AKAMAI WHITE PAPER

5 Reasons Enterprises Need a New Access Model

Akamai
FASTER FORWARD

Today, enterprises are providing employees and third parties with remote access to their applications in much the same way they did 20 years ago – through VPNs, proxies, and remote desktops. These technologies require enterprises to establish trust with each user and device, then provide access through a network security perimeter to the resources the user needs. Traditionally, the asset you are protecting is inside a trusted zone, and any access to it would be from an outside, untrusted zone. This outside-to-inside access requires passing through this shared perimeter. Enterprises have acknowledged this perimeter is especially permeable to attack, and yet they continue to provide access in the same old ways.

New and growing realities are forcing enterprises to take a different path. Given the mounting number of high-profile security breaches resulting from third-party access, it is clear a new methodology for providing third-party access is needed. Shedding light on what a new access methodology is requires us to explore five key changes in the enterprise landscape: growing partner ecosystems, taming the mobility explosion, challenges of cloudification, adopting a zero-trust model, and the "SaaSification" of IT applications.

1. Growing Partner/Third-Party Ecosystems

Increasingly, we rely on partners, contractors, suppliers, franchisees, and other third parties to drive business forward. From occasional access for a third-party contractor to the complete outsourcing of services, enterprises are opening up their networks. These partners are accessing enterprise applications from outside the enterprise network via the Internet.

With each partner added to an enterprise's ecosystem, a number of outside-to-inside access rules need to be put in place in the perimeter firewalls to allow these partners to connect to the applications and resources they need. When these applications and resources reside in multiple locations, the rules need to be replicated in each site. This is not a new problem – back in 2004, Network World declared that firewalls were "shot so full of holes that they barely provide any protection at all."

Since then, the problem has gotten worse, with the effects clearly seen in every breach reported in the news. Access into the network was the root cause of the Target breach — the HVAC contracting company who had access to Target's network was hacked, and from there attackers gained access to Target's most sensitive systems.

Enterprises have been coping with the permeability of the perimeter by adding more layers of security to catch the bad stuff that gets through: IDS/IPS, DLP, WAF, and others. Every new layer comes with its own complexity and overhead to manage the new policies, and despite the complexity — or perhaps because of it — the perimeter remains permeable.

Countering this permeability is why a new access methodology is needed. In the security world, the "principle of least privilege" is basic: give access to only the resources a user needs to get their job done, and no more. The trouble is many of the access methodologies that exist today – particularly VPN and remote desktop – by default allow broad access to all resources on the network. That means any malware sitting on the user's device is free to roam as far as the access method allows. Enterprises need to adopt a new access methodology that eliminates broad access to the network and provides connectivity to only the resources partners need to get their work done.

2. Taming the Mobility Explosion

In 2014, the number of mobile devices exceeded the population of planet Earth – 7.2 billion devices. More dizzying, they are multiplying at 5 times the rate of the world population. For enterprise security teams tasked with protecting access to internal resources from these devices, this growth is staggering.

Over the last 15 years, enterprises have tried to deal with the issues of mobility growth and BYOD by extending trust to mobile devices. Technologies like NAC (Network Access Control), and more recently Mobile Device Management (MDM) or Enterprise Mobility Management (EMM), have sought to bring users and devices back into a trusted zone by installing clients and certificates on each device. Instead of bringing the users inside the existing security perimeters, these controls are essentially extending the enterprise perimeter to encompass all external users. But these technologies are complicated to implement and manage. Further, malware such as Stagefright can silently take over a device, nullifying any notion of trust. Unfortunately, NAC, MDM, and EMM have failed to live up to their promise.

These "extend the perimeter" strategies have led to greater workloads on IT, greater complexity, and because complexity is the enemy of security, have actually weakened security. With the growing number of Internet-enabled devices, trying to establish trust with user devices is a losing battle. We need a model that does not rely on an assumption of a 'trusted device'.

3. Challenges of Cloudification

There is no doubt cloud computing has gone mainstream. According to IDG, 69% of enterprises in 2014 were using public cloud computing services, up from 57% percent in 2012. Hybrid cloud adoption, the integration of cloud computing services such as AWS, Microsoft Azure, and IBM Softlayer with existing virtualized enterprise infrastructure, is expected to triple in the next three years. And while most enterprises are adopting a hybrid cloud strategy, some, like Time, Inc. and Yamaha, have decided to eliminate private data centers and move completely to the cloud.

