

Once Again, it Really IS About the Applications.



Don MacVittie, 2011-20-09

(Booming voiceover voice); Are you running the same tired old network tools? Does your network staff have to administer security and load balancing for each and every application? Do you find application analysts and owners show a growing frustration with the network team's response times due to overloading? Well get in there and fix that network! Get the tools that you need to make your network more application friendly, reduce fatigue amongst your network staff, and give application owners more control of their applications!



That was, of course, a joke poking fun at both the way we run our networks and the advertisement that tries to sell by listing common problems in a booming voice. But as is almost always the case, there's a grain of serious in that joke.

Many organizations have their infrastructure configured such that the networking staff must intercede with a lot of functionality that is in the application domain. Be it more capacity, granular security, or routing to a new instance of the application, the network staff carries these burdens, while the application staff waits for them to do so and in many cases, the application owner gets frustrated.

But the days when ADC functionality – be it security, adding servers, or shipping connections to a remote instance of the application – had to rest completely in the realm of networking staff are behind us. If you still have those problems, you need to look into a state-of-the-art ADC (yes, like F5 sells, but we *do* have competition if you prefer). Assuming the application people can spin up new instances, they can also get them included in the ADC's available servers. Since most application folks *can* spin up a new instance, this extra step means less waiting around for another team. When security issues crop up relative to a particular application, you'll have the application owner, systems administrators, security... Do you really need to throw the network folks in there too? You used to have to, but technology has relieved that burden. When application owners (or sysadmins) can administer the security policy for a given application, then they just need the advice of the security team (assuming you're a big enough org to have a security team). This not only makes the organization more nimble, it reduces errors by having those directly responsible for the application implementing policy for the application without a middle-man.

Need to do cloud-bursting? The networking team needs to set that all up for you, but once it's configured and the application can take advantage of it, then when/where/how is up to the application staff, not the networking team. Again, more agile.

Just in terms of reducing burden on the networking staff, and thus making them more productive on the other important things they need to do, the move to a newer ADC is worth it. But throw in the concept that the application staff is also empowered to act without waiting to consult with yet another busy team, and the improved IT response time makes the overall organization more adaptable.

If you choose an ADC that also resolves other pressing issues your organization has, you can really drive home solutions, while laying the groundwork for future architectural developments. Pick an ADC that enhances VMotion over long distances, for example, and moving apps from DC-to-DC becomes simple and reliable.

So if your load balancing solution is just that – load balancing – it is time to look into where the market has gone. If you use a command line for most of your ADC configuration and management, it is again time to check where the market has gone. Enable applications staff to free up time for networking staff. And take advantage of a whole new set of capabilities while you're at it. Explore what's out there that might just make your life easier and your company more productive. And if you have an older solution, check out scalability too. Things have come a long way in a few short years, that's for sure.

That's not to say that you shouldn't have a command line – F5's tmsh is a complete command line version of the UI – but not everyone wants to type 50 lines of script when one webpage will do, and to push functionality out beyond the network team, web interfaces are definitely needed, both to increase accessibility and to reduce errors.

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113