SPF-запись - проверяем валидность отправителя

Опубликовано muff в Пнд, 2010-07-12 04:16

Как всем известно, протокол отправки электронной почты SMTP, подразумевает, что в качестве отправителя можно указать любой почтовый ящик. Таким образом можно послать письмо, подставив в поле "From" вымышленное значение. Процесс такого почтового обмана называется Спуфинг (e-mail spoofing). Чтобы бороться с этим явлением, был разработан и введен в действие стандарт SPF – ***Sender Policy Framework (структура политики отправителя).***

SPF позволяет владельцу домена указать в TXT-записи домена специальным образом сформированную строку, указывающую список серверов, имеющих право отправлять email-сообщения с обратными адресами в этом домене.

Рассмотрим простой пример SPF-записи.

```
example.org. IN TXT "v=spf1 +a +mx -all"
```

Теперь более детально о допустимых опциях. Рассмотрим варианты поведения получателя, в зависимости от используемых опций:

- **"v=spf1"** - используемая версия SPF.
- **"+"** - принимать корреспонденцию (Pass). Этот параметр установлен по умолчанию. Тоесть, если никаких параметров не установлено, то это "Pass";
- **"-"** - Отклонить (Fail);
- **"~"** - "мягкое" отклонение (SoftFail). Письмо будет принято, но будет помечено как СПАМ;
- **"?"** - нейтральное отношение;
- **"mx"** - включает в себя все адреса серверов, указанные в MX-записях домена;
- **"ip4"** - опция позволяет указать конкретный IP-адрес или сеть адресов;
- **"a"** - указываем поведение в случае получения письма от конкретного домена;
- **"include"** - включает в себя хосты, разрешенные SPF-записью указанного домена;
- **"all"** - все остальные сервера, не перечисленные в SPF-записи.

Итак, попробуем разобраться, что же значит SPF-запись, указанная выше.

- **"+a"** - разрешает прием писем от узла, IP-адрес которого совпадает с IP-адресом в A-записи для example.org;
- **"+mx"** - разрешает прием писем, если отправляющий хост указан в одной из MX-записей для example.org;
- **"-all"** - все сообщения, не прошедшие верификацию с использованием перечисленных механизмов, следует отвергать.

Для лучшего понимания того, как работает SPF, рассмотрим еще один, более сложный пример.

```
example.org. IN TXT "v=spf1 mx ip4:195.3.159.250 +a:smtp.mail.ru include:gmail.com ~
all"
```

Теперь более подробно о используемых опциях...

- **"mx"** - принимать письма от серверов, указанных в MX-записях;
- **"ip4:195.3.159.250"** - принимать письма, отправленные с IP-адреса **195.3.159.250**;
- **"+a:smtp.mail.ru"** - то же, что и **a:smtp.mail.ru**. Принимать от **smtp.mail.ru**;

- **"include:gmail.com"** - принимать письма с серверов, разрешенных SPF-записями **gmail.com**;
- **"~all"** - принимать письма со всех остальных серверов, но помечать их как СПАМ

А теперь рассмотрим еще более "экзотичный" пример. В описании возможных опций указывалось, что возможно указание сетей ip-адресов. Стоит отметить, что это применимо и к записям "a" и "mx". Рассмотрим следующий пример.

```
example.org. IN TXT "v=spf1 mx/24 a:muff.kiev.ua/24 -all"
```

- **"mx/24"** - в список разрешенных отправителей входят все IP-адреса, находящихся в тех же сетях класса C, что и MX-ы домена;
- **"a:muff.kiev.ua/24"** - в список разрешенных отправителей входят все IP-адреса, находящихся в тех же сетях класса C, что и A-записи домена muff.kiev.ua;
- **"-all"** - всех остальных отправителей - блокируем.

Иногда можно встретить следующие записи (очень редко):

- **"ptr"** - проверяет PTR-запись IP-адреса отправителя. Если она сходится с указаным доменом, то механизм проверки выдает положительный результат. Тоесть, разрешено отправлять всем IP-адресам, PTR-запись которых направлены на указанный домен. Серьезным недостатком даного метода есть то, что генерируется очень большое количество DNS-запросов;
- **"exists"** - выполняется проверка, резолвится ли домен на какой-либо IP-адрес. Тоесть, по существу, выполняется проверка работоспособности доменного имени. Кстати, не имеет значения, на какой IP-адрес резолвится домен, даже если это "серые" сети (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) или loopback (127.0.0.1).

Пример использования:

```
example.org. IN TXT "v=spf1 ptr:example.org exist:example.org -all"
```

Также не будет излишним ознакомиться со следующими опциями: **redirect** и **exp**.

"redirect" - указывает получателю, что нужно проверять SPF-запись указаного домена, вместо текущего домена. Пример:

```
example.org. IN TXT "v=spf1 redirect:example.com ~all"
```

В даном примере будет проводится проверка SPF-записи домена **example.com**, а не **example.org**.

"exp" - использование даной опции позволяет задать сообщение о ошибке, которое будет передано отправителю при возникновении таковой. Размещается в конце SPF-записи, даже после опции **all**. Рассмотрим более детально механизм работы опции **exp**.

Допустим, что у домена example.org следущая SPF-запись:

```
example.org. IN TXT "v=spf1 +a +mx -all exp=spf.example.org"
```

Теперь содаем TXT-запись для домена spf.example.org:

```
spf.example.org. IN TXT "You host not allowed e-mail to me from this domain!"
```

В результате этих шаманских действий SPF-запись будет контролировать, чтобы почта доставлялась только от валидных хостов, а всем остальным будет отправляться сообщение о ошибке, прописанное в TXT-записи домена spf.example.org.

На этой позитивной ноте, пожалуй, статью можно закончить. Азы использования SPF-записи описаны, а механизм работы можно изучить более детально при практическом использовании.

Источник (получено *2026-11-23 20:09*):
http://muff.kiev.ua/content/spf-zapis-proveryaem-validnost-otpravitelya