# 邮件服务器添加spf过滤规则

# 一、描述

1、SPF(Sender Policy Framework)是为了防范垃圾邮件而提出来的一种DNS记录类型，它是一种TXT类型的记录，它用于登记某个域名拥有的用来外发邮件的所有IP地址。当你定义了你的domain name的SPF记录之后，接收邮件方会根据你的SPF记录来确定连接过来的IP地址是否被包含在SPF记录里面，如果在，则认为是一封正确的邮件，否则则认为是一封伪造的邮件。

2、目的：实现防伪装，过滤伪装的域名所发的大量垃圾邮件

3、邮件服务器架构：Postfix+Dovecot+Clavmd+Spamd+amavisd

# 二、具体步骤:

## 1、安装Perl模块

#### 1)下载软件

wget <https://launchpad.net/postfix-policyd-spf-perl/trunk/release2.010/+download/postfix-policyd-spf-perl-2.0.10.tar.gz>

#### 2)安装模块

perl –MCPAN –e ‘install version’

perl –MCPAN –e ‘install NetAddr::IP’

perl –MCPAN –e ‘install Mail::SPF’

perl –MCPAN –e ‘install Sys::Hostname::Long’

#### 3)解压软件

tar zxf postfix-policyd-spf-perl-2.010.tar.gz

cd postfix-policyd-spf-perl

cp postfix-policyd-spf-perl /usr/libexec/postfix/policyd-spf-perl

## 2、配置命令

1)配置postfix使postfix调用policy-spf程序

vim /etc/postfix/master.cf

#spf check

Policy-spf unix - n n - - spawn

User=nobody argv=/usr/bin/perl /usr/libexec/postfix/policyd-spf-perl

2)配置postfix主配置文件，将检查spf选项添加到permit\_mynetworks之后，使内网中的网段不受spf的影响

vim /etc/postfix/main.cf

smtpd\_sender\_restrictions =

permit\_mynetworks,

check\_policy\_service unix:private/policy-spf,

header\_checks = pcre:/etc/postfix/header\_checks

3)spf产生的三种状态pass，softfail，none 将后两种状态的邮件视为垃圾邮件拒绝掉

vim /etc/postfix/header\_checks

/Received-SPF: none/ REJECT

/Received-SPF: softfail/ REJECT

4)执行postmap生成header\_checks.db文件，重启postfix使之生效

postmap /etc/postfix/header\_checks

/etc/init.d/postfix restart

## 3、测试查看日志

查看spf状态为none

