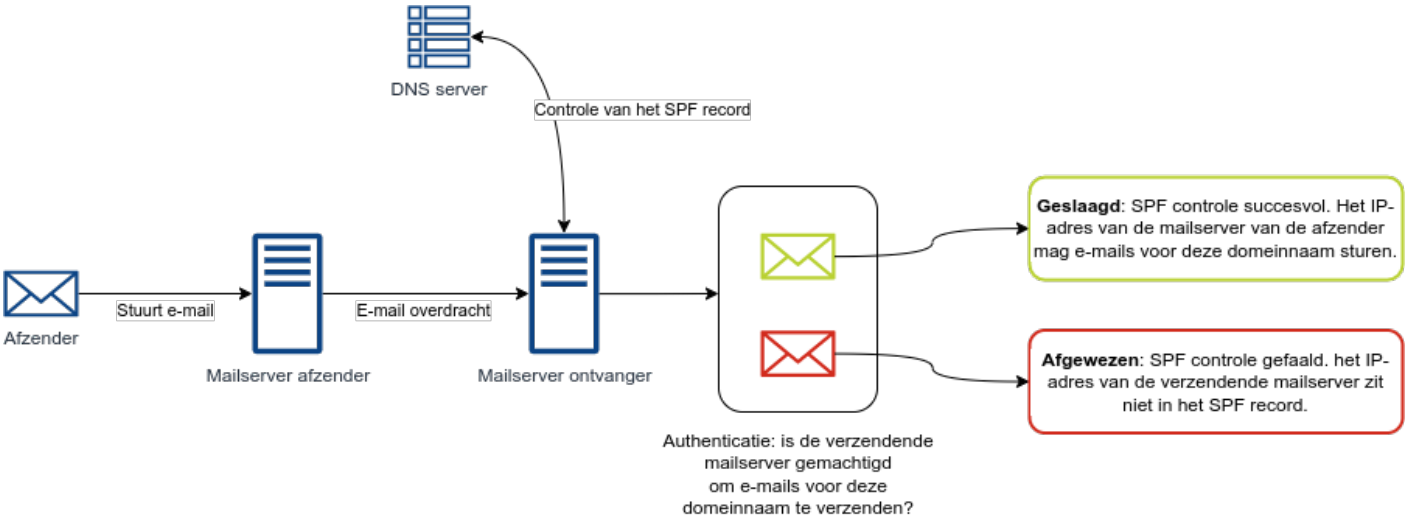
DNS beveiliging

- Een SPF record instellen
- Een DKIM record instellen

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 verwijs je naar Google's TXT record waarin zij hun mailservers up-to-date houden.	include:_spf.google.com
all	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: • `-all` wat de e-mail afwijst. • `~all` wat de e-mail markeert als verdacht. • `?all` wat de e-mail als neutraal markeert en het aan de e-mail client overlaat.	~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.

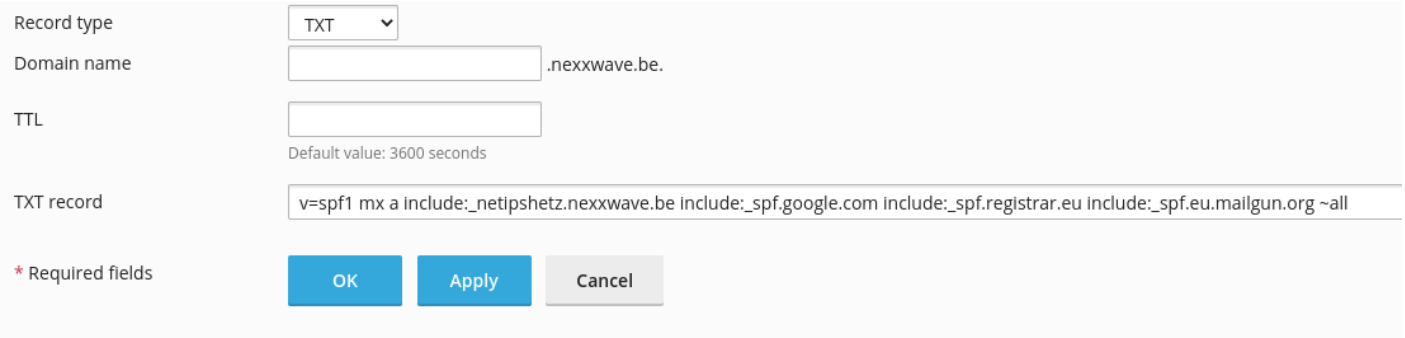
Start met `~all` om te voorkomen dat je mailservers bent vergeten op te nemen en je e-mails daardoor niet zullen toekomen bij de ontvanger. Na enkele weken kan je dit vervangen door `-all`.

