Solving security and performance challenges of cloud and SaaS applications in 2015

Michael Koyfman, 2014-30-12

As 2015 is almost upon us, many people are focus on predictions and trends for the New Year. There are plenty of articles being published describing those predictions, but there's one that caught my eye: Hybrid Cloud Adoption set for Big Boost in 2015. The focus of the article is around analysis of the IDC numbers regarding past and projected growth in the cloud market. IDC predicts that the global cloud market, including private, public and hybrid clouds, will hit $118 billion in 2015 and crest at $200 billion by 2018, and average year-over-year growth of 25%.

This highlights the expanding needs today's enterprises are experiencing on two fronts. First, enterprises are increasingly moving to SaaS applications, such as Microsoft Office 365, Salesforce.com, Oracle, NetSuite, and SAP in ever-increasing numbers. On the other hand, enterprises are either deploying their own new applications or migrating existing ones to the cloud.

Moving to the cloud and SaaS applications is a very significant and drastic shifts for enterprises. There are many operational and scalability benefits that are achieved with these moves, but there are also new security challenges and end-user performance concerns that arise.

For example, when the enterprise is hosting their applications within their own datacenter and within their own WAN, they have much greater predictability and control over the QoS, round trip times, and predictability of service and capacity. However, when a company moves significant portion of its business-related applications to the cloud or migrates from in-house applications to SaaS, they are faced with new challenges, such as:

- A need to federate user's identity across disparate number of applications and SaaS providers
- End-user performance concern about page load times and overall application performance
- Additional load placed on external firewalls and the overall Internet pipe that needs to be accounted for
- The need for overall security and traffic prioritization control over the Internet pipe to ensure that non-business traffic is minimized and that cloud and SaaS applications are guaranteed certain bandwidth and are prioritized over viral YouTube videos du jour, for instance.

Fortunately, F5 has ability to help with every single one of those challenges. First, F5 BIG-IP Access Policy Manager (APM) is a a full-featured SAML Identity Provider(IdP) as well as Service Provider(SP), thereby facilitating the challenge of federating a user's local enterprise identity to the cloud and SaaS applications.   Many F5 customers have deployed APM to perform Cloud Identity Federation to SaaS applications such as Office 365, Salesforce.com,Brainshark, WebEx, Concur, Google apps, and more. Doing so allows customers to leverage APM's extensive capabilities in providing remote access, context-aware access control, and single sign-on(SSO) across the entire spectrum of the applications.

Secondly, let's consider the concern about application performance and end-user experience. Almost 10 years ago, F5 purchased Swan Labs and has been successfully integrating, refining, and improving that technology into F5 TMOS.

There is a fantastic ten-part series on DevCentral that goes into great detail on how F5 Application Acceleration Manager helps accelerate various web applications. While the focus and the context of web acceleration conversations have mostly been focused on the inbound reverse-proxy applications that customers have within their domain control(mostly due to SSL certificate issues), with the introduction of the SSL Forward Proxy feature in TMOS version 11.3, F5 has introduced the concept of SaaS acceleration, which leveraged the newly-introduced SSL Forward Proxy feature with the same application acceleration technology that has been successfully used to accelerate on-premise applications for many years.

Now, let's consider the challenge of controlling user's web access and prioritizing business over non-business traffic. With workers spending 60% of their day web-surfing for personal reasons, the need to control employee access to Internet-based sites and applications while prioritizing business-critical traffic in the wake of rising cloud and SaaS usage is now more important than ever. At the RSA 2014 conference, F5 launched Secure Web Gateway Services product. Riding on top of F5 BIG-IP Access Policy Manager, Secure Web Gateway(SWG) does many things to ensure that employee web access is as secure as possible. Combining SWG Services and APM's context-aware controls with the flexible bandwidth control mechanisms of the BIG-IP enables enterprises to achieve balance and prioritization of the business-related traffic, ensuring fast user access to and top performance of the cloud and SaaS applications.

When viewed individually, it may appear that F5 has three independent solutions addressing each of the challenges described earlier. And there are certainly other vendors that have relatively good products to address each individual challenge on their own. But the true strength and uniqueness of F5 comes to shine when you realize that you can achieve a great synergy and significant TCO savings by consolidating services, devices, security and acceleration policies within the footprint of one device - the BIG-IP platform - that can address all three challenges at the same time.

For starters, I wrote about combining enterprise web access control and federated identity management on the same device a few months ago. That's a unique value proposition that only F5 can offer today, all on the same device. Enterprises that are concerned with their user's productivity and satisfaction when accessing cloud and SaaS applications, can now combine the unique unparalleled trio of F5 Access Policy Manager(APM), Secure Web Gateway Services(SWG), and Application Acceleration Manager(AAM) to provide easy identity federation, improve employee productivity, and conserve Internet bandwidth and system resources (by leveraging Application Acceleration Manager), while simultaneously controlling and securitng context-based outbound web access through a single BIG-IP platform.