



FORTINET[®]

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

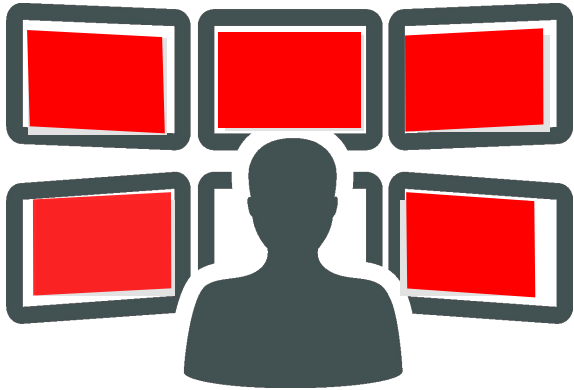


資訊安全的需求



IT人員的困境

複雜的管理環境



太多事件需處理

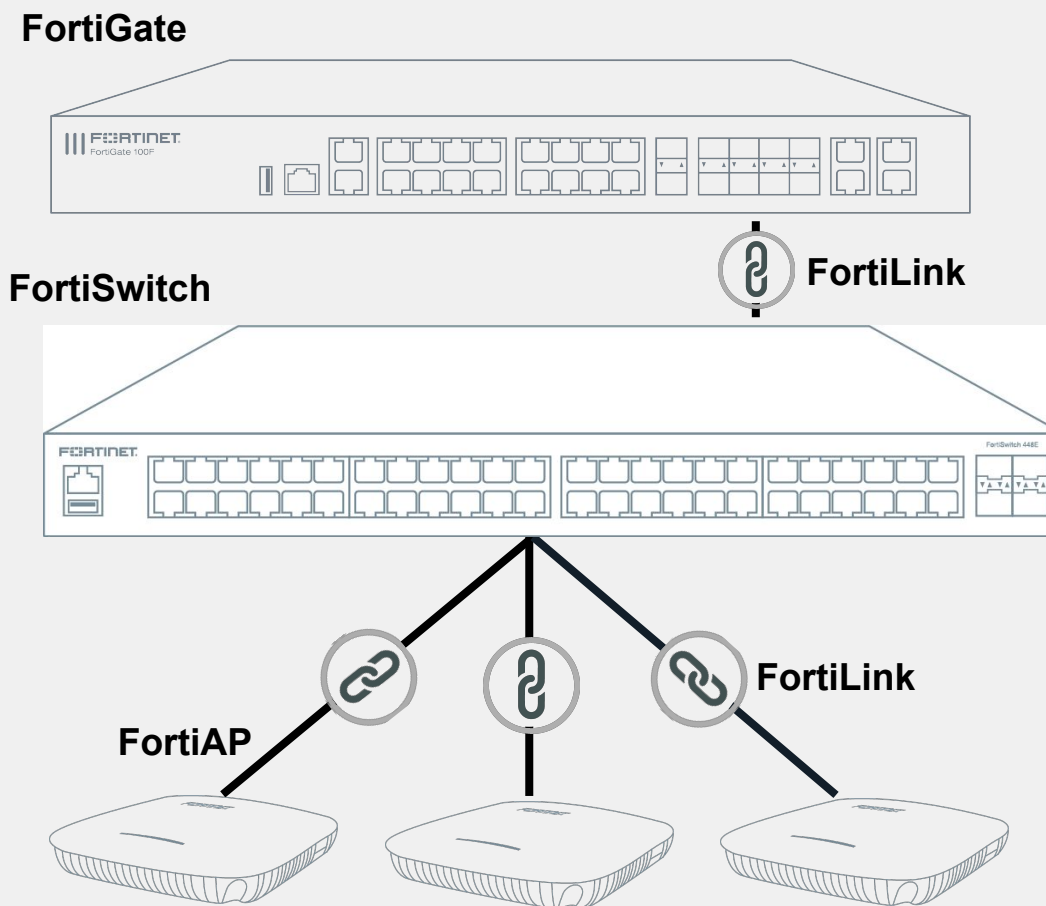


不完整的資安解決方案



Fortinet 解決方案：資安鐵三角

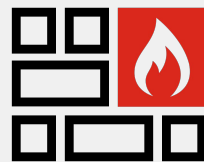
- 簡化管理
 - 自動化的部屬
 - 可隨時依照需求擴充架構
- 增加可視性
 - 自動生成網路架構
 - 豐富的終端設備資訊
- 整合的資訊安全架構
 - 中央控管,將資安擴展到全網路
 - 提供NAC功能