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

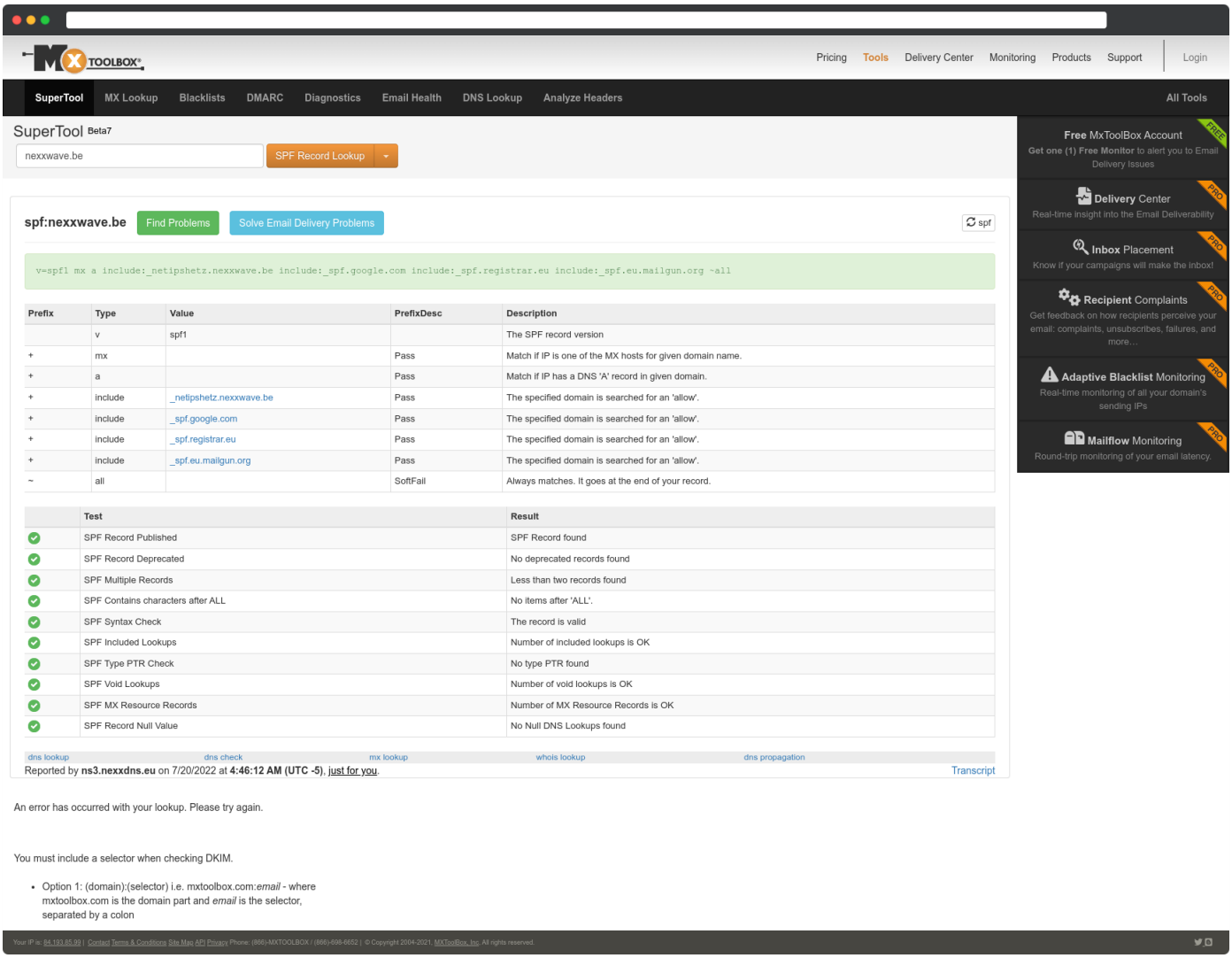
Zodra je je TXT record met je SPF gegevens samengesteld hebt, plaats je deze in de DNS van je domeinnaam. Dit doe je door in te loggen op het DNS beheerpaneel van je DNS provider.

