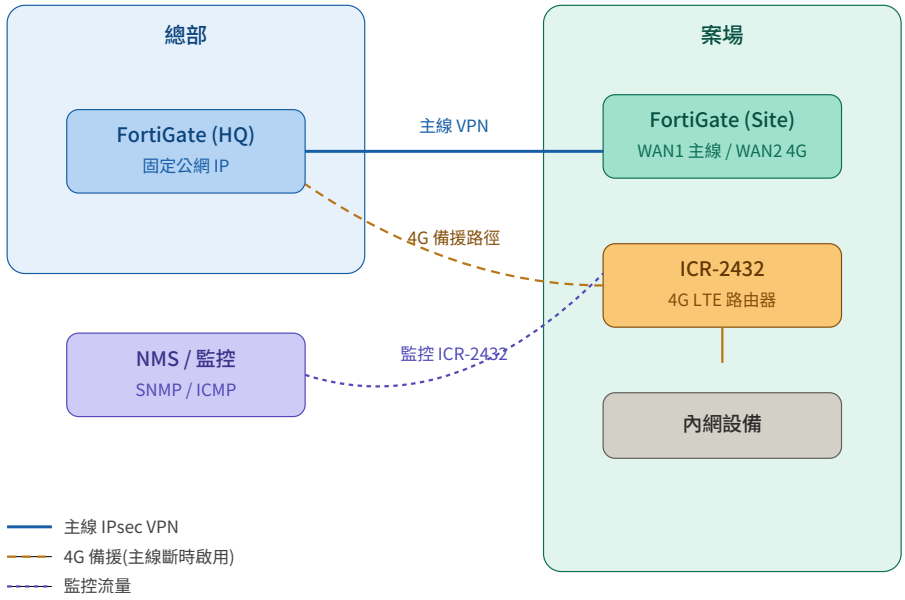
FortiGate + ICR-2432 4G 備援架構建議

設備:Advantech ICR-2432 (4G LTE 工業路由器) ・ 案場 / 總部 FortiGate

需求摘要

- 總部 FortiGate 已與案場 FortiGate 建立 IPsec VPN。
- 案場 FortiGate 下接 ICR-2432,作為實體網路異常時的 4G 行動網路備援。
- 系統需要持續監控 ICR-2432 的狀態。

拓撲示意



圖一:總部與案場之間的 VPN 主線與 4G 備援拓撲

結論:SIM 卡不需要固定 IP

> **動態 IP(浮動 IP)即可滿足需求。**因為所有連線都是由案場端「主動向外發起」,沒有需要從外部主動連入 ICR-2432 的情境,所以即使電信商配發的是 CGNAT 私有 IP,也能正常運作。

為什麼動態 IP 就夠用

主線 VPN 由案場 FortiGate 主動撥到總部(Dial-out 模式),所以只有總部端需要固定公網 IP,案場端不需要。當實體線路斷線、流量改走 4G 時,案場 FortiGate 一樣是主動往總部發起 VPN,只是出口介面換成 ICR-2432,IPsec 隧道照樣可以重新建立。

監控也可以設計成由內往外發起或經由 VPN 內部存取,這是讓動態 IP 方案可行的關鍵。詳見下節。

ICR-2432 監控建議做法

做法 A:走 VPN 內部監控(推薦做為主要手段)

將 ICR-2432 的 LAN 介面 IP 納入總部 FortiGate VPN 的 Phase 2 Selector,讓總部的 NMS 透過 VPN 隧道直接以 SNMP 或 ICMP 存取 ICR-2432 的管理介面。

- 平時:主線 VPN 通暢,監控流量走主線進入案場 → NMS 可達 ICR-2432。

- 主線斷線:VPN 改走 4G,監控流量仍走 VPN → NMS 仍可達 ICR-2432。

> **注意:**當切換到 4G 備援時,ICR-2432 自己變成 VPN 出口路徑的一部分。要確保 ICR-2432 管理介面 IP 與案場其他內網不同網段,且案場 FortiGate 的路由能將該 IP 的回應導回 VPN。

做法 B:ICR-2432 主動回報

Advantech ICR-2432 支援以下主動回報機制,搭配動態 IP / CGNAT 完全無影響:

- **SNMP Trap**:主動推送告警事件到總部 NMS。
- **Syslog**:主動將系統日誌送往日誌伺服器。
- **R-SeeNet**:Advantech 自家雲端管理平台,設備主動連雲端,管理者從雲端介面集中監看。

做法 C:ICR-2432 自建管理 VPN(頻外管理)

ICR-2432 本身支援 IPsec 與 OpenVPN client 功能,可以讓它主動向總部建立一條獨立於 FortiGate 的管理 VPN。這樣即使案場 FortiGate 整台故障,管理人員仍可透過 4G + ICR-2432 自建的 VPN 連入案場進行救援。這是**頻外管理 (Out-of-Band Management)** 的概念,強烈建議搭配做法 A 一併實作。

哪些情況才真的需要固定公網 IP

本案不需要,但供日後評估參考:

- 需要從外部「主動」SSH / HTTPS 直接連到 ICR-2432 的 WAN 介面進行管理。
- 案場需要對外網提供服務(例如 Web、影像串流)。
- VPN 是由總部主動撥到案場(與本案相反方向)。

SIM 卡與電信商選擇建議

方案	是否適合本案	備註
一般 4G / 物聯網 SIM(浮動 IP)	**推薦**	月租便宜,中華電信 M2M 約 NT$200–400/月
固定公網 IP SIM	非必要	月租通常為一般方案的 3–5 倍
私有 APN / 企業專網	視預算評估	SIM 直接進企業內網,安全性最高
CGNAT 浮動 IP	可接受	本案連線皆由內往外發起,可正常運作

實作建議步驟

1. 選用一般物聯網 / M2M 浮動 IP SIM,並向電信商確認 APN 設定。
2. ICR-2432 設定 WAN 連線、APN、PIN 碼;啟用 SNMP 與 Syslog。
3. 案場 FortiGate 設定 SD-WAN:WAN1 為實體主線,WAN2 接 ICR-2432 作為備援。
4. 設定 Link-Monitor / Performance SLA 健康檢查,自動切換主線與 4G。
5. 將 ICR-2432 LAN IP 納入 IPsec VPN Phase 2 Selector,使總部 NMS 可透過 VPN 監控。
6. 於 ICR-2432 設定 SNMP Trap 與 Syslog 主動回報至總部。
7. 建議額外設定 ICR-2432 自建管理 VPN(IPsec / OpenVPN client),做為頻外管理通道。
