# 景文科技大學

## 台北區網中心第85次管理委員會
## 網路管理及建置經驗分享

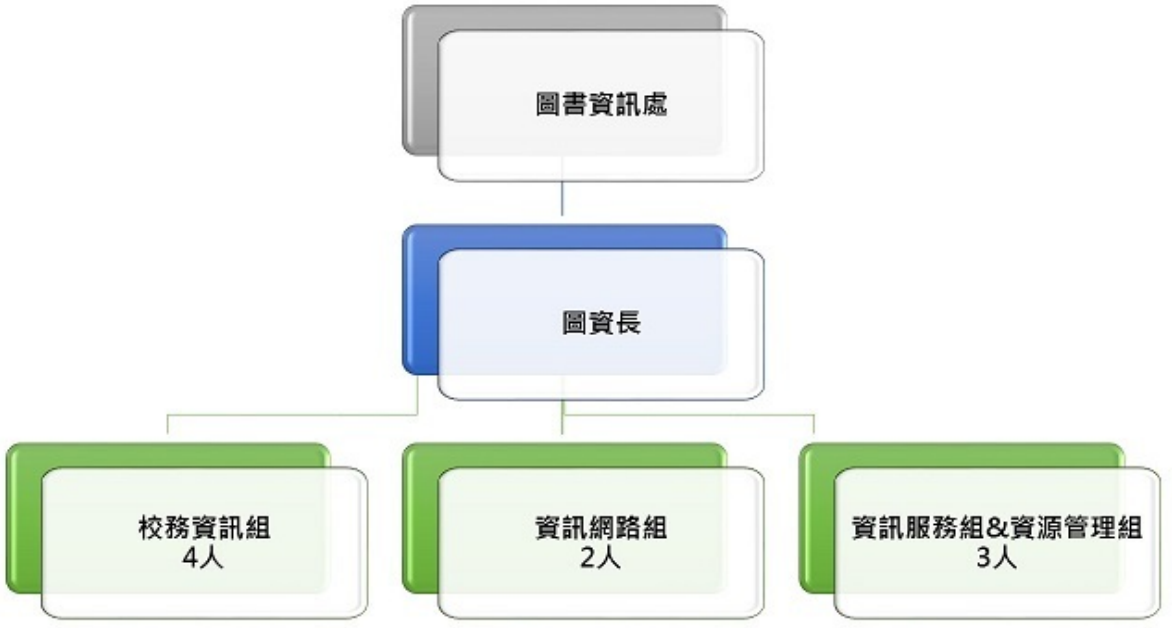
單位: 圖資處資訊網路組
主講人: 謝秉成
日期: 2021/12/28(二)
(V1.0)

# 簡報內容

- 圖書資訊處簡介
- 網路架構環境
- IDC機房
- 系統使用介紹

# 圖書資訊處簡介

- 2012年8月1日起組織整併運作與管理，命名為「圖書資訊處」，簡稱「圖資處」。
- 合併後由5組變成4組，原15人力變成9人。
- 全校歷年行政單位滿意度評比圖資處均在前二名。
- 承辦2005、2015 CCDS全國大專校院資訊行政主管研討會。
- 支援考選部國家考場/師大閩南語,原住民檢定考場



# 網路架構環境

- 骨幹交換器-Cisco
- 各大樓Edge switch和骨幹交換器10G介接。
- 各樓層及研究室-網管Giga Dlink
- WAN負戴平衡-

  WAN:TANet 800Mbps(中華)

  FTTX:HiNet 光世代300/100Mbps*3

- UTM防火牆3台(4年租賃)

  WAN端:

  內部(宿舍/電腦教室):

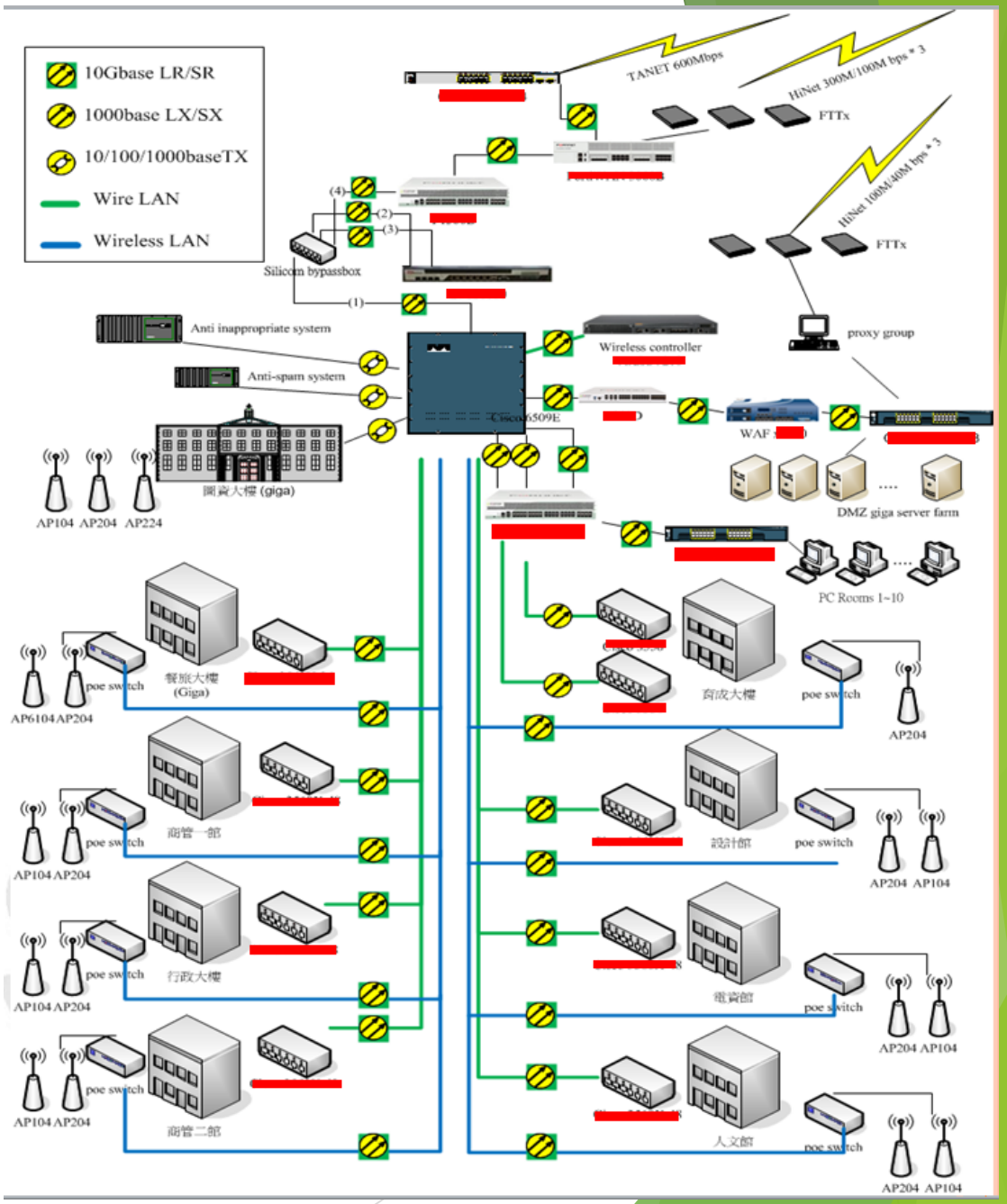
  DMZ:

