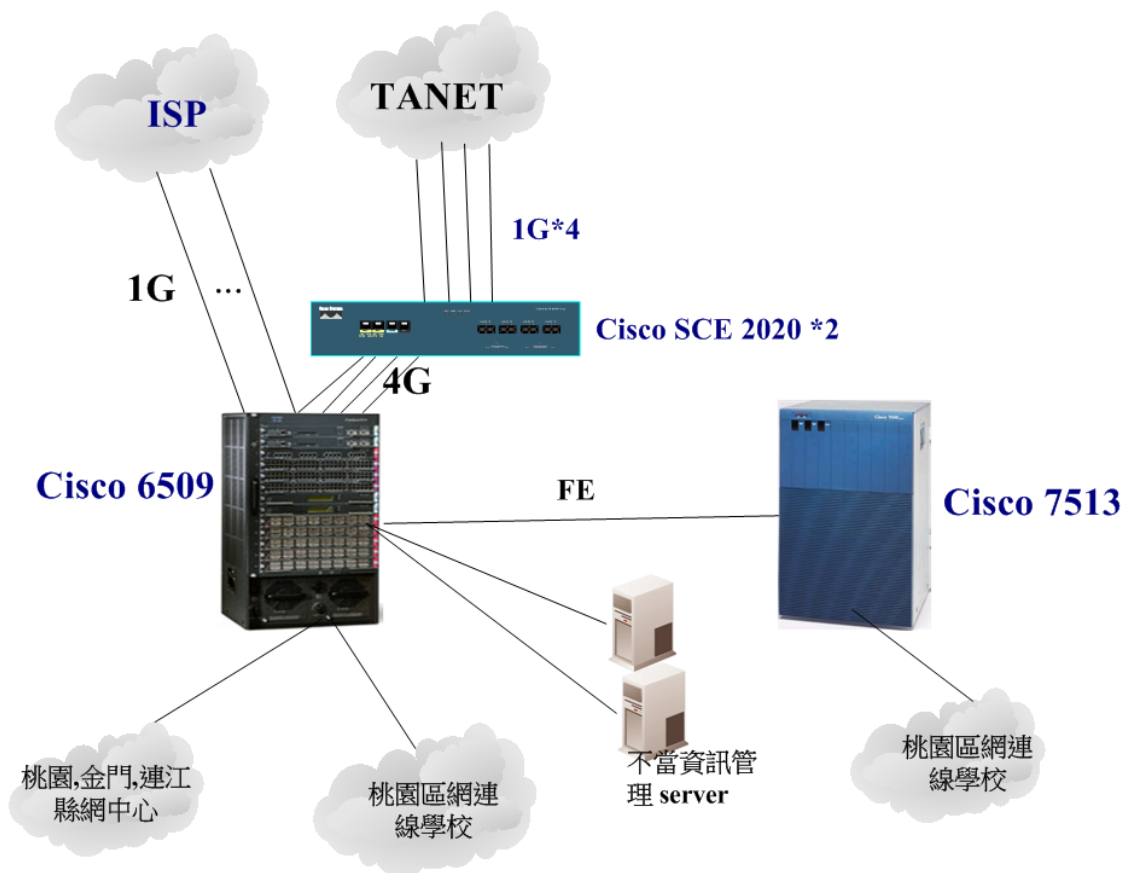
- ☐ 在5/7 23:40 到5/8 00:40 桃園區網到tanet 骨幹斷線
- ☐ 6/30 09:40 ~10:00 骨幹斷線
- ☐ 7/20 15:10 ~15:50 區網對外網路連線緩慢
- ☐ 解決:bypass IPS及clear arp



