



ChiefNET

Secured, Managed
Cloud native SD-WAN

Overview

A cloud-native SD-WAN (Software-Defined Wide Area Network) is a networking solution built on cloud principles like microservices and scalability. It is designed to be managed and delivered from a centralized cloud platform, simplifying management, and providing flexible, on-demand connectivity.

ChiefNET transforms enterprise networking by unifying headquarters, branch offices, and cloud environments into a single, streamlined platform. With just one on-premises device per location—physical or virtual—deployment is fast, scalable, and cost-efficient.

Every customer network is automatically provisioned with secure site-to-site connectivity, along with seamless access to data centers and cloud services. Whether you're expanding across geographies or integrating hybrid infrastructure, ChiefNET delivers simplicity without compromise.

Key Components

- **Cloud Orchestrator/Controller:** This is the centralized management and policy engine. It provides a single pane of glass for configuring, provisioning, monitoring, and troubleshooting the entire network. It enables zero-touch provisioning for new devices and automated policy enforcement across all sites.
- **SD-WAN Edge:** A physical or virtual appliance located at branch offices, data centers, or in the cloud. It connects the local network to the SD-WAN fabric. These devices are typically "zero-touch" provisioned, meaning they can be deployed without on-site technical expertise.
- **Private Backbone:** Cloud-native SD-WAN offers a private, global network of Points of Presence (PoP). This backbone is used to route traffic and provide a secure, low-latency connection between sites and to cloud applications, often bypassing the public internet.



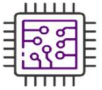
Simplified Networking

ChiefNET (on-cloud, on-prem or hybrid) solution interconnects multiple locations of your organization together to help access applications deployed on any site, HQ, DC or on cloud.



Secured Network

ChiefNET networking is secured with encryption and isolated from all other customers and Internet users. Traffic steering, local Internet breakout, industry-standard firewall and Private DNS allow organizations to keep your enterprise network isolated from unwanted traffic and intrusions.



Open & hardware Independent

ChiefNET can run on any standard hardware (x86, ARM, etc.) and virtualization platforms that can run standard Linux operating system. There are no proprietary hardware and vendor lock-in which makes it to significantly reduce the lifecycle costs of the solution. Open Architecture of the solution enables its interoperability with the existing networking solutions and thereby providing investment protection.



Scalability

With the cloud native micro services architecture, ChiefNET solution is scalable from a few devices to thousands of devices for a single enterprise. The ChiefNET VPN gateways can be launched on demand as containers in datacentres closer to your location. This enables unlimited scalability and provides lowest end-to-end latency.



Easy Provisioning

ChiefNET is easy to deploy at remote sites without requiring skilled personnel on site. With on-cloud centralized management UI, IT personnel can operate, maintain, and monitor the network with ease and security.



CPE Options

- Hardware Appliance Models
- Virtual CPE, Cloud CPE



Intelligent Routing and QoS

ChiefNET supports multiple WAN links with automatic failover and load balancing features. Traffic can be steered to specific WAN links based on different criteria such as source address, source port, destination address and destination port.

Built-in dynamic routing ensures local subnets are automatically learned over the ChiefNET instance without the need for any manual configuration.

With advanced bandwidth manager with hierarchical and fair scheduling algorithms, guaranteed bandwidth can be allocated for critical applications and fairly shared by other applications.



5G Ready

The ChiefNET solution is architected to be deployed as a service in the “5G Edge cloud” to provide secure low latency connectivity to IOT/IIOT edge devices with massive scalability to support millions of devices.

Key Features

Architecture

- Cloud native microservices based architecture
 - Massively scalable with Kubernetes
 - Pay as you go subscription model
 - Complete traffic isolation
 - Dynamic discovery of secure WAN gateways
 - High Availability (HA) on Orchestrator / Gateway and CPE
 - On-Prem deployment option
-

Security

- Built-in industry-standard firewall
 - Strong encryption of enterprise traffic
 - Private DNS, Split Horizon DNS
 - Sensitive-traffic exclusive forwarding
 - Hardened CPE
 - Integration with third-party SASE clouds
-

Routing

- Policy based traffic steering to WAN links as well as secure tunnels
 - Automatic WAN failover with configurable threshold (Packet loss, Latency & Jitter)
 - Intelligent Load-Balancing
 - Dynamic routing
 - Static route re-distribution
 - Application based routing
-

Provisioning & Management

- Cloud-based centralized management and monitoring with Web UI and dashboards
 - Zero-touch provisioning and automatic configuration
 - Mobile and Email alerts
-

QoS

- Fair Sharing of Bandwidth
 - Traffic shaping, minimum and maximum BW allocations
 - Real-time and non-real time traffic classes
 - Guaranteed BW for critical applications
-

Networking

- Policy-based traffic steering, Local Internet breakout
 - Automatic WAN link quality monitoring with failovers, fine-grained failover policies
 - Intelligent load-balancing
 - Dynamic routing
-

Security

- Strong Encryption
 - Hardened CPE
 - Strong Authentication of CPE
 - Integration with Firewalls at Edge/Cloud
 - DNS based filtering
 - URL / IP and port filtering
-

Core Networking

Interfaces	4x10/100/1000 Ethernet (2 LAN, 2 WAN default), LTE /5G (Optional)
VLAN tagging	IEEE 802.1Q VLAN tagging on all ports
Bridging for switching	Yes (as LAN or as WAN)
Routing	OSPF, Static Routes, Policy-Based Routing, BGP
WAN failover	Yes, with Link Quality Monitoring, Quality-based Failovers
WAN load balancing	Yes, with weights
Simultaneous WAN load balancing and failover	Yes
Supported devices	Physical-CPE (various models), Virtual-CPE available as VM, Cloud-CPE on all major public clouds
Device autonomous offline mode	Yes, Device need not be in contact with the Orchestrator backend all the time
Application aware networking	Application-DNS maps and Application-based traffic steering and Domain-based QoS
NAT/PAT/NAPT/DNAT	Yes
Firewall	5-tuple filters, hardened OS, no open ports, DNS security, App-group filters
SASE/SSE/ZERO-TRUST	Integration with well-known SASE vendors

