ChiefNET

CHIEFNET SD-WAN · APPLICATION NOTE

Remote IoT and Edge Sites

Secure LTE/5G connectivity for kiosks, ATMs, telecom shelters and unmanned sites

Utilities · Telecom · Banking · Retail

Document reference	Version	Date	Published by
CN/SDW/AN/IOT/v1.0	1.0	November 2026	ChiefNET Private Limited

Contents

1. Overview
2. The Challenge
3. The ChiefNET Solution
4. Reference Architecture
5. Key Benefits
6. Capability Map
7. Deployment Summary
8. Conclusion

Also available online at chiefnet.io/use-cases/sd-wan/remote-iot-edge-sites/

Overview

Many organisations operate large numbers of small sites that no one works at: self-service kiosks, ATMs, telecom equipment shelters, water pumping stations, environmental monitoring posts, digital signage and similar installations. Each site has only a few connected devices, often a controller, some sensors, a terminal or a camera, but every one of them must be reachable by the operations team, and none should be reachable by anyone else.

This application note describes how ChiefNET SD-WAN connects these remote and unmanned sites over cellular networks, using the compact CN-IOT-1 CPE, zero-touch provisioning and a private network that exposes no ports to the Internet.

The Challenge

Consider a utility with 300 pumping stations and monitoring posts, or a bank with several hundred off-site ATMs and kiosks. The sites share common problems:

- **No wired service.** Many sites are in places where fixed broadband is unavailable or uneconomic. Cellular is the only practical option.
- **No local staff.** Nobody on site can configure a router, and every visit by a technician is costly.
- **Exposed devices.** Controllers, terminals and cameras are often reached by forwarding ports on a cellular router or by relying on a public IP address. These devices rarely have strong authentication.
- **Small, metered data plans.** Cellular plans have limited data allowances, and unexpected traffic can exhaust them.
- **Large fleets.** Hundreds or thousands of sites must be deployed, monitored and updated consistently.

The ChiefNET Solution

ChiefNET places a compact, pre-provisioned CPE at each site and connects it over the mobile network to the ChiefNET Cloud WAN, managed from the ChiefNET Orchestrator.

CN-IOT-1 for small sites

The CN-IOT-1 is ChiefNET's CPE for IoT and edge sites. It is a Raspberry Pi-based device in a custom enclosure, with one Gigabit Ethernet port and Wi-Fi, a maximum power consumption of 20 W, 50 Mbps of WAN/Internet throughput and 5 Mbps of VPN throughput, and a recommended load of five endpoints. That profile suits telemetry, alarms, transaction traffic and remote management sessions at sites with a small number of devices.

At remote sites, the CN-IOT-1 connects to the mobile network through a qualified USB LTE or 5G modem. Sites that need more capacity or more endpoints can use a CN-4, which offers optional built-in LTE/5G.

Zero-touch provisioning

Every CPE is pre-provisioned for its organisation before it ships, and site configuration can be prepared in the ChiefNET Orchestrator in advance. At the site, the installer only connects power, the cellular modem and the local device. The CPE then connects to the Orchestrator and the ChiefNET Cloud WAN on its own, and is reported online. No skilled personnel are needed on site.

Software is updated remotely from the Orchestrator, and every new device provisioning raises an event, so an unexpected device appearing in the network is visible immediately.

Private access with no open ports

The CPE does not accept inbound connections on its WAN interface; all WAN ports are blocked by default and the CPE initiates every connection itself. Traffic between the site and the operations centre is carried over an AES-256 encrypted tunnel, authenticated by the CPE's own X.509 certificate.

Operators reach the controller, terminal or camera at each site through this tunnel as if it were on the local network. Because nothing is published to the Internet, the devices cannot be found or attacked from outside, even if their own passwords are weak. Where sites reuse the same private address range, which is common in large fleets, DNAT within the secure SD-WAN network gives each site's devices a distinct, reachable address. Port forwarding to LAN-side devices is available only after explicit configuration.

