# F5 Friday: Creating a DNS Blackhole. On Purpose

**Lori MacVittie, 2012-06-01**

#infosec #DNS #v11 *DNS is like your mom, remember? Sometimes she knows better.*

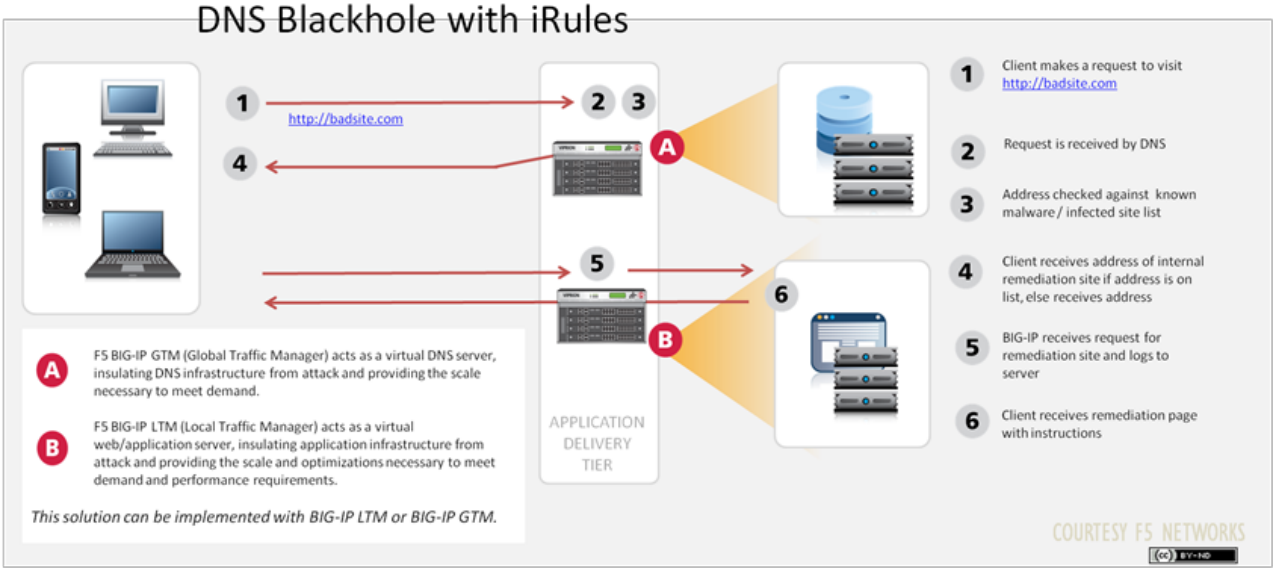
Generally speaking, blackhole routing is a problem, not a solution. A route to nowhere is not exactly a good thing, after all. But in some cases it's an approved and even recommended solution, usually implemented as a means to filter out bad packets at the routing level that might be malformed or are otherwise dangerous to pass around inside the data center.

This technique is also used at the DNS layer as a means to prevent responding to queries with known infected or otherwise malicious sites. Generally speaking, DNS does nothing more than act like a phone book; you ask for an address, it gives it to you. That may have been acceptable through the last decade, but it is increasingly undesirable as it often unwittingly serves as part of the distribution network for malware and other malicious intent.

> *In networking, black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient.*
>
> *When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic; hence the name.*
>
> (http://en.wikipedia.org/wiki/Black_hole_(networking))

What we'd like to do is prevent DNS servers from returning addresses for sites which we know – or are at least pretty darn sure – are infected. While we can't provide such safeguards for everyone (unless you're the authoritative server for such sites) we can at least better protect the corporate network and users from such sites by ensuring such queries are not answered with the infected addresses.

Such a solution requires the implementation of a DNS blackhole – a filtering of queries at the DNS level. This can be done using F5 iRules to inspect queries against a list of known bad sites and returning an internal address for those that match. What's cool about using iRules to perform this function is the ability to leverage external lookups to perform the inspection. Sideband connections were introduced in BIG-IP v11 and these connections allow external, i.e. off device, lookups for solutions like this. Such a solution is similar to the way in which you'd want to look up the IP address and/or domain of the sender during an e-mail exchange, to validate the sender is not on the "bad spammer" lists maintained by a variety of organizations and offered as a service.



Jason Rahm recently detailed this solution as architected by Hugh O'Donnel, complete with iRules, in a DevCentral Tech Tip. You can find a more comprehensive description of the solution as well as the iRules to implement in the tech tip.

## v11.1: DNS Blackhole with iRules

Happy (DNS) Routing!

- F5 Friday: No DNS? No … Anything.
- BIG-IP v11 Information
- High-Performance DNS Services in BIG-IP Version 11
- DNS is Like Your Mom
- F5 Friday: Multi-Layer Security for Multi-Layer Attacks
- The Many Faces of DDoS: Variations on a Theme or Two
- High-Performance DNS Services in BIG-IP Version 11

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