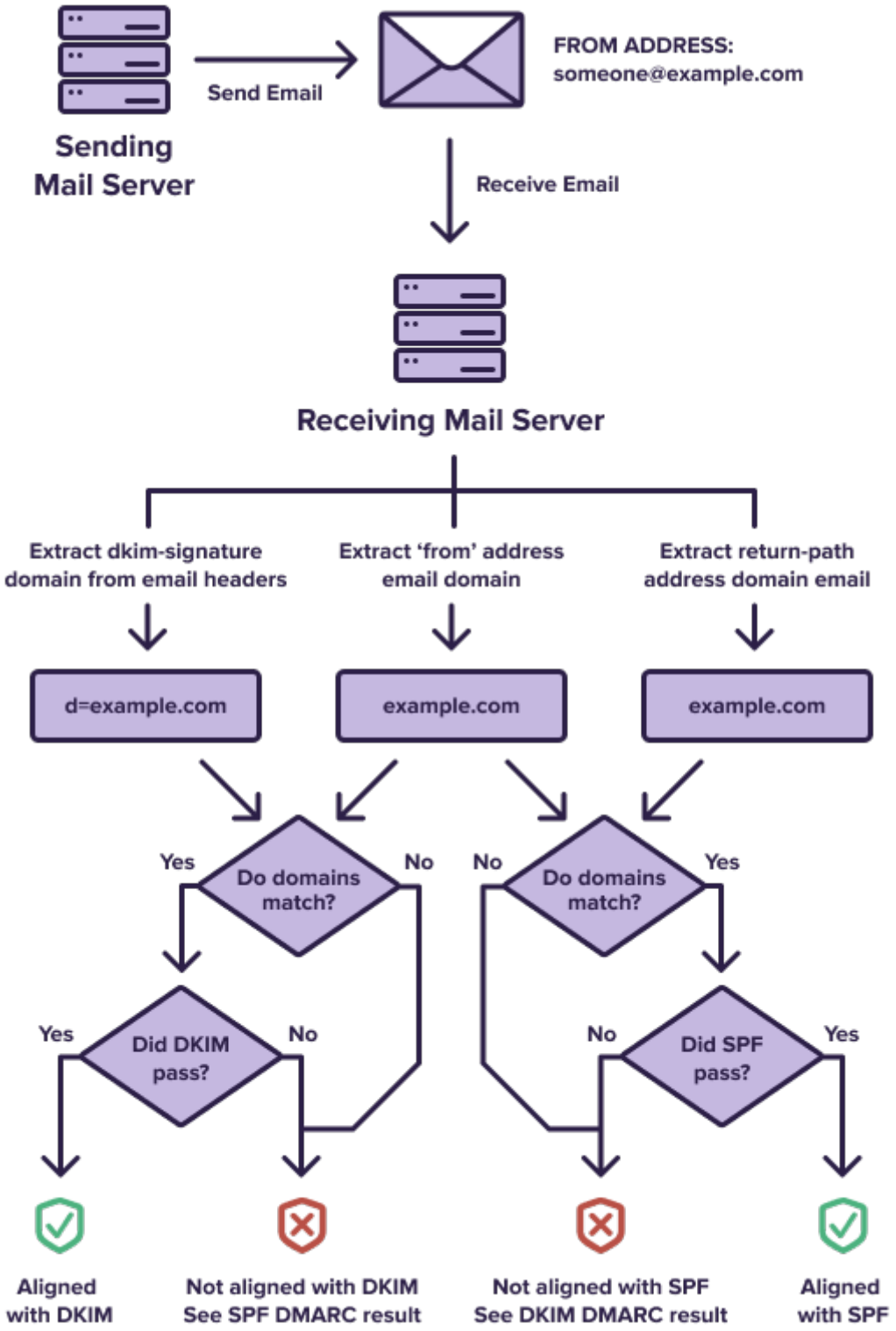
DMARC

Bienvenue

Pour accéder à cette page, vous devez être connecté. Pour vous connecter vous devez nous écrire via cette adresse: yogapartout@satoshi.yoga. Seulement les amis de TéléPartout peuvent se connecter.

Qu'est-ce que SPF – DKIM – DMARC et Auth SMTP

Ces accronymes peuvent faire peur à prime abord. C'est, pour plusieurs, inclus votre humble serviteur, un domaine sérieux qui par expérience personnelle peut devenir intimidant et totalement inintéressant. Pourtant, si vous prenez le temps d'étudier le tout, de vérifier ce qu’ils signifient vraiment, vous découvrirez que ces bibites déterminent la qualité de vos communications à savoir s'ils se rendent à leurs destinations.



