*Mise en place DMARC*

## Introduction

La mise en place de DMARC va permettre de rajouter une couche de sécurité sur SPF ou DKIM par exemple pour SPF dans le cas ou le serveur smtp qui transfère le mail n'est pas un serveur autorisé quel comportement le serveur destinataire doit -il adopter ?

On pourra lui dire de ne réaliser aucune action mais juste envoyer un rapport comme quoi il y'a eu une tentative d'usurpation ou demander de mettre en quarantaine ou rejeter.

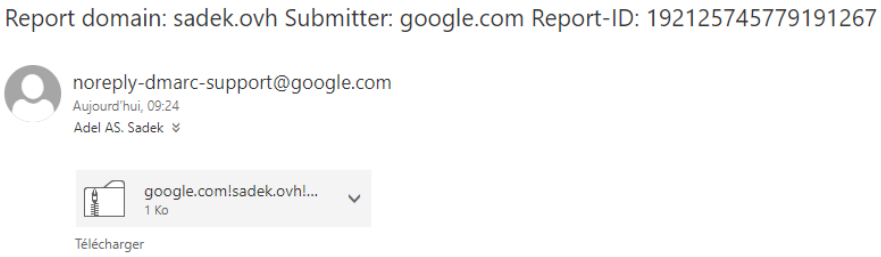
## Mise en place


- **aspf=s** :
  - **"s"** signifie *Strict*. Cela signifie que l'adresse de l'expéditeur dans l'en-tête "From" de l'e-mail doit correspondre exactement au nom de domaine de l'expéditeur dans l'enregistrement SPF pour que l'alignement SPF soit respecté. Idéal pour lutter contre le phishing, le spam, etc.
  - **"r"** signifie *Relaxed* (mode par défaut). Cela signifie que l'alignement SPF est respecté tant que le domaine de l'expéditeur dans l'en-tête "From" de l'e-mail et l'adresse de l'expéditeur dans l'enregistrement SPF partagent le même domaine principal (ce qui permet d'autoriser les sous-domaines).

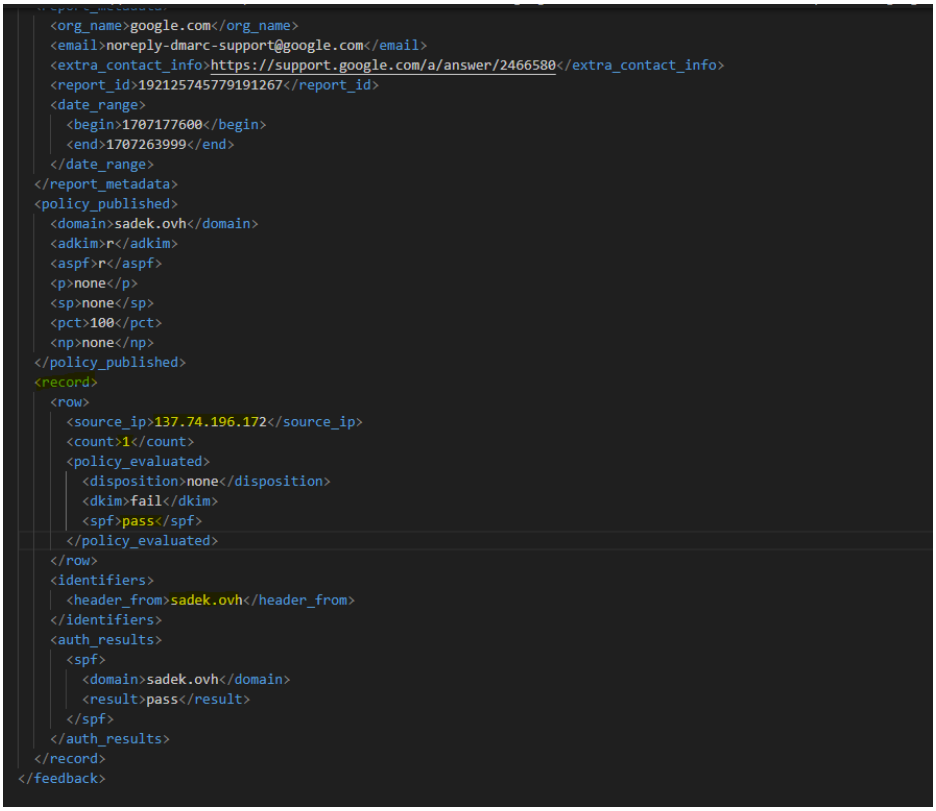
Résultat :


Le jour d'après le matin à 9h00

Je reçois ce mail




Un rapport DMARC qui mentionne cela



Il y’a tous les mails qui ont été envoyées récemment avec une adresse qui contient mon domaine

On y voit l’ip + le nombre de mails avec le test spf et dkim, je n’ai pas configuré DKIM c’est normal mais spf ça passe

On voit bien que ça nous permet de surveiller tous les mails envoyés avec des adresse qui comportent notre domaine.