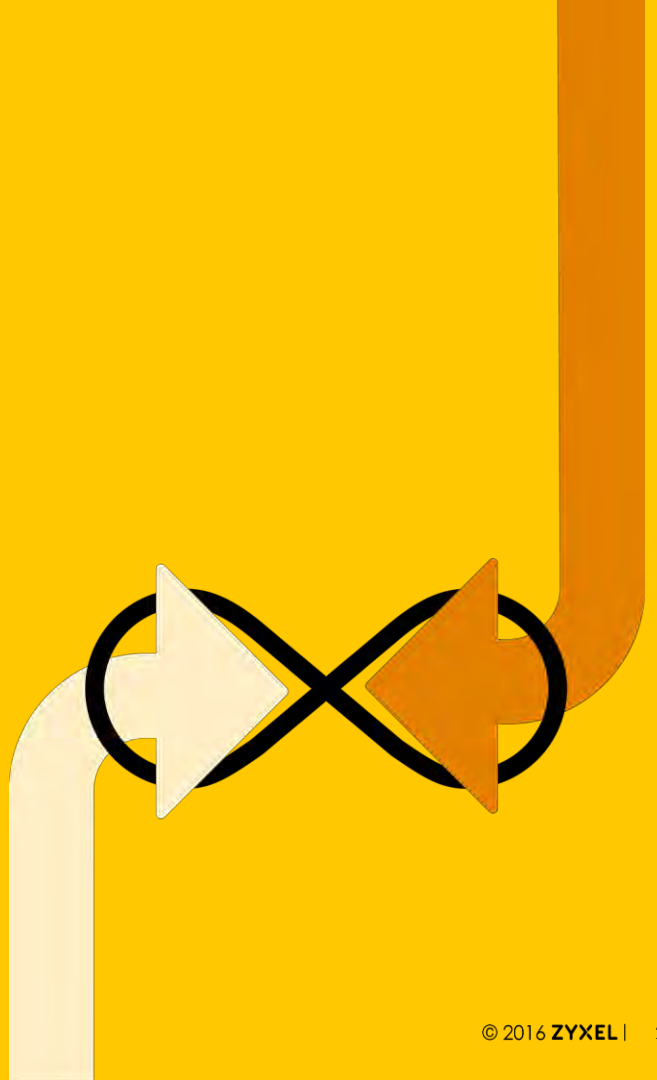
資安防禦策略及雲端運用

主講人：合勤科技 PMO 資深經理 丁弘培

ZYXEL
Your Networking Ally

內容綱要

- 資安網管的挑戰
- 資安網管的對策
- 合勤資安網路方案
- 案例設計與討論



資安網管的挑戰

企業持續營運的威脅與衝擊

	威脅	衝擊	趨勢
第一名	網路攻擊	無預警的資訊與通訊中斷	使用互聯網進行惡意攻擊
第二名	資料外洩	惡劣天候	社群媒體的影響
第三名	無預警與通訊		流失重要員工
第四名	安全事故	網路攻擊	新法規和更嚴謹的監管審查
第五名	惡劣天候	安全事故	互聯網相關服務的普及和高度採用

穩定安全的網路
就是企業的命脈

資料來源: 英國持續營運管理協會, 2017年5月

資安事件發燒議題(IT)

2016危機重重　有資訊科技存在，就有安全議題

IT(Information Technology)

DDoS_Mirai病毒

- 2016/10 Dyn.com遭受大規模DDoS攻擊，CNN、Twitter、Wikia、Netflix等知名網站均受到影響
- 2016/11 幾乎造成賴比瑞亞全國網站癱瘓

APT攻擊

- 台灣：惡意程式入侵銀行自動櫃員機電腦系統，60小時內以遠端操控模式，盜領新台幣8,000多萬元

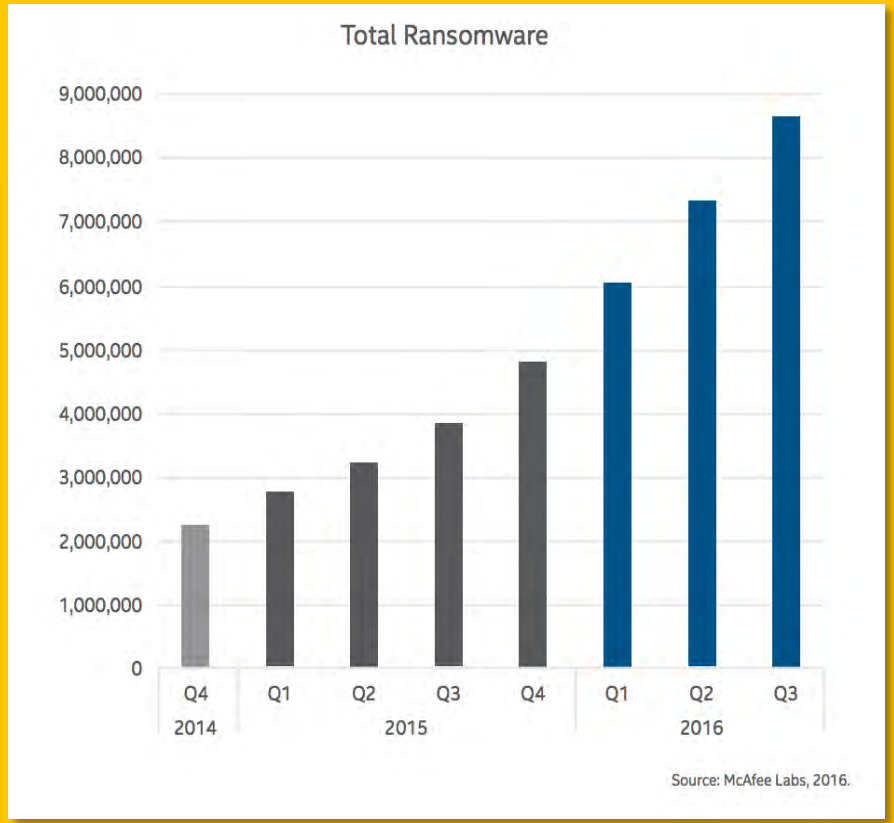
圖片取自：Dyn.com

圖片取自：The Hacker News

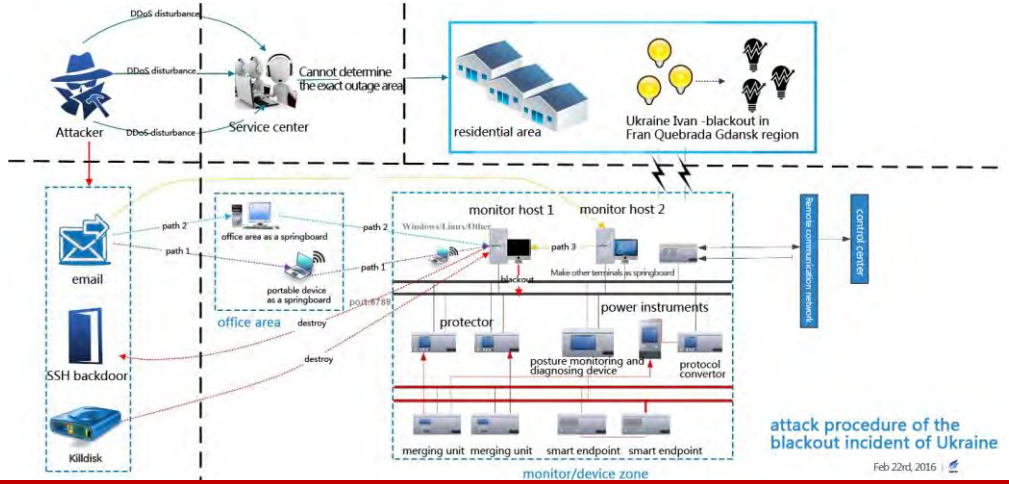
資安事件發燒議題(IT)_勒索軟體的肆虐

勒索軟體

- 突破1,000萬， 2015~2016勒索軟體數量成長一倍
- WannaCry: 全球超過150國、30萬台電腦受感染



資安事件發燒議題(OT)



