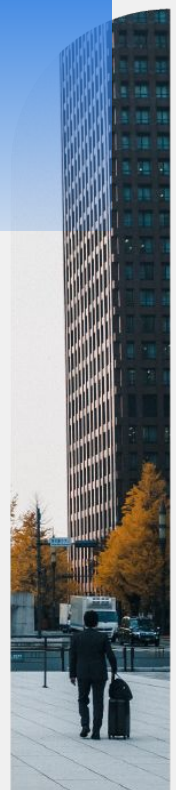
FORTINET資安鐵三角

擴展資訊安全的邊界

技術顧問 陳弘治

2021



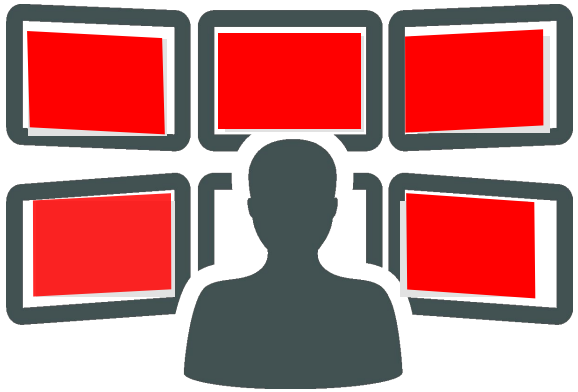
企業網路的現況

多品牌環境

終端設備快速增加

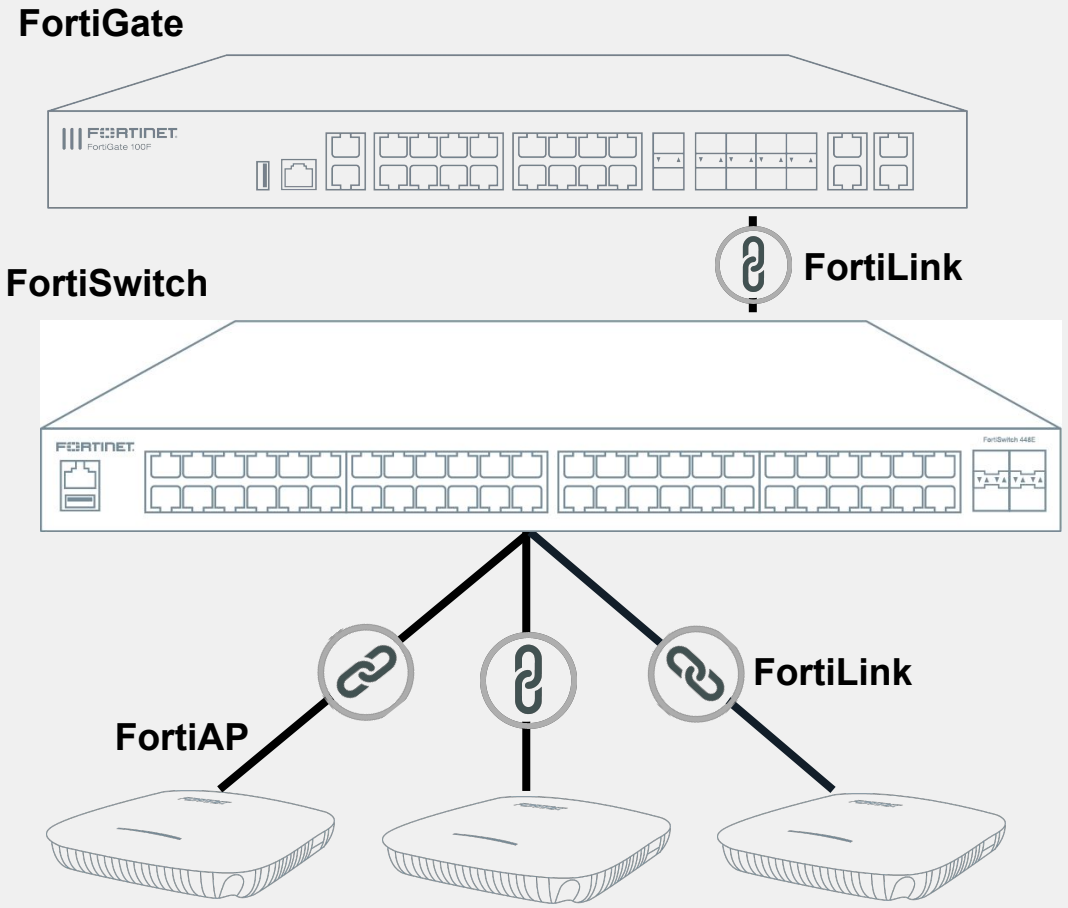
資訊安全的需求

IT人員的困境

複雜的管理環境	太多事件需處理	不完整的資安解決方案
		

Fortinet 解決方案：資安鐵三角

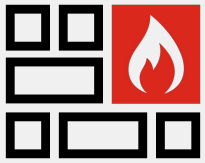
- 簡化管理
  - 自動化的部屬
  - 可隨時依照需求擴充架構
- 增加可視性
  - 自動生成網路架構
  - 豐富的終端設備資訊
- 整合的資訊安全架構
  - 中央控管,將資安擴展到全網路
  - 提供NAC功能



