

# Bonnes pratiques pour l'authentification des courriels : moyens optimaux de déployer SPF, DKIM et DMARC

## Table des matières

---

### [Introduction](#)

[Connaissances requises du produit](#)

### [Authentification des e-mails - Brève présentation](#)

[SPF \(Sender Policy Framework\)](#)

[Messagerie identifiée par les clés de domaine \(DKIM\)](#)

[Authentification, signalement et conformité des messages basés sur le domaine \(DMARC\)](#)

### [Considérations relatives au déploiement SPF](#)

[SPF pour récepteurs](#)

[Si Vous Fournissez Des Services De Messagerie Électronique Pour D'Autres Domaines Ou Tiers](#)

[Si Vous Utilisez Des Services De Messagerie Tiers](#)

[\(Sub\)Domaines sans trafic de messagerie](#)

### [Considérations relatives au déploiement DKIM](#)

[DKIM pour les récepteurs](#)

[Préparation de la signature avec DKIM](#)

[Si Vous Utilisez Des Services De Messagerie Tiers](#)

### [Considérations relatives au déploiement DMARC](#)

[DMARC pour récepteurs](#)

[Si Vous Fournissez Des Services De Messagerie Électronique Pour D'Autres Domaines Ou Tiers](#)

[Si Vous Utilisez Des Services De Messagerie Tiers](#)

[\(Sub\)Domaines sans trafic de messagerie](#)

[Problèmes spécifiques au DMARC](#)

### [Exemple De Plan D'Action Pour Implémenter L'Authentification Des E-Mails](#)

[Étape 1 : DKIM](#)

[Étape 2 : SPF](#)

[Étape 3 : DMARC](#)

### [Références supplémentaires](#)

---

## Introduction

Ce guide décrit les trois principales technologies d'authentification des e-mails actuellement utilisées : SPF, DKIM et DMARC, et aborde divers aspects de leur mise en oeuvre. Plusieurs situations réelles d'architecture de messagerie sont abordées, ainsi que des directives pour les mettre en oeuvre sur l'ensemble de produits de sécurité de la messagerie Cisco. Étant donné qu'il s'agit d'un guide pratique des meilleures pratiques, certains des documents les plus complexes

seront omis. Au besoin, certains concepts peuvent être simplifiés ou condensés pour faciliter la compréhension de la matière présentée.

## Connaissances requises du produit

Ce guide est un document de niveau avancé. Pour poursuivre avec le matériel présenté, le lecteur doit posséder une connaissance du produit de l'appareil de sécurité de la messagerie électronique Cisco jusqu'au niveau de certification Ingénieur de terrain de sécurité de la messagerie électronique Cisco. En outre, les lecteurs doivent maîtriser le DNS et le SMTP et leur fonctionnement. La connaissance des bases de SPF, DKIM et DMARC est un plus.

## Authentification des e-mails - Brève présentation

### SPF (Sender Policy Framework)

Sender Policy Framework a été publié pour la première fois en 2006 sous le nom de RFC4408. La version actuelle est spécifiée dans le document RFC7208 et mise à jour dans le document RFC7372. En substance, il offre un moyen simple pour un propriétaire de domaine d'annoncer leurs sources de messagerie légitimes aux destinataires à l'aide du DNS. Bien que SPF authentifie principalement l'adresse du chemin de retour (MAIL FROM), la spécification recommande (et fournit un mécanisme) d'authentifier également l'argument SMTP HELO/EHLO (nom de domaine complet de la passerelle de l'expéditeur tel qu'il a été transmis lors de la conversation SMTP).

SPF utilise des enregistrements de ressources DNS de type TXT de syntaxe assez simple :

```
spirit.com text = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.spirit.com  
a:mx4.spirit.com include:spf.protection.outlook.com ~all"
```

L'enregistrement de Spirit Airlines ci-dessus permet aux e-mails provenant d'adresses @spirit.com de provenir d'un sous-réseau /24 particulier, de deux machines identifiées par un nom de domaine complet et de l'environnement Office365 de Microsoft. Le qualificatif «~all» à la fin indique aux récepteurs de considérer toute autre source comme une défaillance logicielle : l'un des deux modes de défaillance du SPF. Notez que les expéditeurs ne spécifient pas ce que les destinataires doivent faire avec les messages défaillants, mais uniquement dans quelle mesure ils échoueront.

Delta, pour sa part, utilise un schéma SPF différent :

```
delta.com text = "v=spf1 a:smtp.hosts.delta.com  
include:_spf.vendor.delta.com -all"
```

Pour réduire le nombre de requêtes DNS requises, Delta a créé un enregistrement A unique répertoriant toutes ses passerelles SMTP. Ils fournissent également un enregistrement SPF distinct pour leurs fournisseurs dans «\_spf.vendor.delta.com ». Ils incluent également des

instructions pour faire échouer tous les messages non authentifiés par SPF (qualificateur « tout »). Nous pouvons rechercher plus en détail l'enregistrement SPF des fournisseurs :

```
_spf.vendor.delta.com text = "v=spf1 include:_spf-delta.vrli.com  
include:_spf-ncr.delta.com a:delta-spf.niceondemand.com  
include:_spf.airfrance.fr include:_spf.qemailserver.com  
include:skytel.com include:eps11.com ?all"
```

Ainsi, les e-mails des expéditeurs @delta.com peuvent légitimement provenir, par exemple, des passerelles de messagerie d'Air France.

United, pour sa part, utilise un schéma SPF beaucoup plus simple :

```
texte united.com = "v=spf1 include:spf.enviaremails.com.br  
include:spf.usa.net include:coair.com ip4:161.215.0.0/16  
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx ~all"
```

Outre leurs propres passerelles de messagerie d'entreprise, ils incluent leurs fournisseurs de marketing par e-mail (« usa.net » et « enviaremails.com.br »), les passerelles Continental Air Lines héritées, ainsi que tout ce qui figure dans leurs enregistrements MX (« mécanisme MX »). Notez que MX (une passerelle de messagerie entrante pour un domaine) peut ne pas être identique à outgoing. Alors que pour les petites entreprises, elles seront généralement les mêmes, les grandes organisations disposeront d'une infrastructure distincte pour le traitement du courrier entrant et pour le traitement de la livraison sortante.

Il convient également de noter que tous les exemples ci-dessus font largement appel à des renvois DNS supplémentaires (« inclure » des mécanismes). Cependant, pour des raisons de performances, la spécification SPF limite à dix le nombre total de recherches DNS nécessaires pour récupérer un enregistrement final. Toute recherche SPF avec plus de 10 niveaux de récursivité DNS échouera.

## Messagerie identifiée par les clés de domaine (DKIM)

DKIM, spécifié dans les RFC 5585, 6376 et 5863, est une fusion de deux propositions historiques : les clés de domaine de Yahoo et la messagerie Internet identifiée de Cisco. Il permet aux expéditeurs de signer les messages sortants de manière cryptographique et d'inclure les signatures (ainsi que d'autres métadonnées de vérification) dans un en-tête d'e-mail (« DKIM-Signature »). Les expéditeurs publient leur clé publique dans le DNS, ce qui facilite la récupération de la clé par les destinataires et la vérification des signatures. DKIM n'authentifie pas la source des messages physiques, mais se base sur le fait que si la source est en possession de la clé privée de l'organisation émettrice, elle est implicitement autorisée à envoyer un e-mail en son nom.

