为何企业/ 工业环境需要 VPN

现代企业或工控 IoT 系统常见需求

- 多地办公室、分公司与总公司之间、安全地互联 (Site-to-Site)。
- 远程或外包人员从家中、异地或行动装置存取公司资源 (Remote Access)，如 ERP、内部服务器、SCADA 系统。
- 工业设备 PLC、RTU、Modbus 装置等，工厂、仓储、户外站点分散各地，需要集中监控及管理。
- 混合云及公有云资源的安全联机，如 VM、数据库、云平台。
- 在网络条件不佳或联机不稳定的场域，需要维持通讯稳定与安全。

选择 IPsec 协议? 还是 WireGuard 协议?

IPsec 优势

- **广泛支持、兼容性高**
  企业广泛应用，许多硬件、网络设备原生支持，方便与现有架构如 Windows、VPN 客户端、防火墙等整合。
- **功能完整、弹性大**
  设定复杂通道、安全政策、多种加密算法，适合对安全、合规、有严格访问控制需求的企业或跨境公司部署。
- **适合大型复杂网络拓扑**
  多区域、多子网、多 VLAN、跨防火墙的复杂架构，IPsec 的弹性更高，容易与既有网络设备整合。

WireGuard 优势

- **简洁设计、轻量高效**
  代码库小、协议简单，设定容易且易于维护。这降低了错误配置的风险。
- **高效能与低延迟**
  数据吞吐 (Throughput) 和延迟 (Latency) 表现佳，适合需低延迟或高带宽应用，如监控、VoIP、远程桌面等。
- **支持 NAT、动态 IP、行动设备**
  支持 NAT Traversal，对行动装置使用情境友好，员工在家、出差、使用 LTE/ Wi-Fi 切换时维持 VPN 稳定联机。
- **资源消耗低**
  对于运作资源有限的嵌入式设备，WireGuard 的轻量特性非常有利。

配置建议

- 重视高效能、简单部署、支持行动与动态 IP 如远程员工、分公司、IoT 装置等，WireGuard 是理想选择。
- 已有复杂网络拓扑，需支持多种设备、兼容性、与合规性，如大型企业或工控网络，使用 IPsec 较为稳健。
- 在混合环境中，两者并存，使用 IPsec 建立内部 Backbone 隧道，WireGuard 提供给远程或 IoT 装置 Access VPN。

企业及工业情境下的 IAD200 应用

分支办公室、多地办公室 Site-to-Site 互联

企业在跨区域设有多个办公室，每个地点都连接到 IAD200 工业级 4G LTE 路由器：

- 在总公司与各分公司之间建立 VPN 隧道 (IPsec 或 WireGuard)，将各地局域网络 LAN 安全互联。
- 各地员工能像在同一内网般存取文件服务器、ERP 系统、内部资源。
- 当某地区因 ISP 故障造成网络断线时，IAD200 的双 SIM 及 Failover 功能，LTE 自动切换 确保办公网络不中断。
- 企业网络具有工控 Modbus、SCADA、IoT 设备，IAD200 Modbus、RS485、RS232 将装置纳入整体网络管理。

远程员工/ 移动工作者 Remote Access

企业面临需要支持远程在宅工作 (Work Form Home)、出差、工地巡检、维运人员外派等情境:

- WireGuard 为远程员工提供 VPN 客户端 (Windows/ macOS/ Linux/ Android/ iOS 等)，快速、低延迟连回内网。
- 行动装置经常在行动网络与 Wi-Fi 间切换，WireGuard 支持 NAT Traversal/ Roaming，确保联机稳定不中断。
- 企业对于安全、合规、网络政策有较高的要求，IAD200 支持 TACACS+、防火墙、TLS/ HTTPS 管理、权限分级管理等，可配合企业既有身份管理系统如 LDAP、RADIUS、TACACS 实现集中管理。

工业自动化、IoT、远程监控

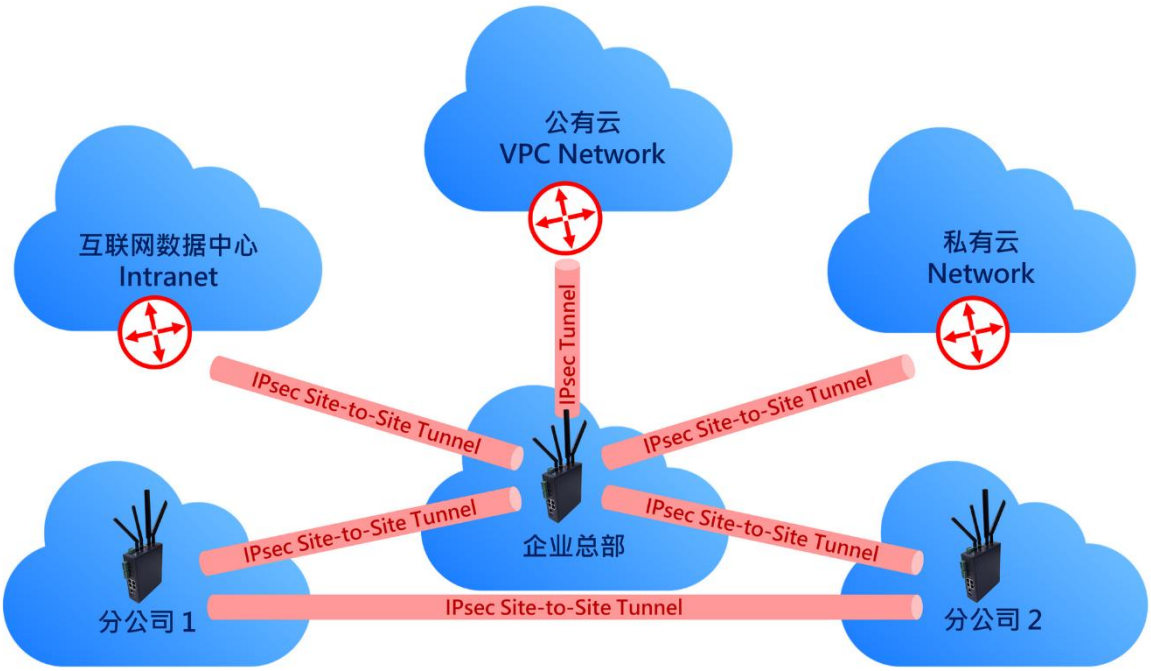
对于设备散布在工厂、仓库、户外站点、分公司的工业及 IoT 系统:

