為何企業/ 工業環境需要 VPN

現代企業或工控 IoT 系統常見需求

- 多地辦公室、分公司與總公司之間、安全地互聯 (Site-to-Site)。
- 遠端或外包人員從家中、異地或行動裝置存取公司資源 (Remote Access)，如 ERP、內部伺服器、SCADA 系統。
- 工業設備 PLC、RTU、Modbus 裝置等，工廠、倉儲、戶外站點分散各地，需要集中監控及管理。
- 混合雲及公有雲資源的安全連線，如 VM、資料庫、雲平台。
- 在網路條件不佳或連線不穩定的場域，需要維持通訊穩定與安全。

選擇 IPsec 協議? 還是 WireGuard 協議?

IPsec 優勢

- **廣泛支持、兼容性高**
  企業廣泛應用，許多硬體、網路設備原生支援，方便與現有架構如 Windows、VPN 用戶端、防火牆等整合。
- **功能完整、彈性大**
  設定複雜通道、安全政策、多種加密演算法，適合對安全、合規、有嚴格存取控制需求的企業或跨境公司部署。
- **適合大型複雜網路拓撲**
  多區域、多子網、多 VLAN、跨防火牆的複雜架構，IPsec 的彈性更高，容易與既有網路設備整合。

WireGuard 優勢

- **簡潔設計、輕量高效**
  代碼庫小、協議簡單，設定容易且易於維護。這降低了錯誤配置的風險。
- **高效能與低延遲**
  資料吞吐 (Throughput) 和延遲 (Latency) 表現佳，適合需低延遲或高頻寬應用，如監控、VoIP、遠端桌面等。
- **支援 NAT、動態 IP、行動設備**
  支援 NAT Traversal，對行動裝置使用情境友好，員工在家、出差、使用 LTE/ Wi-Fi 切換時維持 VPN 穩定連線。
- **資源消耗低**
  對於運作資源有限的嵌入式設備，WireGuard 的輕量特性非常有利。

配置建議

- 重視高效能、簡單部署、支援行動與動態 IP 如遠端員工、分公司、IoT 裝置等，WireGuard 是理想選擇。
- 已有複雜網路拓撲，需支援多種設備、兼容性、與合規性，如大型企業或工控網路，使用 IPsec 較為穩健。
- 在混合環境中，兩者並存，使用 IPsec 建立內部 Backbone 隧道，WireGuard 提供給遠端或 IoT 裝置 Access VPN。

企業及工業情境下的 IAD200 應用

分支辦公室、多地辦公室 Site-to-Site 互聯

企業在跨區域設有多個辦公室，每個地點都連接到 IAD200 工業級 4G LTE 路由器：

- 在總公司與各分公司之間建立 VPN 隧道 (IPsec 或 WireGuard)，將各地區域網路 LAN 安全互聯。
- 各地員工能像在同一內網般存取檔案伺服器、ERP 系統、內部資源。
- 當某地區因 ISP 故障造成網路斷線時，IAD200 的雙 SIM 及 Failover 功能，LTE 自動切換 確保辦公網路不中斷。
- 企業網路具有工控 Modbus、SCADA、IoT 設備，IAD200 Modbus、RS485、RS232 將裝置納入整體網路管理。

遠端員工/ 移動工作者 Remote Access

企業面臨需要支援遠端在宅工作 (Work Form Home)、出差、工地巡檢、維運人員外派等情境：

- WireGuard 為遠端員工提供 VPN 客戶端 (Windows/ macOS/ Linux/ Android/ iOS 等)，快速、低延遲連回內網。
- 行動裝置經常在行動網路與 Wi-Fi 間切換，WireGuard 支援 NAT Traversal/ Roaming，確保連線穩定不中斷。
- 企業對於安全、合規、網路政策有較高的要求，IAD200 支援 TACACS+、防火牆、TLS/ HTTPS 管理、權限分級管理等，可配合企業既有身份管理系統如 LDAP、RADIUS、TACACS 實現集中管理。

