Don’t Conflate Virtual with Dynamic

Lori MacVittie, 2011-10-01

Focusing on form factor over function is as shallow and misguided as focusing on beauty over brains.

The saying goes that if all you have is a hammer, everything looks like a nail. I suppose then that it only makes sense that if the only tool you have for dealing with the rapid dynamism of today's architectural models is virtualization that everything looks like a virtual image. Virtualization is but one way of implementing a dynamic infrastructure capable of the rapid provisioning and configuration gyrations needed to address the fluidity of the "perimeter" of the network today.

Dynamic is not a synonym for virtualization and virtualization does not inherently provide the fluidity of the network architecture required to address the challenges associated with highly dynamic environments.

COMPLEXIFICATION

Consider for a moment the conclusion that the perimeter must become virtual because it is trying to contain a moving target:

> In the world of cloud infrastructures (IaaS), it is not so easy to determine the "area" that is supposed to be surrounded. Resources are shared among different clients (multi-tenancy) and they are allocated in data-centers of external providers (outsourcing). Moreover, computing resources get virtual – physical resources are transparently shared – and elastic – they are allocated and destroyed on demand. Since this can be done via APIs in a programmable and automated way, cloud computing infrastructures are highly dynamic and volatile. How can one build a perimeter around a moving target?
>
> Well, the short answer is: the perimeter must also become virtual, highly dynamic, and automated.
>
> -- Why The Perimeter Must Become Virtual

There are a number of issues this raises, not the least of which is the mechanism for scaling and managing such a virtual perimeter especially given the topological sensitivity to a variety of network-hosted services, especially those that are focused on security. I'll simply paraphrase Hoff at this point from his "The Four Horsemen of the Virtualization Security Apocalypse" – there are issues with a fully virtualized approach to security around topology, routing, scalability, and resiliency. In short, there are myriad architectural challenges associated with a fully virtualized approach to enabling a dynamic data center model.

[An easy answer as to why security and virtual network devices aren't always compatible is any situation in which FIPS-140 Level 2 compliance is necessary.]

That's in addition to the complexity introduced by replacing what are high-speed network components capable of handling upwards of 40 and 100 Gbps with commodity hardware, limited compute resources, and constrained network connections. Achieving similar throughput rates using virtual components will require multiple instances of the virtual network appliance which introduce architectural and topological challenges that must be addressed, not the least of which is controlling flow which subsequently introduces overhead that will negatively impact those throughput rates. This also assumes that the protocols typically associated with the network perimeter will scale across multiple, dynamic instances without noticeable disruption to services. If you've ever changed a routing table or a VLAN on a router and then had to wait for spanning tree to converge you'll know what I'm talking about. It's anything but rapid and will almost certainly have a detrimental effect on availability of every dependent service (which, at the network perimeter, is everything).

IT'S NOT ABOUT THE FORM FACTOR

In order to implement the kind of dynamic network perimeter introduced by the author of "Why The Perimeter Must Become Virtual" we do, in fact, need a more flexible, automated perimeter.

However, that perimeter does not have to be virtual and in fact the key to implementing such a fluid network is the inherent dynamism of its components, not its form factor. If the components are dynamic themselves – programmable, if you will – and can be configured, deployed, modified and shut-down automatically and on-demand then they ***can*** be leveraged to address the dynamism inherent in a cloud computing and highly virtualized architectural model. Because they can be integrated. Because they are collaborative.

The strategic points of control that exist in every data center model must be dynamic – both from a configuration and execution point of view. Not only must the components that form a strategic net across the data center - effectively virtualizing business resources such as applications and storage – be dynamic in their management they must themselves be contextually aware and capable of taking action at run-time.

The kind of dynamic action required to address "moving targets" is not inherent in virtualization. Virtualizing a component only makes provisioning easier. Without a means to remotely invoke services (APIs) and modify configuration dynamically (APIs) as well as the means by which the component can dynamically adjust its behavior based on events within the data center, a virtualized component is little more than a virtual brick. Fluidity of the network is not a result of virtualization.

There are myriad examples already of how traditional "iron" not only enables but stabilizes the management and control of dynamic environments. Programmability, on-demand contextual-awareness, APIs, scripting, policy-based networking. All these capabilities enable the fluidity necessary to address the "moving targets" comprising cloud-based and highly virtualized modern data center models, but without the instability created by the lack of topological and architectural control inherent in a "toss another virtual appliance" at the problem approach. It's more about designing an architecture comprised of highly dynamic and interactive components that can be provisioned ***and managed*** on-demand, as services.

Yes - dynamic, highly automated data centers are necessary to combat the issues arising from constantly changing infrastructure. But dynamism and automation do not require virtualization, they require collaboration and integration and a platform capable of providing both.

- Provisioning a Virtual Network is Only the Beginning
- The Four Horsemen Of the Virtualization Security Apocalypse
- Why The Perimeter Must Become Virtual
- Are You Ready for the New Network?
- VM Sprawl is Bad but Network Sprawl is Badder
- The Devil is in the Details
- Infrastructure 2.0 + Cloud + IT as a Service = An Architectural Parfait

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