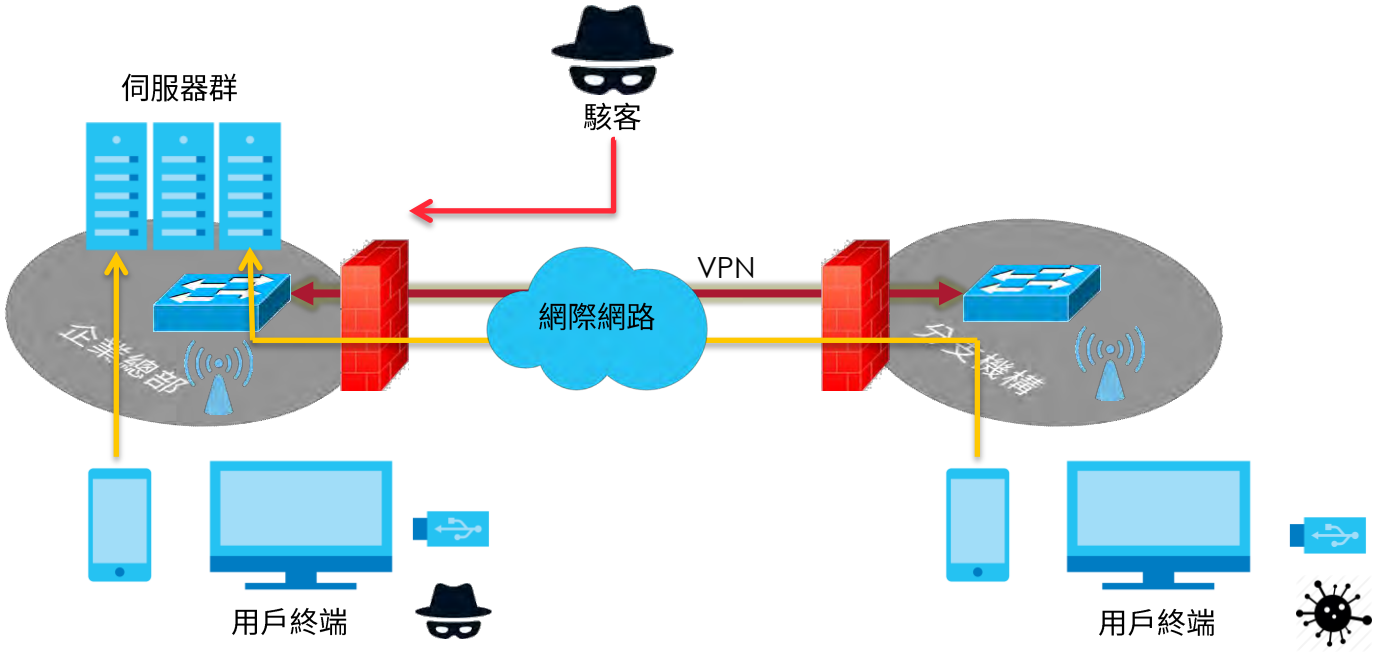
OT(Operation Technology)

- 40% 工業電腦曾遭受攻擊
- 2016/11/25~26 舊金山鐵路收費系統感染勒索軟體，市民無需付款即可搭車
- 2015/12/23 烏克蘭電力網路受到駭客攻擊，導致數十萬戶大停電

圖片來源：科技新報

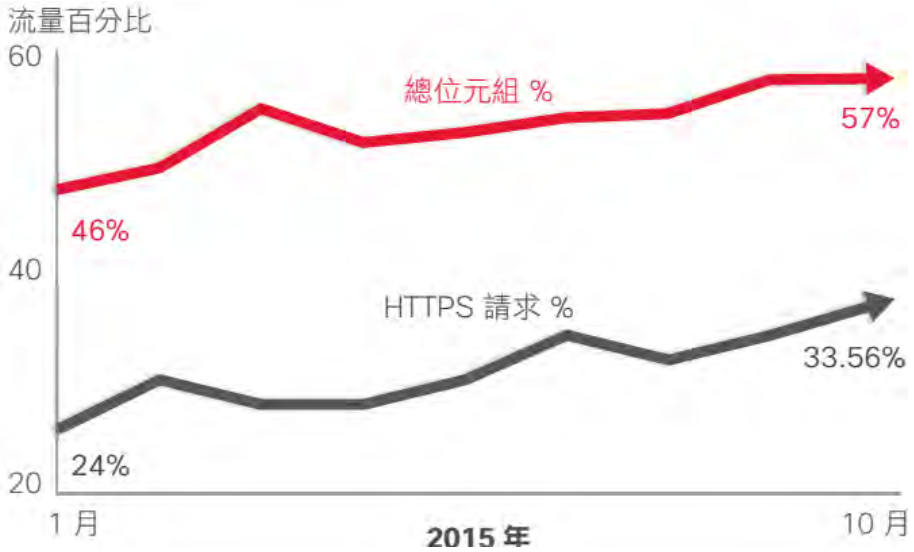
傳統防火牆架構防禦力不足

- 行動裝置與隨身碟都是潛在的資安漏洞。
- 駭客蒐集情報、竊取身分、橫向移動、提升權限，進而支配網域，發動全面攻擊。



HTTPS成為主要網際網路流量形式

- SSL佔資料傳輸57%、
  連線需求33.56%，
  成為最主要網際網路流量形式
- 加密流量可能造成防火牆誤判

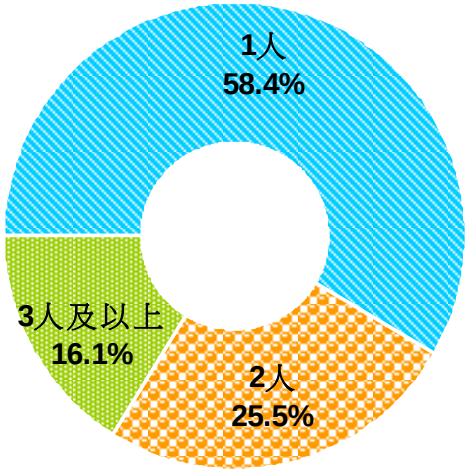


資料來源: Cisco資安研究

缺乏資安管理人才

資料來源： EventTracker

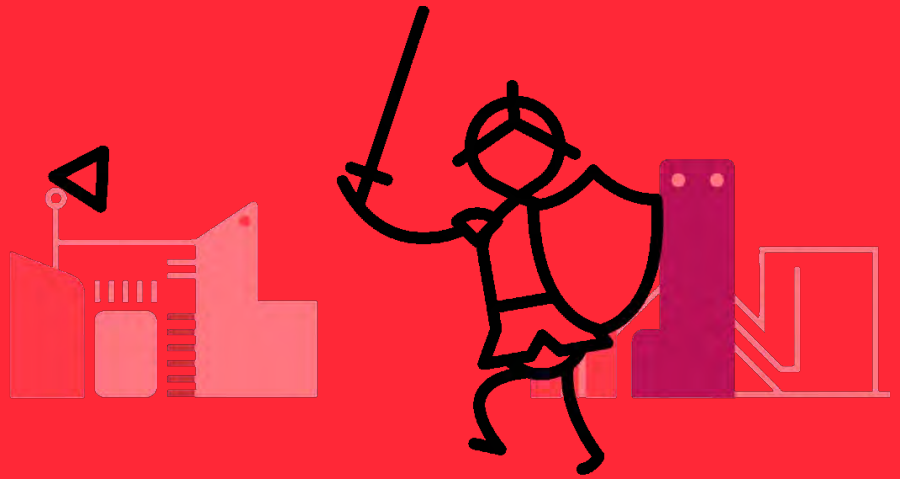
國內企業資安人力數量



資料來源：MIC，2016年4月
備註：N = 500

EU GDPR

資安網管的對策



層層防禦、區區安全

- 防火牆：邊境＋內部，層層把關
- 交換器：網管功能，聯合禦敵
- 無線網路：L2 隔離

資安防禦新觀點-區域聯防

當1號船艙不慎進水時，
系統將第一時間通知控制中心，
同時立即關閉2號及3號艙門，
以防止災情擴散。

大數據分析_看得廣、管得深

入侵、偵測、防禦(IPS)

