

# Sécuriser l'acheminement du courrier

Pour sécuriser votre serveur de messagerie et l'envoi de vos mails, nous vous recommandons d'utiliser les trois protocoles suivants :

## SPF

Le Sender Policy Framework (SPF) permet de déclarer votre serveur de messagerie comme étant autorisé à émettre du courrier pour votre (vos) domaine(s).

Pour le configurer, vous n'avez qu'un seul enregistrement DNS à ajouter :

Type :

Hôte:  (selon votre fournisseur DNS, il peut s'agir de votre nom de domaine  (avec un point final), d'une chaîne vide, d'un , etc.)

Valeur :

## DKIM

DomainKeys Identified Mail (DKIM) est une méthode d'authentification du courrier électronique conçue pour lutter contre l'usurpation d'identité.

Pour le configurer, vous devez ajouter deux enregistrements DNS. Pour obtenir ces deux enregistrements spécifiques, il suffit d'accéder à [l'interface Plesk de votre serveur](#), puis :

1. cliquez, dans le menu latéral gauche, sur **Boîte mail** ;
2. cliquez sur l'onglet **Paramètres de la messagerie** ;
3. cochez la case **Utiliser le système anti-spam DKIM[...]** au bas de la page ;
4. récupérer les 2 enregistrements DNS à ajouter en cliquant sur **Comment configurer le DNS externe**.

## DMARC

Une fois que SPF et DKIM sont configurés et opérationnels, vous pouvez régler le Domain-based Message Authentication, Reporting and Conformance (DMARC), un protocole standard d'authentification du courrier électronique, en ajoutant simplement un enregistrement DNS supplémentaire :

Type :

Hôte :

Valuer :

Si vous configurez DMARC avant de configurer et de valider SPF et DKIM, vous ne pourrez pas envoyer correctement des courriels à partir de votre serveur.

## Tester votre configuration

Pour tester votre configuration SPF + DKIM + DMARC, vous pouvez utiliser des outils tels que :

- [Red Sift's Investigate tool](#)
- [M@ilGenius](#)
- [Mail-Tester](#)

---

Revision #6

Created 6 November 2023 14:09:34 by Pierre Lannoy

Updated 6 November 2023 15:05:36 by Pierre Lannoy