Goodbye VPNs – Hello Zero Trust Network Access

by Sharon D. Nelson, Esq. and John W. Simek

Virtual private networks (VPN) are very standard these days. But they are riddled with vulnerabilities – and subject to a “man in the middle attack.” They have wreaked havoc in 2020 in a work-from-home environment.

Enter zero trust network access (ZTNA).

An October 2020 Forrester study (commissioned by Cloudflare) offered some key findings.

Working from home compelled firms to transform how they operated in the cloud. However, 80% of the IT decision-makers interviewed said their companies were unprepared to make the transformation. Existing IT practices made it difficult to support employee productivity without security compromises.

As a result, 76% of the decision-makers said their firms intend to accelerate their shift to the Zero Trust security framework. More than three-quarters (76%) of decision-makers polled said their companies' security practices were "antiquated" and needed to shift towards Zero Trust Network Access.

The report found that 82% of the firms said they were "committed" to migrating to a Zero Trust security architecture. To achieve this goal, close to half (49%) of the firms elevated the role of CISO to board visibility while 39% had a Zero Trust oriented pilot for 2020.

The migration towards Zero Trust faces various challenges, with 76% of the firms identifying Identity and Access Management (IAM) as the major challenge.

For those who are unfamiliar with the Zero Trust security model, it allows remote workers to access applications through a secure web-based gateway. The solution implements least-privilege principles and supports multi-factor authentication (MFA) and device security checks. Unlike a VPN infrastructure, Zero Trust is highly scalable, more affordable, and easily integrates with various single sign-on (SSO) platforms already available in the marketplace. It also permits the configuration of access control policies to manage permissions based on users' privileges and devices.

More than half of all businesses have experienced data breaches (58%) or increased phishing attempts (55%) during COVID-19. Ransomware attacks affected 29% of the respondents.

Infrastructure outages and VPN connection latency issues disconnected 33% and 46% of workers, respectively.

Several vendors offered their services for free or on extended trial periods to allow customers to test their Zero Trust security solutions during COVID-19. The free trial period allowed companies to migrate to a Zero Trust security model and test advanced security solutions from reputable vendors. They could then select the products that met their security needs and sign up on a permanent basis.

Why the sudden interest in a Zero Trust architecture? The short answer is our migration to the cloud, increase in third-party service providers and the need for mobility. Protecting the security perimeter was fine as long as all the services and people were within the network boundaries. A VPN assumes that a trusted device is now outside of the perimeter and needs to connect securely to inside resources. With more cloud services and a mobile workforce, we need an architecture that provides security for the user and application regardless of location or device.

Even though Zero Trust Network Access as a VPN replacement is right around the corner, it is not a solution for everyone or every application. Zero Trust works great for applications that have migrated to the cloud where you can clearly identify the users that need authentication. In other words, you have identified those users that need access and you trust nobody else.

Where ZTNA doesn't work well is for applications that need to be exposed to the public. Think about Zillow, Amazon, Expedia, Airbnb, etc. Applications such as these need to be open to the public. You really can't have a user logging on just to see what's available for sale or hotel rates in a particular city. Those users want to be anonymous until they make a purchasing decision.

Users are still a problem even with ZTNA. If a cyber criminal gains access to a valid user's credentials, they can access resources just like the authorized user. In other words, if the user continues to reuse passwords or doesn't utilize MFA, an attacker can act just like a valid user.

We always knew Zero Trust Network Access was coming, but COVID has accelerated its arrival. Just like any other technology, ZTNA has to be securely implemented with strong authentication controls, thereby protecting users from themselves.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com