安全資訊蒐集與
事件管理(SIEM)

大數據安全
資訊分析(BDSA)

機器自動學習與
分析(AutoML)

偵測
(Detection)

蒐集
(Collection)

分析
(Analysis)

作動
(Action)

進階防火牆功能

- 防火牆具備進階UTM功能

- 防火牆具備 SSL (HTTPS / TLS) 封包檢測功能

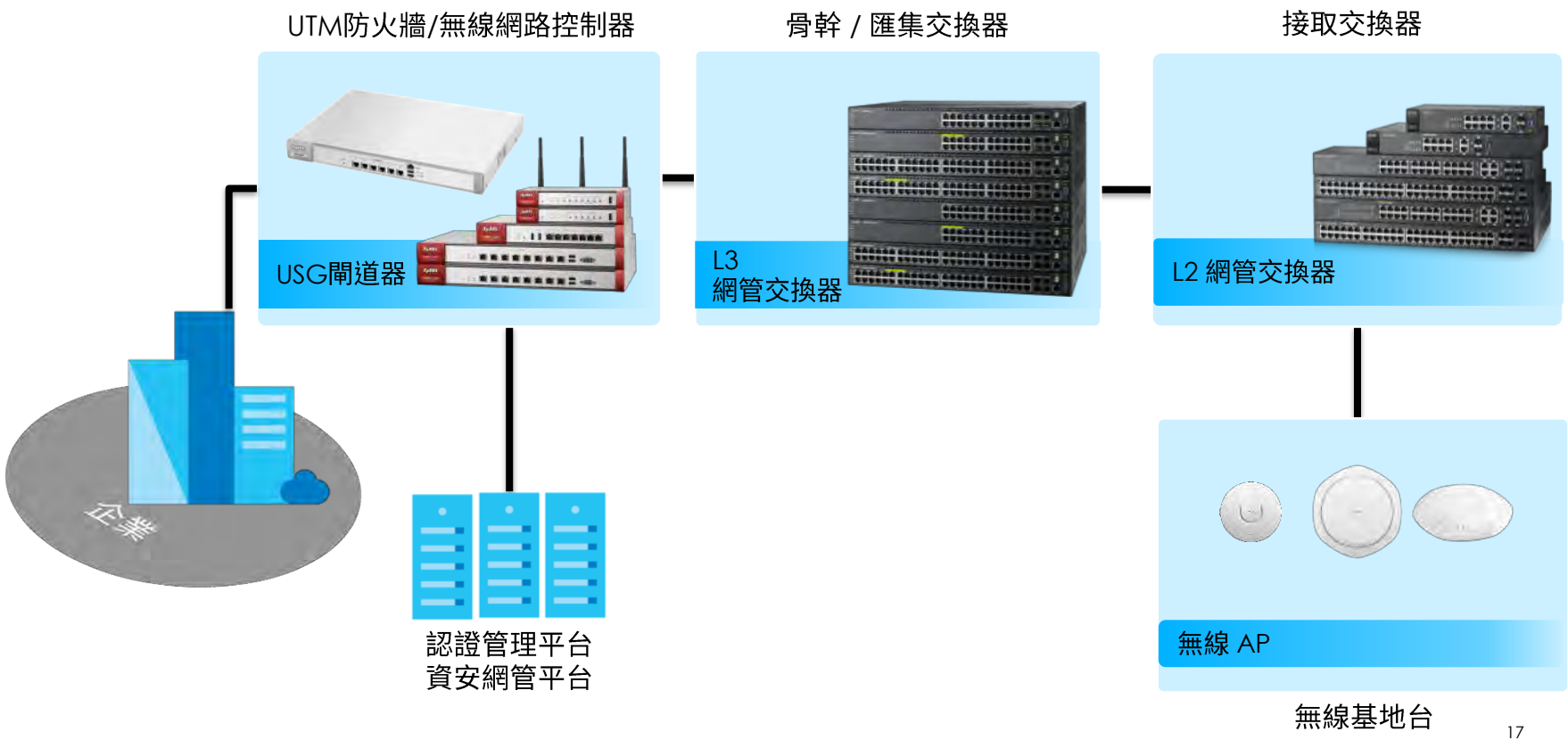
資安網管的對策

- 大型企業機關
  - 增加防禦寬度
  - 增加防禦深度
- 中小企業機關
  - IT委外、雲端管理，共享專家資源
  - 啟動身分驗證，確保存取安全

合勤資安網路方案

- 資安防禦新趨勢-合縱連橫

傳統企業網路架構


UTM防火牆/無線網路控制器
骨幹 / 匯集交換器
接取交換器
USG閘道器
L3
網管交換器
L2 網管交換器
企業
認證管理平台
資安網管平台
無線 AP
無線基地台

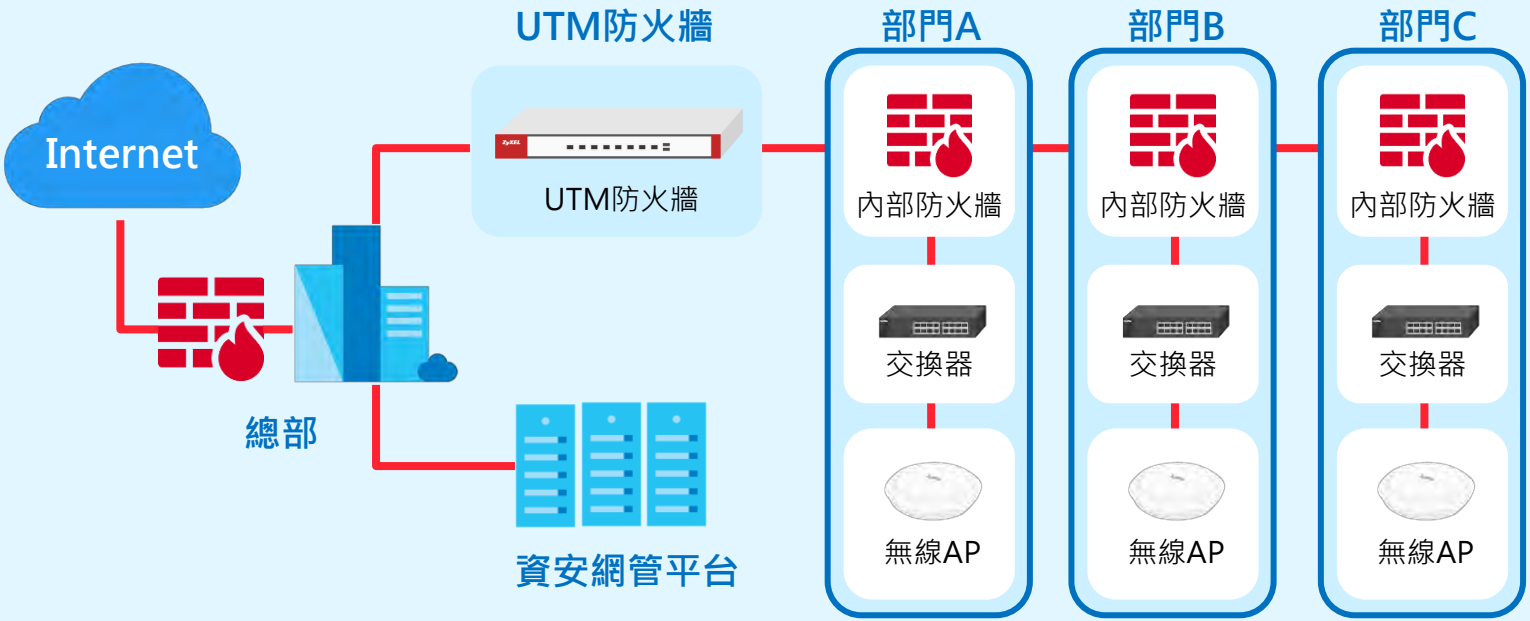
增加防禦寬度

- Zyxel 防火牆具備加密封包檢測功能(HTTPS & TLS)
- Zyxel 防火牆 結盟最優秀資安防護專家

- 強化內網區域防護
  - 交換器
    - 802.1X認證 / IP-MAC-Port 綁定 / ACL存取控制表
    - ARP 偵測 / 網路埠隔離 / DHCP snooping (防私設DHCP伺服器) / CPU保護
    - 迴圈防護 / Port Security (防非法MAC存取) / 入侵防護
  - 無線網路 (ZLD)
    - Layer-2 隔離
    - Intra-BSS 阻隔

