ChiefNET

CHIEFNET SD-WAN · APPLICATION NOTE

Cloud Security and SASE Integration

Local breakout with network-level protection, plus optional Palo Alto Networks Prisma Access per site

Cross-industry · Regulated enterprises

Document reference	Version	Date	Published by
CN/SDW/AN/SASE/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/cloud-security-sase/

Overview

Branch users now spend most of their time on Internet and SaaS applications. Sending all of that traffic back to a central firewall wastes bandwidth and adds latency, but sending it straight to the Internet from each branch raises the question of how it is protected.

This application note describes the two layers of protection available with ChiefNET SD-WAN. The first is built into every ChiefNET CPE: a network firewall, DNS filtering, application control and a hardened edge with no open ports, combined with Local Internet Breakout. The second is an optional integration, configurable per CPE, with Palo Alto Networks Prisma Access, a cloud-delivered security service that adds content-level inspection. Enterprise traffic continues to travel over the ChiefNET Cloud WAN in both cases.

The Challenge

Consider an organisation with 80 branches and a single firewall at headquarters. Today, all branch traffic is backhauled to headquarters for inspection. The IT team sees the following:

- **Backhaul congestion.** SaaS and general web traffic consume headquarters bandwidth and slow down enterprise applications.
- **Added latency.** Users in distant branches experience slow cloud applications because traffic travels to headquarters and back.
- **Uneven security needs.** Some sites, such as finance offices or sites handling regulated data, need content inspection; others need only solid network-level controls.
- **Cost of full appliances everywhere.** Placing a full content-inspection firewall at every branch is expensive to buy and maintain.

The ChiefNET Solution

ChiefNET combines network-level security built into every CPE with Local Internet Breakout, and adds content-level inspection through Prisma Access only at the sites that need it.

Built-in network-level security on every CPE

ChiefNET is a network firewall. Every CPE provides the following without additional products:

- **No open ports.** All WAN ports are closed by default. Only outbound connections, from LAN to Internet and LAN to enterprise, are permitted, and this is verified with Nessus and Nmap sweeps. ChiefNET also provides a periodic WAN-side vulnerability assessment report.
- **Hardened CPE.** The CPE runs a hardened operating system with long-term support, local access is disabled entirely, and software is updated remotely from the Orchestrator.

- **Stateful filtering.** 5-tuple filters on source and destination address, protocol and ports, with domain names usable in place of IP addresses.
- **DNS filtering.** Curated, automatically updated blocklists for categories such as malware, phishing, spyware and adware, trackers, adult content and cryptocurrency, plus organisation-specific allow and block lists. Because whole domains are blocked, this also covers most needs traditionally met by URL filtering.
- **Application control.** Predefined and custom applications, defined by their domains, can be blocked or given specific QoS and link policies.
- **Split-horizon DNS.** Lookups for internal domains go only to the organisation's DNS servers, so internal names are not exposed to ISP resolvers.
- **Strong encryption and identity.** Enterprise traffic is encrypted with AES-256, each CPE has its own certificate-based identity, and every customer's traffic is isolated from all others.

Local Internet Breakout

With Local Internet Breakout, ChiefNET separates traffic at the branch. Enterprise traffic, such as ERP, databases or CCTV, is sent over encrypted tunnels to the ChiefNET Cloud WAN. Selected Internet traffic, such as Microsoft 365, goes directly to the Internet from the branch under the CPE's network firewall and DNS filtering. This reduces latency for cloud applications, removes unnecessary load from headquarters, and keeps Internet traffic away from the enterprise network.

Alternatively, a site can be configured to send all of its traffic, including Internet-bound traffic, through the encrypted tunnels. Internet traffic is then also protected from observation on the local access network, and leaves the ChiefNET network with the same network-level controls applied.

Optional content-level security with Prisma Access

ChiefNET does not perform content inspection itself. Capabilities such as deep packet inspection, TLS/SSL inspection, antivirus, URL-level filtering and email or attachment scanning are delivered through integration with a cloud security service. ChiefNET has interoperated with Palo Alto Networks Prisma Access for this purpose.

The integration is an option configured per CPE:

- On a CPE with Prisma Access enabled, ChiefNET builds an IPsec tunnel to the Prisma Access service using a dedicated Prisma interface type. Internet-bound traffic from that site is sent through the tunnel and inspected by Prisma Access before reaching Internet destinations.
- Enterprise traffic from the same site continues to use ChiefNET Cloud WAN tunnels to headquarters, data centres and other branches, with ChiefNET's routing, QoS and failover policies.
- CPEs without Prisma Access continue to use local breakout or full tunnelling with ChiefNET's network-level protection.

