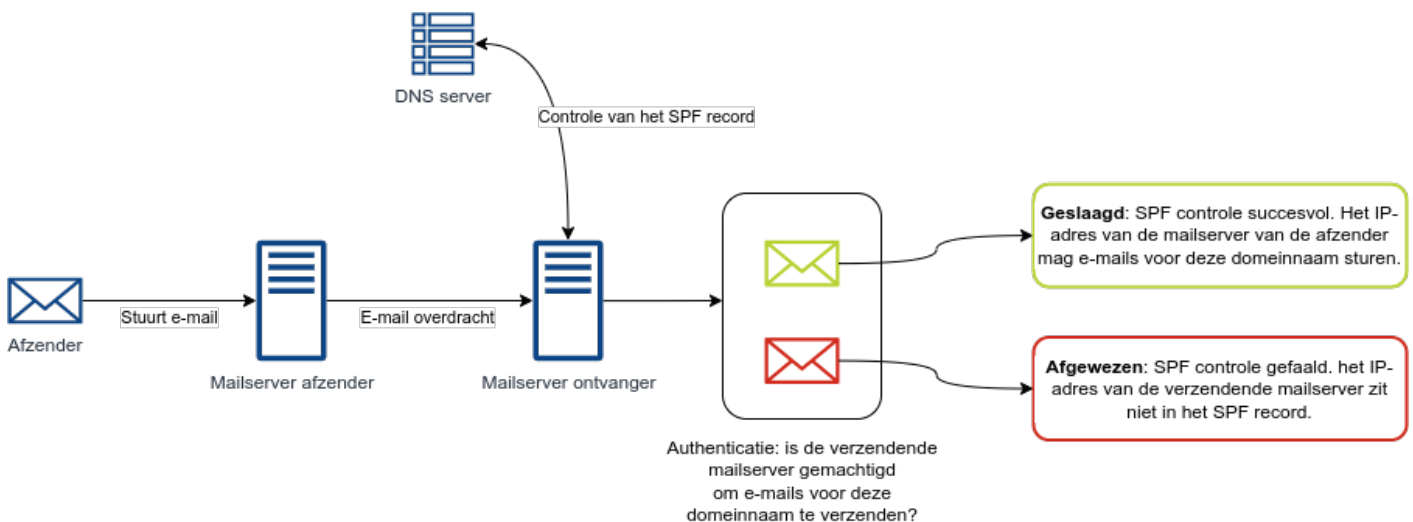


# Een SPF record instellen

## Wat is SPF?

SPF staat voor Sender Policy Framework. Dit is een DNS TXT record van je domeinnaam wat een lijst bevat van servers die vanuit jouw domeinnaam e-mails mogen verzenden. De ontvanger controleert of het IP-adres van de mailserver van waarop het e-mailbericht verzonden werd in het DNS record opgenomen is.



## Stap 1: een SPF TXT record samenstellen

Je SPF gegevens sla je op in een TXT record van je domein en kan je zelf samenstellen in bijvoorbeeld kladblok. Wil je hierbij hulp, dan kan je een handige online SPF generator gebruiken zoals deze van [MXToolbox](#).

We starten met een voorbeeld SPF TXT record:

```
v=spf1 mx include:_spf.google.com ~all
```

Wat bevat een SPF TXT record allemaal?

Tag	Beschrijving	Voorbeeld
v	De versie van je SPF record. Tot op heden is dit altijd 'versie 1'.	v=spf1
mx	De mailservers wat je in je DNS MX records opgenomen hebt.	mx of mx:nexxwave.be
a	Het A en/of AAAA record van je domein.	a of a:nexxwave.be
ip4	Een IPv4 adres of range.	ip4:1.2.3.4 of ip4:1.2.3.4/24
ip6	Een IPv6 adres of range.	ip6:2001:0db8:0123:4567:89ab:cdef:1234:5678 of ip6:2001:0db8:0123:4567::/64
include	Hiermee kan je een lijst van adressen vanuit een ander TXT record aanwijzen. Als je bijvoorbeeld Google Workspace gebruikt, dan verwijst je naar Google's TXT record waarin zij hun mailservers up-to-date houden.	include:_spf.google.com
all	<p>Als afsluiter kies je hoe een ontvangende mailserver e-mails moet behandelen die hij ontvangen heeft en waarvan het IP adres van de verzendende mailserver niet in het SPF record staat. De mogelijkheden zijn:</p> <ul style="list-style-type: none"> <li>• <code>-all</code> wat de e-mail afwijst.</li> <li>• <code>~all</code> wat de e-mail markeert als verdacht.</li> <li>• <code>?all</code> wat de e-mail als neutraal markeert en het aan de e-mail client overlaat.</li> </ul>	~all

Een SPF record moet per subdomein gemaakt worden als je vanuit dat domein e-mails verzendt. Een SPF record op je hoofddomein, geldt enkel en alleen voor dat hoofddomein.

Mail je bijvoorbeeld vanaf `@example.com`, dan maak je een SPF record voor de e-mails die gestuurd worden met het `@example.com` adres. Gebruik je ook het domein `@demo.example.com`, dan maak je een apart SPF record met een lijst van e-mailservers wat mogen mailen uit naam van het domein `@demo.example.com`.

