An introduction to SPF

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

About the author:

Bruno is a student in Portugal. He dedicates his spare time to Linux and photography.

Abstract:

SPF stands for Sender Policy Framework and it aims to be an antiforgery standard to prevent the forging of e−mail addresses. This article gives a short introduction to SPF, its advantages and disavantages.

SPF was born on the year 2003, his mentor, Meng Weng Wong picked up the best features of Reverse MX and DMP (Designated Mailer Protocol) to bring SPF to life.

SPF uses the return−path (or MAIL FROM) present on the email message header, since all MTAs work with these fields. However there is a new notion proposed by Microsoft: The PRA, which means the Purported Responsible Address. The PRA corresponds to the address of the end−user that a MUA uses (like thunderbird).

So when we put together the SPF and the PRA we can obtain the so−called Sender ID, which allows an user who receives email to perform the check of the MAIL FROM (SPF check) and the PRA check. Somehow it's said that MTAs will check the MAIL FROM and the MUAs will do the PRA check.

Actually SPF needs DNS to work properly. This means that the "reverse MX" records must be published, these records tell what machines *send* email from a given domain. It is different from the MX records, used nowadays, that specify the machines that *receive* email for a given domain.

What SPF needs to work?

In order to protect your system with SPF you must:

1. Configure your DNS to add the TXT record where is introduced the information that SPF queries.
2. Configure your email system (qmail, sendmail) to use SPF, this means to perform the verification on each message received on your server.

The first step will be accomplished on the DNS server where the domain is. In the next section we will discuss the details of the record. One thing that you must have present is the syntax that your DNS server uses (bind or djbdns). But don't be afraid, the official site of SPF provides an excellent wizard that will instruct you.

The TXT Record of SPF

The SPF record is contained on a TXT record and its format is as follows:

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

The meaning of each parameter is the following:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>v=spf1</td><td>Version of SPF. When using SenderID you might see v=spf2</td></tr>
<tr><td>pre</td><td>Defines a return code when a match occurs.

The possible values are:
Value — Description
+ — Default. Means pass when a test is conclusive.
– — Means fail a test. This value normally is applied on –all to tell that there are no previous matches.
~ — Means a soft fail. This value normally is applied when a test is not conclusive.
? — Means neutral. This value normally is applied when a test is not conclusive.</td></tr>
<tr><td>type</td><td>Defines the type to use for verification.

The possible values are:
Value — Description
include — to include the tests of a supplied domain.
It is written in the form of include:domain
all — to terminate the sequence of the tests.
For instance if it is –all then if all the tests have not been met until here than fail. But if there is uncertainty it can be used on the form of ?all whih means the test will be accepted.
ip4 — Use a IP version 4 for verification.
This can be used on the form of ip4:ipv4 or ip4:ipv4/cidr to define a range. This type is the most recommended since incurs least load on the DNS servers.
ip6 — Use a IP version 6 for verification.
a — Use a domain–name for verification.
It will make a look–up on the DNS for an A RR.
It can be used in the form of a:domain, a:domain/cidr or a/cidr.
mx — Use the DNS MX RR for verification.
The MX RR defines the receiving MTA, for instance if it is not the same as the sending MTA, the tests based on the mx will fail.
It can be used in the form of mx:domain, mx:domain/cidr or mx/cidr.
ptr — Use DNS PTR RR for verification.
In this case it is used a PTR RR and a reverse map query. If the returned host name lies in the same domain the communication is</td></tr>
</table>

<table>
<tr><td></td><td>verified.
It can be used in the form of ptr:domain

exist
Test for the existance of a domain.
It can be written in the form of exist:domain.</td></tr>
<tr><td>ext</td><td>Defines an optional extension to the type. If it is omitted then it is used only a single record type for interrogation.</td></tr>
<tr><td>mod</td><td>It is the last type directive and acts as a record modifier.

modifier Description

redirect
Redirects the verification to use the SPF records of the defined domain.
It is used in the form of redirect=domain.

exp
This record must be the last and it allows to customize a failure message.

<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>

Hey, I'm an ISP

ISPs will have some "trouble" with their roaming users if they are using mechanisms like POP−before−Relay instead of SASL SMTP.

Well, if you are an ISP worried about spam and about forgeries you must consider your politics about email and start using SPF.

Here are some steps you might consider.

1. First configure your MTA to use SASL, for instance you can enable it on ports 25 and 587.
2. Warn your users about the politics you are implementing (The spf.pobox.com provides you an example, see references).
3. Give your users a grace period, this means you will publish your SPF records into DNS, but with softfail (~all) instead of the fail (−all) tests.

And with this you are protecting your servers, your clients and the world from spam...

There's a lot of information on the official site of SPF for you, what are you waiting for?

What are the things to watch out for?

SPF is a perfect solution to protect against fraud. It has however one limitation: Traditional e−mail forwarding will no longer work. You can not just receive mail in your MTA and re−send it. You must rewrite the sender address. Patches for common MTAs are provided on the SPF side. In other words if you start to publish SPF

DNS records you should also update your MTA to do sender address rewriting even if you do not yet check for SPF records.

Conclusion

You may think that the implementation about SPF might be somehow confusing. Well indeed it is not complicated, and by the way you have a great wizard that help you out to accomplish your mission (see the references section).

If are you worried about spam then SPF will help you, protecting your domain from forgeries, and all you have to do is to add a text line on your DNS server and configure your email server.

The advantages that SPF brings are big. However, like I said to someone, it is not a difference between the day and the night. The benefits of SPF will come with the time, when others adhere to it.

I have referred the Sender ID and its relation to SPF, but I didn't extend myself on any explanation about it. Probably you know already the reason, the politics of Microsoft is always the same, patents of software. On the references you can see the position of the openspf.org about SenderID.

On a next article we will talk about the configuration of the MTA, see you then.

I hope to give you a short introduction to SPF. If you are interested in learning more about it, just use the references that were used to make this article.

References

The official site of SPF.
The official FAQ of SPF.
The official wizard of SPF.
The position of the openspf.org about SenderID.
An excellent article about SenderId and SPF.
warn your users about the SASL convertion
HOWTO – Define an SPF Record