

The full proxy makes a comeback!



Ed, 2014-11-07



Proxies are hardware or software solutions that sit between an End-user and an Organization's server, and mediate communication between the two. The most often heard use of the term "proxy" is in conjunction with surfing the Internet. For example, an End-user's specific requests are sent to the Organization's server and its dedicated responses are sent back to the End-user, via the proxy. However, neither the End-user nor the web server is connected directly.

There are different kinds of proxies, but they mainly fall into either of two categories: the half proxies or the full proxies.

There are two types of half proxies. The deployment-focused half-proxy is associated with a direct server return (DSR) configuration. In this instance, requests are forwarded through the device; the responses, however, do not return through the device, but are sent directly to the client. With just one direction of the connection (incoming) sent through the proxy, this configuration results in improved performance, particularly when streaming protocols. The delayed-binding half proxy, on the other hand, examines a request before determining where to send it. Once the proxy determines where to route the request, the connection between the client and the server are "stitched" together. Because the initial TCP "handshaking" and first requests are sent through the proxy before being forwarded without interception, this configuration provides additional functionality.

Full proxies terminate and maintain two separate sets of connections: one with the End-user client and a completely separate connection with the server. Because the full proxy is an actual protocol endpoint, it must fully implement the protocols as both a client and a server (while a packet-based proxy design does not). Full proxies can look at incoming requests and outbound responses and can manipulate both if the solution allows it. Intelligent as this configuration may be, performance speeds can be compensated.

In the early 1990s, the very first firewall was a full proxy. However, the firewall industry, enticed by faster technology and greater flexibility of packet-filtering firewalls, soon cast the full proxy to the back room for various reasons, including having too many protocols to support. Each time any of the protocols changed, it required the proxy to change, and maintaining the different proxies proved too difficult. The much slower CPUs of the 90s were another factor. Performance became an issue when the Internet exploded with End-users and full proxy firewalls were not able to keep up. Eventually firewall vendors had to switch to other technologies like the stateless firewall, which uses high-speed hardware like ASICS/FPGAs. These could process individual packets faster, even though they were inherently less secure.

Thankfully, technology has evolved since and today's modern firewalls are built atop a full proxy architecture, enabling them to be active security agents. Featuring a digital Security Air Gap in the middle allows the full proxy to inspect the data flow, instead of just funneling, thus providing the opportunity to apply security in many ways to the data, including protocol sanitization, resource obfuscation, and signature-based scanning. Previously, security and performance was usually mutually exclusive: being able to implement security capabilities led to lower performance abilities. With today's technology, full proxies are moving towards tightened security at a good performance level. The Security Air Gap aids that, and, it has proven itself to be a secure and viable solution for organizations to consider. With this inherent Security Air Gap tier, a full proxy now provides a secure and flexible architecture supportive of the challenges of volatility today's organizations must deal with.

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