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

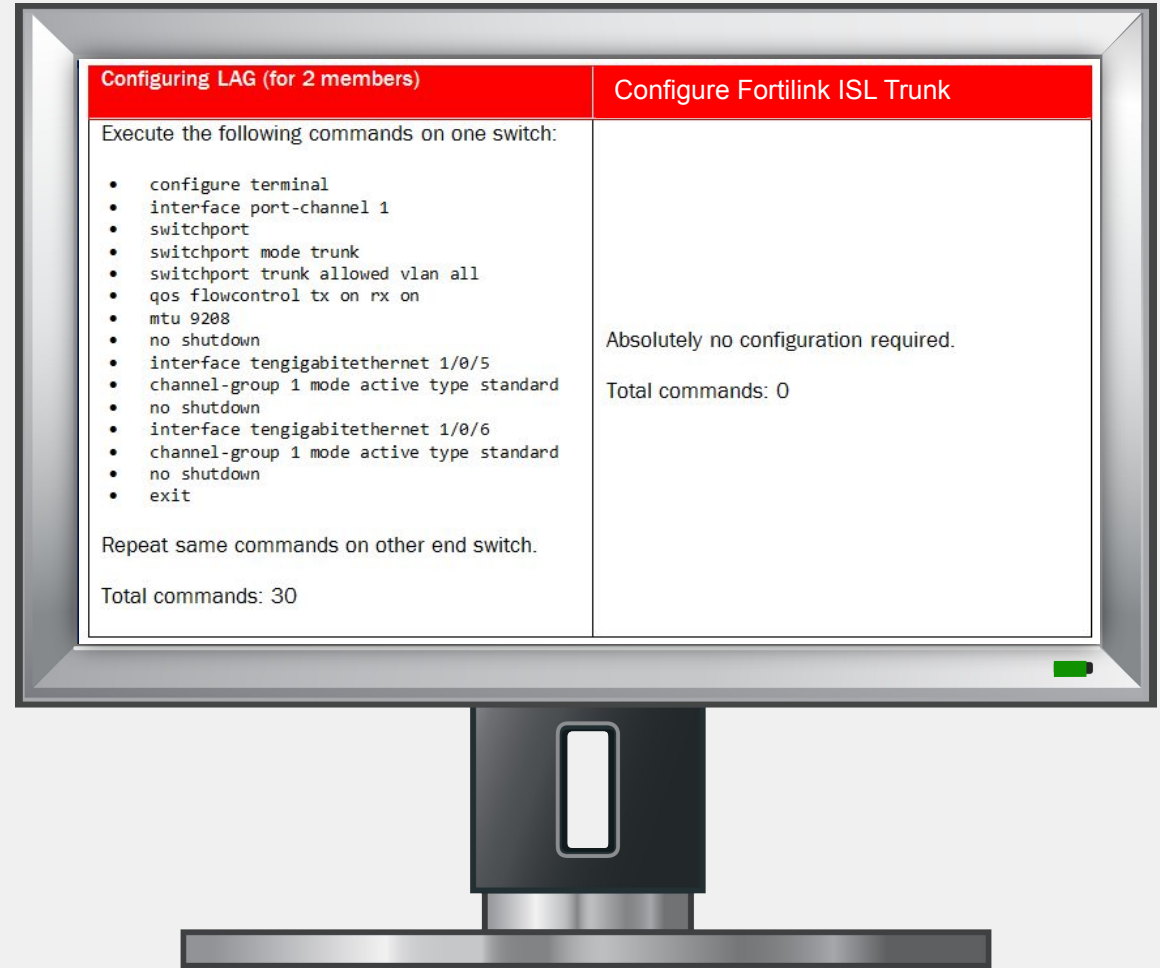


簡化管理

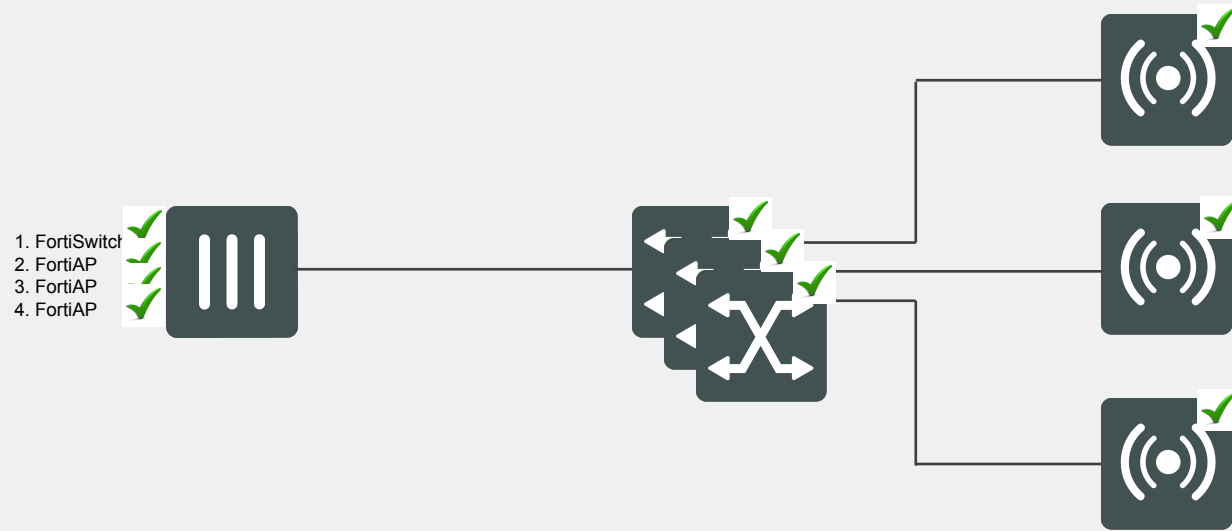


傳統的網路設定

- 每台switch間的trunk 與LACP皆得手動設定:
 - » Step 1: Config terminal
 - » Step 2: interface port-channel 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-channel 2
 - » [...]
 - » Step 106: switchport mode trunk
 - » [...]
 - » Step 114: switchport trunk allow vlan20
 - » [...]