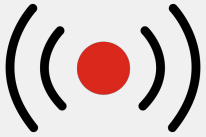
資安鐵三角特色

網路架構

NGFW



無線網路



交換器

NAC

整合管理

單一管理介面

單一設定檔

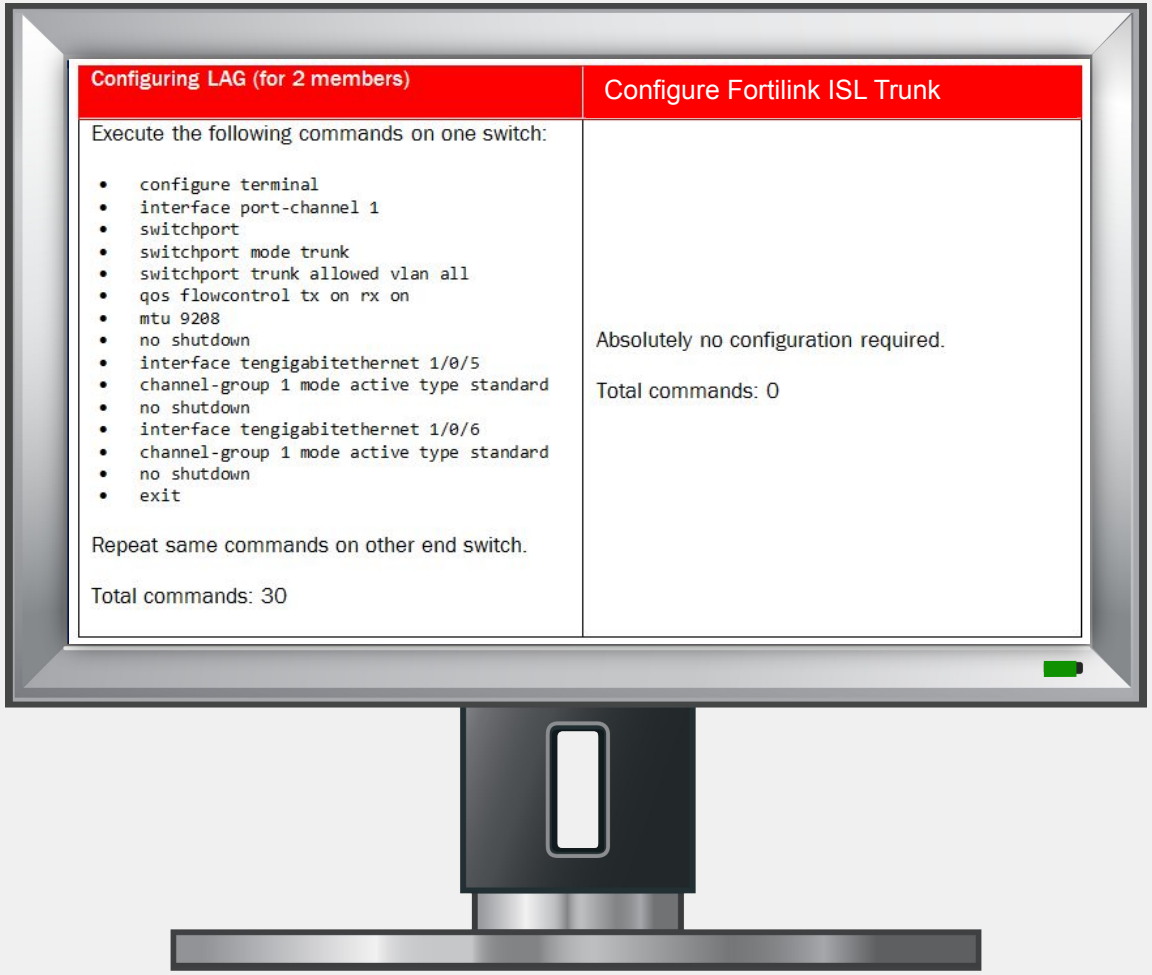
降低營運成本

簡化管理

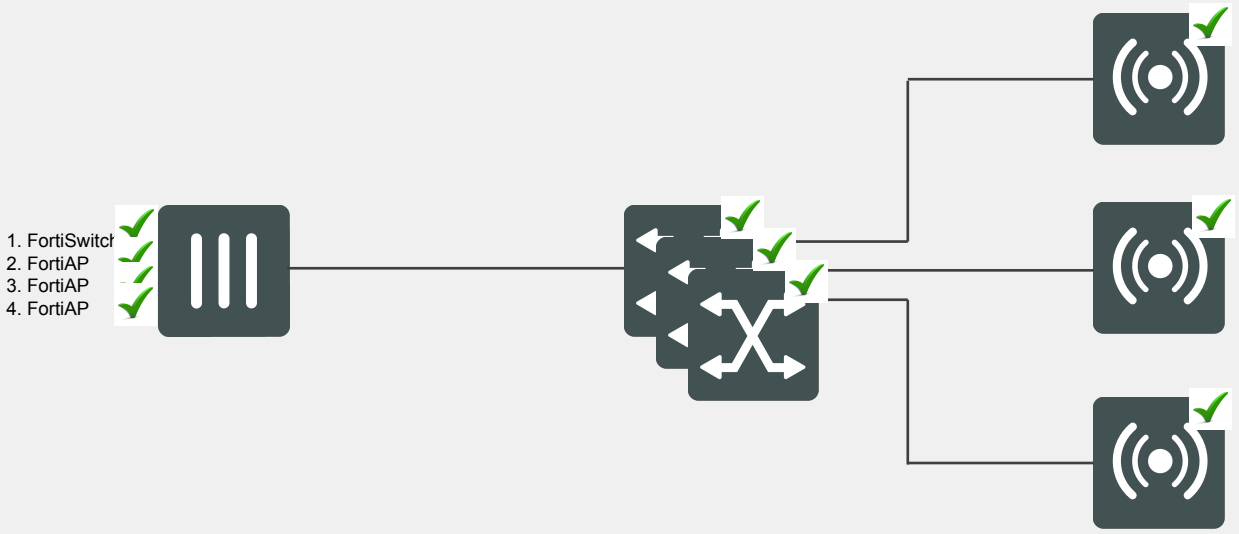
簡化管理

傳統的網路設定

- 每台switch間的trunk 與LACP皆得手動設定:
  - » Step 1: Config terminal
  - » Step 2: interface port-cannel 1
  - » Step 3: switchport
  - » Step 4: switchport mode trunk
  - » […]
  - » Step 19: interface ge-1/0/0
  - » Step 20: switchport mode access
  - » Step 21: switchport access vlan10
  - » […]
  - » Step 101: interface port-cannel 2
  - » […]
  - » Step 106: switchport mode trunk
  - » […]
  - » Step 114: switchport trunk allow vlan20
  - » […]