增加防禦寬度_層層防禦架構

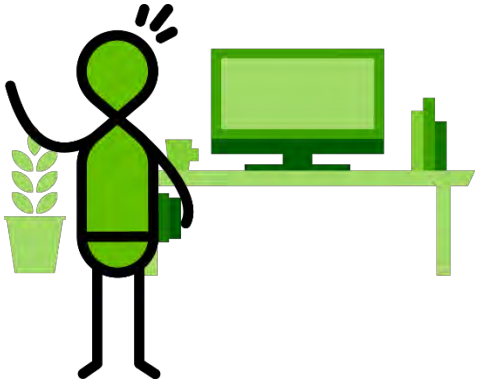
- 資安要從規劃開始
- 藉由網路流量、事件資訊，掌握異常與威脅

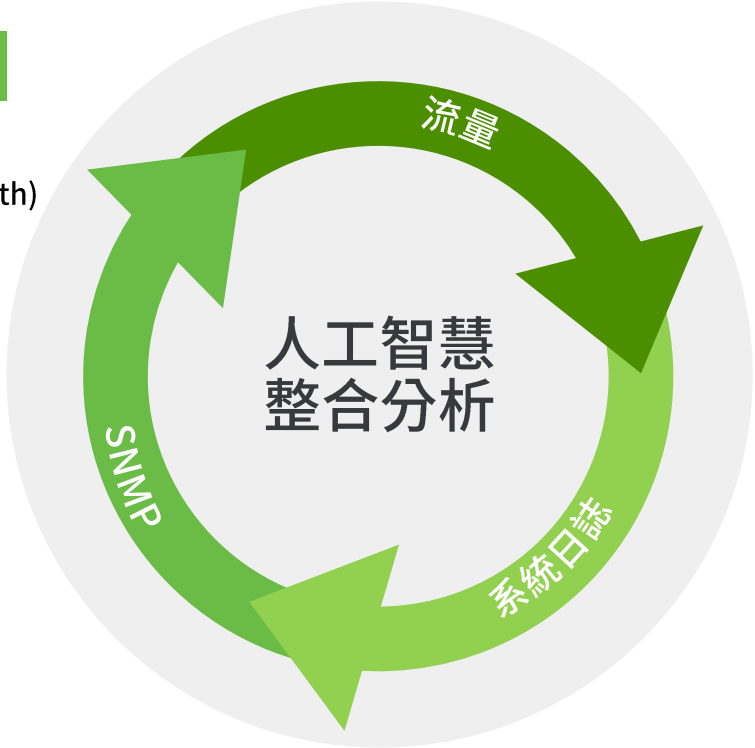


增加防禦寬度_資安分析管理平台

SNMP

. 設備健康狀態(Up/Down)
. 效能使用率(CPU/Memory/Bandwidth)
. 資產清單





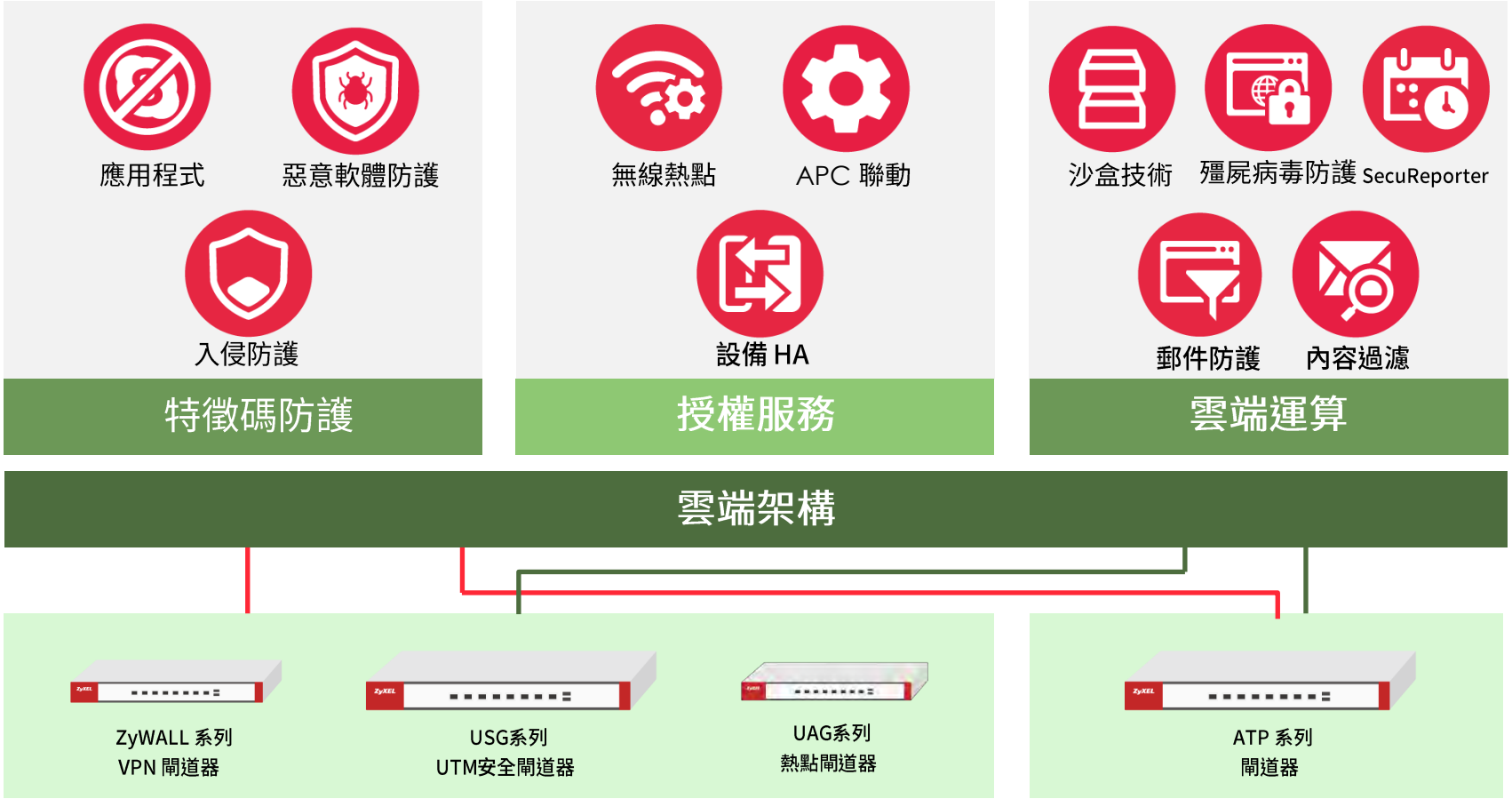
流量

. NetFlow/sFlow
. L3/L4 資訊
. 流量使用分析
. 封包大小與Protocol監控
. 流量型DDoS分析
. 了解流量大小的問題
. 繪製流量圖