IPS 架構調整-bypass Tanet



IPS 架構調整-bypass Tanet及isp



- 台大希望桃園區網流量導入ASOC
- 10/19 將Tanet及isp所有對外連線流量 mirror到 M8000 IPS設備

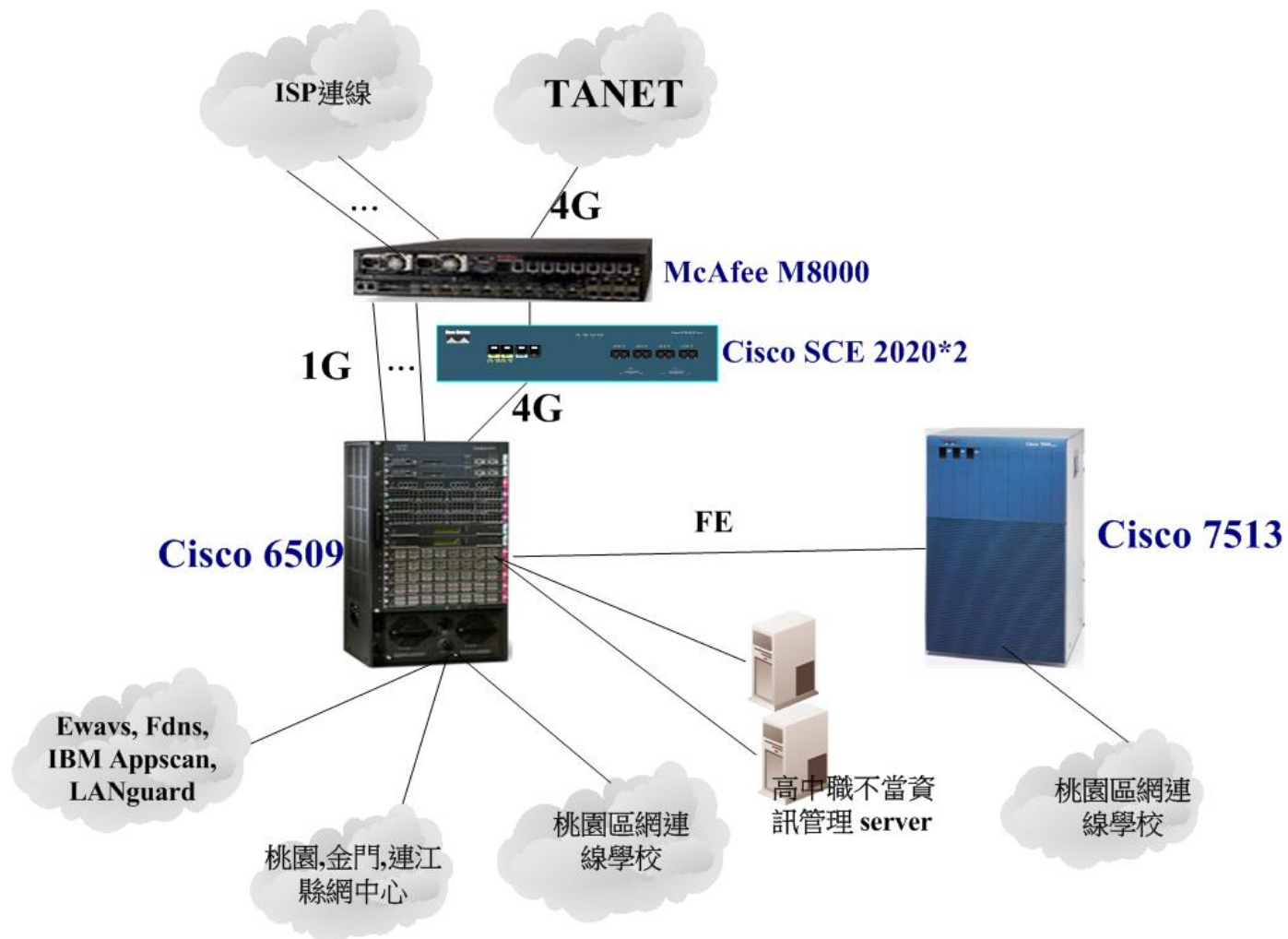


流量導入ASOC後之問題?

- ❑ IPS M8000管理server NSM多次停止送出log 資料給ASOC.
- ❑ IPS M8000或 NSM有問題?
- ❑ McAfee原廠 提出改善方案
 - NSM 改成2008 server 英文版(11/10已完成)
 - 解決M8000主機loading 過重問題:
 - Http scanning response 超過 80 %, 建議disable
 - 'Bridge Vlan' 更改成VLAN interface
 - 台大試行一組合適穩定的policy ,再導入中央,最後希望以in-line mode維運



