# CASE STUDY
# TRUEGEN

TrueGEN is a dynamic company specialized in IT Network Security. Our portfolio combines mature technologies with cutting-edge solutions. As every company has different needs and desires, TrueGEN believes that the secret of a dynamic and secure future can be found in the customized delivery of solutions, support and services. After immersing ourselves in the customer environment and examining the current state of the network, we design a futureproof architecture based on the customers' needs and best practices.

TrueGEN
securing your network

## Challenge

Today's Wide Area Networks (WAN) were made possible by Multiprotocol Label Switching (MPLS), a data-carrying technique relying on forwarding and routing between multiple network routers to connect geographically dispersed sites within a same network. It's a robust, time-tested solution that, on paper, is impervious to attacks. But, since the client doesn't own the routes where the data transits, it has no way of knowing who could be listening in. To top it all off, MPLS is among the very least flexible connectivity solutions on the market today.

TrueGEN has many security conscious customers who understand that private networks such as MPLS do not provide security, as they lack visibility over how and where their traffic is routed. This exposes organizations to potential information leaks, among other threats.

Another threat to network connectivity is the rigidity of private networks. Because they're so robust, setting up failover mechanisms can prove tricky.

Already a provider and integrator of multiple security solutions such as firewalls, TrueGEN was looking for an additional level of sophistication in terms of network uptime and encryption. They were looking for a single solution that could keep their clients both online and safe.

> "Connectivity failure for our customers' offices, datacenter and remote connections to third parties or remote workers caused severe business damage."

MARTELLO | Powering Network Performance

# Solutions

One of the most popular ways to add security to the WAN is to set up encrypted Virtual Private Network (VPN) tunnels between sites, allowing users to transfer data and access sensitive information, mitigating the risks of data leakage. But that approach doesn't address the business continuity angle: when a circuit is down, what then?

Firewalls provided part of the solution. Most Next-Generation Firewalls are equipped with VPN engines capable of creating encrypted tunnels, and are also capable of performing basic active-passive failover between a limited number of ISP routers. Should one router go down, the traffic will eventually be redirected to the secondary one. The limitation here is in terms of failover speed and flexibility. Even with two circuits, customers can only use one at the time, and will inevitably suffer up to minutes of downtime while the traffic is being redirected.

"Our customers were looking for transparent multi-site connectivity with seamless failover and fallback mechanisms. Flexible and stable public and private connectivity are essential for business continuity."

# Working with Martello

TrueGEN started working with Elfiq Networks, now a subsidiary of Martello, to offer its customers a business continuity solution that would mitigate the failover delay encountered with firewalls. The Elfiq LBX edge appliances were capable of managing and optimizing multiple ISP circuits concurrently, completely mitigating the failover delay encountered with Firewalls. By continuously monitoring link health, the devices are capable of identifying the best possible path at any given moment, and to redirect traffic in real time, avoiding any downtime.

There are several instances where TrueGEN assisted multi-site customers in Europe to migrate from one MPLS provider to another. Even as the original circuit went down, the customer still experienced good connectivity, as though nothing had happened.

Moving into SD-WAN was only a short step away. The Elfiq Operating System is capable of emulating a Wide Area Network by creating VPN tunnels over public and private circuits alike. By communicating with each other and sharing information with Central, the company's centralized orchestrator, the edge appliances can create a web of secured paths. In recent years, Elfiq Networks further developed a new VPN approach, STREAM VPN, encrypting traffic per flow instead of maintaining tunnels open at all times, freeing up processing power and bandwidth for the business critical traffic that matters.

To top it all off, Elfiq Networks' Layer-2 approach makes it completely agnostic to existing Firewalls, requiring no reconfiguration in that regard. For TrueGEN, an IT security provider, this represents a considerable advantage.

"As a networking and security company, TrueGEN investigated several ISP balancing and SD-WAN solutions. Martello's Elfiq provided the best and most stable results, and created new possibilities which allow even more flexibility to our customer's network."

## Potential

From the onset, TrueGEN has been capable of deploying Elfiq SD-WAN technology on its own, relying only on support when encountering new scenarios. Adding Martello's fault & performance management capabilities, TrueGEN now has deeper visibility into their customers' network, with the capacity to monitor and inspect the health of individual components, and to prioritize traffic by application.

### About Martello

Founded in 2009, Martello Technologies is headquartered in Ottawa, Canada with staff in Canada, the United States and France. In January of 2018, Martello merged with SD-WAN player Elfiq Networks to offer a solution that pairs performance management software with SD-WAN technology to provide stellar UC performance. Martello's solutions deliver confidence in the performance of real-time services on cloud and enterprise networks and is a proven provider of performance management software for Mitel customers.