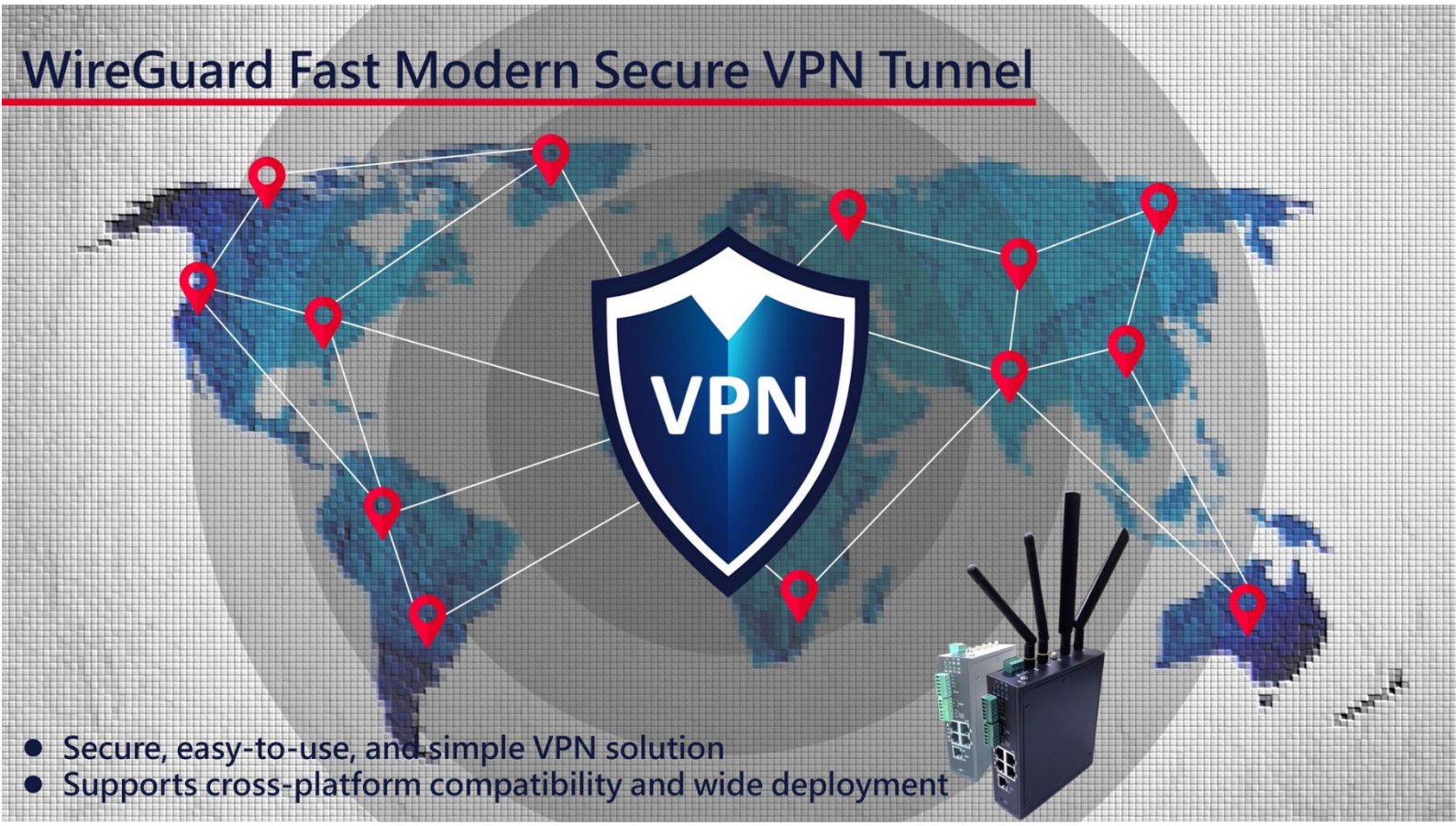


Why do Enterprise/ Industrial environments need VPN

Common Needs of Modern Enterprises or Industrial Control IoT Systems

- Secure interconnection between multiple offices, branch offices, and headquarters (site-to-site).
- Remote access for remote or outsourced personnel from home, remote locations, or mobile devices, such as ERP, internal servers, and SCADA systems.
- Centralized monitoring and management of industrial equipment such as PLCs, RTUs, and Modbus devices, located in factories, warehouses, and outdoor sites.
- Secure connectivity to hybrid cloud and public cloud resources, such as VMs, databases, and cloud platforms.
- Maintaining stable and secure communication in environments with poor network conditions or unstable connections.

