ChiefNET

CHIEFNET SD-WAN · APPLICATION NOTE

Hybrid and Multi-Cloud Connectivity

One private network across branches, data centres and AWS, Azure, GCP and DigitalOcean

Cross-industry · Enterprise IT

Document reference	Version	Date	Published by
CN/SDW/AN/CLOUD/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/hybrid-multi-cloud/

Overview

Enterprise applications no longer live in one place. A typical organisation runs some workloads in its own data centre, some in one or more public clouds, and some as SaaS. Users in branches and offices need reliable, secure access to all of them, and applications in different clouds increasingly need to talk to each other.

This application note explains how ChiefNET SD-WAN extends a single private network across branches, on-premises data centres and multiple public clouds, using physical, virtual and cloud CPEs that are all managed from the ChiefNET Orchestrator.

The Challenge

Consider an enterprise with 30 branch offices, a data centre running VMware, an application tier in AWS, ERP and databases in Azure, and analytics services in GCP. Its network team faces the following:

- **A separate VPN for every cloud.** Each cloud has its own VPN service, configuration model and limits. Connecting every branch to every cloud multiplies tunnels and routing work.
- **Inconsistent policy.** Security and QoS rules differ between the branch routers, the data centre firewall and each cloud's native gateway.
- **Private DNS across environments.** Internal names are hosted in the data centre and in cloud DNS services, and must resolve correctly from every site without being exposed to ISP resolvers.
- **Overlapping address ranges.** Cloud VPCs, acquired businesses and legacy sites often reuse the same private subnets.
- **Hardware dependency.** Traditional appliances do not run in a cloud VPC, so the cloud edge is managed differently from the branch edge.

The ChiefNET Solution

ChiefNET uses the same software on every type of CPE, so a branch appliance, a data-centre virtual machine and a cloud instance all behave as members of one network with one policy model.

A CPE for every location

Model	Where it runs	WAN/VPN throughput	Recommended endpoints
CN-4	Hardware appliance at branches and offices	2.5 Gbps / 800 Mbps	100

Model	Where it runs	WAN/VPN throughput	Recommended endpoints
CN-VM-1	Virtual machine on VMware or KVM in a data centre	1 Gbps (variable) / 200 Mbps	150
CN-Cloud-1	Instance in a VPC or VNET on AWS, Azure, GCP or DigitalOcean	1 Gbps (variable) / 200 Mbps	150

CN-VM-1 and CN-Cloud-1 each provide four virtual Ethernet interfaces. A Cloud CPE deployed in a VPC turns that VPC into an edge location of the enterprise network, exactly like a branch. Because ChiefNET runs on standard x86 and ARM hardware and on common virtualisation platforms, there is no dependency on proprietary hardware.

Site-to-cloud and site-to-site connectivity

Every CPE builds AES-256 encrypted tunnels to the ChiefNET Cloud WAN, authenticated with a per-device X.509 certificate. The Cloud WAN forms a hub-and-spoke network over which routes are exchanged automatically, so branches, the data centre and every cloud VPC can reach each other as soon as their CPEs come online. Each customer's network is isolated from all others.

For paths that need a more direct route, ChiefNET's on-premises VPN server feature creates tunnels between sites without passing through the Cloud WAN, for example between the data centre and a cloud VPC. Several sites can host such servers, enabling hub-and-spoke, hub-mesh or custom-mesh topologies within the same network.

The Cloud WAN itself runs on public cloud infrastructure and is operated by ChiefNET; the choice of underlying cloud is transparent to the customer. When hosted on a provider with a global backbone, such as GCP, branches in different countries can use that backbone between regions. ChiefNET VPN gateways are built as containers and can be launched on demand in data centres closer to the customer's sites.

Routing into cloud and data-centre networks

Routing is preconfigured and automatic between CPEs. Where a cloud VPC or data centre has additional subnets behind the CPE, static routes on that CPE can be redistributed into the dynamic routing protocol so that every site learns them. ChiefNET supports OSPF and BGP for integration with existing data-centre routing.

ChiefNET also supports IPsec in both client and server modes, which allows interconnection with native public-cloud VPN services and with IPsec-capable firewalls where a Cloud CPE is not used.

Where two environments use overlapping address ranges, DNAT within the secure SD-WAN network lets a site publish selected servers to the rest of the network without renumbering.

Private DNS across environments

Split-horizon DNS lets each CPE send queries for the organisation's own domains to designated DNS servers, such as a DNS service in the data centre or a cloud DNS service, while other lookups go to public resolvers. If the designated servers return "no such domain", the ISP's resolvers are not consulted, so internal names and addresses do not leak.

Consistent policy and local breakout

The same traffic policies, QoS profiles, DNS filtering and application control are available on every CPE type. Branches can apply minimum-bandwidth QoS to traffic for ERP in Azure, while sending SaaS traffic such as Microsoft 365 directly to the Internet through Local Internet Breakout instead of hairpinning through a data centre or cloud.

