par Bruno Sousa
<bruno/at/linuxfocus.org>

Une introduction à SPF

L´auteur:

Bruno est étudiant au Portugal. Il dédie son temps libre à Linux et à la photographie.

Résumé:

SPF est l'acronyme de Sender Policy Framework (Cadre de Politique d'Expéditeur). SPF vise à être une norme anti−contrefaçon pour prévenir la contrefaçon d'adresses de courriels. Cet article donne une courte introduction à SPF, ses avantages et ses désavantages.

Traduit en Français par:
Jean−Etienne Poirrier
(homepage)

SPF est né en 2003. Son créateur, Meng Weng Wong, a repris les meilleures fonctionnalités de Reverse MX et DMP (Designated Mailer Protocol ou Protocole Désigné de Courrier) pour faire naître SPF.

SPF utilise le chemin de retour (return−path ou MAIL FROM) présent dans l'en−tête de message, puisque tous les MTA travaillent avec ces champs. Cependant, il y a une nouvelle notion, proposée par Microsoft : le PRA, qui signifie Purported Responsible Address (Adresse Prétendue Responsable). Le PRA correspond à l'adresse de l'utilisateur final qu'un MUA (comme Thunderbird) utilise.

Ainsi, quand nous mettons ensemble le SPF et le PRA, nous pouvons obenir le prétendu Sender ID qui permet, à un utilisateur recevant un courriel, d'effectuer les vérifications des champs MAIL FROM (vérification SPF) et PRA. D'une certaine manière, il est dit que les MTA vont vérifier le champ MAIL FROM et que les MUA vont vérifier le champ PRA.

Pour le moment, SPF a besoin du DNS pour fonctionner correctement. Cela signifie que les enregistrements « reverse MX » doivent être publiés. Ces enregistrements spécifient quelles machines *envoient* un courriel pour un domaine donné. C'est différent des enregistrements MX, utilisés de nos jours, qui spécifient les machines qui *reçoivent* un courriel pour un domaine donné.

De quoi a besoin SPF pour fonctionner ?

Pour protéger votre système avec SPF, vous devez :

1. Configurer votre DNS pour ajouter l'enregistrement TXT où sont introduites les informations que SPF requiert.
2. Configurer votre système de courriel (qmail, sendmail) pour utiliser SPF ; cela signifie d'effectuer la vérification sur chaque message reçu sur votre serveur.

La première étape sera accomplie sur le serveur DNS où le domaine se trouve. Dans la section suivante, nous allons discuter les détails des enregistrements. Une chose que vous devez garder à l'esprit est la syntaxe que votre serveur DNS utilise (bind ou djbdns). Mais ne soyez pas effrayés : le site officiel de SPF fournit une aide excellente qui vous instruira.

L'enregistrement TXT de SPF

L'enregistrement SPF est contenu dans un enregistrement TXT et son format est le suivant :

```
v=spf1 [[pre] type [ext] ] ... [mod]
```

La signification de chaque paramètre est la suivante :

<table>
<tr><th>Paramètre</th><th>Description</th></tr>
<tr><td>v=spf1</td><td>Version de SPF. Lorsque vous utilisez SenderID, vous pourriez voir v=spf2</td></tr>
<tr><td>pre</td><td>Définit un code de retour lorsqu'une correspondance survient.

Les valeurs possibles sont :
<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>+</td><td>Par défaut. Signifie « passe » lorsqu'un test est concluant.</td></tr>
<tr><td>−</td><td>Signifie « rate un test ». Cette valeur est normalement appliquée à −all pour dire qu'il n'y a pas eu de correspondances, précédemment.</td></tr>
<tr><td>~</td><td>Signifie un « échec mou » (softfail). Cette valeur est normalement appliquée lorsqu'un test n'est pas concluant.</td></tr>
<tr><td>?</td><td>Signifie « neutre ». Cette valeur est normalement appliquée lorsqu'un test n'est pas concluant.</td></tr>
</table></td></tr>
<tr><td>type</td><td>Définit le type à utiliser pour les vérifications

Les valeurs possibles sont :
<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>include</td><td>pour inclure les tests d'un domaine fourni.
Cela s'écrit sous la forme : include:domaine</td></tr>
<tr><td>all</td><td>pour terminer la séquences des tests.
Par exemple, si c'est −all, alors tous les tests qui n'ont pas été rencontrés jusqu'à présent sont ratés. Mais s'il y a une incertitude, il peut être utilisé sous la forme de ?all qui signifie que le test sera accepté.</td></tr>
<tr><td>ip4</td><td>Utilise une IP version 4 pour la vérification.
Cela peut être utilisé sous la forme ipv4:ipv4 ou ipv4:ipv4/cidr pour définir une gamme. Ce type est le plus recommandé car il donne la plus petite charge sur les serveurs DNS.</td></tr>
<tr><td>ip6</td><td>Utiliser une IP version 6 pour la vérification.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>a</td><td>Utilise un nom de domaine pour la vérification.
Cela effectuera une recherche sur le DNS pour un A RR.
Il peut être utilisé sous la forme a:domaine, a:domaine/cidr ou a/cidr.</td></tr>
<tr><td></td><td>mx</td><td>Utilise le MX RR du DNS pour la vérification.
Le MX RR défini le MTA qui reçoit ; par exemple, si ce n'est pas le même que le MTA qui envoie, les tests basés sur le MX seront ratés.
Il peut être utilisé sous la forme mx:domain, mx:domain/cidr ou mx/cidr.</td></tr>
<tr><td></td><td>ptr</td><td>Utilise le PTR RR du DNS pour la vérification.
Dans ce cas, un PTR RR est utilisé, ainsi qu'une requête de carte inverse (reverse map query). Si le nom d'hôte retourné est dans le même domaine, la communication est vérifiée.
Il peut être utilisé sour la forme ptr:domain</td></tr>
<tr><td></td><td>exist</td><td>Teste l'existence d'un domaine.
Il peut être écrit sous la forme exist:domain.</td></tr>
<tr><td>ext</td><td colspan="2">Définit une extension en option au type. S'il est omis, alors un seul enregistrement est utilisé pour l'interrogation.</td></tr>
<tr><td>mod</td><td colspan="2">C'est la dernière directive de type et elle agit comme modificateur d'enregistrement.

