F5 Friday: Secure Remote Access versus En Masse Migration to the Cloud

Lori MacVittie, 2011-04-11

Being too quick to shout "cloud" when the solution may be found elsewhere can lead to unintended consequences.

As with all technology caught up in the hype cycle, cloud computing is often attributed with being "the solution" to problems irrespective of reality. Cloud is suddenly endowed with supernatural powers, able to solve every business and operational challenge merely by being what it is.

Take, for example, the attribution of cloud as being "the solution" to the very real issue of severe snow in the UK.

> Cloud solutions can help businesses to overcome severe weather issues – with your business' IT in the cloud, 100 percent of your staffs could work from home. Moreover, working in the cloud – anywhere, anytime – is good for your employees' morale: 76 percent said that off-premise working is great.
>
> http://www.thecloudinfographic.com/2011/10/27/cloud-computing-solves-severe-snow-problem.html

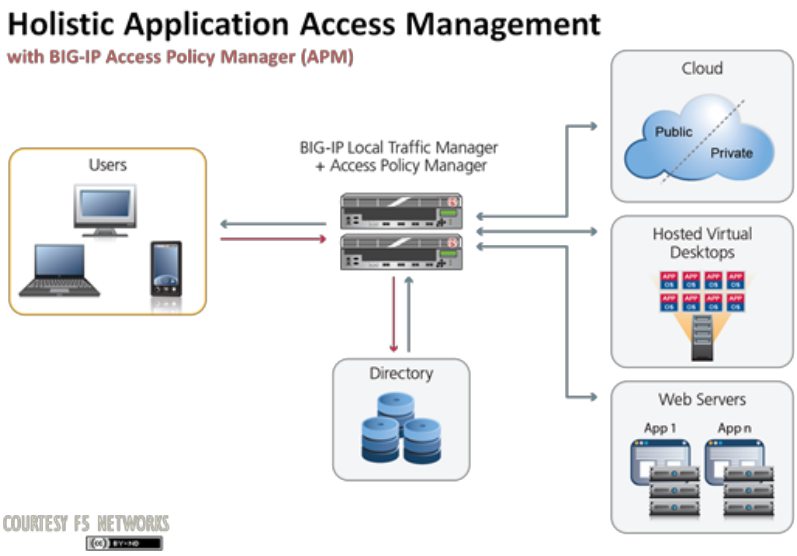
Now, the premise of this "solution" is that severe snow often prevents employees from working because they can't get to work or because they lack the means to do so. Given. The claim is that putting IT in "the cloud" (narrowly defined as Software as a Service only) eliminates these issues because employees can access the cloud from anywhere, including their homes during periods of severe weather.

One wonders why employees cannot simply access the same applications and resources at their corporate location. Has the business no Internet connectivity? Have they no web applications? Are they, perhaps, the last holdouts against the electronic age? The real solution here has nothing to do with cloud, it is enabling remote access. Cloud computing as part of the strategy to enable that solution is certainly valid, but it isn't the solution, it's part of a strategy – a remote access strategy.

OPERATIONAL CONSISTENCY

The reason touting "cloud" as a the "solution" to snow-bound employee access is somewhat misguided is twofold. First, it completely ignores the need for enterprise-grade security. Simply put "IT" (as if one can move an enterprise-grade data center wholesale) in the cloud and voila! Instant, ubiquitous, access. Granted, the purported solution is SaaS, which implies some level of credentials are required for access, but in doing so it completely ignores the second issue: it assumes all IT functions are commoditized to the point they are offered "as a service" in the first place, which is utterly untrue at this point in the evolution of any kind of cloud.

This conflation further dismisses the costs and importance of integration to those systems being "moved" en masse to the cloud, and seems not at all concerned with the operational management costs of now needing to manage not one but perhaps multiple cloud environments. As my toddler would say, "Are you *seriously*?"



Interestingly, before cloud computing came along and became the answer to life, the universe and everything, there was a less disruptive solution to the problem of remote access and business continuity: secure remote access.

One of the foremost capabilities provided by secure remote access solutions, like BIG-IP Access Policy Manager (APM), is that of supporting telecommuting. Having been a telecommuter for over a decade now I've never had access to corporate resources *without* the assistance of some kind of remote access (VPN) solution.

There are simply too many pieces and parts (resources and applications and services) that are too sensitive to leave unprotected "in the cloud." Now that's not saying a cloud isn't secure, it's saying that it's not (currently) enabled with the same level of security and support for secure access best practices required by both operational and business stakeholders.

I absolutely agree with the premise that severe weather and other mitigating factors that prevent employees from getting to work is costly to the business. But the solution is not likely to be a wholesale migration of its data center to a cloud, it's to enable remote access without disrupting existing security and access policies. The bonus is that using BIG-IP APM can actually enable a migration of applications or services to a cloud environment without sacrificing the control necessary to consistently replicate and enforce access policies.

CLOUD is FOR EVERYONE but NOT for EVERYTHING

"Cloud is for everyone, but not for everything." (Rackspace) That is especially true in this case, but even more so when folks are conflating a solution with its model and location because it fails to address the root cause and instead tries to force fit "cloud" as being an integral part of every solution to every IT challenge.

Cloud is not a solution, but a deployment option that has both advantages and disadvantages over traditional data center-based deployments. While the issue with severe weather is certainly real, claiming "cloud" is a solution is shortsighted and fails to recognize the difficulties inherent in such an "en masse" migration. Unfortunately the reply of "cloud" as though it's answer D (all of the above) to every operational and business challenge we encounter will continue to be an issue until the hype cycle finally tires of hearing itself talk and we can get down to the real business of exploiting "the cloud" in ways that are not only meaningful but that do not introduce myriad other (costly and potentially risk inducing) challenges.

In this case, a secure remote access solution – BIG-IP Access Policy Manager – is a much better option for folks who are annually plagued by productivity and cost woes due to severe weather. Rather than transplant applications from the data center to a cloud, and likely losing in the process the control and enforcement of security and access policies necessary to comply with regulations and business requirements, enable secure remote access. Keep the control, leverage the flexibility, maximize the benefits.

Happy Working from Home!

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