

spf-dmarc-dkim

Test zone -> <https://www.appmaildev.com/fr/dkimModifier>

L'enregistrement SPF

L'enregistrement SPF, pour Sender Policy Framework, est un enregistrement tout bête qui permet d'indiquer au niveau des enregistrements DNS quels serveurs mails sont autorisés à envoyer des mails en votre nom. Rien d'autre.

Le principe est très simple, l'enregistrement devrait l'être aussi.

Ce que je vous conseille, et que normalement vous avez déjà, c'est d'avoir des enregistrements MX pour chacun de vos serveurs d'envoi d'email.

Si vous avez ça, alors, l'enregistrement SPF sera le plus simple du monde.

Vous faites simplement l'enregistrement suivant de type SPF (pour n'importe quel domaine) :

```
v=spf1 mx -all
```

La première partie, c'est la version de SPF, **mx** sert à indiquer que l'on doit se référer aux MX existants sur le domaine pour avoir le serveur d'envoi et le **-all** permet de rejeter tous les emails qui ne sont pas envoyés de vos serveurs.

Alors ça c'est la version tout le monde il est beau, tout le monde il est content, en production, j'éviterais quand même.

Personnellement, j'indique **MX**, au cas où on oublierait de modifier les DNS, mais je rajoute tous les enregistrements **A:** avec les enregistrements de mes serveurs. Aussi, il est possible que les enregistrements MX globaux soit mal traités par l'antispam de

destination (problèmes software ou autre).

Dernière chose, je remplace le **-all** par **~all**, ce qui permet de ne pas rejeter tout ce qui ne correspond pas en cas d'erreur légère sur le traitement du SPF (toujours si vous avez un antispam mal foutu de l'autre côté).

En gros, l'enregistrement réel pour mon domaine c'est ça :

```
v=spf1 mx a:mx1.nicolas-simond.ch a:mx2.nicolas-simond.ch a:mx3.nicolas-simond.ch ~all
```

L'enregistrement DKIM

Je résume vite fait, DKIM ajoute une signature chiffrée dans chaque entête d'email sortant (et juste une partie de l'entête, pas la totalité).

Cette signature, lorsque l'on réceptionne l'email permettra de savoir après déchiffrement si l'email a été altéré en cours de route.

La mise en place de DKIM se fait dans votre serveur email avant se faire dans le DNS.

- Pour Exchange : <https://www.abyssproject.net/2020/04/mettre-en-place-dkim-avec-exchange-2019/>
- Pour Office 365 : <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide>
- Pour tout ce qui est basé sur Postfix (le reste en gros) : <https://wiki.debian-fr.xyz/OpenDKIM>

dkim=selector

dkim._domainkey 14400 TXT "v=DKIM1;k=rsa;t=s;s=email;p=..key.."

L'enregistrement DMARC

Le dernier concurrent pour la fin. Toujours de façon simple, DMARC permet d'indiquer dans vos DNS ce qui doit se passer au cas où un serveur mail de destination aurait un souci avec vos enregistrements SPF ou DKIM, histoire que vous soyez prévenu.

Le côté maboulien du truc, c'est que vous pouvez indiquer depuis vos DNS de traiter tous VOS emails si jamais le destinataire n'arrive pas à valider votre SPF ou votre DKIM par exemple.

Si vous ne voulez pas que vos emails arrivent en quarantaine, mais que vous voulez avoir des rapports en cas de soucis, alors créez une règle comme ceci :

Enregistrement : `_dmarc`

Type : `TXT`

Contenu : `"v=DMARC1;p=none;sp=none;pct=100;rua=mailto:dmarc@domaine.com"`

Comme pour le SPF, on commence par la version du protocole.

S et **SP** c'est respectivement les actions à appliquer pour les emails non conformes aux enregistrements SPF/DKIM venant de votre domaine ou d'un sous-domaine (**none**, **quarantine** ou **block**).

PCT c'est le pourcentage d'email qui tombent sous le coup de DMARC, on indique 100 pour filtrer tous les emails.

RUA c'est l'adresse email qui recevra les rapports en cas de souci de conformité sur SPF et/ou DKIM.

Test[Modifier](#)

Attendez bien 30 minutes avant de vous lancer dans cette section.

Selon votre hébergeur, cela pourrait même prendre jusqu'à 48h avec les propagations DNS.

Rendez-vous sur <https://www.mail-tester.com/>, le site vous fournira une adresse mail, envoyez-y simplement un email de test depuis n'importe quelle adresse de votre Exchange et cliquez sur « Check your score ».

Étendez la troisième rubrique et regardez tout ce qui est en rouge sur ma capture, vous devriez être pareil pour le DKIM, le SPF et le DMARC :

<https://www.abysproject.net/wp-content/uploads/2020/04/dkim-spf-dmarc-1024x853.p>

Revision #1

Created 4 February 2021 23:32:00 by garfi

Updated 4 February 2021 23:32:38 by garfi