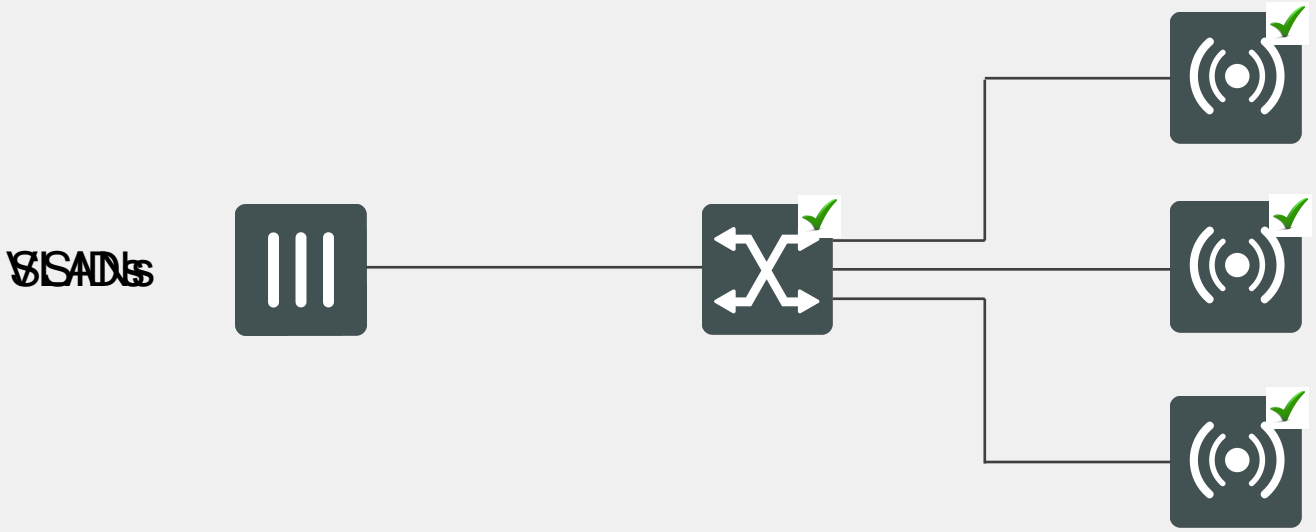


資安鐵三角:一鍵完成設定



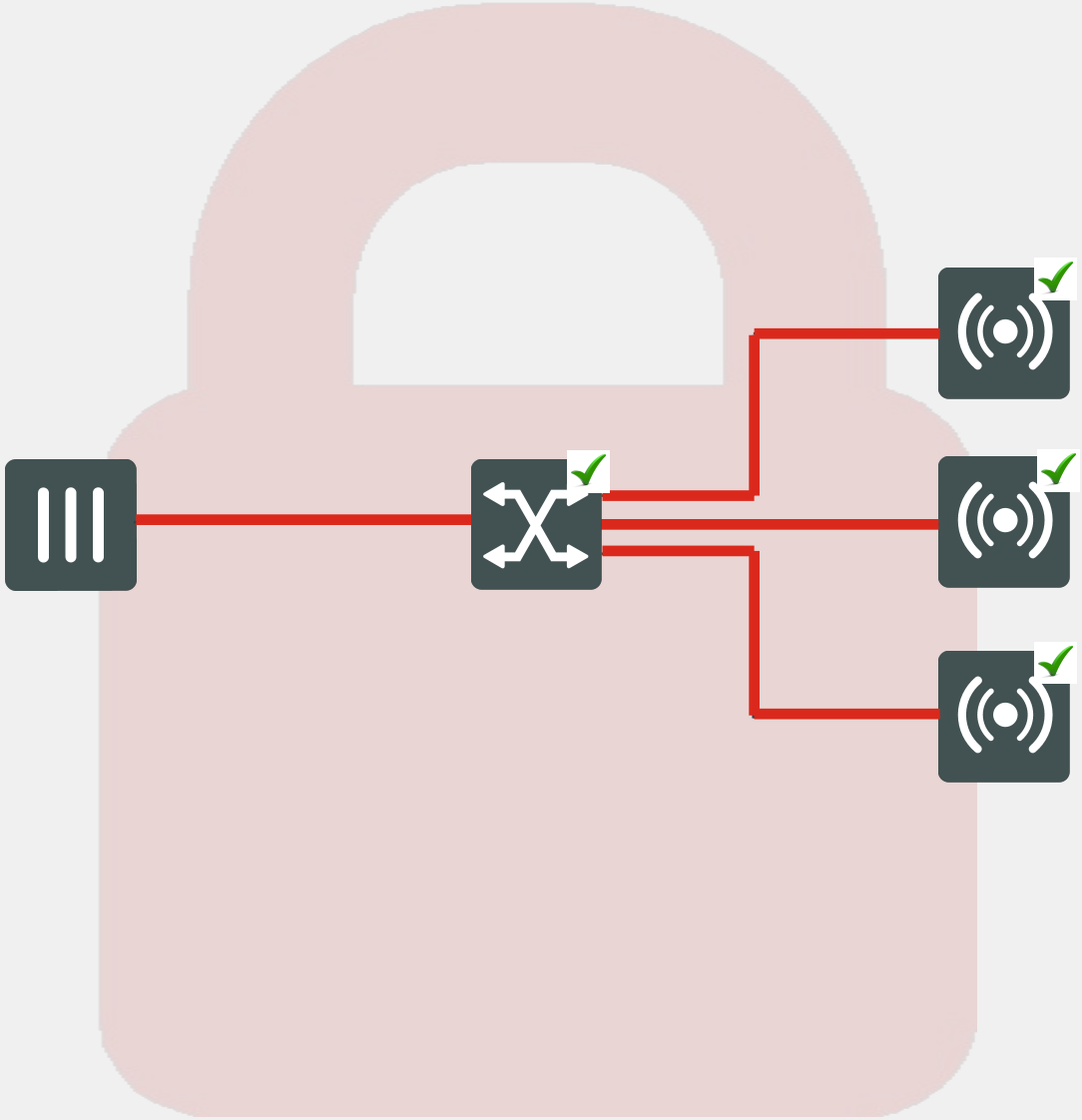
- 將交換器與無線基地台接上
- 在FortiGate上點選授權
- 完工!
- 重複此步驟新增交換器與無線基地台
- 無須額外的設定

