COMMENT CONFIGURER DMARC POUR VOTRE ENTREPRISE

Avant de se voir attribuer un certificat VMC (Verified Mark Certificate), une entreprise doit d'abord se conformer au protocole DMARC (Domain-based Message Authentication, Reporting & Conformance). Découvrez dans ce guide toutes les mesures à prendre pour garantir une bonne implémentation de DMARC.

digicert®

DMARC, C'EST QUOI ?

DMARC est un protocole de politiques, de reporting et d'authentification d'e-mails qui permet aux entreprises de protéger leur domaine contre toute utilisation non autorisée (usurpation d'identité, attaques de phishing, etc.).

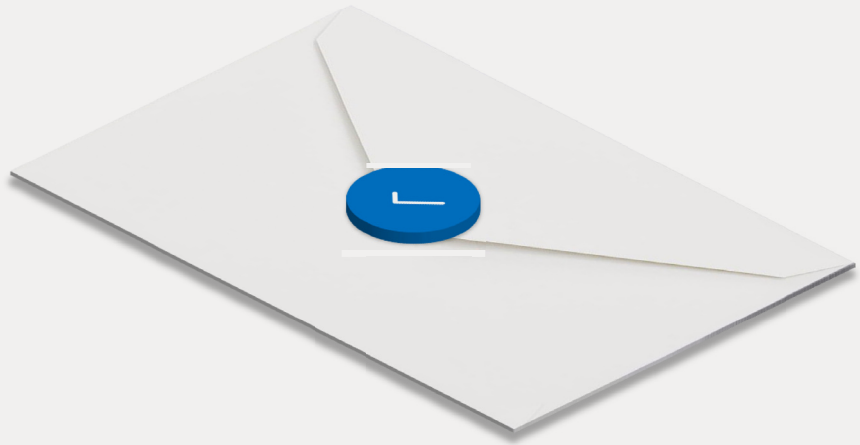
DMARC en quelques points :

- Enregistrement TXT dans le registre DNS qui permet aux destinataires de vos e-mails de vérifier l'authenticité des messages reçus.
- Conçu pour s'intégrer au processus existant d'authentification des communications entrantes d'une entreprise, DMARC aide les destinataires à vérifier qu'un message présente bien tous les attributs connus sur l'expéditeur.
- Les entreprises peuvent choisir parmi trois configurations pour traiter les messages en apparence suspects :

- « p=none » (aucune règle activée)
- « p=quarantine » (mise en quarantaine)
- « p=reject » (refus)

- Pour un fonctionnement optimal de DMARC, les protocoles SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail) doivent être paramétrés au préalable.
- L'enregistrement DMARC d'une entreprise peut être vérifié au moyen d'outils disponibles sur Internet tels que le site valimail.com.

digicert®



DMARC : POINT DE DÉPART D'UNE MEILLEURE AUTHENTIFICATION DES E-MAILS

L'objectif du protocole DMARC est de créer un réseau d'expéditeurs et de destinataires qui collaborent pour améliorer les pratiques d'authentification des expéditeurs et permettent aux destinataires de refuser les messages non authentifiés.

digicert®

LA DIFFÉRENCE DMARC

En adoptant le protocole DMARC, les entreprises bénéficient d'avantages sur quatre fronts essentiels :

1. **Sécurité**

   Bloquez l'utilisation frauduleuse de votre domaine de messagerie pour protéger vos destinataires des campagnes de spams, fraudes et phishing.

2. **Visibilité**

   Obtenez des rapports détaillés sur les individus et/ou systèmes qui utilisent votre domaine pour envoyer des e-mails.

3. **Livrabilité**

   Augmentez de 5 à 10 % les taux de délivrabilité dans les boîtes mail de vos destinataires et évitez que vos e-mails ne soient signalés comme spams.

4. **Protection de la marque**

   Défendez votre marque contre les attaques par usurpation d'identité.

des clients sont moins enclins à interagir avec une marque après avoir subi une attaque de phishing usurpant l'identité de celle-ci.