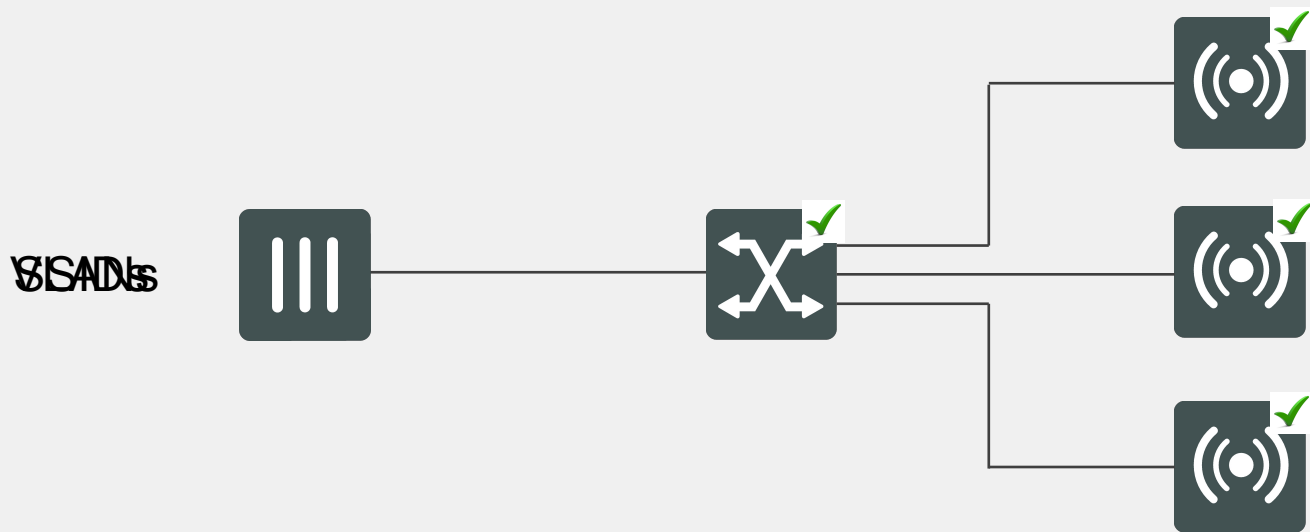


資安鐵三角：一鍵完成設定



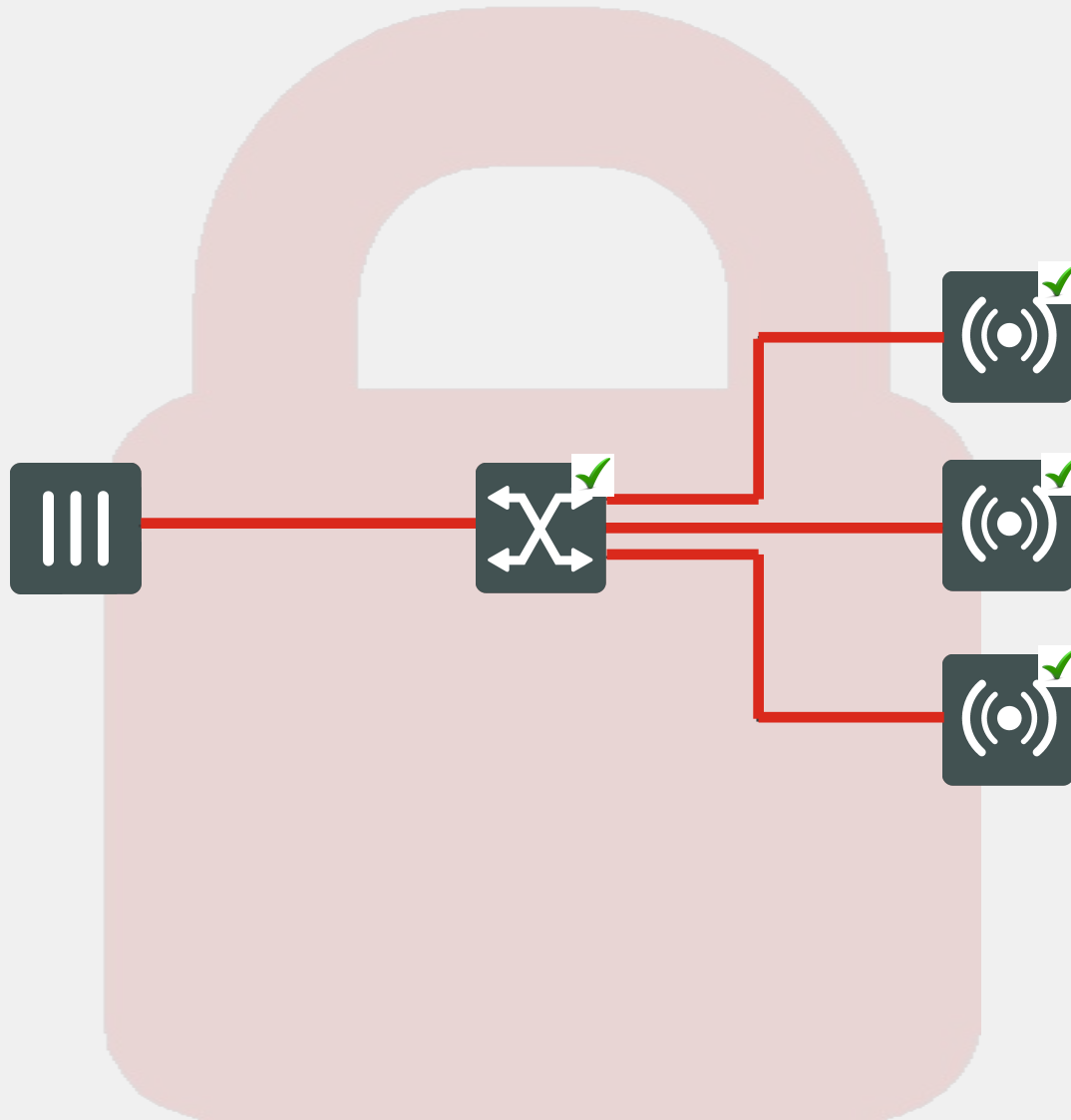
- 將交換器與無線基地台接上
- 在FortiGate上點選授權
- 完工!
- 重複此步驟新增交換器與無線基地台
- 無須額外的設定