- 應用內容頻寬管理:

  P2P/PerIP limit /L7 limit

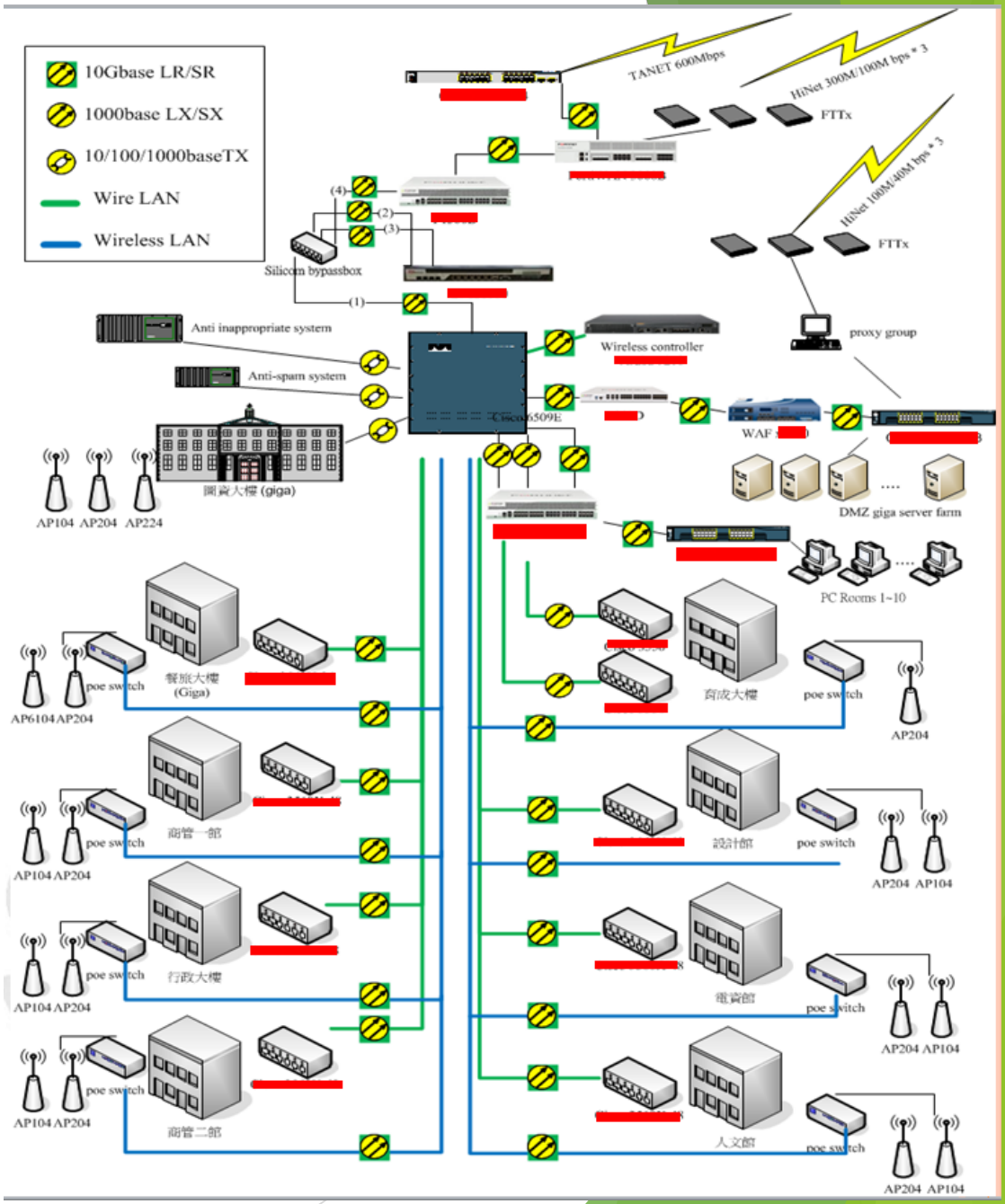
  bypassBox

  自動更新國家資通安全會報 / FireHOL / Malware Patrol / Cisco Talos中繼站黑名單，阻擋C&C連線



# 網路架構環境(續)

- 反垃圾郵件系統: SPAM
- 防治不當資訊系統: websense(forcepoint)
- 應用程式防火牆:
  - 升v14.3完整支援TLS1.2
  - VM150管理介面拉出
- 無線網路
  - 263台Wifi 5-802.11n dual-band、802.11ac
  - 有線無線實體分開
  - 各大樓10G poe switch介接
  - ClearPass 1次性認證
  - Eduroam/802.1X尚待導入
