

ChiefNET

Solution Description



Secure WAN Connectivity, Simplified!

CONNECTING THE FUTURE

Contents

1. Introduction.....	4
2. Major Issues Addressed	5
Internet Based Enterprise Networking.....	5
Managed Internet Access Gateways	6
3. Use of Internet as the Core.....	6
Reliability and Availability and Serviceability	6
Cost and Available Bandwidth.....	7
Wireless Access with Wifi, 4G and 5G	7
ChiefNET's Use of Internet	8
4. Cloud WAN Networking.....	8
ChiefNET Subsystems.....	9
Provisioning and Management Plane	9
VPN, Traffic Encryption, and Isolation	10
Firewall and Traffic Filtering	11
Sensitive Traffic Exclusive Forwarding	11
Keeping Sensitive Traffic Private.....	12
Protecting Expensive ISP Links	12
Enterprise DNS Privacy.....	12
Application and Domain Identification	13
Traffic Steering	13
Internet Breakout.....	13
Quality of Service.....	14
5. Advantages of ChiefNET over Competitors.....	15
Open and Hardware Independent.....	15
Instant Provisioning	15
Secure By Design.....	16
Intelligent Routing and QoS	16
5G Ready	17
ChiefNET Software Security	17



Introduction

ChiefNet is a revolutionary cloud native networking solution that provides the enterprise interconnecting framework to securely connect offices, remote workers, IOT devices and datacenters in hybrid multi-cloud environment. With an innovatively architected cloud orchestration platform, ChiefNet enables completely software defined enterprise WAN for SME to large organizations.

This document describes the major problems addressed by ChiefNET. There is another document available on request for a more detailed description of the security features of the ChiefNET solution. For more information about specific features that may be in our forthcoming releases, please contact us.

The document should help in evaluating ChiefNET in its applicability to a customer's enterprise network.

Major Issues Addressed

Internet Based Enterprise Networking

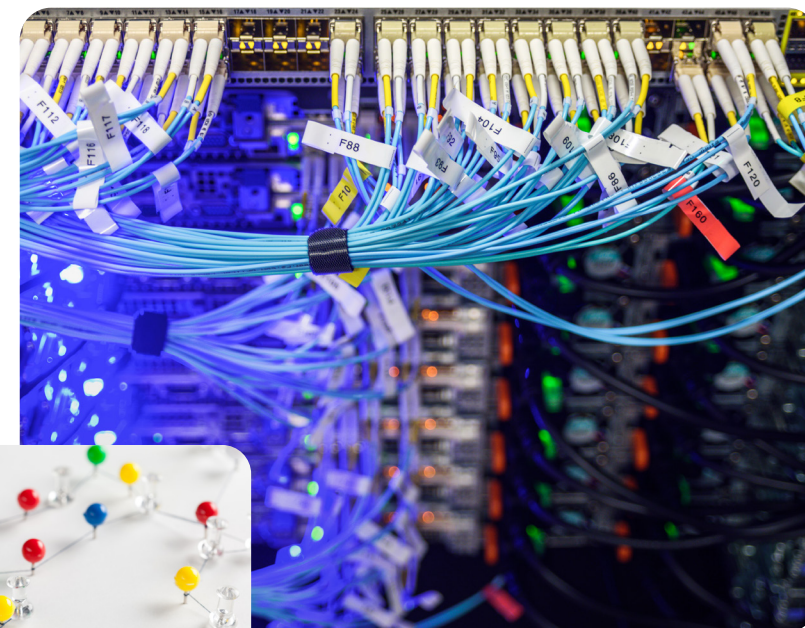
There is a proliferation of Internet-based connectivity all over the world. The concept of private networking whether it be physical (leased lines) or traditional VPNs (MPLS) are quickly being replaced with secure overlay tunnels using the Internet as the core.

With ChiefNET, it is now possible to spin up a fully functional, multi-branch, global enterprise network connectivity with no CapEx in a span of minutes. There is no need for any proprietary switches, routers any longer.

For each customer, ChiefNET enables a secure cloud-based, scalable routing functionality in the cloud. We ship a CPE device to each physical office location, whether it be a branch office, SOHO or a HQ that is pre-provisioned. For some locations such as a data-center or cloud VPC, a virtual CPE option is also available.

All the CPEs, physical or virtual, automatically connect to the ChiefNET Network Orchestrator that supports full configuration and visibility into the customer's network. It supports features such as traffic engineering, quality of service, firewall rules, VPN tunnels and routing functions that are essential for any enterprise.

