Programmable Proxies are the Duct Tape of the Internet

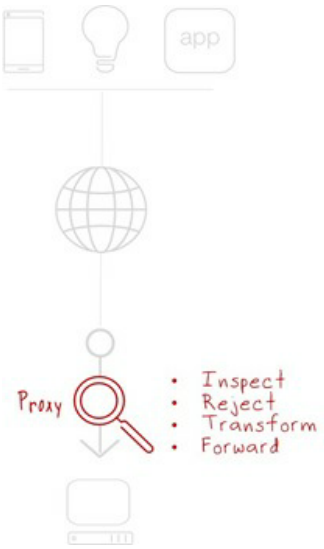
Lori MacVittie, 2017-14-08

Programmable proxies protect ports from predators – like those targeting SMB today.

When the Internet was in its infancy, my three oldest children were teenagers. Even then – with a far smaller Internet - unfettered access was not something we wanted to allow. Trust me, kids type the darndest things into browser address bars. Despite the proliferation today of "parental controls", back then we had to build out own out of duct tape and bailing wire.

Okay, we actually used Squid but that doesn't sound as cool. Still, it is the point of this post. Not Squid, per se, but the use of a proxy as something other than a mechanism for load balancing web applications.

See, proxies aren't just for web apps today. They can be used to control just about any traffic you want, on any port. While at home we used Squid primarily to control outbound Internet web traffic for three curious teenagers, in the office we employed it to provide a central location for logging outbound traffic to understand why we chewed up so much bandwidth with so few employees.



There are plenty of examples of using proxies to gate outbound access to the Internet, and unsurprisingly plenty of examples on the inbound route as well.

Proxies are the basis for load balancing, for access control, for translation (gateways) and a wealth of other "network hosted" services that control, enrich, and manage traffic to and from valuable resources inside the 'data center' (whether it's physically on-premises on in a public cloud). Proxies provide a strategic point of control over ingress traffic that can be used for a variety of purposes including security and defense of downstream resources.

The recent outbreak of WannaCry/SambaCry is a good example of how proxies can provide protection against attacks that target resources ***other*** than web apps. A quick glance at our latest iHealth statistics shows me a good number of publicly exposed SMB services accessible via port 445. Just where you'd expect it to be. As of May 30, a shodan.io search for "port:445" nets 1,928,046 devices/systems. And while the initial WannaCry attack targeted Microsoft SMB specifically, its latest target is samba.org's Linux implementation, making the more than 722,000 Unix operating systems with port 445 wide open to the world significantly scary.

F5 has a "blocker" available, but the point is not so much that we have one, but the reason we have one: BIG-IP is a programmable, proxy based platform.

The thing is that a proxy – and specifically a ***full*** proxy, with a dual stack – can provide precision discovery and denial of security threats merely by being in the data path. Inspection is part and parcel of a proxy; its ability to do so is a requirement as a means to enable more advanced and flexible capabilities such as protocol translation. Because it intercepts and inspects traffic, it has full visibility. Thus, it can be directed to watch for specific anomalies that indicate an imminent threat or the beginning of an attack.

This is the nature of a proxy; to act as a go-between on behalf of two parties involved in an exchange. In the case of technology, that's a requester system and a responder system. A client and an app. And it doesn't matter whether the exchange is taking place using HTTP over port 80 or SMB over port 445. A proxy can provide the visibility into the traffic necessary to recognize (and one hopes, subsequently reject) malicious traffic.

Proxies aren't just for web apps, or teenagers. They're for serious professionals who need visibility – and control – over any inbound traffic in order to detect and prevent attacks from causing serious (and costly) damage to resources.

Programmable proxies are the duct tape of the Internet. If you've got one, you can do just about anything you need to do, when you need to do it.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.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