- 宿舍大樓僅有線網路-網管Giga Dlink
- DNS server加入啟用TWNIC RPZ機制

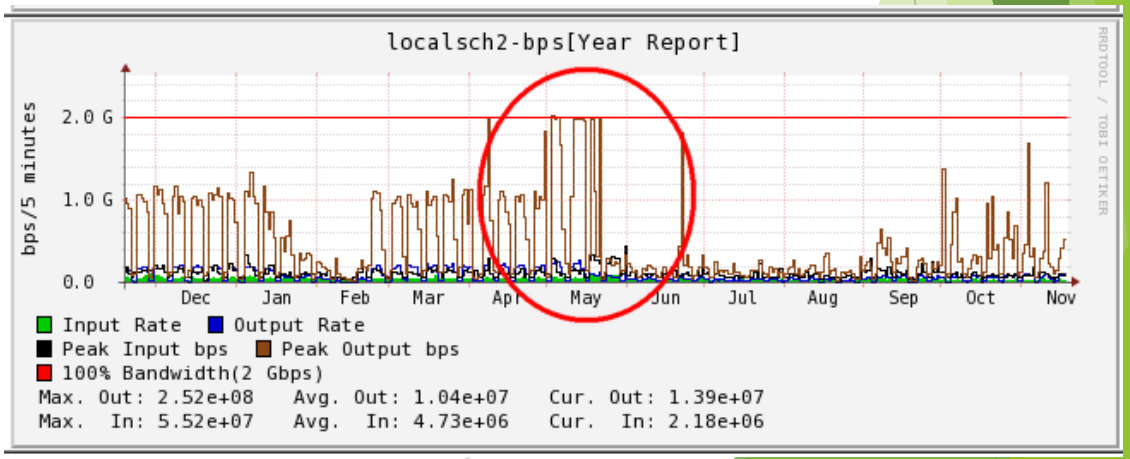


# 網路架構環境(續)

5/31 完成改接獨立線路脫離2G共用(TANet)

中華電信 YVxxxx =>YDxxxxx

**~感謝政大區網中心協助~**




資料來源: http://mrtg.tp2rc.tanet.edu.tw/netflow/

# IDC機房

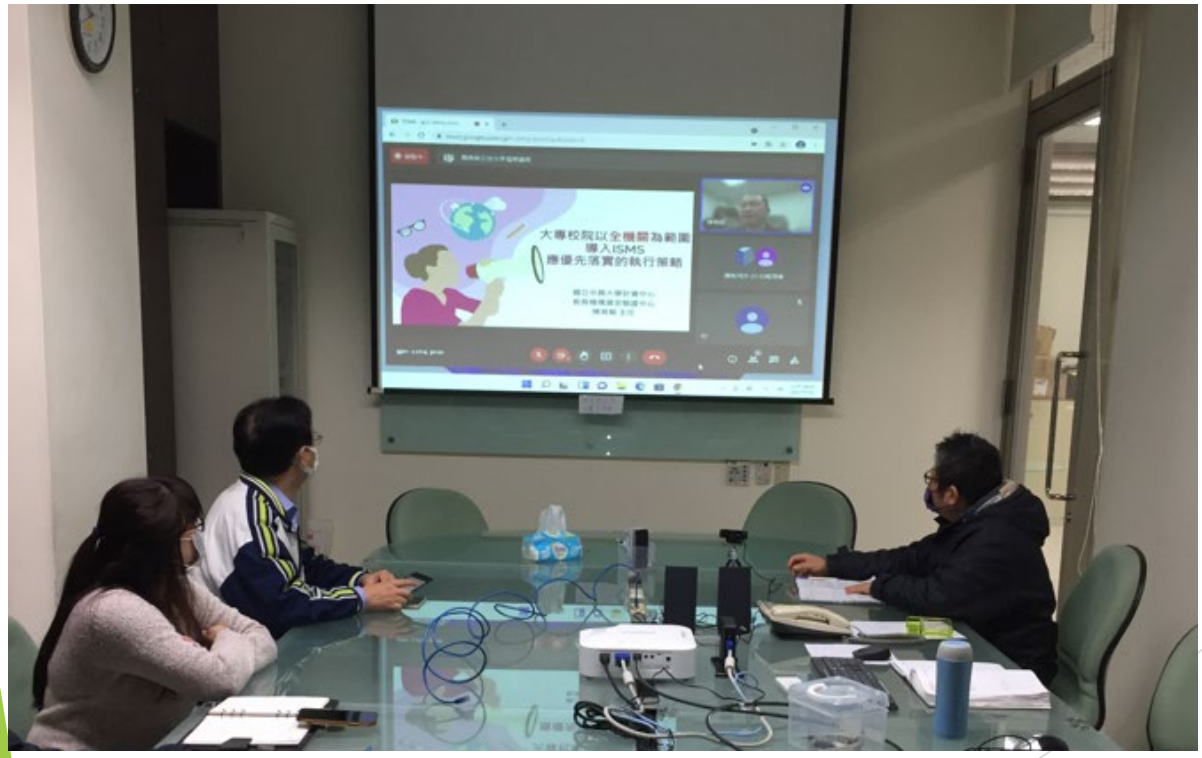
- 94年8月完工，面積80米平方(約24坪)。
- 具有獨立空調、獨立ATS、發電機及UPS、獨立消防(氣體式)
- 獨立環控系統、門禁及監視系統，全程24小時運作。
- 實體伺服器上線數量由106台因虛擬化已減至58台。
- PUE值維持1.8以下。
- 空調設備待更新。


