BIZCOMMUNITY

Is it the end of the road for VPN?

By Simeon Tassev

5 Jul 2022

As organisations have moved increasingly into the cloud and remote working has become both a requirement and the norm, the traditional borders of the enterprise have shifted and become more amorphous. This means that securing networks and connections can become challenging given the limitations of certain technologies. As a result, there has been a lot of hype around Zero-Trust Network Access (ZTNA) replacing the traditional Virtual Private Network (VPN) solutions.

Simeon Tassev | image supplied

While ZTNA is definitely a more effective solution for a remote or cloud-based environment, VPN technology is by no means dead. Completely cloud-native enterprises are few and far between, with the vast majority looking to run in hybrid scenarios for the foreseeable future, which means VPN still has many practical uses and will for years to come.

The case for VPN

The original Internet Protocol Security (IPsec VPN) protocol was developed and designed for a very specific purpose – to connect sites and individuals to an internal network. Another variation of this, known as Secure Sockets Layer (SSL VPN), was evolved to enable users to connect remotely to a client site using their browser as a client. These narrow use cases meant that there are inherent limitations built into the design of the VPN. It was built specifically to allow policies to be designed and enforced before connecting, to limit and control access per user and per network. This works hand in hand with firewalling rules and segmentation on the network.

These inherent limitations are the most common reason given as to why VPN technology is outdated and has reached end of life. However, the reality is that for the purposes of a large number of businesses, it remains a practical solution in many scenarios. Most businesses are not entirely invested into the cloud, and legacy solutions remain in place, so VPN is still useful. Simply replacing this protocol with the latest and greatest for the sake of having new technology is expensive, disruptive and unnecessary.

Where zero trust becomes a must

Where ZTNA becomes essential is as more and more cloud solutions are adopted, as the perimeter becomes less defined and therefore requires different controls. The zero-trust model provides access based on identity, irrespective of the location of the user, and permissions can be dynamically granted based on the specific characteristics of the network a user is connecting from. For example, if the user is on a trusted network, they can be given a greater level of access than if they were connecting from a public network in an airport or coffee shop. This is not something that can easily be achieved using VPN

ZTNA gives organisations the ability to control access and assign policies on a far more granular level, which makes it a more flexible solution better suited to borderless networking. However, organisations need to remember that ZTNA is not a solution on its own, it is simply a concept and a model that needs to form part of a greater architecture. ZTNA forms part of the Secure Access Service Edge (SASE) framework, and works in tandem with other components like Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB)and Software-Defined Wide Area Network (SD-WAN) to provide secure network access.

Taking the complexities in stride

The more businesses open to the cloud, the more difficult it becomes to control the perimeter, so technologies that are applicable in a borderless world become important. ZTNA is the next evolution of security for borderless networking environments, but it is not a silver bullet. The best solution, or rather mix of solutions, depends on a variety of different factors, including the specifics of the network and the environment, and the budget and risk appetite of the business.

VPN is not dead, it still has a role to play especially with regard to securing legacy systems on premises, but ZTNA becomes important when making use of cloud or Software as a Service (SaaS) solutions. However, as with any new implementation, a zero-trust approach comes at a cost and has implications on the business. To ensure that a business is leveraging the best (and most cost-effective) solution for its needs, it is essential to engage with a technology partner that understands the requirements and dependencies of the environment and can deliver secure access without the risk.

ABOUT THE AUTHOR

Simeon Tassev, is MD and QSA at Galix.

For more, visit: https://www.bizcommunity.com