He Who Defends Everything Defends nothing&hellip; Right?

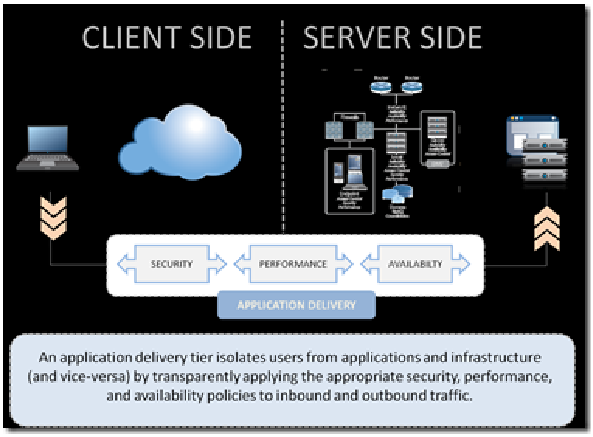
Don MacVittie, 2011-22-11

There has been much made in Information Technology about the military quote: “He Who Defends Everything Defends Nothing” – Originally uttered by Frederick The Great of Prussia. He has some other great quotes, check them out when you have a moment. The thing is that he was absolutely correct in a military or political context. You cannot defend every inch of ground or even the extent of a very long front with a limited supply of troops. You also cannot refuse to negotiate on all points in the political arena. The nature of modern representative government is such that the important things must be defended and the less important offered up in trade for getting other things you want or need. In both situations, demanding that everything be saved results in nothing being saved. Militarily because you will be defeated piecemeal with your troops spread out, and politically because your opponent has no reason to negotiate with you if you are not willing to give on any issue at all.

But in high tech, things are a little more complex. That phrase is most often uttered to refer to defense against hacking attempts, and on the surface seems to fit well. But with examination, it does not suit the high-tech scenario at all. While defense in depth is important in datacenter defense, just in case someone penetrates your outer defenses. But we all know that there are one or two key choke-points that allow you to stop intruders who do not have inside help – your Internet connections. If those are adequately protected, the chances of your network being infiltrated, your website taken down, or any of a million other ugly outcomes are much smaller.

The problem, in the 21st century, is the definition of “adequate”. Recent attacks have taken down firewalls previously assumed to be “adequate”, and the last several years have seen a couple of spectacular DNS vulnerabilities focusing on a primary function that had seriously seen little attention from attackers or security folks. In short, the entire face you present to the world is susceptible to attack. And at the application layer, attacks can slip through your outer defenses pretty easily.

That’s why the future network defensive point for the datacenter will be a full proxy at the Strategic Point of Control where your network connects to the Internet. Keeping attacks from dropping your network requires a high-speed connection in front of all available resources. The Wikileaks attacks took out a few more than “adequate” firewalls, while the DNS vulnerabilities attacked DNS through its own protocol. A device in the strategic point of control between the Internet and your valuable resources needs to be able handle high-volume attacks and be resilient enough to respond to new threats be they at the protocol or application layers.



An application delivery tier isolates users from applications and infrastructure (and vice-versa) by transparently applying the appropriate security, performance, and availability policies to inbound and outbound traffic.

It needs to be intelligent enough to compare user/device against known access allowances and quarantine the user appropriately if things appear fishy. It also needs to be adaptable enough to adapt to new attacks before they overwhelm the network. Zero day attacks by definition almost never have canned fixes available, so waiting for your provider to plug the hole is a delay that you might not be able to afford.

That requires the ability for you to work in fixes and an environment that encourages the sharing of fixes – like DevCentral or a similar site. So that you can quickly solve the problem either by identifying the problem and creating a fix, or by downloading someone else’s fix and installing it. While an “official” solution might follow, and eventually the app will get patched, you are protected in the interim.

You *can* defend everything by placing the correct tool at the correct location. You can manage who has access to what, from which devices, when, and how they authenticate. All while protecting against DOS attacks that cripple some infrastructures. That's the direction IT needs to head. We spend far too many resources and far too much brainpower on defending rather than enabling. Time to get off the merry-go-round, or at least slow it down enough that you can return your focus to enabling the business and worry less about security. Don't expect security concerns will ever go away though, because we can – and by the nature of the threats must – defend everything.

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