

天主教輔仁大學
FU JEN CATHOLIC UNIVERSITY

輔仁大學網路管理經驗分享

網路組 梁士杰

天主教

輔仁大學

FU-JEN
CATHOLIC
UNIVERSITY

輔仁大學

FU-
CATH
UNIVE



網路組服務簡介

- 網路組主要業務為：
 - 負責規畫與建置校園網路基礎建設
 - 提供高速與安全的網路使用環境
 - 提供多元化網路資源服務
 - 提供各單位與使用者在建置與使用上的問題諮詢
 - 提供輔醫網路支援



1. 服務規模

- 全校約28000人、48棟大樓、戶外設施(ex:運動場)
- 全校有線網路
 - 終端使用者設備近8000台
- 全校無線網路
 - 無線網路基地台包含室外內共約1500台
 - 每日最大同時線上使用人數超過10000人
- 兩間全校核心網路機房
 - 網管設備近140台
 - 全校型系統服務實體主機與設備96台。
- 區域型網路機房48間
 - 網路設備近400台





2. 骨幹網路與資訊安全

- 對外頻寬
 - － 國際線路: NTT 1.5G
 - － 國內線路: CHT 1G*2(教育部、政大區網)
- 校園頻寬
 - － 有線網路: 骨幹10G
 - － 無線網路: 全校教學、研究、行政、會議等所有室內空間皆提供訊號無死角服務，以及戶外的大部分。
 - － 宿網委外
- 資安管理
 - － 防火牆、IPS、DNS、WAF、頻寬管理設備、入口網加密、郵件防護、網路異常行為阻斷防護



3. 系統服務

- 主機維運
 - 校務雲、行政雲、教學雲
 - 代管維運52台實體主機
 - 413台虛擬主機與網頁服務
- 服務系統
 - 全校單一帳號認證系統、全校電子郵件服務、全校電子公告服務系統、全校教學平台系統、Google Apps for Education...
 - 網路組各項服務申請全部系統化



