Securing sendmail

How to protect your mail server
from use by spammers.

James Lick jlick@jameslick.com

Contents

- What is an open relay?
- What minimum version is safe?
- How do I configure anti-relay?
- How to white-list my networks?
- What if I can’t upgrade?
- How can I test my servers?
- What about roaming users?

What is an open relay?

- Mail is sent from server to server until it reaches the destination
- Traditionally, most servers would forward (relay) mail for anyone
- This allowed for simple configurations and high reliability
- Spammers use this as a “free ride” to send mail, and to mask the true origin

What is an open relay?

- Current software will only forward mail for authorized senders
- Now you need to configure each server for what is authorized
- Most anti-spam tools block mail sent through open relays
- Known open relays will find it increasingly difficult to send mail

What minimum version is safe?

- Sendmail 8.8 is first capable of anti-relay
- Sendmail 8.9 is first version safe from anti-relay by default
- Sendmail 8.10 through current have progressively added more safety features
- Sendmail 8.12.10 is latest with no known security bugs
- It is best to run a fairly recent version

What minimum version is safe?

- You need to use a .cf file which matches your sendmail version
- You should use m4 configs to make changes to the .cf file
- You should not enable any relaying features without careful consideration
- Some vendors patch older versions instead of upgrading to the latest

How do I configure anti-relay?

- For version 8.8 see http://www.sendmail.org/antispam.html
- For version 8.9 and higher, relay is off by default.
- Check your m4 config file, usually /etc/mail/sendmail.mc or /usr/lib/mail/cf/main.mc for dangerous settings

How do I configure anti-relay?

- Dangerous settings include the following features: relay_based_on_MX, relay_local_from, loose_relay_check, or promiscuous_relay
- Add domains you accept or relay mail to in /etc/mail/relay-domains

How to white-list my networks?

- Only white-list your own networks
- /etc/mail/access:

  192.168.2 RELAY
- makemap hash /etc/mail/access < /etc/mail/access
- access.db doesn’t support CIDR style network addresses
- Beware of open-relays on your network

What if I can’t upgrade?

- Make sure that older versions are not accessible
  - Disable sendmail if not needed
  - Firewall the server’s port 25 from remote access
  - Disable daemon mode if only used for sending by removing –bd option from startup script (leaving –q15m or similar) and add MX records for receiving mail

How can I test my servers?

- Be sure to test your servers from outside your network to avoid confusion
- http://www.abuse.net/relay.html can test via any web browser
- http://www.unicom.com/sw/rlytest/ is a perl script to test for open relay – good for automation

What about roaming users?

- Users sending mail from off network often don’t have a good solution
- Use the host network’s mail server
  - May reject foreign domains
  - Recipient may reject on domain mismatch
  - Less control over how mail is sent
- Use Virtual Private Network (VPN)
  - Complex to support

What about roaming users?

- Use pop-before-smtp
  - Security is not very good
  - Not always reliable
- Use SMTP AUTH
  - Usually not supported by default
  - Requires client support
  - Standardized, and gaining support
  - Can use SSL certs for optimal security

What about roaming users?

- Use SMTP AUTH (continued)
  - Vulnerable if weak passwords are used
  - Non-SSL transactions can have passwords snooped
  - http://www.sendmail.org/~ca/email/auth.html for installing and enabling

For more information?

- http://www.sendmail.org/ has good online documentation.
- “sendmail” by Bryan Costales and Eric Allman aka The Bat Book ISBN: 1565928393