SPF

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 SPF...

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

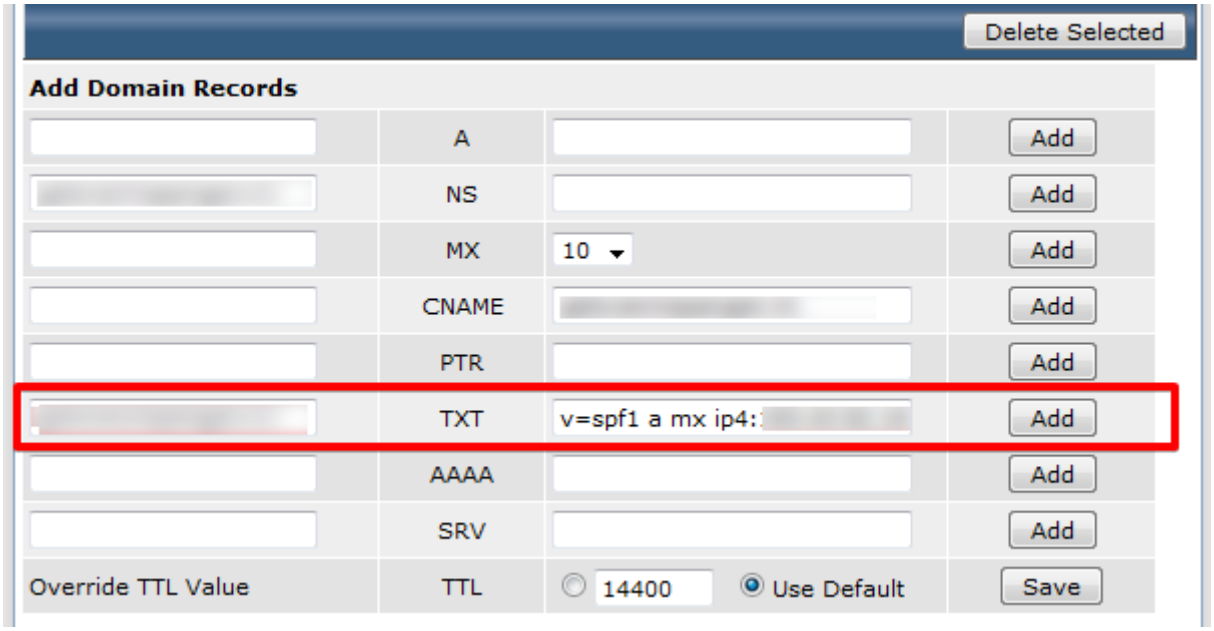
SPF

Comment fonctionne SPF

La courte définition de de SPF: Sender Policy Framework

SPF est un mécanisme de sécurité créé pour empêcher les personnes malveillantes d'envoyer des courriels en votre nom.

Exemple d'entrée SPF dans un panneau DNS



Ce mécanisme repose sur la communication entre les serveurs DNS.

Supposons que vous ayez envoyé un courriel à Marie. SPF permet au serveur de Marie (donc, ça passe par le

DNS en tout premier lieu) de savoir que ce courriel a bel et bien été envoyé par vous. Le problème, c'est qu'il ne le sait pas vraiment. À moins que vous ayez configuré SPF sur votre serveur DNS.
SPF définit quelles adresses IP sont autorisées à envoyer des courriels à partir de votre domaine. Imaginons donc deux «conversations» possibles entre serveurs. Pour faciliter la compréhension, supposons que vous vous appelez Georges.

Scénario 1 – Vous n'avez pas configuré SPF

Votre serveur (George): Bonjour serveur de Marie. Ici George, j'ai un nouveau pour vous Marie.
Le serveur de Marie : Bonjour serveur de Marie. Quel est votre SPF?
Le serveur George: Oui, à propos du SPF… Franchement, qui s'en soucie? Je n'en ai pas. Fais-moi confiance, c'est moi George.
Le serveur de Marie : Si tu n'as pas de SPF, je ne peux pas être certain que c'est bien toi Marie qui a envoyé ce message. Donne-moi la liste des adresses IP autorisées par George, pour que je puisse la comparer avec la tienne.
Le serveur de George : Je n'ai pas la liste des adresses IP autorisées par George.
Le serveur de Marie: Alors je ne veux pas de ton message. Livraison refusée. Désolé, mon ami…

Scénario 2 – Vous avez bien configuré SPF

Le serveur (George): Bonjour serveur de Marie. Ici George, j'ai un nouveau message pour vous Marie.
Le serveur de Marie : Bonjour serveur de George. Quel est votre SPF?
Le serveur George : Le voici : voici mon SPF. Il contient toute une liste d'adresses IP que George lui-même a déclarées comme étant autorisées à envoyer des courriels en son nom.
Le serveur de Marie : D'accord, voyons voir… Le message que vous voulez me transmettre a été envoyé depuis l'adresse IP 108.108.108.08. Parfait, elle est bien dans votre liste. Tout semble correct. Donnez-moi le message, je vais le montrer à Marie. Merci!

La morale de ces deux petits dialogues est la suivante: configurez votre SPF. Si vous ne le faites pas, vous risquez que votre courriel soit piraté ou usurpé, ou encore d'avoir l'air d'un expéditeur douteux. Résultat : une partie de vos courriels pourrait ne jamais être livrée.

Voir

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

Contact

Utiliser notre adresse yoga: yogapartout@satoshi.yoga