# 系統使用介紹

- 虛擬化系統: VMWare 6.7u3, SAN架構
  - JVM_Cluster: 64 VMs
  - Moodle_Cluster: 16 VMs
  - J-Cloud私有雲服務: 11 VMs
  - 1VC+14 processors academic basic support 1year payment (10 ↓)
  - Veeam 備份軟體
    - Proxy-Virtual appliance
    - Backup Repository – NAS/Windows(ReFS; fastclone for synthetic full backup)
    - Instant recovery (vPower NFS)

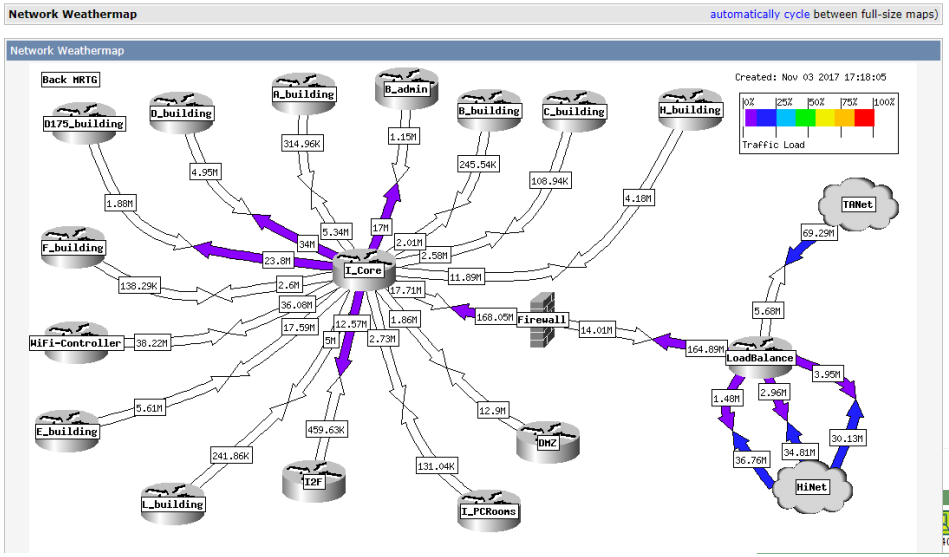
# 系統使用介紹

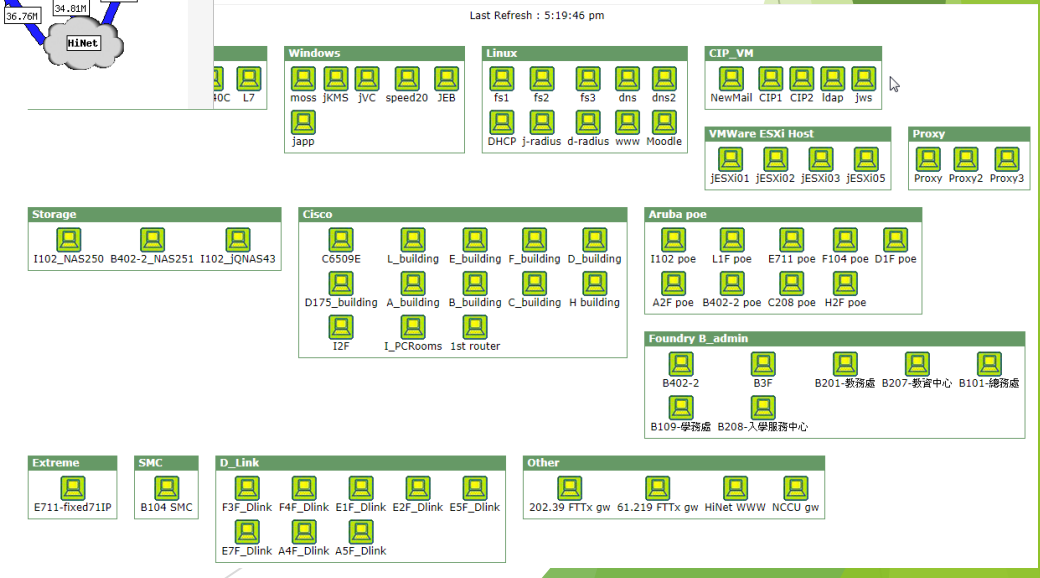
- VDI系統: 國產VDI; ezVDI-R
  - AMD R6515 server-CPU EPYC 7502P 32 cores (1P)/U.2 SSD/SAS SSD
  - Web Client/Zero Client CT-600/RDP Client
  - Support Windows 11
  - Zero client 不支援local usb printer…
  - 應用中….會議室/查詢平台/公共電腦/家中連線…



# 網路管理系統

- Cacti – Weathermap、monitor



# 網路管理系統

fprobe + flow-capture w/mysql
+ tablesorter-master

**JUST TOP 30 IP Flow Dashboard**

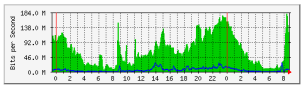
[Dashboard TOP3] [search history] [trace ip] [trace port] [check db]