- 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.



Stap 3: validatie van je DNS record

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:

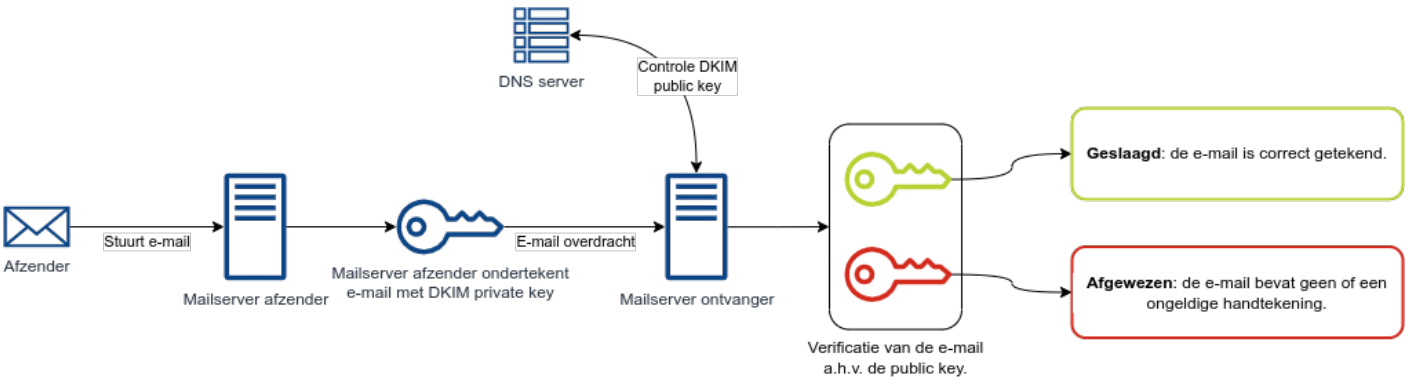
Je kan ook een validatie van je SPF record doen door vanaf al je e-mailservers een e-mail te sturen naar een (best extern) e-mailadres. In de headers van deze e-mail vind je terug of de SPF validatie geslaagd al dan niet geslaagd is:

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 Learn more
DKIM:	'PASS' with domain docs.nexxwave.be Learn more
DMARC:	'PASS' Learn more

Een DKIM record instellen

Wat is DKIM?

DKIM staat voor Domain Keys Identified Mail. DKIM wordt op zowel het niveau van een DNS record op je domeinnaam geregistreerd alsook op je e-mailserver. DKIM 'ondertekent' digitaal iedere e-mail wat je verzendt en stuurt die digitale handtekening mee in de 'headers' van iedere verzonden e-mail. De ontvanger controleert of de digitale handtekening in de e-mail overeenkomt met het publieke DNS record. Komt de digitale handtekening overeen? Dan is het zeker dat de e-mail en de bijlagen niet gewijzigd zijn.



DKIM werkt op basis van een private en een public key. Op je mailserver staat een private key geconfigureerd. Wanneer je mailserver een e-mail verzend, dan wordt dat bericht automatisch ondertekend met de private key. De ontvangende e-mailserver controleert deze handtekening aan de hand van de public key wat in het DNS record staat.

In zeven stappen ziet het technische DKIM teken- en validatieproces er als volgt uit:

1. Op je e-mailserver is een DKIM public key gegenereerd.
2. Een eindgebruiker stuurt een e-mail.
3. Deze e-mail komt terecht op je e-mailserver. Je e-mailserver tekent met de public key de e-mail en plaatst de handtekening in de headers van het e-mailbericht en verzend de e-mail naar de ontvanger.
4. Het bericht komt aan op de e-mailserver van de ontvanger.
5. De ontvangende e-mailserver vraagt de DNS records op van het domein wat achter het @-teken van het 'From' adres staat.
6. De ontvangende e-mailserver ziet in het DNS record dat er een public DKIM key opgegeven is.
7. Met behulp van deze public key valideert de ontvangende e-mailserver de handtekening in de headers van het e-mailbericht.

