F5 Firewall Like No Other - Bringing Proxy Back

David Holmes, 2013-07-08

Who doesn't love a Justin Timberlake reference when talking about security technology? The guy helped bring back the Fedora, which I am pleasantly delighted to see on the heads of hipsters and kids all over the place.

In this third and final blog entry on what makes the F5 firewall different from all the others, let's think about what F5 is bringing back.

Starting with the original Firewall Toolkit in the 90's, the full proxy has been the best, most-flexible firewall solution. By using one connection to the client and a completely separate connection with the server, a full proxy can validate the inbound data before establishing and consuming server resources. For example, a full proxy is much more resilient to a TCP replay attack than a typical FPGA-based firewall.

The firewall industry went away from full proxy architecture for two reasons:

1. There were too many protocols to support. Back then it wasn't just Internet Protocol, it was SNA and IPX, too, and a dozen other protocols we don't even remember. Each time any of the dozen changed, it required the proxy to change. It was too difficult to maintain all the different proxies.
2. With the much slower CPUs of the 90s, performance became an issue as the Internet exploded and full proxy firewalls were not able to keep up. Eventually firewall vendors had to switch to FPGAs which were not smart enough to be full proxy but could process individual packets faster.
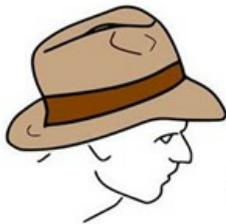
"F5 Is Bringing Proxy Back"

F5's Advanced Firewall Manager (AFM) module is bringing full proxy back as the right security solution. This is possible now for two reasons.

1. The network protocol space has converged around TCP, DNS, SIP, HTTP and SSL. These are also the protocols that F5 specializes in. Everything is converging our way and our customers and analysts know it.

2. F5 has spent over ten years building the world's fastest full proxy traffic management microkernel for these four protocols. It is multi-processor capable and hardware-assisted. We have millions and millions of lines of custom code and custom hardware devoted specifically to the full proxy for just these popular protocols. All that development is a significant barrier to entry for anyone wanting to do what we do. Even if others come around to our way of thinking, it will take some time before they can start to compete.

What? You say you want some proof about the virtues of the full proxy solution for firewalling?

Here is a **short list** of threat vectors that are mitigated just by the virtue of a full proxy firewall:

Layer	Threat	Mitigated?
4	TCP Replay	Yes
4	SYN+FIN Floods	Yes
4	SYN Floods	Yes
5	SSL Replay	Yes

5	SSL Empty flood	Yes
7	Slowloris	Yes
7	HTTP Floods	Yes

That's just off the top of our heads. Hopefully you get the picture. If your firewall isn't full proxy, is it blocking modern threats? Or is it relying on another full proxy device (like an F5 load – balancer) to pick up the slack?

The full proxy is back. The fedora is back, too. Interesting times we live in.

Connect with David: Connect with F5:

Related blogs & articles:

F5 Firewall Like No Other – Application-Centric Logging

F5 Firewall Like No Other – Ruling the Application

Whitepaper: Replacing Abstract Zones with Real Application Security Policy

Whitepaper: The New Data Center Firewall Paradigm