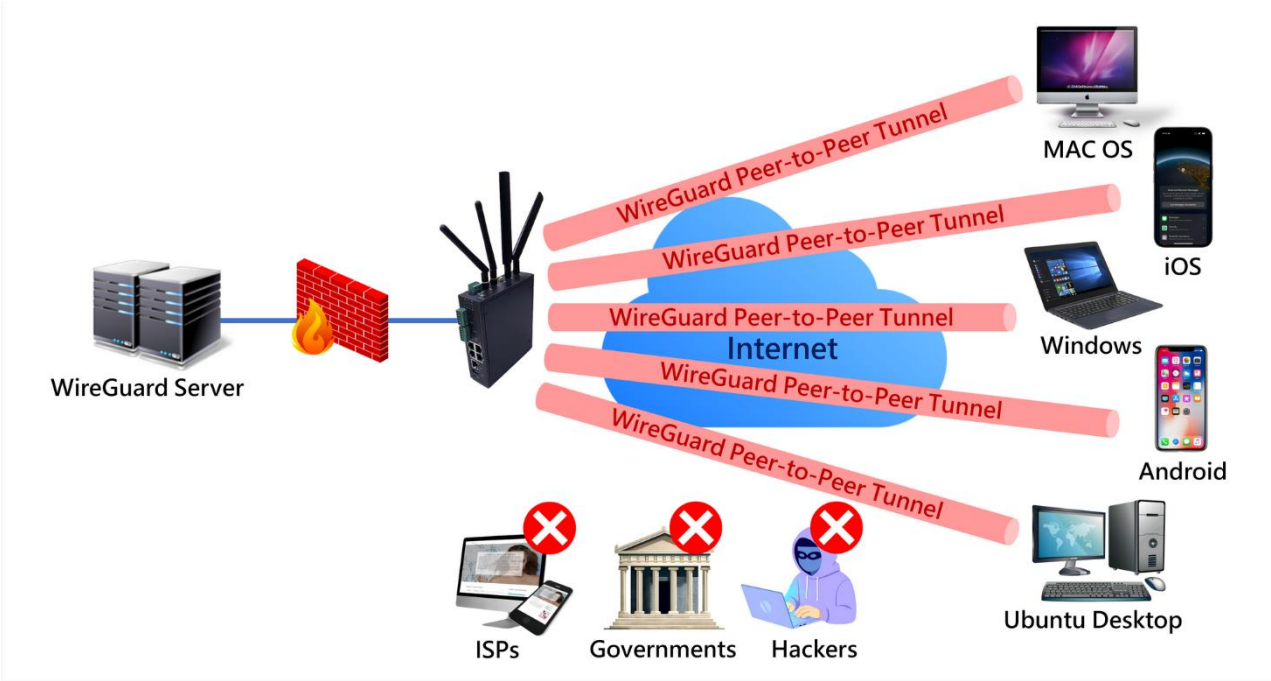
Choose IPsec or WireGuard Protocol

IPsec Advantages

- **Widespread support and High Compatibility**
  Widely used by enterprises, natively supported by many hardware and network devices, facilitating integration with existing architectures such as Windows, VPN clients, and firewalls.
- **Full Functionality and High Flexibility**
  Supports complex channel configurations, security policies, and multiple encryption algorithms, making it suitable for enterprises or cross-border companies with stringent security, compliance, and access control requirements.
- **Suitable for Large and Complex Network Topologies**
  IPsec offers greater flexibility and easier integration with existing network equipment in complex architectures involving multiple regions, subnets, VLANs, and firewalls.

WireGuard Advantages

- **Simple Design, Lightweight and Efficient**
  Small codebase and simple protocol, easy to configure and maintain. This reduces the risk of misconfiguration.
- **High Performance and Low Latency**
  Excellent data throughput and latency performance, suitable for applications requiring low latency or high bandwidth, such as monitoring, VoIP, and remote desktops.
- **Supports NAT, Dynamic IP, and Mobile Devices**
  Supports NAT Traversal, making it user-friendly for mobile devices, maintaining stable VPN connections for employees at home, traveling, or switching between LTE and Wi-Fi.
- **Low Resource Consumption**
  The lightweight nature is highly advantageous for embedded devices with limited operating resources.