Moving to the cloud has many advantages in terms of agility, flexibility, and overall cost, but it comes with two major challenges: First, you don't have low-level control of the network components and servers in the cloud. That means you must build infrastructure in the cloud differently than you would in a private data center. Second, your users cannot physically be "in the cloud". Nobody is on the network in the cloud, everyone has to come in from outside. The network between users and private applications in the cloud is the Internet.

The cloud is not one static environment but many dynamic individual environments. Very few companies have one cloud. They have many separate clouds – what AWS calls Virtual Private Clouds or VPCs. Unlike traditional data centers, VPCs can be created and torn down in minutes, and each VPC is its own network with its own perimeter. With traditional access solutions, security and access policies would need to be controlled on a per-VPC basis. For example, if access is via a VPN, there would need to be a VPN termination point in every cloud. Users would need to run multiple VPNs on their devices and have knowledge of which VPN to use to access which VPC and which VPCs run the application they need to access. An alternative is to build an overlay wide-area network that connects every VPC to every other and unifies access to a few Internet breakout points. This would be a huge expense in terms of both the cost to acquire the equipment and the hundreds of man-hours necessary to design, deploy, and troubleshoot the implementation. Neither VPNs nor overlay WANs are practical alternatives.

Because of "cloudification", enterprises need a better solution for users to reach applications, wherever they may be, and for IT departments to manage access policy and security in a way that is agnostic to the location of the application. Access architectures need to move to a model that eliminates infrastructure dependencies between the user and the resources.

4. Adopting a Zero-Trust Model

Our ability to trust another person is based on our capability to identify that person. Identity is essential to establishing trust, but even if trust is established initially, we can never be sure that trust has not been compromised. Augmenting simple username and password identity with 2-factor and multi-factor authentication as well as adaptive access policies are strategies to help ensure identity, even if simple credentials are stolen. Even so, the recent Stagefright outbreak, and before it the Heartbleed vulnerability, have redefined the trust relationship enterprises have with user devices because of the fear of latent flaws in, or silent takeover of, the base operating systems.

If we must treat all devices and all users as untrusted, it's easy to see that traditional access models like VPNs — which allow users to punch through network perimeters into the trusted zone — are doomed. With a zero-trust approach to user devices, all users are essentially strangers on the Internet. Clearly, giving internal network access to that class of user is a huge security risk. New access architectures must assume no user is trusted from the outset, and when trust is established, it is transient, of minimum duration and scope.

Taking this approach to the limit, rather than bringing users inside the network to access these applications and data, we can think of a model to selectively bring applications out to meet users. With the exception of administrative access, we don't ever let anyone inside the network. Instead, new access architectures should create broad separation between users and applications.

5. "SaaSification" of IT Applications

As consumers, we live in an SaaS world. Witness Facebook, Gmail, and Uber — applications that can be readily accessed on any device, anywhere, with high performance. For enterprises, the same SaaS trend is underway. Led by Salesforce.com, Workday, and Microsoft Office 365, enterprise users are getting easy and simple interfaces to the applications they need. This SaaSification is reshaping enterprise user expectations just as consumerization did.

While SaaS adoption in enterprises is growing quickly, the sheer number of private and specialized applications running in enterprises today precludes the idea that all apps will move to SaaS anytime soon. The trouble is, users want the same experience accessing all of these non-SaaS, private apps that they get from SaaS applications: Access from anywhere, on any device, no VPN required, and no client software required.

Delivering this SaaS experience is far easier said than done. In addition to the security measures of a traditional enterprise perimeter, SaaS companies have had to front end their applications with Internet-scale protections from DDoS attacks, add acceleration to mitigate performance and latency issues, and add specific application-layer attack protections. New access architectures must meet the expectations of users and deliver private applications as simply as if they were SaaS applications with the same level of protection these applications require.

The New Access Architecture

To address these 5 fundamental changes, enterprises need a new architecture for providing access to their private applications. Whether running inside a private data center or in a public cloud-computing environment, private applications need to be delivered to partners, contractors, and customers with greater security and simplicity than existing access methods provide.

Enterprises need a new access architecture that meets today's challenges by:

- Separating and isolating access to the underlying network and providing access to only the applications users need to get their work done
- Moving to a model where trust is device-independent, transient, and of minimum duration and scope
- Eliminating dependencies on the infrastructure between the user and the resources they are trying to get at
- Meeting the high-performance and simple user experience expectations of users and delivering private applications as if they were SaaS applications