Stap 1: DKIM activeren door een private en public key te genereren

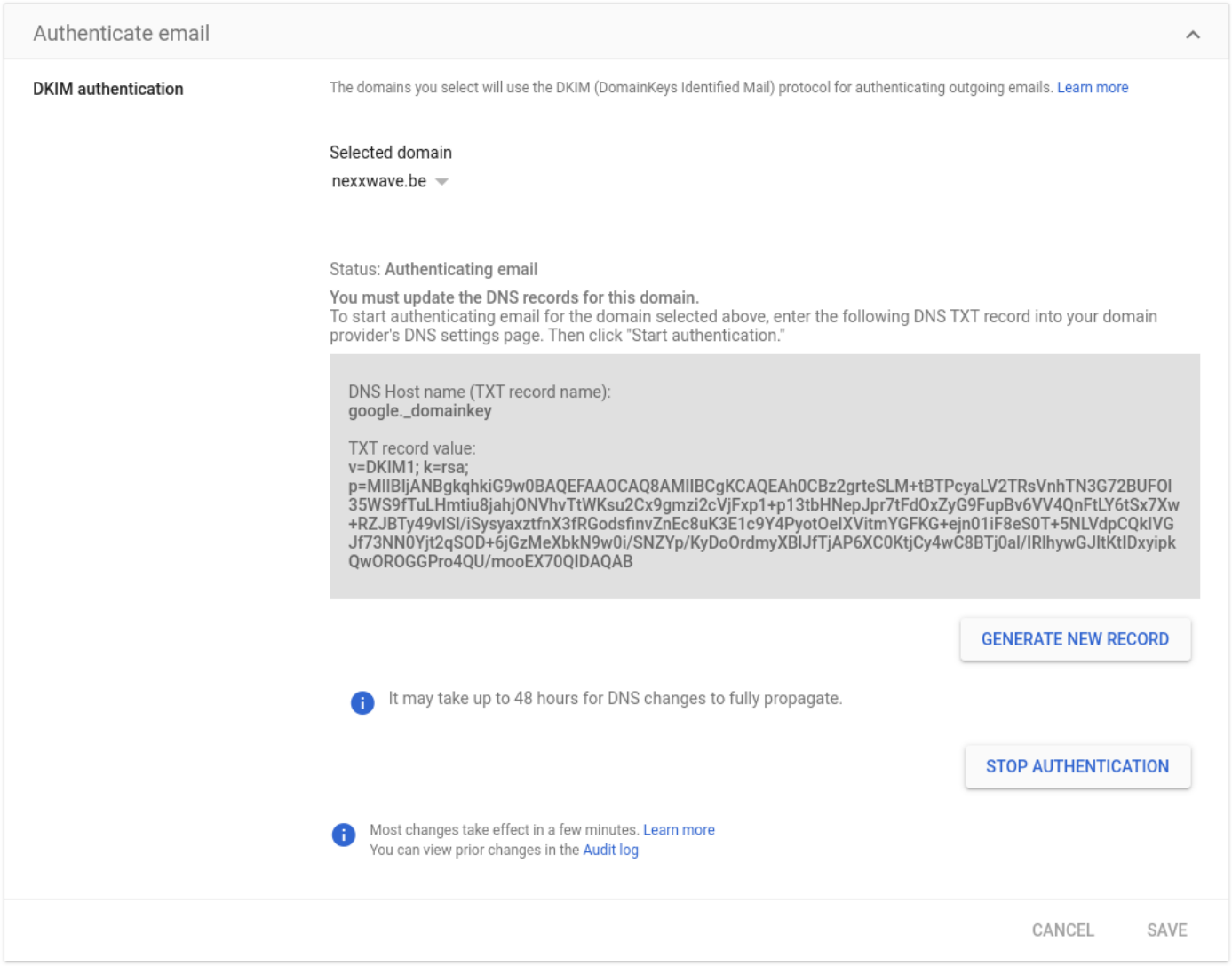
Om je berichten digitaal te ondertekenen, moet op je e-mailserver een public en private DKIM RSA keypair gegenereerd worden. Hoe je dat precies moet doen, is volledig afhankelijk van het type mailserver of de mailprovider wat je gebruikt.

Wanneer je DKIM geactiveerd hebt, dan krijg je van je mailprovider de '**public**' key te zien. Deze public key heb je straks nodig om in je DNS record te configureren.

Daarnaast krijg je ook een '**selector**'. Deze selector is uniek per e-mailserver. De selector van Google Workspace is bijvoorbeeld `google` en de selector van Plesk is `default`. Ook deze 'selectors' heb je straks nodig om je DNS record te configureren.

