CASE STUDY

Remote Users Switch From VPNs to Universal ZTNA for Easier and More Secure Application Access

For several years now, virtual private networks (VPNs) have been the go-to solution for creating secure online spaces for remote work. Launching a VPN creates an encrypted tunnel, through which users can access privileged on-campus and cloud resources, without worrying about the security of their local internet connection. It has been a godsend during the pandemic and continues to be so, as many people have settled into hybrid remote and on-campus work routines. But for large global companies like Fortinet, the surge in VPN use has created new challenges.

For one, the need to establish VPN connections has proved to be somewhat of an obstacle to accessing internal web applications. This has put remote users at a disadvantage to their on-campus peers. "Sometimes launching the VPN in the middle of a Microsoft Teams call—say to access an ERP application—would break the connection," says Senior Director of Information Systems James Gu. "Users had to reconnect their internet and intranet separately, which was a hassle. We needed a better way to provide seamless access to applications, no matter where the users are."

On the enterprise side, all that VPN demand was causing bottlenecks at the VPN gateway. This increased latency for users, reducing their productivity. One solution might have been to add more headend capacity. But like widening roadways, adding gateways can be an expensive and short-lived reprieve from the bandwidth crunch.

Instead, the Fortinet IT team reframed the way it approached application access. Rather than categorically permitting broad access to internal applications once a user was connected through a VPN, the team decided to deny access to all internal resources by default. They would allow the creation of a secure tunnel for each particular application only for authorized users on verified secure endpoint devices.

This is the essence of zero-trust network access (ZTNA) as applied to applications. Gu saw ZTNA as more stable and resilient than VPNs, as any internet or intranet outages are automatically resolved without user intervention. But the problem that now faced the team was how to roll it out. Although VPNs were onerous, Fortinet employees were used to them. Would they now have to install new software and learn new access protocols? Would the IT team have to onboard and manage another new tool?

For Fortinet, these concerns proved to be unfounded. "Everyone has been talking about ZTNA, how it changes everything in how we protect the infrastructure and the users," recalls Jayden Ye, the team's IT security architect. "When we first heard about it, we were a bit worried. But when we actually got down to implementing it, it was much simpler than we thought."

"We are looking forward to a totally VPN-less world for all our users, giving them an easy and secure way to connect to all those applications."

– James Gu, Senior Director of Information Systems, Fortinet

Details

Customer: Fortinet

Industry: Technology

Location: Sunnyvale, CA

Business Impact

- Improved security by adopting zero-trust approach to application access
- Days of IT staff time saved in managing access policies
- Increased user productivity by eliminating need to set up VPN tunnels
- Ability to scale services to the home-based workforce through more efficient bandwidth use

ZTNA the Security Fabric Way

Fortinet was able to ease into ZTNA thanks to its existing Fortinet Security Fabric. The Fortinet ZTNA solution is a no-added-cost feature available for all organizations that have both FortiClient endpoint protection and FortiGate Next-Generation Firewalls (NGFWs). FortiClient comes standard with both VPN and ZTNA agents, so giving VPN users access to ZTNA was simply a matter of turning on the feature in the endpoints. Administrators use the FortiClient Endpoint Management Server (EMS) to authenticate users and create ZTNA permission tags for their authorized applications.

Then, the FortiGate NGFW uses these tags to permit access through a secure ZTNA tunnel, which it establishes in conjunction with the FortiClient agent on the remote user's device. Notably, the FortiGate NGFWs are the same devices that serve as the VPN gateways. When they are functioning as VPN gateways, they rely on policies to control access to internal network resources. According to Sean Zhang, a senior software engineer on Gu's team, policy management with VPNs was a significant burden. "As a global company with numerous regional branches, we were creating specific policies for each of the FortiGate firewalls in each of our regions," he says.

Gu elaborates: "Like many large companies, we applied a defense-in-depth strategy, meaning we have several layers of firewalls between the remote user and the internal resources. If we want to create secure access from the VPN gateway to the internal resource, it would take us several days of work to create dedicated policies for different teams and different usage. In comparison, when an application's traffic goes through the ZTNA gateway, we just have a single policy, with all of the controls for each application in one place."

Solutions

- FortiGate Next-Generation Firewalls
- FortiClient ZTNA Agent
- FortiAuthenticator
- FortiToken

"For a big company with a complex network infrastructure, the reduction in firewall-based policy management with ZTNA is going to be very noticeable."