IoT devices can also be configured as **enterprise-only systems**, allowed to communicate with the operations centre but not with the Internet. DNS filtering blocks malware and phishing domains, and application control can block unwanted services entirely.

Protecting the cellular data plan

ChiefNET traffic policies classify traffic by address, port, protocol or application domain and decide what is allowed and on which link. On a metered cellular connection, administrators can:

- Allow only the operational traffic the site needs and drop everything else.
- Apply maximum bandwidth limits to non-critical flows, and real-time QoS to telemetry and monitoring traffic.
- At sites with both a fixed line and a cellular link, use exclusive WAN port selection to keep low-priority traffic off the cellular link entirely.

Remote management and troubleshooting

The Orchestrator shows the status and quality of each site's WAN link and tunnel, and raises alerts for link loss, poor link quality and tunnel latency. Administrators can configure ping-latency monitoring to a device at the site, such as a pump controller, so that loss of reachability is reported

by email or Telegram.

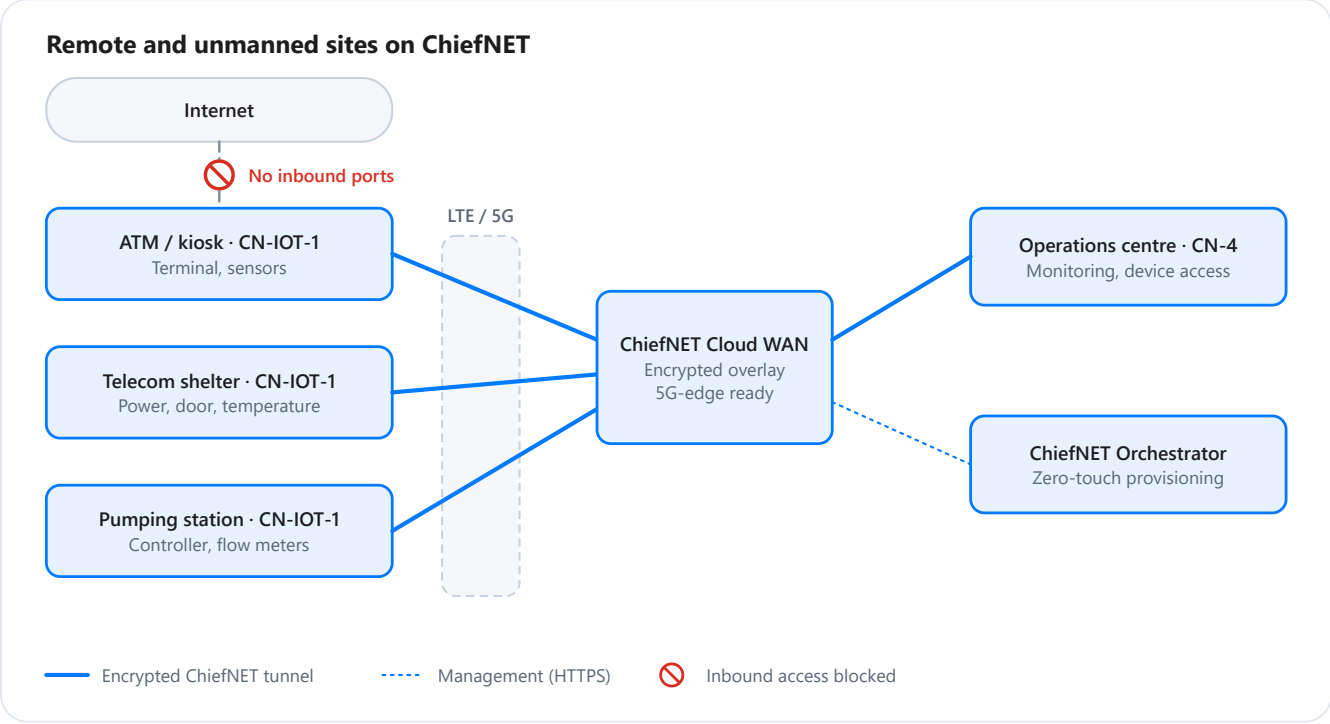
A USB cellular interface can also be fitted for remote management, giving support staff an additional way to reach a CPE for diagnosis. Each CPE also operates autonomously and does not need constant contact with the Orchestrator to keep forwarding traffic.