Pour mettre en oeuvre le DKIM, l'organisation d'envoi générerait une ou plusieurs paires de clés publiques et publierait les clés publiques dans le DNS sous forme d'enregistrements TXT. Chaque paire de clés est référencée par un « sélecteur » afin que les vérificateurs DKIM puissent différencier les clés. Les messages sortants sont signés et l'en-tête DKIM-Signature est inséré :

```
DKIM-Signature : v=1 ; a=rsa-sha1 ; c=relaxed/relaxed ; s=united ;
d=news.united.com ; h=MIME-Version : Content-Type : Content-Transfer-
Encoding : Date:To:From:Reply-To:Subject:List-Unsubscribe:Message-ID ;
i=MileagePlus@news.united.com ; bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=;
```

```
b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNL08j4DGmKhH1
WRQLf3BxZ3jaYtLoJMRwxtgoWdfHU35CsFG2CNYLo=
```

Le format de la signature est assez simple. la balise « a » indique les algorithmes utilisés pour la signature, « c » indique le ou les schémas de canonisation utilisés [1], « s » est la référence du sélecteur ou de la clé, « d » est le domaine de signature. Le reste de cet en-tête DKIM-Signature est spécifique au message : « h » répertorie les en-têtes signés, « i » répertorie l'identité de l'utilisateur signataire et enfin l'en-tête se termine par deux hachages distincts : « bh » est un hachage d'en-têtes signés, tandis que « b » est la valeur de hachage du corps du message.

Lors de la réception d'un message signé DKIM, le destinataire recherche la clé publique en créant la requête DNS suivante :

```
<selector>._domainkey.<domaine de signature>
```

comme indiqué dans l'en-tête DKIM-Signature. Pour l'exemple ci-dessus, notre requête serait « united.\_domainkey.news.united.com » :

```
united._domainkey.news.united.com text = "g=*\\; k=rsa\\; n=" "Contact"
"postmaster@responsys.com" "with" "any" "questions" "about" "this"
"signing" "\\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGMXX/Q2KkWg135h
AwqxLiz9d0jBaxtuvYALj1Gkxmk5MemgAOcCr97G1W7Cr11eLn87qdTmyE5LevnTXxVDMjIfQJt60F
```

L'enregistrement DNS renvoyé contient la clé, ainsi que d'autres paramètres facultatifs. [2]

Le principal problème avec le DKIM est que la spécification initiale ne permettait pas la publicité qu'un expéditeur utilise le DKIM. Par conséquent, si un message n'est pas signé, il n'existe aucun moyen facile pour un destinataire de savoir qu'il aurait dû l'être et que, dans ce cas, il n'est probablement pas authentique. Étant donné qu'une seule entreprise peut (et le plus souvent utilisera) plusieurs sélecteurs, il n'est pas facile de « deviner » si un domaine est compatible DKIM. Une norme distincte, Author Domain Signing Practices, a été développée pour couvrir ce problème, mais en raison d'une faible utilisation et d'autres problèmes a été obsolète en 2013 sans successeur.

## Authentification, signalement et conformité des messages basés sur le domaine (DMARC)

DMARC est la plus jeune des trois technologies d'authentification des e-mails couvertes et a été développée spécifiquement pour remédier aux lacunes de SPF et DKIM. Contrairement aux deux autres, il authentifie l'en-tête From d'un message et établit une liaison avec les vérifications

précédemment effectuées par les deux autres. DMARC est spécifié dans la RFC7489.

La valeur ajoutée de DMARC par rapport à SPF et DKIM comprend :

- S'assurer que toutes les identités disponibles (HELO, MAIL FROM et/ou domaine de signature DKIM) sont alignées (correspondant exactement ou subordonnées) avec l'en-tête From
- Fournir au propriétaire du domaine expéditeur un moyen de spécifier une stratégie pour les destinataires sur la façon dont ils doivent gérer les messages défaillants
- Fourniture d'une fonction de rétroaction permettant aux propriétaires de domaines d'expéditeurs d'être informés de tout message défaillant, ce qui facilite l'identification des campagnes d'hameçonnage ou des erreurs dans l'attribution des politiques SPF/DKIM/DMARC

DMARC utilise également un mécanisme de distribution de politiques basé sur DNS simple :

```
_dmarc.aa.com text = "v=DMARC1\; p=none\; fo=1\; ri=3600\;  
rua=mailto:american@rua.agari.com,mailto:dmarc@aa.com\;  
ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com"
```

La seule balise obligatoire dans la spécification de stratégie DMARC est « p », qui spécifie la stratégie à utiliser sur les messages défaillants. Il peut s'agir de l'un des trois éléments suivants : aucun, quarantaine, rejet.

Les paramètres facultatifs les plus souvent utilisés concernent la création de rapports : « rua » spécifie une URL (soit une adresse de messagerie : soit une adresse URL http:// utilisant la méthode POST) pour envoyer des rapports d'agrégation quotidiens sur tous les messages défaillants censés provenir d'un domaine particulier. « ruf » spécifie une URL pour envoyer des rapports d'échec détaillés immédiats sur chaque message défaillant.

Selon les spécifications, un destinataire doit respecter la politique annoncée. Si ce n'est pas le cas, ils doivent avertir le propriétaire du domaine expéditeur dans le rapport d'agrégation.

Le concept central de DMARC est ce qu'on appelle l'alignement d'identificateur. L'alignement d'identificateur définit comment un message peut passer la vérification DMARC. Les identificateurs SPF et DKIM sont alignés séparément, et un message doit passer l'un d'entre eux quelconque pour passer le DMARC dans son ensemble. Cependant, il existe une option de stratégie DMARC où l'expéditeur peut demander qu'un rapport d'échec soit généré même si un alignement réussit, mais que l'autre échoue. Nous pouvons le voir dans l'exemple ci-dessus avec la balise « fo » définie sur « 1 ».

Il existe deux façons pour les messages d'adhérer à l'alignement d'identificateur DKIM ou SPF, strict et détendu. L'adhésion stricte signifie que le nom de domaine complet de l'en-tête de doit correspondre entièrement à l'ID de domaine de signature (balise « d ») de la signature DKIM ou au nom de domaine complet de la commande SMTP MAIL FROM pour SPF. Relaxed, d'autre part, permet à Header From FQDN d'être un sous-domaine des deux mentionnés ci-dessus. Cela a des implications importantes lors de la délégation de votre trafic de messagerie à des tiers, qui seront abordées plus loin dans le document.

# Considérations relatives au déploiement SPF

## SPF pour récepteurs

La vérification SPF est triviale à configurer sur les appareils virtuels Cisco Email Security Appliance ou Cloud Email Security. Pour le reste du présent document, toute référence à l'ESA inclura également la CES.

La vérification SPF est configurée dans les stratégies de flux de messagerie. La façon la plus simple de l'exécuter globalement consiste à l'activer dans la section Paramètres de stratégie par défaut du ou des écouteurs appropriés. Si vous utilisez le même écouteur pour la collecte des messages entrants et sortants, assurez-vous que la vérification SPF de votre stratégie de flux de messages « RELAYED » est désactivée.

