SPF
RECORDS

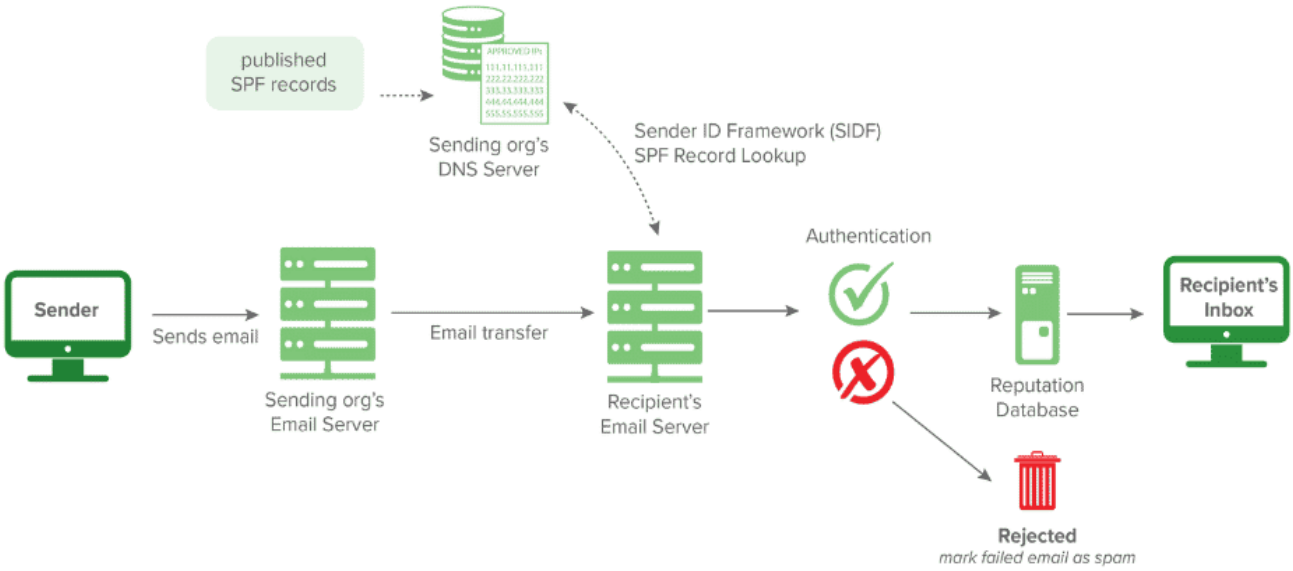
SPF & SPF RECORDS

The Sender Policy Framework (SPF) is a popular email validation which can help ward off attacks like email spoofing and preventing spam. Using an SPF record can also help prevent your emails from being flagged as spam by other servers before reaching your targeted audience.

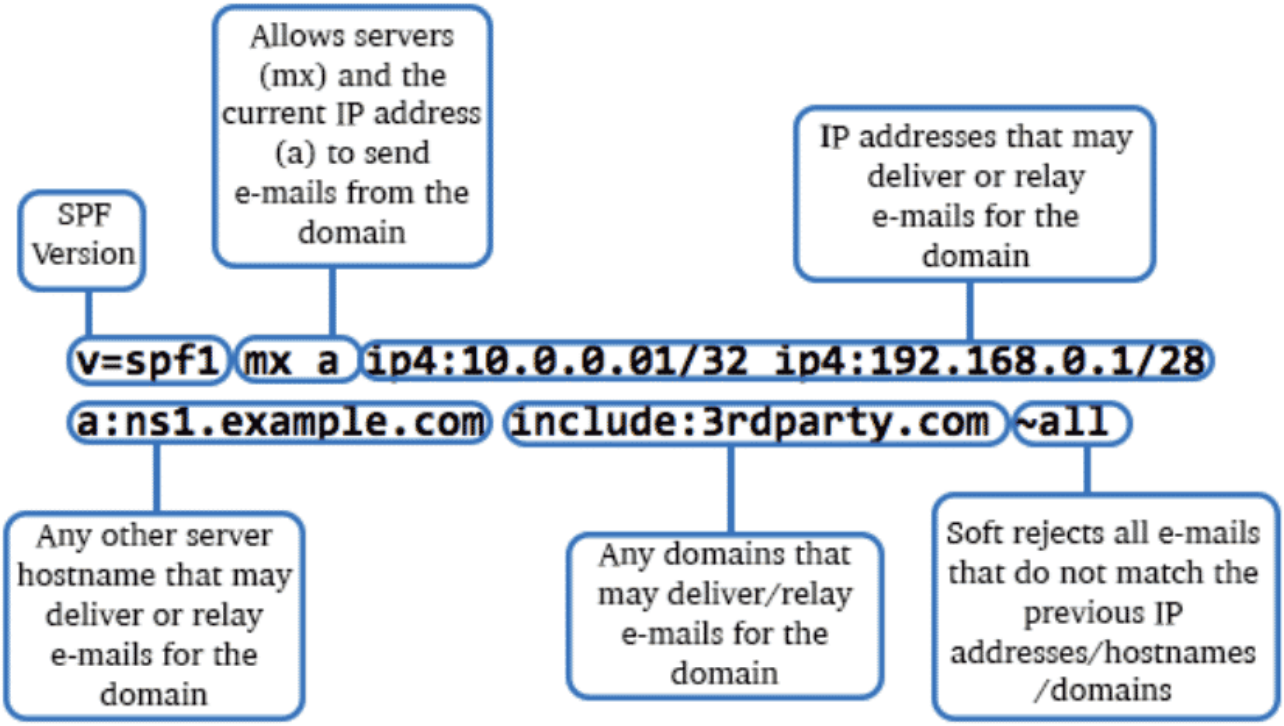
Attackers often spoof sender addresses, making them look genuine, like a regular user's address. SPF can help spot these messages and quarantine them, derailing hem for their attacks. SPF allows the server on the receiving end to check whether an email appearing to come from a given domain is actually originating from an authorized IP address of that domain. The list containing all the authorized IP addresses and hosts for a specific domain can be found on that domain's DNS records.

An SPF record is a TXT record published in a DNS zone file, containing a list of all the authorized mail servers that can send emails on behalf of your domain. It is an implementation of SPF that must be added to your DNS to help identify and mitigate spammers from sending malicious emails with forged addresses on your domain's behalf.

diagrammatic representation of SPF working procedure



and SPF record:



SPF Record syntax

An SPF record is a single string of text published on the domain in the DNS. All SPF records start with exactly "v=spf1", followed by a series of "terms". Note that the version part "v=spf1" is mandatory: everything else like "v=spf2" would render the SPF record invalid and cause the receiving server to ignore the record.

Example of an SPF record:

```
<v=”spfl a include: spf.google.com -all”>
```

- v=spf1 is the SPF version 1, a component that identifies a TXT record as an SPF record.
- a authorizes the host detected in the A record of the domain to send the emails.
- Include is used to authorize emails that the sender can send on behalf of a domain (here, google.com)
- -all tells the receiver’s server that the addresses not listed in this SPF record are unauthorized to send any email. It also tells the servers to reject such addresses.

Here is another example of SPF record which shows the before & after of it getting published on a domain

```
v=spfl mx a:example.com/28 -all
```

when published, the above SPF record looks like this in a domain zone file

```
example.com          TXT  “v=spfl mx a:example.com/28 -all”
```

REFERENCE

- What is An SPF Record and How does It Work: SPF Record Explained - DMARCLY
- What Is an SPF Record? A Complete Guide (kinsta.com)