IETF 79
Beijing, China

IPv6 DNS Whitelisting: Overview and Implications

DNS Whitelisting

I-D: *draft-livingood-dns-whitelisting-implications*

- How does it work?
- Why are some sites implementing/considering it?
- What are the implications?
- What are the solutions and alternatives?

DNS Whitelisting – How It Works

- 1 - The authoritative DNS server for example.com receives a DNS query for www.example.com, for which both A (IPv4) and AAAA (IPv6) address records exist.
- 2 - The authoritative DNS server examines the IP address of the recursive resolver sending the query.
- 3 - The authoritative DNS server checks this IP address against the access control list (ACL) that is the DNS whitelist.
- 4 - If the resolver's IP address **is not** listed in the ACL, then the response to that specific resolver can contain only A (IPv4) address records and therefore cannot contain AAAA (IPv6) address records.
- 5 - If the resolver's IP address **is** listed in the ACL, then the response to that specific resolver can contain both A (IPv4) and AAAA (IPv6) address records.

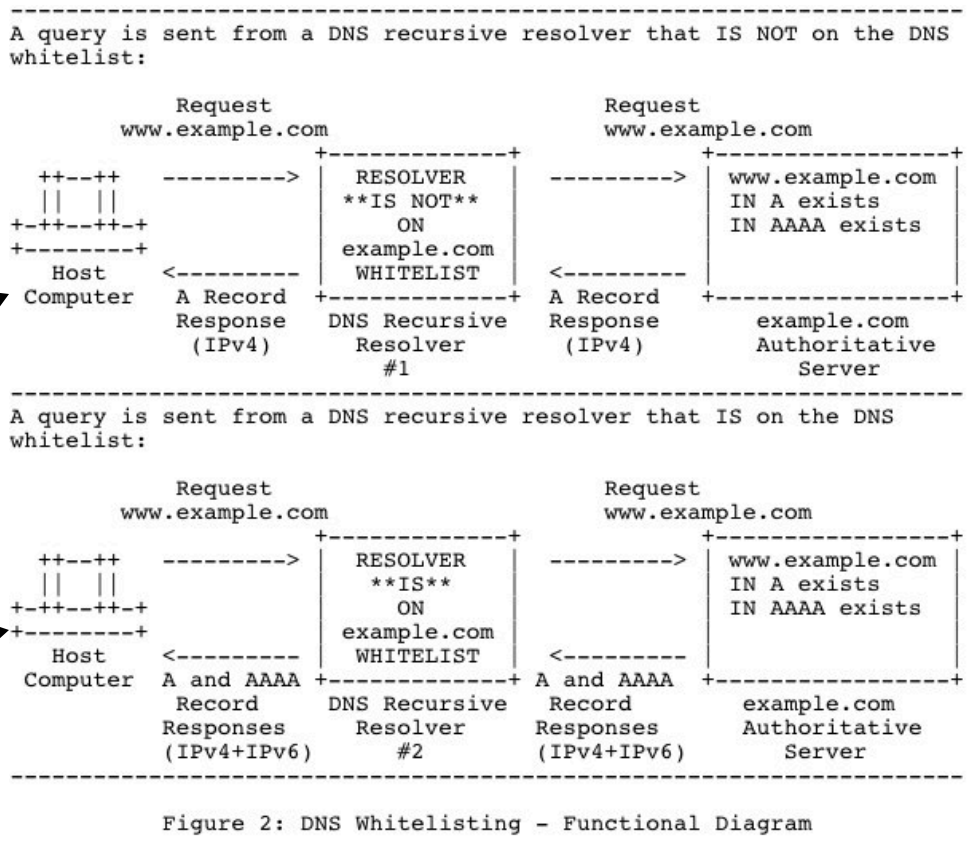

Figure 2: DNS Whitelisting - Functional Diagram

DNS Whitelisting – Why Are Some Considering It?

- As websites add IPv6 address records to their authoritative DNS (AAAA records), this can impair the ability of a few end users to access a site that has added AAAA records with IPv6 addresses.
  - The impairment can range from slow access to no access
- These users have a range of OS, home gateway, and web browser issues that are gradually being fixed by software and hardware vendors and/or may be using non-managed tunnels.
- Site owners are concerned that if these users experience very slow or no access to a given site, that they will switch to a competitor's site
  - Of course a competing site, if they've also implemented IPv6, will present the same impairment for the end user

DNS Whitelisting – Why Are Some Considering It?

