SECURE REMOTE CONNECTIVITY FOR BRANCH OFFICES

HIGHLIGHTS

- Remote workers need secure networking and reliable access to company systems, but home internet connections and ISP-provided routers aren't built for enterprise-grade uptime or control, leaving businesses exposed.
- RUTM30 delivers dependable remote connectivity by combining 5G connectivity with automatic LTE Cat 19 and 3G fallback, cutting the risk of costly internet outages.
- Dual SIM, eSIM, and automatic carrier failover provide backup internet the moment the primary connection drops, so work doesn't stop when one network does.
- Built-in VPN support keeps company systems secure over any internet connection, while the Teltonika Remote Management System (RMS) enables remote monitoring and provisioning for IT teams, cutting setup time and support overhead instead of sending staff on-site.

SECURING REMOTE ACCESS WITHOUT LOSING CONNECTIVITY

Companies built around office life have spent years locking down their networks against security threats. But now a good chunk of that workforce is logging in from home, and those remote workers still need the same access to company systems and data they'd have at a desk in the office.

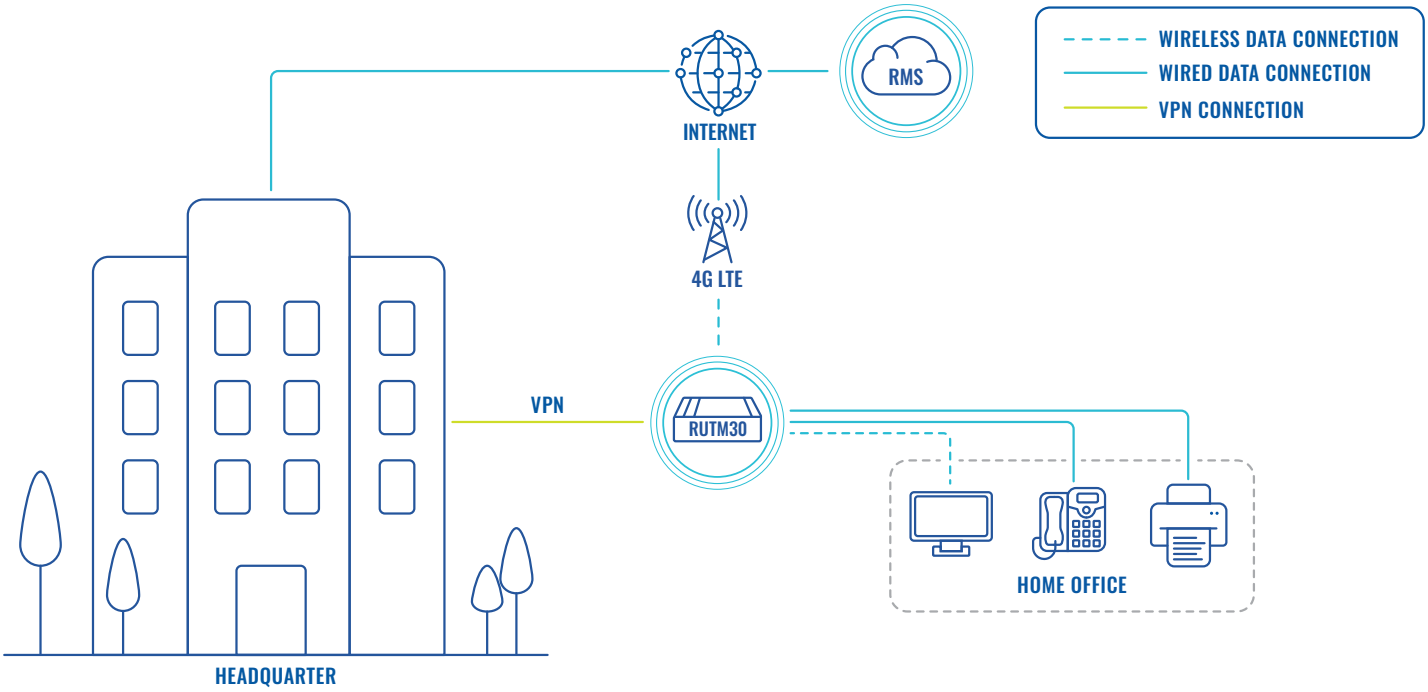
The problem is that home networks aren't office networks. Employees are usually working through whatever router their ISP handed to them, with none of the secure networking controls an enterprise remote office setup would normally provide. IT teams lose visibility and control the moment work moves off-site.

Then there's the connection itself. Most home setups run on a single internet connection. If that line goes down, so does everything else, work is cut off until the ISP sorts it out. There's no backup internet path to fall back on, so even a short outage is enough to stall someone's entire workday.

Put together, that leaves companies facing two unresolved problems: how to give employees secure, properly controlled access to corporate systems from networks the company doesn't own or manage, and how to maintain reliable remote connectivity when a single internet connection is the only path online and internet outages can happen at any time.

Copyright © 2026, UAB TELTONIKA NETWORKS.
Specifications and information given in this document are subject to change by UAB TELTONIKA NETWORKS without prior notice.

TOPOLOGY



SECURE VPN ACCESS WITH RELIABLE 5G CONNECTIVITY

The solution breaks down into a few simple components. First, an industrial cellular router, such as RUTM30, strengthens remote connectivity by providing 5G with automatic fallback to LTE Cat 19 and 3G, reducing the risk of internet outages. It can be used as a standalone product or as backup internet for an existing router, with dual SIM and eSIM support enabling seamless, automatic switching among up to 7 carrier profiles per eSIM

RUTM30 also supports a wide range of VPN protocols, including OpenVPN, IPsec, and WireGuard, making it an ideal foundation for secure networking between internal enterprise systems and remote offices. With a Gigabit Ethernet port and dual-band Wi-Fi, it can connect multiple devices, including PCs, laptops, VoIP phones, and printers, ensuring essential equipment stays online. Since the router has Ethernet ports (typically used for the primary WAN/internet connection), additional wired devices can be connected via an external switch, while other devices can connect wirelessly over Wi-Fi.

The router is fully compatible with Teltonika Remote Management System (RMS), which enables remote monitoring of the device, along with remote setup and configuration. This gives IT support teams the ability to configure many devices quickly and centrally before shipping them out to remote workers or remote offices. Through RMS, IT teams can take advantage of zero-touch provisioning: the router arrives at the employee's location fully configured, so all they need to do is power it on and connect their laptop to start working immediately.

Finally, RUTM30 also supports traffic segregation through VLANs, allowing different traffic sources (e.g., guest devices, VoIP, or corporate systems) to be kept separate and secure on the same network. Additionally, RutOS provides data limit controls, letting IT teams monitor and cap cellular data usage to keep connectivity costs predictable and under control.

Ready to secure and connect your remote workforce? Explore RUTM30 or get in touch with the Teltonika team to discuss a deployment tailored to your business.

Copyright © 2026, UAB TELTONIKA NETWORKS.
Specifications and information given in this document are subject to change by UAB TELTONIKA NETWORKS without prior notice.