CONFIGURATION SPF : MODE D'EMPLOI

1. **Faites l'inventaire des adresses IP qui serviront à envoyer des e-mails depuis votre domaine, y compris :**
    - Serveur web
    - Serveur de messagerie interne
    - Serveur de messagerie du FAI
    - Autres serveurs de messagerie externes
2. **Dressez une liste des domaines d'envoi, mais aussi de ceux qui ne serviront pas à l'envoi d'e-mails.**
3. **Créez un enregistrement SPF au format .txt pour chaque domaine à l'aide d'un éditeur de texte (Notepad ++, Vim, Nano, etc.)**

   Exemple 1 : v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -all
   Exemple 2 : v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:autremessagerie.fr -all

4. **Publiez l'enregistrement SPF sur votre registre DNS.**

   Si vous gérez vous-même votre DNS, il vous suffit d'ajouter un nouvel enregistrement TXT contenant le texte SPF. Sinon, demandez à l'administrateur de votre serveur d'ajouter l'enregistrement.

5. **Vérifiez ensuite votre registre DNS à l'aide d'un outil de vérification SPF.**

digicert®

LE SPF, C'EST QUOI ?

Ne laissez pas des expéditeurs non autorisés ternir votre réputation

Le standard SPF a révolutionné le concept d'authentification des e-mails basée sur les domaines. Il empêche l'usurpation d'identité en permettant au propriétaire d'un domaine d'approuver automatiquement les adresses IP des serveurs autorisés à envoyer des e-mails sous le nom dudit domaine. En clair, si l'adresse IP d'un serveur de messagerie ne figure pas sur la liste, tout e-mail envoyé depuis le domaine en question échouera au test d'authentification SPF.

CONFIGURATION DKIM : MODE D'EMPLOI

1. **Choisissez un sélecteur DKIM.**

   Il doit s'agir d'une simple chaîne de texte définie par l'utilisateur qui sera ajoutée au nom de domaine pour aider à identifier la clé publique DKIM (ex. « standard »).

   Exemple : « standard._domaine.exemple.fr » = nom d'hôte

2. **Générez une paire de clés publique/privée pour votre domaine.**

   - Les utilisateurs Windows peuvent utiliser PUTTYGen
   - Les utilisateurs Linux et Mac peuvent utiliser ssh-keygen

3. **Créez et publiez un nouvel enregistrement TXT.**

   Créez un nouvel enregistrement depuis votre console de gestion DNS à l'aide de la clé publique générée.

   Exemple : v=DKIM1; p=Votreclépublique

digicert®

LE DKIM, C'EST QUOI ?

Prévenez toute altération de vos e-mails en cours de route

DKIM est un standard d'authentification des e-mails qui se base sur la cryptographie à clé publique/privée pour signer des e-mails.

Il permet de vérifier si le message provient bien du domaine associé à la clé DKIM et si l'e-mail n'a pas été modifié pendant son acheminement.

CONFIGURER DMARC EN MODE DE SURVEILLANCE

1. **Assurez-vous d'avoir correctement paramétré les protocoles SPF et DKIM**

2. **Créez un registre DNS**

   Le nom de l'enregistrement DMARC « txt » doit ressembler à ceci :
   « _dmarc.votre-domaine.fr. »

   Exemple : « v=DMARC1;p=none; rua=mailto:rapportsdmarc@votre-domaine.fr »

   Si vous gérez vous-même le DNS de votre domaine, créez un enregistrement DMARC « p=none » (mode de surveillance)
   de la même manière que pour les enregistrements SPF et DKIM.

   Sinon, demandez au gestionnaire de votre DNS de créer l'enregistrement DMARC pour vous.

3. **Testez votre enregistrement DMARC à l'aide d'un outil de vérification DMARC**

   Remarque : la durée de réplication se situe généralement entre 24 et 48 heures.
   Outil de vérification DMARC

digicert®

LE MODE SURVEILLANCE DMARC, C'EST QUOI ?