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

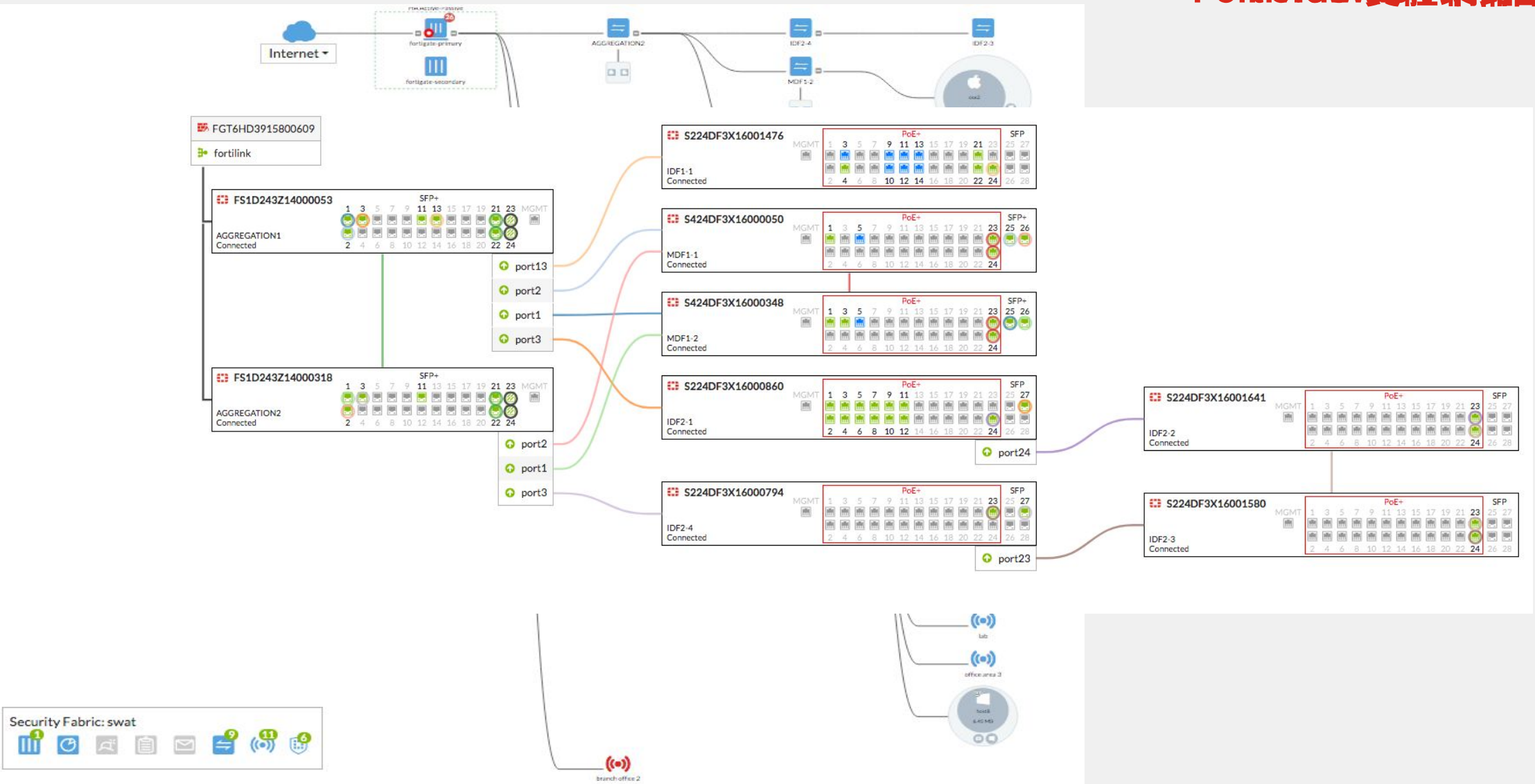


目前網路接線??



