ChiefNET

Overview and Security Features

Secure WAN Connectivity, Simplified!

Secure WAN Connectivity, Simplified!

Secure WAN Connectivity, Simplified!

Secure WAN Connectivity, Simplified!

Contents

Introduction

ChiefNET is characterized as a **secure networking infrastructure focused on interconnecting remote offices**, HQ locations, colocated data centers and public cloud locations in a secure, flexible and managed from the cloud.

This document describes some of the security features supported by ChiefNET. There is a focus here more about the details of the security features that are already supported. 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.

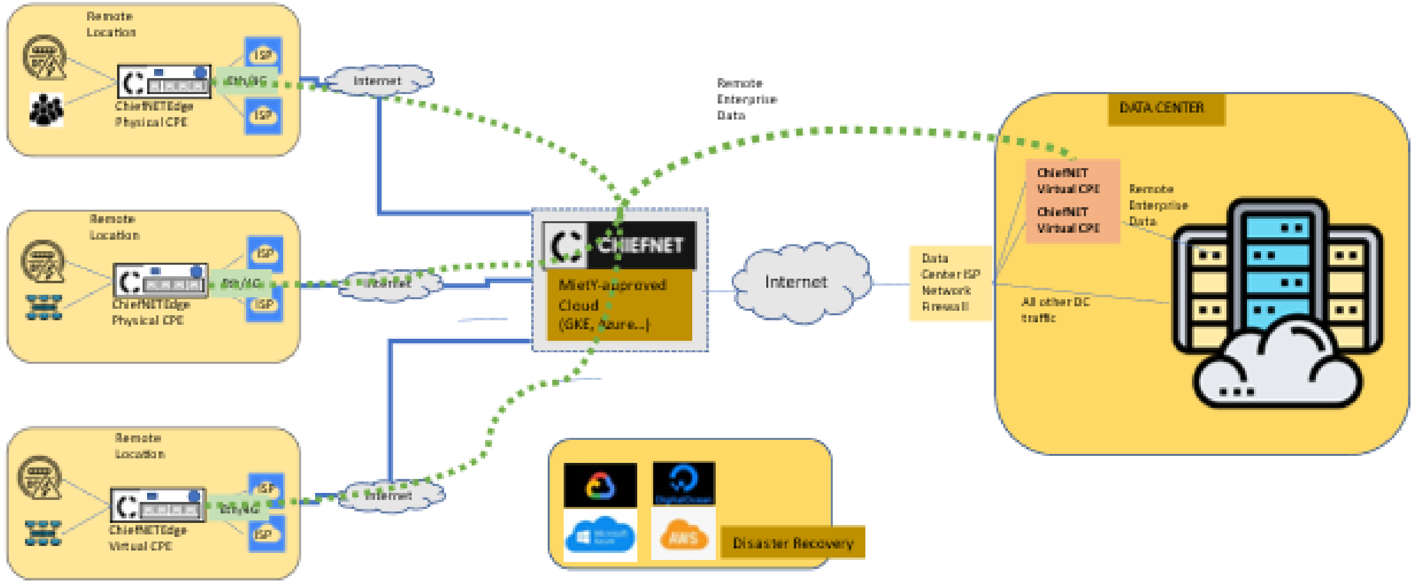
Primary Use Cases

There are **two primary use-cases** that we are focused on.

Cloud WAN Networking

Teleworking and Edge Gateway Fleets (CPE)

ChiefNET Enterprise Networking Topology



Cloud WAN Networking

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 all of selected traffic to the cloud-WAN over a VPN.

Teleworking and Edge Gateway Fleets (CPE)

This use case connects remote edge locations to the Internet, whether for SOHO, Residential or Branch offices, HQ offices to the Internet, with a central management framework for setting up network access and usage policies.

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.

There are other use-cases as well but the above two use-cases provide an insight into the various capabilities of the full ChiefNET solution.

All the use-cases, including the two primary ones mentioned above, have been designed with security and ease-of-use in mind from product inception.

