AKAMAI WHITE PAPER

VPNs Are Not as Secure as You Think

Akamai
FASTER FORWARD

Introduction

Virtual Private Networks (VPNs) have been the de-facto solution for enabling secure user access to enterprise applications for 20+ years. During this time, the core VPN security model has not fundamentally changed; a VPN is used to connect remote assets – users, databases, or whole offices – to an organization's secured network. VPNs are less expensive than a dedicated leased line, making them attractive to large and small enterprises.

The core VPN security model has not fundamentally changed in 20+ years.

But VPNs have several shortcomings, inherent problems, and management complexities — many of which become more pronounced now that cloud, mobility, and enterprise digital ecosystems dominate the landscape. From providing excessively wide network access and the inability to control user identities, to providing inadequate solutions for third-party access, VPNs are not as easy, flexible, or as secure as you think. For end users, VPNs can be an unreliable, clunky irritation. It is finally time for enterprises to rethink their reliance on this aging technology. Here are 5 reasons why:

1. VPNs Give Devices — and their Users — Full Network Access whether they Need it or Not.

VPNs securely extend your data center network to an end point – e.g., a laptop or a smart phone. Data transmission over the VPN is private. However, with VPN access, users have access to many resources and enterprise applications in a network or within a configured IP subnet. If most end users only need remote access to a limited number of applications, why do we give them access to the entire network?

Beyond the questionable need to provide users with network-wide access is another scary, unintended scenario: malware infested on devices, once they gain network access over the VPN, may start looking for vulnerabilities within your internal applications. Instead, if you grant only application-level access, the malware's attack surface is naturally constrained.

2. VPNs do not Control Remote Access Based on User Identities.

Although VPNs require end users to identify themselves through a set of credentials, the user identity is not used to manage authorization policies for applications. Just because a user has been authenticated does not mean the user should have unrestricted access to everything in the network.

Typically, VPNs are placed within the DMZ and are used in conjunction with a firewall that provides network-level filtering of IP/port combinations. However, network policies tend to mutate over time, and it is not possible to maintain complete visibility into the applications accessible to a VPN user. All access control should be based on the user's identity rather than the IP to or from which they connect. IP/port qualifiers serve as a poor substitute for access control, and they leave the company susceptible to information leakage.

3. VPNs are a Weak Security Solution and Management Burden for Third-Party Remote Access.

If your company routinely interacts with third parties — consultants, contractors, suppliers, partners, and customers — who need remote access to enterprise applications hosted in your data center environment or hybrid cloud, a VPN is a poor solution. After all, you don't want to give untrusted third parties carte-blanche access to the network when all they need is access to a limited number of applications.

Typically, third parties only need access to a given application for a limited time. The time it takes to configure, manage, and deploy a separate set of subnets for third parties — coupled with managing user moves, adds, and changes — are all time-intensive activities. Whether the process takes days or weeks, it is clearly an impediment to business.

All access control should be based on the identity of the user, not the IP to and from which the user connects.

If a third-party user needs access to a specific application, you should easily be able to set a policy to bind the user to the given application without making changes to your network. VPNs do not, will not, and cannot function in this fashion

4. VPNs Result in Fragmented Security Policies for Distributed Enterprises.

If your enterprise applications are deployed in different locations (e.g., multiple on-premise data centers or multiple VPCs in the public cloud), you may need to deploy VPN gateways in each location or VPC. In this case, you need to ensure that all policies are applied consistently to all gateways. You don't want to be in a situation where some applications are not as secure as others. This is usually a manual exercise.

With multiple VPN gateways in the mix, end users must have a prior knowledge of which VPN gateway to connect to for a specific application. This is a poor option from a usability perspective.

An alternative to deploying VPN gateways in each location is to build a perimeter in one network location and drive all user traffic through this location. Traffic destined for other locations will then need to be routed via an overlay network and routed back before it is sent to the end-point. In this scenario, you are building a complex routing environment that must be managed on an ongoing basis. Such complexity tends to result in security vulnerabilities over time.

5. Users Hate the VPN Experience.

Using a VPN is often a poor experience. While not a security issue, any aspect of a solution that reduces user productivity is something that security teams should be aware of. Most VPNs require a client to be installed on the endpoint, which is a challenge for both the administrator and the user. In this era of ubiquitous connectivity and mobile device proliferation, client distribution to a variety of devices is a huge task for administrators. Thus, administrators often restrict the number of different devices they will support with VPNs.

Most VPN users have experienced VPN-induced pain – frequent disconnects, inability to log onto the networks, slow response times, etc.

For end users, VPNs tend to illicit a visceral negative reaction. Most users have experienced VPN-induced pain — frequent disconnects, inability to log onto the networks, slow response times, etc. — when accessing critical applications remotely. Moreover, users want universal access — a Gmail-like experience — such that it doesn't matter what device they are using or where they are when accessing critical applications.

The Enterprise Application Access Solution

Akamai brings a radical new access approach for enterprise applications hosted in data centers and hybrid cloud environments that is more simple, secure, and convenient than traditional solutions. Enterprise Application Access (EAA) is the industry's only perimeter service that locks down all inbound firewall ports while providing end users remote access to only their specific applications — without VPNs. In contrast, VPNs provide overly broad network-wide access, giving entry to applications and compute infrastructure beyond a typical user's day-to-day requirements. EAA separates an organization's infrastructure from the Internet, minimizes the application attack surface, and hides applications from public Internet exposure. It also integrates data path protection, identity access, application security, and management visibility and control into a single solution. EAA can be deployed as an application's first line of defense in minutes, at a fraction of the cost of build-it-yourself solutions. The result is a secure access-delivery model that enables a zero CapEx, low OpEx model for critical workloads deployed in any environment.

Simple

- Collapse a whole rack of equipment into a cloud service
- Stand up new applications and provision users in minutes
- Easily add MFA to any app with the click of a button
- No device or client software
- Easy to deploy, provision, change, and monitor

Secure

- Keep all users off of your network
- Lock down your firewall or security group to all inbound traffic
- Make your applications invisible to the Internet
- Minimize the network attack surface
- Zero open ports on your edge firewall

Convenient

- Users access applications from any device on any browser without any additional software — including VPNs and browser plugins
- Use a service that consolidates ADCs, Wan Optimization, VPN, and Multi-Factor Authentication
- No hardware or network changes required – i.e., firewall rules, IP address white listing, etc.
- Complete auditing and reporting of user activity
- Available as built-in reports or can be integrated with your existing tools

No CapEx, Lower OpEx, and Lower Integration

- Enable secure access, stand up new apps/users in minutes, and save 100s of man hours per app
- One-time deployment works for any number of apps — eliminate projects for additional apps
- Deploy service at a fraction of the cost of competitive, appliance-based solutions

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.