

How to avoid Backscatter in Sendmail

What is Backscattering?

Your email server is a victim of backscattering if you are receiving complaints from legitimate external users indicating that THEY are receiving "user unknown" bounce emails from YOUR domain that they supposedly sent to YOUR internal users, which they didn't. The bounced "user unknown" message contains SPAM.

Example: A <john.doe@yahoo.com> is receiving "user unknown" emails from your <MAILER-DAEMON@your.domain.com> indicating that they sent email to a <jane.doesnotexist@your.domain.com>. The message itself is in fact a SPAM....

This happens in large companies that have their MX server receive email for <whomever@your.domain.com> and later forwards it to its internal Message Store Server (MSS - where their users retrieve their email . a.k.a the POP or IMAP server). Only then, your MSS server rejects email for unknown users causing an email to "bounce" back to legitimate external user who have never sent the email in the first place..!

What to do?

Your MX servers should reject email for unknown users at the SMTP initial transaction and NOT forward them to internal SMTP servers without a "user check".

How to do this in sendmail with access_db?

Example scenario:

- **your domains for which you provide email service:** "example.com" and "my.org"
- **Name of the MX server for your domains:** mx.my.org
- **Name of your POP/IMAP server:** imap.my.org

- **Step1:** In **mx.my.org**, add these 4 lines to your ".mc" file in the right place..
FEATURE(access_db, hash -T<TMPF> /etc/mail/access)dnl FEATURE(`blacklist_recipients')dnl
define(`VIRTUSER_TABLE', `hash -o /etc/mail/virtusertable')dnl
VIRTUSER_DOMAIN_FILE(`/etc/mail/virtuserdomain')dnl
- **Step2:** In **mx.my.org**, put YOUR internal valid domains in **/etc/mail/virtuserdomain**

example.com
my.org
- **Step3:** In **mx.my.org**, add these lines to your "access" file (**/etc/mail/access**):
-----insert to access file-----
For each domain you serve . equals to class w
From:example.com OK
From:my.org OK

list of internal domains that have their own servers and you do not serve them, only receive email from them. equal to "internal domains that you receive email via MX"

How to avoid Backscatter in Sendmail

From:marketing.my.org OK
From:marketing.example.com OK

```
#####  
# Reject Forgery - Not required for Backscattering  
#####  
# FOR TEST USE: /usr/lib/sendmail -bt  
# check_mail <valid.user@example.com> --> ACCESS DENIED  
From:example.com REJECT  
# check_mail <valid.user@my.org> --> ACCESS DENIED  
From:my.org REJECT
```

```
#####  
## Reject Backscatter....  
# reject unknown recipients, because SPAMMERS use this to spam other  
# domains through bounces messages (user unknown).  
#  
#####  
# general rejection strings  
To:example.com error:5.1.1:"550 User unknown"  
To:my.org error:5.1.1:"550 User unknown"  
#  
#####  
# Valid internal EMAIL addresses  
#  
To:john.doe@example.com RELAY  
To:jane.joe@my.org RELAY  
To:postmaster@example.com RELAY  
etc...  
-----end access-----
```

- **Step4:** In **mx.my.org**, **regenerate** your "sendmail.cf" and **re-makemap** your "access" database
- **Step5:** In **mx.my.org**, **TEST** the configuration using an external IP address (in this example **200.89.70.8 mx.uchile.cl**):

```
$ /usr/lib/sendmail -bt -d21.4
```

```
.D{client_addr}200.89.70.8  
.D{client_name}mx.uchile.cl
```

```
check_rcpt <john.doe@example.com>  
# should produce a ---> RELAY
```

```
check_rcpt <user.notexist@example.com>  
# should produce a ---> "550 User unknown"
```