F5 Friday: When the Solution to a Vulnerability is Vulnerable You Need a New Solution

Lori MacVittie, 2011-05-08

#v11 Say hello to DNS Express

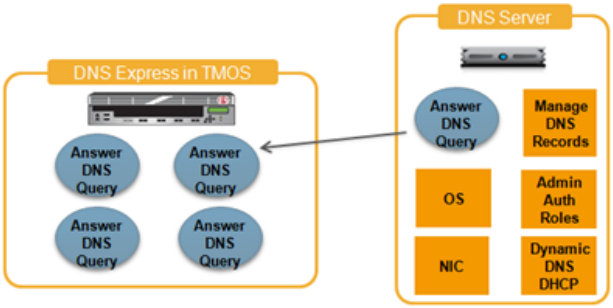
You may recall we recently expounded upon the need for the next generation of infrastructure to provide more protection of critical DNS services. This is particularly important given recent research on behalf of Versign that found "60% of respondents rely on their websites for at least 25% of their annual revenue." Combined with findings that DDoS attacks, DNS failures and attackers comprised 65% of unplanned downtime in the past year, the financial impact on organizations is staggering.

We also described the most popular solution today, DNS caching, and mentioned that it turns out this solution is itself vulnerable to attack. DNS caching can be defeated by simply requesting non-existent resources. This is not peculiar to DNS, by the way, but rather to caching and the way it works. Caching is designed as a proxy for content; content that is always obtained from the originating server. Thus if you request a resource that does not exist in the cache, it must in turn query the originating server to retrieve it. If you start randomly creating host names you know don't exist to lookup, you can quickly overwhelm the originating server (and potentially the cache) and voila! Successful DDoS.

Like an increasing number of modern attacks, this vulnerability is no one's fault per se; it's an exploitation of the protocol's assumptions and designed behavior. But as has been noted before, expected behavior is not necessarily acceptable behavior. For IT, that only matters forasmuch as it aids in finding a more secure, i.e. non-vulnerable, solution.

INTRODUCING DNS Express

BIG-IP v11 introduced DNS Express, comprising several new capabilities that provide comprehensive DNS protection and addresses just this vulnerability as part of its overall features designed to maintain availability for critical DNS services.



DNS Express is a new DNS service available in BIG-IP v11 that implements an authoritative in-memory DNS service capable of storing tens of millions of records. This caching-style solution is enhanced by the CMP (Clustered Multi-Processing) enabled TMOS platform, which allows BIG-IP Global Traffic Manager (GTM) to respond to hundreds of thousands of queries per second (millions per second on the VIPRION hardware platforms). Rounding out this strategic trifecta of DNS goodness is IP Anycast integration, which has the result of obfuscating the number and topological attributes of DNS servers while simultaneously distributing load. This is an important facet as attackers often target DNS servers one by one, and without the ability to determine how many servers may be present attackers must make a choice whether to forge ahead – possibility wasting their valuable time – or concede defeat themselves.

A DNS infrastructure based on DNS Express allows customers to leverage the ability of BIG-IP to withstand even the most persistent DDoS load by enacting a zone transfer from a DNS pool to BIG-IP GTM, which subsequently acts as a high-speed authoritative slave DNS service. It is an architectural solution that is fairly non-disruptive to existing architecture and by leveraging core TMOS features such as iRules, adds control and flexibility in designing solutions specifically for a data center's unique needs and business requirements.

This solution realizes the benefits of a DNS-caching solution while mitigating the risk an attacker will exploit the behavior of caching solutions with a barrage of randomly generated host name requests.

Happy Safe Resolving!

- DNS is Like Your Mom
- All F5 Friday Posts on DevCentral
- It's DNSSEC Not DNSSUX
- Introducing v11: The Next Generation of Infrastructure
- BIG-IP v11 Information Page
- The End of DNS As We Know It
- Taking Down Twitter as easy as D.N.S.
- Cloud Balancing, Cloud Bursting, and Intercloud
- Achieving Enterprise Agility in the Cloud (Cloudbursting with VMware, BlueLock, and F5)
- DNSSEC: The Antidote to DNS Cache Poisoning and Other DNS Attacks

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