TrustLeap
Global-WAN

Executive Summary

Cyberspace – the Internet – is now the most critical infrastructure of modern societies. Finance, energy, water, telecoms, transportation, logistics, and governments rely on it. Economic and social stability depend on these interconnected networks. One single destructive act can cost several billions of dollars and disrupt the most advanced societies. The Economist calls today's network monitoring and cyber security a *"market failure"*[1]. The Internet of Things (IoT) will make it a cataclysm.

It's not an easy problem to resolve – either from a political, technical, or financial point of view.

TWD's decade of government-audited expertise in "post-quantum" and "unconditional" security helped to create a unique breakthrough: for the first time in cyber ***Defense is cheaper than Offense***.

This lets TWD partner with critical infrastructure operators to deploy ubiquitous ***future-proof*** security profitably rather than as at a cost. TWD generates new profits while cutting costs and liabilities.

What is Global-WAN?

Vendors and consumers can plug Global-WAN[2] ASIC microchips in their devices to secure datacenters, corporate networks, network appliances, mobile and embedded systems, the IoT, and even RFID tags.

Global-WAN *provably-secures* public (wired or wireless) networks. This is a distributed Level-2 VPN platform relying on mathematically provably-safe "post-quantum" security.

> "Post-quantum" security aims at *"resisting unlimited computing power"*. Its effective security relies on assumptions such as the lack of known tools and methods able to compromise it.
>
> In contrast, Global-WAN "provably-safe" post-quantum encryption relies on a mathematical demonstration that guaranties its security. Its strength is well-understood and independent from future scientific discoveries or technological progress.

Global-WAN scales seamlessly on RFID tags (logistics, passports, cashless wallets, shop price tags, etc.), smartphones, connected cars, as well as on high-performance servers and datacenter gateways.

As a "zero-configuration" VPN Global-WAN makes remote hosts appear on networks just like if they had always been there. Users chose *when* this is happening and *what* services are available to *whom*.

Global-WAN lets you share what you want (and nothing more) with the people of your choice (and nobody else): it excludes *anonymous* denial of service (DoS) attacks and hacking attempts, by-design.

[1] The Economist, *"Market failures - Not my problem"* (July 2014)
[2] Global-WAN website: http://global-wan.com/

With Global-WAN salesmen can reach corporate resources from abroad, Government Officials can communicate freely – *all online services can safely be deployed globally*.

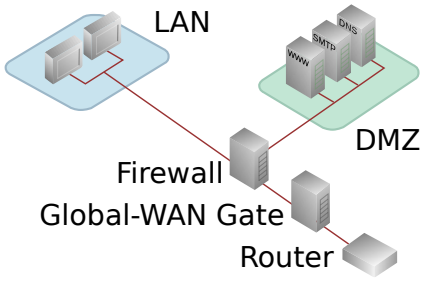
Each user needs to use a Global-WAN Gate to securely communicate:

TrustLeap's mission is to help vendors provide a wide range of Global-WAN Gates to cover every possible needs, including mobile devices, embedded systems, modems and network adapters.

Since Global-WAN executes on self-sufficient hardware, it *transparently* protects every device, operating systems, and applications (whatever the vendor) without having to change anything:

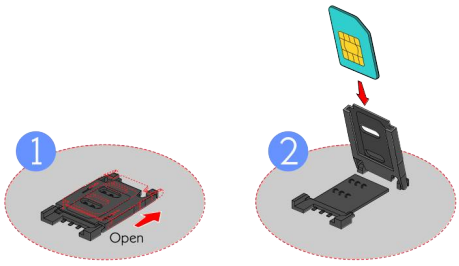
Global-WAN as a Compliant Platform

Global-WAN was first implemented on network appliances with ample CPU and storage capabilities. While suitable for the Corporate environment, this ”heavy” form-factor and pure peer-to-peer topology limited its deployment (costs per unit), applications (unsuitability of bulky equipment for mobile users), as well as the compliance required for regulated users (banks).



> To foster Global-WAN's market penetration, **ASIC microchips** were mandatory to both (a) isolate Global-WAN's *provably-secure* cryptographic capabilities, (b) expand the reach of Global-WAN to the IoT ecosystem (low-power consumption, small-factor, cheap deployment costs), and (c) make it suitable for regulated users.

The VHDL design and these ASIC chips can be inserted everywhere (SIM cards, SD cards, UMTS modems, network adapters, micro-controllers, CPUs...) to let Global-WAN reach mobile users and the IoT world (smartphones, automation, FINtech, healthcare, video surveillance, etc.).



This versatility lets Global-WAN push and mix third-party Cloud services in a Cloud-hosted back-office as well as protect communications and endpoints.

Preserved Provably-Safe Security

As database records are protected with each end-user's encryption key, there's no way for Cloud infrastructure operators (or unwanted exterior influence) to interfere with Global-WAN operations: only duly Global-WAN authorized users can use Global-WAN's *provably-secure* administration Console to safely manage it from anywhere on the Planet (cf. *"Global-WAN User's Manual"*):

From this Web Console, consumers can remotely manage their own Gates and enterprises can administer their WAN. Both can provision users and Gates, define credentials and policies, download log files, as well as use SQL requests to extract statistics and generate usage and incident reports.

Never before such *remote administration* capabilities have been made *provably-secure*.

> This technology makes it possible to finally reconcile three traditionally opposed goals:
>
> 1. protecting consumers, enterprise and the critical infrastructure from criminals,
> 2. securing regulated access for duly authorized regulated users – and only them,
> 3. provably securing the IoT world to prevent it from turning into a global disaster.
>
> Global-WAN delivers a much-needed technically-proven and financially-sound solution.

"If provably-unbreakable security is available then it is irresponsible to use anything else."