Name:Erfan Ahmadbeigi

Master:Mr.milad nourian nasab

Subject :Spf record

**What is a DNS SPF record?**

A sender policy framework (SPF) record is a type of [DNS TXT record](https://www.cloudflare.com/learning/dns/dns-records/dns-txt-record/) that lists all the servers authorized to send emails from a particular domain.

A DNS TXT (“text”) record lets a [domain](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) administrator enter arbitrary text into the [Domain Name System (DNS)](https://www.cloudflare.com/learning/dns/what-is-dns/). TXT records were initially created for the purpose of including important notices regarding the domain, but have since evolved to serve other purposes.

SPF records were originally created because the standard protocol used for email — the Simple Mail Transfer Protocol ([SMTP](https://datatracker.ietf.org/doc/html/rfc5321)) — does not inherently authenticate the “from” address in an email. This means that without SPF or other authentication records, an attacker can easily impersonate a sender and trick the recipient into taking action or sharing information they otherwise would not.

Think of SPF records like a guest list that is managed by a door attendant. If someone is not on the list, the door attendant will not let them in. Similarly, if an SPF record does not have a sender’s IP address or domain on its list, the receiving server (door attendant) will either not deliver those emails or mark them as spam.

SPF records are just one of many DNS-based mechanisms that can help email servers confirm whether an email comes from a trusted source. Domain-based Message Authentication Reporting and Conformance ([DMARC](https://www.cloudflare.com/learning/dns/dns-records/dns-dmarc-record/)) and DomainKeys Identified Mail ([DKIM](https://www.cloudflare.com/learning/dns/dns-records/dns-dkim-record/)) are two other mechanisms used for email authentication.

It is worth noting that, at one point, SPF records had a dedicated DNS record type. The dedicated record type has since been [deprecated](https://datatracker.ietf.org/doc/html/rfc7208#section-3.1) and only TXT records are to be used.

**How does a mail server check an SPF record?**

Mail servers go through a relatively simple process when checking an SPF record:

* Server One sends an email. Its IP address is *192.0.2.0* and the return-path the email uses is email@returnpath.com. (A return-path address is different from the “from” address and is used specifically for collecting and processing bounced messages.)
* The mail server that is receiving the message (Server Two) takes the return-path domain and searches for its SPF record.
* If Server Two finds an SPF record for the return-path’s domain, it searches the SPF record for Server One’s IP address in its list of authorized senders. If the IP address is listed in the SPF record, the SPF check passes and the email will go through. If the IP address is not listed in the SPF record, the SPF check fails. In this case, the email will be rejected or marked as spam.

**What does an SPF record look like?**

SPF records must follow certain standards in order for the server to understand how to interpret its contents. Here is an example of the core components of an SPF record:

v=spf1 ip4=192.0.2.0 ip4=192.0.2.1 include:examplesender.email -all

This example lets the server know what type of record this is, states the approved IP addresses and a third-party for this domain, and tells the server what to do with non-compliant emails. Let’s break down how the individual components accomplish this:

* v=spf1 tells the server that this contains an SPF record. Every SPF record must begin with this string.
* Then comes the “guest list” portion of the SPF record or the list of authorized IP addresses. In this example, the SPF record is telling the server that ip4=192.0.2.0 and ip4=192.0.2.1 are authorized to send emails on behalf of the domain.
* include:examplesender.net is an example of the include tag, which tells the server what third-party organizations are authorized to send emails on behalf of the domain. This tag signals that the content of the SPF record for the included domain (examplesender.net) should be checked and the IP addresses it contains should also be considered authorized. Multiple domains can be included within an SPF record but this tag will only work for valid domains.
* Finally, -all tells the server that addresses not listed in the SPF record are not authorized to send emails and should be rejected.
  + Alternative options here include ~all, which states that unlisted emails will be marked as insecure or spam but still accepted, and, less commonly, +all, which signifies that any server can send emails on behalf of your domain.

While the example used in this article is fairly straightforward, SPF records can certainly be more complex. Here are just a few things to keep in mind to ensure SPF records are valid:

* There cannot be more than one SPF record associated with a domain.
* The record must end with the all component or include a redirect: component (which indicates that the SPF record is hosted by another domain).
* An SPF record cannot contain uppercase characters.

Check out the [official SPF record documentation](https://datatracker.ietf.org/doc/html/rfc7208) for more information.

**Why are SPF records used?**

There are many reasons domain operators use SPF records:

* **Preventing attacks:** If emails are not authenticated, companies and email recipients are at risk for [phishing](https://www.cloudflare.com/learning/access-management/phishing-attack/) attacks, spam emails, and email spoofing. With SPF records, it is harder for attackers to imitate a domain, reducing the likelihood of these attacks.
* **Improving email deliverability:** Domains without a published SPF record may have their emails bounce or be marked as spam. Over time, bounced emails or emails marked as spam can hurt a domain’s ability to reach their audience’s inboxes, compromising efforts to communicate with customers, employees, and other entities.
* **DMARC compliance:** DMARC is an email validation system that helps ensure that emails are sent only by authorized users. DMARC policies dictate what servers should do with emails that fail SPF and DKIM checks. Based on the DMARC policy instructions, those emails will either be marked as spam, rejected, or delivered as normal. Domain administrators receive reports about their email activity that help them make adjustments to their policy.

The Cloudflare Email Security DNS Wizard makes it simple to set up the correct DNS TXT records and block spammers from using a domain. [Read more about the Wizard here](https://blog.cloudflare.com/tackling-email-spoofing/).

Learn more about DNS records for email: