Beyond VPN: Securing your network with ZTNA

Barracuda

VPNs then and now

Since the advent of the internet and the increase in access to both information and devices, security organisations have tried to secure and protect devices and users connected to it from a growing number of malicious actors online. In 1996 the Virtual Private Network (VPN) was created for this exact purpose, to secure the connection between a user's device and the web. Initially used mainly by businesses, VPNs have since spread to the masses and are regularly used by individuals for data privacy and security. In a business context, both of these use cases are vital.

Businesses have used VPNs to provide secure access to their networks for decades now, but many organisations started to use them even more in the wake of the pandemic, when remote working and work from anywhere policies became more common. A 2021 survey by Coupon Follow found that in March 2020 alone there was a 142% increase in VPN usage compared to the previous month. Bring-your-own-device policies, necessitated by the lack of access to offices, meant that a multitude of employees using their own computers needed quick, easy-to-implement security protocols to secure their connections to the business network.

VPNs are no longer enough to secure your network connection

While they worked to fill the gap in a crisis situation, VPNs are no longer optimal for keeping businesses safe from the risk of a breach. As Mike Vizard of Techstrong Group states, “There’s no doubt VPNs play a critical role in enabling employees to work from home during the pandemic. It’s just the time has come to transition to a more flexible network architecture that just happens to be more secure.” The National Security Agency also issued a warning to organisations using VPNs that unless they are properly secured, VPNs are vulnerable to network scanning, brute force attacks, and zero-day vulnerabilities.

Cybersecurity experts agree that it’s time to move on from VPNs, no matter how useful they’ve been in the past. On top of the security risks, VPNs often don’t meet compliance requirements, can expose your network if not properly configured, and tend to be slow when overloaded with users, which can impact user experience. But what’s next for securing business’ online activity, especially in the wake of a fundamental shift away from the office to remote working?

Enter Zero Trust Network Access

The solution to the VPN problem lies in Zero Trust Network Access (ZTNA). ZTNA isn't a single product or solution — it's a philosophy around how you grant access to different users. We'll get into that soon. The Zero Trust philosophy is a tenet of Secure Access Service Edge (SASE), which Gartner defines as:

"A new package of technologies including software-defined WAN (SD-WAN), secure web gateway (SWG), cloud access security brokers (CASB), Zero Trust Network Access (ZTNA), and firewall as a service (FWaaS) as core abilities, with the ability to identify sensitive data or malware and the ability to decrypt content at line speed, with continuous monitoring of sessions for risk and trust levels."

The goal of SASE is to provide a multi-faceted suite of tools to protect organisations' IT landscapes in today's hybrid, multi-cloud world in which users and devices could be almost anywhere. Now that society is moving from a "work from home" to a "work from anywhere" understanding of hybrid/remote working, the ability to secure devices wherever they are is all the more important. And that's exactly what SASE and ZTNA can provide.

Now, back to ZTNA. While traditional network security has been based on a 'trust but verify' model, ZTNA subverts this approach, preferring a 'never trust, always verify' stance. This is called the principle of least privilege. It means that an organisation will treat all users with the same level of discernment, never automatically giving a user access to networks or assets. Instead, it manages permissions in a way that users are only granted access to the specific data, assets, and applications that they personally need. It employs continuous verification to make sure the user is who they say they are, reducing the potential of a network breach and lateral movement of threats.

How ZTNA works

The term “Zero Trust” may evoke an air of suspicion, but in today’s cyber threat landscape of increasing sophistication, this level of verification is absolutely necessary. While it sounds somewhat negative, ZTNA is a model based on enablement, rather than restriction, allowing for better remote access, improved performance, increased productivity, and strengthened security.

One way to understand ZTNA is to compare it to moving through an airport. When a passenger arrives at the check-in desk, they need to authenticate their identity with their passport. This gets them through one stage of the process of making a journey across borders. However, this does not grant them permission to board the plane: they still need a boarding pass. Without both documents, they will be denied access. Applied to ZTNA, if you can’t both authenticate your identity — with your passport — and prove that you have the required permissions to access the network — with your boarding pass — you won’t be able to continue your journey. Just as individual passengers are thoroughly checked at security and must prove their identity and authorisation to proceed, Zero Trust requires that of every user as they attempt to access your network.

As well as the benefit of thoroughly identifying and validating users before giving them network access, thus reducing the likelihood of a breach, another key benefit of ZTNA that may not be as immediately obvious is the robust system of record that it provides. As users attempt to access the network, the device, location, and identity of each individual requesting access is recorded, creating an audit log and a layer of automated accountability that other solutions don't offer. As well as the security benefit, the record of access attempts can be useful for compliance and audit needs. Other benefits include time savings thanks to automation and the lack of need for IT tickets or management approval for network access.

VPNs cannot compare to the diligence and thorough vetting that ZTNA enables. The level of granularity with which you can manage permissions is only possible with a solution like ZTNA, and cannot be replicated with a VPN. Additionally, while VPNs route traffic firstly through multiple servers and subsequently through a central location within an organisation's network, ZTNA connects the user directly to applications without the need to send them through this central point, meaning latency is reduced too. With the rise in number of cloud applications used by organisations, the improvement of cloud application performance makes a tangible difference in efficiency in terms of both time and usability.

The time to deploy ZTNA is now

With the exploitation of privileged credentials kickstarting so many successful data breaches in recent years, it's vital that businesses securely manage their privileges and network access, before it's too late.

Try Barracuda's Zero Trust Network Access solutions for free.

Barracuda CloudGen Access makes it easy to simplify compliance and secure third-party access to your systems, providing Zero Trust Access to all your apps and data from any device and location. Barracuda CloudGen Access provides employees and partners with access to corporate apps and cloud workloads without creating additional attack surfaces.

Barracuda SecureEdge, a cloud-first SASE platform, enables businesses to easily control access to data from any device, anytime, anywhere, and allows security inspection and policy enforcement in the cloud, at the branch, or on the device. Barracuda SecureEdge includes Zero Trust Network Access (ZTNA), Firewall-as-a-Service, web security, and fully integrated office connectivity with Secure SD-WAN.

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.