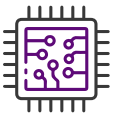
A Cloud Native SD-WAN

ChiefNET

- Overview
- Key Features
- ChiefNET Differentiators
- Technical Specifications
- Devices Specifications
- Deployment Architecture

Overview

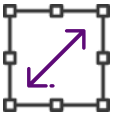


Open & hardware Independent

ChiefNET can run on any standard hardware (x86, ARM, etc.) and virtualization platforms that can run standard Linux operating system. There is 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.

Instant Provisioning

Provisioning ChiefNET solution is as easy as installing a new SIM to your phone. A CPE can be provisioned in less than 10 minutes. There is no need of any network expert at site. As soon as you connect the CPE to the Internet, the device securely connects to the Orchestration platform. The device is instantly provisioned.



Massively Scalable

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 datacenters closer to your location. This enables unlimited scalability and provides lowest end to end latency.

Secure by Design

Every customer network is an instance in the ChiefNET framework which is completely isolated from other instances and end to end encrypted. The CPEs and gateways are hardened and secured with strong authentication to prevent intrusion and MIM attacks.

Trafic can be steered to local Internet or to secure enterprise network at the CPE level or at the cloud edge. Internet gateway security can be provided by integrating with plethora of open source/commercially available security solutions at the edge or at cloud.

Intelligent Routing and QoS

ChiefNET supports multiple WAN links with automatic failover and load balancing feature. Trafic 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 the Hierarchical Fair-Service curve (HFSC) scheduler, 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 trafic isolation
- Dynamic discovery of secure WAN gateways (Future)

Provisioning & Management

- Cloud Management and Monitoring with WebUI
- Zero-touch Provisioning and Automatic Configuration
- Centralized Dashboard
- Mobile/Email Alerts
- Integration with enterprise management systems

Routing

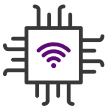
- Policy based trafic steering to WAN links as well as secure tunnels
- Automatic WAN failover
- Intelligent Load Balancing
- Dynamic routing

QoS

- Fair Sharing of Bandwidth
- Guaranteed Bandwidth to critical applications
- Trafic Shaping and Policing

Security

- Strong Encryption
- Hardened CPE
- Strong Authentication of CPE
- Integration with Firewalls at Edge/Cloud



CPE Options

- Hardware Appliance (x86)
- IoT appliance (ARM/RasperryPi)
- Virtual CPE
- Cloud (Future)

ChiefNET Differentiators

Features	Traditional SD-WAN	ChiefNET
On-Prem devices have proprietary/ closed software	• Proprietary hardware does not support customization by MSP • Proprietary/ closed software function-ality. No API support for adding custom applications	• Only flexible and core software on on-prem devices, automatic cloud managed provisioning and updates, advanced services on cloud, virtual CPE for enterprise private cloud • Supports Open standards
Warranty	• Expensive to extend hardware and software support beyond EOL periods	• Long-range support and lifecycle for products and services, replacement/ upgrade procedures
Maintenance	• Truck rolls, on-site technician visits are expensive	• Remote management, zero-touch provisioning, remote reprovisioning
Scalability	• Many SDWAN solutions have limited scalability	• With distributed micro-services architecture & Kubernetes, ChiefNet can scale to thousands of devices per network instance
Future Proof	• Many solutions are not ready for future technologies such as 5G	• With cloud native and open software centric solution, ChiefNET can easily be integrated with any future technologies • The Kubernetes based micro-services architecture makes it ideal to be deployed on 5G edge datacenters to provide massive scalability required for IoT/IIoT devices.