ChiefNET simplifies the configuration tasks considerably with pre-selected defaults and a comprehensive set of validations that avoids misconfiguration entirely.



Managed Internet Access Gateways

For some enterprises, almost all the services are in the cloud and there is only a need for Internet Access from each physical location or a virtual location (a cloud VPC). For such customers, it is still essential to manage the edge networks to ensure seamless connectivity to the Internet with multiple links, and to ensure fairness with the use of application identification and traffic engineering.

Use of Internet as the Core

Using Internet as the core of the Enterprise offers several advantages. For one, Internet access is more ubiquitous. Secondly, Internet access costs are going down and the available bandwidth is increasing as time goes by.

Reliability and Availability and Serviceability

There is an argument that Internet is generally considered as unreliable. However this viewpoint is changing quickly and its reliability is just as much as the traditional networking technologies such as physical leased lines and MPLS-VPNs.

Connections such as physical leased lines and MPLS VPNs have a huge serviceability disadvantage. When such networks are stable, they stay very reliable. However, should anything go wrong, the downtime is in multiple days. The lack of expertise available to diagnose the problem and provide solutions or alternate paths is the main cause.

On the other hand, any issues with Internet access are more readily and quickly diagnosed, isolated, and fixed by the operators. The reason is that Internet connectivity and the global routing exchanges are maintained with utmost reliability as the public, the governments, private enterprises, healthcare solutions, social networks, office solutions, industrial IoT, people, home and city automation sensors and machines in every walk of life depend on the Internet. Internet Service Providers have begun to offer service level guarantees even to the residential users.

Cost and Available Bandwidth

Internet access is getting cheaper and cheaper as time goes by as the entire world moves to the use of Internet, both for personal as well as commercial networking purposes.

The available bandwidth is also increasing day by day as the users demand more. While traditional enterprise networks require deployment of custom hardware with custom routing/MPLS-VPN software, those technologies come with very high cost on a per-port basis and per unit of bandwidth. The costs quickly multiple for the providers which are then passed on to the customers. This is a limiting architecture and does not take advantage of the ever-increasing capabilities of basic and core Internet access.



Wireless Access with Wifi, 4G and 5G

A huge advantage of using the Internet is the availability of wireless technologies that are not available with traditional enterprise networking technologies such as physical leased lines and

Wireless connectivity makes it simpler to roll out new locations for your enterprise. Such locations may include physically distant locations where wired connection is not feasible.

For some use cases such as Industrial IoT, City and Home Automation IoT, it is only feasible to offer wireless solutions both on the LAN as well as on the WAN.

