CASE STUDY

Security Fabric Solutions Create Work-from-Home Options Quickly

As COVID-19 grew into a pandemic, IT teams at global security leader Fortinet began to prepare. Like businesses around the world, Fortinet needed to enable almost every employee to work from home. Fortinet's Europe, Middle East, and Africa (EMEA) division leveraged firewalls, client solutions, and other security technologies they already owned. They had to change some configurations on the security solutions, and they optimized FortiVoice phone systems to give remote employees extended telephony capabilities by using a softclient on their computers. As a result of these efforts, they expanded their virtual private network (VPN) capacity to serve three times as many concurrent users as they served previously, in a way that IT staff can secure from their own home offices.

The Sudden Onset of Work-from-Home

Among its many effects, the COVID-19 pandemic has forced businesses to immediately enable employees to work from home wherever possible—both for their own safety and to reduce community spread of the virus. IT teams enabling this transition do not have the luxury of time. Their typical months-long planning processes for major technology rollouts are taking a back seat to pressing business needs. At the same time, connections must be secure, because cyberattackers are as busy as ever; physical distancing measures are not slowing their malicious activities. IT groups that can leverage existing security solutions are well-positioned to facilitate new work-from-home policies without sacrificing the protection of their users, applications, and data.

This is the approach taken by the EMEA division of Fortinet. The group already supported remote users, reports IT Manager Cyrille Carrasco, but most employees worked in one of the offices across Europe. "Our business unit has 1,600 employees," Carrasco says. "Previously, about 600 of them were remote workers. When COVID-19 hit, we needed to make that option available to everyone."

He continues: "Employees need access to file servers, application servers, and other back-office resources, as well as to our laboratory devices for use in testing and in proofs of concept. These resources are not available via the internet, and for many employees, this was their first experience of working remotely."

Even more daunting, staff across Europe need access to their Fortinet phones. "This is important for all employees, but particularly for workers in our call center," Carrasco says. "They answer between 40,000 and 50,000 calls each month. They are used to working in one large location, and to move these workers home, we needed to provide remote access to our phone system."

Rick Huang, Fortinet's senior director of IT for the United States and Asia-Pacific (APAC), reports that the EMEA group's experience reflects the circumstances of entities across Fortinet. "In the United States, we are in the same situation, just on a larger scale," he says.

"Without this security infrastructure, I cannot imagine giving all our employees home access to the valuable resources located in Fortinet EMEA offices."

– Cyrille Carrasco,
IT Manager, Fortinet

Details

Customer: Fortinet

Industry: Technology

Location: Sunnyvale, CA

Business Impact

- Enables 99% of employees to be productive from the safety of their homes
- Provides threat protection on par with on-premises network security
- Enables call center employees to continue answering up to 50,000 customer calls each month, from their homes
- Streamlines network security management for homebound IT staff

Preparing for Widescale Rollout of SSL VPN

The Fortinet EMEA group was already using FortiGate next-generation firewalls (NGFWs) to give remote users VPN access to the corporate network. They were using secure sockets layer (SSL) VPNs because some remote users had previously experienced challenges with IPsec, particularly when they tried to connect from customer offices. "SSL VPN tunnels are better handled by firewalls, so they make VPNs easier to establish and more reliable," Carrasco explains. "For years, SSL VPN has allowed us to establish connections from anywhere in the world without any trouble." In addition, company-issued laptops were already running the FortiClient Secure Fabric Agent prior to the pandemic.

The company had in place the basic technology needed to enable widespread work-from-home policies, but Carrasco still had concerns about expanding capacity so dramatically and so quickly. "Just before European governments decided 'nonessential' workers should not leave our homes for work, our IT group anticipated that this type of confinement was coming," Carrasco says. "We verified the number of concurrent connections that our FortiGates allow, and we tested those capacities. We ended up replacing our FortiGate 1500D firewalls with FortiGate 2200E models, to ensure that our infrastructure could handle the sudden, massive growth in traffic." They turned on intrusion prevention system (IPS), antivirus protection, and application control features within the new NGFWs.

In anticipation of containment, the IT group also established redundant options for SSL VPN connectivity throughout the region. "We now have several points of presence in EMEA, and every employee can access VPN through any point of presence," Carrasco says. "If one of our VPN gateways were to become unreachable, users' FortiClients would give them options of other available gateways that they could connect to."

Streamlined Transition to Secure Connectivity

For end-users who already had company-issued laptops, the technology transition has been essentially transparent. The FortiClient solution provides options for SSL VPN connections to appropriate FortiGate firewalls, and the central IT team can seamlessly push out any necessary configuration changes. "The end-users do not control any of the parameters within FortiClient," Carrasco says. "This makes the VPN easy for them. It also benefits corporate security, because users cannot relax security on their VPN connections."

The SSL VPN connection enables all traffic to be encrypted. Then, the FortiGate firewalls scan all traffic that comes in through the VPN. The FortiAuthenticator user identity management server utilizes the corporate Active Directory (AD) to confirm user credentials and permissions to access specific network resources, while the FortiToken solution verifies user identity. "The clients, the FortiGates, the servers, the switches—all the equipment that needs authentication is controlled by two-factor authentication within FortiAuthenticator," Carrasco explains.

In order to optimize communication efficiency, the IT group installed a voice softclient for every Fortinet EMEA employee. "Our staff needed all the same capabilities they have in the office, so we set up a softclient that connects employees' computers to the FortiVoice PBX [private branch exchange]," Carrasco says. "As a result, all our employees are able to stay connected without losing their productivity."

Solutions

- FortiGate
- FortiClient
- FortiAuthenticator
- FortiToken
- FortiAnalyzer
- FortiSIEM
- FortiVoice

"The end-users do not control any of the parameters within FortiClient. This makes the VPN easy for them. It also benefits corporate security, because users cannot relax security on their VPN connections."

– Cyrille Carrasco,
IT Manager, Fortinet

Security-driven Networking at Scale

Because all these solutions integrate into the Fortinet Security Fabric, IT staff can manage the security architecture through a single pane of glass, even though they are also working from home. “We use two tools to monitor, troubleshoot, and investigate security events,” Carrasco says. FortiAnalyzer consolidates information from all the logs across devices and laptops, providing regular reports about denied data flow, information on intranet services and availability, and Simple Network Management Protocol (SNMP) traps. Meanwhile, FortiSIEM helps Carrasco’s team monitor the entire network through a graphical interface that shows security alerts, internet bandwidth usage, and concurrent SSL VPN connections. “We use both tools to understand our traffic and detect abnormalities on the network,” Carrasco says.

In fact, Carrasco adds, the close coordination of Fortinet EMEA’s various security solutions is the reason that 99% of the region’s workforce is now staying safe by working from home. “Without this security infrastructure, I cannot imagine giving all our employees home access to the valuable resources located in Fortinet EMEA offices,” he says. “We have a full, integrated security ecosystem, and each of the solutions serves a specific purpose within that ecosystem.”

The resulting security rivals the security Carrasco’s team delivers when employees are in the office. “When we are working in the offices, a lot of network traffic does not pass through the firewalls because it does not enter or exit the network,” he says. “Today, however, every time a VPN user accesses any network resource, that traffic is inspected by a FortiGate. So, actually, security on our corporate network is even better than ever.”

February 18, 2021 6:57 AM

D:\Fortinet\2021 Rebranded templates\Case Studies\February\Teleworker Security Fabric\cs-security-fabric-solutions-create-worh-from-home-2182021\cs-security-fabric-solutions-create-worh-from-home-2182021

651783-0-0-EN