Technical Specifications

Architecture

Architecture	Scalability

Core Networking

Interfaces	4x10/100/1000 Ethernet (2 LAN, 2 WAN default, configurable), 4G Dongle
VLAN Tagging	802.1q VLAN Tagging in all ports
Bridge for Switching	Yes (as LAN or as WAN)
Routing	OSPF, Static Routes, Policy based routing
WAN Failover	Yes
WAN Load balancing	Yes
Simultaneous WAN LB and Failover	Yes
Supported physical devices	"CNEG-4x (Inquire for additional devices). Supported on any compatible whitebox hardware. Contact us for whitebox hardware sizing for your requirements."
Virtual Cloud CPE	Yes. Available as a VM.
Device Offline Mode	Yes
Per VPN QoS	Yes
VPN Link integration with WAN LB and Failover	Yes
Full Configuration Validation on UI	Yes
Deployment Architecture	Cloud Hub or On-Premises Hub
Deployment with an existing firewall at Branch	Integrates with existing firewall either on the LAN side or WAN side
NAT/PAT	Yes
DNAT	Yes
Firewall	Stateful firewall with IP Based and port based access control
Application Identification	Rule-based identification.
Device HA	Active/Passive*

QoS

QoS Mechanism	Full fine-grained QoS using HFSC
Minimum BW guarantee	Yes
Maximum BW limit and shaping	Yes
Low latency/real-time QoS	Yes
Hierarchical QoS	Yes
Application-specific QoS	Yes
5-tuples	Yes
Integration with WAN failover and Load balancing	Yes
Per Tunnel QoS	Yes
VPN QoS with WAN QoS/LB/Failover Integration	Yes
Sensitive Traffic Exclusive Forwarding	Yes

Security

Orchestration Platform	On a secure cloud platform.
Orchestration Access	HTTPS
Multi-tenancy	A user can view only their devices. Individuals customer's traffic is isolated
CPE OS	Hardened Linux OS
CPE Local Access	Disabled for extra security to prevent unauthorized local access
Data Encryption	AES-256
WAN Security	Only LAN to Internet, LAN to Enterprise-Cloud are allowed by default.
Firewall	• Stateful firewall with IP Based and port based access control • Enabled by default. All WAN access blocked by default.
Firewall Configuration	Through Orchestration platform (WebUI)
Next Generation Firewall Capabilities	Integration with Cloud Firewalls, DNS Security and Web Security Gateways

Management

Orchestration Method	WebUI with HTTPS, Customer Login, Isolated Device Listing
Network Statistics Dashboards	Yes
Rule based Alerts	Yes
Zero-Touch Provisioning	Yes
Full remote troubleshooting	Yes
Remote troubleshooting method	SSH with DNAT
Generic Port-forwarding	Yes
Full remote software upgrade, OS upgrade	Yes
Authentication	WebUI, 2FA
Custom dashboards, alerts, data collection	Available on our cloud visualisation portal
Live view statistics and Graphing	Yes

Devices Specifications

Parameters	CNEG-4	CNEG-VM-2	CNEG-VM-4	CNEG-IOT-1*
Hardware	–	2 vCPU/4GB	4vCPU/8GB	RasperryPi-4
Number of Ports	4 Gig Ethernet (2 LAN, 2WAN), USB for 4G Dongle	4 Virtual Ports (2LAN, 2WAN)	4 Virtual Ports (2LAN, 2WAN)	1 LAN, 1WAN, USB (4G)
WAN/Internet throughput	Upto 500Mbps (Measured with Speedtest)	500Mbps	1Gbps	50Mbps
WAN VPN Throughput	Upto 80Mbps (Measured with SpeedTest)	100Mbps	200Mbps	5Mbps
Required Power Supply on Site	90 to 270V/50Hz	N.A.	N.A.	12Vdc
Power Supply Adapter Shipped with Device	Yes	N.A.	N.A.	No
General Deployment	Commercial, Residential, Industrial, Retail	Commercial	Commercial	Industrial
Total Power Consumption	12V/5A, 60W	N.A.	N.A.	N.A.
Management	Only through the orchestration portal (WebUI). Access controlled SSH for troubleshooting. No local access for enhanced security.	Only through the orchestration portal (WebUI). Access controlled SSH for troubleshooting. No local access for enhanced security.	Only through the orchestration portal (WebUI).Access controlled SSH for troubleshooting. No local access for enhanced security.	Only through the orchestration portal (WebUI). Access controlled SSH for troubleshooting. No local access for enhanced security.
Recommended Users/Endpoints	50	75	150	5

Deployment Architecture