Orchestrator on cloud, on premises or hybrid

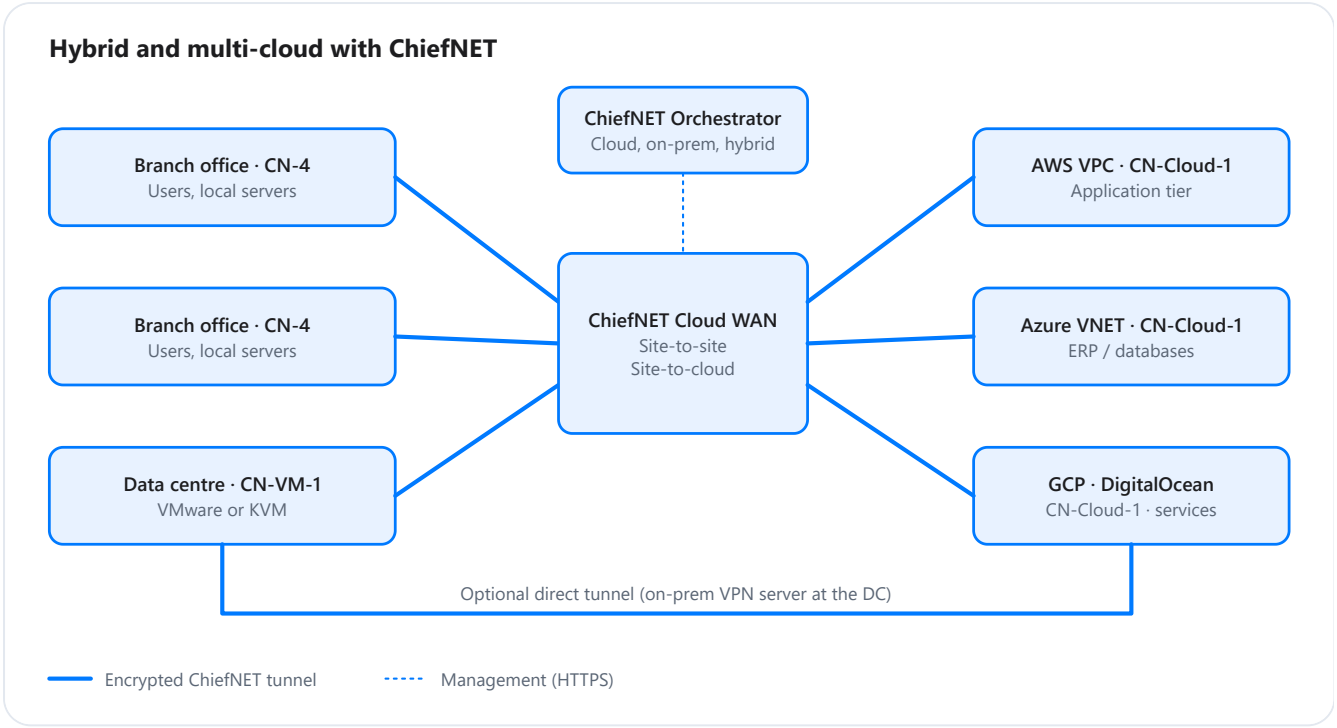
The ChiefNET Orchestrator can be deployed in three ways:

- **On cloud.** ChiefNET hosts and maintains all backend services. Devices can be pre-provisioned before they ship, or while they are in transit.
- **On premises.** The ChiefNET team installs the backend services and gateway on virtual machines provided by the customer, as a one-time service, and maintains them afterwards.
- **Hybrid.** A combination of both, for example on-premises paths preferred with cloud fallback.

The Orchestrator, gateways and CPEs all support redundant, high-availability deployment.

Reference Architecture

The diagram shows two branches with CN-4 appliances and a data centre with a CN-VM-1 on VMware or KVM, connected through the ChiefNET Cloud WAN to CN-Cloud-1 instances in AWS, Azure, and GCP or DigitalOcean. An optional direct tunnel links the data centre to a cloud VPC through the on-premises VPN server feature. The ChiefNET Orchestrator, hosted in the cloud, on premises or in a hybrid model, manages every CPE.



Branches and a data centre with a virtual CPE connect through ChiefNET Cloud WAN to Cloud CPEs in AWS, Azure, GCP and DigitalOcean.

Key Benefits

- **One network, many clouds.** Branches, data centres and multiple public clouds join one encrypted network with automatic routing.
- **One policy model.** QoS, filtering and steering rules are the same on hardware, virtual and cloud CPEs.
- **Flexible topology.** Hub-and-spoke through the Cloud WAN, plus direct tunnels where latency or volume requires them.
- **Private name resolution.** Split-horizon DNS keeps internal domains resolvable everywhere and private.
- **No hardware lock-in.** CPEs run on standard hardware, VMware, KVM and the major public clouds.
- **Management that fits policy.** The Orchestrator can run in the cloud, on premises or in a hybrid model.

Capability Map

ChiefNET capability	How it is used here
CN-Cloud-1 on AWS, Azure, GCP and DigitalOcean	Makes each VPC or VNET an edge location of the enterprise network

ChiefNET capability	How it is used here
CN-VM-1 on VMware or KVM	Connects the private data centre with the same software as branches
ChiefNET Cloud WAN with automatic routing	Provides site-to-site and site-to-cloud connectivity
On-premises VPN server	Adds direct tunnels between selected sites or clouds
Static route redistribution, OSPF and BGP	Advertises cloud and data-centre subnets to all sites
IPsec client and server	Interconnects with native cloud VPN services and IPsec-capable firewalls
Split-horizon DNS	Resolves internal domains through enterprise or cloud DNS servers only
DNAT within the SD-WAN	Reaches servers in environments with overlapping address ranges

Deployment Summary

1. Map applications to their locations and list the subnets, DNS zones and traffic volumes for each environment.
2. Choose the Orchestrator deployment model and the topology (hub-and-spoke, plus any direct tunnels).
3. Deploy CN-Cloud-1 instances in each VPC or VNET and CN-VM-1 in the data centre; ship CN-4 units to branches.
4. Configure route redistribution, split-horizon DNS, QoS and breakout policies centrally.
5. Verify reachability between every branch and every cloud, then enable monitoring and alerts.

Conclusion

As applications spread across data centres and several clouds, the network has to follow them without multiplying complexity. ChiefNET SD-WAN provides one encrypted network and one policy model across branches, VMware and KVM data centres, and AWS, Azure, GCP and DigitalOcean, with a management plane that can run wherever the organisation prefers.

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