VLAN interface 架構





100教育體系資安通報演練

- ❑ 演練時間:10/6到10/14
- ❑ 桃園區網收到35件演練事件
- ❑ 評分

給分標準	3	2	1	0
評分項目				
及時率	時限內完成	24 小時內完成	完成通報	未完成
完成率	時限內完成	(時限+4 小時) 內完成	(時限+8 小時) 內完成	未完成
正確率	至少 2 個資安聯絡人所有欄位資料均填寫正確	至少 2 個資安聯絡人少數欄位資料未填寫正確	只填寫 1 位資安聯絡人但資料完整	只填寫 1 位資安聯絡人且資料也不完整

學校	及時率	是否依通報應變流程時限內完成通報
	完成率	是否依通報應變流程時限內完成處理
	正確率	單位聯絡人資料準確度及完整性



83th TANET技術小組討論議題

桃園區網中心

2011-11-08



OUTLINE

- ❑ 1. DNSSEC 推廣佈建
- ❑ 2. 惡意網站威脅來源阻擋機制
- ❑ 3. edu.tw domain
- ❑ 4. 資安防護設備運作現況



1. DNSSEC 推廣佈建

□ DNSSEC

- DNS Security Extension
- 可與 DNS 並行
 - Windows 7 DNS
- 2010 July
 - Root DNS server

□ 教育訓練 Training

- TWNIC
- TANET 技術小組



2. 惡意網站威脅來源阻擋機制



- ☐ 目前國外網路攻擊
- ☐ 惡意網站威脅來源阻擋機制
- ☐ 單位分工及職責
- ☐ 惡意網站威脅來源名單
- ☐ 國外單位申訴
- ☐ 惡意網站威脅來源阻擋之執行
 - Abuse 佈建機制



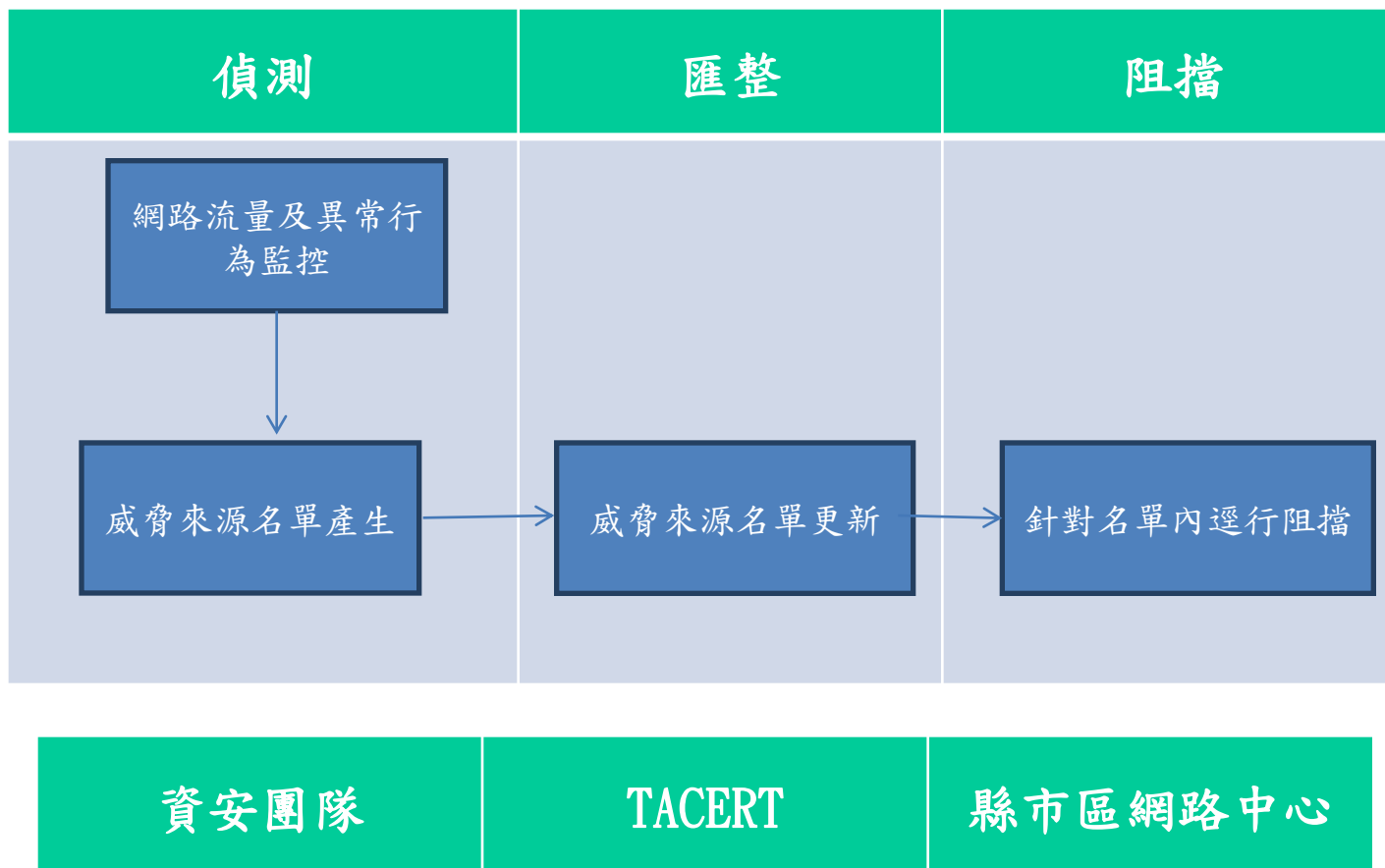
2.惡意網站威脅來源阻擋機制(cont.)