Bénéficiez d'une visibilité sur tous les messages envoyés depuis votre domaine

Le mode surveillance (ou monitoring) permet aux propriétaires de domaine de consulter des rapports DMARC portant sur tout le trafic e-mail rattaché à leur domaine.

Ces rapports signalent les messages qui seront soit mis en quarantaine, soit refusés lorsque les règles DMARC seront mises en application. Ils affichent également des informations sur tous les systèmes et services qui envoient des e-mails à partir du domaine surveillé.

REMARQUE : en mode surveillance, aucune règle n'est appliquée. Les e-mails dont l'authentification a échoué sont envoyés normalement pour éviter toute perturbation pendant la phase d'implémentation de DMARC.

digicert®

ÉTIQUETTES COURAMMENT UTILISÉES DANS LES ENREGISTREMENTS DMARC .TXT

NOM DE L'ÉTIQUETTE	OBLIGATOIRE	OBJET
V	OBLIGATOIRE	VERSION DU PROTOCOLE
P	OBLIGATOIRE	VERSION DU POLITIQUE
PCT	FACULTATIVE	% D'E-MAILS À FILTRER
RUA	FACULTATIVE	ADRESSE E-MAIL À LAQUELLE SONT ENVOYÉS LES RAPPORTS DE SITUATION AGRÉGÉS
SP	FACULTATIVE	POLITIQUE POUR LES SOUS-DOMAINES

digicert®

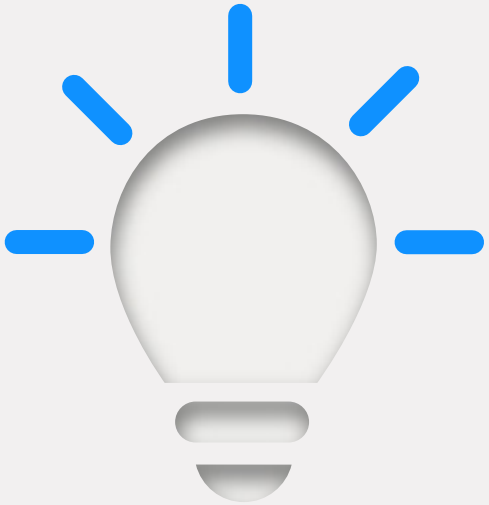
INFORMATIONS FOURNIES PAR LES RAPPORTS DMARC

Les rapports indiquent aux propriétaires de domaine le nombre de messages frauduleux qui ont utilisé leur domaine et la provenance de ces messages, tout en précisant s'ils seraient mis en quarantaine ou refusés une fois les règles DMARC appliquées.

Un rapport pour chaque destinataire est disponible au format XML et inclut les éléments suivants :

- Nombre de messages provenant de chacune de ces adresses IP
- Mesures appliquées à ces messages selon la règle DMARC activée
- Résultats SPF pour ces messages
- Résultats DKIM pour ces messages

Bien qu'il soit lisible, le format XML n'est pas toujours pratique. Pour plus de simplicité, les propriétaires de domaine pourront recourir à un logiciel de traitement de rapports DMARC, tel que Valimail ou autre.



RAPPORTS DMARC : 4 MODES D'UTILISATION

Établissez une base de référence fiable avant d'activer les règles DMARC

1. Identifiez le trafic signalé comme illégitime.

2. Repérez les e-mails légitimes signalés comme illégitimes par DMARC. Selon la règle configurée, ces e-mails seraient soit rejetés, soit mis en quarantaine.

3. Contactez les propriétaires de systèmes/applications concernés pour vérifier l'authenticité des e-mails signalés comme illégitimes.

