Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Best Practices for Managing SPF Records

August 2017

The reference URL for this document: www.m3aawg.org/Managing-SPF-Records

1. Executive Summary

Defining and maintaining a Sender Policy Framework (SPF) record is an important part of establishing an email sender's online identity. SPF, as defined by the IETF (Internet Engineering Task Force) standard RFC 7208 (https://www.rfc-editor.org/rfc/rfc7208.txt)[1], enables senders to identify servers that are authorized to send email on behalf of a domain owner.

Unfortunately, it can be challenging for non-experts to correctly define an appropriate SPF record for their domain. Moreover, SPF records need to be actively maintained. Failure to do so can lead to an outdated policy which, over time, can pose a security risk and may provide a vehicle for malicious entities to hijack established reputation.

This document is targeted at those with a basic understanding of the purpose and usage of SPF— for example, administrators responsible for maintaining the SPF policy for one or more domains who seek the latest best practices for defining, publishing, and maintaining SPF records. It is not intended to serve as an introduction to the syntax and use of SPF. Nor is it aimed at experts who want an exhaustive understanding of all SPF options and implications.

2. Introduction

SPF is a mechanism that allows domain owners to publish and maintain, via a standard DNS TXT record, a list of systems authorized to send email on their behalf. This provides a powerful anti-abuse tool, protecting against spoofing and other unauthorized sending of email on behalf of a domain. In addition, SPF helps large mail receivers attribute reputation to a domain which, in turn, serves to improve mail deliverability for non-abusive domaina.

Publishing an incorrect SPF record, however, can have serious unintended consequences that leaves the domain vulnerable to email abuse. This document covers best practices for how to properly construct and maintain an SPF record, as well as common errors and unintended consequences.

---

[1] RFC 7208: Sending Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, https://www.rfc-editor.org/rfc/rfc7208.txt, October 2015.

3. Constructing an SPF Record

At its most basic, an SPF record is a rule set that defines a list of IP addresses that are explicitly permitted—or forbidden—to send email on behalf of a domain. The SPF record is processed from left to right until a rule matching the IP from which the incoming email was sent is found. If they exist, directives including references to other SPF records are processed recursively. Once a match is made, processing stops and the SPF status is determined. If an IP is listed multiple times, only the first match matters.

The following process will help in the construction of appropriate SPF records for each domain under consideration that needs an SPF record. For each domain:

1. Make certain the record starts with `v=spf1.`

2. Identify internally managed systems that send mail using this domain name. List their IP addresses using **ip4** and **ip6** directives.

3. Identify third-party senders that send on behalf of the domain, and use the SPF **include** parameter recommended by the sender.

4. Make certain the record ends in `~all` or `-all`. This ensures that any IP addresses not already matched are not permitted to send email for the domain. Most receivers treat `~all` and `-all` similarly, although some are more likely to reject unauthenticated email when the latter is used.

5. Ensure the new SPF record is the only SPF record published for the domain. Delete any other SPF records on the domain.

NOTE: *Consider using reports provided by publishing a DMARC record to verify that all legitimate senders are being properly authenticated with SPF. More information about DMARC can be found on the DMARC.org website* (https://dmarc.org/).

3.1 Example Records

`"v=spf1 -all"`
For any domain that does not send email.

`"v=spf1 ip4:192.0.2.50 -all"`
Only the host with IP address 192.0.2.50 is authorized to send email for this domain.

`"v=spf1 ip4:192.0.2.50/29 -all"`
Only hosts with one of the eight IP addresses in the 192.0.2.50/29 CIDR block are authorized to send email for this domain.

`"v=spf1 ip6:1080::8:800:200C:417A/121 -all"`
Only hosts with one of the 128 IP addresses in the 1080::8:800:200C:417A/121 CIDR block are authorized to send email for this domain.

`"v=spf1 include:_spf.example.com -all"`
Only IPs that pass the _spf.example.com SPF check can send on behalf of this domain.

`"v=spf1 include:_spf.example.com include:example.net ~all"`
Any IP that passes either the SPF record defined at _spf.example.com or the SPF record defined at example.net can send on behalf of this domain. All others are not authorized.

`"v=spf1 ip4:192.0.2.0/24 ip4:198.51.100.17 include:_spf.example.com ~all"`

There is a range of 256 hosts, one host outside of that range, and any IP that passes the SPF record defined at _spf.example.com is authorized to send on behalf of this domain. All other IP addresses are not authorized.

3.2 Common issues

Even though mail may be delivered successfully to some receivers, that does not necessarily mean the domain's SPF record is correct. Some receivers may attempt to interpret SPF records despite syntax errors. Therefore, an SPF record that is not well constructed can create inconsistent behavior across different receivers and sometimes even within the same receiver.

