Network Working Group
Internet-Draft
Intended status: Standards Track
Updates: RFC6147, RFC7208
Expires: 12 August 2022

K. Frank

8 February 2022

An Extension ~~of~~ to DNS64 ~~(RFC6147)~~ for Sender Policy Framework (SPF) ~~SPF~~Awareness ~~(RFC7208)~~

draft-frank-dns64-spf-extension-01

Abstract

This document describes interoperability issues and resolutions between DNS64 and SPF records for mail transfer agents. This ~~RFC~~document also aims to simplify the IPv6 migration for mail transfer agent operators.

This document updates ~~[~~RFC6147~~]~~ and ~~[~~RFC7208~~]~~.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 12 August 2022.

Table of Contents

1. Introduction 2
2. Rewriting SPF records 2
3. SPF Mechanism Definitions 3
4. Informative References 3
Author's Address 4

1. Introduction

Network Address and Protocol Translation from IPv6 clients to IPv4 servers (NAT64) function [RFC6146] is widely deployed, especially in cellular networks. Such a function is solicited when an IPv6-only host communicates with an IPv4-only server. In such context, IPv4-only servers are represented in the IPv6 domain by synthesizing IPv6 addresses based on IPv4 addresses. The address translation algorithm defined in [RFC60525] uses a dedicated IPv6 prefix that can be the Well-Known Prefix (i.e., 64:ff9b::/96) or a Network-Specific Prefix (NSP).

DNS64 [RFC6147] specifies a companion DNS mechanism to represent IPv4-only servers in the IPv6 domains.

The~~-~~ DNS64 specification [RFC6147] ~~definition~~ causes issues for mail transfer agent operators as it ~~failed~~ does not ~~to consider the existance~~discuss the implications on ~~of~~ SPF records [RFC7208]. ~~Because of this~~Therefore, and assuming a NAT64 is present on the path, when an SPF validator tries to validate It, it wi~~l~~ll fail because the originating IP address ~~NAT64 [RFC6146] IP~~ isn't within the SPF records allow-/denylist~~...~~.

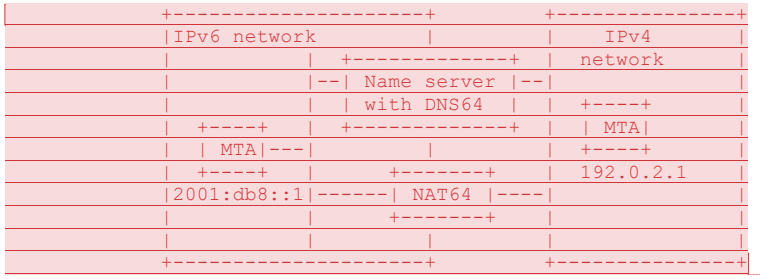

Figure 1: Sample Deployment (RFC6146)

X. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

Commenté [BMI1]: To be defined as I don't see the term in rfc7208

Commenté [BMI2]: Be explicit about to what "it" refers to.

Commenté [BMI3]: I suggest you add a figure so that the reader can see where the various entities are located: which one is IPv4, IPv6, etc. Then, walk through an example to illustrate the failure that is experienced

You can use this one as starting point

The reader should be familiar with the terms defined in [RFC6147] and [RFC7208].

2. Updates to RFC6147: Rewriting SPF Rrecords

The sSection 5.1 of [RFC6147] gets ammended with anotheris updated with this new subsection (5.1.9):

NEW:

> 5.1.9. Dealing Handling with SPF recordsRecords
>
> If the DNS64 server receives an SPF- record (within either the TXT-RR or the SPF- RR [RFC4408RFC7208]) containing the "ip4" mechanism (Section 5.6 of [RFC7208]), it MUST rewrite rewrites the ipv4 IPv4 address according to the same rules as an A- RR and synthesize a new SPF record within the response that contains it as an additional "ip6" entry. If an ip4-cidr-length is present, it gets converted as well (adding 96 will generate the new ip6-cidr-length). The original "ip4" mechanism MUST NOT be removed from the response. If any "a" or "mx" mechanism contains a dual-cidr-length without an ip6-cidr-length, it also gets generated. (Ee.g., : "v=spf1 a:a.example.com/24 mx:mx.example.com/24 ip4:192.0.0.1/32 -all" becomes: "v=spf1 a:a.example.com/24/120 mx:mx.example.com/24/120 ip4:192.0.0.1/32 ip6:64:ff9b::c000:1/128 -all"). This example uses the Well-Known Prefix defined in [RFC6052].
>
> NOTE: Everything else is done by the SPF validator (as already defined in the standard). * When it checks a.example.com, it'll query queries the A-RR and AAAA-RR and, thereby, gest a response containing the synthesized AAAA- RR and validation will pass accordingly. * When it checks the NAT64 generated IPv6 source address against the SPF, it'll find the "ip6" mechanism and also pass. * For any macro-string, the SPF validator will generate new DNS lookups, which will be rewritten according to this RFC document and therefore pass as expectedthe validation checks.

Commenté [BMI4]: It was obsoleted

Commenté [BMI5]: Add a reference

Commenté [BMI6]: You may format this as bullets

Commenté [BMI7]: Not sure to get this part. Do you mean the original IPv6 address?

3. Updates to RFC7208: SPF "exists" Mechanism ~~Definitions~~

~~The s~~Section 5.7 of [RFC7208] currently explicitely ignores the presence of IPv6 and to future proof~~e~~ it for IPv6-only it gets updated ~~from~~as follows:

OLD:

> This mechanism is used to construct an arbitrary domain name that is used for a DNS A record query.

~~to~~NEW:

> This mechanism is used to construct an arbitrary domain name that is used for a dual DNS A~~-~~ RR and AAAA~~-~~ RR query.

~~and from~~
OLD:

> The <domain-spec> is expanded as per Section 7. The resulting domain name is used for a DNS A RR lookup (even when the connection type is IPv6). If any A record is returned, this mechanism matches.

~~to~~NEW:

> The <domain-spec> is expanded as per Section 7. The resulting domain name is used for ~~a~~ DNS A~~-~~ RR and AAAA~~-~~ RR lookups, depending on when the host is single-stack IPv6 or IPv4. For dual-stack, an SPF resolver MUST query both. If any A or AAAA record is returned, this mechanism matches.

4. References

4.1 Normative References

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

4.2 Informative References

~~[RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, DOI 10.17487/RFC4408, April 2006, <https://www.rfc-editor.org/info/rfc4408>.~~

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

Commenté [BMI8]: There is no such query. Do you mean both A and AAAA queries?

Commenté [BMI9]: This will be difficult to characterize.

For your information, there are deployments where only an IPv6 prefix is assigned to the mobile host, but the host sends both A and AAAA queries, not only AAAA.

Commenté [BMI10]: I would just delete this part.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

Author's Address

Klaus Frank

Email: klaus.frank@posteo.de