單一介面完成所有設定



- 從單一介面做網路設定
- 設定檔自動派送至相對應的設備
- 無線網路設定也在此處完成

單一介面完成網路資安設定



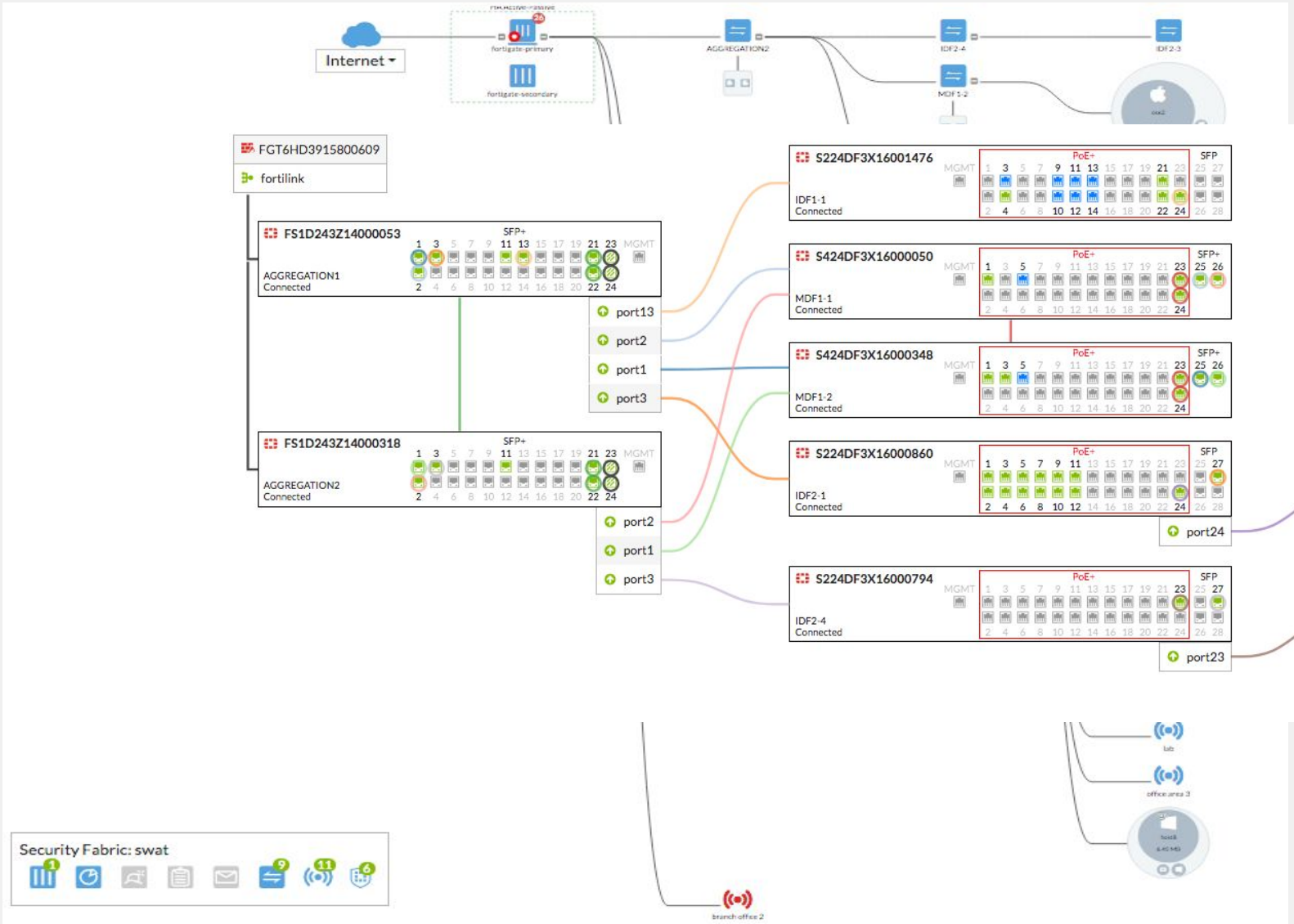
- 設定資安政策
- FortiGate 自動將資安政策派送至相對的設備上執行
- 資訊安全政策由防火牆延伸至網路接取點

增加可視性

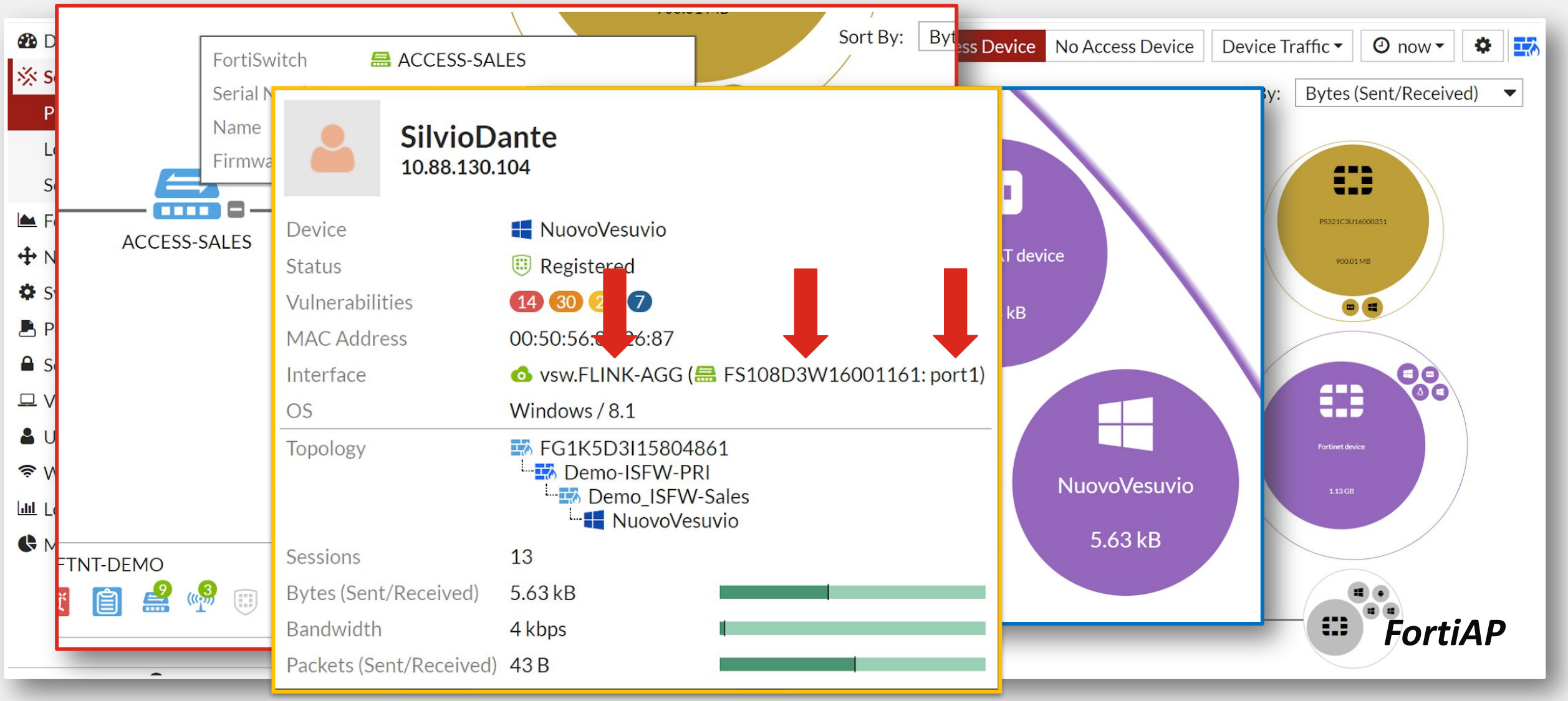
目前網路接線??

