How do I create an SPF (Sender Policy Framework) DNS record?

This article introduces the *Sender Policy Framework* or *SPF* record to you - a type of DNS record that strictly defines which servers can send e-mail in your name. It is a useful e-mail security tool in preventing spam or phishing attacks and after reading this article, you will discover that there is no reason *not* to implement SPF records for your domain!

Together with DKIM and DMARC, SPF is a crucial element of e-mail security.

This article contains the following sections:

Introduction: the purpose of SPF

Let's come straight to the point: you cannot trust e-mail senders. The e-mail protocol is set up in such a way, that everyone can use any "From" address that he likes. See for an example our article about testing your e-mail configuration. While this opens a lot of opportunities, it's also abused to make unsolicited e-mail look like coming from a trusted source.

The *Sender Policy Framework* project was started to prevent exactly this from happening. The outcome of this project is a specific type of DNS record, the *SPF record*. An SPF record simply defines which servers are allowed to send from a specific "From" address. If an e-mail comes from a different server, the receiving mail server may choose to reject specific e-mails or mark them as suspicious.

Although the name "SPF record" suggests that it's a special record type in a DNS zone, SPF records are always stored inside regular TXT records. "Real" SPF records were removed from the standards in RFC 7208.

SPF records in Openprovider

The Openprovider DNS management supports the TXT type for DNS records, that can be used to store SPF information. Ensure that your record contents is encapsulated by "straight quotes" and follows the correct syntax rules as described in this article.

SPF record syntax

Each SPF record starts with a version number, followed by one or more trust-definitions and ends with an "all-others" statement. An example is the following DNS record:

```
"v=spf1 a mx ip4:185.87.187.6 -all"
```

which tells the receiving mailserver to accept e-mail from servers that match the domain's A- and MX-records and e-mail from the server with IP address 185.87.187.6. All other e-mail should be considered as invalid.

NB! Please put your record between quotation marks every time you specify an SPF record with any DNS zone configured within Openprovider. Incorrect SPF record specification may lead to the domain name unavailability.

Read on for more details about the syntax.

Version number

Each SPF record starts with a version number, followed by a space. At this moment, the version number is always the same: *v=spf1*

Mechanisms

Immediately after the version number, the set of hosts which are designated outbound mailers for the domain are defined. Those are called *mechanisms*. Mechanisms are evaluated from left to right and evaluation stops as soon as a mechanism results in a hit. That makes the order of the mechanisms important. The so-called *qualifier* that prefixes the mechanism defines what the validator should do at that moment.

Qualifiers

A quantifier defines what the receiving mail server should do in case that specific mechanism results in a hit. The available options are:

- "+" means a "pass": the sender is explicitly allowed to send; accept the e-mail.
- "-" means a "fail": the sender is explicitly not allowed to send; reject the e-mail.
- "~" means a "softfail": the sender is probably not allowed to send, but we cannot be 100% sure about that. The validator may choose to accept the e-mail, but may want to perform some additional tests.
- "?" means "neutral": the validator cannot validate or invalidate the e-mail, but does probably want to accept it.

If no qualifier is given for a certain mechanism, the "+" qualifier is assumed. That means that the following two SPF records are exactly similar:

```
"v=spf1 +a +mx +ip4:185.87.187.6 -all"
"v=spf1 a mx ip4:185.87.187.6 -all"
```

The "ip4" and "ip6" mechanisms

Use the "ip4" and "ip6" mechanism to specify a single IP address or an IP range. Needless to say, "ip4" tests IPv4 address and "ip6" tests IPv6 addresses. The following example SPF records will allow any IP addresses between 192.168.0.1 and 192.168.255.255 (first example) or any IPv6 addresses between 1080::8:800:0000:0000 and 1080::8:800:FFFF:FFFF (second example) and will reject all others.

```
"v=spf1 ip4:192.168.0.1/16 -all"
"v=spf1 ip6:1080::8:800:68.0.3.1/96 -all"
```

