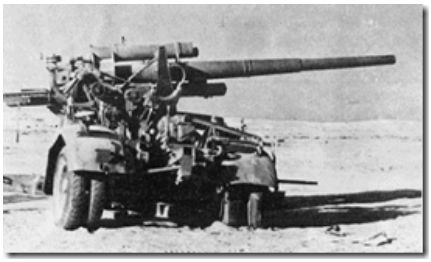
Force Multipliers and Strategic Points of Control Revisited

Don MacVittie, 2011-31-03



On occasion I have talked about military ***force multipliers.*** These are things like terrain and minefields that can make your force able to do their job much more effectively if utilized correctly. In fact, a study of military history is every bit as much a study of battlefields as it is a study of armies. He who chooses the best terrain generally wins, and he who utilizes tools like minefields effectively often does too. Rommel in the desert often used Wadis to hide his dreaded 88mm guns – that at the time could rip through any tank the British fielded. For the last couple of years, we've all been inundated with the story of ***The 300*** Spartans that held off an entire army. Of course it was more than just the 300 Spartans in that pass, but they were still massively outnumbered. Over and over again throughout history, it is the terrain and the technology that give a force the edge. Perhaps the first person to notice this trend and certainly the first to write a detailed work on the topic was von Clausewitz. His writing is some of the oldest military theory, and much of it is still relevant today, if you are interested in that type of writing.

For those of us in IT, it is much the same. He who chooses the best architecture and makes the most of available technology wins. In this case, as in a war, winning is temporary and must constantly be revisited, but that is indeed what our job is – keeping the systems at their tip-top shape with the resources available. Do you put in the tool that is the absolute best at what it does but requires a zillion man-hours to maintain, or do you put in the tool that covers everything you need and takes almost no time to maintain? The answer to that question is not always as simple as it sounds like it should be. By way of example, which solution would you like your bank to put between your account and hackers? Probably a different one than the one you would you like your bank to put in for employee timekeeping.

An 88 in the desert, compliments of WW2inColor

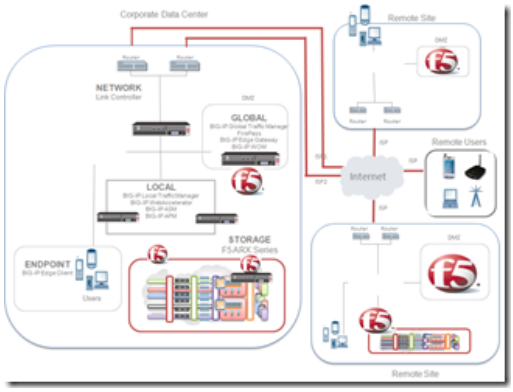
Unlike warfare though, a lot of companies are in the business of making tools for our architecture needs, so we get plenty of options and most spaces have a happy medium. Instead of inserting all the bells and whistles they inserted the bells and made them relatively easy to configure, or they merged products to make your life easier.

When the terrain suits a commanders' needs in wartime, the need for such force multipliers as barbed wire and minefields are eliminated because an attacker can be channeled into the desired defenses by terrain features like cliffs and swamps. The same could be said of your network. There are a few places on the network that are Strategic Points of Control, where so much information (incidentally including attackers, though this is not, strictly speaking, a security blog) is funneled through that you can increase your visibility, level of control, and even implement new functionality. We here at F5 like to talk about three of them… Between your users and the apps they access, between your systems and the WAN, and between consumers of file services and the providers of those services. These are places where you can gather an enormous amount of information and act upon that information without a lot of staff effort – force multipliers, so to speak.

When a user connects to your systems, the strategic point of control at the edge of your network can perform pre-application-access security checks, route them to a VPN, determine the best of a pool of servers to service their requests, encrypt the stream (on front, back, or both sides), redirect them to a completely different datacenter or an instance of the application they are requesting that actually resides in the cloud… The possibilities are endless. When a user accesses a file, the strategic point of control between them and the physical storage allows you to direct them to the file no matter where it might be stored, allows you to optimize the file for the pattern of access that is normally present, allows you to apply security checks before the physical file system is ever touched, again, the list goes on and on. When an application like replication or remote email is accessed over the WAN, the strategic point of control between the app and the actual Internet allows you to encrypt, compress, dedupe, and otherwise optimize the data before putting it out of your bandwidth-limited, publicly exposed WAN connection.

The first strategic point of control listed above gives you control over incoming traffic and early detection of attack attempts. It also gives you force multiplication with load balancing, so your systems are unlikely to get overloaded unless something else is going on. Finally, you get the security of SSL termination or full-stream encryption. The second point of control gives you the ability to balance your storage needs by scripting movement of files between NAS devices or tiers without the user having to see a single change. This means you can do more with less storage, and support for cloud storage providers and cloud storage gateways extends your storage to nearly unlimited space – depending upon your appetite for monthly payments to cloud storage vendors. The third force-multiplies the dollars you are spending on your WAN connection by reducing the traffic going over it, while offloading a ton of work from your servers because encryption happens on the way out the door, not on each VM.

Taking advantage of these strategic points of control, architectural force multipliers offers you the opportunity to do more with less daily maintenance. For instance, the point between users and applications can be hooked up to your ADS or LDAP server and be used to authenticate that a user attempting to access internal resources from… Say… and iPad… is indeed an employee before they ever get to the application in question. That limits the attack vectors on software that may be highly attractive to attackers. There are plenty more examples of multiplying your impact without increasing staff size or even growing your architectural footprint beyond the initial investment in tools at the strategic point of control.



For F5, we have LTM at the Application Delivery Network Strategic Point of Control. Once that investment is made, a whole raft of options can be tacked on – APM, WOM, WAM, ASM, the list goes on again (tired of that phrase for this blog yet?). Since each resides on LTM, there is only one “bump in the wire”, but a ton of functionality that can be brought to bear, including integration with some of the biggest names in applications – Microsoft, Oracle, IBM, etc.

Adding business value like remote access for devices, while multiplying your IT force. I recommend that you check it out if you haven’t, there is definitely a lot to be gained, and it costs you nothing but a little bit of your precious time to look into it.

No matter what you do, looking closely at these strategic points of control and making certain you are using them effectively to meet the needs of your organization is easy and important. The network is not just a way to hook users to machines anymore, so make certain that’s not all you’re using it for. Make the most of the terrain.

And yes, if you also read Lori's blog, we were indeed watching the same shows, and talking about this concept, so no surprise our blogs are on similar wavelengths.

Related Blogs:

- What is a Strategic Point of Control Anyway?
- Is Your Application Infrastructure Architecture Based on the ...
- F5 Tech Field Day – Intro To F5 As A Strategic Point Of Control
- What CIOs Can Learn from the Spartans
- What We Learned from Anonymous: DDoS is now 3DoS
- What is Network-based Application Virtualization and Why Do You ...
- They're Called Black Boxes Not Invisible Boxes
- Service Virtualization Helps Localize Impact of Elastic Scalability
- F5 Friday: It is now safe to enable File Upload

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