AmZetta Digital Workspaces

SOLUTIONS BRIEF

Is My VPN a Vulnerablility to My Company?

For the majority of time that the Internet has been widely used, the go-to solution for secure remote access has been VPN. Unfortunately, VPN technology is falling behind with advances in cloud adoption for applications and an increased remote work presence in organizations worldwide. With these adoptions, VPNs are starting to be exposed, with the following being some common security holes:

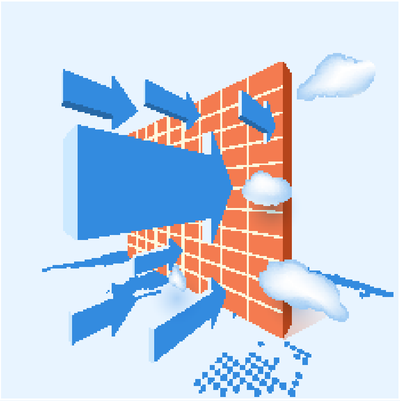
- VPN devices are internet facing, which makes it easy for attackers to scan the internet for their vulnerabilities.
- VPN vulnerabilities give attackers remote access to a network without login credentials. In all cases, attackers can then run their own code to access internal systems, exfiltrate data, install and/or wipe devices.
- Research has found that as of January 3, 2020, there were 3,825 unpatched Pulse Secure VPN servers. Of those, 30% of them were in the U.S. (1,148).

Because of these new challenges, a different technology is starting to overtake VPN as the option for secure remote access. Zero trust network access (ZTNA) is being adopted at a rapid pace by organizations because it enables secure, agile, targeted access.

Why you need more than a firewall & generic VPN to secure remote devices

AmZetta's zGateway is the perfect ZTNA solution to ensure employees can access what they need, when they need it and nothing more. AmZetta's solution focus on alleviating three main painpoints with remote access that VPN improve upon:

- Security
- Access Controls and Auditing
- User Experience



Reduce your attack surface

Three in ten employees will continue to work from home even in times of stability, and they'll need secure access to resources - including SaaS and web-based apps - from new locations and different devices. AmZetta's solution empowers organizations to migrate from a traditional network-centric approach in terms of security and instead focus on an app- and user-centric security approach. One of the biggest advantages of this is that application access becomes disassociated from network access, meaning when users log in, they are given access to specific applications, not the entire network. This drastically narrows the exposure of an organization's sensitive corporate environment by coupling a user to specific applications, not an entire network.

Enable BYOD with proper security controls

Traditional VPNs require constant device management and are limited to recording a device's IP address, port data, and protocols. This robs administrators of crucial insights concerning what users' activity while on the network.

AmZetta's solution gives administrators a solution that gives them a way to easily monitor, identify, and diagnose potential security threats. This is done by allowing administrators to see not only the basic information afforded by a VPN, but also insights into user identity, application access, latency, location, and much more.

Furthermore, the solution enables BYOD while still enforcing all of the security policies and insights mentioned above. This way, a user can truly use any device and the organization can rest assured that all access will be tightly scrutinized for potential security flaws.

Improve the user experience

When it comes to the employee experience, traditional VPNs fall short. VPNs are inconvenient to use as they require users to constantly log in or out and there can be noticeable latency. All user traffic is backhauled to data centers that can be hundreds of miles away, increasing latency and user frustration with it. Another consequence of that backhauling is the concern of employee privacy as all data is transmitted between the tunnel.

With AmZetta's solution, employees will have the same experience whether they are in the office, at the local coffee shop, at an airport, or even hundreds of miles away. Employees get to enjoy a simple, intuitive way to access the corporate resources they require from any device or location.

Interested in testing Digital Workspaces in Your Environment?

Just click the link below, input your name and email ID. We will send you the URL, username and password to evaluate the Digital Workspace solution. **https://amzetta.com/demo/**

AmZetta

AmZetta Technologies
5555 Oakbrook Parkway,
Suite 280
Norcross, GA 30093

Technical Support
support@AmZetta.com
1-800.892.6625

Sales & Product Info
sales@AmZetta.com
1-877.991.1809
https://amzetta.com