- Estimates ~6 months ago indicated that in a network such as Comcast's, with ~15.5M customers, that 0.073% of customers may experience some IPv6-related impairment when accessing a dual-stack site.
- More recent estimates place the fraction of customers with IPv6-related impairment closer to 0.064%.
  - In the Comcast network of ~15.5M customers, this is a range of 9,920 (0.064%) to 11,315 (0.073%) customers

DNS Whitelisting – Downsides and Risks

- Those in the community who have raised concerns regarding DNS whitelisting have explained that given the relatively small number of users affected, DNS whitelisting as a solution seems:
  - out of proportion with the underlying problem
  - costly in comparison to the benefits (impaired customer equipment can likely be replaced less expensively than the cost to implement and maintain DNS whitelisting globally)
  - may cause other, unintended problems
  - may cause a fragmented, two-tiered Internet to emerge
  - may cause users to resist or avoid transitioning to IPv6
  - may cause networks to delay or avoid transitioning to IPv6
  - may cause networks to implement multi-layer NAT systems, like NAT444, which could cause problems for existing or the emergence of new applications and could be perceptibly slower than direct, native access

DNS Whitelisting – Implications

- Policies for controlling whitelists are opaque and administratively challenging:
  - They are likely to vary on a domain-by-domain basis
  - There is no centralized or easy way to discover the policies/criteria to be added to the whitelist
  - There is no centralized or easy way to discover the policies/criteria to *remain* on a whitelist once you have been added (de-whitelisting)
  - What are the turnaround expectations to review an application to be added to a whitelist? Minutes, hours, days, weeks, or months?
  - Is there a process for appeals of whitelisting denials or de-whitelisting actions?
  - Do whitelisting denials and de-whitelisting actions open whitelisting parties up to legal or regulatory risks?
  - Can whitelists be used in a discriminatory fashion?
  - How will whitelisting parties maintain transparency, fairness, non-discrimination, and due process of their policies?

DNS Whitelisting – Implications

- Extra staff may need to be added to manage whitelisting:
  - Content owners will need to accept, review, and process requests, as well as manage appeals and de-whitelisting decision-making processes
  - Recursive DNS resolver operators will all need to staff to submit DNS whitelisting requests to all domains that all of their users are interested in or may be potentially interested it.
- IPv6 reachability will likely compare unfavorably with IPv4 reachability since with IPv4 access is a given in most cases when an IPv4 address record is added to the DNS, while this is not the case with IPv6.
- It does not scale well:
  - Content is no longer globally available; it is made accessible based on countless bilateral agreements
  - Managing these bilateral agreements is difficult to scale for both the content owner that has implemented DNS whitelisting and the recursive DNS resolver operator who wishes to be added to a DNS whitelist
  - As the number of sites increases, staff may need to be added proportionally.

DNS Whitelisting – Implications

- Monitoring and troubleshooting will be more challenging:
  - How will network operators monitor to ensure that DNS whitelisting to all domains is functioning, so as to detect when de-whitelisting has occurred?
  - How will end users determine, during the course of troubleshooting, whether they cannot reach a site's IPv6 address due to connectivity problems or a DNS whitelisting problem?
- Also:
  - operational impacts for both authoritative and recursive DNS server operators
  - architectural, end-to-end impacts
  - ad-hoc vs. universal deployment impacts
  - end point homogeneity may be encouraged
  - technology policy implications
  - read the I-D for more…

DNS Whitelisting – Solutions & Alternatives

- Deploy DNS whitelisting, either ad-hoc or universally
- Or, fix end user hosts with IPv6-related impairments
- Or, accept that a level of 0.05% - 0.10% of users having impaired connectivity is normal
  - Statistics for IPv4 impairment do not appear to be well known, but it is possible that IPv4-related impairment could equal or exceed that for IPv6 for a range of reasons
- Or, advise users of these IPv6 impairments and help them solve these issues:
  - Major web sites that currently detect and measure IPv6 impairment levels could add a special message to affected users, with guidance on how to solve these problems
  - A centralized, industry-wide or country-wide IPv6 readiness website could be released that enables end users to test their readiness to support IPv6, advising the users with IPv6-related impairments of this fact and making recommendations on how to solve these problems
    - Perhaps ISOC or the IETF could setup such a site?

Questions / Requests

- What is the appropriate WG / venue for this document?
  - V6OPS
  - DNSOP
  - INT AREA
  - IAB
  - Individual submission
  - Other?
- Please review the document and provide feedback for a -01 version
  - Many sections in the document are marked where I'd really like more feedback.
    - Marked "[EDITORIAL: Question posed to reader]"
  - In particular I want to be sure to fully capture the motivations for this practice and potential benefits, so this is a well balanced document looking at all sides of the issue.
  - Would like to identify a few volunteers willing to perform a review of the document.

Thank You!

Info on Comcast's IPv6 work at:
http://www.comcast6.net