自動生成網路架構圖

For FortiView 實體網路構圖



查看終端設備資訊

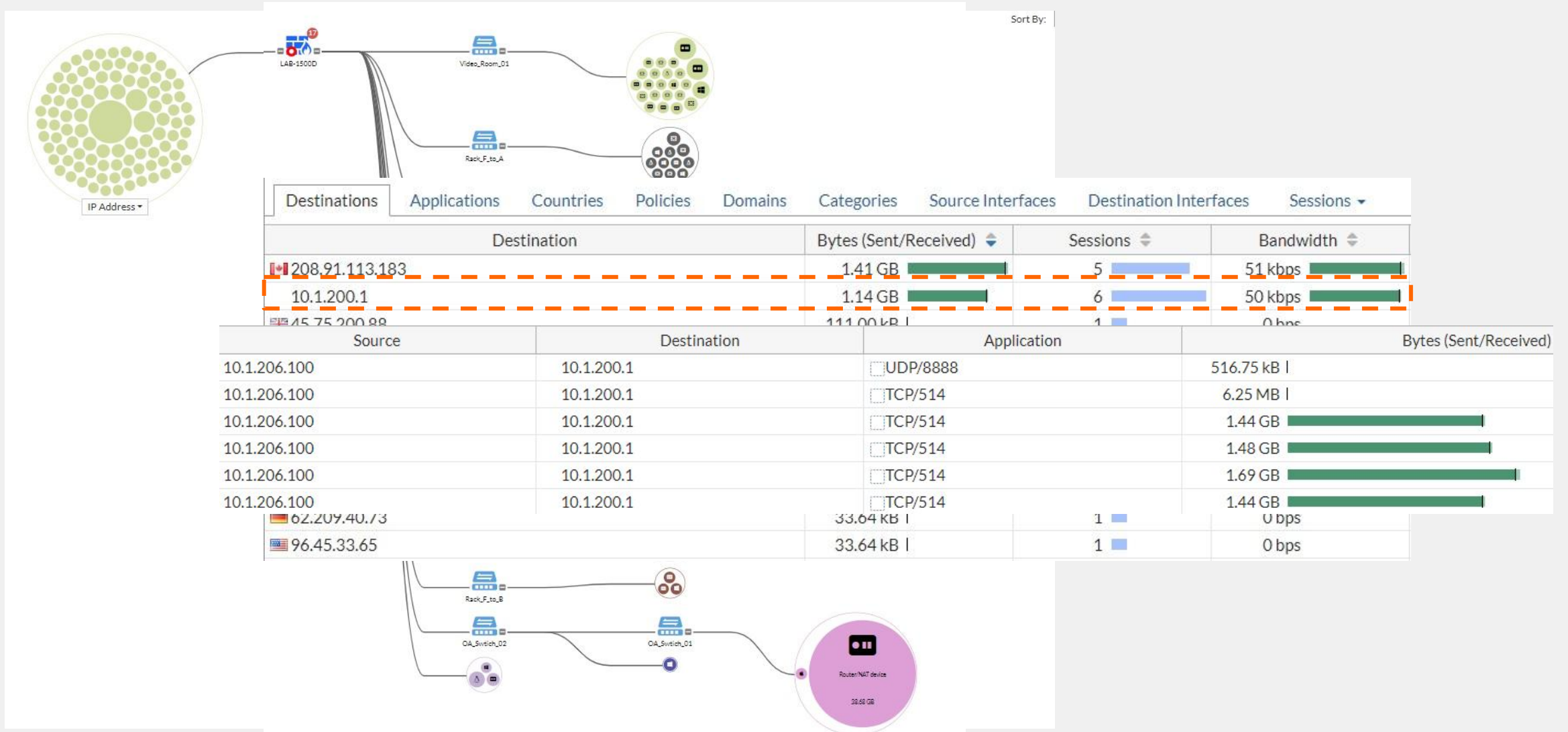
The screenshot displays the FortiNMS interface for a device named 'ACCESS-SALES'. The main panel shows the following details:

- Device:** NuovoVesuvio
- Status:** Registered
- Vulnerabilities:** 14 (red), 30 (orange), 2 (yellow), 7 (blue)
- MAC Address:** 00:50:56:00:02:87
- Interface:** vsw.FLINK-AGG (FS108D3W16001161: port1)
- OS:** Windows / 8.1
- Topology:** FG1K5D3I15804861 -> Demo-ISFW-PRI -> Demo_ISFW-Sales -> NuovoVesuvio
- Sessions:** 13
- Bytes (Sent/Received):** 5.63 kB
- Bandwidth:** 4 kbps
- Packets (Sent/Received):** 43 B

Three red arrows point to the Vulnerabilities, MAC Address, and Interface fields. A blue-bordered box highlights the Bytes (Sent/Received) field and its corresponding bar chart. The background shows a network topology with other devices like 'FTNT-DEMO' and 'FortiAP'.



查看終端設備流量使用狀況



資安管理



傳統查找方法

FortiGate 1500D Demo-NGFW-PRI

- ★ Favorites
- Dashboard
- Security Fabric
- FortiView

Traffic From LAN/DMZ

Sources	Destinations	Countries
Source	Source Device	Source Interface
10.88.23.9		FSA-DMZ
169.254.1.2		FSW-AGG

Threats

- WiFi Clients
- Traffic Shaping
- Traffic From WAN



5 min

Category	Threat Level	Threat Score (Blocked/Allowed)
Connection Attempts	Low	25870
Firewall Policy	High	19680
	Critical	350

Bytes (Sent/Received)	Sessions (Blocked/Allowed)
0 B	488
0 B	12

bsites	High	30
bsites	High	30
bsites	High	30
bsites	High	30



在資安鐵三角中查找使用者

FortiGate 1500D Demo-NGFW-PRI

Refresh Add Filter 5 min

Threat Score (Blocked/Allowed)

25870	<div style="width: 100%;"></div>
19680	<div style="width: 100%;"></div>
350	

Sessions (Blocked/Allowed)

488	<div style="width: 100%;"></div>
12	
30	
30	
30	

10.88.23.9

Device 18:66:da:51:80:37

Server Web Server

MAC Address 18:66:da:51:80:37

Interface FSA-DMZ (S448DF3X16000158:port13)

