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

Over de auteur:

Bruno is een student in Portugal. Zijn vrije tijd besteedt hij aan Linux en fotografie.

Een introductie tot SPF

Kort:

SPF staat voor Sender Policy Framework en probeert een standaard te zijn om het vervalsen van e−mail adressen te vervalsen (forging). Dit artikel geeft een korte introductie in SPF, de voordelen en de nadelen.

Vertaald naar het Nederlands door:
Guus Snijders
<ghs(at)linuxfocus.org>

SPF is ontstaan in 2003, zijn mentor Meng Weng Wong nam de beste features van Reverse MX en DMP (Designated Mailer Protocol) om SPF tot leven te wekken.

SPF gebruikt het return−path (of MAIL FROM), zoals die voorkomt in de headers van e−mail berichten, omdat alle MTA's deze velden gebruiken. Er is echter ook een nieuw idee, geopperd door Microsoft: De PRA, het Purported Responsible Address. De PRA komt overeen met het adres van de eindgebruiker die een MUA gebruikt (zoals Thunderbird).

Als we dus SPF en PRA bij elkaar nemen, krijgen we een zogenaamd Sender ID, welke de gebruiker die de e−mail ontvangt, in staat stelt om de de MAIL FROM (SPF check) en de PRA check uit te voeren. Er wordt gezegd dat MTA's de MAIL FROM zullen controleren en de MUA's de PRA check.

SPF heeft DNS nodig om goed te werken. Dit betekend dat het "reverse MX" record gepubliceerd moet worden, deze records vertellen welke machines e−mail *versturen* voor een bepaald domein. Dit verschilt van de MX records zoals die vandaag de dag worden gebruikt, die geven aan welke machines e−mail *ontvangen* voor een bepaald domein.

Wat heeft SPF nodig om te werken?

Om jouw systeem te beschermen met SPF, moet je:

1. Het TXT record dat wordt gebruikt door SPF aan je DNS toevoegen.

2. Je e−mail systeem configureren (qmail, sendmail) om SPF te gebruiken, dit wil zeggen dat ieder ontvangen bericht gecontroleerd wordt.

De eerste stap gebeurd op de DNS server van het domein. In de volgende sectie zullen we de details van het record bespreken. Een ding dat je klaar moet hebben, is de syntax die jouw DNS server gebruikt (bind of djbdns). Wees echter niet bang, de officiële SPF−site levert een uitstekende wizard die je instrueerd.

Het TXT Record van SPF

Het SPF record wordt opgeslagen in een TXT record, het formaat is als volgt:

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

Waarbij iedere parameter de volgende betekenis heeft:

<table>
<tr><th>Parameter</th><th>Beschrijving</th></tr>
<tr><td>v=spf1</td><td>Versie van SPF. Bij SenderID kan hier v=spf2 voor komen.</td></tr>
<tr><td>pre</td><td>Definieerd een retourcode als een treffer optreedt.

De mogelijke waarden zijn:
Waarde — Beschrijving
+ — Standaard. Betekend doorgaan als de test doorslaggevend is.
− — Betekend dat de test faalt. Deze waarde wordt meestal toegepast op −all om aan te geven dat er geen eerdere treffers zijn.
~ — Betekend een zacht falen (soft fail). Deze waarde wordt meestal gebruikt als een test niet doorslaggevend is.
? — Betekend neutraal. Deze waarde wordt meestal gebruikt als een test niet doorslaggevend is.</td></tr>
<tr><td>type</td><td>Definieerd het type om te gebruiken voor verificatie.

De mogelijke waarden zijn:
Waarde Beschrijving
include — om de tests van een gegeven domein mee te nemen.
Het wordt geschreven in de vorm include:domein
all — Om een serie tests af te sluiten.
Bijvoorbeeld als het −all is maar niet nog niet alle tests zijn al zijn doorlopen, dan falen. Maar als er hier onzekerheid is, kan het gebruikt worden in de vorm van ?all, wat betekent dat alle tests geaccepteerd worden.
ip4 — Gebruik IP versie 4 voor verificatie.
Dit kan gebruikt worden in de vorm van ip4:ipv4 of ip4:ipv4/cidr om een bereik aan te geven. Dit type is het meest aan te raden omdat het de minste belasting op de DNS servers geeft.
ip6 — Gebruik IP versie 6 voor verficatie.
a — Gebruik een domeinnaam voor verificatie.
Dit zorgt voor een look−up van een A RR in de DNS.
Kan gebruikt worden in de vorm a:domein, a:domain/cidr of a/cidr.
mx</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>Gebruik de DNS MX RR voor verificatie.
De MX RR definieerd de ontvangende MTA, als dit bijvoorbeeld niet dezelfde is als de verzendende MTA, zullen de tests gebaseerd op de mx falen.
Kan gebruikt worden in vorm van mx:domein, mx:domein/cidr of mx/cidr.</td></tr>
<tr><td>ptr</td><td>Gebruik DNS PTR RR voor verificatie.
In dit geval wordt een PTR RR en een reverse map query gebruikt. Als de geretourneerde hostname in hetzelfde domein ligt, is de communicatie geverifieerd.
Kan gebruikt worden in de vorm van ptr:domein</td></tr>
<tr><td>exist</td><td>Test voor het bestaan van een domein.
Kan geschreven in de vorm van exist:domein.</td></tr>
</table>
</td></tr>
<tr><td>ext</td><td>Definieerd een optionele extensie voor het type. Als deze niet wordt gebruikt, wordt er een enkel type record voor de ondervraging gebruikt.</td></tr>
<tr><td>mod</td><td>Dit is het laatste type directive en fungeert als een record modifier.
<table>
<tr><th>modifier</th><th>Beschrijving</th></tr>
<tr><td>redirect</td><td>Leidt de verificatie door naar de SPF records van het opgegeven domein.
Wordt gebruikt in de vorm van redirect=domein.</td></tr>
<tr><td>exp</td><td>Dit record komt als laatste en staat het toe om een eigen foutmelding te maken.