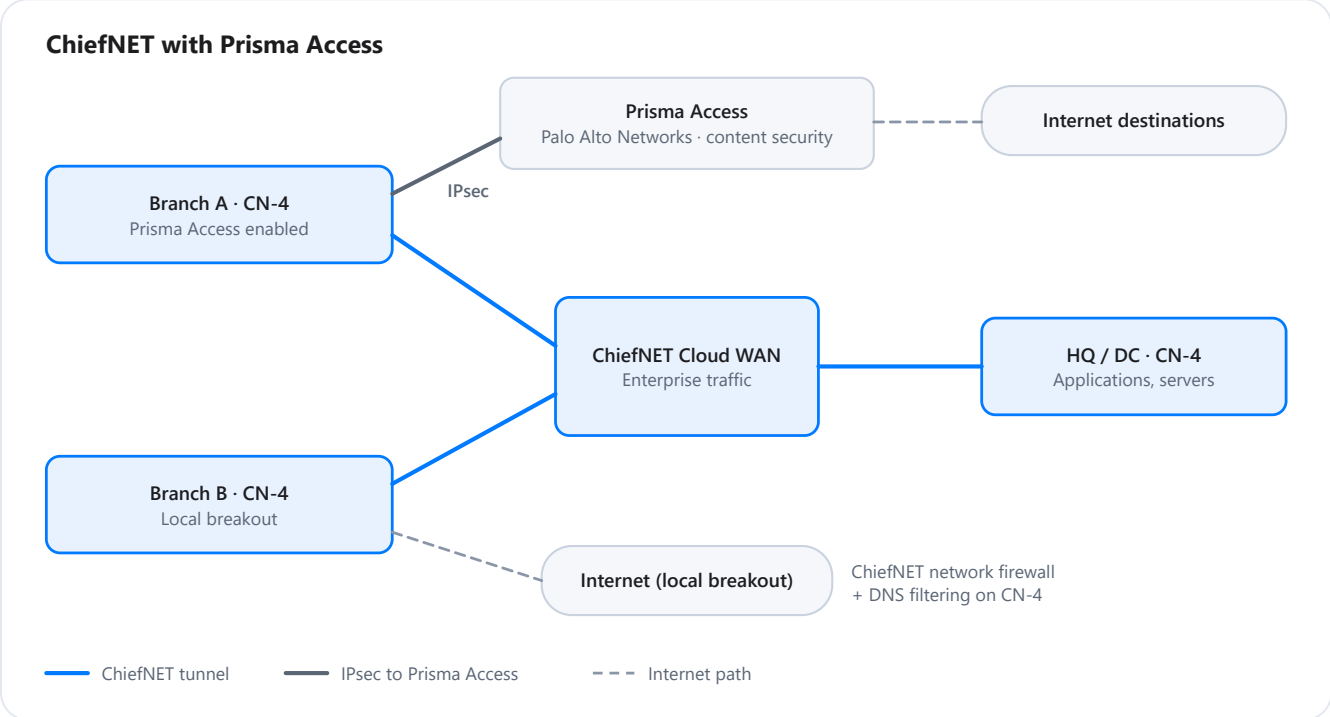
This allows an organisation to apply content inspection where it is needed, for example at headquarters and finance offices, without changing the design of the rest of the network. Prisma Access is subscribed to separately; ChiefNET can operate the integration as part of a managed service.

Working with existing firewalls

ChiefNET also works alongside firewalls already at a site. The CPE can be placed in front of the firewall, connected directly to the ISPs, or behind it on the LAN side. Its IPsec client and server modes allow it to interconnect with IPsec-capable firewalls and other security services. Many organisations keep a firewall only at headquarters and rely on ChiefNET's local breakout and network firewall at branches.

Reference Architecture

The diagram shows two branches. Branch A has Prisma Access enabled: its Internet-bound traffic travels over IPsec to Prisma Access for content security, while its enterprise traffic uses the ChiefNET Cloud WAN to reach HQ. Branch B does not use Prisma Access: its Internet traffic breaks out locally with ChiefNET's network firewall and DNS filtering, and its enterprise traffic also uses the Cloud WAN.



Branch A sends Internet traffic over IPsec to Prisma Access; branch B uses local breakout with ChiefNET's network firewall; both carry enterprise traffic over ChiefNET Cloud WAN.

Key Benefits

- **Lower latency to SaaS.** Local breakout removes the round trip to headquarters for cloud applications.
- **Strong baseline at every branch.** No open ports, DNS filtering, application control and encryption come with every CPE.
- **Content inspection where needed.** Prisma Access can be enabled per site rather than across the whole estate.
- **Enterprise traffic stays private.** Branch-to-HQ traffic remains on encrypted ChiefNET Cloud WAN tunnels in every design.
- **Full-tunnel option.** Sites that need it can send all traffic, including Internet traffic, through the encrypted tunnels.
- **Fits existing security investments.** ChiefNET works in front of, behind or alongside existing firewalls.

Capability Map

ChiefNET capability	How it is used here
Local Internet Breakout	Sends selected SaaS and web traffic directly to the Internet from each branch
Network firewall with 5-tuple and domain filters	Controls what each branch can reach
DNS filtering with curated blocklists	Blocks malware, phishing and unwanted categories at every site
Split-horizon DNS	Keeps internal domain names away from ISP resolvers
No open WAN ports, hardened CPE	Removes inbound attack surface at the branch edge
ChiefNET Cloud WAN tunnels (AES-256)	Carries enterprise traffic between branches, HQ and data centres
IPsec client with Prisma interface	Connects selected CPEs to Palo Alto Networks Prisma Access
Per-CPE configuration	Enables content-level security only at the sites that require it

Deployment Summary

1. Classify sites by security requirement: network-level controls only, or network plus content inspection.
2. Define breakout rules, DNS filtering categories and application controls in the ChiefNET Orchestrator.

3. For sites that need content inspection, obtain Prisma Access and configure the Prisma IPsec interface on those CPEs.
4. Confirm that enterprise traffic uses Cloud WAN tunnels and Internet traffic follows the intended path at each site.
5. Review DNS filtering and application-control events and adjust allow and block lists.

Conclusion

ChiefNET SD-WAN gives every branch a secure starting point: no open ports, DNS filtering, application control and encrypted enterprise connectivity, with local breakout to keep cloud applications fast. Where content-level inspection is needed, Palo Alto Networks Prisma Access can be added per CPE, alongside the ChiefNET Cloud WAN. Organisations can therefore match the level of security to each site's needs within one design.

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