4. 其他

- 其他
 - 推動資安ISO27001與個資BS10012
 - 提供全校第一線使用者資訊問題諮詢與障礙排除



網路維運之點線面

- 點
 - 使用者端點
- 線
 - 聯外線路
 - 校園骨幹線路
 - 內網線路
- 面
 - 有線網路、有線認證網路、無線認證網路



網路維運

- 監控、設定備份
- 網路設備認證管理
- 流量監控-校園頻寬政策
- 日誌檔儲存及分析
- 線路備援及除錯



網路維運-監控



聯外電路監控儀錶板

首頁 上頁 下頁 末頁 Goto 頁 總紀錄數: 40 第 1/1 頁

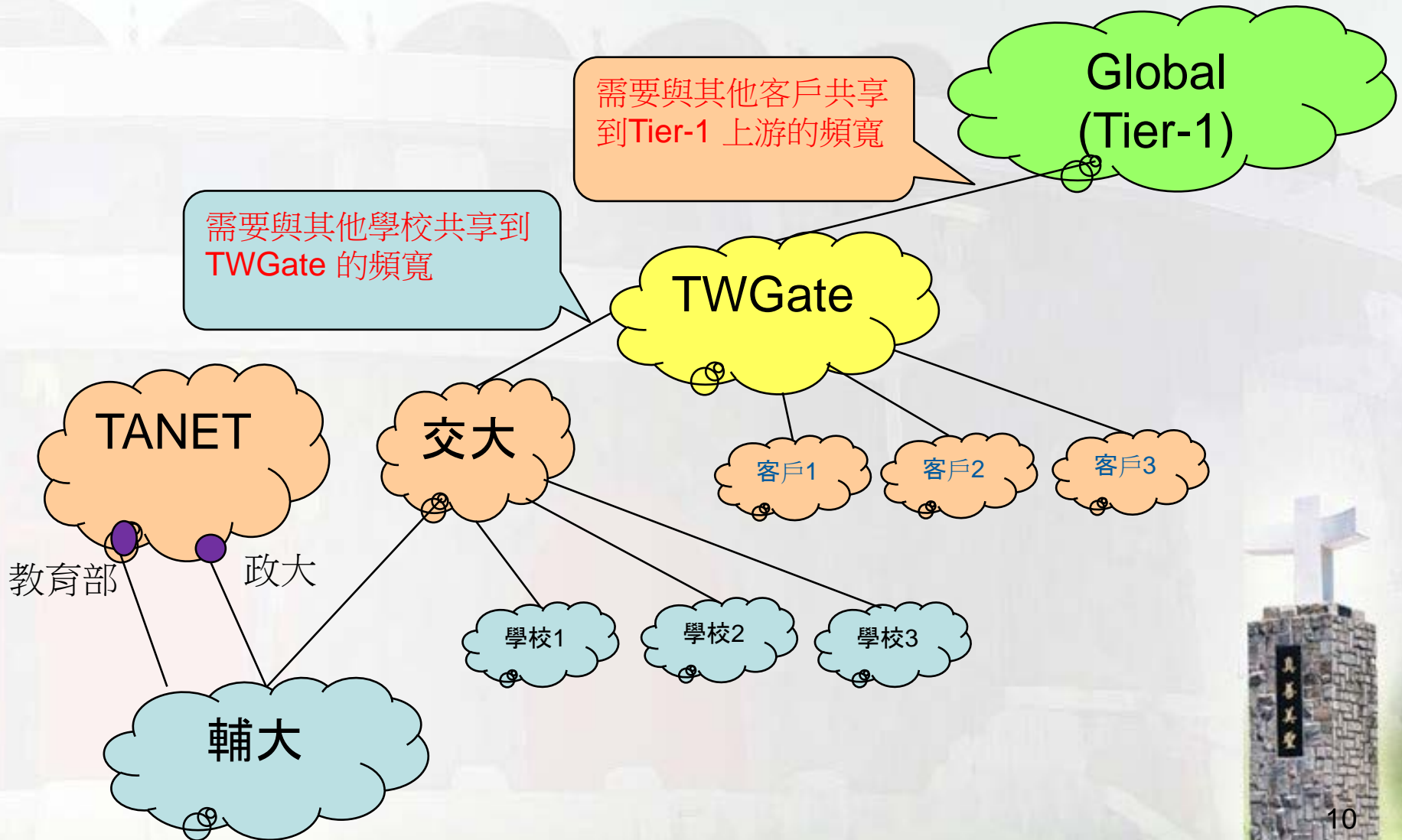
聯外電路列表

編號	狀態	資訊資產名稱	臨界頻寬	目前狀態	關道設備IP	趨勢圖
1	■	政治大學	1G	66.261% (662 Mbps)	140.136.254.17	
2	■	NTT	1G	47.303% (473 Mbps)	140.136.254.17	
3	■	NTT2	1G	43.965% (439 Mbps)	140.136.254.17	
4	■	教育部線路	1G	41.801% (418 Mbps)	140.136.254.17	