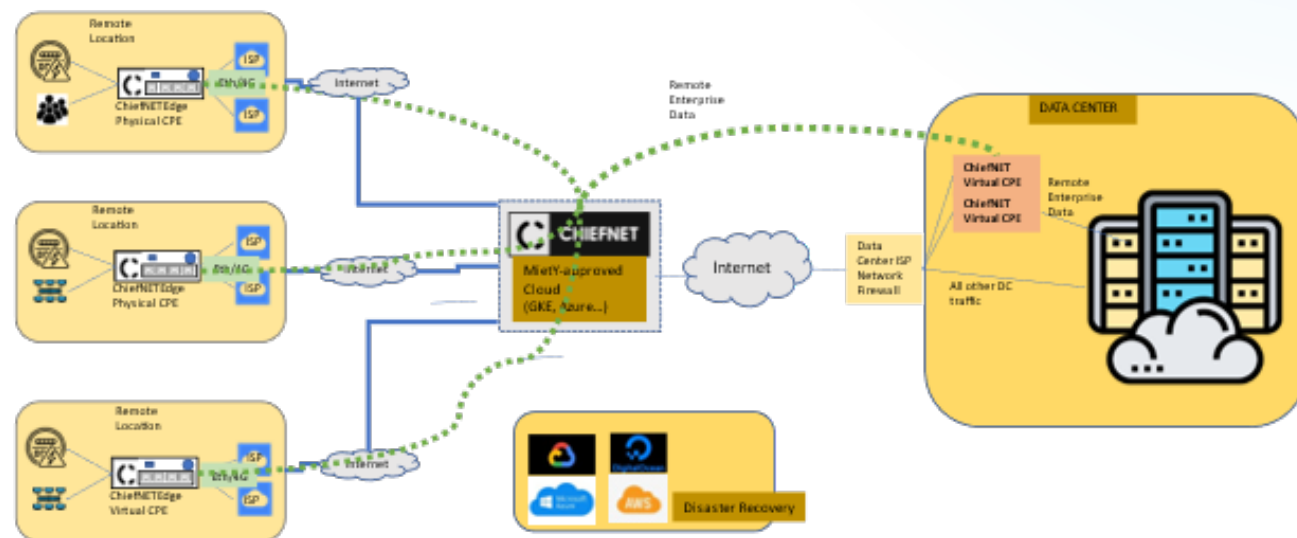
ChiefNET's Use of Internet

ChiefNET takes all such emerging requirements and provides a comprehensive networking solution utilizing Internet. It is also compatible with existing private leased lines as well as MPLS networks as they stay transparent to the ChiefNET deployments.

The end-users at the remote locations and the data centers can be individual users, IOT devices or servers

Cloud WAN Networking

The following figure illustrates a primary use case of ChiefNET.



This use-case connects multiple locations together using the Internet as the core transport. This eliminates the need for deploying or using leased lines or MPLS trunks.

Internet Breakout feature supports both Enterprise Connectivity using secure tunnels as well as Internet Connectivity for non-Enterprise traffic. It is also possible to forward the selected traffic to the cloud-WAN over a VPN.

The CPE can be physical or virtual, at various scales.

The virtual-CPE can be deployed in your cloud VPCs as well so that the VPC acts as an edge location.

ChiefNET Subsystems

ChiefNET consists of various servers and devices in the following three categories.

	Architectural Subsystem	Description
1	Provisioning and Management Plane	These are servers that run in the cloud and are accessible through secure HTTPS protocol on browsers.
2	Cloud-Based WAN VPN and Routing	The devices at various edge locations connect to the cloud-based WAN routers using secure VPN tunnels.
3	CPE (physical and virtual)	Physical CPE devices or Virtual CPE OS distributions are placed at the edge locations that support customer's devices and networks at the edge

Each subsystem has been designed and implemented with security in the focus from the design stage.

Provisioning and Management Plane

When a customer requests a ChiefNET service, we ship them a physical CPE or a virtual CPE. The virtual-CPE option is preferable for locations such as a data center or a cloud VPC, where deploying a physical CPE may not be feasible and where a virtualization solution is available.

The CPE is pre-provisioned in the factory for that customer. The user needs to

- Connect power to the device, if it is a physical CPE, (or in the case of a virtual CPE set up a virtual machine on host platforms such as VMWare)
- Connect the WAN port to the Internet Service Provider
- Connect the LAN ports

No local configuration is necessary. The device automatically connects to the ChiefNET orchestrator. The customer can access the WebUI and visualize the network, view and configure the devices.

VPN profiles are created in advance for each customer and the device may be configured to connect to the VPN profile.

All configuration and monitoring are performed with https access using a web browser. The backend server and the database are positioned on a cloud compute instance. The database and the backend servers are not directly accessible by the end-users. The only means of configuring/managing the devices and the networks is using the browser.

All data exchange for configuration, monitoring and troubleshooting are secured with public key cryptography.



VPN, Traffic Encryption, and Isolation

Each customer's traffic is entirely isolated from others, both at the management level as well as the data level.

All enterprise traffic that is forwarded over the VPN tunnels is encrypted with AES algorithms. With Internet breakout/Traffic Steering feature set, the customer may configure the rules for classification of traffic into critical/enterprise-class to be forwarded over secure tunnels.



Firewall and Traffic Filtering

A stateful-firewall is nowadays a universal feature supported in all edge gateways. ChiefNET supports it as well. This feature is almost a given and required with the use of NAT/PAT/Masquerading features that are commonly supported in all gateway devices from any vendor.

In addition, additional filters may be configured using source IP, destination IP, source TCP/UDP ports, and destination TCP/UDP ports to discard specific classes of traffic. Instead of specifying 'destination IP addresses', one may also specify entire domain names in the traffic filter.

Only LAN-Internet and LAN-Enterprise are connected by default. All traffic from WAN to LAN, from WAN to Enterprise are disabled and security holes removed.

We periodically run security probes on all our subsystems to ensure that there are no open ports or other such unknown security holes.