ChiefNET's Cloud-WAN concept is unique and is inclusive of the features of the centrally managed fleets of remote edge gateways. It distinguishes ChiefNET from other networking solutions.

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

ChiefNET Components

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

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.

Access Control

A user would be able to view only their own organization's devices and network. Two levels of access control are supported for each user account.

Administrator   Read-Only

User accounts with an administrator level privilege may add or configure additional user accounts. All access is authenticated using a two-factor authentication mechanism.

Unauthorized access to the CPE device is disabled. All configuration and monitoring are done only using WebUI available over the Internet. All CPE, whether physical or virtual, are pre-provisioned. Once they are powered up and connected to the Internet, they register with the central orchestrator. All configurations may be done whether the device is online or offline in advance or during operation.

Security Hardened CPE

ChiefNET CPE is hardened against all known threats with a secure OS installation. There are no backdoors or unauthorized access.

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.

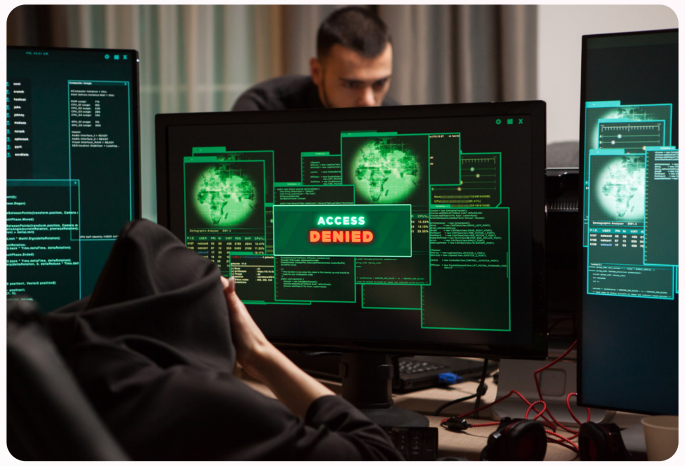
All enterprise traffic that is forwarded over the VPN tunnels is encrypted with AES algorithms. With Internet breakout/Traffic Steering feature set, the customer may configure the rules for classification of traffic into critical/enterprise-class to be forwarded over secure tunnels.

All CPE devices that use the secure tunnels are authenticated using X.509 certificates unique to a deployment.

Customer Traffic Privacy

All customer traffic is private and secure. ChiefNET does not peek into customer's traffic, nor does it allow any other third-party as all Enterprise traffic is encrypted and decrypted with dynamically negotiated keys with a public key authentication mechanism widely adopted in the industry.

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.

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.

Enterprise DNS Privacy

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.

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.

Deployment and Supply Chain Protection

ChiefNET deployments at a customer site are not bound to a specific hardware. Our hardware is chosen among multiple vendors and can be varied over time, keeping the software features identical. There are many benefits to such an architecture.

Hardware platform is not a specific one. Any of the available platforms can be used should there be any issues in the supply chain.

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.

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.

ChiefNET Software Security (Cont..)

ChiefNET does not use any custom operating system. We use standard open-source Ubuntu OS as our core. This makes it safe because security threats if any are identified and patched immediately.

Features Not Supported by ChiefNET

It is important to know the features that ChiefNET does not support in the current release, though they are included in our product roadmap.

- Deep packet inspection, unified threat monitoring
- TLS/SSL Inspection
- Anti-virus, Email-scanning, URL filtering

In the past, by default all traffic was allowed, and explicit filters were configured to discard malicious/suspected traffic. However, these days, including ChiefNET, all traffic is discarded by default, and only those that are known to be safe are allowed.

While DPI features are useful in some scenarios, those are best deployed in the cloud, and not at the edge as they require a lot of compute-power to be truly effective.

For customers that need such content-based filtering features, the recommended solution is to funnel the Internet-bound traffic over VPN to the cloud and deploy a cloud-firewall solution through one of the cloud-partners. Our partners and resellers can help with such a network design with ease, should such a requirement arise.

ChiefNET

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

www.chiefnet.io