

# Programmability in the Network: Filtering Favicons



Lori MacVittie, 2015-27-08

There's really an unlimited number of ways in which programmability in the network (data path scripting) can solve problems, address risk, and simplify architectures. In the area of DevOps it can be used to facilitate continuous delivery (CD) initiatives by supporting the implementation of a variety of architectures like [Blue/Green](#), [Canary](#), and even A/B testing patterns. In the network, where SDN (Software Defined Networking) holds sway, the usage of data path scripting can enable modern, sometimes complex application architectures that overcome network complexity associated with [sharding for scale](#) as easily as it implements simple, application routing.

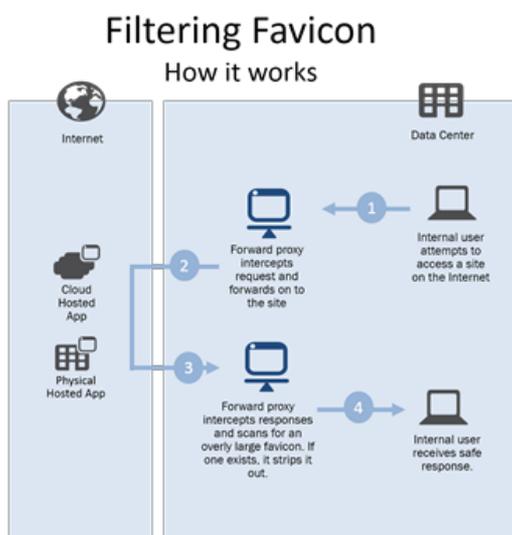
When it comes to security, however, the use of programmability in the network is invaluable when considering how to address any number of flaws, vulnerabilities and risks that crop up virtually out of no-where. From [ShellShock](#) to [Heartbleed](#) to [ApacheKiller](#), data path scripting has enabled organizations to take immediate action to prevent exploitation in the face of threats.

But rarely do you hear of programmability in the network being used to fix other people's applications; the ones your employees might be accessing from inside the organization.

One such issue was [raised in June 2015, when a report revealed problems with large favicons](#). You know, the icons that are displayed in the address bar or bookmarks of a browser that are usually the brand or logo of the site. It turns out that if it's larger than the browser expects, the browser crashes. At issue is the fact that neither the browser nor the user can stop the transfer of the favicon. It's kind of built into the basic behavior. It's stealth; the user likely has no reason why their browser is suddenly (and abruptly) crashing.

Certainly at the moment this particular "vulnerability" is more prank than practical, but if someone were able to exploit it, it could be highly disruptive to productivity and, consequently, business.

Given that potential, wouldn't it'd be nice if there were some way to say, detect an overly large favicon and stop it before it hits your users' browsers?



You already know there is or I wouldn't have written this blog in the first place.

The first thing you need is a forward proxy capable of data path scripting. A forward proxy acts like any other proxy except it's positioned in the network to proxy *outbound* connections. Reverse proxies – ones that act like load balancers – are positioned such that they proxy *inbound* connections.

The forward proxy sits between the users (clients) and the Internet, intercepting and inspecting requests and/or responses. In this case, only the response is necessary as it is what contains the offending data.

The script inspects responses and, upon finding the favicon, can simply remove it or remove it and send a message to the client. The exact behavior is up to you because, well, it's code. That's the power of programmability anywhere; you can tailor behavior to meet your specific needs or requirements.

If you'd like to see an example, [Satoshi Toyosawa](#) – an F5 ENE familiar with our [LineRate programmable proxy](#) – has [written up a node.js script that implements this behavior](#).

Ultimately, the favicon problem is not a significant threat but it could be potentially highly disruptive if it turns up on a site or application that is relied upon by employees. While IT or even users could certainly submit tickets or bugs to the site or application owner, there's no guarantee it will be resolved in a timely manner. Thus the ability to resolve it yourself using data path scripting would be a boon.

And it's also a fine example of how programmability in the network can be a valuable tool in your IT toolbox.

Script on, my friends. Script on.

---

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | [f5.com](http://f5.com)

F5 Networks, Inc.  
Corporate Headquarters  
[info@f5.com](mailto:info@f5.com)

F5 Networks  
Asia-Pacific  
[apacinfo@f5.com](mailto:apacinfo@f5.com)

F5 Networks Ltd.  
Europe/Middle-East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

F5 Networks  
Japan K.K.  
[f5j-info@f5.com](mailto:f5j-info@f5.com)