Mail: SPF - Sender Policy Framework

What is SPF?

SPF (Sender Policy Framework) is an email authentication mechanism that helps protect the domain from:

- **spoofing** (impersonation of email addresses),
- **phishing**,
- abuse of servers to send unauthorised messages.

SPF allows a domain owner to determine which servers **have the right to send emails** on its behalf.

How does SPF work?

1. the domain owner adds a special record **TXT** to the DNS of his domain. 2. When the recipient's server (e.g. Gmail) receives an email:

- checks from which **IP address** message was sent from,
- compares this address with the list of servers defined in the SPF record of the sender's domain.

3 Based on this, the message:

- passes the SPF test (**pass**),
- or fails (**fail**, **softfail**, **neutral**, etc.).

SPF record - Where and how to add it

The SPF record is added as a **TXT** to the DNS of the domain.

Type	Name	Value (example)
TXT	ostrowski.net.pl	`v=spf1 include:mx.ovh.com -all`

* `Name`: is the main domain (without prefix, e.g. not `_spf`). * `Value`: the SPF declaration (details below).

SPF record syntax

```
v=spf1 [elementy] [mechanizmy końcowe]
```

The most common elements of the SPF

Element	Description
`ip4:x.x.x.x`	Allows sending from an IPv4 address
`ip6:xxxx::xxxx`	Allows sending from an IPv6 address
`include:domain`	Acknowledges the SPF record of another domain (e.g. an email service provider)
`a`	Allows the servers indicated in the domain's A record
`mx`	Allows MX servers defined for the domain
`exists:`	Permit based on DNS existence
`all`	Matches all - used at the end as default behaviour

Mechanisms modifiers

Symbol	Meaning
`+`	Pass (default - no need to write)
`-`	Fail - reject
`~`	SoftFail - accept, but mark as suspicious
`?`	Neutral - no clear result

Examples of SPF Records

Simple record for one IP only

```
v=spf1 ip4:192.0.2.1 -all
```

Only IP `192.0.2.1` can send emails from this domain. Everything else is rejected (`-all`).

2. SPF for OVH servers.

```
v=spf1 include:mx.ovh.com -all
```

Allows all OVH servers (defined in `mx.ovh.com`) to send emails.

3. combination of IP + mail servers + fallback

```
v=spf1 ip4:203.0.113.0/24 include:_spf.google.com ~all
```

Allows:

- IP addresses in the range `203.0.113.0/24`.
- to Gmail servers

Everything else gets **softfail** (goes into spam, for example, but is not rejected).

Security recommendations

1. **Always end the SPF record with the `all` mechanism.**:

- `-all` → everything outside the list = discard
- `~all` → everything outside the list = mark as suspicious

2. **Avoid excessive `include:`.** - each one is an additional DNS query (limit: 10). 3. **Do not use SPF without `all`.** - is an open invitation to spammers. 4. **Test after each change** - e.g. to https://mxtoolbox.com.

SPF testing tools

- https://mxtoolbox.com/spf.aspx
- https://dmarcian.com/spf-survey/
- https://www.kitterman.com/spf/validate.html
- https://dnschecker.org/spf-record-checker.php

What happens when the SPF fails?

This depends on the receiving server's policy. Possible reactions:

- accept, but mark as SPAM (softfail),
- rejection of the message (fail),
- complete neutrality - treating as any other message.

Common problems with SPF

- No `all` → record ineffective.
- Too many `include:` → DNS query limit exceeded.
- Syntax error (e.g. double `v=spf1`).
- Outdated provider entries (e.g. after server migration)

Summary

SPF is a simple but very effective tool to protect your email domain from abuse. Properly configured:

- reduces the possibility of your email address being impersonated,
- improves the reputation of your domain,
- increases message deliverability.

SPF should be used **together with DKIM and DMARC** for complete mail protection.