OS Linux / 3.16.0

Topology Demo-NGFW-PRI 18:66:da:51:80:37

Sessions 142

Bytes (Sent/Received) 0 B

Threat Score 4260

Sources Destinations Countries

Source	Source Device	Source Interface
10.88.23.9		FSA-DMZ
169.254.1.2		FSW-AG

Threats

WiFi Clients

Traffic Shaping

Traffic From WAN



在交換器上將問題主機隔離

The screenshot displays the FortiGate 500E management interface for device FG5H0E-ET-1. A sidebar on the left shows navigation options: Favorites, Dashboard, Security Fabric, and Physical Topology. The main area shows a network topology with a red circle representing a compromised host. A context menu is open over this host, offering actions: Drill Down to Details by Source Address (10.111.0.2), Drill Down to Compromised Hosts, Quarantine Host, and Ban IP. A red arrow points from the 'Quarantine Host' option to the host's details panel on the left.

fortinet
10.111.0.2
Compromised

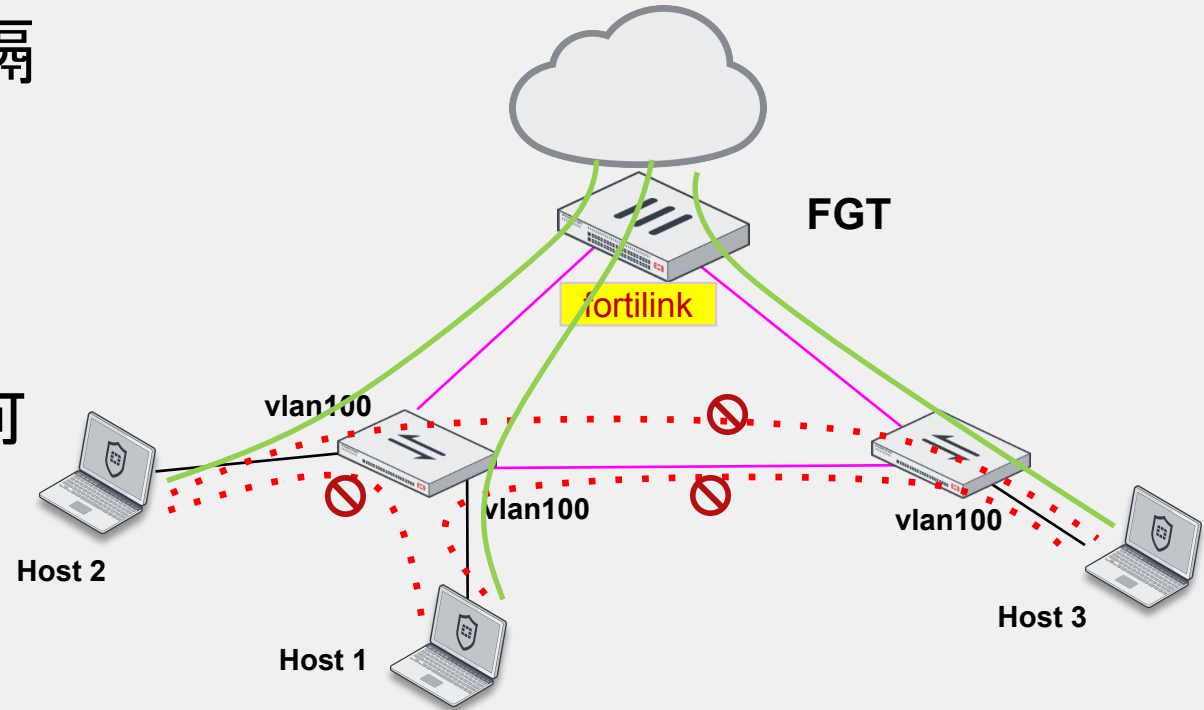
Device	mis-PC
MAC Address	10:0b:a9:31:28:b4
Other MAC Addresses	74:de:2b:9a:d2:ad 10:0b:a9:31:28:b5 d4:be:d9:0d:a7:2f
Online Interfaces	AV-Qtn (AV-Qtn)
OS	Windows / 7 Service Pack 1
Topology	FG5H0E-ET-1 AV-60-DEMO 10:0b:a9:31:28:b4
Sessions	625
Bytes (Sent/Received)	105.18 kB
Bandwidth	58 kbps
Packets (Sent/Received)	1.39 kB

- Drill Down to Details by Source Address (10.111.0.2)
- Drill Down to Compromised Hosts
- Quarantine Host
- Ban IP