□ 目前國外網路攻擊

- 每月有超過5000萬筆的網路攻擊行為來自海外
 - 包含釣魚網站、網頁掛碼、網路掃描、密碼暴力破解…等網路攻擊行為等。
- 為阻擋來自國際的網路攻擊
 - TACERT規劃『惡意網站威脅來源阻擋機制』
 - 希望降低這些惡意網站與威脅來源所帶來的危害以及潛在風險，維護學術網路的網路安全。



2. 惡意網站威脅來源阻擋機制(cont.)





2.惡意網站威脅來源阻擋機制(cont.)

□ 單位分工及職責

➤ 資安團隊：

- 教育部資安計畫團隊，負責網路流量及異常行為監控
- 將偵測到之威脅來源產出名單及佐證資料，提供給TACERT

➤ TACERT：

- 匯整更新威脅來源名單
- 公告威脅來源名單
- 提供技術支援及問題處理
- 進行橫向聯繫作業



2. 惡意網站威脅來源阻擋機制(cont.)

➤ 縣市區網中心：

- 各區縣市網資訊人員自行根據『惡意網站威脅來源名單』
 - 於現有『TANet不當資訊防治機制』的資安設備上進行阻擋。
- 提供偵測到之威脅來源名單給TACERT



2.惡意網站威脅來源阻擋機制(cont.)

❑ 惡意網站威脅來源名單執行狀況

- 從100年9月底開始執行採每週更新
- 至100/11/01已更新五次，共有筆數595筆
- 目前來源由臺中市網，S-ASOC，N-ASOC所提供

❑ 國外單位申訴

- 透過TWCERT或是直接透過TACERT
 - 反應其IP被封鎖。
- TACERT乃.edu.tw之對外窗口。
- TACERT將會請原情資提供單位提出佐證資料，再轉送給該國外申訴單位。



2.惡意網站威脅來源阻擋機制(cont.)

項次	討論事項	事項說明
1	惡意網站威脅來源名單的 門檻值 設定	針對攻擊次數累計每週超過 10000次 的惡意網站威脅來源的名單，由TACERT統一通報國際CERT組織並通知ABUSE。
2	惡意網站威脅來源名單的 限制時間及名單數量	針對國外對TANet進行攻擊次數累計每週超過10000次的IP清單，將限制該IP與TANet連接 1個月 ，考量路由器負載將限制IP數量控制在 500筆 以內。
3	惡意網站威脅來源之 阻擋機制	威脅阻擋機制由教育部ABUSE機制阻擋或是通知各區縣（市）網阻擋較為合適？