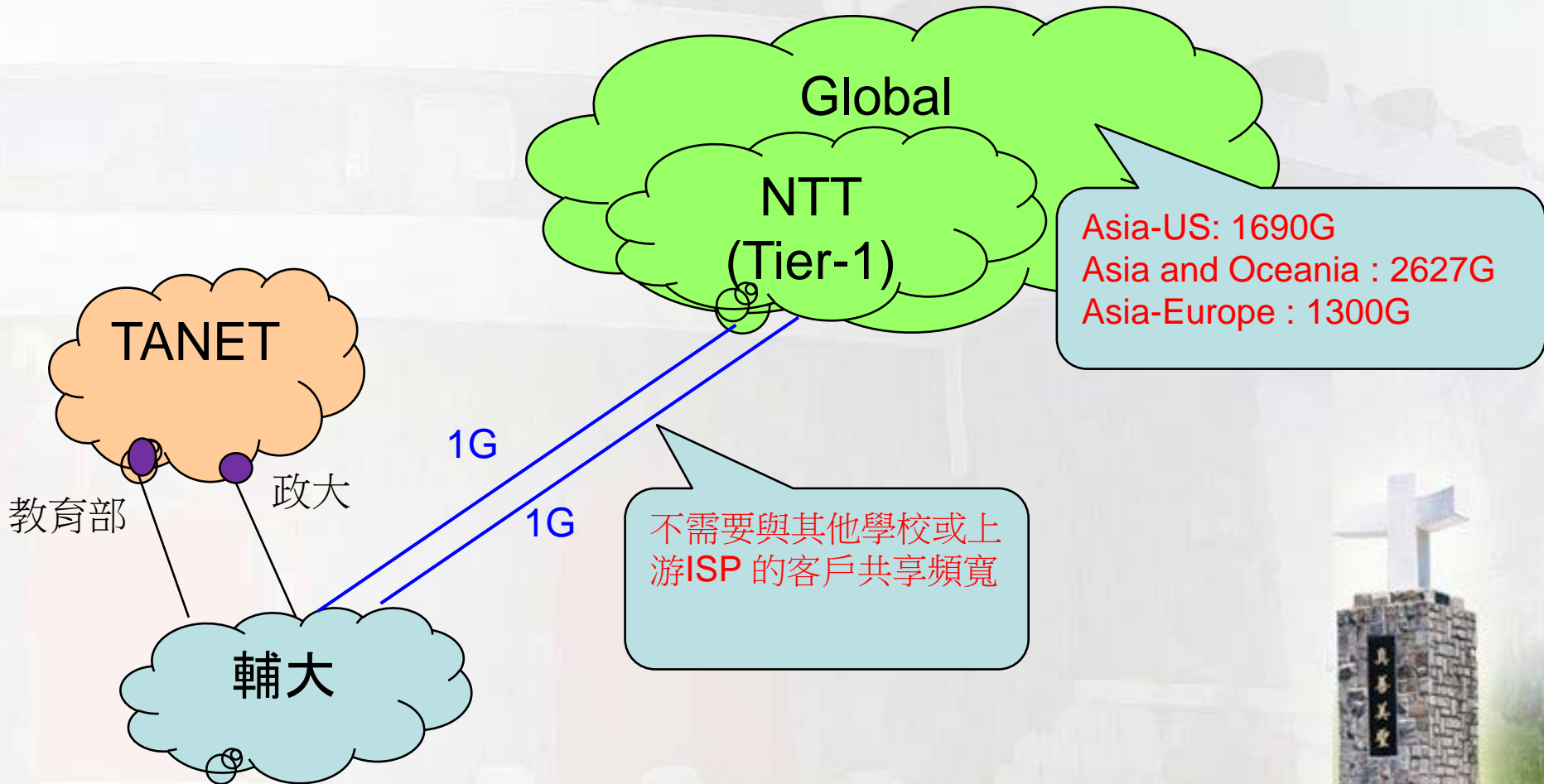


輔仁大學Internet架構(2015年前)





輔仁大學Internet架構(現在)