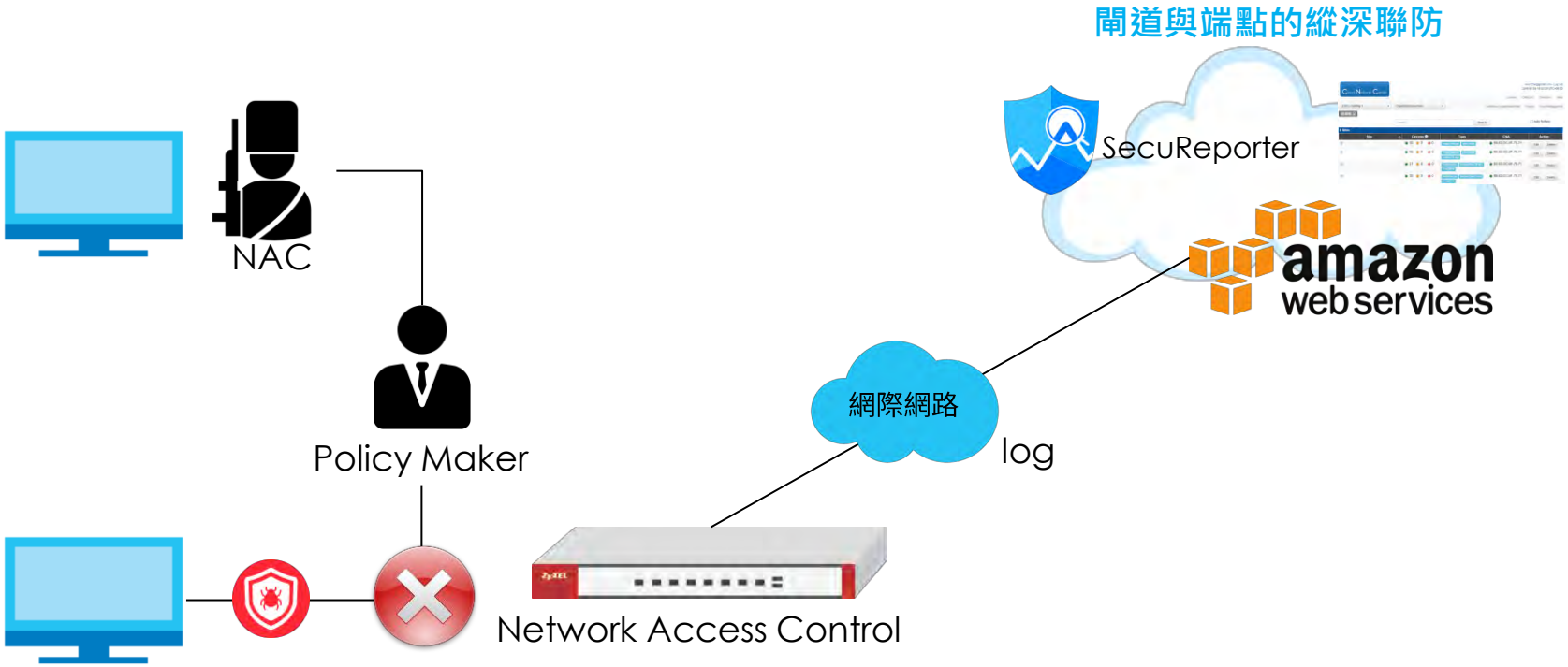
系統日誌

. Syslog已經成為標準
. 安全產品、網路設備、伺服器均可透過 syslog將事件 / 稽核 / 日誌資訊匯出
. 事件 (Event) 記錄人的使用行為
. 可以用來分析資安狀態
. 提供L7應用層資訊

