臺北科大
網路資安防護與控管方式

臺大區網會議分享

分享人：網路作業組 陳志豪

2025.12.30

TAIPEI TECH Since 1912 國立臺北科技大學 National Taipei University of Technology

Agenda

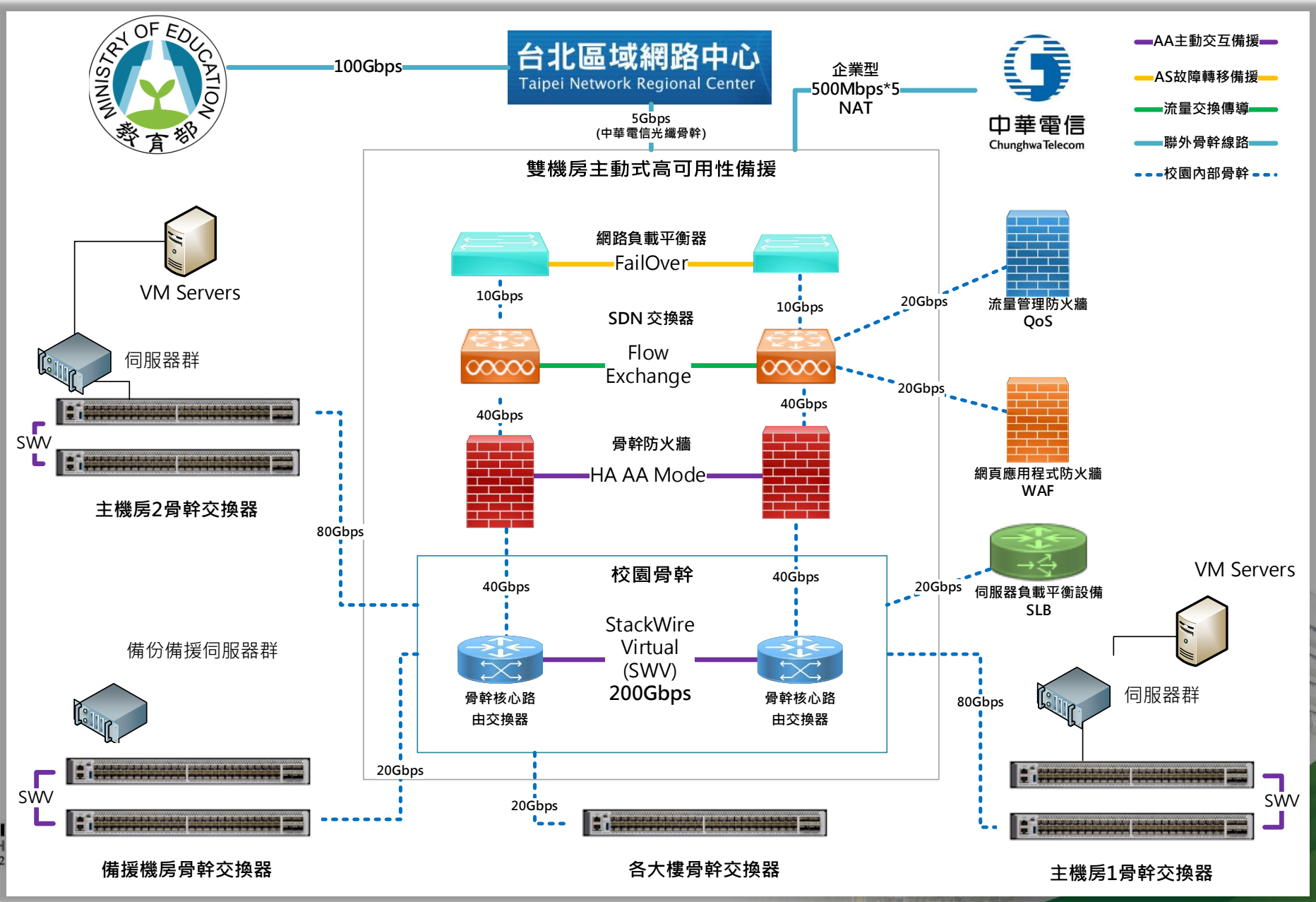
- 整體網路架構
- 使用者網路控管劃分
- 伺服器向上集中
- 資安設備與管理平台
- 資安與流量管理措施實作方式