– Sean Zhang, Senior Software Engineer, Fortinet

The ZTNA gateway supports permission granularity down to the level of the user. "For a big company with a complex network infrastructure, the reduction in firewall-based policy management with ZTNA is going to be very noticeable," Zhang says. And because the ZTNA policies are specified in terms of the user, not the network segment, they don't have to change as users relocate, either to their home offices, or to different Fortinet sites around the world.

When a user's role changes, however, their access permissions must change. When application access is controlled through a VPN, users can change roles and still use their old VPN settings to access applications from a former role. Fortinet ZTNA closes this security gap. The policy engine in FortiClient EMS integrates with Microsoft Active Directory (AD), which Fortinet uses to manage all its Windows user accounts. So, when someone in HR changes an employee's role in the human capital management (HCM) system, that change is updated in AD and automatically propagated to the ZTNA policy engine, which changes the user's application access permissions. "None of this needs to involve the IT team, or the security team," Gu says. "For companies with separate network and security teams—which have to collaborate on these changes—this can save a lot of time."

A Cautious Application-by-Application Migration

Starting with Fortinet's internal DevOps websites, the team selected a slate of 15 web-based applications to migrate to ZTNA. They prioritized applications whose migration to ZTNA would have the largest impact on the VPN gateway bottleneck. In the case of DevOps, the migration also provided an opportunity to establish more granular, restrictive access to the company's intellectual property. The new ZTNA-controlled applications will affect thousands of Fortinet employees.

The team moved one application at a time, testing the access protocol with users before applying ZTNA controls to the application. During the transition, users had the option to failover to VPN if the ZTNA protocol did not work for them. The range of options in FortiClient made it relatively simple for administrators to enable this dual-access option. According to Ye, "that was the smoothest possible process for users to take advantage of the ZTNA, without impacting their productivity."

For users, the transition has been seamless. They do not have to install anything new on their devices, nor do they need to change anything with their existing VPN configurations. They can continue to use VPN tunnels for applications that have not been migrated. When they launch a ZTNA-controlled application through their browser, FortiClient automatically redirects the access request through the ZTNA tunnel instead of the VPN tunnel.

Ye notes that the ZTNA option actually saves the users time. "Before, they had to first log onto the VPN, which takes about 10 to 20 seconds. Then they had to log into the application. But with ZTNA, they just log into the application." The authentication and creation of the ZTNA tunnel happens automatically, in the background, and takes less time than with the VPN, according to Ye.

Fortinet has made sure that the authentication process includes two-factor authentication, using FortiToken (on the client) and FortiAuthenticator (on the enterprise network). "It is a testament to the power of the Fortinet Security Fabric," Gu says. "Now, even applications that themselves do not require two-factor authentication get that added layer of security through these components of the Security Fabric." It is important to note that, although Fortinet used FortiToken and FortiAuthenticator as the identity service, other Security Fabric Partner identity solutions would work as well.

Unlike other secure access protocols, the FortiClient ZTNA Agent goes beyond user identification and authentication. "The ZTNA agent is continually checking endpoint security posture," Gu explains. "For example, it checks the compliance of the user's device with company IT policies, such as having antivirus enabled, critical vulnerabilities patched, disk encrypted, and prohibited software removed. Only then does it allow the authenticated authorized user to access the internal resource."

Lowering Barriers to ZTNA Adoption

Despite all the enthusiasm about ZTNA in the industry, Fortinet's ZTNA development team has found that many enterprises are still holding back. It is not just the perceived complication of introducing a whole new access scheme, but the hurdle of obtaining funding and assigning responsibility for a ZTNA migration project. As a security solution, ZTNA would be in the purview of the security operations team, whereas VPNs and remote access are typically handled by the networking team. The latter are concerned primarily about providing reliable, high-quality connectivity. If VPN tunnels seem secure enough, it can be hard for them to justify the expense and staff time to change that.

For Gu, Ye, and Zhang though, the decision was a no-brainer. "With Fortinet ZTNA, there is no additional infrastructure or licensing cost, Ye explains. "You just enable the ZTNA feature; it is pretty easy and transparent."

Fortinet's Universal ZTNA solution supports both on-premises and Software-as-a-Service (SaaS) applications, and the IT team has already set its sights on migrating the company's cloud-based applications to ZTNA control. "Applications like GitHub and GitLab, for example, are really crucial to our DevOps team," Gu says. "We are looking forward to a totally VPN-less world for all our users, giving them an easy and secure way to connect to all those applications.

August 8, 2022 5:01 AM
1684501-0-0-EN