Do you control your application network stack? You should.

Lori MacVittie, 2009-25-02

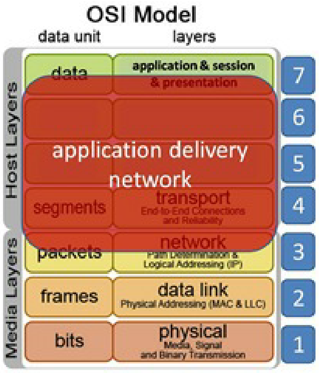
Owning the stack is important to security, but it's also integral to a lot of other application delivery functions. And in some cases, it's downright necessary.

Hoff rants with his usual finesse in a recent posting with which I could not agree more. Not only does he point out the wrongness of equating SaaS with "The Cloud", but points out the importance of "owning the stack" to security.

> *Those that have control/ownership over the entire stack naturally have the opportunity for much tighter control over the "security" of their offerings. Why? because they run their business and the datacenters and applications housed in them with the same level of diligence that an enterprise would.*
>
> *They have context. They have visibility. They have control. They have ownership of the entire stack.*

Owning the stack has broader implications than just security. The control, visibility, and context-awareness implicit in owning the stack provides much more flexibility in all aspects covering the delivery of applications. Whether we're talking about emerging or traditional data center architectures the importance of owning the application networking stack should not be underestimated.

The arguments over whether virtualized application delivery makes more sense in a cloud computing-based architecture fail to recognize that a virtualized application delivery network *forfeits that control* over the stack. While it certainly maintains some control at higher levels, it relies upon other software – the virtual machine, hypervisor, and operating system – which shares control of that stack and, in fact, processes all requests *before* it reaches the virtual application delivery controller.


OSI Model
data unit
layers
Host Layers
Media Layers
data
application & session & presentation
application delivery network
segments
transport
End-to-End Connections and Reliability
packets
network
Path Determination & Logical Addressing (IP)
frames
data link
Physical Addressing (MAC & LLC)
bits
physical
Media, Signal and Binary Transmission
7
6
5
4
3
2
1

This is quite different from a hardened application delivery controller that maintains control over the stack and provides the means by which security, network, and application experts can tweak, tune, and exert that control in myriad ways to better protect their unique environment.

If you don't completely control layer 4, for example, how can you accurately detect and thus prevent layer 4 focused attacks, such as denial of service and manipulation of the TCP stack? You can't. If you don't have control over the stack at the point of entry into the application environment, you are risking a successful attack.

As the entry point into application, whether it's in "the" cloud, "a" cloud, or a traditional data center architecture, a properly implemented application delivery network can offer the control necessary to detect and prevent myriad attacks at every layer of the stack, without concern that an OS or hypervisor-targeted attack will manage to penetrate before the application delivery network can stop it.

The visibility, control, and contextual awareness afforded by application delivery solutions also allows the means by which finer-grained control over protocols, users, and applications may be exercised in order to improve performance at the network and application layers. As a full proxy implementation these solutions are capable of enforcing compliance with RFCs for protocols up and down the stack, implement additional technological solutions that improve the efficiency of TCP-based applications, and offer customized solutions through network-side scripting that can be used to immediately address security risks and architectural design decisions.

The importance of owning the stack, particularly at the perimeter of the data center, cannot and should not be underestimated. The loss of control, the addition of processing points at which the stack may be exploited, and the inability to change the very behavior of the stack at the point of entry comes from putting into place solutions incapable of controlling the stack.

If you don’t own the stack you don’t have control. And if you don’t have control, who does?

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