TAG CYBER

Controlling remote access to company assets is more important now than ever before. The COVID19 pandemic has amplified and accelerated the need with most workforces now working from home. Traditionally a virtual private network (VPN) was coupled with a firewall to provide secure remote access controls, but with today's hybrid computing environments and the untrusted networks from which users are accessing assets, the shortcomings of VPNs are being highlighted.

Secure Access for Road Warriors

Like many people working from home today, when I was constantly on the road as a sales engineer I had to rely on the company VPN to do my job. I often found myself in remote locations with questionable internet or at security tradeshows where traffic snooping is a competitive sport. The VPN was my lifeline which allowed me to connect to the internal demo network, which by design was isolated from the corporate network given the questionable locations me and my colleagues would connect from. However, this isolation also caused issues when I needed to connect to other networks like the production cloud where I could provision a POC environment. In order to do this, I had to switch VPNs which made for bumpy presentations.

This scenario is not uncommon these days and highlights why VPNs are an outdated means of secure connection to modern infrastructure. VPNs are unable to support simultaneous connections to multiple destinations and require constant juggling if you want to connect to different network segments. This is even more of an issue in today's hybrid infrastructure where employees often need to connect to on premises data centers and cloud environments daily to do their jobs.

It's not just operational issues that cause friction for employees as tighter security requirements are also placing VPNs under strain. They lack the necessary security controls required to meet the new secure remote access standards such as intra-network traffic inspection, secure authentication mechanisms, and mechanisms to prevent lateral movement in a network segment. So, what is the future of secure remote access?

A Modern Approach with SDP

The team at TAG Cyber recently met with Appgate to discuss how software-defined perimeters (SDP) are quickly replacing VPNs as the go-to solution for secure remote access. SDP is a network security model that dynamically creates one-to-one network connections between users and resources. They essentially give an individualized, micro-segmented network tailored for each user (or group) to allow access only to the resources required while hiding everything else. They also provide access controls that allow for both remote and on-premises environments connections simultaneously, which is a must in the hybrid computing model most enterprises utilize today.

Appgate's SDP solution is built using an identity-centric architecture that is designed around authenticating the user before allowing any connection. Appgate embraces the Zero Trust model and uses single packet authorization (SPA) to enforce an "authenticate first, connect second" approach. SPA cloaks infrastructure ports so that they are invisible to port scans and ensures that only authorized users can connect to the network resources. Appgate SDP uses a local client on the user's endpoint to make access requests to a controller which evaluates credentials, applies access policies, and sends a cryptographically signed token that contains the authorized set of network resources back to the client. The client then uses SPA to send this token to a set of gateways which provides access to the authorized resources they protect. Appgate's patented multi-tunneling driver also provides users the ability to simultaneously connect to multiple environments, removing the need to juggle connections during a workday.

As employees remain working from home, the market for secure remote access will continue to grow. By enforcing a Zero Trust model which allows users to only connect to specified resources, Appgate is primed to capture this growing market with a solution that addresses many of the issues with VPNs. The secure remote access and Zero Trust market is quickly filling up with some big players, but Appgate's unique and patented approach should set them apart and provide enterprises with the secure remote access controls they have been searching for.

About TAG Cyber: TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

About the author: Adam LeWinter is a senior analyst at TAG Cyber where he collaborates with security product companies on market messaging, positioning, and strategy. Prior to joining TAG Cyber he held technical sales roles in multiple IT and cyber security companies.