- Partners
- Support
- Community
- Ubuntu.com

- Page History
- Login to edit

Search

Postfix/SPF

Introduction

Contents

This guide explains how to install and integrate Sender Policy Framework (SPF) checking with Postfix. It applies all supported Ubuntu releases.

SPF is an e-mail anti-forgery technology the enables domain owners to list, in the Domain Name Service (DNS), authorized sources of mail from their domains. It enables mail receivers to reject mail that does not come from authorized sources. This guide describes the second part of the protocol, rejecting mail from unauthorized sources. It assumes you have your Postfix set up and running. Setting up and running Postfix is described elsewhere in the wiki and in the Postfix documentation.

SPF Package selection and installation

In Ubuntu there are two RFC 4408 compliant policy servers for postfix you can use. One is written in Python. The other is written in Perl. The Perl package meets most basic requirements. The Python package is significantly more sophisticated (it provides a sane set of defaults, so setup is not necessarily more complex).

For the Python programs, installation is:

```
sudo apt-get install postfix-policyd-spf-python
```

For the Perl system, installation is:

```
sudo apt-get install postfix-policyd-spf-perl
```

Postfix Integration

There are a number of changes the need to be made to integrate SPF checking with Postfix. In this guide, integration of the Python programs is described. The Perl programs are integrated very similarly. See man postfix-policyd-spf-perl for details.

Enabling the Policy Service

In /etc/postfix/main.cf you will need to add the following line (it doesn't matter where, usually they get added to the end.

```
policy-spf_time_limit = 3600s
```

This changed the ups the policy time limit so the policy server won't time out while a message is still being processed.

Add this section to /etc/postfix/master.cf for the Python script

```
policy-spf  unix  -       n       n       -       -       spawn
     user=nobody argv=/usr/bin/policyd-spf
```

or for the Perl script

```
policy-spf  unix  -       n       n       -       -       spawn
     user=nobody argv=/usr/sbin/postfix-policyd-spf-perl
```

Finally, you need to add the policy service to your smtpd_recipient_restrictions in file /etc/postfix/main.cf:

```
smtpd_recipient_restrictions =
     ...
     permit_sasl_authenticated
     permit_mynetworks
     reject_unauth_destination
     check_policy_service unix:private/policy-spf
     ...
```

Note: Put the policy service after reject_unauth_destination to prevent unexpected responses from the policy service from making your system an open relay (this is recommended for all policy services). Moreover, put the policy service after you permit local senders. You only want SPF to check inbound mail from the internet, not outbound mail from your users.

Note: Executable path for master.cf corrected 10/27/07.

Reload Postfix

```
sudo /etc/init.d/postfix reload
```

Verifying It's Working

Check your mail logs. The Python server logs mail that is rejected or deferred due to SPF. If there is a problem with the policy server or its integration with Postfix, it will be logged.

```
tail -f /var/log/mail.log
```

or

```
less /var/log/mail.log
```

Postfix/SPF (last edited 2013-10-04 07:52:14 by phunehehe @ 115.79.207.194[115.79.207.194]:phunehehe)