3.2.1 Syntax Issues

- **Multiple SPF records published in DNS for the same domain**
  A domain must publish no more than one SPF record. A SPF record is defined as a DNS TXT record starting with `v=spf1`. Publishing multiple TXT records beginning with `v=spf1` in the same zone is an error, negating all SPF verification results. Some receivers might try to guess which SPF record is correct, but most receivers will not try to interpret the sending domain's intention. Delete any SPF record that is not the primary record for the domain.

- **Unresolvable hostnames**
  Some SPF directives take hostnames that may require a DNS lookup to evaluate. If a hostname is specified as part of a directive (for example, `a:does.not.exist.example.com`), but that hostname is not resolvable, then the SPF record will cease to be processed. If an **include** fails to resolve, evaluation of the SPF record will stop with an error.

- **Too many DNS lookups**
  As part of SPF record evaluation, receivers may need to do DNS lookups (e.g., to evaluate **include**, **a**, and **mx** directives). The SPF standard specifies limitations on how many DNS lookups a receiver can do. The receiver must fail a message if more than 10 DNS lookups are required to evaluate the record.

  It is therefore important that, when constructing an SPF record, no more than 10 domain lookups are needed to fully evaluate the record. All DNS lookups, including lookups from within **include** directives, count against this limit. It is also important to note that some **include** directives might use two, three, or more lookups. All of these count against the limit.

- **An "all" directive in the middle of a record**
  Example:
  `"v=spf1 ip4:192.0.2.0/24 ~all include:_spf.example.com ~all"`

  In this example everything after the first `~all` would be ignored, since that `~all` would match every IP. Processing would never reach the `"include:_spf.example.com"` directive.

- **DNS syntax errors**
  An SPF record is essentially a collection of text strings published within DNS. Each string is thus limited to a maximum length of 255 bytes. Strings are added together with no additional whitespace. If constructing a record from multiple strings, make certain to add whitespace if appropriate where the strings join.

DNS servers that do not support TCP require all DNS responses—including SPF records—to be a maximum of 512 bytes in size. In practice, this should not be a concern for most SPF records. For maximum portability, consider limiting the size of the SPF record to 512 bytes.

- **DNS "SPF" Resource Record type**
  There is a now-obsolete DNS Resource Record (RR) type called SPF (type 99) that is distinct from the currently supported SPF record published as a simple TXT RR. The DNS RR type 99 record type should not be used and any obsolete type 99 SPF RR in DNS should be deleted.

- **"Redirect" directive**
  The use of a **redirect** directive should only be used by advanced users as it can have unintended consequences. Additionally, if a **redirect** directive and an **all** directive appear in the same record, the **redirect** is ignored.

3.2.2 Over-authorization

It is possible to authorize more IPs than intended. This can lead to abuse through the unintentional authorization of unknown or bad actors. Doing any of the following can lead to this overly permissive state:

- **Using `all` or `+all` in the SPF record**
  Ending a record with `all` or `+all` states that anyone not explicitly denied in the record can send email on behalf on the domain. Avoid the use of `all` or `+all` directives.

- **Authorizing large numbers of IPs with wide netblocks /16 or larger**
  In an **ip4** directive, the smallest possible netblock(s) for IPs authorized to send on behalf of the domain should be used. A /16 authorizes 65,536 IPs to send on behalf of the domain. Instead of a wide block, consider multiple **ip4** directives with smaller blocks for a more precise record.

  Note that historically, some large ISPs have included wide netblocks in their SPF records. Most ISPs have now abandoned this practice, restricting themselves to /16 blocks or smaller.

  In an **ip6** directive, the smallest possible netblock should be used. While best practices have not yet been established, it is expected that major receivers will treat **ip6** netblocks in a similar manner to **ip4** netblocks.

- **Using unvetted third-party include directives in the SPF record**

  - Just because an **include** is provided by a third party does not mean it is well constructed or defines precisely which IPs are authorized. An **include** that uses large netblocks, or that references an **include** that uses large netblocks, can lead to unauthorized activity on a domain's behalf.

  - Additionally, an **include** from an untrusted party is a vector for a bad actor to inject authorization for itself or others to send on behalf of a domain that did not intend to authorize this activity. When using third-party **include** directives, ensure an understanding of the contents of the **include** being added.

  - Finally, care must be taken to stay under the 10-domain lookup limit discussed previously because each **include** can results in multiple lookups.

3.2.3 Other Issues and Sources of Confusion

- **The validated domain**
  An email message typically contains a number of different domains that could be used to authenticate the message. When evaluating SPF, receivers use the domain taken from the **Return-Path** address (technically known as the **RFC5321.MailFrom address**). Other domains found in the message are not relevant for SPF.

  This is a common source of confusion, as some sources may indicate that the domain in the header FROM address (or other domains) is used for SPF. Even the instructions provided by some email service providers confuse this issue. When configuring an SPF record, always confirm that the mail to be authenticated uses the domain identified in the **Return-Path**.

  In instances when there is no **Return-Path**, as in the case of email bounce messages, SPF will be evaluated using the EHLO domain of the originating mail server.