Configuration Recommendations

- For environments prioritizing high performance, simple deployment, and support for mobile and dynamic IPs, such as remote employees, branch offices, and IoT devices, WireGuard is an ideal choice.
- For existing complex network topologies requiring support for multiple devices, compatibility, and compliance, such as large enterprise or industrial control networks, IPsec is more robust.
- In hybrid environments where both methods coexist, use IPsec to establish an internal backbone tunnel, and WireGuard to provide access VPN for remote or IoT devices.

IAD200 Applications in Enterprise and Industrial Scenarios

Site-to-Site Interconnection for Branch Offices and Multi-Location Offices

Enterprises with multiple offices across regions, each connected to the IAD200 industrial-grade 4G LTE router：

- Establish VPN tunnels between headquarters and branch offices, securely interconnecting regional LANs.
- Employees in each location can access file servers, ERP systems, and internal resources as if on the same intranet.
- When a network outage occurs in a region due to an ISP failure, the IAD200 dual SIM and failover functions, along with automatic LTE switching, ensure uninterrupted office network connectivity.
- For enterprise networks with industrial control Modbus, SCADA, and IoT devices, the IAD200 Modbus, RS485, and RS232 interfaces integrate these devices into the overall network management.

Remote Access for Remote Employees/ Mobile Workers

Enterprises face scenarios requiring support for WFH, business trips, site inspections, and maintenance outsourcing：

- WireGuard provides remote employees with VPN clients (Windows/ MacOS/ Linux/ Android/ iOS, etc.) for fast, low-latency connections back to the intranet.
- Mobile devices frequently switch between mobile networks and Wi-Fi; WireGuard supports NAT Traversal/Roaming to ensure stable and uninterrupted connections.
- For enterprises with high requirements for security, compliance, and network policies, the IAD200 supports TACACS+, firewalls, TLS/HTTPS management, and hierarchical access control, and can be integrated with existing enterprise identity management systems such as LDAP, RADIUS, and TACACS for centralized management.

Industrial Automation, IoT, Remote Monitoring

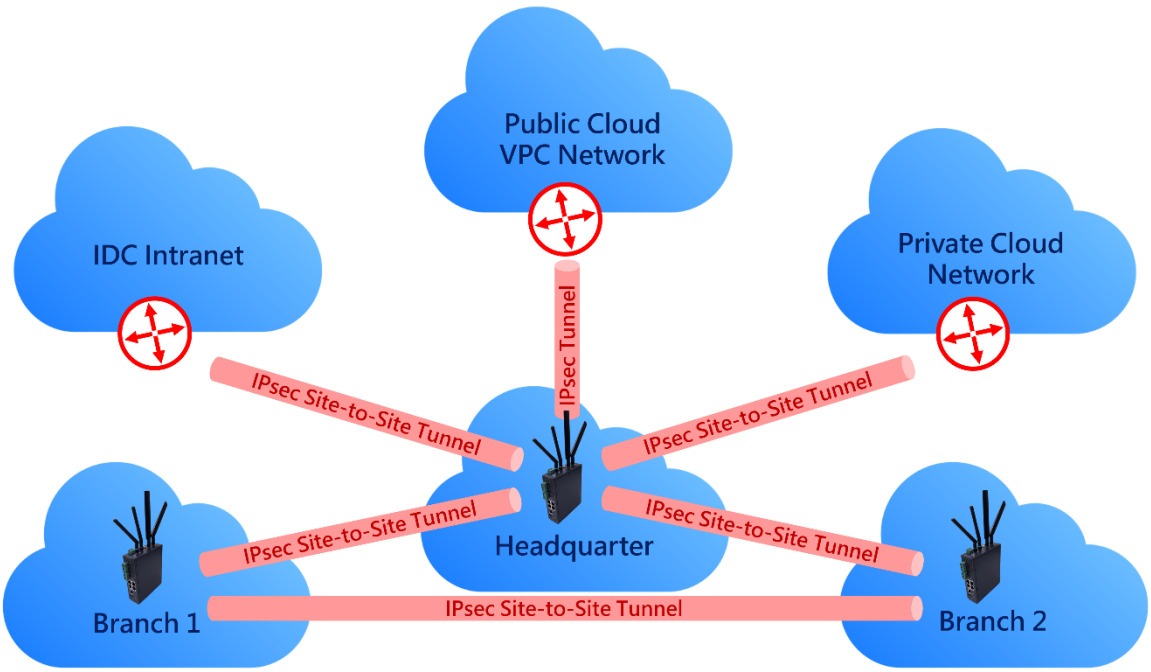
For industrial and IoT systems with equipment distributed across factories, warehouses, outdoor sites, and branch offices：