modificateur Description
redirect — Redirige la vérification vers l'utilisation des enregistrements SPF d'un domaine défini.
C'est utilisé sous la forme redirect=domain.
exp — Cet enregistrement doit être le dernier et il permet de personnaliser le message d'échec.

<pre>IN TXT "v=spf1 mx -all exp=getlost.exemple.com"
getlost IN TXT "Vous n'êtes pas autorisé à envoyer un message pour</pre></td></tr>
</table>

Hé, je suis un FAI

Les FAI auront quelques « problèmes » avec leurs utilisateurs itinérants s'ils utilisent des mécanismes comme POP−before−Relay à la place de SASL SMTP.

Bien, si vous êtes un FAI inquiet du spam et des contrefaçons, vous devez considérer votre politique à propos des courriels et commencer à utiliser SPF.

Voici quelques étapes que vous devriez considérer :

1. Tout d'abord, configurez votre MTA pour utiliser SASL ; par exemple, vous pouvez l'activer sur les ports 25 et 587.
2. Avertissez vos utilisateurs sur la politique que vous êtes en train d'implémenter (le spf.pobox.com vous fournit un exemple, voyez les références).
3. Donnez à vos utilisateurs une période de grâce ; cela signifie que vous allez publier vos enregistrements SPF dans le DNS mais avec un échec mou (softfail) (~all) à la place d'un échec (−all) aux tests.

Et, avec cela, vous protégez vos serveurs, vos clients et le monde contre le spam...

Il y a beaucoup d'informations pour vous sur le site officiel de SPF... Qu'est–ce que vous attendez ?

Quelles sont les choses auxquelles il faut faire attention ?

SPF est une solution parfaite pour vous protéger contre la fraude. Elle a cependant une limitation : le suivi (forwarding) traditionnel de courriel ne fonctionnera plus. Vous ne pouvez pas simplement recevoir un courriel dans votre MTA et le renvoyer. Vous devez réécrire l'adresse de l'expéditeur. Des correctifs pour les MTA répandus sont fournis sur le site de SPF. En d'autres mots, si vous commencez à publier des enregistrements SPF dans le DNS, vous devriez également mettre à jour votre MTA pour qu'il réécrive les adresses d'expéditeur, même si vous ne vérifiez pas encore les enregistrements SPF.

Conclusion

Vous pourriez penser que l'implémentation de SPF pourrait être quelque peu confuse. Et bien, en effet, ce n'est pas compliqué et, en passant, vous avez une aide géniale qui vous aide à accomplir votre mission (voyez la section des références).

Si vous êtes préoccupés à propos du spam, alors SPF vous aidera en protégeant votre domaine de contrefaçons et tout ce que vous avez à faire est ajouter une ligne de texte dans votre serveur DNS et configurer votre serveur de courrier électronique.

Les avantages que SPF apporte sont géants. Cependant, comme je l'ai dit à quelqu'un, ce n'est pas une aussi grande différence qu'entre le jour et la nuit. Les bénéfices de SPF viendront avec le temps, lorsque les autres y adhéreront.

J'ai fait référence au Sender ID et sa relation à SPF, mais je ne me suis pas étendu en explications à ce sujet. Vous en connaissez déjà probablement la raison : la politique de Microsoft est toujours la même, à savoir le brevetage de logiciels. Dans les références, vous pouvez voir la position d'openspf.org sur SenderID.

Dans un prochain article, nous parlerons de la configuration de MTA. A plus tard !

J'espère vous avoir donné une courte introduction à SPF. Si vous souhaitez en apprendre plus à ce sujet, utilisez simplement les références qui ont été utilisées pour écrire cet article.

Références

Le site officiel de SPF.
La FAQ officielle de SPF.
L'aide officielle de SPF.
La position d'openspf.org à propos de SenderID.
Un excellent article à propos de SenderID et SPF.
Avertissez vos utilisateurs sur la conversion SASL.
COMMENT (HOWTO) – Définir un enregistrement SPF.

Translation information:
en −−> −− : Bruno Sousa <bruno/at/linuxfocus.org>
en −−> fr: Jean−Etienne Poirrier (homepage)

2005−02−08, generated by lfparser_pdf version 2.51