Comme SPF ne permet pas de spécifier l'action à entreprendre, la vérification SPF (ainsi que DKIM, comme nous le verrons plus loin) vérifie uniquement le message et insère un ensemble d'en-têtes pour chaque contrôle SPF effectué :

```
Received-SPF : Pass (mx1.hc4-93.c3s2.smtpi.com : domaine de
united.5765@envfrm.rsys2.com désigne 12.130.136.195 comme
expéditeur autorisé) identity=mailfrom;
client-ip=12.130.136.195 ; receive=mx1.hc4-93.c3s2.smtpi.com ;
envelope-from="united.5765@envfrm.rsys2.com";
x-sender="united.5765@envfrm.rsys2.com";
x-conformance=sidf_compatible ; x-record-type="v=spf1"
```

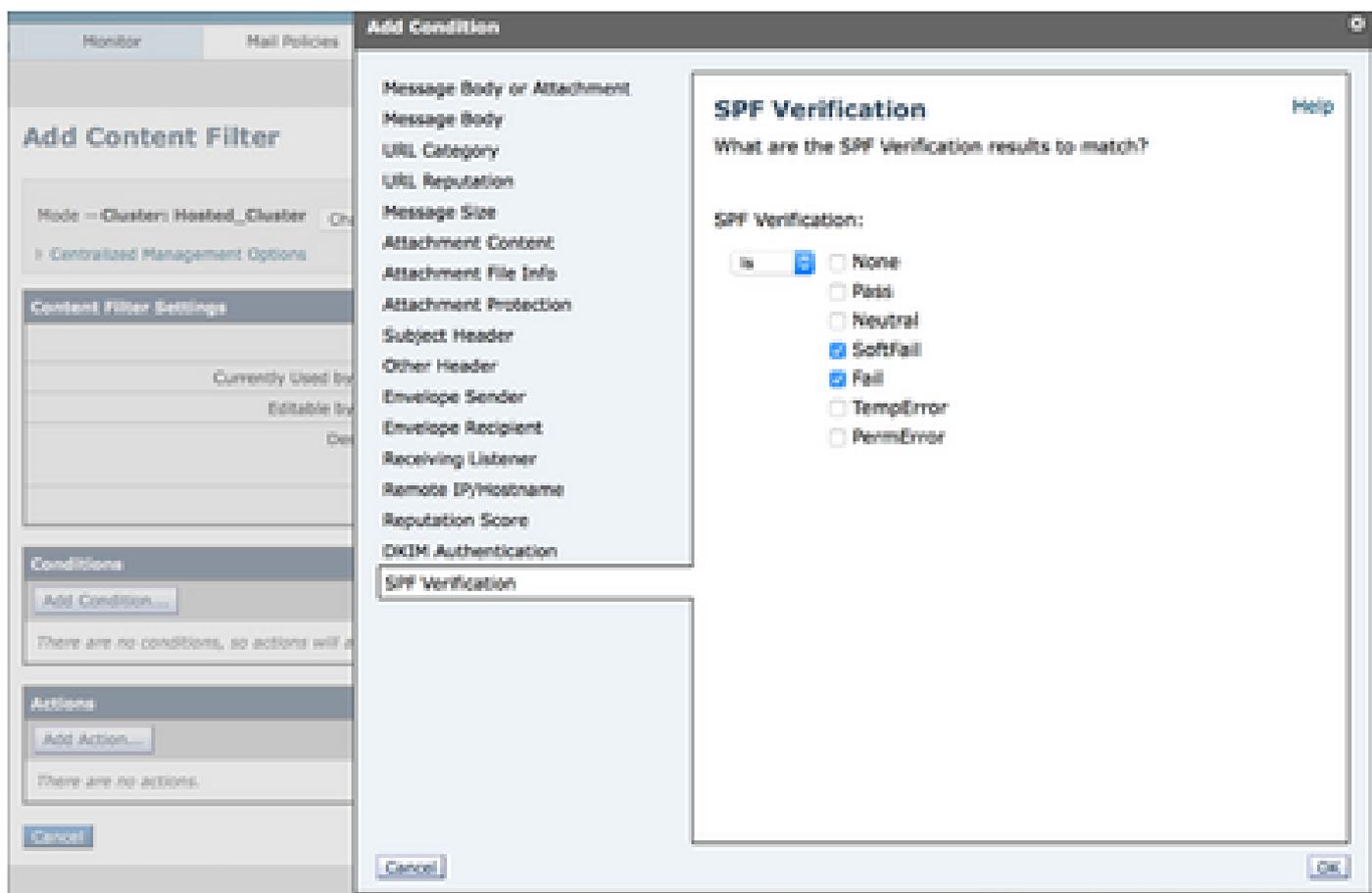
```
Received-SPF : Aucun (mx1.hc4-93.c3s2.smtpi.com : aucun expéditeur)
informations d'authenticité disponibles dans le domaine de
postmaster@omp.news.united.com) identity=helo ;
client-ip=12.130.136.195 ; receive=mx1.hc4-93.c3s2.smtpi.com ;
envelope-from="united.5765@envfrm.rsys2.com";
x-sender="postmaster@omp.news.united.com";
x-conformance=compatible_sidf
```

Notez que pour ce message, deux « identités » ont été vérifiées par SPF : « mailfrom » comme prescrit par la spécification et « helo » comme recommandé par la même. Le message passe formellement le SPF, car seul le premier est pertinent pour la conformité SPF, mais certains

destinataires peuvent sanctionner les expéditeurs qui n'incluent pas les enregistrements SPF pour leurs identités HELO également. Par conséquent, il est recommandé d'inclure les noms d'hôte de vos passerelles de messagerie sortantes dans vos enregistrements SPF.

Une fois que les stratégies de flux de messagerie ont vérifié un message, il revient aux administrateurs locaux de configurer une action à entreprendre. Pour ce faire, utilisez la règle de filtre de messages SPF-status() [3], ou créez un filtre de contenu entrant en l'utilisant et en l'appliquant aux stratégies de messages entrants appropriées.

Image 1 : Condition du filtre de contenu de vérification SPF



Les actions de filtrage recommandées consistent à supprimer les messages qui échouent (« -all » dans l'enregistrement SPF) et les messages de quarantaine qui échouent (« ~all » dans l'enregistrement SPF) dans une quarantaine de stratégie. Toutefois, cela peut varier en fonction de vos exigences de sécurité. Certains destinataires se contentent de marquer les messages défaillants ou n'entreprennent aucune action visible, mais les signalent aux administrateurs.

Récemment, la popularité du SPF a considérablement augmenté, mais de nombreux domaines publient des enregistrements SPF incomplets ou incorrects. Pour être sûr, vous pouvez mettre en quarantaine tous les messages SPF défaillants et surveiller la mise en quarantaine pendant un certain temps, afin de vous assurer qu'il n'y a pas de « faux positifs ».