- The IAD200 supports Modbus TCP, RS232/ RS485, and DI/ Relay, enabling industrial control equipment such as PLCs, RTUs, sensors, controllers, and data acquisition devices to connect to Ethernet or LTE, and to a central SCADA and Cloud Gateway.
- For enterprise equipment located in outdoor racks or remote sites, the IAD200 -40°C to 70°C wide temperature range, fanless metal design, IP30 rating, and dual DC power input make it ideal for outdoor and industrial environments.
- VPN tunnels ensure encrypted and uninterrupted communication over public networks, making it suitable for industrial control and IoT applications with high security and equipment monitoring requirements.
- For enterprises with centralized management needs, such as equipment monitoring, asset management, and remote maintenance, VPNs can unify the access of devices from various locations to the enterprise network, facilitating centralized maintenance, deployment updates, data collection, and alarm push notifications.

Secure Connections to Hybrid Cloud/ Public Cloud Services

Many enterprises place some systems, such as databases, applications, log servers, and cloud storage, on AWS, Azure, GCP, or private clouds：

- The IAD200 can act as an edge gateway, establishing a secure tunnel between the enterprise intranet and the cloud via a Site-to-Site VPN, making cloud resources protected and securely accessible like on-premises resources.
- Multi-location, multi-cloud VPCs can be configured using WireGuard and IPsec to form mesh or hub-and-spoke networks, offering high flexibility.
- The IAD200 supports dynamic routing (RIP v1/v2), NAT/Port Forward, firewalls, and ACLs, helping enterprises achieve more granular and secure traffic separation and control across hybrid cloud networks.



IAD200 is an essential tool for enterprises, industrial control systems, and IoT

In summary, the IAD200 industrial-grade design, supporting VPN/ firewall/ AAA/ multi-interface/ LTE/ Wi-Fi/ Modbus/ Serial, and the combination of router and IPsec/ WireGuard make it particularly suitable for the following trends：

- **Distributed/ Hybrid/ Remote/ Multi-location Enterprise Architectures**
  As enterprises shift from a single headquarters to cross-location, multi-branch, and multi-country office and production monitoring, the IAD200 with VPN simplifies deployment and unifies management.
- **Industrial Control/ IoT Convergence with IT (IT/ OT Convergence)**
  Secure integration of OT networks (Modbus/ PLC/ SCADA) and IT networks (LAN/ Cloud/ Office) reduces security risks and improves management and maintenance efficiency.
- **Flexibility, Security, and Cost-Effectiveness:**
  Compared to purchasing dedicated equipment such as industrial gateways, LTE routers, and Wi-Fi APs, the IAD200 integrates multiple functions and reduces procurement and maintenance costs.
- **Mobile/ Remote/ Hybrid Cloud/ Flexible Workplace:**
  It offers high adaptability and flexibility for enterprises supporting remote work, business trips, mobile inspections, hybrid cloud/ SaaS/ cloud storage, and distributed architectures.

Important Notes

- When using WireGuard, ensure stable device support, including the WireGuard core/ kernel module, appropriate firmware, and resources (CPU/ memory), and key management methods (Public Key/ Allowed-IPs/ ACL).
- For large enterprises, multi-subnet, multi-VLAN, multi-user scenarios with many simultaneous VPN connections, WireGuard static Peer/ Allowed IPs may be more complex to manage than IPsec policy management flexibility in large deployments.
- For enterprises with strict compliance requirements, needing support for encryption standards, compatibility with existing devices, LDAP/ AD integration, and especially scenarios using AES/ IKEv2/ Certificate-based Authentication, IPsec is more suitable.
- The resources (CPU/ memory) of industrial control and IoT devices, communication stability, network packet maximum transmission unit (MTU), NAT, firewalls, and routing planning need to be carefully configured to avoid packet loss, disconnection, and retransmission issues.
- The IAD200 is designed for outdoor or harsh environments and can be equipped with LTE, Wi-Fi, GNSS extended antennas, power stabilization, waterproof cabinet protection, and other supporting measures.