NTT Tier1 ISP 特色

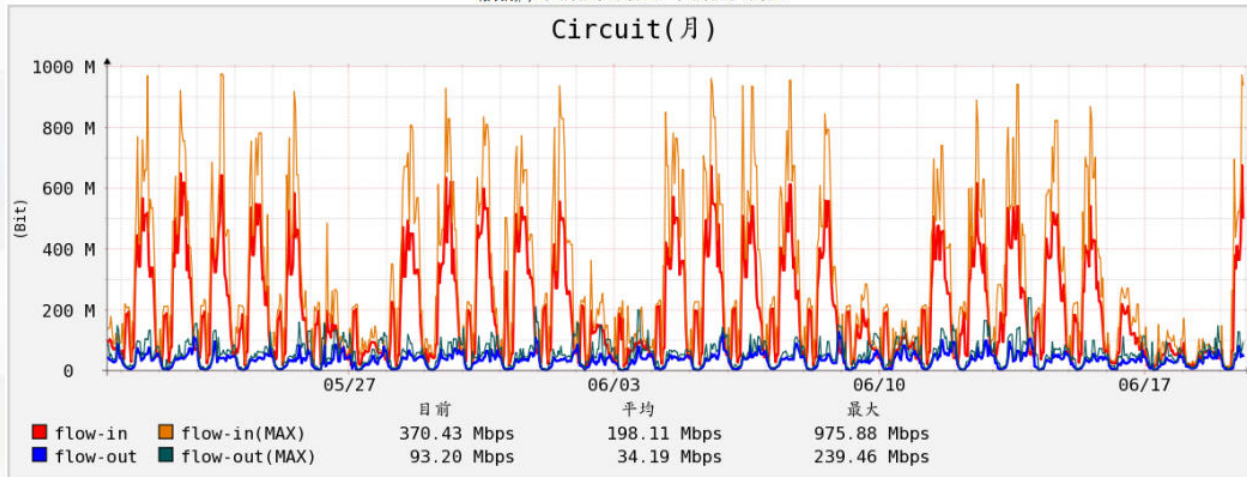
- 單一Single AS(2914)
- 清洗流量服務
- DDoS防護
- BGP community機制
- 全球網路覆蓋率高，骨幹節點遍及全球
- Tier1彼此間採交換 Peering 的方式介接
- 提供Tier2, Tier3 網路Transit 服務
- 提供無集縮比的真實頻寬服務
- 多重完善路徑備援機制
- 高可用性的SLA服務等級
- 完善的NOC、SOC 監控管理機制
- 與大型Content/Cloud Provider高速直連(Google, FB, Amazon, Microsoft..)



輔仁大學聯外流量現況(一)