增加防禦深度_特徵碼防護與雲端運算

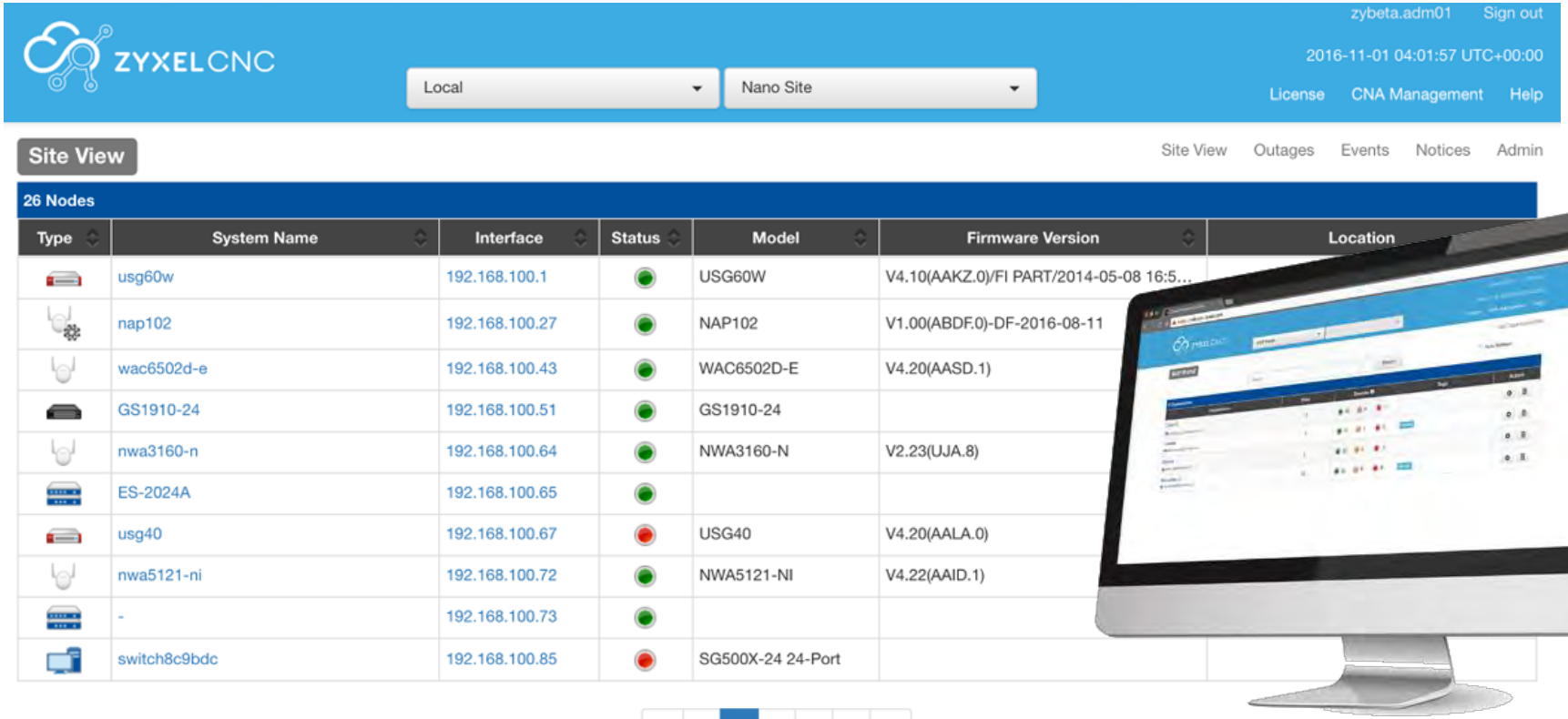


增加防禦深度_防火牆與端點精準防禦



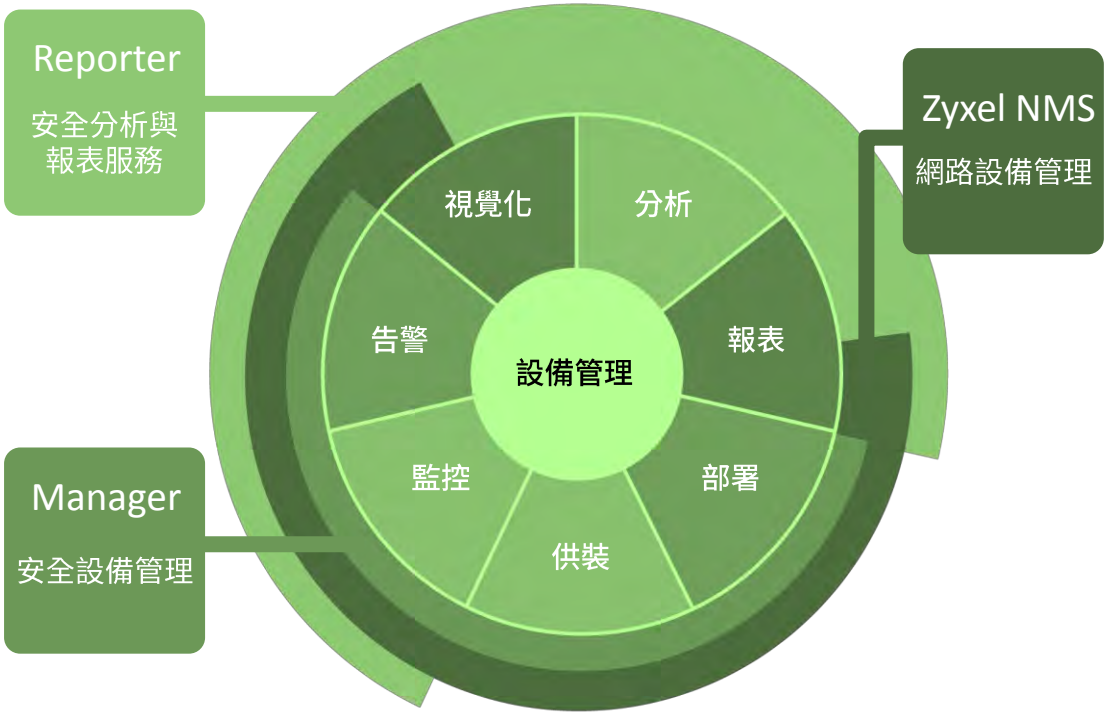
設備管理協防_Zyxel One Network

- ZON: 設備相互辨識、合作分工
- CNC: 雲端網路管理中心



完整的報表呈現與掌控

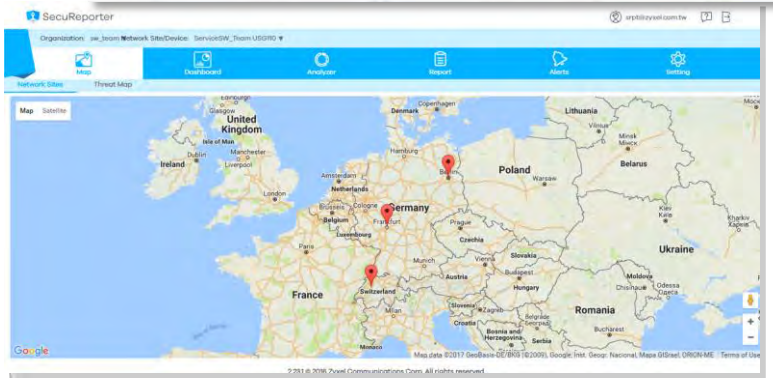
- 虛擬化落地平台
- 支援多租戶分層管理
- 具備端點解決方案
- 具備收集sFlow/Netflow流量資訊能力，可分析應用服務使用分佈狀況
- 具備資安事件分析，並產出報表功能
- 搭配Zyxel設備可下Action，完善區域聯防機制

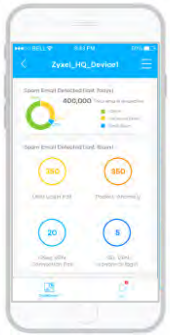


整合系統儀表板與地圖

系統儀表板

地圖





行動App

行動App 即時掌控訊息

Timestamp	Severity	Organization \ Network	Event Type	Description
2016.09.09 21:00:00	1	ZYXEL DE\ Device1	Malware/virus	Malware/virus counts > threshold
2016.09.09 19:50:00	1	ZYXEL TW\ Device A	Attack counts	Attack counts > threshold
2016.09.09 18:00:00	1	ZYXEL TW\ Device B	IP/URL/DNS reputation	Bad reputation connection over 2 times
2016.09.09 18:30:00	2	ZYXEL DE\ Device 2	Storage usage	> 95%