自動生成網路架構圖

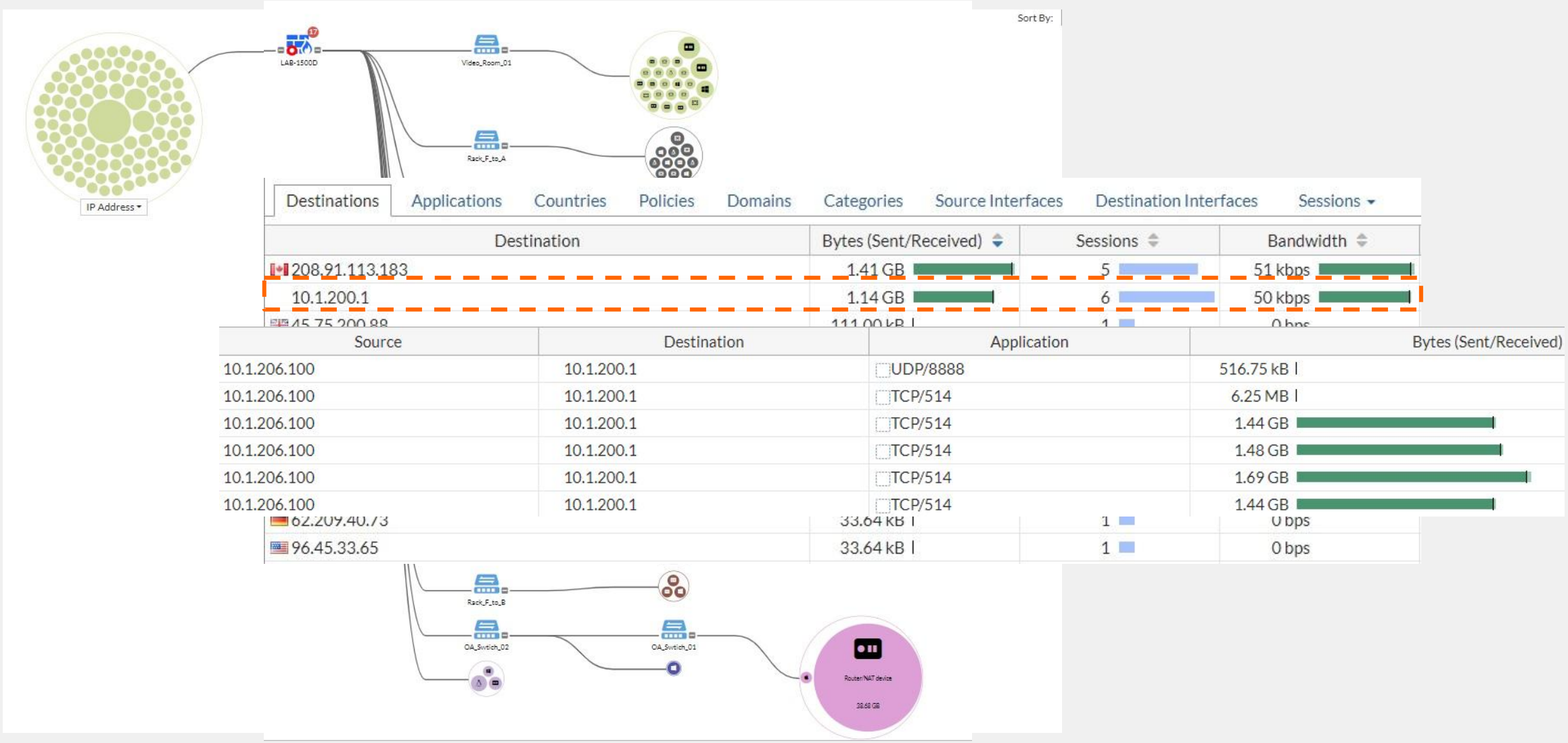
FortiExplorer 實體網路架構圖



查看終端設備資訊

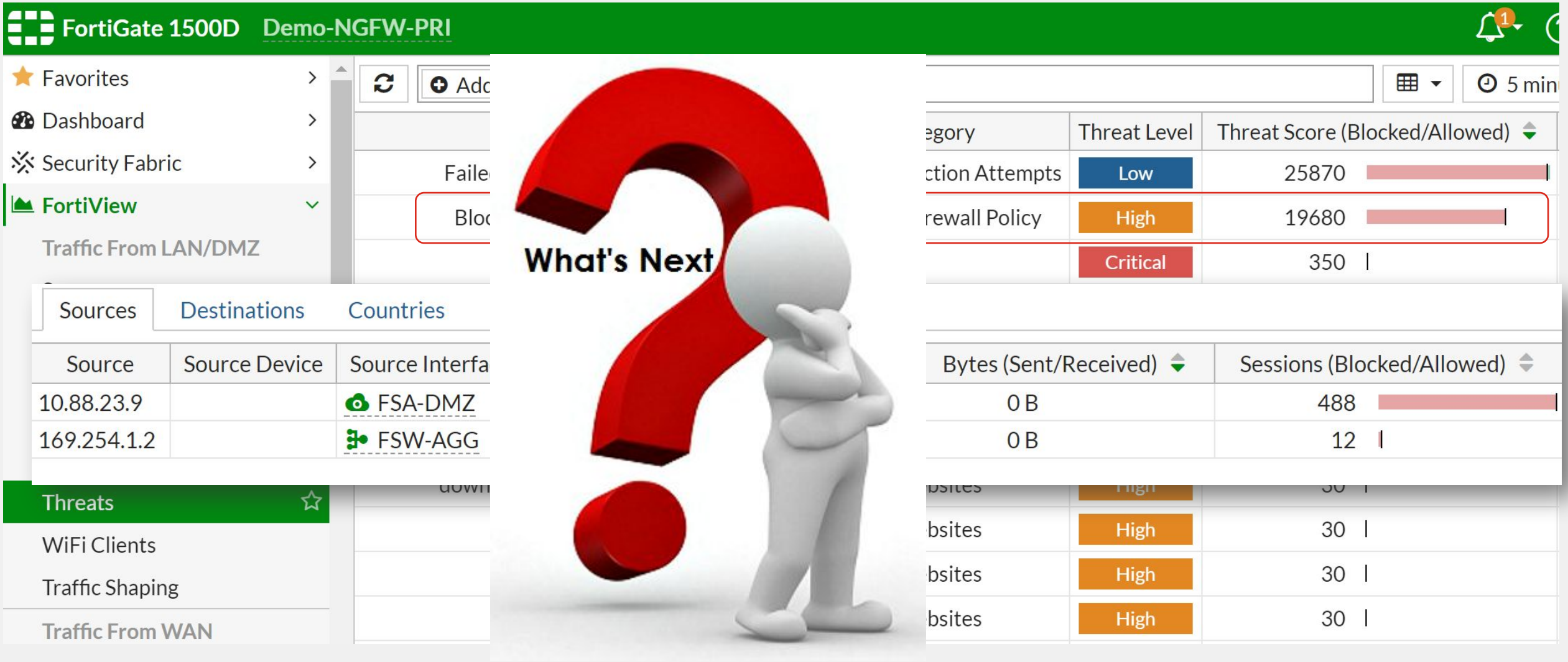


查看終端設備流量使用狀況