現在時間: 8時51分43秒

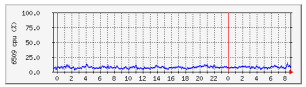
更新時間:
2017-12-11 08:51:14

搜尋範圍:
2017-12-11 08:21:14
to
2017-12-11 08:41:14

**Core-switch to TANet Traffic**

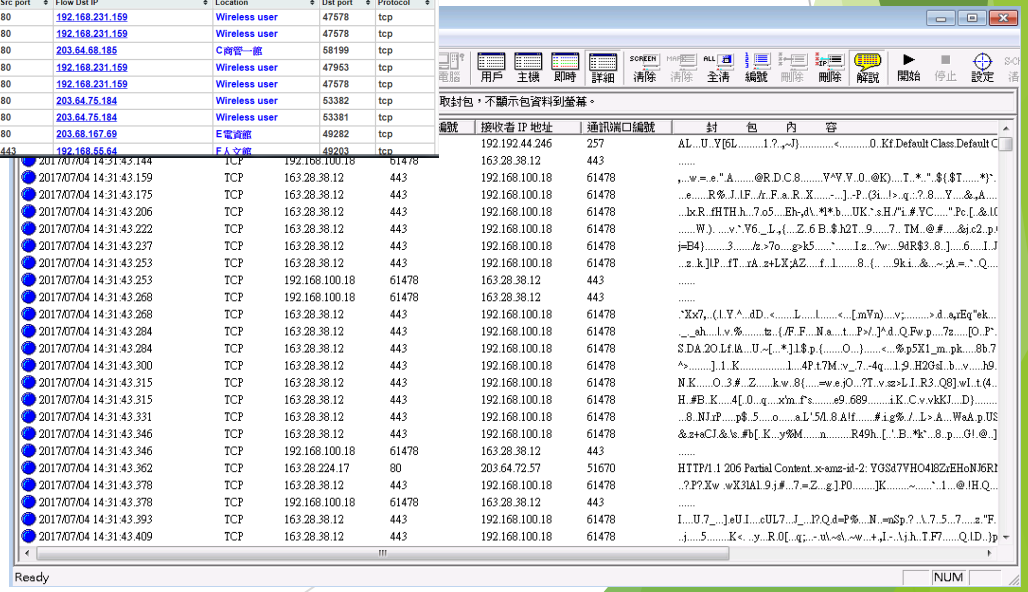



**Core-switch CPU**



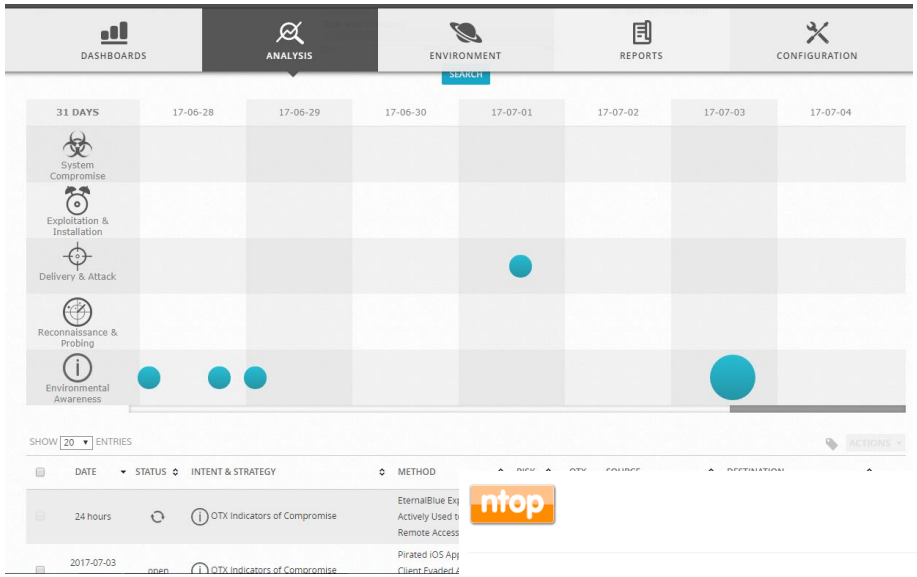

| TOP1 flow | TOP2 flow | TOP3 flow |
|---|---|---|
| 2017-12-11 08:25:21 | 2017-12-11 08:30:26 | 2017-12-11 08:36:16 |
| IP:192.168.231.159 | IP:192.168.231.159 | IP:203.64.68.185 |
| Wireless user | Wireless user | C商管一館 |
| 289,980,999 bytes | 287,521,966 bytes | 278,940,019 bytes |
| 203,421 Pkts(tcp) | 201,699 Pkts(tcp) | 187,510 Pkts(tcp) |

