Private Communications Corporation

An MSP’s Perspective: The Time for ZTNA

By Guest Author Joshua Liberman

President, Net Sciences, Inc.

Memories. Some of us remember when remote connectivity meant port forwarding of traffic from WAN to LAN, but hopefully nobody reading this is doing that. Then came firewalls and the need for protocols such as PPTP, L2TP, and then SSLVPN connectivity, which has been the gold standard for years. Next was the shift to cloud, remote and hybrid work, and the gradual dissolution of the network perimeter. While this shift from a “defined perimeter” to a more diffuse boundary has enabled new ways to work, it has made network defense much harder.

The Problem. I do not need to explain why port forwarding makes no sense today, as it is the first thing any intruder checks when attempting a network penetration. And simply changing the RDP port from 3389 to an alternate port has not been “clever” since, well, forever. But with SSLVPN considered the go-to for road warriors today, why the change?

The first issue is that in its simplest sense, connecting to a LAN from the WAN by means of VPN bridges your remote device (and its network) to that LAN. You can constrain traffic across that connection, but it is proving to be increasingly challenging and difficult to manage. VPN technology precedes cloud computing, hybrid working, and other connectivity pathways of 2024. It falls short in several ways, including granularity, manageability, user experience, and most importantly, security. But there is a better way; Zero Trust Network Architecture (ZTNA).

What is Zero Trust and ZTNA? I used to joke that Zero Trust (ZT) was the “Peace on Earth” of networking, and just about as attainable. And ZT/ZTNA suffer from rather amorphous definitions. For our purpose, I see this broken out as ZT for control of local applications (allow-listing, privilege limitations, etc.), and as ZT Network Access, which is what we are discussing here. ZTNA controls traffic routing and access to just about any resource, on premise, or in the cloud. Of course, both fall within the overall umbrella term of Zero Trust.

What is An Ideal Remote Connection? From the standpoint of an MSP owner, the ideal remote connection embodies three attributes; granularity, improved user experience, and superior security. And of course, it must be affordably priced, whether we break it out or bundle it into a larger solution offering. Here is a bit more detail on each of these qualities.

Granularity. This refers to the ability to limit remote users' access to network resources based upon several factors. These can include user identity, user location, device ID and even their pre-defined application needs. VPN alone offers few of these fine-grained controls, and in their absence the entire network is open to the remote user.

Improved User (and MSP) Experience. ZTNA also offers both simplified connectivity and improved end user experience, not to mention easier management for the MSP. There is little for the users to do to initiate their connection, it essentially just works. Further, with lesser latency and optimized traffic routing, most users will experience improved performance and responsiveness. And MSPs can expect to experience less after-hours ticketing, when most users seem to struggle with VPN, as the ZTNA experience is usually trouble free.

Enhanced Security. ZTNA can consider the device ID of remote devices prior to connection. This capability, coupled with an inherent reduction in the "attack surface" of the network, and offering more robust authentication than VPN (including integrated SSO and Certificate-based authentication), makes ZTNA inherently more secure. With VPNs trust is established only upon initial connection, while ZTNA provides ongoing inspection. ZTNA can also provide real-time analytics, allowing the MSP to identify and respond to anomalies.

Cloud Connectivity Protections. ZTNA really differentiates itself from VPN connectivity when it comes to cloud access. ZTNA can protect any data pathway, and it can provide a single point of control and enforcement of security policies. Granularity also plays a role in cloud access, limiting users to only designated applications. Finally, with real-time monitoring, ZTNA can provide timely alerts of anomalous or suspicious behaviors.

What About the Pain of Change? There is no truly painless way to migrate users, as any time you move their cheese, it gets noisy as even something better is still something different. However, the move to ZTNA can be one of the most anodyne changes. With preparation and a carefully staged deployment, the transition to ZTNA can be smooth. With the right ZTNA partner, you'll find the deployment of ZTNA solutions to be straightforward. And finally, once in place, ZTNA solutions are quite stable, with minimal ongoing support requirements.

The Time For ZTNA. From the standpoint of the end user, ZTNA has a high degree of “it just works” feel to it. Performance is also better, which may well also lead to happier users. From the standpoint of the MSP, the enhanced granularity, an improved user experience, and various the security benefits, all make ZTNA the right choice for the times.

The most powerful inducement to move to ZTNA might be the reduced support load and greater peace of mind afforded by ZTNA, but other reasons abound. VPN has served us well for years, but our new world of the dissolved perimeter, work from anywhere, and the hostile Internet, all argue for the transition from VPN to ZTNA. Now is the time for ZTNA.