ChiefNET

CHIEFNET SD-WAN · APPLICATION NOTE

Manufacturing Plant Connectivity

One secure network for factory floors, remote monitoring stations and corporate offices

Manufacturing · Industrial

Document reference	Version	Date	Published by
CN/SDW/AN/MFG/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/manufacturing-plant-connectivity/

Overview

Manufacturers run some of the most geographically spread networks in any industry. Production plants sit in industrial zones, remote monitoring stations sit at tank farms, substations or water intakes, and planning, finance and IT teams work from a corporate office. All of them depend on shared applications: Enterprise Resource Planning (ERP) for orders, inventory and finance, and Manufacturing Execution Systems (MES) for production scheduling, tracking and quality.

This application note describes how ChiefNET SD-WAN interconnects these locations into one managed, encrypted network, and how it handles the realities of plant connectivity: unreliable links, remote sites without wired access, and a small central IT team.

The Challenge

Consider a manufacturer with three plants, a dozen remote monitoring stations and a corporate office. ERP runs in a public cloud, and each plant runs MES servers that exchange data with ERP and with each other.

- **Unreliable links in industrial areas.** Plants often rely on whichever ISP is available locally, and link quality varies through the day.
- **Remote stations without wired access.** Monitoring stations may be far from any fixed-line service and must rely on 4G or 5G.
- **ERP and MES must stay in step.** Production orders, material consumption and finished-goods data move constantly between MES and ERP. Delays lead to wrong stock positions and late shipments.
- **Large campuses.** Plants with several buildings depend on optical LAN links between them; a cut cable can isolate a building.
- **Third-party and engineering access.** Engineers and equipment vendors need access to specific plant servers, which is often provided by opening ports or installing remote-access tools.
- **Separation of IT and OT.** Plant control networks must be kept apart from business IT traffic.

The ChiefNET Solution

ChiefNET places a pre-provisioned CPE at every plant, station and office, and connects them through the ChiefNET Cloud WAN. All configuration and monitoring are done centrally in the ChiefNET Orchestrator, which can be hosted in the cloud, installed on premises, or used in a hybrid arrangement.

Plants and offices on one encrypted network

Each plant and the corporate office receive a CN-4 appliance. The CN-4 provides four 2.5 GbE ports, with optional optical ports and optional built-in LTE/5G, and supports up to 800 Mbps of VPN throughput. Its listed deployment environments include retail and industrial sites; because it is a fanless, low-power appliance, it should be installed where there is adequate airflow.

All traffic between sites is encrypted with AES-256, and each CPE authenticates with its own X.509 certificate. Routing between sites is automatic. Where plants already run their own routers, ChiefNET supports OSPF and BGP, and static routes on a CPE can be redistributed into the dynamic routing protocol so that every site learns them.

The cloud-hosted ERP joins the same network through a CN-Cloud-1 instance in the VPC or VNET. If ERP runs in a private data centre instead, a CN-VM-1 virtual CPE on VMware or KVM serves the same role.

Remote monitoring stations over LTE

Small, remote stations use the CN-IOT-1, a compact, low-power CPE intended for sites with a handful of devices. Paired with a qualified USB LTE or 5G modem, it connects over the mobile network and builds the same encrypted tunnel as a plant CPE. Its VPN throughput of 5 Mbps is suited to telemetry, alarms and remote management sessions rather than bulk data.

Because ChiefNET's architecture is designed for deployment in 5G edge clouds, the same approach extends to private and public 5G networks as they become available at industrial sites.

Resilient plant connectivity

Each CPE can use two or more WAN links, such as a fibre service and a 4G/5G connection. ChiefNET continuously measures packet loss, latency and jitter on every link and tunnel and switches traffic when configured thresholds are crossed. Traffic can also be load-balanced across links with per-flow balancing. Each CPE operates autonomously and does not need continuous contact with the Orchestrator to keep forwarding traffic.

For large campuses, ChiefNET can use on-premises paths as the preferred route between buildings, with the Cloud WAN as a fallback if an optical LAN link between buildings fails.

Critical sites can deploy two CN-4 units as a VRRP hot-standby pair, so that a device or interface failure does not interrupt the plant.

Predictable MES and ERP performance

ChiefNET's QoS engine classifies traffic by subnet, port, protocol or application domain. Typical policies are:

- **Minimum bandwidth** for ERP and MES traffic between plants and the cloud.
- **Real-time** profiles for monitoring applications, IoT traffic and plant VoIP.
- **Maximum bandwidth** limits for software updates, backups and general browsing.

At plants where cameras verify assembly or packing, video can be carried on the same network with its own QoS profile.

Controlled access to plant systems

Engineers at the corporate office can reach specific plant servers through the encrypted tunnels. Port forwarding to LAN-side servers is available only after explicit configuration, and DNAT within the SD-WAN network allows access to plants that use overlapping private address ranges. No ports are opened on any WAN interface, so plant servers are never published to the Internet.

