Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Linux BIND DNS Configure Sender Policy Framework (SPF) an e-mail Anti Forgery System

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

Q. How do I configure Sender Policy Framework (SPF) anti spam forgery system under Redhat Linux BIND server? I was advised to configure SPF for our corporate domain to identify and reject forged addresses in the SMTP MAIL FROM (Return-Path), a typical nuisance in e-mail spam.

A. Spammer always tries to spoof e-mail. Normal SMTP [2] allows any computer to send an e-mail claiming to be from anyone. Thus, it's easy for spammers to send e-mail from forged addresses. This makes it difficult to trace back to where the spam truly comes from, and easy for spammers to hide their true identity in order to avoid responsibility. Many believe that the ability for anyone to forge sender addresses (also known as Return-Paths) is a security flaw in modern SMTP, caused by an undesirable side-effect of the deprecation of source routes.

Steps to configure Sender Policy Framework

First, you need to access to DNS server zone files. Some domain registers / ISPs provides front end (control panel) to define SPF records. You need to set a TXT record by editing zone file. It allows you define real IP address of your mail server and other hosts such as webserver.

Set SPF for a domain called theos.in

Open your dns zone file such as /var/named/data/zone.theos.in and append something as follows:

```
@                       86400    IN TXT   "v=spf1 a mx ~all"
```

OR

```
theos.in.              IN TXT "v=spf1 a mx ~all"
```

Save and close the zone file. Restart bind:

```
# service named restart
```

Where,

- **v=spf1** : Define an SPF recored.
- **a** : theos.in IP address is xx.yy.zz.eee and that server is allowed to send mail from theos.in.
- **mx** : theos.in has one MX server called smtp.theos.in. It is allowed to send mail from theos.in.
- **~all** : SPF queries that do not match any other mechanism will return "softfail". Messages that are not sent from an approved server should still be accepted but may be subjected to greater scrutiny. If you need tight control replace ~all with -all (hard fail).
  For example, following recored the "a" and "mx" specify the systems permitted to send messages for the given domain. The "-all" at the end specifies that, if the previous mechanisms did not match, the message should be rejected.

```
cyberciti.biz.              IN TXT "v=spf1 a mx -all"
```

Large network setup

Let us say you have a corporate domain called nixcraft.com with static IP network 74.86.49.128/28. All IPs in this range can send an email. Your email server is called smtp.nixcraftmail.com. You need to SPF as follows for nixcraft.com domain:

```
nixcraft.com. IN TXT "v=spf1 ip4:74.86.49.128/28 a mx ~all"
```

Also you need to set SPF for nixcraftmail.com as follows:

```
smtp.nixcraftmail.com. IN TXT "v=spf1 a -all"
```

tinydns (djbdns) DNS Setup

If you run tinydns / djbdns, enter following:

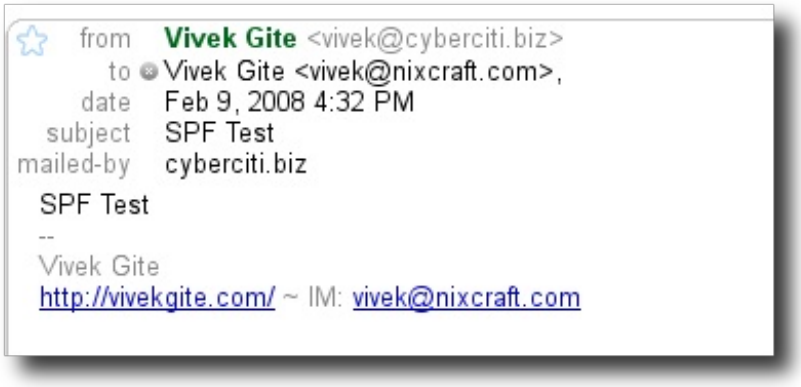
```
'nixcraft.com:v=spf1 ip4\07274.86.49.128/28 a mx ~all:3600
'smtp.nixcraftmail.com:v=spf1 a -all:3600
```

Test SPF / spf recored lookup

First make sure SPF TXT recored updated using dns client tool such as host or dig:

```
$ host -t txt domain.com
$ host -t txt nixcraft.com
$ host -t txt nixcraft.com ns1.isp.com
```

If your SPF configured correctly webmail service such as Gmail or Yahoo mail can display spf result by viewing email headers:



[3]

(Fig. 01: SPF in action - Gmail confirms email is send by my own server [mailed-by cyberciti.biz])
To view email headers click on Reply down arrow > Show original:

```
Received-SPF: pass (google.com: domain of vivek@cyberciti.biz designates 74.86.48.98 as per
Authentication-Results: mx.google.com; spf=pass (google.com: domain of vivek@cyberciti.biz
```

Microsoft 2000 / 2003 / 2008 DNS SPF Configurations

If you run Microsoft DNS server, see these instuctions [4].

Sample BIND zone file for cyberciti.biz domain

```
$ORIGIN cyberciti.biz
$TTL 86400
@ IN SOA ns1.cyberciti.biz. vivek.cyberciti.biz. (
                        2008020302        ; Serial
                        3600              ; Refresh
                        300               ; Retry
                        604800            ; Expire
                        3600)             ; Minimum

@                       86400     IN NS    ns1.cyberciti.biz.
@                       86400     IN NS    ns2.cyberciti.biz.

@                       3600      IN MX 10 smtp.cyberciti.biz.

@                       86400     IN TXT   "v=spf1 ip4:74.86.49.128/28 a mx ~all"
```

```
feeds                   86400    IN CNAME feeds.feedburner.com.
*                       3600     IN A     74.86.49.130
@                       86400    IN A     74.86.49.130
rd                      86400    IN A     74.86.49.130
www                     3600     IN A     74.86.49.130
vpn         86400    IN A     10.10.2.5
```

Recommended readings:

- Wizard based system to set SPF
- Test SPF online [5]
- Wikipedia SPF article [2]
- BIND DNS Server [6]
- djbdns DNS Server [7]
- Microsoft DNS server specific SPF instructions [4]