- IAD200 支持 Modbus TCP、RS232/ RS485、DI/ Relay，可将工控设备 PLC、RTU、传感器、阀门控制器、远程采集等装置接入以太网或 LTE，并经由 VPN 安全通道与中央 SCADA、Cloud Gateway 联机。
- 企业设备位于户外机柜或偏远站点，IAD200 -40°C ~ 70°C 宽温、金属无风扇 IP30 设计、DC 双电源输入，非常适合户外、工业环境使用。
- WireGuard 或 IPsec VPN 隧道，可确保通讯数据在公共网络 (LTE、互联网) 中加密、不被拦截，适合对安全性、设备监控高要求的工控及 IoT 应用。
- 企业有集中管理需求如设备监控、资产管理、远程维护，透过 VPN 可将各地装置统一接入企业网络，便于集中维运、部署更新、资料收集、告警推送等。

混合云/ 公有云服务安全联机

许多企业将部分系统如数据库、应用程序、记录系统、云端储存，置放在 AWS、Azure、GCP、私有云:

- IAD200 可作为边缘 Gateway，在企业内网与云端之间建立安全隧道 Site-to-Site VPN，使云端资源像本地资源一样受保护、可被安全访问。
- 有多地点、多云端 VPC 可透过 WireGuard、IPsec 组成 Mesh 或轴辐网络 (Hub-and-Spoke) 结构，弹性高。
- IAD200 支持动态路由 (RIP v1/v2)、NAT/ Port Forward、防火墙与 ACL，可协助企业在混合云网络间做更细致、安全的流量分隔与控管。



IAD200 加 VPN 是现代企业、工控、IoT 的必备神器

总结来说，IAD200 的工业级设计、支持 VPN、防火墙/ AAA/ 多接口/ LTE/ Wi-Fi/ Modbus/ Serial，路由器加 IPsec/ WireGuard 的组合，特别适合以下趋势：

- **分布式/ 混合式/ 远程/ 多地点企业架构**
  随着企业从单一总部转向跨地、多分支、多国办公生产监控，IAD200 加 VPN 能简化部署、统一管理。
- **工控/ IoT 与 IT 融合 (IT/ OT Convergence)**
  OT 网络 (Modbus/ PLC/ SCADA) 与 IT 网络 (LAN/ Cloud/ Office) 安全整合，降低资安风险，提升管理维运效率。
- **弹性、安全、成本效益**
  相较购置专用设备如工控 Gateway、LTE Router、Wi-Fi AP 等，IAD200 可整合多重功能、降低采购与维运成本。
- **行动/ 远程/ 混合云/ 弹性办公**
  对于企业支持远程工作、出差、行动巡检、混合云/ SaaS/ 云端储存、分布式架构等，有极高的适应性与灵活性。

注意事项

- 使用 WireGuard，需确保设备的稳定支持，包括 WireGuard 核心/ kernel module、适当的韧体及资源 (CPU/ 内存)、密钥管理方式 (Public Key/ Allowed-IPs/ ACL) 等。
- 对于大型企业、多子网、多 VLAN、多用户，大量同时 VPN 联机的情境，WireGuard 的静态 Peer/ Allowed-IPs 模型可能管理较复杂，不如 IPsec 在大型部署上的政策管理弹性。
- 企业有严格合规要求，需支持加密标准、兼容既有设备、LDAP/ AD 整合，尤其有使用 AES/ IKEv2/ Certificate-based Authentication 情境，IPsec 会更适合。
- 工控及 IoT 设备的资源 (CPU/ 内存) 与通讯稳定性、网络封包最大传输单元 (MTU)、NAT、防火墙、路由规划等，需要在配置时小心设定，以避免封包丢失、断线、重新传送等问题。
- IAD200 用于户外或恶劣环境，可搭配 LTE、Wi-Fi、GNSS 展延天线、电源稳定、防水机柜保护等配套措施。