資安防禦四部曲

偵測

- 設備提供syslog／flow數據

交換器

防火牆

蒐集

- 根據蒐集的syslog/flow數據建立歷史用量
- 發現任何異常突增即時告警

作動

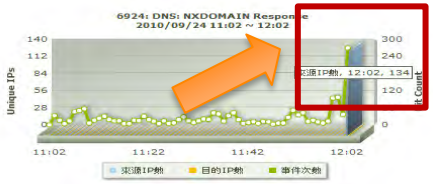
- 外網攻擊由閘道器阻擋
- 內網異常行為由內部交換器阻擋

交換器

防火牆

分析

- 管理者收到異常突增告警後
- 確認攻擊來源，下達封阻指令

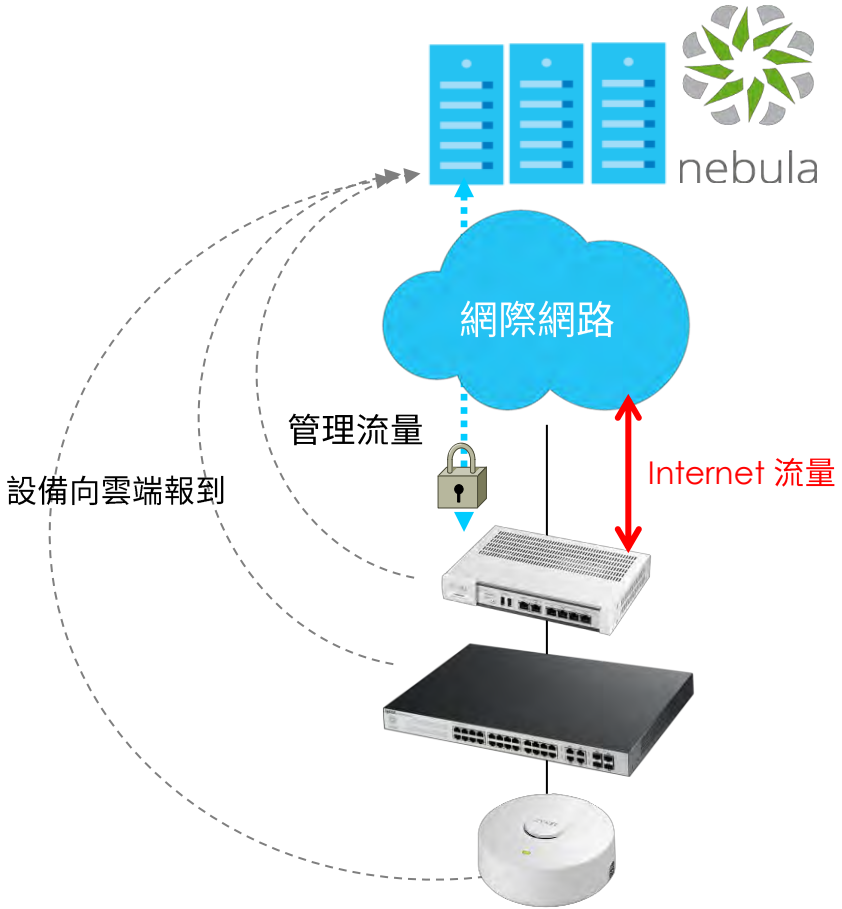


合勤資安網路方案

- 雲端網路方案

雲端網路_架構與特色

- 擴展彈性
- 高度可靠
- 確保資安



雲端網路解決方案

Nebula 雲端管理中心 (NCC)	雲端管理基地台 (NAP)	雲端管理交換器 (NSW)	雲端管理閘道器 (NSG)	Nebula 行動App

雲端控制中心

零接觸設定供裝

多站點管理

集中視覺管理
提供即時監控與歷史報表

多站點管理

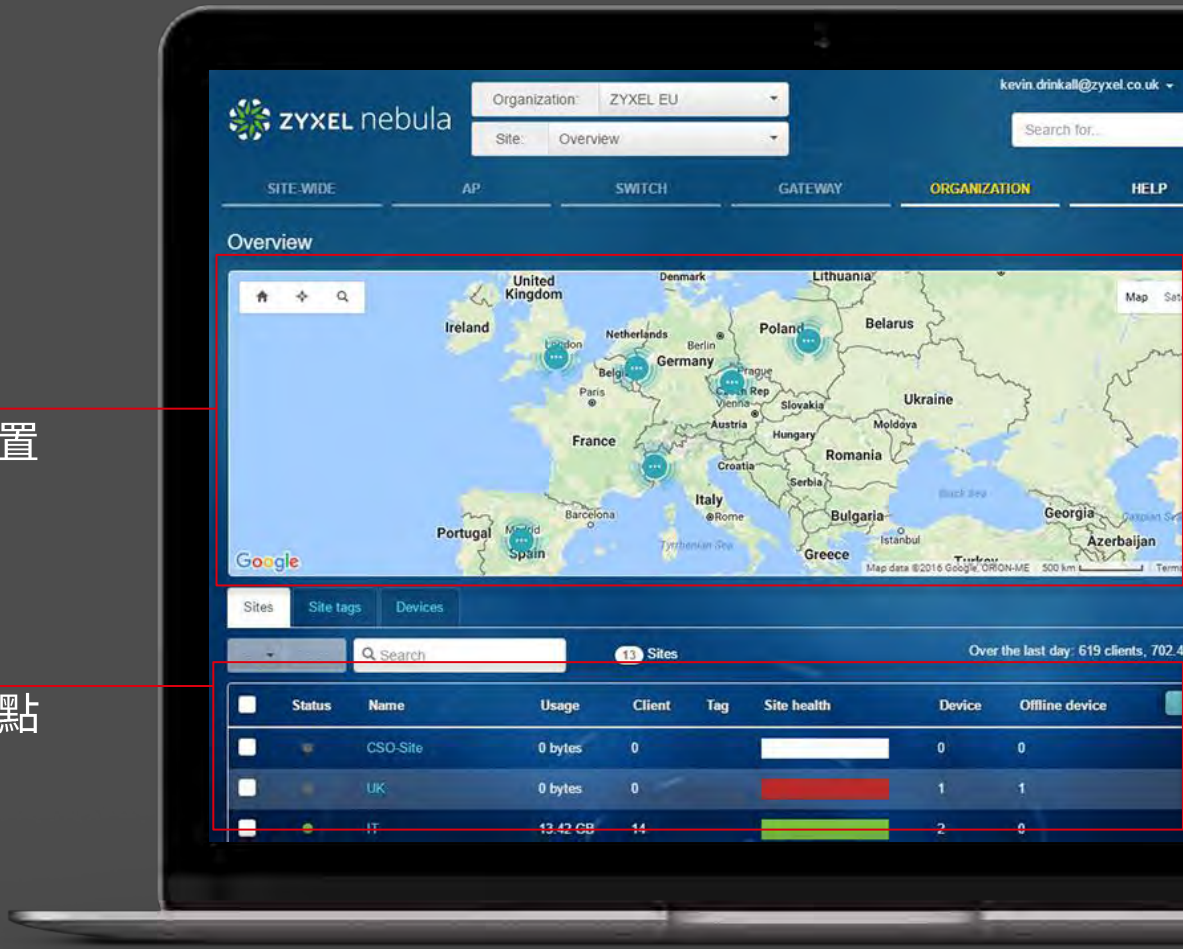
支援管理服務商、多租戶、多站點
和多層級角色管理

快速瀏覽全組織
設備狀態

多站點管理

立即檢視各站點和設備位置

檢視全組織站點
設備健康狀態



集中視覺管理

組織與站點
管理

檢視組織站點
設備狀態

設備搜尋

應用程式
即時流量統計

*: Requires NSG (Gateway) device on a site to provide Application statistics .