3. edu.tw domain

- ❑ edu.tw domain
 - 註冊 ISP IP range
- ❑ 亞卓市
 - Hinet
 - Abuse 比率偏高
- ❑ Others



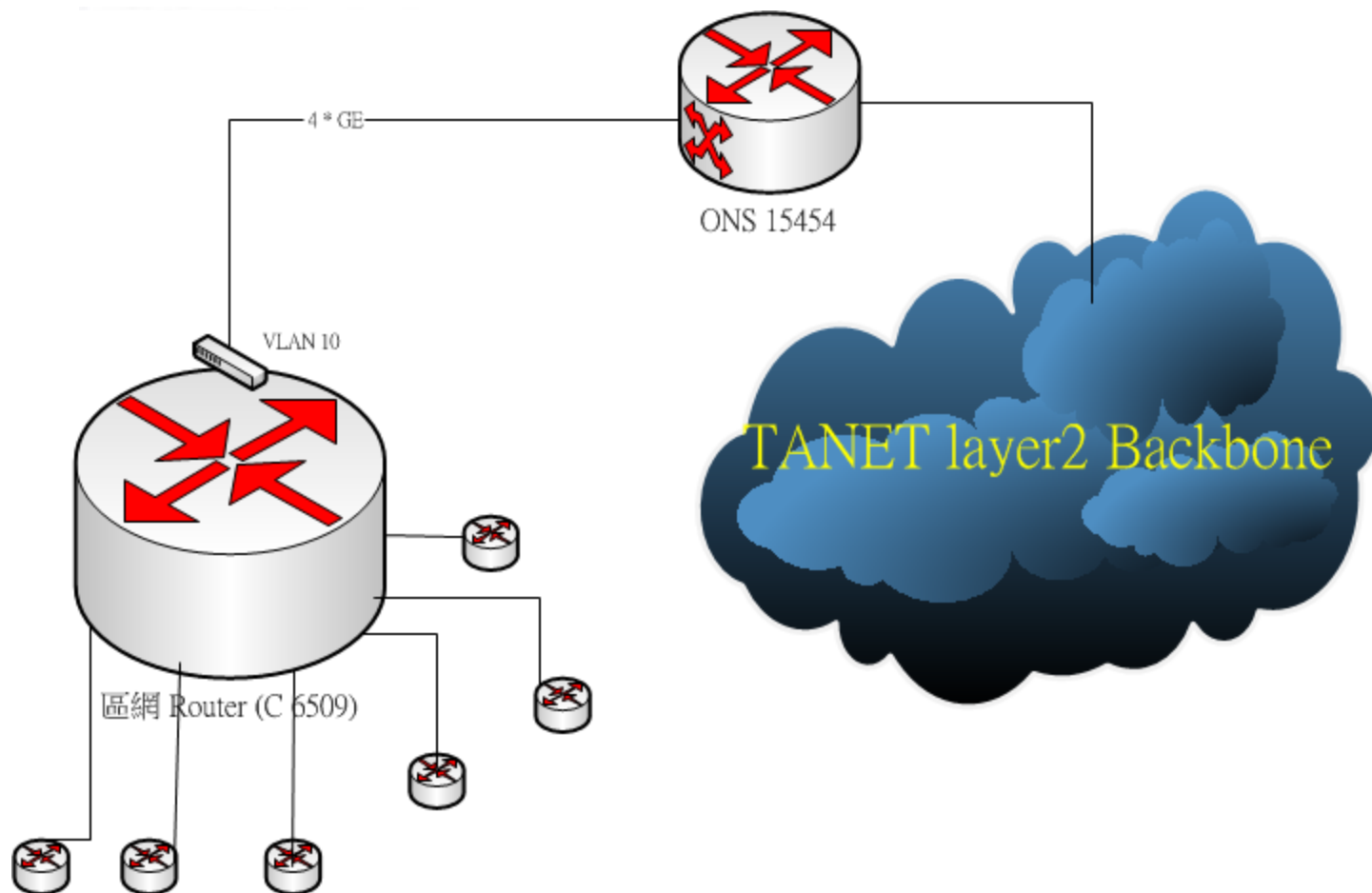
4. 資安防護設備運作現況



- 桃園區網連外網路
- _P2P訊務阻擋系統
- _惡意攻擊偵測與阻擋

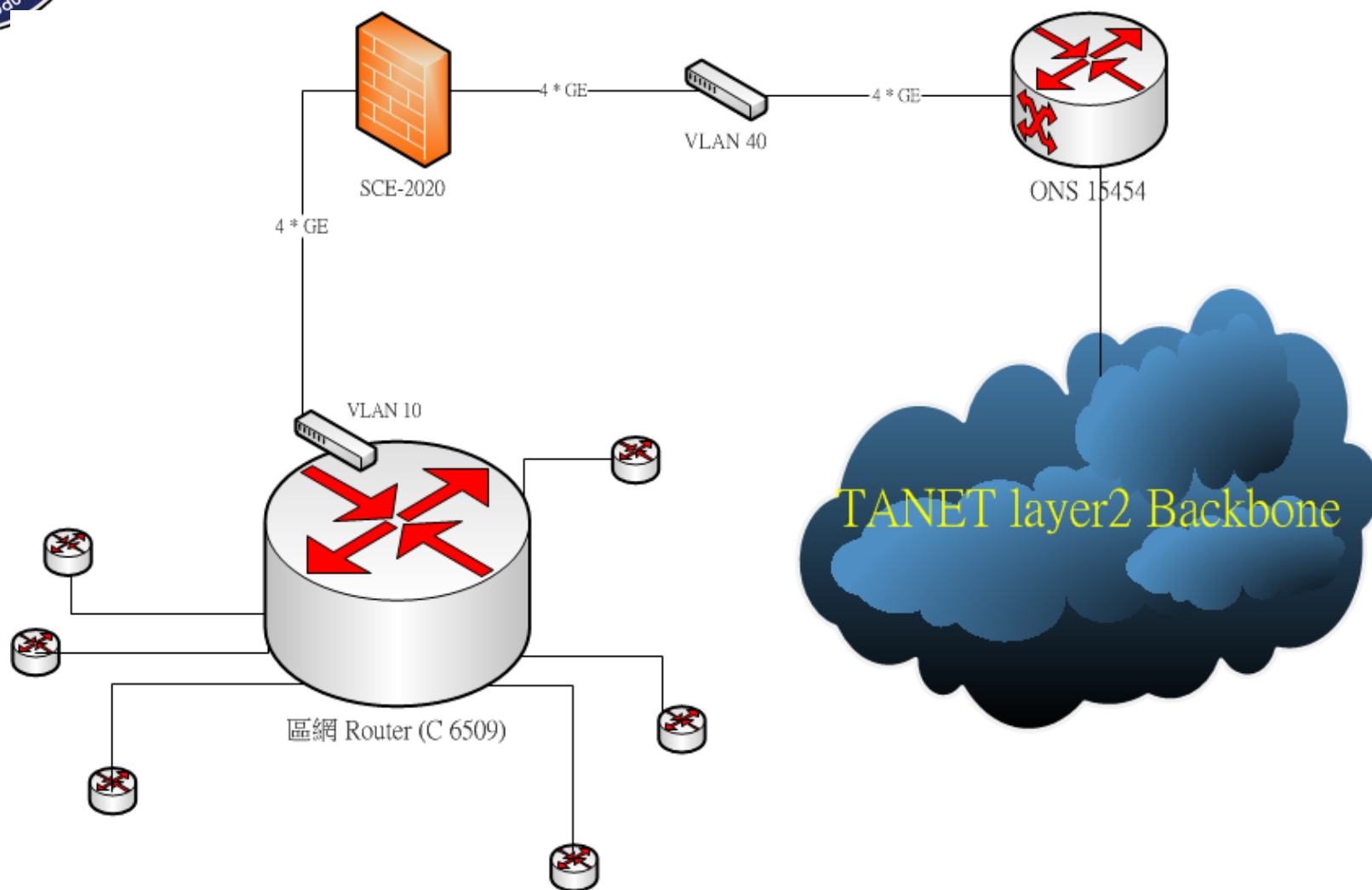