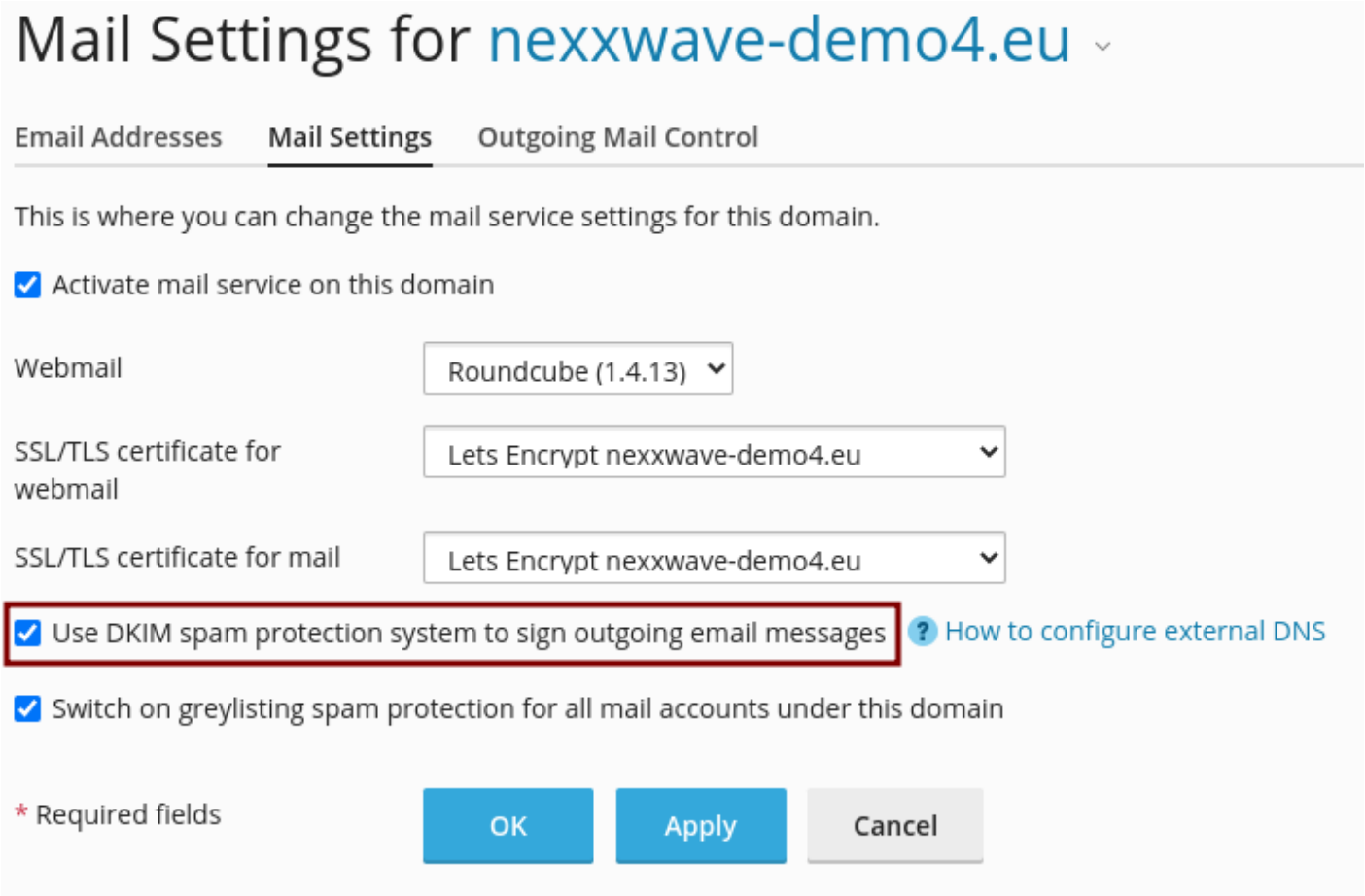
Een DKIM private/public key genereren in Google Workspace

Gebruik je Google Workspace als mailserver, dan kan je een DKIM private key genereren in het admin paneel onder 'Apps > Google Workspace > Settings for Gmail > Authenticate email'. Zodra je dat gedaan hebt, krijg je je public key te zien (deze heb je straks nodig).



