CASE STUDY

New VPN Teleworking Solution Brings Big Gains To Iceland's Leading IT Services Provider During COVID-19 Lockdown

With a long and reputable history dating back to the birth of computing itself, Origo, whose name derives from the Latin for "origin," has grown to become one of the most influential forces behind Iceland's digital revolution.

Combining the skills and ingenuity of its 450 IT specialists with a broad portfolio of business solutions including managed services, software development, and IT infrastructure, Origo now serves around 30% of the country's entire workforce through its broad customer base.

Rising To the Challenge of COVID-19

For a company so dependent on the innovative collaboration of its staff, Iceland's laudably swift response to the COVID-19 pandemic exposed significant weakness in Origo's existing IT infrastructure. Most notably, when demand for secure remote access exploded from around 20 users a day to over 1,000 users a day, the company's pre-existing virtual private network (VPN) solution quickly proved woefully inadequate.

"Our previous VPN solution had been both troublesome and unstable," explains Arnar Gunnarsson, CTO at Origo. "That was a major concern when COVID-19 forced the majority of our employees to start working from home."

Facing growing frustration from the company's internal staff, not to mention its thousands of external users, Origo needed a new solution fast.

As a current customer and partner of Fortinet, Origo had already planned to test how effectively their existing FortiGate next-generation firewalls (NGFWs) could take on the additional load of VPN tunnel termination—a function previously performed by a dedicated third-party solution. But with help-desk workloads already up some 30% to 40% since the onset of the COVID-19 lockdown, Origo's IT team decided to reprioritize this initiative with immediate effect and deploy FortiClient advanced endpoint protection with its integrated VPN capability.

Integrated Access Security Through a Single, Modular Lightweight Client

FortiClient supports both secure sockets layer (SSL) and Internet Protocol security (IPsec) VPN to provide secure, reliable access to corporate networks and applications from

"Our previous VPN solution had been both troublesome and unstable. That was a major concern when COVID-19 forced the majority of our employees to start working from home."

– *Arnar Gunnarsson, CTO, Origo*

Details

Customer: Origo

Industry: MSSP/Service Provider

Location: Iceland

Business Impact

- Increased employee satisfaction and productivity rapidly during the COVID-19 pandemic
- Improved security of remote access through integrated threat protection and two-factor authentication
- Boosted productivity and effectiveness of the IT Team, allowing them to switch focus from staff to external customers

virtually any internet-connected remote location. Regardless of which VPN technology is used by an individual remote user, the tunnel is terminated in the FortiGate NGFW. The firewall's purpose-built security processing unit (SPU) helps to ensure that performing threat protection at the VPN headend does not compromise user experience when numerous remote clients connect.

Following some simple reconfiguration and remote deployment through the FortiManager central management console, Origo emailed instructions to all staff on how to complete the switch to FortiClient VPN for their remote access.

Within just six days, 57% of employees had already moved over to the Fortinet solution with little or no assistance required from the IT team. Two days later, the number was 70%, but more importantly, satisfaction and productivity had skyrocketed. Users were now able to take full advantage of very high-speed broadband, enjoying speeds of up to 1 Gbps from their homes (an experience not too dissimilar from their office-based connectivity) and the volume of help-desk cases had dropped to levels even lower than those of pre-lockdown.

Increased Connection Security and 2FA

By bringing remote access within the sphere of protection of the Fortinet Security Fabric, Origo had already increased control and visibility over their remote access connections, allowing the IT team to tighten security policy compliance as well as track and analyze incoming threats in ways that had not previously been possible.

In early April, for additional protection, Origo subsequently added two-factor authentication (2FA) through the addition of FortiToken Mobile and FortiAuthenticator. FortiToken Mobile, a smartphone application available for both Android and iOS devices, makes use of the unique token provisioning service of FortiGuard. FortiToken Mobile generates a secure one-time passcode every 60 seconds to verify user identity. The code is authenticated by FortiAuthenticator user identity management appliances. FortiAuthenticator further strengthens access security by simplifying and centralizing the management and storage of user identity information.

Solutions

- FortiGate
- FortiClient
- FortiAuthenticator
- FortiToken
- FortiManager

"The rollout of FortiClient for VPNs has solved both our performance and security challenges. But most importantly, our employees are satisfied since they can now be as productive working from home as they were in the office."

– *Gunnlaugur Th. Einarsson, CIO, Origo*

Once again, the deployment was completed in just a few days and with no apparent disruption to user productivity.

"The rollout of FortiClient for VPNs has solved both our performance and security challenges," observes Gunnlaugur Th. Einarsson, CIO, Origo. "But most importantly, our employees are satisfied since they can now be as productive working from home as they were in the office."

FORTINET

www.fortinet.com

October 31, 2020 1:40 PM

796292-0-0-EN

D:\Fortinet\Case Study\Purple Case Study\Origo\cs-FA-new-vpn-teleworking-solution-brings-big-gains-to-iceland-10152020