Si Vous Fournissez Des Services De Messagerie Électronique Pour D'Autres Domaines Ou Tiers

Si vous fournissez des services de livraison ou d'hébergement de courrier électronique pour des tiers, ils devront ajouter des noms d'hôtes et des adresses IP que vous utilisez pour remettre leurs messages à leurs propres enregistrements SPF. Pour ce faire, le plus simple est que le fournisseur crée un enregistrement SPF « parapluie » et que les clients utilisent le mécanisme « include » dans leurs enregistrements SPF.

```
suncountry.com text = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148  
ip4:146.88.177.149 ip4:67.109.66.68 ip4:198.179.134.238 ip4:107.20.2  
7.57 ip4:207.87.182.66 ip4:199.66.248.0/22 include:cust-  
spf.exacttarget.com ~all"
```

Comme nous pouvons le voir, Sun Country contrôle certains de ses e-mails, mais les e-mails marketing qu'ils envoient sont externalisés vers un tiers. L'extension de l'enregistrement référencé révèle une liste des adresses IP actuelles utilisées par leur fournisseur de services de publipostage marketing :

```
cust-spf.exact.target.com text = " v=spf1 ip4:64.132.92.0/24  
ip4:64.132.88.0/23 ip4:66.231.80.0/20 ip4:68.232.192.0/20  
ip4:199.122.120.0/21 ip4:207.67.38.0/24 ip4:207.67.98.192/27  
ip4:207.250.68.0/24 ip4:209.43.22.0/28 ip4:198.245.80.0/20  
ip4:136.147.128.0/20 ip4:136.147.176.0/20 ip4:13.111.0.0/18 -all"
```

Cette flexibilité permet aux fournisseurs de services de messagerie d'évoluer sans avoir à contacter chaque client pour modifier leurs enregistrements DNS.

## Si Vous Utilisez Des Services De Messagerie Tiers

De même que pour le paragraphe précédent, si vous utilisez des services de messagerie tiers et souhaitez établir un flux de messagerie entièrement vérifié par SPF, vous devez inclure leurs propres enregistrements SPF dans le vôtre.

```
jetblue.com texte descriptif "v=spf1 include:_spf.qualtrics.com ?all"
```

JetBlue utilise le service d'analyse Qualtrics, et la seule chose qu'ils doivent faire est d'inclure un enregistrement SPF correct de Qualtrics. De même, la plupart des autres fournisseurs de services électroniques fournissent des enregistrements SPF à inclure dans les enregistrements de leurs clients.

Si votre ESP ou votre e-mail marketing ne fournit pas d'enregistrements SPF, vous devrez répertorier leurs passerelles de messagerie sortante directement dans la vôtre. Cependant, il vous incombe de conserver ces enregistrements exacts et si le fournisseur ajoute des passerelles supplémentaires ou modifie des adresses IP ou des noms d'hôte, votre flux de messagerie risque d'être compromis.

Le partage de ressources représente un autre danger pour les tiers qui ne sont pas sensibles au

SPF : si un fournisseur de services de messagerie électronique utilise la même adresse IP pour envoyer des e-mails à plusieurs clients, il est techniquement possible pour un client de générer un message SPF valide prétendant être un autre client qui envoie des e-mails via la même interface. C'est pourquoi, avant de mettre en place des restrictions SPF, vous devez examiner les politiques de sécurité de votre MSP et connaître l'authentification des e-mails. S'ils n'ont pas de réponses à vos questions, compte tenu du fait que le SPF est l'un des mécanismes de confiance de base sur Internet, il est vivement conseillé de reconsidérer votre choix de MSP. Il ne s'agit pas seulement de sécurité : le SPF, le DKIM, le DMARC et les autres meilleures pratiques des expéditeurs [4] employés par les MSP sont une garantie de livraison. Si votre MSP ne les suit pas ou les suit incorrectement, cela diminuera leur fiabilité avec les grands systèmes de réception et peut-être même retarder ou bloquer vos messages.

## (Sub)Domaines sans trafic de messagerie

La plupart des entreprises possèdent aujourd'hui plusieurs domaines à des fins marketing, mais n'en utilisent qu'un seul activement pour le trafic de messagerie d'entreprise. Même si SPF est correctement déployé sur le domaine de production, les acteurs malveillants peuvent toujours utiliser d'autres domaines qui ne sont pas activement utilisés pour un e-mail pour usurper l'identité d'une organisation. SPF peut empêcher que cela se produise via un enregistrement SPF spécial « deny all » : pour tous vos domaines (et sous-domaines !) qui ne génèrent pas de trafic de messagerie, publiez « v=spf1 -all » dans le DNS. Un excellent exemple est [openspf.org](http://openspf.org) - le site Web du Conseil du FPS.

Étant donné que la délégation SPF n'est valide que pour un seul domaine, il est essentiel de publier également des enregistrements SPF « deny all » pour tous les sous-domaines que vous utilisez et qui risquent de ne pas générer d'e-mail. Même si votre domaine de production possède un enregistrement SPF « normal », faites un effort supplémentaire pour ajouter des enregistrements « deny all » à vos sous-domaines sans trafic. Et encore une fois, n'oubliez pas que la réception n'est pas équivalente à l'envoi : un domaine peut très bien recevoir des e-mails, mais ne sera jamais une source. Cela est très vrai pour les domaines de marketing à court terme (par exemple, les événements, les promotions limitées dans le temps, les lancements de produits...), où les e-mails entrants dans ces domaines seraient livrés à votre domaine de production, et toutes les réponses à ces e-mails seront livrées à partir du domaine de production. Ces domaines à court terme auront un enregistrement MX valide, mais devraient avoir un enregistrement SPF qui les identifie comme aucune source d'e-mail également.