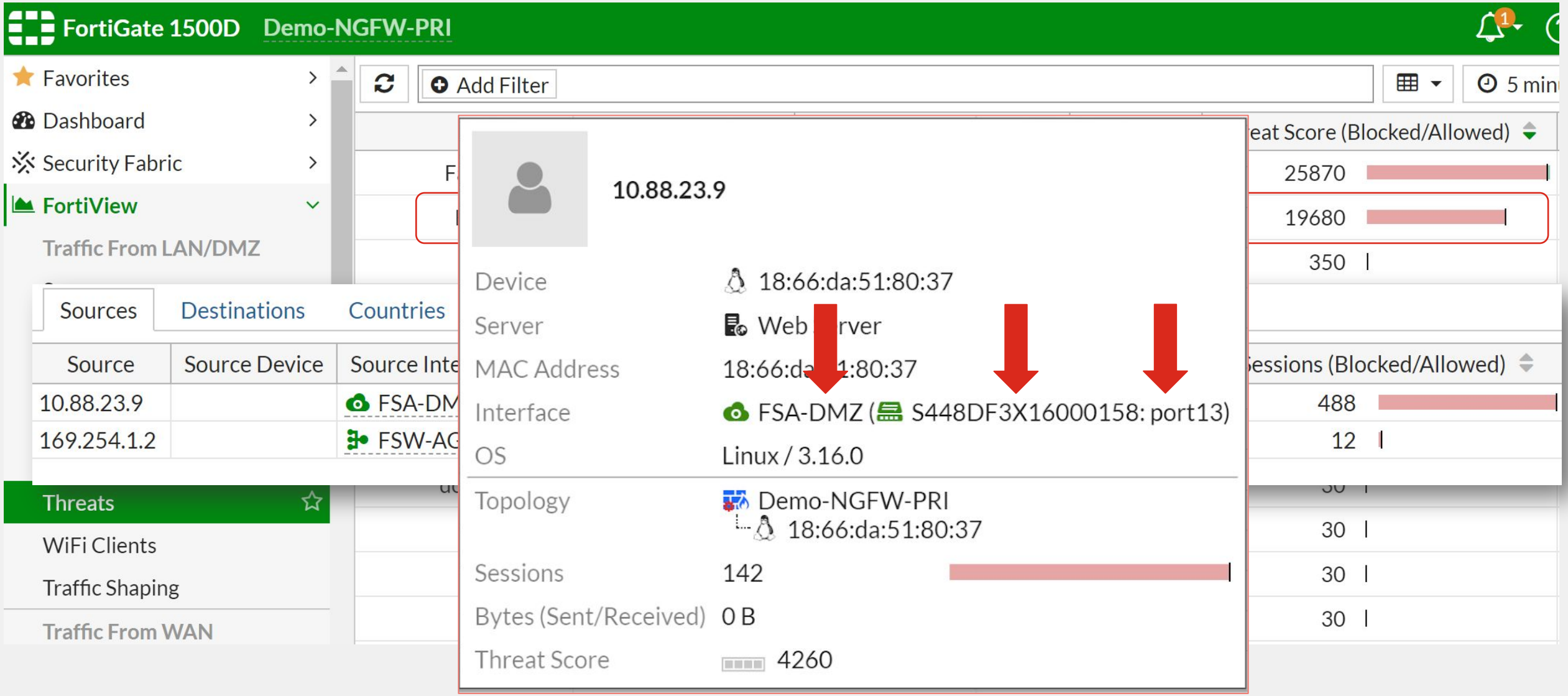


資安管理

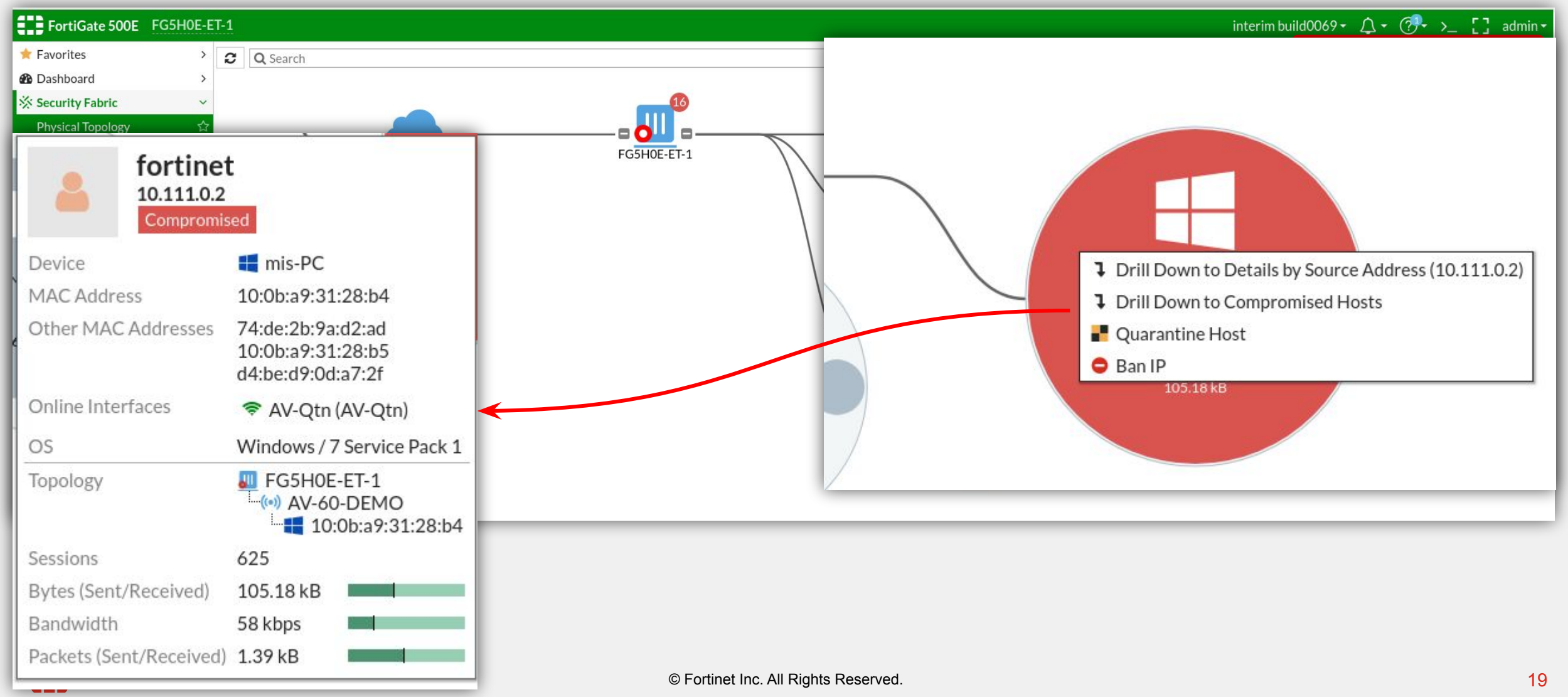
傳統查找方法



在資安鐵三角中查找使用者



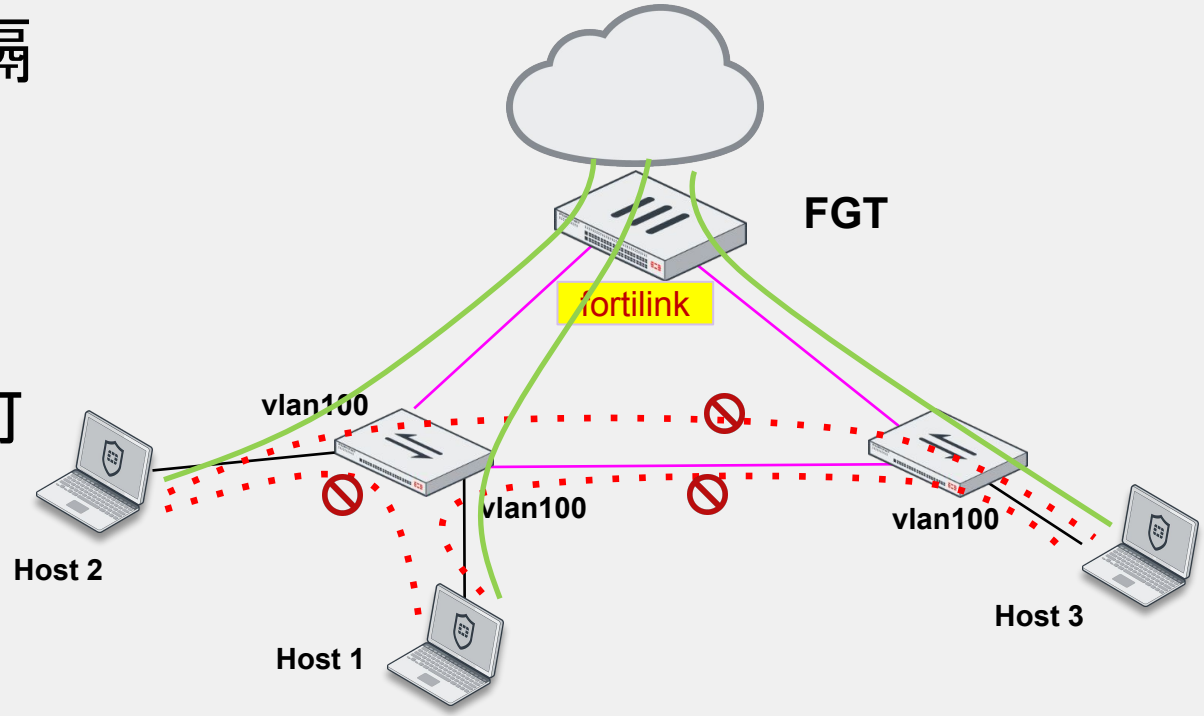
在交換器上將問題主機隔離



阻隔同網段的流量

可讓同網段使用者不能互通,防止橫向感染

- 一鍵開啟 “block intra-vlan traffic”阻隔同網段流量
  - 同網段PC無法看到彼此
  - PC流量只能送往FortiGate
  - 若PC間有特殊需求要能互相傳送資料,可在FortiGate上設定防火牆政策允許