行動 APP

儀表板快速檢視設備狀態

支援照片上傳
紀錄設備安裝位置

內建 QR code 掃描功能
可快速新增大量設備

雲端管理無線AP

全站點設定管理

即時用戶及AP監控

SSID / VLANs 輕鬆設定，
認證登入網頁支援內外RADIUS

雲端管理交換器

- 高效網路供裝
- 即時監控流量
- 連接埠 & PoE 控制

雲端管理安全閘道器

零接觸 VPN 連線

簡化政策管理

身分認證與
應用程式管理

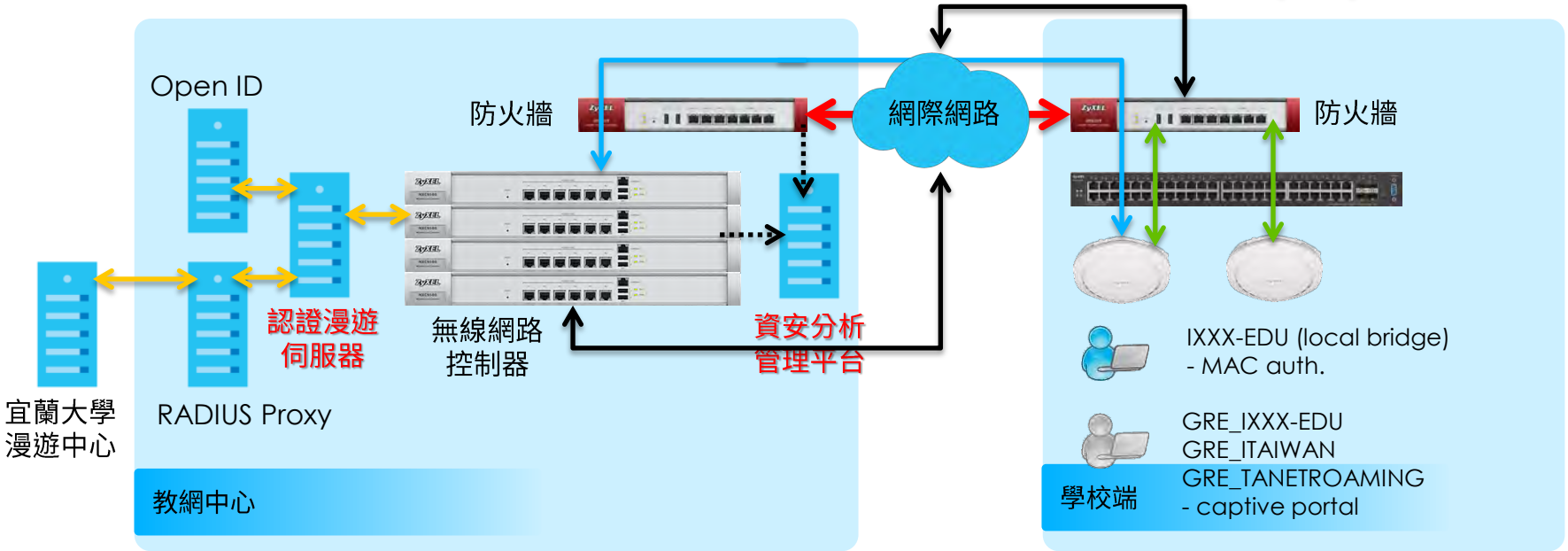
案例設計與討論

- 縣市教網中心網路
- 科技業者新廠房網路
- 連鎖門市VPN

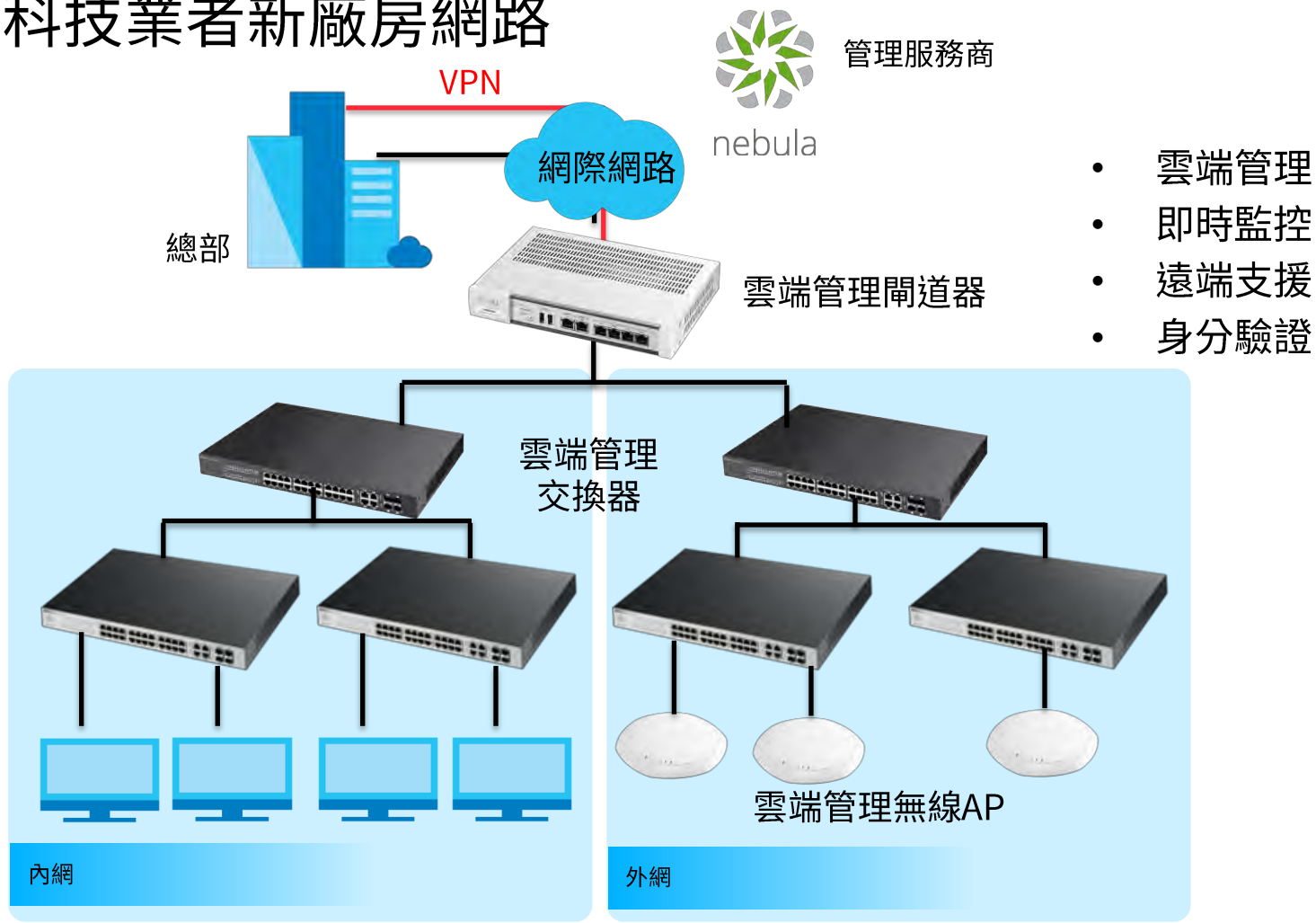
04

縣市教網中心網路

- 偵測、蒐集、分析、作動
- 認證、無線、資安、報表統一管理

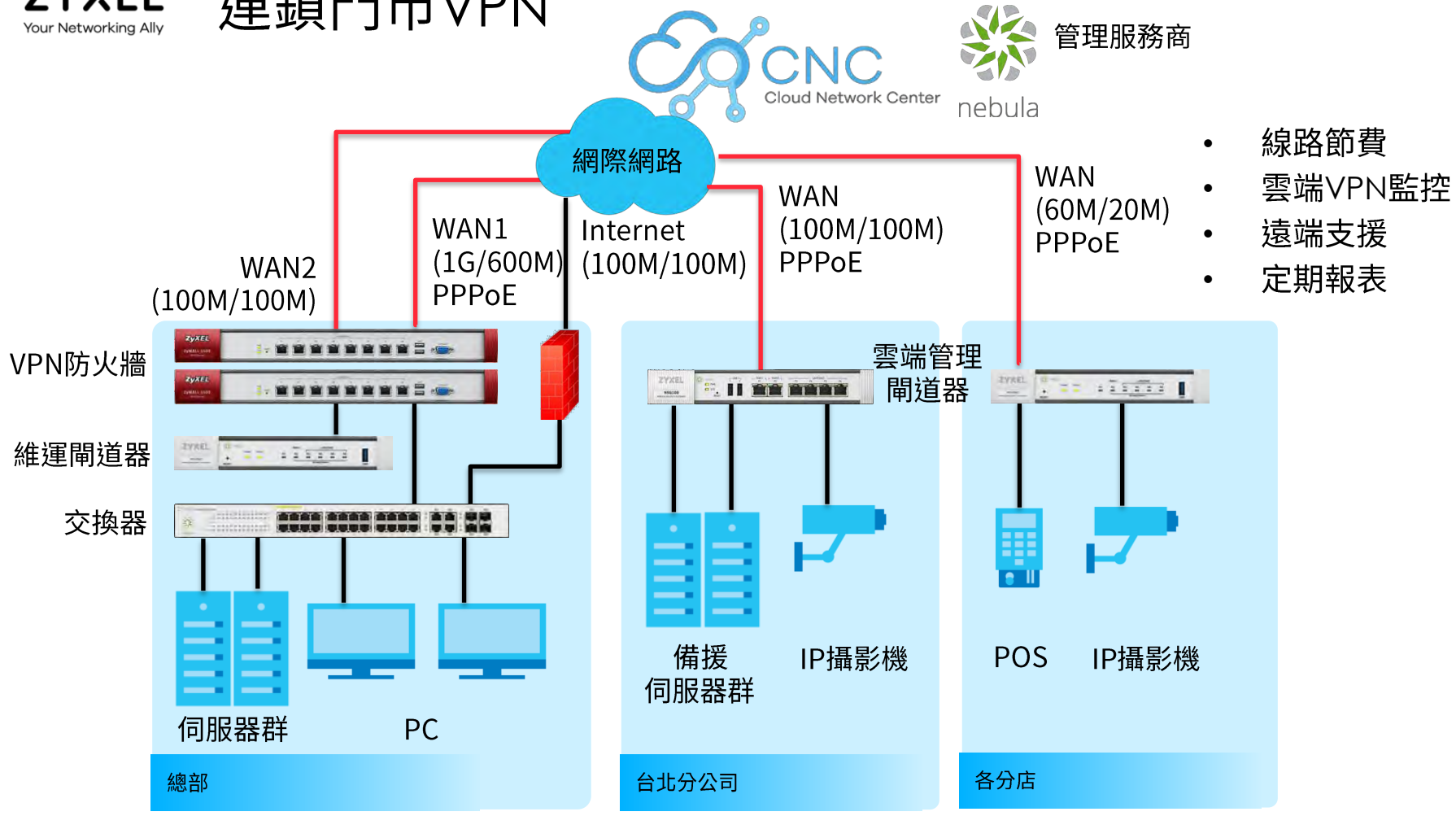


科技業者新廠房網路



- 雲端管理
- 即時監控
- 遠端支援
- 身分驗證

連鎖門市VPN

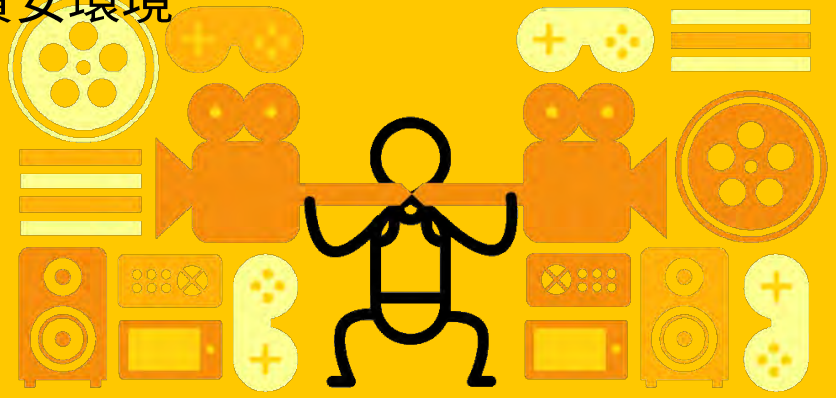


- 線路節費
- 雲端VPN監控
- 遠端支援
- 定期報表

結論

- 聯合防火牆、交換器、無線網路，提升防禦寬度
- 貫穿防火牆與用戶端，加大防禦縱深
- 利用大數據智慧分析，主動防範威脅

- 分享專家知識與資源，優化資安環境



ZYXEL

Your Networking Ally