

Implementing SPF on Mac OS X 10.5.x/10.4.x

- 1. - Introduction**
- 2. - Requirements**
- 3. - Getting and installing SPF components**
- 4. - Using Mail::SPF to verify incoming messages**
- 5. - Setting up an SPF record**
- 6. - Caveats - READ this chapter!**

DISCLAIMER: The author(s) claim(s) no responsibility for any damage that may occur from the use of any information found here or found on links followed from this document. The author(s) will take credit for the good stuff though.

All items and/or companies mentioned on this and other pages are or may be trademarks, registered trademarks, or service marks of the respective companies or individuals.

1. - Introduction

The purpose of this document is to provide instructions on how to implement SPF on OS X 10.5.x/10.4.x Server.

You will not find many explanations as to why something is done one way or the other. Also, I will not discuss whether SPF is useful or not. This is a decision you must make for yourself. There are enough discussions about this available on the internet.

SPF functionality has two sides to it. First, it is used to verify if a sender domain is using SPF records and if the incoming mail came from an allowed mail server. Second, it allows you to publish your own SPF record for recipients to verify if mail came from an authorised server.

SPF functionality depends on several Perl modules and scripts to be installed.

Verification of the SPF record is done through amavisd-new/SpamAssassin. This allows to integrate as closely as possible with the existing components on OS X 10.5.x/10.4.x server. It would be possible to check at the postfix level with a policy server, but it is trickier to implement and if done incorrectly can result in more spam coming in.

The SPF record on the other hand only needs to be added to your DNS.

NOTE: Although not mandatory, for Mac OS X 10.4.x it is strongly recommended you first update amavisd-new and SpamAssassin. This is not necessary for Mac OS X 10.5.x. Some of the Perl modules necessary, may conflict with older versions of amavisd-new. Instructions for installing updating amavisd-new and SpamAssassin on OS X 10.4.x server can be downloaded from <http://osx.topicdesk.com/>

This document will require you to use the command line. If you do not feel comfortable with using the command line, you should look for a ready made installer package or for somebody to assist you.

This document is written for Mac OS X 10.5.x/10.4.x. It does not

apply to 10.3.x. as 10.3.x did not come with the same content filtering components pre-installed.

DISCLAIMER: Whatever you do based on this document, you do it at your own risk! Just in case you haven't understood: Whatever you do based on this document, you do it at your own risk!

This tutorial has been tested on a standard Mac OS X 10.5.x/10.4.x Server installation. If you have already tinkered with your system, be aware that things might differ. It is impossible for me to foresee all changes that one might have applied to a server.

This tutorial contains step-by-step instructions for the terminal. Although you could just type them in line by line, it is recommended you have a basic understanding of the terminal.

2. - Requirements

Before you get started, you need to make sure some basic requirements are met:

- You have made a backup of your system.
- You have the latest version of Apple's Developer Tools (Xcode 2.4 or higher for 10.4.x and XCode 3.0 or higher for 10.5.x) installed.
Dev Tools are available on your Server DVD and as a free download from Apple's Developer Connection.
- You do have a backup
- You are running 10.5.x/10.4.x or greater
- Although not mandatory, for Mac OS X 10.4.x it is STRONGLY (very STRONGLY) recommended you first update amavisd-new and SpamAssassin.
Some of the Perl modules necessary, may conflict with older versions of amavisd-new and SpamAssassin. Instructions for updating amavisd-new and SpamAssassin on OS X 10.4.x server can be downloaded from <http://osx.topicdesk.com/>
- Familiarity with a command line editor or alternatively a GUI plain text editor (do NOT use Word or similar)

3. – Getting and installing SPF components

This chapter will guide you through getting and installing the SPF component (and if required other components as well).

The component we will use is Mail::SPF (to be used with SpamAssassin for SPF verification).

There are other tools and combinations available out there, but this one makes most sense for OS X 10.4.x server.

As mentioned, you will need a few perl modules to be able to use SPF. This chapter will guide you through getting and installing them.

So let's get going:

Make sure you are logged in as root (or alternatively use sudo).

Install the latest version of Mail::SPF by issuing the following commands (*in oblique type*). Issue them one after the other making sure you do not miss any dots or slashes. Also note that the download URLs given may change in the future. In that case just replace the URLs in this document with the current ones.

NOTE: Lines wrapping without line spacing are a single command.

The easiest way to install them is by using CPAN.

```
sudo perl -MCPAN -e shell
```

If you have never used CPAN before you will be prompted to supply a few parameters. Just accept the default values. Once done, you should see the CPAN prompt (*cpan >*):

When at the CPAN prompt issue:

```
o conf prerequisites_policy ask
```

This will prompt you when a modules relies on other pre-requisites that have to be installed first. You should allow it to go ahead if asked.

Now you are ready to install the module(s). Be aware that some modules already exist on your server, but are outdated so it is best to install them all.