## Considérations relatives au déploiement DKIM

### DKIM pour les récepteurs

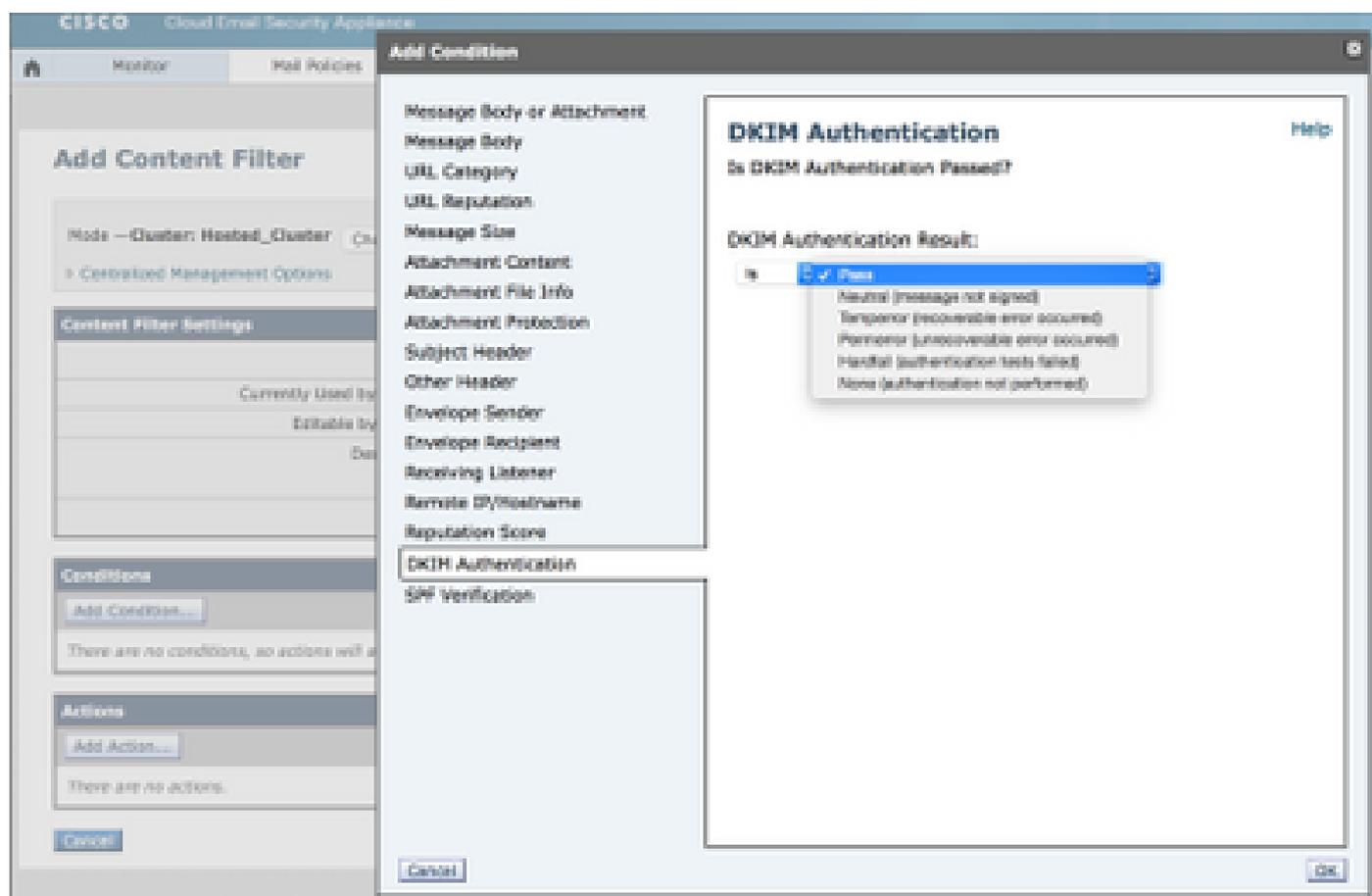
La configuration de la vérification DKIM sur l'ESA est similaire à la vérification SPF. Dans les paramètres de stratégie par défaut des stratégies de flux de messagerie, activez simplement la vérification DKIM. Comme DKIM ne prend en charge aucune spécification de stratégie, il suffit de vérifier la signature et d'insérer un en-tête « Authentication-Results » :

```
Authentication-Results : mx1.hc4-93.c3s2.smtpi.com ; dkim=pass
```

(signature vérifiée) header.i=MileagePlus@news.united.com

Toutes les actions basées sur les résultats de la vérification DKIM doivent être effectuées par les filtres de contenu :

Image 2 : Condition du filtre de contenu de vérification DKIM



Contrairement à SPF, qui est simple, DKIM manipule le texte du message, de sorte que certains paramètres peuvent être limités. Vous pouvez éventuellement créer des profils de vérification DKIM et affecter différents profils de vérification à différentes stratégies de flux de messages. Ils vous permettent de limiter la taille des clés des signatures que vous acceptez, de définir les actions d'échec de récupération des clés et de configurer la profondeur de la vérification DKIM.

Lorsqu'un message passe par plusieurs passerelles, il peut être signé plusieurs fois et transporter ainsi plusieurs signatures. Pour qu'un message passe la vérification DKIM, toutes les signatures doivent être vérifiées. Par défaut, ESA vérifie jusqu'à cinq signatures.

En raison de l'ouverture historique du protocole SMTP et de la messagerie électronique et de la réticence de l'ensemble d'Internet à s'adapter aux changements (positifs), il existe encore plusieurs situations où les signatures DKIM peuvent légitimement échouer, par exemple lorsque les gestionnaires de listes de diffusion relaient directement mais modifient les messages ou lorsque les messages sont transférés directement plutôt que comme pièces jointes aux nouveaux messages. C'est pourquoi, en général, la meilleure pratique pour les messages qui échouent à DKIM serait toujours de les mettre en quarantaine ou de les baliser, plutôt que de les abandonner.

## Préparation de la signature avec DKIM

Avant d'activer la signature DKIM dans votre stratégie de flux de messagerie RELAYED, vous devez générer/importer les clés, créer des profils de signature DKIM et publier la ou les clés publiques dans le DNS.

Si vous signez pour un seul domaine, le processus est simple. Générez la paire de clés, créez votre profil de signature unique dans la section Clés de domaine des stratégies de messagerie, puis cliquez sur l'option « Générer » sous « Enregistrement de texte DNS » lorsque votre profil est prêt. Publiez la clé telle qu'elle est générée dans votre DNS. Enfin, activez la signature DKIM dans votre stratégie de flux de messagerie.

Cela devient plus compliqué si vous signez pour plusieurs domaines distincts. Dans ce cas, vous avez deux options :

1. Utilisez un profil de signature unique pour signer pour tous les domaines. Vous stockerez la clé publique (unique) dans la zone DNS du domaine « principal » et vos signatures DKIM référenceront cette clé. Cette technique était souvent utilisée par les fournisseurs de services électroniques dans le passé - elle leur permettait de signer à grande échelle, tout en n'ayant pas à interagir avec l'espace DNS de chaque client [\[5\]](#).
2. Créez un profil de signature distinct pour chaque domaine auquel vous vous connectez. Cela rend la configuration initiale plus complexe, mais offre beaucoup plus de flexibilité pour aller de l'avant. Créez une paire de clés pour chaque domaine, créez un profil spécifiant un seul domaine (et ses sous-domaines) dans la section « Profile Users », puis publiez la clé publique appropriée dans la zone DNS de ce domaine particulier.

Bien que l'option #1 soit plus facile à utiliser, n'oubliez pas qu'elle finira par casser DMARC. Puisque DMARC exige que l'ID de domaine de signature soit aligné avec l'en-tête de, l'alignement de votre identificateur avec DKIM échouera. Vous pourrez peut-être vous en sortir si vous configurez correctement votre SPF, et compter sur l'alignement de l'identificateur SPF pour réussir la vérification DMARC.

Cependant, en mettant en oeuvre l'option #2 dès le début, vous n'avez pas besoin de vous inquiéter de DMARC et il est assez facile de révoquer ou de reconfigurer le service de signature pour un seul domaine. En outre, si vous fournissez certains services de messagerie pour un domaine tiers, vous devrez très probablement obtenir la clé à utiliser auprès d'eux (et l'importer dans votre ESA). Cette clé sera spécifique au domaine, vous devrez donc créer un profil distinct.

### Si Vous Utilisez Des Services De Messagerie Tiers

En général, si vous utilisez la signature DKIM et que vous déchargez une partie de votre traitement de messagerie (par exemple, les e-mails marketing) vers un tiers, vous ne voulez pas qu'il utilise les mêmes clés que celles que vous utilisez en production. C'est l'une des principales raisons de l'existence des Selecteurs dans DKIM. Au lieu de cela, vous devez générer une nouvelle paire de clés, publier la partie publique dans votre zone DNS et remettre la clé secrète à l'autre partie. Cela vous permettra également de révoquer rapidement cette clé en cas de problème tout en conservant votre infrastructure DKIM de production intacte.

