DATASHEET

DNS Flag Day 2020

DNS FLAG DAY 2020

CHALLENGE

- **Large UDP Packet Fragmentation:** The Internet Protocol (IP) layer fragments large DNS messages on networks that cannot transmit large packets, causing potential reliability and security risks.

SITUATION

- **UDP Packet Reduction:** Starting on DNS Flag Day 2020, the DNS community will begin reducing the size of UDP-based DNS messages to avoid fragmentation. This may cause some DNS servers to send truncated responses over UDP, causing receiving DNS servers to resend queries over TCP.
- **Reliability and Security Risk:** Some DNS servers or operators don't support TCP, causing reliability and security risk.

SOLUTION

- **NIOS 8.5.1 Default Changes:** NIOS 8.5.1 exposes two settings: 1) the maximum size of a UDP datagram a recursive DNS server says it can accept; and 2) the maximum data amount an authoritative DNS server will put into a UDP-based DNS message.

OUTCOME

- **DNS Reliability and Security:** Infoblox enables customers to avoid DNS message fragmentation and improve DNS reliability and Internet security.

DNS Flag Day 2019: Changing How DNS Works on the Internet

February 1, 2019 was the first DNS Flag Day. DNS software developers and DNS operators combined to redefine how DNS works on the Internet. Their efforts resulted in faster name resolution on average for Internet users. However, in the process, DNS users lost the ability to resolve domain names hosted on certain DNS servers that didn't support EDNS0 extensions written back in 1999. In general, however, DNS Flag Day 2019 was a success, so a second event was planned for 2020 focused on resolving issues around large message fragmentation.

DNS Flag Day 2020: Solving Packet Fragmentation to Make Internet Transmissions More Reliable and Secure

Large DNS messages are broken up, or fragmented, by the Internet Protocol, or IP layer, to carry them over networks that cannot handle large packets. However, fragmentation is not always reliable and can result in transmission failures. Further, when fragmentation actually works, it can present security risks.

A community of DNS software and service providers is driving DNS Flag Day 2020, supported by an organization called DNS-OARC, which esearches and facilitates Internet DNS operations. Beginning on DNS Flag Day 2020 (the date of which is still under consideration), these DNS community members will begin reducing the size of UDP-based DNS messages transmitted by their software over the Internet to minimize the potential of fragmentation. This may result in some DNS servers sending truncated responses over UDP, which will cause receiving DNS servers to retry their queries over TCP.

For most, this poses no concern since every RFC-compliant DNS server can process both UDP and TCP queries. Further, firewalls should be configured to allow TCP-based queries to and from DNS servers.

However, a small number of DNS servers don't support TCP, and a few operators don't allow TCP-based queries or responses, so this can cause reliability and security problems. Thus, a coordinated Flag Day effort is needed to create awareness, align expectations and avoid resolution problems.

Since Infoblox supports DNS Flag Day, a new DNS Flag Day 2020 feature in NIOS 8.5.1 helps customers avoid DNS fragmentation on most networks [1]. The feature enables two simple but very important settings. The first setting controls the maximum size of a UDP datagram a recursive DNS server advertises to authoritative DNS servers. The second setting controls the maximum amount of data an authoritative DNS server will put into a UDP-based DNS message.

These new defaults help make DNS on the Internet more reliable and secure while avoiding fragmentation and the potential security risks associated with transmitting large packets.

Infoblox is an ongoing supporter of DNS Flag Day. Learn more about DNS Flag Day at https://dnsflagday.net/2020/.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com