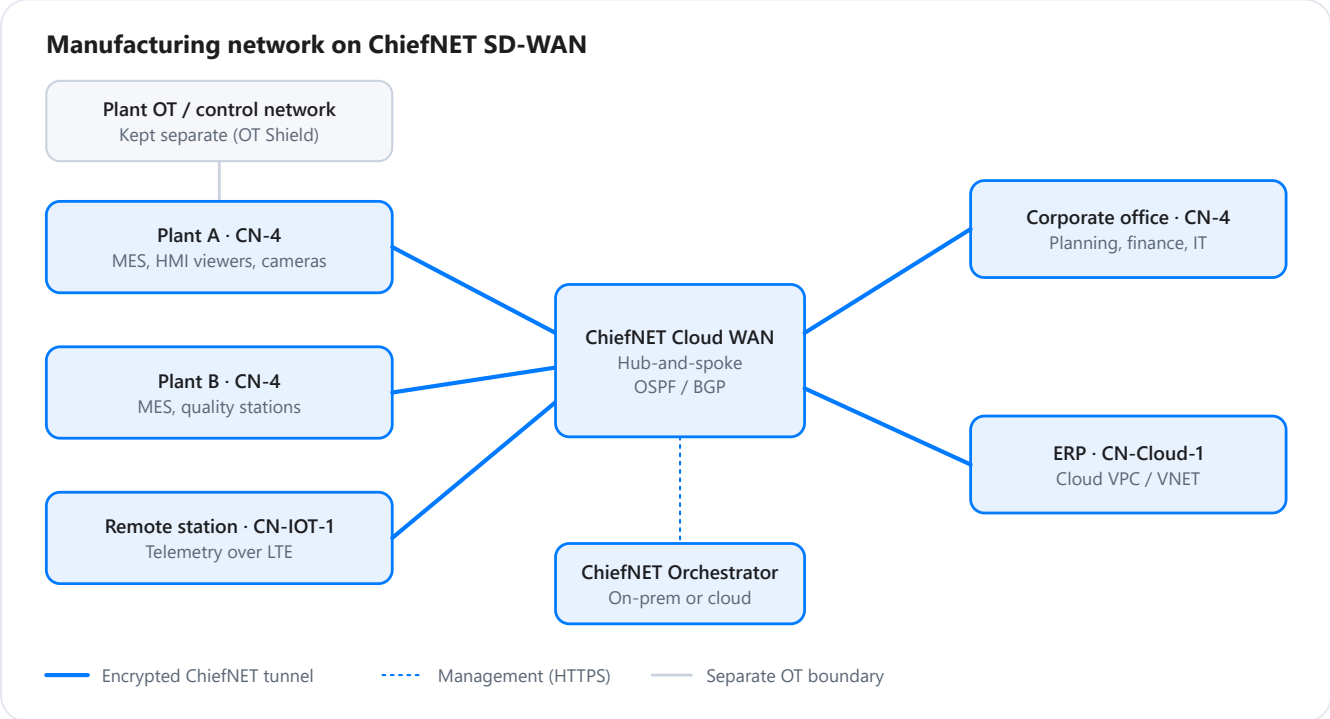
Plant IT networks can be segmented with VLANs, and devices that should communicate only with internal systems can be configured as **enterprise-only systems**, restricted to the enterprise tunnels. DNS filtering blocks malware and phishing domains across all sites.

Keeping OT separate

Plant control networks should stay separate from business IT traffic; for operational technology networks that require hardware-enforced, one-way isolation, ChiefNET offers a separate product line, OT Shield.

Reference Architecture

The diagram shows two plants with CN-4 CPEs, a remote monitoring station with a CN-IOT-1 on LTE, and the corporate office, all connected through the ChiefNET Cloud WAN to ERP running on a CN-Cloud-1 in a cloud VPC or VNET. The ChiefNET Orchestrator manages every device and can run in the cloud or on premises. The plant OT network sits behind its own boundary and is not part of the SD-WAN.



Plants, a remote LTE monitoring station and the corporate office connect to cloud-hosted ERP over ChiefNET Cloud WAN; plant OT networks stay separate.

Key Benefits

- **Synchronised production and business data.** Always-on, prioritised links keep MES and ERP in step across all plants.
- **Remote sites included.** LTE- or 5G-connected CN-IOT-1 units bring stations without wired access into the same network.
- **Resilience to poor local links.** Quality-based failover and load balancing keep plants connected when an ISP degrades.
- **No exposed plant servers.** Access is through encrypted tunnels with explicit policies, not open ports.
- **Fits existing routing.** OSPF, BGP and static route redistribution work with established plant networks.
- **Flexible management.** The Orchestrator can run in the cloud, on premises or in a hybrid model.

Capability Map

ChiefNET capability	How it is used here
ChiefNET Cloud WAN with OSPF, BGP and static redistribution	Connects plants, stations and offices and integrates with existing plant routers
CN-4 with dual WAN, link-quality monitoring and failover	Keeps plant connectivity up when a local ISP degrades
CN-IOT-1 with USB LTE/5G modem	Connects remote monitoring stations without wired service
CN-Cloud-1 or CN-VM-1	Brings ERP in the cloud or data centre into the same network
Hierarchical QoS	Guarantees bandwidth for ERP and MES, real-time handling for monitoring traffic
DNAT within the SD-WAN and explicit port forwarding	Gives engineers controlled access to specific plant servers
Edge Device HA (VRRP)	Protects critical plants against CPE or interface failure
On-premises, cloud or hybrid Orchestrator	Matches the management model to the manufacturer's IT policy

Deployment Summary

1. Survey plants, stations and offices; record available WAN links, existing routers and key MES and ERP flows.
2. Select CN-4 for plants and offices, CN-IOT-1 for remote stations, and CN-Cloud-1 or CN-VM-1 for ERP.
3. Choose cloud, on-premises or hybrid Orchestrator hosting and pre-provision all devices and policies.
4. Ship devices; site staff connect power, WAN links and the plant IT LAN.
5. Validate routing with existing plant routers, test failover, and enable alerts and reports.

Conclusion

Manufacturers need their plants, remote stations and offices to work as one organisation. ChiefNET SD-WAN provides a single encrypted network that keeps ERP and MES synchronised, handles unreliable industrial-area links, brings LTE-only stations into the fold, and gives engineers controlled access to plant systems without exposing them to the Internet.

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