- **SenderID deprecation**
  SenderID is a deprecated standard that was intended as an alternative to SPF. SenderID was officially deprecated with the publication of RFC7208 in 2015, and is no longer considered when authenticating email. SenderID records can be identified by their `v=spf2.0` prefix. A record that starts with this prefix should not be used and any such record should be deleted.

- **Referential loops in the record**
  Consider the following domains and SPF records:

  _spf.example.com.
  IN TXT `"v=spf1 ip4:192.0.2.50/29 include:example.net -all"`

  example.net.
  IN TXT `"v=spf1 ip4:198.51.100.0/24 include:example.org -all"`

  example.org.
  IN TXT `"v=spf1 include:_spf.example.com -all"`

  It is possible to unintentionally create referential loops in SPF records. These have the side effects of exhausting the 10-domain lookup limit and failing to authenticate some or all of the messages.

  Ensure published records do not include such loops by inspecting all **include** directives and any **include** directives within.

- **Use of the "a" and "mx" directives**

  - The use of **a** and **mx** directives in SPF records is no longer recommended. If the domain in question uses a third-party service to host mailboxes, then the service should provide an **include** directive for the SPF record. Similarly, most websites no longer send email directly from their web servers; they use an email service provider to deliver mail generated by web applications. Again, in this case the vendor should provide an **include** directive.

  - Historically, many SPF generators created records that included **a** and **mx** directives by default. As above, these directives should be replaced by **ip4/ip6** directives.

- **a** and **mx** directives count against the 10-DNS lookup limit, and can cause security holes when unintentional changes to DNS or compromise of servers lead to accidentally authorization of mail from unintended IPs.

4. Recommendations

4.1 Implementation

1. **Only authorize IPs or ranges that are actually sent from.**

   It is important to explicitly whitelist only those IPs that send mail from the domain. Specifying additional IPs creates vectors for abuse.

   This is especially important on large shared infrastructure, where it is possible to accidentally authorize all users of the shared infrastructure to send on behalf of the domain. Ensure that only hosts that actually send email for the domain are authorized.

2. **Protect non-sending domains.**

   A domain that does not send email but does not have an SPF record is open for abuse. Such a domain should publish a 'deny all' SPF record—`"v=spf1 -all"`—to prevent spoofing of this domain.

3. **Avoid the use of "a" or "mx" directives unless absolutely required.**

   As discussed above, **a** and **mx** are frequently included in records when they are not required. This is especially true when the record is constructed by an SPF record generator service.

4. **Do not use the "ptr" directive.**

   The SPF protocol defines a **ptr** directive, but the latest revision of the specification explicitly deprecates this directive. This is because evaluating a **ptr** directive may require a large number of DNS queries that place substantial burdens on both the receiving mail server and the .arpa infrastructure.

5. **Be wary of SPF macros and the "exists" directive.**

   SPF includes a number of advanced features that should only be used by experts. One such feature, SPF macros, allows the user to make SPF rules dynamic. This is a very powerful capability, but it is also one that is easy to inadvertently misuse.

   The **exists** directive is a potential security risk. Thus the use of **exists** directives should also be avoided by those who are not experts.

4.2 Ongoing Monitoring

1. **Regularly audit SPF records to ensure they are up-to-date.**

   Keeping SPF records current by managing an up-to-date list of authorized IPs and services—and quickly updating the SPF record when this list changes—is critical to preventing unauthorized senders from being able to send mail as the domain.

   The frequency of audits will differ depending on the organization, its anti-abuse needs and the frequency with which its email-sending environment changes. At a minimum, most organizations will want to do an annual audit to ensure that their SPF record reflects their current set of senders. Most

organizations will probably want to review their SPF configuration more frequently—quarterly, or even monthly. Additionally, a full audit should be performed whenever a sender is added or removed from the SPF record at the end of a contractual relationship.

As part of this regular audit, be sure to review what is being included via SPF **include**. Remove **include** directives that are overly permissive or that are no longer necessary or trusted. As needed, work with the email service provider who suggested the relevant **include** to ensure that only the minimum number of IPs are authorized.

2. **Use DMARC aggregate reporting to detect SPF errors and spoofing.**

   DMARC aggregate reporting provides an excellent mechanism for determining both the efficacy and the potential vulnerabilities of an SPF record, as well as a warning system for detecting spoofing or phishing on behalf of the domain. DMARC reporting is strongly suggested to understand the functionality and effectiveness of an SPF record.

   NOTE: *A domain owner can publish a DMARC "`p=none`" record, requesting aggregate reports, without impacting the deliverability of mail.*

5. Conclusion

SPF records specify which IP addresses can send email on behalf of a domain. These records can be tricky to construct and maintain correctly—but if errors are made, security can be compromised and reputation may suffer harm. M[3]AAWG strongly recommends both the careful review of the common SPF record errors and solutions set out in this paper and conducting regular audits of SPF records to make certain that no unnecessary IPs or services are authorized.

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates to this paper.

© Copyright 2017 by the Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG)
M3AAWG113