前言

- 為配合法遵與稽核
  - 資通安全管理法(數發部)
  - 學術網路使用規範(教育部)
- 校園網路所存在之痛點：
  - 網段過大無法確實清查 > 主機過多
  - 無法透過掃描找出系統 > 弱點掃描困難
  - 內部橫向感染攻擊
  - 教職員工生不同管理維度與力道

整體網路架構

骨幹架構


100Gbps
台北區域網路中心
Taipei Network Regional Center
5Gbps
(中華電信光纖骨幹)
企業型
500Mbps*5
NAT
中華電信
Chunghwa Telecom
AA主動交互備援
AS故障轉移備援
流量交換傳導
聯外骨幹線路
校園內部骨幹
雙機房主動式高可用性備援
網路負載平衡器
FailOver
10Gbps
10Gbps
SDN 交換器
Flow
Exchange
40Gbps
40Gbps
骨幹防火牆
HA AA Mode
20Gbps
流量管理防火牆
QoS
20Gbps
網頁應用程式防火牆
WAF
VM Servers
伺服器群
SWV
主機房2骨幹交換器
80Gbps
校園骨幹
40Gbps
40Gbps
StackWire
Virtual
(SWV)
200Gbps
骨幹核心路
由交換器
骨幹核心路
由交換器
20Gbps
伺服器負載平衡設備
SLB
VM Servers
伺服器群
80Gbps
備份備援伺服器群
SWV
20Gbps
20Gbps
SWV
備援機房骨幹交換器
各大樓骨幹交換器
主機房1骨幹交換器

使用者網路控管劃分

使用者網路控管劃分

- 控管措施說明
- 行政單位(含教學行政)
- 研究中心
- 其他A/B級單位與中心
- 教師與學生

控管措施說明

防火牆管控

- 網段區分並由防火牆進行規則管控
- 各單位政策依據情況進行開放或限縮
- VPN依照帳號進行防火牆存取控管

進階IPS/IDS偵測機制

- 導入流量加解密技術與信任根憑證
- 連外連線解密分析強制納入範圍：
  - 行政單位、研究單位
  - 向上集中伺服器
- 連外連線解密分析強制納入範圍：
  - 計網中心對外服務伺服器

第三方VPN或Tunnel連外

- 避免惡意軟體或程式透過VPN或加密通道連線
- 僅允許連線至國內第三方VPN服務之IP
- 如有國外連線需求由計畫主持人專案申請
  - 研究中心
  - 學術單位

VPN校內跨單位連入

- 行政單位網段
  - 限教職員工帳號連線
- 研究單位網段
  - 限教職員工帳號連線
  - 學生帳號由計畫主持人專案申請
- 學術單位
  - 不受限制

校外連入

- 校外連入：
  - DMZ、行政單位、研究單位全時阻擋
- 學術單位下列BGP可直接連線，其餘阻擋：
  - TANET
  - HCHC
  - GSN

資安通報與資安預警之網路封鎖

- 自動化程式結合防火牆進行規則管控
- 封鎖資訊來源：
  - 教育部資安通報
  - 計網中心資安設備偵測與告警
- 封鎖機制
  - **以人為單位，封鎖員編/學號名下全部IP之設備**
  - 僅限校內可連線
  - 校外僅開放Windows Update、防毒軟體更新