Il est temps d'en apprendre un peu plus sur ce que sont SPF, DKIM, DMARC et Auth SMTP. Apprenez à configurer ces protocoles dans vos enregistrements DNS pour votre serveur de messagerie.... ... ... On commence par DMARC

Je ferai de mon mieux pour expliquer tout cela en termes simples.

DMARC

En résumé, DMARC est une mesure de sécurité pour les courriels qui protège votre domaine contre une utilisation malveillante et vous donne un meilleur contrôle sur la délivrabilité de vos courriels. Il repose sur les mécanismes SPF et DKIM.

Cet acronyme un peu étrange signifie Domain-based Message Authentication, Reporting and Conformance, soit, en français : **authentification, rapports et conformité des messages basés sur le domaine**. Mais qu'est-ce que cela veut dire concrètement?

DMARC vous permet de déterminer si un courriel que vous avez reçu a été envoyé légitimement par la personne qui prétend l'avoir envoyé. C'est la partie **authentification**.

Si le courriel ne réussit pas le test DMARC, il sera traité selon la politique DMARC qui a été définie par le destinataire — je décris cela plus en détail plus loin dans l'article. C'est la partie **conformité**.

DMARC permet aussi au serveur destinataire d'envoyer des rapports à l'expéditeur, en indiquant comment le message a été traité : a-t-il été accepté dans la boîte de réception principale, s'est-il retrouvé dans le dossier pourriels, ou a-t-il été rejeté? C'est la partie **rapports**.

En somme, DMARC permet aux serveurs qui reçoivent des courriels de vérifier si le message entrant correspond à ce qu'ils savent de l'expéditeur. Et si ce n'est pas le cas, DMARC indique aux serveurs destinataires quoi faire avec ce message.

DMARC n'est pas configuré par défaut. Vous devez le mettre en place vous-même si vous souhaitez ajouter une mesure de sécurité supplémentaire à vos mécanismes SPF et DKIM.

Pourquoi DMARC est-il important?

Il y a trois raisons principales pour lesquelles DMARC est très utile pour les utilisateurs de courriel.

1. C'est une mesure de sécurité

Du côté de l'expéditeur, DMARC protège votre domaine contre les utilisations non autorisées, par exemple par des fraudeurs qui tentent de voler des renseignements personnels par hameçonnage.

Du côté du destinataire, DMARC rend plus difficile l'arrivée de courriels frauduleux dans la boîte de réception principale.

DMARC protège contre l'usurpation de domaine, aussi appelée domain spoofing. Cela se produit lorsqu'une personne non autorisée essaie d'utiliser votre domaine pour se faire passer pour vous, ou pour quelqu'un qui travaille dans votre entreprise, afin de tromper une autre personne. Le but est souvent de voler des données personnelles, comme des identifiants de connexion ou un numéro de carte de crédit.

2. Il vous aide à mieux contrôler la délivrabilité de vos courriels

Un autre avantage de DMARC est qu'il vous permet de mieux contrôler combien de vos courriels sont considérés comme légitimes et arrivent dans la boîte de réception principale de vos destinataires.

Et si quelqu'un essaie de se faire passer pour vous et d'envoyer des courriels en votre nom, DMARC peut vous aider à le détecter — j'y reviendrai dans un instant.

3. Il protège la réputation de votre marque

Si quelqu'un se fait passer pour vous et essaie de convaincre des gens de lui envoyer de l'argent ou des renseignements personnels, cela nuit à votre image de marque. DMARC aide à éviter ce genre de situation.

DMARC est publié dans le DNS par le propriétaire du domaine, aux côtés de SPF et DKIM. Il s'agit d'un simple

enregistrement d'une seule ligne.

Voici un exemple :

```
v=DMARC1; p=none; rua=mailto:sandra.wilk@woodpecker.co;
```

Comment fonctionne DMARC?

DMARC précise ce qui doit se produire pour qu'un message puisse arriver dans la boîte de réception, ainsi que ce qui doit arriver si les conditions ne sont pas respectées.

