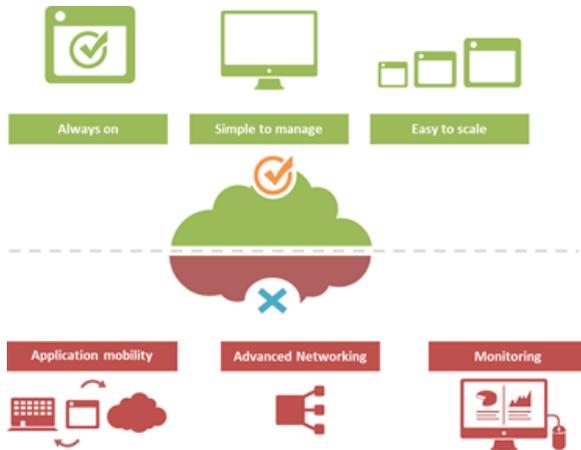


The Limits of Cloud: NICS and Nets



Lori MacVittie, 2012-11-12

#Cloud is great at many things. At other things, not so much. Understanding the limitations of cloud will better enable a successful migration strategy.



You might have noticed that in general, enterprise-grade networking solutions aren't always available for general deployment in public cloud environments.

You might also have noticed that when you provision a compute instance in a public cloud environment you get one public (and usually one private) IP address.

I'll stop for a moment and let you consider the relationship between these two facts.

Many mature enterprise-grade networking solutions require at least two network interfaces – one for traffic (data plane) and one for management (control plane) and often suggest a third

for optimal, best-practice deployment. It's been a long time since I've seen mature networking solutions that don't employ segregated management networks. Those solutions that sit inline and that are in the line of fire, as you will, from concentrated network and application-layer attacks, absolutely need segregated management as a means to control the solution and mitigate an in-progress attack or sudden spike in utilization that might be overwhelming the primary network.

The use of a separate management network also ensures that the control plane is secured from general access.

Generally speaking, it's been considered a best-practice to use a separate, secured management network for critical network components since the web exploded.

Unfortunately, most cloud environments don't support this capability for customers. While certainly cloud is the largest example of control-data plane separation, such environments are designed to transport control of provider functions and service-control, not customer-deployed solutions. Thus the instances provisioned by the customer are expected to exist on the data plane because management functions (control plane) are handled through the provider's framework / API.

That means vendors of mature, enterprise-grade networking solutions have few options for cloud-enabling their solutions when NICs (and networks) are limited. Amazon EC2 is one such environment; it currently does not support multiple IP addresses per instance. Simply AML-enabling a networking solution that requires a separate management network is not going to be enough.

That's why you see enterprise-class networking solutions becoming available for Amazon AWS, but only in its Virtual Private Cloud (VPC) environment. In the VPC environment instances are able to take advantage of more advanced networking capabilities familiar to enterprise operations such as control over IP address ranges, creation of subnets, and configuration of routes and network gateways.

[Rackspace](#), on the other hand, is moving toward enabling multiple networks [capable of broadcasting and multicasting](#) through its [evolving support for OpenStack](#). Such capabilities will enable customers to take advantage of mature networking solutions within its environment. There are restrictions, of course, as will be the case with any provider, but in general such a move toward enabling advanced networking within open cloud environments is a positive one.

What this all means is that when considering cloud providers and migration of applications (and their supporting infrastructure) it is critical to seek out and understand what advanced networking capabilities are – or aren't – available for each provider you are evaluating. Infrastructure support is a key component for many enterprise-class applications now being considered for migration to the cloud and not all clouds will be able to equally support the advanced networking services necessary.

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