IN TXT "v=spf1 mx -all exp=getlost.example.com"

getlost IN TXT "You are not authorized to send mail for the domain"</td></tr>
</table>
</td></tr>
</table>

He, ik ben een ISP

ISPs zullen "wat" problemen hebben met roaming (zwervende) gebruikers als ze mechanismen als POP−before−Relay in plaats van SASL SMTP gebruiken.

Wel, als je je als ISP zorgen maakt over spam en forgeries (vervalsen van afzenders), moet je je beleid over e−mail aanpassen en beginnen met SPF.

Hier zijn enkele stappen om te overwegen.

1. Configureer eerst je MTA om SASL te gebruiken, dit zou je bijvoorbeeld kunnen inschakelen op poorten 25 en 587.
2. Informeer je gebruikers over het beleid dat wordt ingevoerd (spf.pobox.com geeft een voorbeeld, zie de referenties).
3. Geef je gebruikers een periode om wennen, dit betekend dat je je SPF records in DNS publiceerd, maar met softfail (~all) in plaats van de fail (−all) tests.

En hiermee bescherm je je servers, je clients en de wereld tegen spam...

Er is een hoop informatie voor je op de officiële SPF site, waar wacht je nog op?

Wat zijn de dingen om voor uit te kijken?

SPF is een perfecte oplossing om te beschermen tegen fraude. Het heeft echter een beperking: traditionele e−mail forwarding zal niet langer werken. Je kunt niet langer e−mail ontvangen in je MTA en deze doorsturen. Je moet het sender adres veranderen. Patches voor populaire MTAs zijn te vinden op de SPF site. In andere woorden, als je je SPF DNS records publiceert, dien je ook je MTA te updaten, zodat het sender adres herschrijft, ook al controleer je nog niet op SPF records.

Conclusie

Je denkt misschien dat de implementatie van SPF nogal verwarrend is. Wel, het is niet moeilijk, en je hebt een geweldige wizard die je kan helpen deze missie te volbrengen (zie de referenties sectie).

Als je je zorgen maakt over spam, kan SPF je helpen jouw domein te beschermen tegen forgeries, alles wat je hoeft te doen is een regel tekst toevoegen aan je DNS server en je mailserver configureren.

De voordelen van SPF zijn groot. Echter, zoals ik iemand al vertelde, het is geen verschil tussen de dag en de nacht. De voordelen van SPF komen met de tijd, als anderen het ook gaan gebruiken.

We hebben Sender ID en de relatie met SPF reeds genoemd, maar we hebben het er niet erg uitgebreid over gehad. Waarschijnlijk weet je de reden al, de politiek van Microsoft is altijd weer hetzelfde, patenten op software. In de referenties kun je de positie van SenderID zien volgens openspf.org.

In een volgend artikel zullen we de configuratie van de MTA bespreken, tot dan.

Ik hoop je een korte introductie tot SPF te geven. Als je er meer over wilt leren kun je de referenties gebruiken die ik heb gebruikt voor dit artikel.

Referenties

De officiële SPF site.
De officiële SPF FAQ.
De officiële wizard van SPF.
De positie van openspf.org over SenderID.
Een schitterend artikel over SenderID en SPF.
Waarschuw je gebruikers over de overstap naar SASL.
HOWTO – Definieer een SPF Record

Site onderhouden door het LinuxFocus editors team

http://www.LinuxFocus.org

Vertaling info:
en −−> −− : Bruno Sousa <bruno/at/linuxfocus.org>
en −−> nl: Guus Snijders <ghs(at)linuxfocus.org>

2005−02−25, generated by lfparser_pdf version 2.51