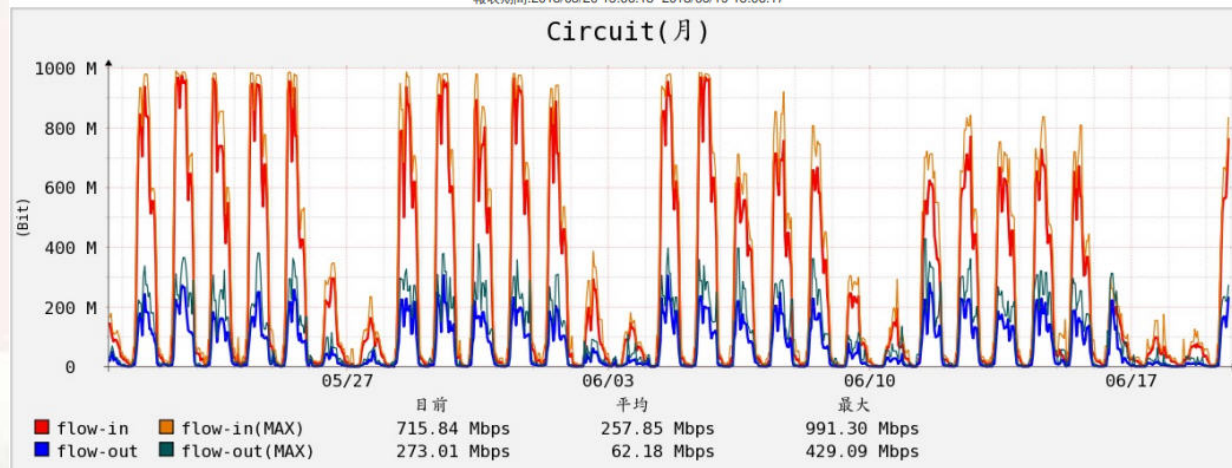
教育部線路

報表期間:2018/05/20 15:06:18~2018/06/19 15:06:17



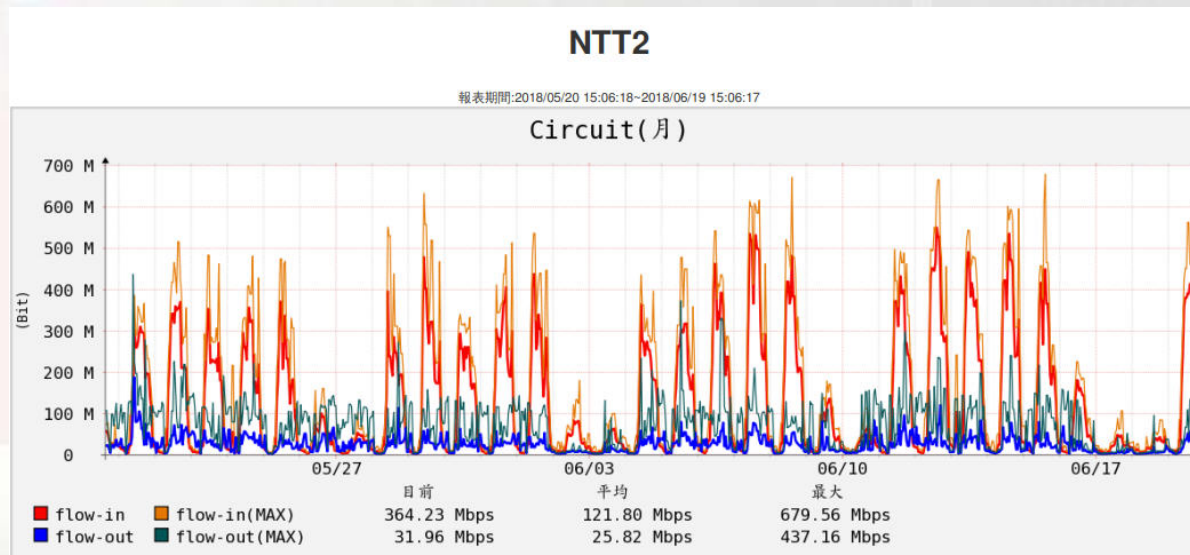
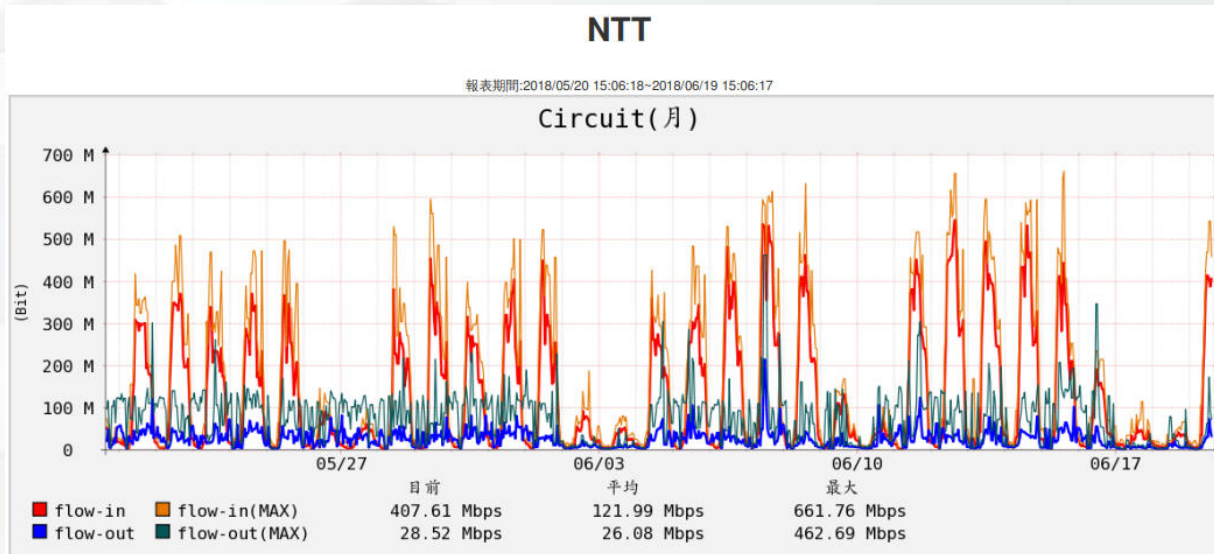
政治大學

報表期間:2018/05/20 15:06:18~2018/06/19 15:06:17





輔仁大學聯外流量現況(二)





資安防護之點線面

- 點
 - － 端點防護 (Client、Server)
- 線
 - － 資安設備 (IPS、firewall、WAF)、網路設備
- 面
 - － 區域聯防



