Access Control in the New Mobile, Hybrid World

Jay Kelley, 2015-04-05

There is a brave new world dawning for the corporate world. There are many "new norms" – and a gold rush of new opportunities, but also new challenges with which they come – streaking like lightning throughout organizations.

The workforce of today and into the future is, and will continue to be mobile. Consider that according to analyst IDC, 37 percent of the worldwide workforce will be mobile by the end of 2015. That's about 1.3 billion mobile workers, worldwide – not to mention there will be two or more times as many mobile devices as mobile workers! – by the end of this calendar year! Then, consider this: According to Orange Business Services, 55 percent of worldwide business IP traffic will be mobile business Internet traffic by 2018. Mobility is here, and it's here to stay.

(In the Asia Pacific region, IDC anticipates the bring your own device (BYOD) market will continue its robust growth. There were an estimated 155 million smartphones and over 4 million tablets in use supporting BYOD initiatives across the region last year (2014), with year-on-year growth of 40.4 percent and 62.7 percent, respectively. And, that's not even considering the burgeoning area of wearable devices, either.)

As the mobile workforce accelerates like a rocket into the stratosphere, cascading torrents of smartphones, tablets, and wearables across organizations in its wake, the number of cloud- and SaaS-based applications used within organizations is also skyrocketing at a breakneck pace. According to a recent study sponsored by SkyHigh Networks, there are on average 759 cloud services in use by today's organizations. The most puzzling piece isn't the magnitude of in use cloud apps and services. Instead, its that, according to a Cloud Security Alliance study, most organization IT teams believe they have fewer than 50 cloud-based apps in use. That means that over 700 cloud apps and services on average are in use within enterprises – but no one (but the user) has control over those apps and services, and any corporate information shared with them! The problem is, you cannot defend what you don't know about!

Finally, the last piece of the "new norm" puzzle for organizations is the hybrid network, an eclectic mix of data center and cloud-based apps and data, with a stew of hosted private, public and cloud infrastructures. According to analyst Gartner, "while actual hybrid cloud computing deployments are rare, nearly three-fourths of large enterprises expect to have hybrid deployments by 2015." Consider that a mobile workforce will drive infrastructure changes, needed to address a more diverse device ecosystem. Then consider that infrastructure addressing mobility requires greater investment in cloud-based apps and services to support that expanding device ecosystem. So, as you can see, the future of the network fabric for the foreseeable future will be hybrid.

So, with a "new norm" of mobility, cloud, and hybrid networks, how can organizations address network, application, and data accessibility? With so many new devices that are mobile and are under limited corporate control, and applications and data scattered about the network and in various clouds and SaaS deployments, how can an enterprise be assured of fast, appropriate, authenticated and authorized access?

With so many variables, there is one constant that remains: Identity. The user – and their identity – is, arguably, the "new perimeter" for the enterprise, today and onward.

As the traditional network perimeter has been broken, fragmented, and in many instances shattered into many pieces, identity has become the new perimeter. As applications, data, and even networks move faster toward the cloud, and the user-controlled, BYOD-driven mobile ecosystem expands exponentially, corporate control has become more difficult, dispersed, and dependent on others – and many times, that's the security uninformed and apathetic user. User identity, though, never changes. And, backed by authentication, authorization, and accounting (AAA), identity is now the first line of defense for secure corporate access.

But, identity is just the tip of the spear for controlling the new parameters of access. The context of a user's access request, and their environment at the time of access request, follow identity; inarguably, they have as much to do with securing appropriate access as identity. The ability to address the 5 w's and 1 h (who, what, when, where, why, and how) assures, enhances, and differentiates secure access to networks, clouds, applications and data – wherever they may reside and however they are comprised.

Insuring user identity is efficiently, securely shared between networks, clouds, applications, and data – wherever they live – is now a necessity. Yet, there are challenges: Identity silos, on-premise identity with cloud- and SaaS-based apps and data, and user password fatigue leading to weak user names and passwords – which are easily compromised. That's where building an identity bridge comes in. Federation builds a trusted chain of user identity between two entities – networks, clouds, applications, etc. – through industry standards, such as SAML. The cumbersome duplication and insertion of identity directories becomes unnecessary. Identity and access is controlled by an enterprise, with authentication occurring between the enterprise, and cloud and SaaS providers. Instant user authentication and its termination is centralized and under enterprise control. Identity federation delivers access visibility and control together.

Leveraging identity for access control, and building identity bridges are now imperative for organizations, as applications move outside the enterprise domain, the workforce and their devices are more mobile and leave the enterprises in droves, and the enterprise domain, too, has moved. It's the "new norm".

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com