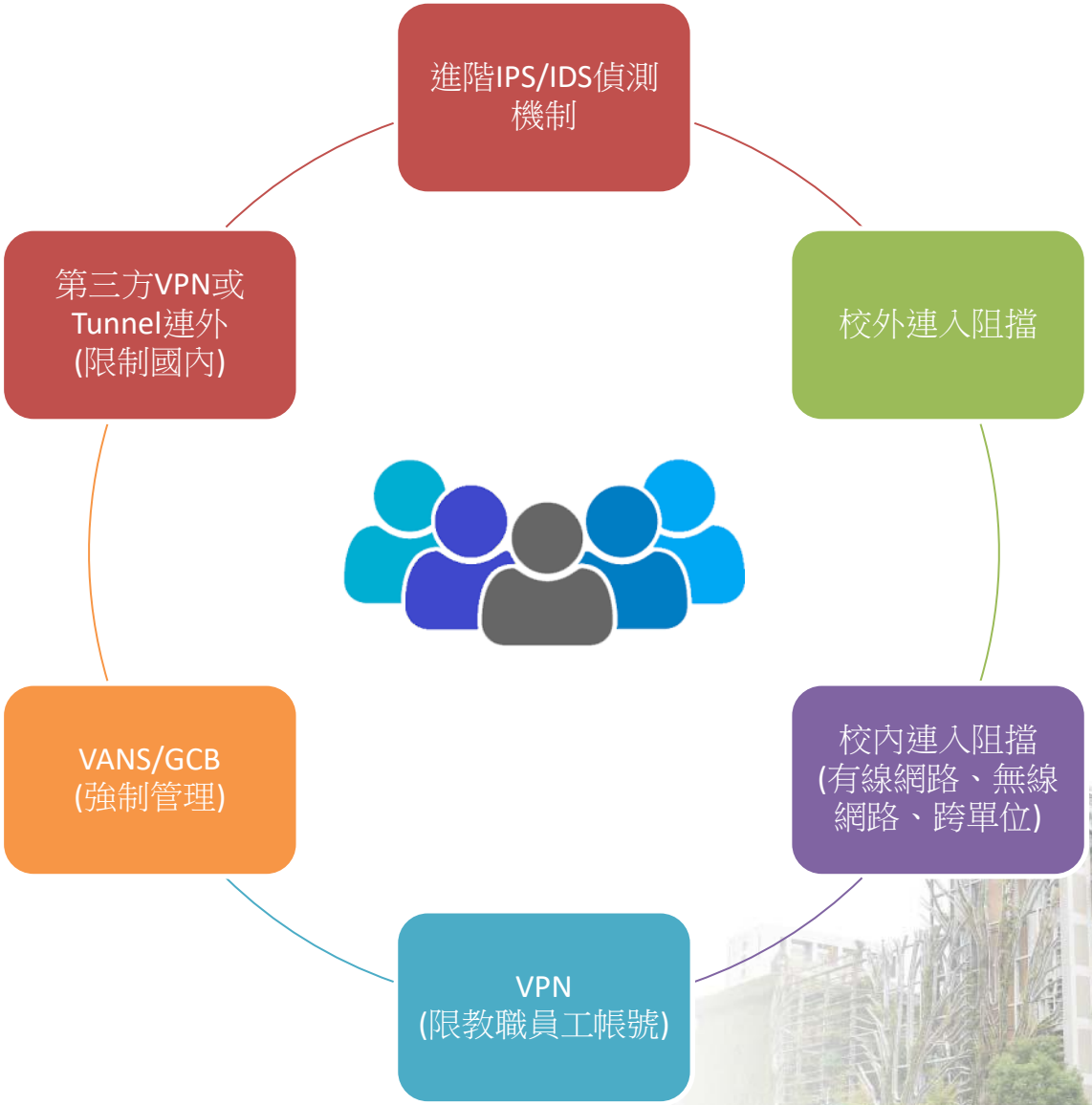
非學術研究與行政事務性質之中高風險通訊協定連外

- 路由協定(rip、ospf、eigrp)
- 通道協定(gre、tor)
- 認證協定(ldap、kerberos)
- 資料協定(iscsi、netbios、smb)
- 遠端呼叫(rpc、upnp)
- 反向代理協定(proxy)與其衍生之遠端桌面協定及各類P2P協定...等