Bien qu'il ne soit pas nécessaire pour le DKIM (les messages d'un même domaine peuvent être signés avec plusieurs clés différentes), il est recommandé de fournir un sous-domaine distinct pour tout e-mail traité par un tiers. Cela facilitera le suivi des messages et permettra une mise en oeuvre beaucoup plus propre de DMARC ultérieurement. Par exemple, considérez ces cinq en-têtes DKIM-Signature issus de plusieurs messages de Lufthansa :

```
DKIM-Signature : v=1 ; a=rsa-sha1 ; c=relaxed/relaxed ; s=lufthansa ;  
d=newsletter.milesandmore.com ;
```

```
DKIM-Signature : v=1 ; a=rsa-sha1 ; c=relaxed/relaxed ; s=lufthansa2 ;  
d=newsletter.lufthansa.com ;
```

```
DKIM-Signature : v=1 ; a=rsa-sha1 ; c=relaxed/relaxed ; s=lufthansa3 ;  
d=lh.lufthansa.com ;
```

```
DKIM-Signature : v=1 ; a=rsa-sha1 ; c=relaxed/relaxed ; s=lufthansa4 ;  
d=e.milesandmore.com
```

```
DKIM-Signature : v=1 ; a=rsa-sha1 ; c=relaxed/relaxed ; s=lufthansa5 ;  
d=fly-lh.lufthansa.com ;
```

Nous pouvons voir que Lufthansa utilise cinq clés différentes (sélecteurs) réparties sur cinq sous-domaines distincts de deux domaines de production primaires (lufthansa.com et milesandmore.com). Cela signifie que chacun d'entre eux peut être contrôlé indépendamment et peut être externalisé vers un fournisseur de services de messagerie différent.

## Considérations relatives au déploiement DMARC

### DMARC pour récepteurs

La vérification DMARC sur l'ESA est basée sur le profil, mais contrairement à DKIM, le profil par défaut doit être modifié pour être conforme à la spécification. Le comportement par défaut de l'ESA est de ne jamais abandonner de messages sauf instruction explicite du client, de sorte que le profil de vérification DMARC par défaut aura toutes les actions définies sur « Aucune action ». En outre, pour activer la génération de rapports correcte, vous devez modifier les « Paramètres globaux » de la section DMARC de « Politiques de messagerie ».

Une fois qu'un profil a été configuré, la vérification DMARC, comme les deux autres, est définie dans la section Paramètres de stratégie par défaut des stratégies de flux de messagerie. Assurez-vous de cocher la case pour envoyer des rapports de commentaires cumulés - il s'agit sans doute de la fonctionnalité la plus importante de DMARC pour l'expéditeur. Au moment de la rédaction de cet article, ESA ne prend pas en charge la génération de rapports d'échec par message (balise « ruf » de la politique DMARC).

Comme les actions de stratégie DMARC sont conseillées par l'expéditeur, contrairement à SPF ou DKIM, il n'y a aucune action spécifique configurable en dehors de la configuration du profil. Il n'est pas nécessaire de créer des filtres de contenu.

La vérification DMARC ajoute des champs supplémentaires à l'en-tête Authentication-Results :

```
Authentication-Results : mx1.hc4-93.c3s2.smtpi.com ; dkim=pass  
(signature vérifiée) header.i=MileagePlus@news.united.com ; dmarc=pass  
(p=none dis=none) d=news.united.com
```

Dans l'exemple ci-dessus, nous voyons que DMARC a été vérifié sur la base de l'alignement de l'identificateur DKIM, et l'expéditeur a demandé la stratégie « none ». Cela indique qu'ils sont actuellement dans la phase de « surveillance » du déploiement DMARC.

## Si Vous Fournissez Des Services De Messagerie Électronique Pour D'Autres Domaines Ou Tiers

La plus grande préoccupation des ESP pour la conformité DMARC est d'obtenir un alignement correct des identifiants. Lors de la planification de DMARC, assurez-vous que votre SPF est correctement configuré, que tous les autres domaines pertinents ont vos passerelles sortantes dans vos enregistrements SPF et qu'ils n'envoient pas de messages qui ne seront pas alignés, principalement en utilisant différents domaines pour l'identité MAIL FROM et Header From. Cette erreur est le plus souvent commise par des applications qui envoient des notifications ou des avertissements par e-mail, car les auteurs d'applications ignorent généralement les conséquences de l'incohérence de leurs identités de messagerie.

Comme décrit précédemment, assurez-vous que vous utilisez un profil de signature DKIM distinct pour chaque domaine, et que votre profil de signature référence correctement le domaine pour lequel vous vous connectez, tel qu'utilisé dans En-tête - De. Si vous utilisez vos propres sous-domaines, vous pouvez signer avec une seule clé, mais assurez-vous que votre adhésion à DKIM est assouplie dans la stratégie DMARC (« adkim=»r«).

En règle générale, si vous fournissez des services de messagerie à un plus grand nombre de tiers que vous ne contrôlez pas directement, il est recommandé de rédiger un document d'instructions sur la manière d'envoyer un e-mail qui est le plus susceptible d'être envoyé. Comme les e-mails entre utilisateurs sont généralement bien traités, cela servira principalement de document de stratégie pour les auteurs d'applications dans les exemples mentionnés ci-dessus.

## Si Vous Utilisez Des Services De Messagerie Tiers

Si vous utilisez des tiers pour acheminer une partie de votre trafic de messagerie, la meilleure façon consiste à déléguer un sous-domaine distinct (ou un domaine complètement différent) au fournisseur tiers. Ils peuvent ainsi gérer les enregistrements SPF selon les besoins, disposer d'une infrastructure de signature DKIM distincte et ne pas interférer avec votre trafic de production. La politique DMARC pour les e-mails externalisés peut alors être différente de celle appliquée en interne. Comme nous l'avons déjà mentionné, lorsque vous envisagez de recevoir des e-mails provenant d'un tiers, assurez-vous que vos identifiants sont alignés et que votre adhésion à DKIM et SPF est définie de manière appropriée dans votre politique DMARC.

(Sub)Domaines sans trafic de messagerie

Une autre amélioration de DMARC par rapport aux technologies d'authentification de messagerie précédentes est la manière dont il gère les sous-domaines. Par défaut, la stratégie DMARC d'un domaine particulier s'applique à tous ses sous-domaines. Lors de la récupération des enregistrements de stratégie DMARC, si aucun enregistrement ne peut être trouvé au niveau de l'en-tête du FQDN, les destinataires sont tenus de déterminer le domaine d'organisation [6] de l'expéditeur et d'y rechercher un enregistrement de stratégie.

Cependant, la stratégie DMARC d'un domaine d'organisation peut également spécifier une stratégie de sous-domaine distincte (balise « sp » d'un enregistrement DMARC) qui s'appliquera à tous les sous-domaines pour lesquels aucune stratégie DMARC explicite n'a été publiée.

