Mature Security Organizations Align Security with Service Delivery

Lori MacVittie, 2012-12-01

#adcfw #RSAC *Traditional strategy segregates delivery from security. Traditional strategy is doing it wrong…*

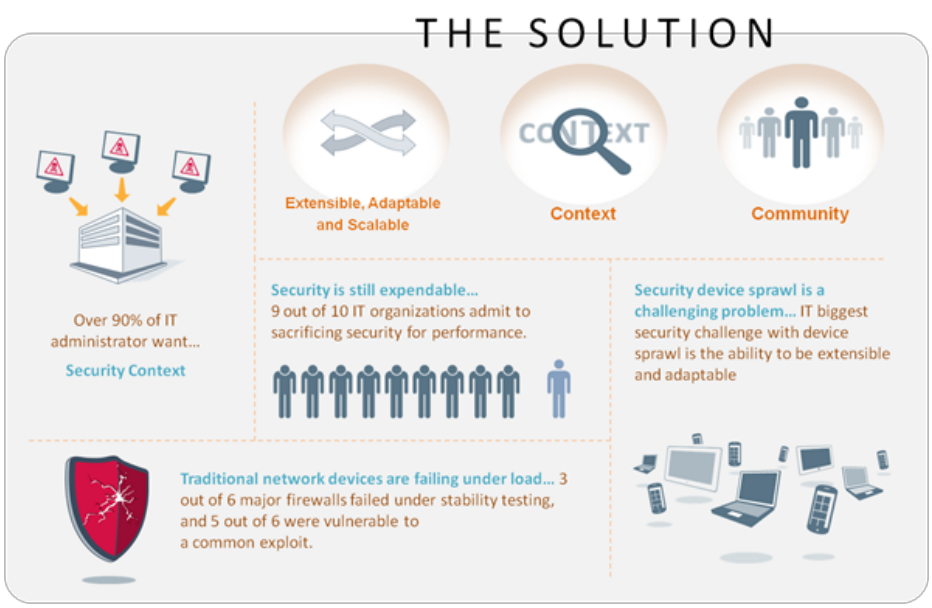
Everyone, I'm sure, has had the experience of calling customer service. First you get the automated system, which often asks for your account number. You know, to direct you to the right place and "serve you better." Everyone has also likely been exasperated when the first question asked by a customer service representative upon being connected to a real live person is … "May I have your account number, please?"

It's frustrating and, for everyone involved, it's cumbersome.

That's exactly the process that occurs in most data centers today as application requests are received by the firewall and then passed on to the service delivery layer.

Traditional data center design segregates security from service delivery. There's an entire complement of security-related components that reside at the perimeter of the network, designed to evaluate incoming traffic for a wide variety of potential security risks – DDoS, unauthorized access, malicious packets, etc… But that evaluation is limited to the network layers of the stack. It's focused on packets and connections and protocols, and fails to take into consideration the broader contextual information that is carried along by every request. It's asking for an account number but failing to leverage it and share it in a way that effectively applies and enforces corporate security policies.

It's cumbersome.



Reality is that many of the functions executed by firewalls are duplicated in the application delivery tier by service delivery systems. What's more frustrating is that many of those functions are executed more thoroughly and to better effect (i.e. they mitigate risk more effectively) at the application delivery layer.

What should be frustrating to those concerned with IT budgets and operational efficiency is that this disconnected security strategy is more expensive to acquire, deploy, and maintain. Using shared infrastructure is the hallmark of a mature security organization; it's a sign of moving toward a more strategic security strategy that's not only more technically adept but is financially sound.

SHARED INFRASTRUCTURE

We most often hear the term "shared infrastructure" with respect to cloud computing and its benefits. The sharing of infrastructure across organizations in a public cloud computing environment nets operational savings not only from alleviating the need to manage the infrastructure from the fact that the capital costs are shared across hundreds if not thousands of customers.

Inside the data center private cloud computing models are rising to the top of the “must have” list for IT for similar reasons. In the data center, however, there are additional technical and security benefits that should not be overlooked. Aligning corporate security strategy with the organizations’ service delivery strategy by leveraging shared infrastructure provides a more comprehensive, strategic deployment that is not only more secure, but more cost effective.

Service delivery solutions already provide a wide variety of threat mitigation services that can leveraged to mitigate the performance degradation associated with a disjointed security infrastructure, the kind that leads 9 of 10 organizations to sacrifice that security in favor of performance. By leveraging shared infrastructure to perform both service delivery acceleration as well as security, neither performance nor security need be sacrificed because it essentially aligns with the mantra of the past decade with regards to performance and security: crack the packet only once.

In other words, don’t ask the customer for their account number twice. It’s cumbersome, frustrating, and an inefficient means of delivering any kind of service.

- F5 Friday: When Firewalls Fail…
- At the Intersection of Cloud and Control…
- F5 Friday: Multi-Layer Security for Multi-Layer Attacks
- 1024 Words: If Neo Were Your CSO
- F5 Friday: No DNS? No … Anything.
- F5 Friday: Performance, Throughput and DPS
- When the Data Center is Under Siege Don’t Forget to Watch Under the Floor
- Challenging the Firewall Data Center Dogma
- What We Learned from Anonymous: DDoS is now 3DoS
- The Many Faces of DDoS: Variations on a Theme or Two

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