Quality of Service (QoS)

QoS mechanism	Fine-grained QoS (hierarchical, fair-sharing, BW guarantees and limits)
Minimum BW guarantee	Yes
Maximum BW limit and shaping	Yes
Low latency / real-time QoS	Yes
Hierarchical QoS	Yes
Application-specific QoS	Yes, defined by domains and application grouping
5-tuple based QoS	Yes
Integration with WAN failover and load balancing	Yes
Enterprise tunnel QoS	Yes, and integrated with WAN QoS/Load Balancing/Failover mechanisms
Sensitive traffic exclusive forwarding	Yes
Maximum BW limit for a port	Yes


Security and NGFW

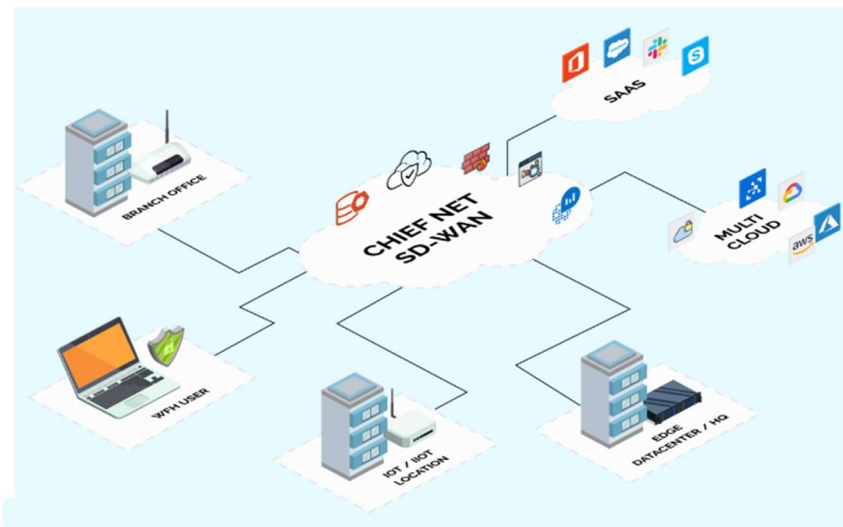
Orchestration platform	Securely accessed on cloud, or installed on-premises
Orchestrator access method	Web browser with https (http redirected to https)
Traffic isolation	Each customer's traffic is isolated from others and encrypted.
Multi-tenancy	Each customer views only own devices
CPE-Operating System	Hardened OS with long term support
CPE local access	Disabled entirely disabled for extra security to prevent unauthorized local access.
Data encryption for https/traffic	AES-256, SHA-256, SHA-512
CPE wan security	Only outbound connections (LAN to internet, LAN to enterprise) are allowed by default. All ports on wan are blocked by default. Verified with NESSUS/NMAP sweeps
DNS	Split horizon DNS allows enterprise DNS preference.
Traffic filters and NGFW-specific	5-tuple filtering, DNS-based domain filtering, application filtering

Management and Provisioning

Orchestrator access	Web-UI with https, customer admin level and read-only level, multi-tenant access
Authentication	Username/password with two-factor authentication
Network statistics packets/bytes	On Web-UI and on dashboards
Zero touch provisioning	Yes. No need for skilled personnel to install physical CPE at any site.
Full remote troubleshooting	Yes. Using ssh from ChiefNET sites after DNAT configuration on CPE.
Generic port forwarding	Yes, only after explicit configuration for accessing servers on the LAN sides of HQ / DC sites or even branch sites
Remote software upgrade	Yes
Custom dashboards, alerts, data collection	On Grafana-based portal available on-cloud or installed on-prem on customer-provided servers
Live view statistics and graphing	Yes
Reports and alerts	Custom SLA reports, WAN and device availability reports, live real-time notifications and alerts over email and SMS
Vulnerability assessment	Periodic WAN side vulnerability assessment report

Devices

Parameters / Device Models	CN-4 	CN-IOT-1	CN-VM-1	CN-Cloud-1
Hardware	Intel x86_64 COTS Appliance / 4 Core CPU / 8GB RAM / 120GB NVMe	Raspberry Pi with Custom Enclosures	x86_64 Virtual	x86_64 Virtual
Ports	4x 2.5GigE, Optional Optical ports, Optional LTE/5G/ Wi-Fi	1xGigE, Wi-Fi	4 x Virtual Ethernet	4 x Virtual Ethernet
WAN/Internet Throughput	2.5Gbps	50Mbps	1Gbps - Variable	1Gbps - Variable
WAN/VPN Throughput	800Mbps	5Mbps	200Mbps	200Mbps
Power Supply	Power Supply adapter shipped with the device (110/220V Input)		N/A	N/A
Deployment Environment	Commercial, SOHO, Residential, Retail, Industrial		Data Centers on VMWARE or KVM Platforms	Azure, GCP, Digital Ocean, AWS
Maximum Power Consumption	60W	20W	Variable	Variable
Recommended Users/Endpoints	100	5	150	150



ChiefNET Private Limited

DVP Building First Floor, No. 4, Kalapatti Main Road,
Civil Aerodrome Post, Nehru Nagar West, Coimbatore – 641014
Visit: www.chiefnet.io