| No. | Time | Duration | Bytes | Pkts | Flow Src IP | Src port | Flow Dst IP | Location | Dst port | Protocol |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2017-12-11 08:25:21 | 00:05:05 | 289,980,999 | 203,421 | 117.18.232.252 | 80 | 192.168.231.159 | Wireless user | 47578 | tcp |
| 2 | 2017-12-11 08:30:26 | 00:05:05 | 287,521,966 | 201,699 | 117.18.232.252 | 80 | 192.168.231.159 | Wireless user | 47578 | tcp |
| 3 | 2017-12-11 08:36:16 | 00:05:00 | 278,940,019 | 187,510 | jptyo5-vip-bx-005.aaplimg.com | 80 | 203.64.68.185 | C商管一館 | 58199 | tcp |
| 4 | 2017-12-11 08:40:31 | 00:04:18 | 262,801,906 | 184,396 | 117.18.232.252 | 80 | 192.168.231.159 | Wireless user | 47953 | tcp |
| 5 | 2017-12-11 08:35:56 | 00:04:28 | 220,708,776 | 154,818 | 117.18.232.252 | 80 | 192.168.231.159 | Wireless user | 47578 | tcp |
| 6 | 2017-12-11 08:46:21 | 00:01:08 | 216,122,572 | 144,198 | 13.107.4.50 | 80 | 203.64.75.184 | Wireless user | 53382 | tcp |
| 7 | 2017-12-11 08:46:21 | 00:01:08 | 214,874,634 | 143,342 | 13.107.4.50 | 80 | 203.64.75.184 | Wireless user | 53381 | tcp |
| 8 | 2017-12-11 08:37:41 | 00:05:05 | 187,047,843 | 124,813 | 8.250.187.254 | 80 | 203.68.167.69 | E電資館 | 49282 | tcp |
| 9 | 2017-12-11 08:48:41 | 00:00:10 | 125,004,225 | 87,017 | 163.28.224.230 | 443 | 192.168.55.64 | F A 文館 | 49203 | tcp |

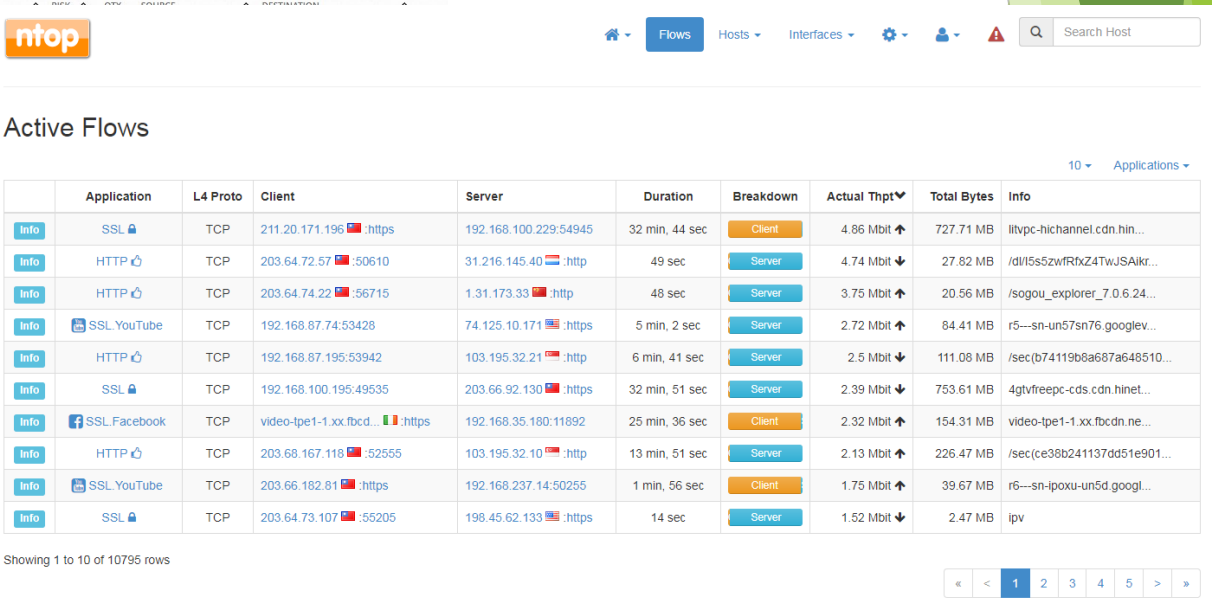


# 網路管理系統

## OSSIM: open source SIEM




## ntop



# 網路管理系統

WhatsUP Gold =>收內部netflow流量、監控switch (cisco error level SNMP Trap)、產出CPU/Memory/Disk報表、interface down訊息

192.192[redacted]0) Cisco Switch 上的 Interface(10101) I_PCROOM_1 gw (192.168.91.254)處於 Up 
least 5 min (with monitor(s) Down at least 5 min)。

詳細資料：
離線的監控工具包括： Interface(10101) I_PCROOM_1 gw (192.168.91.254)

上線的監控工具包括： Interface(4) Vlan4 (192.168.4.254),
Interface(10) Vlan10 (192.168.10.254),
Interface(442) Vlan442 (192.192.44.230),
Interface(10102) I_PCROOM_2 gw (192.168.2.254),
Interface(10103) I_PCROOM_3 gw (192.168.3.254),
Interface(10104) I_PCROOM_4 gw,
Interface(10105) I_PCROOM_5 gw (192.168.5.254),
Interface(10106) I_PCROOM_6 gw (192.168.6.254),
Interface(10107) I_PCROOM_7 gw (192.168.7.254),
Interface(10108) I_PCROOM_8 gw (192.168.8.254),
Interface(10109) I_PCROOM_9 gw (192.168.9.254),
Interface(10110) I_PCROOM_10 gw,

Co_Switch (203.[redacted]4).

Warning!! some error or critical event occurs !