Lorsqu'un courriel est testé par DMARC, quatre choses peuvent — ou devraient — se produire :

a) **Validation** DKIM **réussie**:

La signature additionnelle placée dans l'en-tête du courriel doit être validée. La clé privée correspond à la clé publique publiée dans le DNS.

b) **Alignement** DKIM:

Le domaine parent doit correspondre au domaine indiqué dans le champ **Header From**.

c. **Validation** SPF réussie:

Le serveur destinataire prend le domaine inclus dans l'adresse **Envelope From**, vérifie s'il existe un enregistrement SPF et vérifie si l'adresse IP de l'expéditeur est incluse dans cet enregistrement SPF.

d) **Alignement** SPF:

Le domaine indiqué dans Envelope From doit correspondre au domaine indiqué dans le champ **Header From** du courriel.

Un message échouera au test DMARC s'il échoue à la fois aux tests SPF et DKIM.
Gardez toutefois en tête que si vous transférez un message, seul DKIM reste généralement aligné.

Attendez… SPF et DKIM ne servent-ils pas déjà à protéger les courriels?

Les mécanismes SPF et DKIM servent tous les deux à protéger contre les utilisations non autorisées. Le problème, toutefois, est qu'ils fonctionnent de façon isolée.

Il n'existe pas de règle universelle indiquant ce que le serveur destinataire doit faire lorsque ces vérifications échouent. Chaque destinataire traite les messages échoués différemment. Par exemple, un serveur peut les envoyer directement dans le dossier pourriels, tandis qu'un autre peut leur faire passer des tests supplémentaires pour déterminer où les placer.

Sans compter que le propriétaire du domaine ne reçoit aucune information sur ses courriels ni sur le fait qu'ils aient atteint ou non la boîte de réception principale du destinataire.

DMARC nous permet de définir nos propres règles pour traiter un courriel non conforme, ce qui réduit le risque que notre domaine soit usurpé.

Il permet aussi d'envoyer des rapports à l'expéditeur.

Ajouter un enregistrement DMARC au DNS vous permet donc d'établir des règles pour les courriels entrants : doivent-ils être mis en quarantaine, rejetés ou acceptés?

Politiques DMARC et rapports

Il existe trois politiquesDMARC possibles :

- **None**
- **Quarantaine**
- **Reject**

Dans le contexte du courriel, cela signifie qu'avec une politique **none**, tous les courriels passent, même s'ils ne réussissent pas les tests SPF ou DKIM.

Avec une politique **quarantaine**, les courriels qui échouent aux tests sont redirigés vers le dossier pourriels.

Avec une politique **reject**, les courriels sont rejetés et retournés à l'expéditeur.

Quelques jours après avoir publié un enregistrement DMARC dans le DNS, vous commencerez à recevoir des rapports provenant des fournisseurs de services Internet. Ces rapports incluront des statistiques sur tous les courriels envoyés depuis votre domaine, y compris ceux qui prétendent provenir de votre domaine.

Si vous voyez plus de courriels que ceux que vous avez réellement envoyés, cela signifie qu'une autre personne utilise votre domaine.

Le rapport vous donnera une vue d'ensemble claire de la provenance des courriels et indiquera s'ils auraient été bloqués par une politique **quarantaine** ou **reject**.

Ces rapports vous permettent aussi d'évaluer la santé de vos messages sortants. Que contiennent-ils? Ils indiquent notamment comment les messages ont été traités selon les politiques DMARC mises en place, quelles adresses IP ont utilisé votre domaine pour envoyer des courriels, combien de messages ont été envoyés, ainsi que les résultats SPF et DKIM.

Ces rapports peuvent être lus avec un outil comme **Postmark** ou dmarcian. Vous pouvez aussi utiliser MxToolBox

Comment configurer DMARC?

D'abord, il faut commencer à configuer/vérifier si SPF et DKIM sont bien configurés.

1.Configurer SPF et DKIM

Si vous avez déjà réfléchi à la délivrabilité, vérifié que vos courriels (tous) se rendent bien à destination, cela veut dire que la config SPF et DKIM est déjà faite.

2.Générer un enregistrement DMARC, par exemple à l'aide d'un générateur en ligne

Nous utilisons dmarcian.com, ils ont un testeur qui fonctionne. Pas besoin de vous inscrire.

3.Pour commencer, choisir la politique “none” pour tous les courriels.

4.Ajouter votre enregistrement DMARC au DNS.

5.Modifier la politique au fur et à mesure, selon les données obtenues.

TaDa, c'est fait!

Analysez plusieurs rapports DMARC reçus. Une fois que vous comprenez comment interpréter les politiques DMARC, vous pouvez passer de **none à quarantaine**, puis éventuellement à **reject**.

Vous n'êtes plus connecté

Contact

Utilisez notre adresse yoga: yogapartout @ satoshi.yoga