The "a" and "mx" mechanisms

Use the "a" mechanism to test against the domain's A record(s) and the "mx" mechanism to test against the domain's MX record(s). It's also possible to add another domain instead of the parent domain. The following example SPF records will allow any e-mail that originates from an IP address listed in the sender's domain's A records (first example), listed in the sender's domain's A *and* MX records (second example) or listed in example.com's A records (third example) and will reject all others.

```
"v=spf1 a -all"
"v=spf1 a mx -all"
"v=spf1 a:example.com -all"
```

The "include" mechanism

Use the "include" mechanism to use another domain's SPF record for validation. This is useful, for example, if you allow third-party mailinglist software to send mailings with your own e-mail address as sender. The following example SPF record will allow any e-mail that originates from the domain itself, but also allows MailChimp to send e-mail on your behalf.

```
"v=spf1 a mx include:servers.mcsv.net -all"
```

Note: this is just an example based on information that is valid on the moment of writing. If you indeed want to include MailChimp in your SPF record, check the MailChimp documentation for the correct SPF mechanisms to use!

Be aware that the maximum number of DNS lookups that can be done in an SPF record is 10. This includes recurring lookups. So if you include two locations that each include 6 other locations, SPF validation will break. The SPF standard included this mechanism to prevent delays through too many DNS lookups. Fall back to IP addresses if the number of DNS lookups is more than ten.

The "all" mechanism

Use the "all" mechanism to correctly close the parsing instructions. This mechanism usually is put at the end of the SPF record and defines what to do in case none of the previously parsed mechanisms resulted in a hit.

All of the above examples contain a "-all", which means that the e-mail should be rejected if none of the previous mechanisms results in a hit. This is the safest qualifier. Alternatively, use the neutral ("?") or softfail ("~") qualifier if you want your e-mail be delivered anyway but with some additional care. Use of the "pass" qualifier ("+all") is not recommended ever, because it reduces the benefit of your SPF record to zero.

The "exists" mechanism

A special mechanism is the "exists" mechanism. While in the basic form it's not so exciting (it just looks up the existence of a hostname), the combination with *macros* in SPF makes it a great tool for monitoring which senders send e-mail from your domains.

A macro is a specific string in the record that will be replaced by another value. Some examples are:

- %{i} is replaced by the IP address of the sender
- %{o} is replaced by the domain of the sending client
- %{h} is replaced by the HELO/EHLO domain

An excellent example of use of those macros is the Dutch tax authority. Their SPF record looks as follows:

```
$ dig _spf.belastingdienst.nl in any
_spf.belastingdienst.nl. 599 IN TXT "v=spf1 exists:_i.%{i}._h.%{h}._o.%{o}._spf.belastingdienst.
```

Every time an SPF record is checked by the receiving e-mail server, it will lookup the hostname in the *exists* mechanism. As this hostname is dynamically created, it will provide information about the sending mail server, for example:

```
_i.192.87.102.75._h.filter5-ams.mf.surf.net._o.belastingdienst.nl._spf.belastingdienst.nl.
```

If the tax authority security department runs a DNS logger, they will see requests for such (non-existing) sub domains and they can filter out unauthorized entries for further investigation based on the sender IP address and the HELO/EHLO domain.

Other mechanisms and modifiers

Apart from the mechanisms described above, one can also use a "ptr" mechanism. The optional modifier "redirect" or "exp" is another structure that can be used in an SPF record. Please refer to the OpenSPF website for full information about those mechanisms and modifiers. This website contains also extended information about the mechanisms described in this article.

SPF for domains without e-mail

SPF is useful as well if a domain is not intended to send e-mail. In that case, declare the following SPF record in your DNS. This record only has an "all" mechanism, rejecting any sender. An SPF validator will reject the sender in all cases.

```
"v=spf1 -all"
```

SPF Limitations

There are a number of limitations on your SPF-record.

Since it's a TXT record, there is a limit of 255 characters.

You can work around this somewhat by using includes, but each SPF check has a limit of 10 DNS-lookups, so 1 for the main record and 9 includes.

Useful documentation

- The official OpenSPF website contains full syntax documentation, tools for testing, best practices and much more.
- RFC 7208 is the official standard of SPF and contains in-depth information about all possible qualifiers, mechanisms and modifiers.

Revision #2
Created 2026-08-07 14:31:53 UTC by Sarath
Updated 2026-08-07 15:48:41 UTC by Sarath