POINT OF VIEW

It's Time to Say Goodbye to VPNs

The Advantages of Zero-Trust Network Access (ZTNA)

Introduction

The recent rise in remote working has put a spotlight on the limitations of virtual private networks (VPNs). Although traditional VPNs have been a mainstay for decades, many organizations are now looking for alternatives that better meet their plans and objectives. With better security, more granular control, and a better user experience, zero-trust network access (ZTNA) can be a smarter choice for securely connecting a remote workforce.

54% of employed adults say that they want to work from home all or most of the time when the coronavirus outbreak is over.[1]

Three Key Drawbacks of VPNs

For decades, VPNs have been the de facto method of accessing corporate networks, but they have some serious issues, particularly in terms of security. Here are three key drawbacks of relying on a traditional VPN to secure remote workers and home offices.

1. **A VPN takes a perimeter-based approach to security.** Users connect through the VPN client, but once they're inside the perimeter they often have broad access to the network, which exposes it to threats. Every time a device or user is automatically trusted in this way, it places an organization's data, applications, and intellectual property at risk.
2. **VPNs have no insight into the content they are delivering.** VPNs are used for remote access when working from hotels, coffee shops, or home. Because most home offices are connected to largely unsecured home networks, they have become a primary target for cyber criminals who are looking for an easily exploited point of access into the network. Because they are no longer sequestered behind enterprise-grade security solutions, they become easier targets for social engineering tactics and malware. VPNs can become conduits for malware to return to the network.

3. **Networks are now highly distributed.** Critical resources and applications are now spread across data centers, distributed branch and home offices, and multi-cloud environments. Most VPN solutions weren't designed to manage this level of complexity. A single VPN connection forces backhauling all of the traffic through a central concentrator for inspection, which is resource-intensive and lag-inducing. Split tunneling can address this, but it creates its own set of challenges as traffic goes straight to the internet without going through a firewall.

Only 15% of organizations have completed a transition to a zero-trust security model, which does not automatically assume that anyone inside the network perimeter is trusted.[2]

ZTNA Offers a Better Option

Because so many people are now accessing critical resources and applications from outside the network perimeter, security experts have been promoting the need to shift away from the paradigm of an open network built around inherent trust to a zero-trust model.

Unlike a traditional VPN-based approach, which assumes that anyone or anything that passes network perimeter controls can be trusted, the zero-trust model takes the opposite approach: No user or device can be trusted to access anything until proven otherwise.

Even if a user has been given permission to access one area of the network or an application, it doesn't assume the user is trusted in other areas. To implement a comprehensive zero-trust strategy in a highly distributed environment, network admins need to control who can access which applications no matter where those users or applications may be located. This "least privilege" approach requires rigorous access controls that span the distributed network so devices, users, endpoint, cloud, Software-as-a-Service (SaaS), and the infrastructure are all protected.

Five Advantages of ZTNA

Fortunately, solutions exist that allow organizations to implement an effective zero-trust strategy without extensive retooling of the network. ZTNA solutions offer multiple advantages over VPNs.

1. **Organizations can extend the zero-trust model beyond the network.** Unlike a VPN, which focuses exclusively on the network layer, ZTNA goes up a layer, effectively providing application security independent of the network.
2. **ZTNA works transparently in the background, which improves the user experience.** A user clicks on the desired app and behind the scenes the client agent does all the work. Secure connections are made and security protocols and inspection are applied to ensure an optimal experience. Unlike using a VPN, users don't have to worry about setting up a connection or where an application is located.
3. **Each user and device is verified and validated before it's given access to an app or resource.** This process includes a posture check that verifies that the endpoint is running the right firmware and an endpoint protection program to verify it is safe to connect to the application. The verification is granular, per session, using the same access policy whether a user is accessing resources that are on-premises, in a virtual cloud, or in a public cloud. The same policy also controls who can access that app based on the profile of the authenticating user and device.
4. **Because ZTNA focuses on application access, it doesn't matter what network the user is on.** It simply delivers automatic secure connections to applications no matter where the user may be located by verifying the user and device posture for every application session, even when users are in the office.
5. **ZTNA reduces the attack surface by hiding business-critical applications from the internet.** Connecting securely is seamless by simply clicking the application. A secure connection is established without having to have the application link publicly exposed.

Improve Remote Access

More organizations are recognizing the need to transition away from traditional VPNs. ZTNA is proving to be a better solution, easier to use with the added benefit of adding application security to a remote access solution. Organizations should be careful to select ZTNA solutions that integrate with their existing infrastructure. Building a zero-trust network access solution requires a variety of components, which may include a client, a proxy, authentication, and security that can be used to apply ZTNA to remote users, no matter where they're located.

[1] Kim Parker, et al., "How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work," Pew Research Center, December 9, 2020.

[2] "2019 Zero Trust Adoption Report," Cybersecurity Insiders, November 2019.

FORTINET

www.fortinet.com

March 6, 2021 6:14 AM

D:\Fortinet\2021 Rebranded templates\POV\March\ZTNA\pov-its-time-to-say-goodbye-to-vpns-V1-362021\pov-its-time-to-say-goodbye-to-vpns-V1-362021

920911-0-0-EN