# Full (proxy) Security

**Lori MacVittie, 2007-13-12**

With the increasing number of "data leaks" involving large numbers of affected consumers there is an increased focus on products that prevent such leaks from occurring in the first place. Many of these products have grown out of the IDS (Intrusion Detection System) market and others have been built from the ground up. Some, like F5's BIG-IP Application Security Manager (ASM), have grown out of the WAF (Web Application Firewall) product set.

So what's the difference between them?

One of the biggest differentiators in these product sets is the way in which they are deployed, which is necessitated by their architecture. Products coming out of the IDS space tend to be passive monitors that attempt to recreate streams of data and, upon discovering a potential leak, try to stop the flow of traffic (generally referred to as 'quarantining' the traffic).

Products built atop a full proxy architecture, like ASM and F5 BIG-IP Local Traffic Manager (LTM), can be active monitors because its architecture is such that they are ***part*** of the flow of traffic and therefore less error-prone than their passively deployed cousins. Products that are full proxies provide inherently better security because they actively terminate the flow of data, essentially creating an "air gap" security model inside the product. Traffic coming from the client can be examined ***before*** it is sent on its way to the application tier, ensuring that malicious traffic never passes the proxy barrier. Traffic returning from the server can be fully examined ***before*** it is deemed acceptable to pass back to the client, thereby ensuring that sensitive data such as credit-card or social-security numbers are never passed across the proxy barrier.

Products built on a passive model don't have the luxury of being able to stop traffic in its tracks because they aren't part of the flow of traffic. They must rely on other mechanisms, such as using a TCP reset, in order to prevent data leaks or stop malicious code from entering the data center. Unfortunately, TCP reset mechanisms can result in a race-condition - that is, will the TCP RST reach the offending client ***before*** it receives the real response or will it arrive ***after,*** at which point the process has essentially failed.

Data leak protection is only one of the many security features that can be offered by full-proxy based solutions. The ability to sit in between the flow of data and inspect the data before allowing it to continue - in either direction - offers the opportunity to apply security in many ways to the data including protocol sanitization, resource obfuscation, and signature-based scanning.

It's tempting to give in to the alluring cry of easier configuration and deployment offered by passive monitoring based security systems. A passive deployment is easier, no doubt, but the risks of deploying such a system for the purposes of preventing data leaks are also higher. Consider carefully whether you're willing to accept the risks associated with products based on passive monitoring techniques or if you'd prefer to spend a bit more time up front configuring and deploying a full-proxy based solution in exchange for lowering your risk of being compromised.

*Imbibing: Water*

Technorati tags: MacVittie, F5, security, full proxy, data leaks

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