4. Le cas échéant, actualisez votre enregistrement SPF en ajoutant les adresses IP légitimes à la liste d'autorisation.

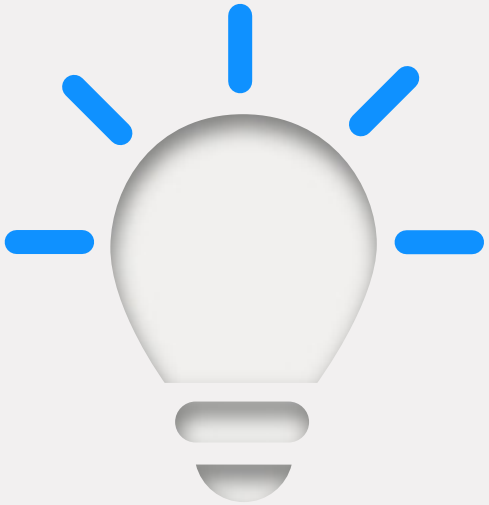
digicert®

EXPLOITEZ LES DONNÉES DES RAPPORTS POUR EFFECTUER LES DERNIERS RÉGLAGES AVANT D'ACTIVER DMARC

L'analyse des rapports DMARC peut certes prendre du temps, mais elle est indispensable. En effet, si les propriétaires de domaine identifient à tort des expéditeurs comme illégitimes, des e-mails authentiques pourront être refusés ou mis en quarantaine lorsque la règle DMARC sera mise en application. Le temps perdu à régler les problèmes pourra alors faire dérailler tout le projet.

D'où l'importance de prendre quelques mesures en interne avant d'appliquer les règles DMARC :

- Dressez l'inventaire de tous les expéditeurs identifiés dans les rapports DMARC et toute autre adresse fournie par les parties prenantes
- Identifiez les propriétaires de chaque adresse/service de messagerie
- Classez les services d'envoi en trois catégories : autorisés, non autorisés ou malveillants
- Avec l'aide des personnes concernées, identifiez tout autre expéditeur absent du rapport DMARC
- Consultez les parties prenantes pour chaque nouvel expéditeur identifié
- Ajoutez l'adresse IP de tout nouvel expéditeur légitime identifié à votre enregistrement SPF



COMMUNICATION AVANT MISE EN APPLICATION

5 conseils pour améliorer l'adoption de DMARC

- Rédigez une politique d'implémentation à faire circuler auprès de toutes les parties prenantes
- Contactez un service DMARC comme Valimail si la tâche est trop complexe ou si vous avez besoin d'assistance
- Communiquez les résultats des rapports DMARC dès qu'ils sont disponibles
- Commencez par déployer DMARC à petite échelle en interne
- Ralliez l'équipe dirigeante à votre projet

COMBIEN DE TEMPS DMARC DOIT-IL RESTER EN MODE SURVEILLANCE ?

La période de surveillance varie d'une entreprise à l'autre, les grands groupes tendant à y consacrer plus de temps que les petites structures. Vous pouvez tabler sur un processus allant de plusieurs semaines à plusieurs mois.

Dès lors que votre inventaire est terminé, que tous les expéditeurs autorisés ont été répertoriés et que votre entreprise est suffisamment informée, vous pouvez passer au mode quarantaine.

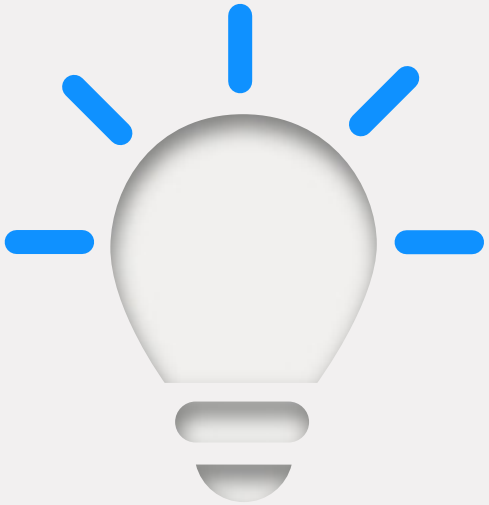
Lorsque le mode quarantaine est activé, les messages qui ne parviennent pas à être authentifiés sont mis en quarantaine. Autrement dit, ces messages atterrissent généralement dans le dossier spam du destinataire.