[Details]

Facility: IP
Severity: 5
Mnemonic: DUPADDR
Description:
Duplicate address 192.168.66.254 on Vlan966, sourced by dc4a.3e49.6e1a

---
This mail was sent on $@$k 06, 2017 at 11:18:06 $W$H Ipswitch WhatsUp Gold

**'Performance Disk Utilization Exceeds 90% for AIS server only' threshold**

**Description:** Average disk utilization during the past 6 hours exceeds 90%

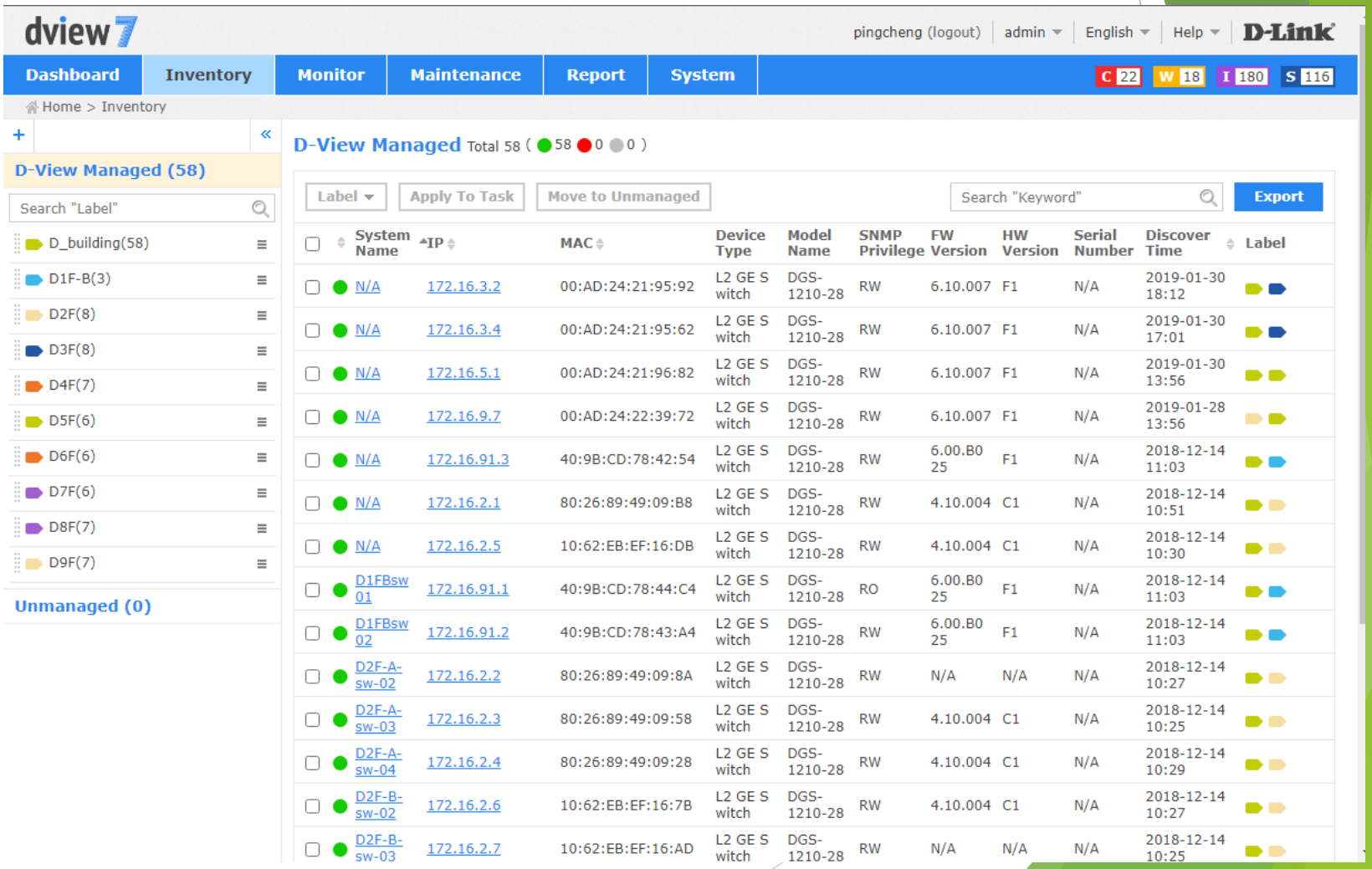
**New Items (1)**

Occurred at 2021/9/25 上午 06:45:03

| Display Name | Aspect Name | Aspect Value |
|---|---|---|
| AISDB2-NEW | E:\ | 90.2 % |