工業自動化、IoT、遠端監控

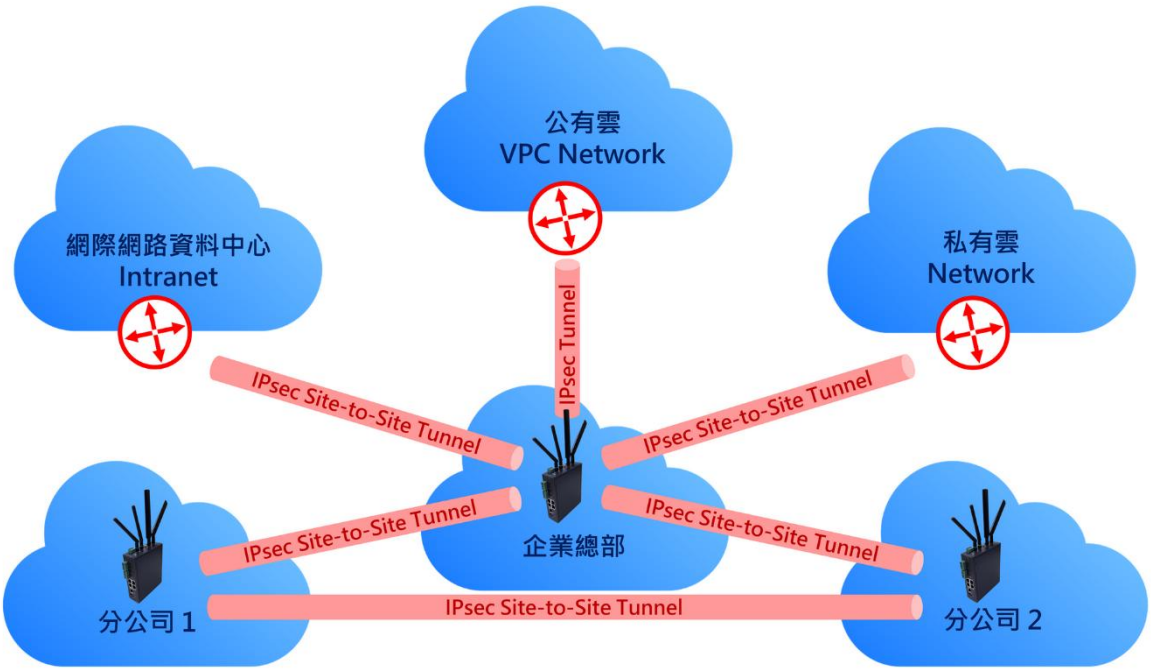
對於設備散布在工廠、倉庫、戶外站點、分公司的工業及 IoT 系統：

- IAD200 支援 Modbus TCP、RS232/ RS485、DI/ Relay，可將工控設備 PLC、RTU、傳感器、閥門控制器、遠端採集等裝置接入乙太網或 LTE，並經由 VPN 安全通道與中央 SCADA、Cloud Gateway 連線。
- 企業設備位於戶外機櫃或偏遠站點，IAD200 -40°C ~ 70°C 寬溫、金屬無風扇 IP30 設計、DC 雙電源輸入，非常適合戶外、工業環境使用。
- WireGuard 或 IPsec VPN 隧道，可確保通訊資料在公共網路 (LTE、互聯網) 中加密、不被攔截，適合對安全性、設備監控高要求的工控及 IoT 應用。
- 企業有集中管理需求如設備監控、資產管理、遠端維護，透過 VPN 可將各地裝置統一接入企業網路，便於集中維運、部署更新、資料收集、告警推送等。

混合雲/ 公有雲服務安全連線

許多企業將部分系統如資料庫、應用程式、記錄系統、雲端儲存，置放在 AWS、Azure、GCP、私有雲：

- IAD200 可作為邊緣 Gateway，在企業內網與雲端之間建立安全隧道 Site-to-Site VPN，使雲端資源像本地資源一樣受保護、可被安全訪問。
- 有多地點、多雲端 VPC 可透過 WireGuard、IPsec 組成 Mesh 或軸輻網路 (Hub-and-Spoke) 結構，彈性高。
- IAD200 支援動態路由 (RIP v1/v2)、NAT/ Port Forward、防火牆與 ACL，可協助企業在混合雲網絡間做更細緻、安全的流量分隔與控管。



IAD200 加 VPN 是現代企業、工控、IoT 的必備神器

總結來說，IAD200 的工業級設計、支援 VPN、防火牆/ AAA/ 多介面/ LTE/ Wi-Fi/ Modbus/ Serial，路由器加 IPsec/ WireGuard 的組合，特別適合以下趨勢：

- **分散式/ 混合式/ 遠端/ 多地點企業架構**
  隨著企業從單一總部轉向跨地、多分支、多國辦公生產監控，IAD200 加 VPN 能簡化部署、統一管理。
- **工控/ IoT 與 IT 融合 (IT/ OT Convergence)**
  OT 網路 (Modbus/ PLC/ SCADA) 與 IT 網路 (LAN/ Cloud/ Office) 安全整合，降低資安風險，提升管理維運效率。
- **彈性、安全、成本效益**
  相較購置專用設備如工控 Gateway、LTE Router、Wi-Fi AP 等，IAD200 可整合多重功能、降低採購與維運成本。
- **行動/ 遠端/ 混合雲/ 彈性辦公**
  對於企業支援遠端工作、出差、行動巡檢、混合雲/ SaaS/ 雲端儲存、分散式架構等，有極高的適應性與靈活性。

注意事項

- 使用 WireGuard，需確保設備的穩定支援，包括 WireGuard 核心/ kernel module、適當的韌體及資源 (CPU/ 記憶體)、密鑰管理方式 (Public Key/ Allowed-IPs/ ACL) 等。
- 對於大型企業、多子網、多 VLAN、多用戶，大量同時 VPN 連線的情境，WireGuard 的靜態 Peer/ Allowed-IPs 模型可能管理較複雜，不如 IPsec 在大型部署上的政策管理彈性。
- 企業有嚴格合規要求，需支援加密標準、兼容既有設備、LDAP/ AD 整合，尤其有使用 AES/ IKEv2/ Certificate-based Authentication 情境，IPsec 會更適合。
- 工控及 IoT 設備的資源 (CPU/ 記憶體) 與通訊穩定性、網路封包最大傳輸單元 (MTU)、NAT、防火牆、路由規劃等，需要在配置時小心設定，以避免封包丟失、斷線、重新傳送等問題。
- IAD200 用於戶外或惡劣環境，可搭配 LTE、Wi-Fi、GNSS 展延天線、電源穩定、防水機櫃保護等配套措施。