資安防護—桃園區網連外網路





資安防護--P2P訊務阻擋系統

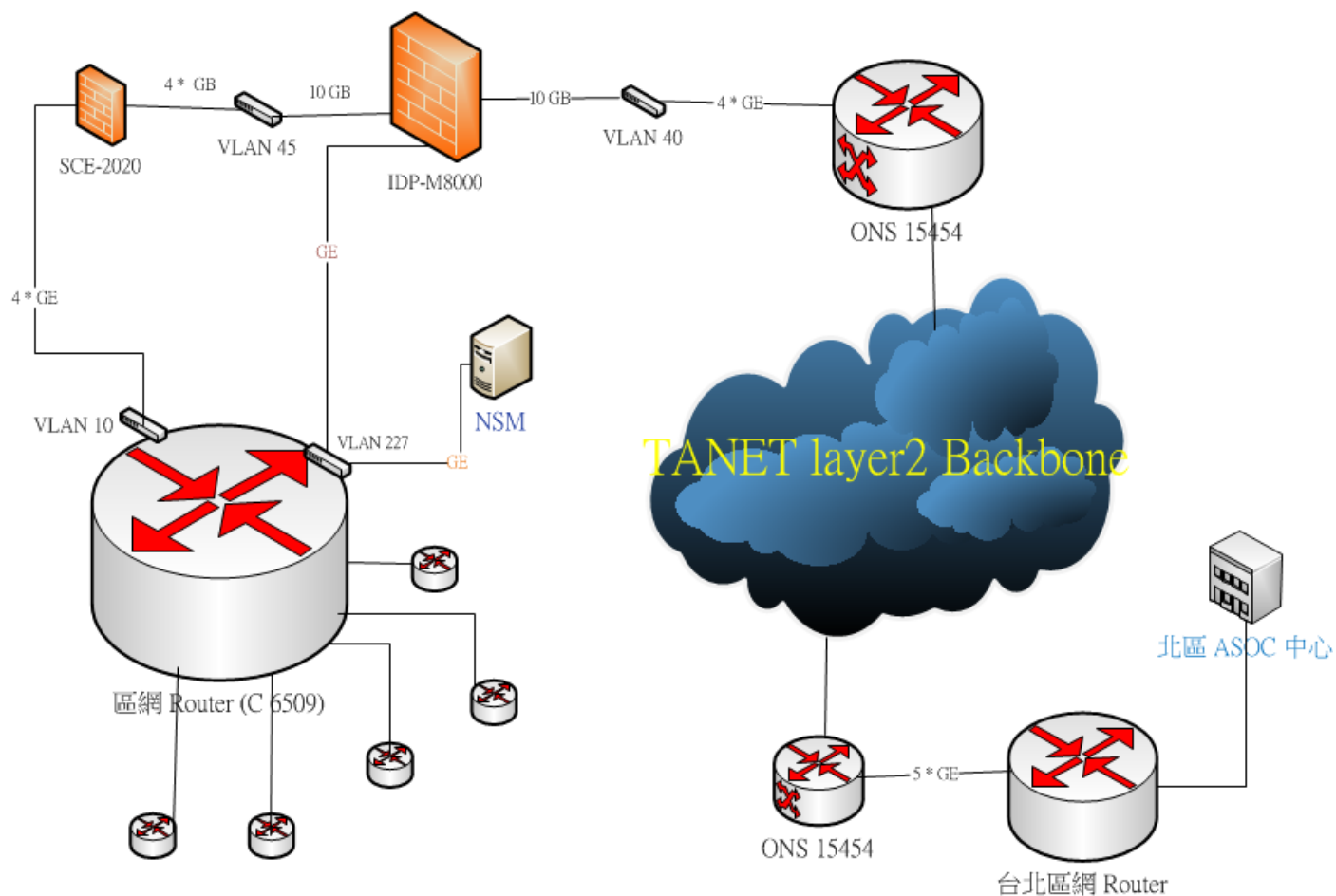




資安防護--區網P2P訊務阻擋系統

- ❑ 區網 P2P 訊務阻擋系統
 - ❑ 2部 SCE 2020 (2-in/2-out GE ports)
 - ❑ 桃園區網連外線路 (4 Gigabit Ethernet)
 - ❑ Block P2P : 連江縣網、中央大學、中原大學、開南大學
- ❑ 2011 年 智財侵權通告(件數)
 - 1月： 10 件 (NCU 7)
 - 2月： 6 件 (NCU 5)
 - 3月：10 件 (NCU 1)
 - 4月： 8 件 (NCU 1)
 - 5月：14 件 (NCU 3)
 - 6月： 1 件
 - 7月： 0 件
 - 8月： 1 件 (NCU 1)
 - 9月： 2 件
 - 10月： 1 件
 - 11月： 0 件