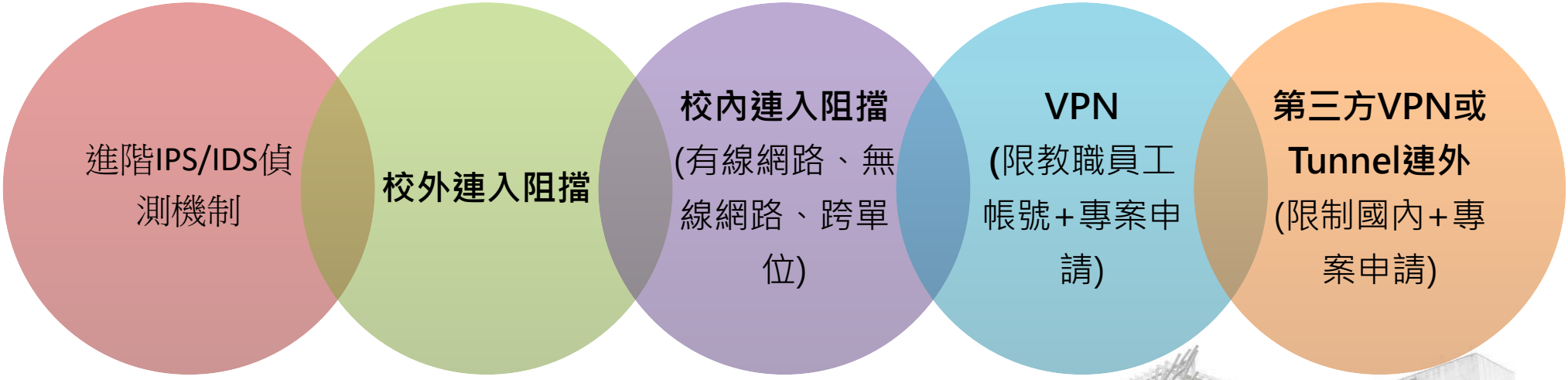
GCB與VANS管控

- 強制導入單位如未導入之設備
  將透過防火牆限制僅限校內連線
- 包括：
  - 行政單位
  - 其他單位如涉及公務與機敏感資料之設備

行政單位(含教學行政)


進階IPS/IDS偵測機制
校外連入阻擋
校內連入阻擋(有線網路、無線網路、跨單位)
VPN(限教職員工帳號)
VANS/GCB(強制管理)
第三方VPN或Tunnel連外(限制國內)

研究單位


進階IPS/IDS偵測機制
校外連入阻擋
校內連入阻擋
(有線網路、無線網路、跨單位)
VPN
(限教職員工帳號+專案申請)
第三方VPN或Tunnel連外
(限制國內+專案申請)

教師與學生

校外連入阻擋

TANET、HCHC與GSN之BGP範圍

可直接連線，其餘阻擋

第三方VPN或Tunnel連外

(限制國內)

其他A/B級單位與中心


進階IPS/IDS偵測機制
校外連入阻擋
校內連入阻擋
(有線網路、無線網路、跨單位)
VPN
(限教職員工帳號)
VANS/GCB
(強制管理)
第三方VPN或Tunnel連外
(限制國內)
APT進階持續攻擊
(MDR)

伺服器向上集中

向上集中清查與控管

- 透過防火牆
  - 防火牆URL filter紀錄
    是否有非本校網域指向本校主機
  - 只允許伺服器DMZ網段防火牆開放

向上集中清查與控管

- 透過DNS
  - 各單位不允許自建DNS伺服器
  - 各層DNS集中管理
  - ACME TXT認證控管
  - 本校DNS僅允許登錄本校IP範圍
  - A紀錄只允許140.124.0.0/16
  - CNAME不允許指向非本校網域

伺服器向上集中安全強化

- 入侵偵測防護(IPS/IDS) + 第七層次世代防火牆(NGFW)
- 網頁應用程式防火牆(WAF)
- 日誌集中管理(Log Server)
- 憑證集中管理(SSL Offload) +校內憑證核發(PKI)
- 負載平衡管理(Server Load Balance)

伺服器向上集中安全強化

- 備份程序：
  - 符合機關ISMS備份程序(3擇1)
    - Data Backup-Extreme (每小時)
    - Data Backup-Advanced (每4小時)
    - Data Backup-Basic (每天)
- 獨立網段IP(VLSM)

資安設備與管理平台

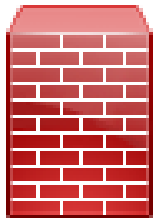
根憑證管理

EJBCA by Keyfactor

- EJBCA-CE (簽發憑證)
  - 根憑證私鑰加密保存
  - 校內資訊系統憑證請求檔簽發 (CSR)
  - 憑證週期管理
  - 資安設備解密憑證核發
  - 非對外校內職員工系統憑證核發
  - 以CA/B及PKI規範核發憑證

- 未來將整合其他開源套件，透過ACME以配合CA/B 極短憑證生命週期機制。

防火牆



- 所需功能：
  - NGFW (L7識別)
  - IPS(IDS)+AV+VA+FileSandbox (對內外各種類型攻擊特徵偵測)
  - Multi Vsys (依不同使用環境分區管理)
  - URL Filter (特定URL放行，監測內外所有URL存取)
  - VPN (結合上述功能進行存取管理)
  - Decryption (結合上述功能進行存取管理)
    - Inspection (Inbound)
    - Forward Proxy (Outbound)

Log管理系統 graylog

- OpenSearch(Elastic)+Graylog架構
  - Graylog (Log蒐集)
    - 進行設備分類
    - 資料欄位切割
    - Indice管理與維護
  - OpeSearch (Log儲存與管理)
    - Log儲存效能管理與分析
    - 自動化系統API存取