Een DKIM private/public key genereren in Plesk

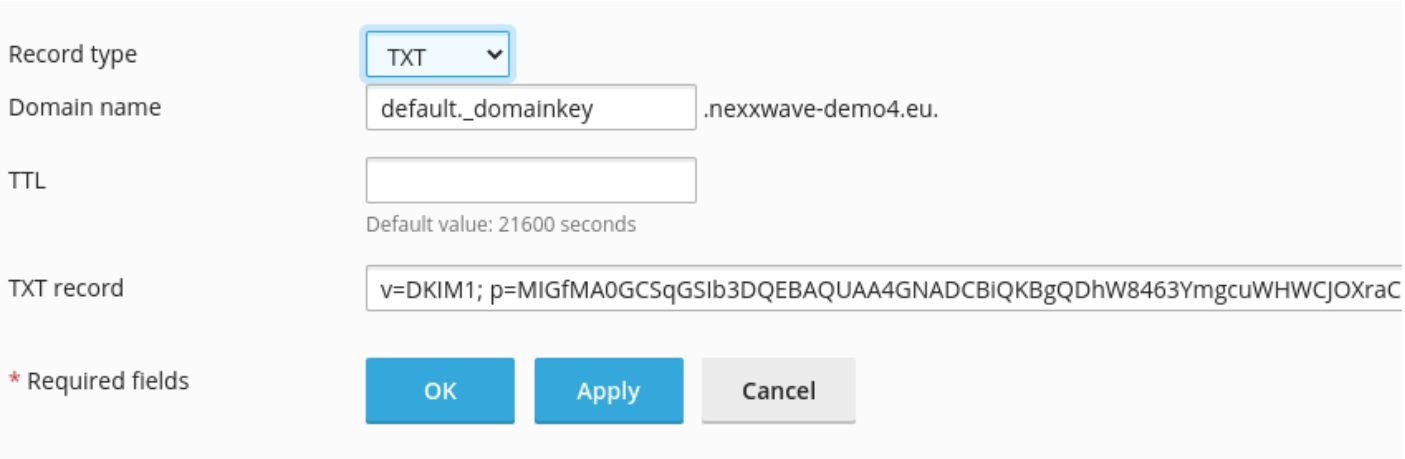
Gebruik je het Plesk controlepaneel, dan kan je een private key generen in je 'Mail Settings'. Klik op 'How to configure external DNS' om je public key te zien.



Stap 2: de public key in je DNS opnemen

Kopieer de public key wat je verkregen hebt bij het aanmaken van je private key. Deze key plaats je in de DNS instellingen van je domeinnaam. Dit doe je door in te loggen op het DNS beheerpaneel van je DNS provider.