資安防護—惡意攻擊偵測與阻擋





資安防護—惡意攻擊偵測與阻擋

❑ IDP M8000 overload

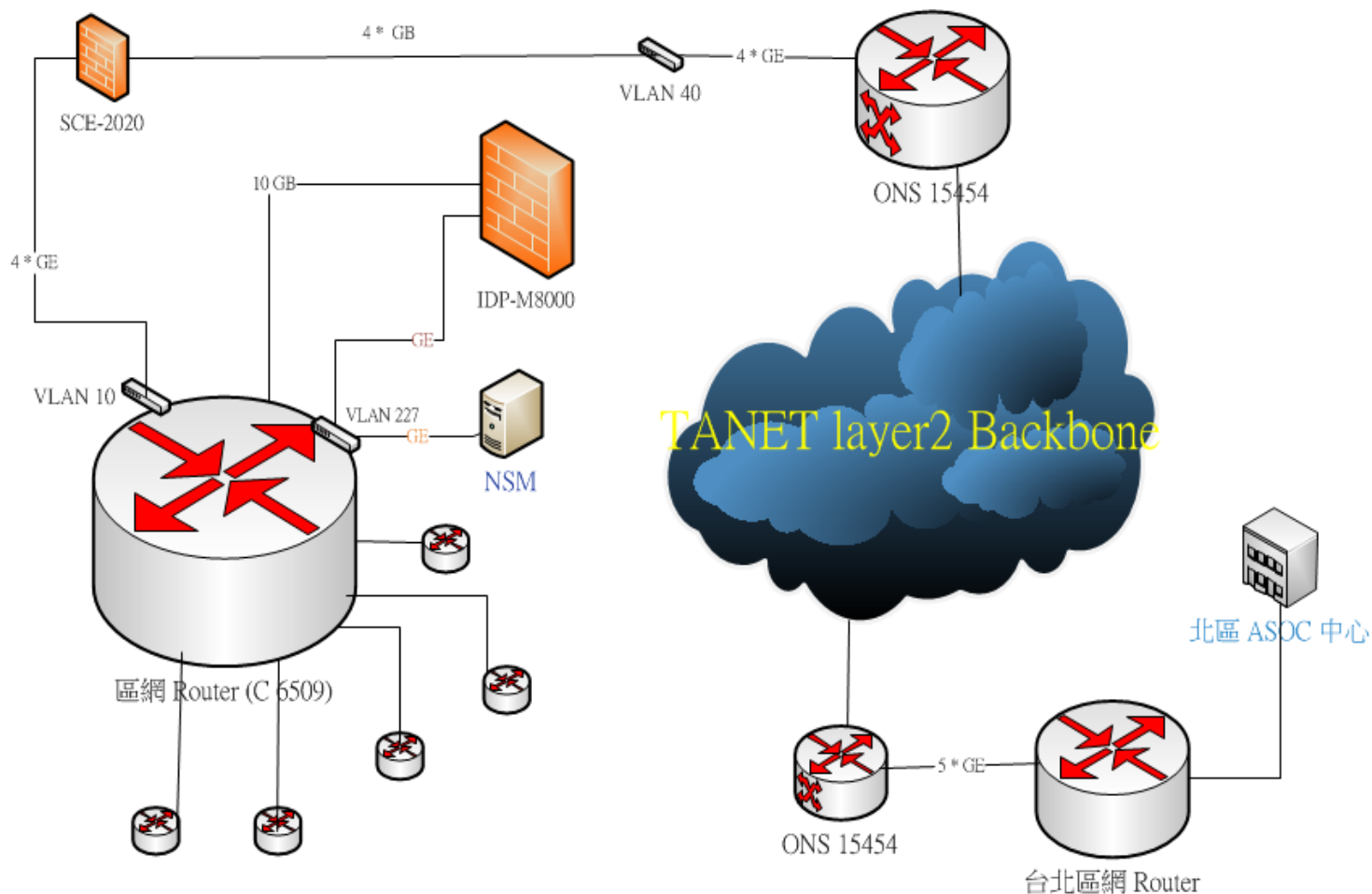
➤ 造成區網連外網路中斷事件

- 5/7 23:40 到5/8 00:40 桃園區網到tanet 骨幹 斷線
- 6/30 09:40 ~10:00 骨幹斷線
- 7/20 15:10 ~15:50 區網對外網路連線緩慢

❑ 暫時因應措施

- Bypass IDP M8000
- Mirror 連外 traffic 供 M8000 分析
- Robust NSM server
- 調整 M8000 detection policies

資安防護—惡意攻擊偵測與阻擋





Computer Center, National Central University.



感謝你的耐心聆聽!

Q&A