資安防護

- 特徵碼偵測、國別攔阻、ACL
 - IPS、firewall
- 異常行為分析(入侵及攻擊)
 - Flowviewer(Netflow分析)
- 網站防護
 - 主機及全校網站防護
- 入口網加密登入
 - SSL VPN
- 頻寬管控
 - P2P、個別IP流量、個別帳號流量

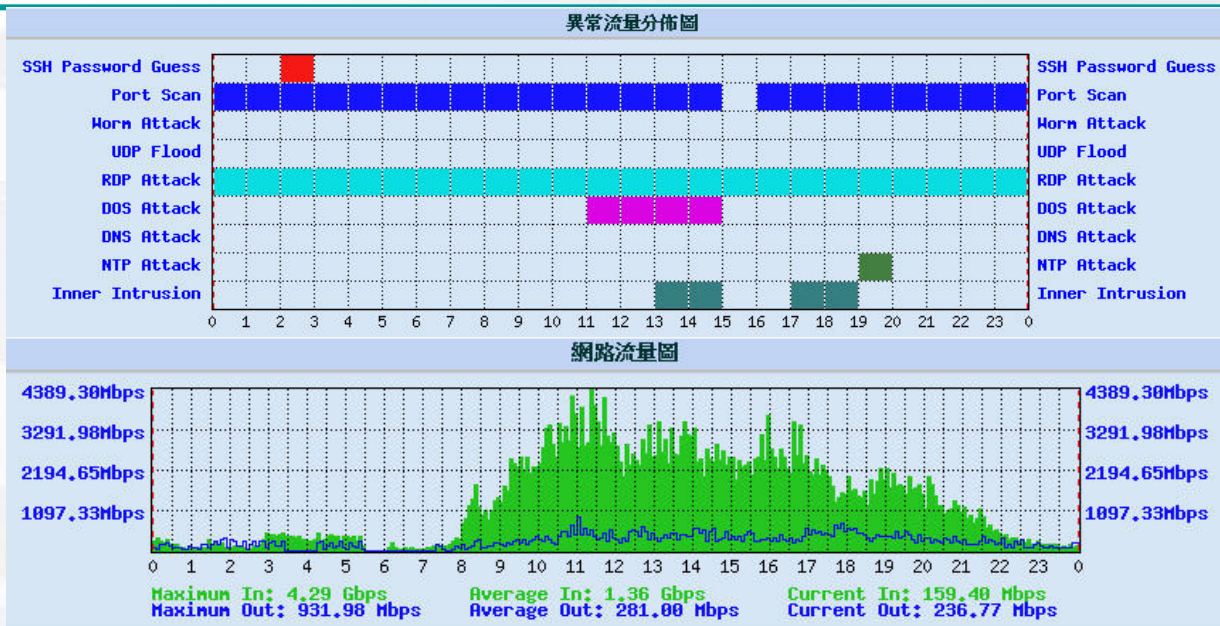


資安防護

- L2及L3 switch
 - L2:storm-control
 - L3:ACL
- 防毒軟體
- 垃圾郵件過濾



資安防護-行為分析



攻擊來源統計

查詢條件

查詢時間: 2018 年 04 月 報表類型: 年報 半年報 季報 月報

顯示前 20 名

查詢 產生 CSV 產生 PDF

查詢完成 (耗時 0.25 秒) 資料接收完畢 (共 20 筆)

順序	來源位址	次數
1	外部	71,534
2	美國	17,793
3	越南	8,798
4	印尼	6,857
5	委內瑞拉(南美洲北部)	5,251
6	印度	5,034
7	中國	4,966
8	臺灣	3,156
9	泰國	1,891
10	日本	1,204
11	墨西哥	1,144
12	內部	978
13	埃及	978
14	菲律賓群島	879
15	南韓	800
16	英國	787
17	香港	769
18	德國	749
19	法國	635
20	智利(南美洲西南部)	584



未來規劃及挑戰

- 暗藏於SSL之入侵及攻擊
- 主機及Client端防護
- 人員老化及短缺