Ready for 5G and large fleets

ChiefNET is built on a cloud-native, microservices architecture that scales from a few devices to thousands for a single enterprise. The platform is designed to be deployed as a service in 5G edge clouds, providing secure, low-latency connectivity for IoT and IIoT devices at very large scale. VPN gateways can be launched on demand, as containers, in data centres close to the sites they serve.

Reference Architecture

The diagram shows an ATM or kiosk, a telecom shelter and a pumping station, each with a CN-IOT-1 connected over the LTE/5G mobile network. Each CPE builds an encrypted tunnel to the ChiefNET Cloud WAN, through which the operations centre monitors and accesses the site devices. The Internet has no inbound path to any site. The ChiefNET Orchestrator handles zero-touch provisioning and central management.



ATMs, telecom shelters and pumping stations with CN-IOT-1 CPEs connect over LTE or 5G to an operations centre through ChiefNET Cloud WAN, with no inbound ports open.

Key Benefits

- **Connect anywhere with coverage.** LTE and 5G bring sites without wired service into the enterprise network.
- **No technician required.** Pre-provisioned CPEs come online with power and a cellular connection.
- **Hidden from the Internet.** No inbound ports means site devices cannot be discovered or attacked from outside.
- **Controlled data usage.** Traffic policies keep metered cellular plans for operational traffic.
- **Fleet-scale operations.** Central provisioning, monitoring and remote software updates cover thousands of sites.
- **Built for growth.** A cloud-native, 5G-ready architecture supports expanding IoT deployments.

Capability Map

ChiefNET capability	How it is used here
CN-IOT-1 compact CPE	Low-power connectivity for sites with a few devices
USB LTE/5G modem, or built-in LTE/5G on CN-4	Connects sites over the mobile network
Zero-touch provisioning	Brings sites online without skilled staff on site
No open WAN ports, AES-256 tunnels	Keeps site devices private and unreachable from the Internet
DNAT within the SD-WAN	Reaches devices at sites that share the same private address range
Traffic policies and QoS	Restricts traffic to what the site needs and protects metered data plans
Link, tunnel and ping-latency alerts	Reports site and device reachability by email or Telegram
Cloud-native, 5G-edge-ready architecture	Scales to large fleets of IoT and edge sites

Deployment Summary

1. List site types, the devices at each, their traffic needs and the available cellular operators.
2. Select CN-IOT-1 for small sites, or CN-4 where more capacity is needed, and qualified LTE or 5G modems.
3. Define traffic policies, address translation and alert settings in the ChiefNET Orchestrator.
4. Ship pre-provisioned devices; installers connect power, the modem and the site device.

5. Confirm each site is online, verify access from the operations centre, and enable reachability alerts.

Conclusion

Remote and unmanned sites need connectivity that installs itself, stays private and uses limited cellular data sensibly. ChiefNET SD-WAN, with the compact CN-IOT-1, brings kiosks, ATMs, telecom shelters and pumping stations into an encrypted private network with no open ports, managed centrally and ready to scale on 5G.

ChiefNET

About ChiefNET Private Limited

ChiefNET Private Limited, founded in 2020 and headquartered in Coimbatore, India, builds secure networking products for enterprises and critical infrastructure: ChiefNET SD-WAN, a cloud-managed network platform for multi-site organisations, and ChiefNET OT Shield, a hardware-enforced data diode for operational technology.

---

contact@chiefnet.io · chiefnet.io
DVP Building, First Floor, No. 4, Kalapatti Main Road, Civil Aerodrome Post, Nehru Nagar West, Coimbatore, Tamil Nadu 641014, India