COMMENT CONFIGURER DMARC EN MODE QUARANTAINE

1. **Connectez-vous à votre serveur DNS et identifiez votre enregistrement DMARC.**
2. **Ouvrez l'enregistrement DMARC correspondant au domaine spécifié et modifiez la politique de « p=none » à « p=quarantine ».**
   Exemple : « v=DMARC;p=quarantine;pct=10;rua=mailto:rapportsdmarc@votre-domaine.fr »
3. **Ajoutez l'étiquette « pct » (% d'e-mails à filtrer). Nous recommandons de commencer par un taux de 10 %.**
4. **À mesure que vous vous familiarisez avec le protocole, augmentez progressivement le pourcentage d'e-mails à filtrer jusqu'à atteindre « pct=100 » (100 %).**

NOTE : pour être conforme aux standards BIMI et VMC, la règle DMARC doit être paramétrée à « pct=100 » en mode « quarantine » ou « reject ».

digicert®



SIGNALEMENT DES E-MAILS SUSPECTS : MODE D'EMPLOI

- Si une règle autre que « p=none » est spécifiée, cette règle peut être appliquée au pourcentage de l'étiquette « pct »
- Une règle moins restrictive sera alors appliquée au reste des e-mails (p. ex. : pour un enregistrement DMARC affichant « p=quarantine » et « pct=10 », 10 % du trafic sera filtré puis mis en quarantaine le cas échéant, tandis que 90 % du trafic sera envoyé normalement)

digicert®

UNE FOIS QUE VOUS AUREZ ATTEINT LA BARRE DES 100 % DE MESSAGES FILTRÉS, VOUS POURREZ PASSER À « P=REJECT », LA RÈGLE LA PLUS STRICTE.

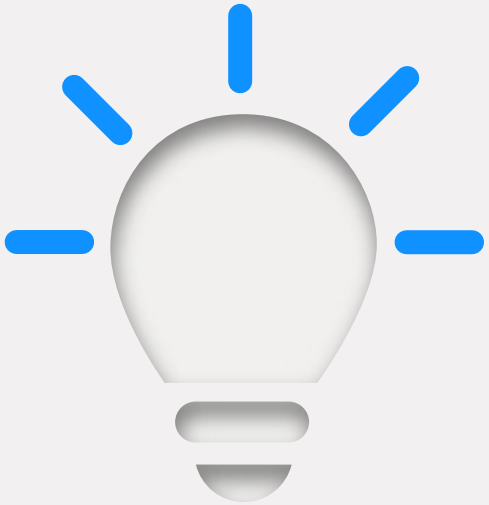
COMMENT CONFIGURER LA RÈGLE DMARC DE REFUS

1. **Ouvrez votre enregistrement DMARC depuis votre console DNS**
2. **Remplacez « p=quarantine » par « p=reject »**
   Exemple : « v=DMARC;p=reject;pct=100;rua=mailto:rapportsdmarc@votre-domaine.fr »
3. **Sauvegardez l'enregistrement**

CONSEIL : il est particulièrement important de continuer à surveiller le trafic d'e-mails pour éviter que des messages légitimes ne soient refusés puis supprimés

As-tu plus de questions? Écrivez-nous dès aujourd'hui à contactus@digicert.com ou visitez-nous à https://www.digicert.com/fr/tls-ssl/verified-mark-certificates/ ?

digicert®



RÈGLE DE REFUS : QU'ADVIENT-IL DES E-MAILS ?

Tous les messages qui échouent à l'authentification DMARC (e-mails non autorisés) seront bloqués/supprimés. Leurs destinataires ne les recevront donc pas et n'auront aucune connaissance de leur existence.