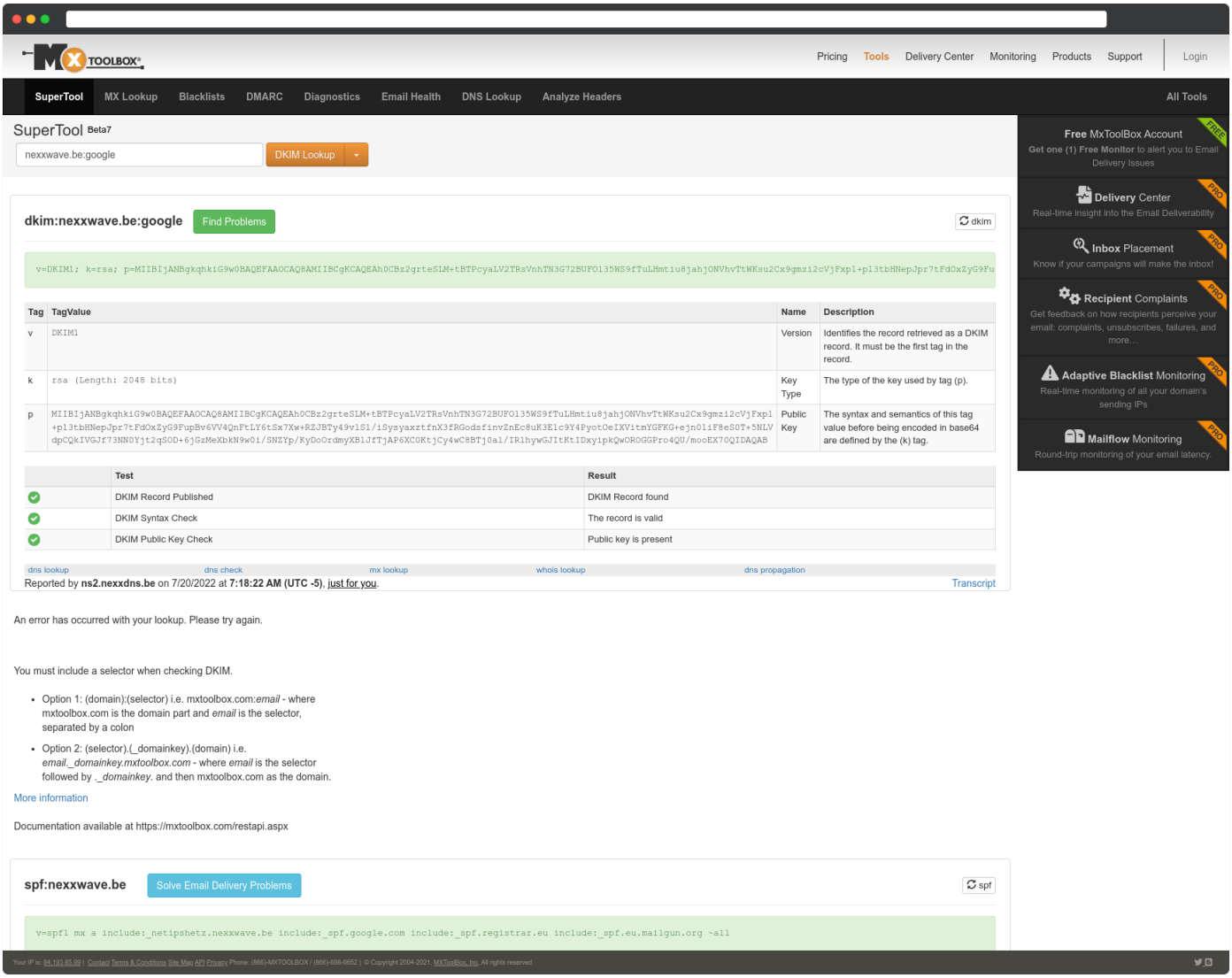
- Voeg een record van het type '**TXT**' toe.
- Afhankelijk van je domein provider, geef je als '**domeinnaam**' twee zaken op: je 'selector' gevolgd door `._domainkey`. Voor Google Workspace is dat bijvoorbeeld: `google._domainkey`.
- Als je het record ingeeft voor een subdomein, dan noteer je hier ook het subdomein. Bijvoorbeeld voor subdomein 'voorbeeld.nexxwave-demo4.eu' zou het record zijn: `google._domainkey.voorbeeld`.nexxwave-demo4.eu.
- 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 de public key wat je gekregen hebt. Afhankelijk van je domein provider, moet dit tussen "aanhalingstekens" getypt worden.