Sensitive Traffic Exclusive Forwarding

ChiefNET supports features such as traffic failover and load-balancing so that the impact of WAN link failures is minimized by traffic redirection appropriately. However, there is a case where traffic must be forwarded on certain WAN/VPN links only, and not on untrusted links. This may include certain DNS traffic that must be forwarded to the Enterprise

network, and not to the general Internet. The actual concerns may be one of confidentiality or privacy. In any case, this feature may be configured with fine-grained or loose-grained traffic classification on ChiefNET.

There are two example use cases of this feature.

Keeping Sensitive Traffic Private

In this use case, one may choose to forward IoT data specifically only over a specific WAN link that is considered reliable. If there are unreliable links, for instance, they may go through data centers or peering points not allowed by regulation, such sensitive traffic should not be forwarded.

Protecting Expensive ISP Links

It is possible to use this case to discard unimportant traffic from utilizing your expensive Internet connection too. For instance, one might not want the use of a 4G/LTE connection for regular browsing traffic such as Netflix or Youtube from the edge locations, whereas they might be acceptable for the wired ISP links that do not have data limits or have higher bandwidths.

Enterprise DNS Privacy

ChiefNET supports split-horizon DNS with which it is possible to configure DNS servers for specific domains. A typical use case is to configure the Enterprise' own DNS servers for their domains even if the remote devices are connected to the Internet. This prevents private DNS information from getting leaked to the Internet.

As an example, a CPE may be configured to get the public DNS from an Internet service provider. It is also possible to configure a static, well-known public DNS server such as those from Google or Cloudflare.

Apart from those, it is possible to configure domain-specific DNS servers. As an example, if your enterprise is "ravi-insurance.com" with its DNS servers, the CPE will only contact those DNS servers for hosts in your enterprise. That prevents the leakage of host-sensitive information to the public Internet.

Application and Domain Identification

ChiefNET statistically samples the traffic and identifies the applications and the domains accessed by the customer's endpoint devices. This helps the operator to identify the top users and create firewall policies.

Traffic Steering

This is one of the key and distinguishing feature of ChiefNET. Traffic Steering refers to the use of multiple WAN links for fine-tuning how your application traffic is forwarded.

It is possible to specify rules in a 5-tuple format and specify which WAN ports they should be forwarded to. For instance, most traffic is forwarded in a load-balanced manner among all WAN links. It is also possible to specifically choose the order of the WAN links, if prioritized forwarding is to be done.

By configuring a weight parameter, it is possible to choose how much of the application traffic should be forwarded on each WAN link. The weight parameter may vary on a per-application basis.

Internet Breakout

This is another key and distinguishing feature of ChiefNET related to traffic steering. Internet Breakout refers to selecting non-Enterprise traffic and forwarding those directly over the Internet, instead of the VPN tunnel. This also prevents unwanted security attacks from internal sources.

There are many use cases for this feature. For instance, if certain application traffic is not considered important to the enterprise, they may be forwarded directly over the Internet without having to reach other branch offices or HQ/DC/Cloud presence of the enterprise.

In another use case, if the users try to access cloud-based third-party services such as Microsoft Office 365 or Google Workplace or Zoho, they do not need to go through the Enterprise VPN network. This is however configurable by the policies adopted by the enterprise.

Quality of Service

ChiefNET supports fine-grained quality of service. The operator can configure QoS profiles in simple parameters such as average bandwidth or in more advanced concepts such as delay and jitter parameters. These profiles may be allocated to all the traffic from the edge as a whole, or for fine-grained 5-tuple traffic rules. It is possible to specify minimum bandwidth as well as maximum bandwidth for any application rule.

As an example, the user may wish to limit the bandwidths of certain domains such as Facebook/ Twitter to just 10Mbps, whereas a minimum bandwidth guarantee may be provided for Microsoft Office 365. In this example, availability of Office 365 is ensured and the potential impact of social networking traffic is limited.