Just issue:

```
install Mail::SPF
```

This should get Mail::SPF and all required modules and bring you back to the CPAN prompt.

Now issue

```
exit
```

to exit CPAN.

NOTE: It is possible that some of the modules will not install. In that case use "*force install*" instead of "*install*" at the CPAN prompt.

NOTE: If you had previously tried to use CPAN without having the Developer Tools installed, you will need to make sure that Developer Tools are now correctly installed and will also need to re-configure CPAN. To do so get to the CPAN prompt and issue:

```
o conf init
```

You will be prompted to supply a few parameters. Just accept the default values.

NOTE: If for some (unlikely) reason the required modules did not get installed, here is a list of what is needed. Just install them manually from the CPAN prompt.:

```
Test::More
```

```
Net::DNS::Resolver::Programmable (do NOT install on 10.5)
```

```
Error
```

```
NetAddr::IP
```

```
URI
```

```
Net::DNS (do NOT install on Mac OS X 10.5)
```

Now everything we need to use SPF has been installed.

The next step is to configure everything for verification of incoming messages and set up our SPF record.

NOTE: You can use incoming verification only, create an SPF record only or both. The choice is yours, they do not have to be used together.

4. – Using Mail::SPF to verify incoming messages

As mentioned, we will use Mail::SPF together with SpamAssassin to verify incoming messages.

Depending on the version of SpamAssassin you have, you will need to either uncomment or add a few instructions.

Just edit `/private/etc/mail/spamassassin/init.pre` and add or uncomment the following line:

```
#loadplugin Mail::SpamAssassin::Plugin::SPF
```

So that it looks like this:

```
# SPF - perform SPF verification.  
#  
loadplugin Mail::SpamAssassin::Plugin::SPF
```

When done save.

Having made changes to the SpamAssassin configuration that do require network access, we also need to make a change in: `/etc/amavisd.conf`

Edit `/etc/amavisd.conf` and change (Mac OS X 10.4.x only. 10.5.x is already set correctly):

```
$sa_local_tests_only = 1;  
to  
$sa_local_tests_only = 0;
```

When done save.

Having made changes to the SpamAssassin configuration, we need to restart amavisd-new:

To do so issue:

```
sudo /bin/launchctl unload /System/Library/  
LaunchDaemons/org.amavis.amavisd.plist
```

```
sudo /bin/launchctl load /System/Library/LaunchDaemons/  
org.amavis.amavisd.plist
```

You may see the following error:

```
"Workaround Bonjour: Unknown error: 0"
```

It's due to a bug introduced in 10.4.7 and safe to ignore.

4. - Using Mail::SPF to verify incoming messages

Now everything is ready for incoming SPF verification. Send yourself an e-mail from a domain that uses SPF (e.g. gmail) and check the headers. You should see something along the lines of:
SPF_PASS =0.001
SPF_NEUTRAL=-0.001
in the X-Spam-Status Tests.

The scores are low on purpose by default. It is up to you to change them if you would like action to be taken based on this information.

Simply edit */private/etc/mail/spamassassin/local.cf* (or wherever you keep your score adjustments) and add:

```
score SPF_PASS 0.001
score SPF_FAIL -0.001
score SPF_NEUTRAL -0.001
score SPF_SOFTFAIL 0.001
score SPF_HELO_PASS 0.001
score SPF_HELO_FAIL -0.001
score SPF_HELO_NEUTRAL -0.001
score SPF_HELO_SOFTFAIL -0.001
```

(replace *0.001* with the score you want)

Remember to restart *amavisd-new* after score changes.

5. - Setting up an SPF record

You will now need to create an SPF record for your domain.

In its simplest form it would look something like this:

```
yourdomain.tld. 0 IN TXT "v=spf1 ?all"
```

If you don't know how to create your SPF record, you can use the wizard on openspf.org:

<http://www.openspf.org/>

Just enter your domain name and answer all sections.

As I mentioned at the beginning of this document, I am not going to go into the details of setting up SPF on a Linux or Windows server. I am just getting it up and running on OS X Server. Everything else is

already well documented.

Once you have created/prepared your record, all you need to do is to add it to your DNS.

This procedure can differ based on what DNS software/provider you use. Many providers use different control panels, so you may have to adjust as needed. If you manage your own DNS, you'll know what to do.

In essence you need to create and add 1 TXT record for each domain you handle.

To verify your SPF record record go here:
<http://www.openspf.org/Tools>

You should be all set now.

6. - Caveats

There most frequent issues to watch out for are:

- a) Incompatible perl modules
- b) Typos made when applying this tutorial
- c) Long lines seen as multiple lines. Watch for incorrect line breaks

Also, if you have modified any paths and or environment variables, make sure you check them against above instructions.

That's all folks.
Hope this helps.
Have fun,
Alex

Doc. Version 1.0.2, 26.10.2007
Athanasios Alexandrides
Lugano, Switzerland
tutorials -at- topicdesk.com