## Tips

Neem voldoende de tijd om alle mailservers op te zoeken die vanuit jouw domein mailen. Denk bijvoorbeeld aan je mailprovider (Google Workspace, Microsoft 365), een contactformulier op je webserver, een dienst wat je gebruikt om nieuwsbrieven te versturen zoals Mailchimp, enz. Welk record je voor die specifieke diensten moet gebruiken, vind je in hun documentatie terug.

We raden aan om je TXT record te valideren voordat je deze in je DNS plaatst. Dat kan bijvoorbeeld met de online tool van [Kitterman](#).

Start met `~all` om te voorkomen dat je mailservers bent vergeten op te nemen en je e-mails daardoor niet zullen toekomen bij de ontvanger. Na enkele weken kan je dit vervangen door `-all`.

Hoewel de tag `include` super gemakkelijk lijkt (dat is het ook!), is er een limiet van 10 domeinen wat je mag vernoemen. Dit is om het aantal DNS look-ups wat een mailserver moet doen, zo beperkt mogelijk te houden. Let op: dit aantal is recursief. Dus als je via 'include' een adres toevoegt wat op zijn beurt 8 andere 'includes' bevat, dan heb je nog plaats voor 1 extra 'include'.

## Stap 2: het TXT record in je DNS opnemen

Zodra je je TXT record met je SPF gegevens samengesteld hebt, plaats je deze in de DNS van je domeinnaam. Dit doe je door in te loggen op het DNS beheerpaneel van je DNS provider.

- Voeg een record van het type '**TXT**' toe.
- Afhankelijk van je domein provider, geef je als '**domeinnaam**' ofwel niets in (blanco dus) ofwel een @-teken als je het record ingeeft voor je hoofddomein (bv. nexxwave.be). Als je het record ingeeft voor een subdomein, dan noteer je hier het subdomein (bv. demo.nexxwave.be).
- Als **TTL** raden we aan om te starten met een lage waarde zodat wijzigingen wat je doet vlug opgepikt kunnen worden. Neem bijvoorbeeld een TTL van 5 minuten: 300.
- Als **TXT-record** noteer je het record wat je gemaakt hebt. Afhankelijk van je domein provider, moet dit tussen "aanhalingstekens" getypt worden.

Record type	<input type="text" value="TXT"/>
Domain name	<input type="text" value=""/> .nexxwave.be.
TTL	<input type="text"/> <small>Default value: 3600 seconds</small>
TXT record	<input type="text" value="v=spf1 mx a include:_netlpshetz.nexxwave.be include:_spf.google.com include:_spf.registrar.eu include:_spf.eu.mailgun.org ~all"/>
* Required fields	<div><input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></div>

Wanneer je TXT record online staat, controleer dan of het goed reageert op aanvragen. Dat kan vanaf je computer of via een online tool zoals deze van **MXToolbox**:

Vanaf je laptop kan je via **dig** eenvoudig de TXT record van je (sub)domein opvragen:

```
klowet@rackpc: ~/Nexxwave/ansible
[klowet@rackpc]~$ dig txt nexxwave.be

;<<> DiG 9.16.27-Debian <<> txt nexxwave.be
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 36784
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;nexxwave.be.                IN      TXT

;; ANSWER SECTION:
nexxwave.be.                3587    IN      TXT      "\"google-site-verification=TERZjH0jCEykT6UAabbWCWGr10AUJDwtzNjbSc-6WHRs\""
nexxwave.be.                3587    IN      TXT      "\"v=spf1 mx a include: netipshetz.nexxwave.be include: spf.google.com include: spf.registrar.eu include: spf.eu.mailgun.org ~all\""
nexxwave.be.                3587    IN      TXT      "\"stripe-verification=261e161e15876fc0de16dbca4925894924ee65e23a13f39b96d0ce2a4ab798cff\""

;; Query time: 0 msec
;; SERVER: 10.55.10.254#53(10.55.10.254)
;; WHEN: Wed Jul 20 13:00:07 CEST 2022
;; MSG SIZE rcvd: 359

[klowet@rackpc]~$
```

Je kan ook een validatie van je SPF record doen door vanaf al je e-mailservers een e-mail te sturen naar een (best extern) e-mailadres. In de headers van deze e-mail vind je terug of de SPF validatie geslaagd al dan niet geslaagd is:

Message ID	<43d5b6d6ef15af4b13496b3b65288699@docs.nexxwave.be>
Created at:	Tue, Jul 19, 2022 at 4:07 PM (Delivered after 1 second)
From:	BookStack <bookstack@docs.nexxwave.be>
To:	kris.lowet@nexxwave.be
Subject:	Test Email
SPF:	PASS with IP 2a01:4f8:c17:2520:0:0:0:1 <a href="#">Learn more</a>
DKIM:	'PASS' with domain docs.nexxwave.be <a href="#">Learn more</a>
DMARC:	'PASS' <a href="#">Learn more</a>

---

Revisie #6

Gemaakt: 20 juli 2022 09:07:09 door Kris Lowet

Bijgewerkt: 20 juli 2022 12:17:50 door Kris Lowet