自動化

- **Airflow**
  - 透過自行撰寫的DAG (工作)實現自動化
  - DAG執行狀況記錄與分析
  - DAG執行失敗之管理

網路資訊管理平台

- 網路與資訊安全管理系統 (自行開發)
  - IP分配與管理
  - 封鎖管理
  - 自動化系統API
  - 流量管理
  - IP資訊管理 (防毒、VANS)
  - 外部黑名單管理(IP與FQDN)

其他輔助設備

- 負載平衡設備
  - 線路負載平衡
  - 伺服器負載平衡
  - SSL Offloading
- 具FIPS 140-2 Log Server
  - 供稽核與跡證調閱
  - 至少存放1年
- SDN導流設備
  - 多介面合併與拆分
  - 資安設備運用最大化
- 資料庫稽核
  - 資料庫所有CRUD存取軌跡

其他資安防護平台

- DLP
  - 螢幕側錄
  - 網路側錄
  - 端點資料流側錄
- GCB/VANS
  - 端點弱點管理
  - 端點安全政策管理
- APT進階持續防禦
  - 透過MDR平台進行偵測與應變
- Keycloak
  - 跳板機OTP認證

資安與流量管理措施實作方式

自動化作業

- 設備網路存取管理
  - 每日清除靜態ARP並寫入最新ARP資料
  - 每5分鐘清除並寫入變更之ARP資料
- 流量統計、分析與封鎖
  - 每10分鐘寫入流量統計資料 (含統計與封鎖)
  - 統計每日、每週、每月、每年流量資料
- IP管理與分析
  - 每天記錄內部IP使用資訊紀錄
  - 每10分鐘確認防毒軟體與VANS運作資訊
  - 黑名單IP與FQDN更新
- 資安管理、分析與封鎖
  - 防火牆規則到期通知(到期前月、週、日)
  - 資安事件封鎖

Apache Airflow

資安事件封鎖

內外部情資
- 教育部資安通報
- 資安設備偵測

Log分析系統
- 調閱相關跡證資料

網路與資訊管理平台
- 事件IP使用人資訊

防火牆
- IP使用人資訊封鎖

寄發封鎖通知
- IP使用人封鎖資訊與跡證資料

Apache Airflow

流量管理封鎖

防火牆

- 每筆Session資訊產生

Log分析系統

- 儲存防火牆存取資訊
- 調閱每10分鐘

網路與資訊管理平台

- 事件IP使用人資訊
- 儲存IP每10分鐘統計
- 調閱使用人週期流量資訊

防火牆

- IP超過流量封鎖

Apache Airflow

其他輔助管理套件

- 網路設備狀態管理平台
  - LibreNMS (設備狀態告警、紀錄、MRTG)
  - Cacti (Mactrack)
- 網路設備狀態分析
  - Grafana
  - SNMP Exporter
  - Prometheus
- 弱點掃描工具
  - OpenVAS (Greenbone)、Tenable

未來自動化整合項目

- DLP偵測自動化
  - 偵測未加密個資傳遞，IP使用者封鎖機制
- IP活化
  - 久未使用IP通知並強制釋放
- VANS弱點偵測整合
  - 針對VANS偵測結果進行IP使用者通知與封鎖機制
- 弱點掃描自動化
  - 弱點掃描與矯正預防流程自動化

結語

- 縱深的資安防護必須具備以下幾點：
  - 設備的支援
  - 架構與技術的具備(機關管理維運人員)
  - 即時諮詢與快速回應(廠商)
  - 法規的支撐與強制力(資安法)
  - **最重要的是長官的支持與肩膀**

- 兼具以上幾點，方才能將資安風險與事故降至最低
- 題外話：北科目前正C級被升級B級的降級申覆

本校相關政策公告

- 有關本校各單位及體系環境依據資通安全管理法及相關法規與行政命令之防護差異與配套措施說明
- 有關本校　網路連入政策變動說明，請務必詳讀以避免影響自身權益
- (資安法)為有效達到網路應用程式辨識與網路封鎖告知，請依說明將資訊設備導入本中心自簽根憑證
- 有關網路封(解)鎖機制與權益說明，請詳閱使用校內網路遭到資安事件封鎖帳號與IP時，解鎖申請注意事項說明
- 為配合資通安全管理法，本中心導入VANS(含GCB)控管機制，相關衝擊請詳閱

Q&A


工業推手一世紀．企業搖籃一百年
100 Years of Excellence · Cultivating Entrepreneurs of Tomorrow
TAIPEI TECH
Since 1912
國立臺北科技大學
National Taipei University of Technology
國立臺北科技大學