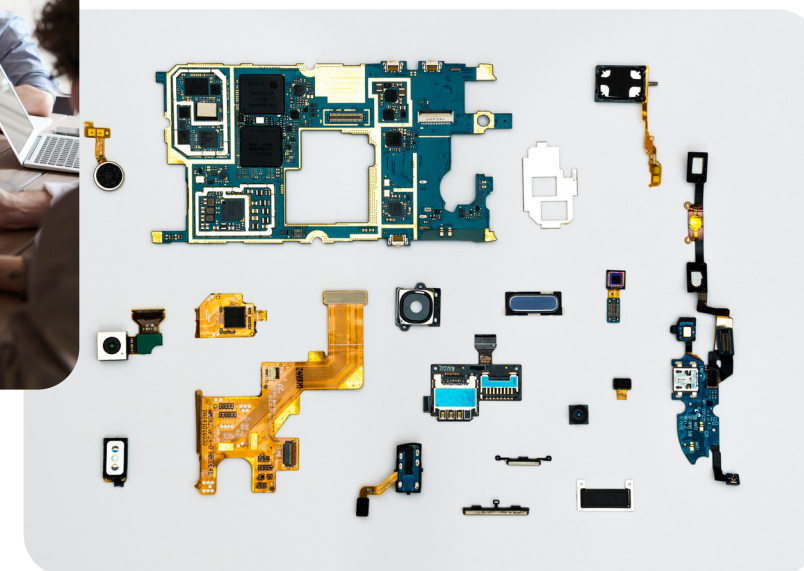
Advantages of ChiefNET over Competitors

Open and Hardware Independent

ChiefNet runs 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.

The devices in a deployment do not all need to be the same. They can vary and can have their own performance needs met.

Virtual-CPE availability also protects the customer deployments from any hardware specificity and dependency.



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.

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.

Traffic 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. 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 the Hierarchical Fair-Service curve (HFSC) scheduler, guaranteed bandwidth can be allocated for critical applications and fairly shared by other applications.



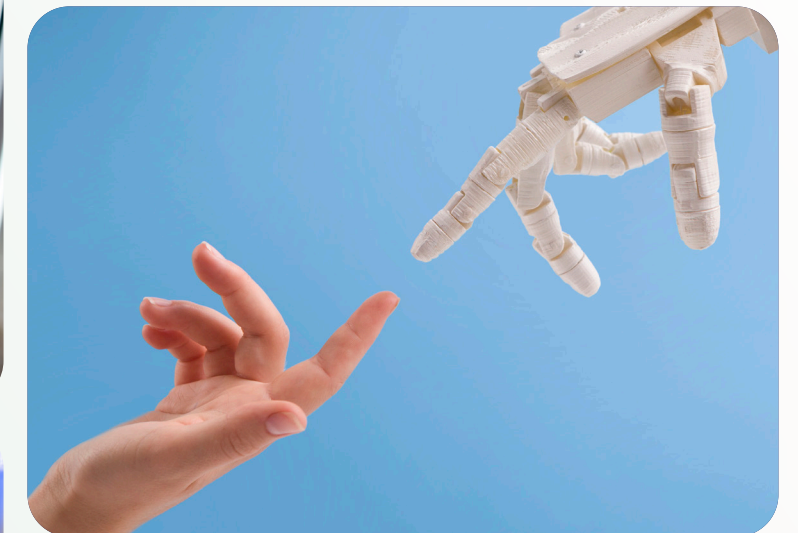
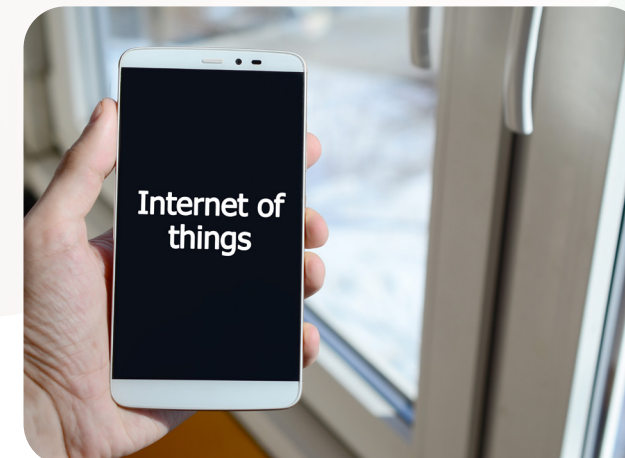
5G Ready


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.

ChiefNET Software Security

ChiefNET software is based on standard Linux operating systems that are latest and hardened. They are upgradable from the Orchestrator to keep up to date with the patches. The devices never need manual access for any purpose once deployed.

We also continuously upgrade the OS and the ChiefNET software on the cloud so that security threats are avoided.





Connecting the future



4th Floor, N Towers,
25, Tex Park Road, Nehru Nagar West,
Coimbatore Aerodrome(P.O),
PIN 641014

contact@chiefnet.io

www.chiefnet.io