內建NAC 為IoT設備提供安全控管

資訊安全

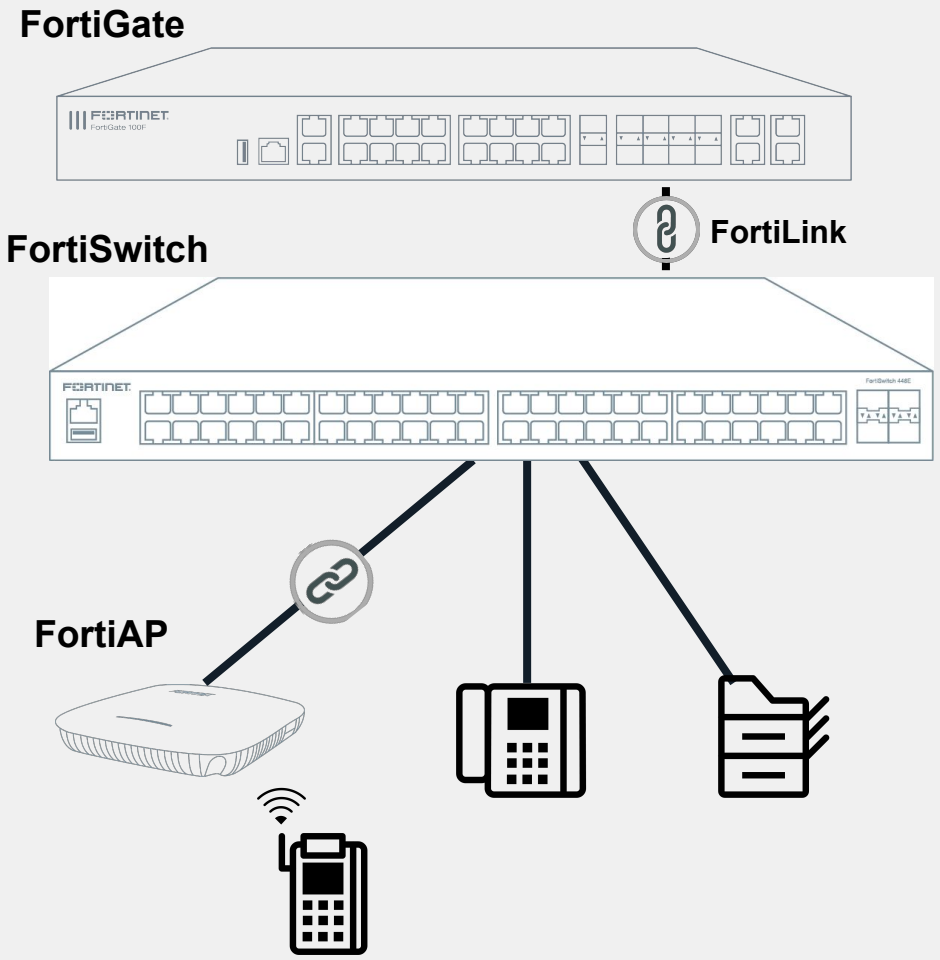
- 自動為IOT設備做識別並分類
- 依據IOT設備的類別指派至不同的網段的
- 持續監控網路異常行為與風險評估,並自動針對狀況反應

簡化 – 使用FortiGate來偵測設備

- 無須額外的設備
- 集中化的管理

不須大量的投資

- 不須License便可使用
- 可增購FortiGuard擴增設備辨識服務



Gartner 魔力象限2020

網路防火牆魔力象限

Fortinet 為此象限的領導者

廣域網路邊緣基礎架構魔力象限

Fortinet 為此象限的領導者

有線與無線網路魔力象限

Fortinet 為此象限的有遠見者

資安鐵三角的好處

簡化管理

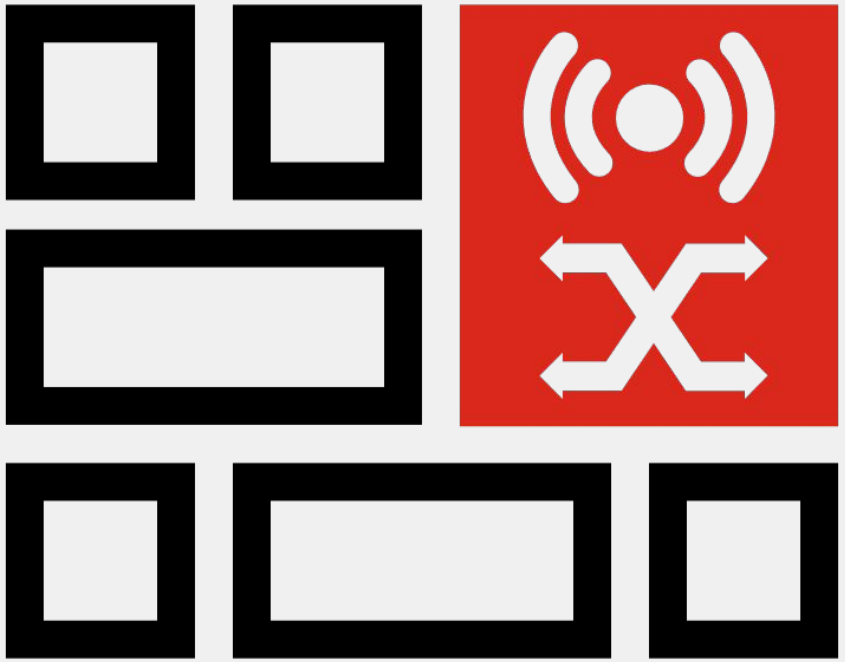
單一管理介面與自動化設定

增加可視性

看的到,找的到,管的到

整合的資訊安全架構

將資訊安全由單點推展至全網




FORTINET