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

Uma Introdução ao SPF

Sobre o autor:

O Bruno é um estudante em Portugal. Os seus tempos livres dedica−os ao Linux e à Fotografia.

Abstrato:

O SPF quer dizer "Sender Policy Framework" e pretende ser um padrão de anti−forjamento ou seja para prevenir a forja de endereços de email. Este artigo dá−lhe uma breve introdução ao SPF, as suas vantagens e desvantagens.

Traduzido para Português por:
Bruno Sousa
<bruno/at/linuxfocus.org>

O SPF nasceu no ano de 2003, o seu mentor, Meng Weng Wong aproveitou as melhores características do Reverse MX e do DMP (Designated Mailer Protocol) para dar vida ao SPF.
O SPF usa a "return−path" (ou MAIL FROM) presente no cabeçalho da mensagem de email, visto que todas as MTAs trabalham com estes campos. Contudo existe um novo conceito proposto pela Microsoft o PRA, que quer dizer "Purported Responsible Address". O PRA corresponde ao endereço final do utilizador que um MUA (como o thunderbird) utiliza.
Assim quando juntamos o SPF e o PRA podemos obter o SenderID. Assim o SenderID permite a um utilizador que recebe email, verificar o campo MAIL FROM (verificação SPF) e a verificação PRA. De algum modo, se diz que as MTAs verificam o campo MAIL FROM e as MUA fazem a verificação PRA.
Actualmente o SPF necessita do DNS para trabalhar devidamente. Isto quer dizer que os registos "reverse MX" têm de ser publicados, estes registos dizem que máquina é que enviam email para um dado domínio. É diferente dos registos MX, usado nos dias de hoje, que significam que máquinas é que recebem email para um dado domínio.

O que é que o SPF necessita para trabalhar?

No sentido de proteger o seu sistema com o SPF deve:

1. Configurar o seu DNS para adicionar os registos TXT onde é introduzida a informação que o SPF consulta.
2. Configurar o seu sistema de email (qmail, sendmail) para usar o SPF, isto quer dizer, para ser feita a verificação em cada mensagem recebida no seu servidor.

O primeiro passo é feito no servidor de DNS onde o seu domínio se encontra. Na próxima secção vamos discutir os detalhes do registo TXT. Uma das coisas que deve ter presente é a sintaxe que o seu servidor DNS usa (bind ou djbdns). Mas não tenha receio o site oficial do SPF fornece um bom wizard que o instrui.

O registo TXT do SPF

O registo SPF está contido num registo TXT e o seu formato é como o que se segue:

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

O significado de cada parâmetro é o seguinte:

<table>
<tr><th>Parâmetro</th><th>Descrição</th></tr>
<tr><td>v=spf1</td><td>Versão do SPF. Ao usar o SenderID poderá ver v=spf2</td></tr>
<tr><td>pre</td><td>Define um código de retorno quando é encontrada uma pesquisa.

Os valores possíveis são:
Valor Descrição
+ Por omissão. Quer dizer passa quando um teste é conclusivo.
− Significa Falha um teste. Este valor normalmente é aplicado em −all para dizer que não foram encontrados valores para pesquisas anteriores.
~ Significa uma falha ligeira. Este valor normalmente é aplicado quando um teste não é conclusivo.
? Significa Neutricidade. Este valor também é usado quando um teste não é conclusivo.</td></tr>
<tr><td>type</td><td>Define o tipo a usar para verificação.