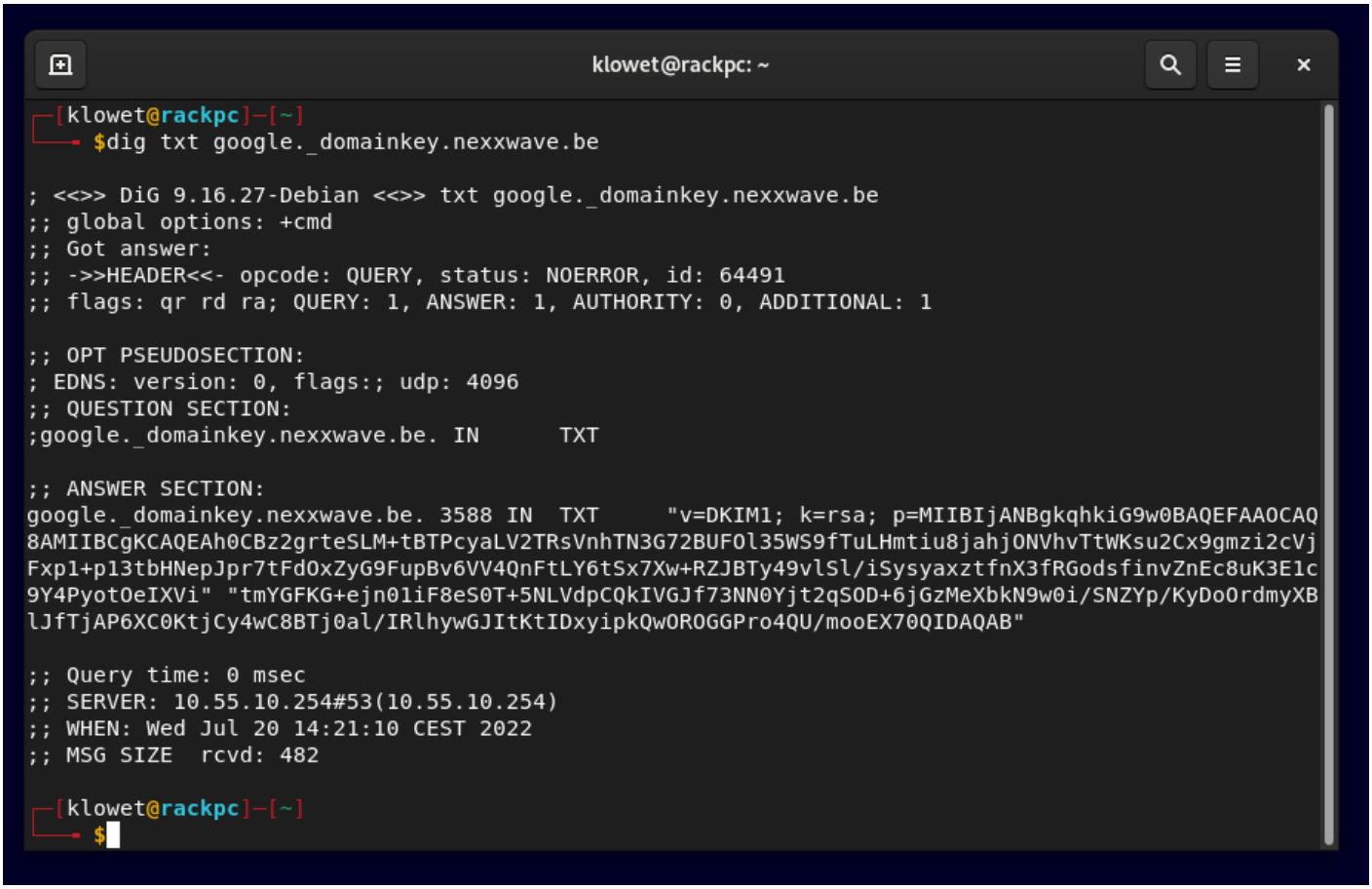
Stap 3: validatie van je DNS record

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:

Geef hiervoor het volledige adres van je TXT record op, met de 'selector'. Zoals in onderstaand voorbeeld: `google._domainkey.nexxwave.be`.



Vanaf je computer kan je via `dig` eenvoudig de TXT record van je (sub)domein opvragen. Hiervoor geef je ook weer het volledig adres, met selector, op.



Je kan ook een validatie van je DKIM 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 DKIM 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 Learn more
DKIM:	'PASS' with domain docs.nexxwave.be Learn more
DMARC:	'PASS' Learn more

Wil je dieper in de headers duiken, dan zal je in je headers `DKIM-Signature` tegenkomen. Zie dit voorbeeld:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=docs.nexxwave.be; s=nexx; t=1658239666;
bh=RbX1G9lD6lVhuqtj1C/P7MzkydOmr82ZR1IFtfu+pP8=; h=Date:Subject:From:To:From;
b=hHW8OWA8zh/pRKZ+smWDxmlLVQ21tdEb0rumXOhxyGig94uyGXGMIeTOjvQFcmw0H
 VXH+m/L/pieUSroXb4xDD6DhTWkSuhes/FTDM951fmVcwu3ViaGGD0AUDXhHxcMpUP
```

bJzI+vy7AEwN0q03pCoFsR6lyfhydfq/grGORRCqb+LgAKRNpaX8tyg5728XhRmMmM
ybgElQ5rUUo4VaTSUF2F1wRd3R+EC9iRKv4Odg/dim/RifTxql2r0J24Z9D+mYpdHU
WmxbdVbZfupQC5KAsGwJhqTXZvqUyLV3IrwSDAfk9S9OLRCwHBrDx1WUHyuLREwJ0Q
2yd5/eZ82Mbdg==

Hier vind je:

- `d=docs.nexxwave.be` = het domein van de afzender. De ontvangende e-mailserver gaat in de DNS records van dit domein de public DKIM key opzoeken.
- `s=nexx` = de selector wat in de e-mailserver geconfigureerd staat. Dus de ontvangende e-mailserver weet zo dat de public DKIM key te vinden is op adres nexx._domainkey.docs.nexxwave.be
- Vervolgens zie je de digitale handtekening achter `b=`.