Dans le scénario décrit plus haut dans le chapitre sur le SPF, vous devriez :

1. Publier un enregistrement DMARC explicite pour tous les sous-domaines qui sont des sources légitimes d'e-mail.
2. Publiez une stratégie de sous-domaine « Refuser » dans votre enregistrement de stratégie de domaine d'organisation pour rejeter automatiquement tous les e-mails qui usurpent des domaines non émetteurs

Ce type de structuration de l'authentification de vos e-mails garantit la meilleure protection possible de votre infrastructure et de votre marque.

## Problèmes spécifiques au DMARC

Il existe plusieurs problèmes potentiels avec DMARC, qui proviennent tous de la nature et des lacunes d'autres technologies d'authentification sur lesquelles il repose. Le problème est que DMARC a fait apparaître ces problèmes en poussant activement une politique de rejet de l'e-mail et en corrélant tous les différents identifiants d'expéditeur dans un message.

La plupart des problèmes concernent les listes de diffusion et les logiciels de gestion de listes de diffusion. Lorsqu'un e-mail est envoyé à une liste de diffusion, il est redistribué à tous ses destinataires. Cependant, l'e-mail résultant, avec l'adresse de l'expéditeur d'origine, sera envoyé par l'infrastructure d'hébergement du gestionnaire de liste de diffusion, échouant ainsi à la vérification SPF de l'en-tête de (la plupart des gestionnaires de liste de diffusion utilisent l'adresse de liste comme Enveloppe de (MAIL FROM) et l'adresse de l'expéditeur d'origine comme En-tête de).

Comme DMARC échouera pour SPF, nous pouvons nous appuyer sur DKIM, cependant, la plupart des gestionnaires de listes de diffusion ajoutent également des pieds de page aux messages, ou balisent les sujets avec le nom de la liste, cassant ainsi la vérification de signature DKIM.

Les auteurs de DKIM proposent plusieurs solutions au problème, qui se résument à ce que les gestionnaires de listes de diffusion doivent utiliser l'adresse de la liste dans toutes les adresses de l'expéditeur, et indiquer l'adresse de l'expéditeur d'origine par un autre moyen.

Des problèmes similaires surviennent lorsque des messages sont transférés en copiant simplement le message d'origine sur SMTP vers le nouveau destinataire. Cependant, la plupart

des agents d'utilisateurs de messagerie utilisés aujourd'hui formeront correctement un nouveau message et incluront le message transféré soit en ligne, soit en pièce jointe au nouveau message. Les messages transférés de cette manière transmettront le DMARC si l'utilisateur de transfert le fait (bien sûr, l'authenticité du message d'origine ne peut pas être établie).

## Exemple De Plan D'Action Pour Implémenter L'Authentification Des E-Mails

Bien que les technologies elles-mêmes soient simples, la mise en oeuvre d'une infrastructure complète d'authentification des e-mails peut s'avérer longue et difficile. Pour les petites entreprises et celles dont les flux de messagerie sont contrôlés, cela sera relativement simple, alors que les environnements plus importants peuvent trouver cela particulièrement difficile. Il n'est pas rare pour les grandes entreprises d'embaucher des consultants pour gérer le projet de mise en oeuvre. ,

### Étape 1 : DKIM

Le DKIM est relativement discret, car les messages non signés ne seront pas rejetés. Avant la mise en oeuvre effective, il convient de tenir compte de tous les points mentionnés précédemment. Contactez les tiers auxquels vous pourriez déléguer la signature, assurez-vous que vos tiers prennent en charge la signature DKIM et réfléchissez à votre stratégie de gestion des sélecteurs. Certaines organisations conserveraient des clés (sélecteurs) distinctes pour les différentes unités organisationnelles. Vous pouvez envisager la rotation périodique des clés pour plus de sécurité, mais assurez-vous de ne pas supprimer vos anciennes clés tant que tous vos messages en transit n'ont pas été remis.

Une attention particulière doit être portée aux tailles clés. Bien qu'en général, « plus c'est mieux », vous devez tenir compte du fait que la création de deux signatures numériques par message (y compris la canonicalisation, etc.) est une tâche très coûteuse pour le processeur et peut influencer les performances des passerelles de messagerie sortantes. En raison de la surcharge de calcul, 2 048 bits est la taille de clé pratique la plus importante pouvant être utilisée, mais pour la plupart des déploiements, les clés 1 024 bits constituent un bon compromis entre performances et sécurité.

Pour réussir la mise en oeuvre ultérieure de DMARC, vous devez :

1. identifier tous les domaines que vous envoyez, y compris les sous-domaines
2. générer des clés DKIM et créer des profils de signature pour chaque domaine
3. fournir les clés privées appropriées à tout tiers
4. publier toutes les clés publiques dans les zones DNS appropriées
5. vérifier que les tiers sont prêts à commencer à signer
6. activer la signature DKIM dans la politique de flux de messages RELAYED sur tous vos ESA
7. signaler aux tiers le début de la signature

### Étape 2 : SPF

La mise en oeuvre correcte de SPF sera probablement la partie la plus longue et la plus lourde de toute mise en oeuvre d'infrastructure d'authentification de messagerie. Comme la messagerie était très simple à utiliser et à gérer, et complètement ouverte du point de vue de la sécurité et de l'accès, les entreprises n'appliquaient pas de politiques strictes concernant qui et comment pouvait l'utiliser. De ce fait, la plupart des entreprises ne disposent pas aujourd'hui d'une vue complète de toutes les différentes sources d'e-mails, qu'elles soient internes ou externes. Le plus gros problème de la mise en oeuvre de SPF est de découvrir qui envoie actuellement des e-mails en votre nom.

Choses à rechercher :

1. cibles évidentes : serveurs Exchange ou autres serveurs groupware ou passerelles de messagerie sortante
2. toute solution DLP ou tout autre système de traitement des e-mails pouvant générer des notifications externes
3. Systèmes CRM envoyant des informations interagissant avec les clients
4. diverses applications tierces pouvant envoyer des e-mails
5. serveurs de laboratoire, de test ou autres qui peuvent envoyer des e-mails
6. ordinateurs personnels et périphériques configurés pour envoyer directement un e-mail externe

La liste ci-dessus n'est pas complète, car les organisations ont des environnements différents, mais elle doit être considérée comme une ligne directrice générale sur ce qu'il faut rechercher. Une fois que (la plupart) de vos sources de courrier électronique ont été identifiées, vous pouvez prendre du recul et, au lieu d'autoriser chaque source existante, nettoyer la liste. Idéalement, tous vos e-mails sortants doivent être remis via vos passerelles de messagerie sortante, à quelques exceptions près. Si vous disposez de votre propre solution de messagerie marketing ou si vous utilisez une solution tierce, vous devez utiliser une infrastructure distincte des passerelles de messagerie de production. Si votre réseau de remise des messages est exceptionnellement compliqué, vous pouvez continuer à documenter l'état actuel dans votre SPF, mais ne prenez pas le temps de nettoyer la situation à l'avenir.

Si vous desservez plusieurs domaines sur la même infrastructure, vous pouvez créer un enregistrement SPF universel unique et le référencer dans des domaines individuels à l'aide du mécanisme d'inclusion. Assurez-vous que vos enregistrements SPF ne sont pas trop larges ; par exemple, si seulement cinq machines dans un réseau /24 envoient SMTP, ajoutez ces cinq adresses IP individuelles à votre SPF, plutôt que le réseau entier. Veillez à ce que vos enregistrements soient aussi précis que possible afin de minimiser les risques de compromission de votre identité par des e-mails malveillants.