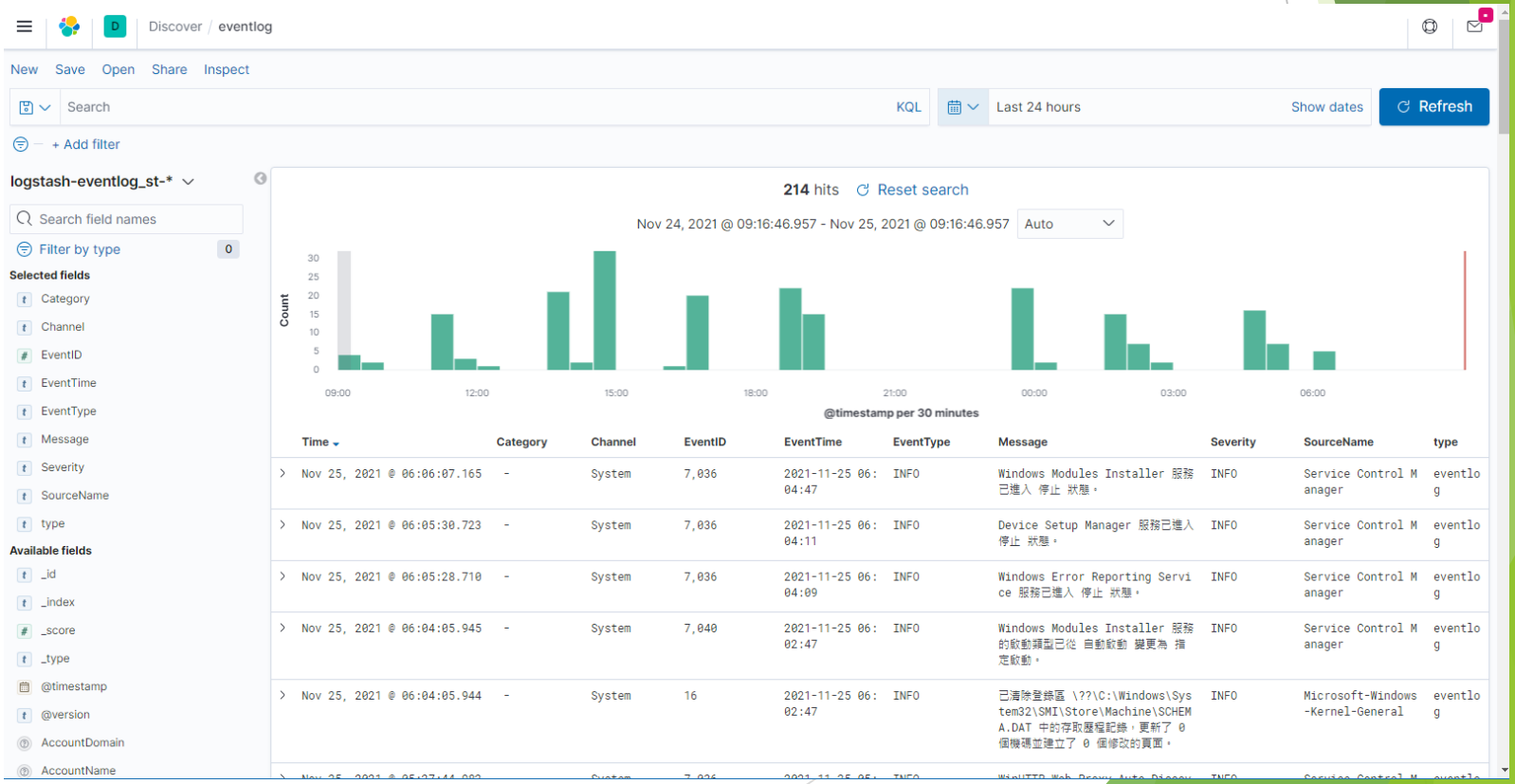
# 網路管理系統

Dview7 =>Dlink switch syslog/snmp/monitor



# log系統

- Syslog
- ELK; Elasticsearch+Logstash+Kibana
  - EventLog、IISLog: nxlog (中文O.K)
  - Shard/indexing 優化問題
- Fortianalyzer
- SQl log => N-reporter….待測…



# 其它

- 景文Office 365 – 線上申請365帳號,結合轉向idp認證(訂閱A1才有Teams授權)
- *.just.edu.tw => Wildcard SSL, RapidSSL, 年費(5K↓)
- 卡巴斯基企業版 => .lnk捷徑病毒.
- rPage, ePage
- Google Workspace for edu (G suite for edu).....
- Bruteforce攻擊每天上映，SSH/RDP....
- ISMS走ISO 27001認證(範圖:圖書資訊處負責的學生教務相關系統、校園骨幹網路及IDC機房之管理活動)；ISMS全機關導入...ISCB不再發證...教育部實地稽核....私校等級不明....
- 警政署防詐騙網站公文...(TWNIC RPZ尚未納入, 只好自己建RPZ policy, blocklist zone, 2 weeks update)
- 零時差攻擊雖IPS特徵碼均即時更新，但預設為PASS/detect，仍要人工調Block。(Apache Log4j攻擊已經來了)

# 其它

FG10E1TB20903352 ▾ 最近12小時 ▾ 20:45:32 To 08:45:31 自定檢視

訊息 = "apache: Apache.Log4j.Error.Log.Remote.Code.Execution," Add Filter

| # | ▲日期/時間 | 設備 ID | 嚴重性 | 來源 | 目的 IP | Action | 服務 | 攻擊名稱 |
|---|---|---|---|---|---|---|---|---|
| 1 | 12-16 20:50 | FG10E1TB20903352 | critical | 172.104.248.192 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 2 | 12-16 20:50 | FG10E1TB20903352 | critical | 172.104.248.192 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 3 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 4 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 5 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 6 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 7 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 8 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 9 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 10 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 11 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 12 | 12-16 20:51 | FG10E1TB20903352 | critical | 61.175.202.154 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 13 | 12-16 20:53 | FG10E1TB20903352 | critical | 148.66.57.50 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 14 | 12-16 20:53 | FG10E1TB20903352 | critical | 148.66.57.50 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 15 | 12-16 20:58 | FG10E1TB20903352 | critical | 139.59.70.139 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 16 | 12-16 20:58 | FG10E1TB20903352 | critical | 139.59.70.139 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 17 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 18 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 19 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 20 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 21 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 22 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 23 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 24 | 12-16 21:20 | FG10E1TB20903352 | critical | 34.80.118.173 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 25 | 12-16 21:38 | FG10E1TB20903352 | critical | 172.104.248.192 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 26 | 12-16 21:38 | FG10E1TB20903352 | critical | 172.104.248.192 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 27 | 12-16 21:38 | FG10E1TB20903352 | critical | 172.104.248.192 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |
| 28 | 12-16 21:38 | FG10E1TB20903352 | critical | 172.104.248.192 | 203. | dropped | HTTP | Apache.Log4j.Error.Log.Remote.Code.Execution |

報告完畢，謝謝聆聽
敬請不吝指教

**祝 大家2022新年快樂**
**校園網路平平安安順順利利**