Os valores possíveis são:
Valor Descrição
include para incluir os testes de um dado domínio.
É escrito na forma de include:domínio
all para terminar a sequência de testes.
Por exemplo se for −all e todos os testes, até aqui, não foram concluídos com sucesso então falha. Mas se não existirem certezas pode ser usado na forma ?all que aceita o teste.
ip4 Usa a versão 4 do ip para verficação.
Este pode ser usado na forma de ip4:ipv4 ou ip4:ipv4/cidr para definir um intervalo. Este tipo é o mais recomendado visto que induz menos carga nos servidores de DNS.
ip6 Usa a versão 6 do Ip para verificação.
a Usa o nome de domínio para verificação.
Induz numa pesquisa no DNS por um registo A.
Pode ser usado na forma a:domain, a:domain/cidr ou a/cidr.
mx Usa o registo MX para verificação.
O registo MX define a MTA que recebe o correio, por</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>exemplo, se não for a mesma que a MTA que envia, os testes baseados no mx falharão.
Pode ser usado na forma de mx:domain, mx:domain/cidr ou mx/cidr.</td></tr>
<tr><td>ptr</td><td>Usa o registo PTR do DNS para verificação.
Neste caso é usado um registo PTR e uma consulta reverse.
Se o nome retornado reside no mesmo domínio então a comunicação é feita.
Pode ser usada na forma ptr:domain</td></tr>
<tr><td>exist</td><td>Testa a existência de um domínio.
Pode ser escrita na forma exist:domain.</td></tr>
</table>
</td></tr>
<tr><td>ext</td><td>Define uma extensão opcional ao tipo. Se é omitida significa que só é usado um tipo de registo para as questões.</td></tr>
<tr><td>mod</td><td>É a última directiva e actua como um modificador do registo.

<table>
<tr><th>modificador</th><th>Descrição</th></tr>
<tr><td>redirect</td><td>Redirecciona a verificação para usar os registos SPF do domínio definido.
É usado na forma redirect=domain.</td></tr>
<tr><td>exp</td><td>Este registo deve ser o último e permite a personalização de uma mensagem de erro.

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

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

Hey, Sou um ISP

Os ISPs terão problemas com os seus utilizadores roaming se estiverem a usar mecanismos como o POP−before−Relay em vez de SASL SMTP.
Bem, se é um ISP preocupado com o spam, com o forjamento deve reconsiderar as suas políticas de email e começar a usar o SPF.
Ficam aqui apontados alguns passos que deve considerar.

1. Primeiro configure o seu servidor MTA para usar SASL, por exemplo pode activá−lo nos portos 25 e 587.
2. Avise os seus utilizadores acerca das políticas que está a implementar (O Site spf.pobox.com fornece um exemplo, veja as referências).
3. Dê aos seus utilizadores um período de graça, quer isto dizer que deve publicar os seus registos de SPF no DNS mas com softfail (~all) em vez da falha dos testes (−all).

E com isto está a proteger os seus servidores, os seus clientes e o mundo do spam...

Existe uma grande quantidade de informação no site oficial do SPF, do que é que está à espera ?

Quais são as coisas com que se deve preocupar?

O SPF é a solução perfeita para proteger contra a fraude. Contudo tem uma limitação: O tradicional re−encaminhamento de e−mail não trabalhará mais. Não pode simplesmente re−enviar o email que recebeu. Deve reescrever o endereço do emissor. Os patches para as MTAs mais comuns são fornecidos no site SPF. Por outras palavras se publicar os seus registos SPF no DNS, deve também actualizar a sua MTA para fazer a re−escrita do endereço do emissor mesmo que não verifique os registos SPF.

Conclusão

Pode pensar que a implementação do SPF pode ser algo confusa. Bem, na verdade não é complicada e, para além disto, tem um bom wizard que o ajuda a cumprir a sua missão (veja a secção das referências).

Se está preocupado com o spam então o SPF ajudá−lo−á. Protegendo o seu domínio do forjamento, tudo o que tem de fazer é adicionar uma linha de texto ao seu servidor de DNS e configurar o seu servidor de email.

As vantagens do SPF são grandes. Contudo, como eu disse a alguém, não representa uma diferença entre o dia e a noite. Os Benefícios do SPF vêm com o tempo, quando outros também aderem ao mesmo.

Eu referi o SenderID e as suas relações com o SPF, mas não me estendi em nenhuma explicação acerca do mesmo. Provavelmente já sabe a razão, as políticas da Microsoft são sempre as mesmas, patentes de software. Nas referências pode ver a posição do openspf.org acerca do SenderID.

Num próximo artigo falaremos da configuração de uma MTA, até então.

Espero ter dado uma breve introdução ao SPF. Se está interessado em aprender mais acerca de, veja as referências que foram usadas para fazer este artigo.

Referências

O Site oficial do SPF.
A FAQ oficial do SPF.
O wizard oficial do SPF.
A posição do openspf.org acerca do SenderID.
Um artigo excelente acerca do SenderID e do SPF.
Avise os seus utilizadores acerca da conversão SASL
Como definir um registo SPF