Commencez par une option softfail pour les expéditeurs non correspondants («~all »). Ne le changez en hardfail (-all) qu'une fois que vous êtes sûr à 100 % d'avoir identifié toutes vos sources de courrier électronique, sinon vous risquez de perdre le courrier électronique de production. Par la suite, après avoir implémenté DMARC et l'avoir exécuté en mode surveillance pendant un certain temps, vous serez en mesure d'identifier les systèmes que vous avez manqués et de mettre à jour vos enregistrements SPF pour qu'ils soient complets. C'est seulement alors qu'il sera sûr de régler votre SPF sur hardfail.

## Étape 3 : DMARC

Une fois que vos DKIM et SPF sont configurés aussi complets que possible, il est temps de créer vos stratégies DMARC. Prenez en compte toutes les situations mentionnées dans les chapitres précédents et préparez le déploiement de plusieurs enregistrements DMARC si votre infrastructure de messagerie est complexe.

Créez des alias de messagerie qui recevront les rapports ou créez une application Web qui peut les ingérer. Il n'y a pas d'adresses e-mail strictement définies à utiliser pour cela, mais il est utile de les décrire, par exemple `rua@domain.com`, `dmarc.rua@domain.com`, `mailauth-rua@domain.com`, etc. Assurez-vous qu'un opérateur dispose d'un processus pour surveiller ces adresses et modifier la configuration SPF, DKIM et DMARC de manière appropriée, ou alerter l'équipe de sécurité en cas de campagne d'usurpation d'identité. Au départ, la charge de travail sera importante lorsque vous ajusterez les enregistrements pour couvrir tout ce que vous avez manqué pendant la configuration SPF et DKIM. Au bout d'un certain temps, les rapports indiqueront probablement uniquement les tentatives d'usurpation.

Initialement, définissez votre stratégie DMARC sur « aucun » et votre option d'analyse pour envoyer des rapports pour tout échec de vérification (« fo=1 ») - ceci permettra de détecter rapidement toute erreur dans votre SPF et DKIM tout en n'influençant pas le trafic. Une fois que vous êtes satisfait du contenu des rapports soumis, changez la stratégie en « quarantaine » ou en « rejet », selon votre stratégie de sécurité et vos préférences. Veillez à ce que les opérateurs analysent en permanence les rapports DMARC reçus pour détecter d'éventuels faux positifs.

L'implémentation complète et correcte de DMARC n'est pas une tâche de petite envergure ou de courte durée. Bien que certains résultats (et la « mise en oeuvre » formelle de DMARC) puissent être obtenus en publiant un ensemble incomplet d'enregistrements et une politique de « aucun », il est dans l'intérêt de l'organisation émettrice et d'Internet dans son ensemble que chacun mette en oeuvre cette politique dans toute la mesure de ses capacités.

En ce qui concerne les échéanciers, voici un aperçu très sommaire des étapes individuelles d'un projet type. Encore une fois, comme chaque organisation est différente, ces informations sont loin d'être exactes :

1. Planification et préparation de la DKIM	2 à 4 semaines
2. Séries de tests DKIM	2 semaines
3. SPF - identification légitime de l'expéditeur	2 à 4 semaines
4. Élaboration des politiques du DMARC	2 semaines

5. Essai des enregistrements SPF et DMARC	4 à 8 semaines
6. Essai SPF avec défaillance matérielle	2 semaines
7. Essai DMARC avec mise en quarantaine/rejet	4 semaines
8. Suivi des rapports du DMARC et adaptation du SPF/DKIM en conséquence	continuel

Les plus petites entreprises sont susceptibles de connaître une durée plus courte de la plupart des étapes, en particulier les étapes 3 et 4. Quelle que soit la simplicité de votre infrastructure de messagerie, consacrez toujours suffisamment de temps aux tests et surveillez attentivement les rapports de commentaires pour tout ce que vous avez manqué.

Les grandes entreprises peuvent connaître une durée encore plus longue des mêmes étapes, avec des exigences de test plus strictes. Il n'est pas rare pour les entreprises disposant d'une infrastructure de messagerie complexe d'embaucher une aide externe, non seulement pour l'aspect technique de la mise en oeuvre de l'authentification de la messagerie, mais également pour gérer l'ensemble du projet et coordonner les équipes et les services.

## Références supplémentaires

- Site de référence pour SPF : <http://www.openspf.org>
- Le Conseil DKIM : <http://www.dkim.org>
- Site Web principal de DMARC, géré par le Trusted Domain Project : <http://www.dmarc.org>
- dmarcian - un site d'aide et de ressources géré par Tim Draegen, un des auteurs de DMARC. N'oubliez pas de consulter la section « Outils » : <http://www.dmarcian.com>
- Outil de validation des enregistrements Online Trust Alliance : <https://otalliance.org/resources/spf-dmarc-record-validator>
- Assistant Enregistrement DMARC - autre outil utile pour vous aider à créer vos enregistrements DMARC : <http://www.kitterman.com/dmarc/assistant.html>
- Outils de test des enregistrements SPF : <http://www.kitterman.com/spf/validate.html>
- « Don't Be A Phish: Deep Dive Into Email Authentication Techniques », présentation Cisco Live 2014 BRKSEC-3770 : [https://www.ciscolive.com/online/connect/sessionDetail.wv?SESSION\\_ID=76627](https://www.ciscolive.com/online/connect/sessionDetail.wv?SESSION_ID=76627)

[1] La canonicalisation sort du cadre du présent document. Reportez-vous à la section « Références supplémentaires » pour plus d'informations sur la canonisation DKIM.

[2] Les paramètres d'enregistrement DNS DKIM sont également hors du champ d'application de ce document.

[3] La création de filtres de messages sort du cadre de ce document. Pour obtenir de l'aide, consultez les guides d'utilisation d'AsyncOS for Email.

[4] Le M3AAWG a défini un excellent ensemble de meilleures pratiques appliquées et respectées par la plupart des acteurs du secteur. Le document Meilleures pratiques courantes pour les expéditeurs est disponible à l'adresse

[https://www.m3aawg.org/sites/maawg/files/news/M3AAWG\\_Senders\\_BCP\\_Ver3-2015-02.pdf](https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf)

[5] Ce comportement tire parti du fait qu'à l'origine, DKIM ne vérifie pas du tout la source du message comme indiqué dans MAIL FROM ou Header From. Il vérifie uniquement que l'ID de domaine de signature (paramètre « d » de la signature DKIM et paramètre « Domain Name » de votre profil de signature) héberge bien la clé publique de la paire utilisée pour signer le message. L'authenticité de l'expéditeur est impliquée par la signature de l'en-tête « From ». Assurez-vous simplement de répertorier tous les domaines (et sous-domaines) auxquels vous vous connectez dans la section « Utilisateurs de profil ».

[6] Généralement, un domaine situé un niveau au-dessous du TLD ou un préfixe ccTLD approprié (.ac.uk, .com.sg, etc.)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.