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

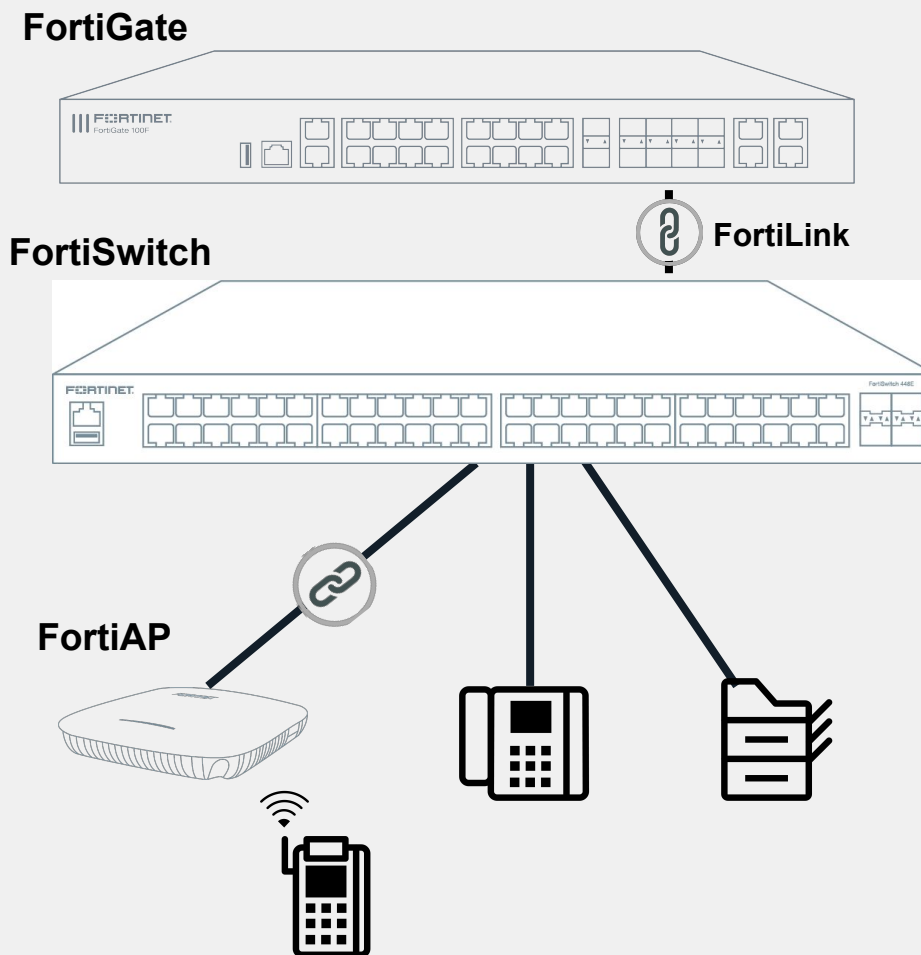
- 自動為IoT設備做識別並分類
- 依據IoT設備的類別指派至不同的網段的
- 持續監控網路異常行為與風險評估,並自動針對狀況反應

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

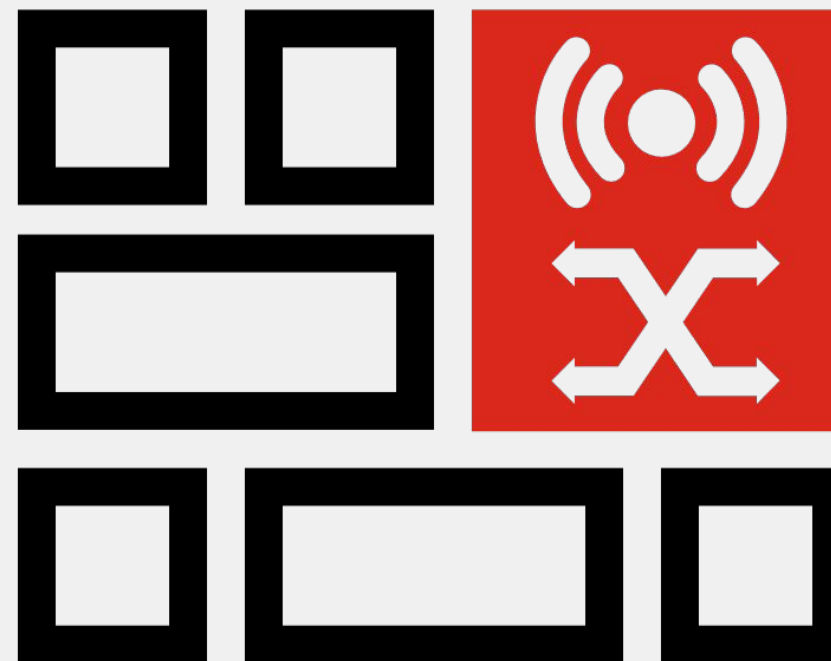
單一管理介面與自動化設定

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®