

Re: IS MY SERVER A RELAY?

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2006-10/msg03357.html>

- *From:* "Leif Pedersen [MVP]" <Leif.pedersenNO-SPAM@xxxxxxxxxxx>
 - *Date:* Wed, 25 Oct 2006 22:26:43 +0200
-

Hi,

Are the mails for internal or external users. If the mails are for internal users it is not considered relaying.

Leif

"GC Postmaster" <gc_postmaster@xxxxxxxxxxxxxxxxxxxx> wrote in message news:Otvso4G%23GHA.3456@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello,

I recently came to know something unsettling. Our internal servers can send mail via our exchange smtp protocol without the ip address being in the relay list. I have been using the relay list exclusively, so I'm not sure how this is possible. Below are the settings we have. If you can think of any way this is possible and how to fix it, please let me know.

mailserver.ourdomain.com is the smtp address people are supposed to put into programs for the smtp server. it is a dns cname for one of our exchange servers.

in the exchange system manager, we have the smtp protocol with these settings:

Administrative Groups -> First Admin Group -> exserver -> protocols -> smtp -> default smtp server ->

1. under IP address advanced settings, then "edit" the setting for "apply sender filter" is checked.

2. Access tab

a. authentication button

i. anonymous access is checked

ii. resolve anonymouse email is not checked

iii. basic authentication is checked

iv. requires TLS is not checked

v. there is no default domain listed

Re: IS MY SERVER A RELAY?

vi. integrated windows authentication is checked

USERS button

1. we have two users listed who can send via the server if they authenticate. they are myself and another admin account. no one knows their pwds but me.

b. connection button

i. the radio button for "all except the list below" is selected.

there are no ip addresses in the list.

c. relay button

i. the radio button for "only the list below" is selected. many servers' ip addresses are in this list. there are servers who's ip address IS NOT in the list, yet I confirmed that they have programs sending mail via this server. I used telnet from them to the exchange server and it worked fine sending e-mails. I was under the impression that unless i authenticated as one of the users in the list described above or on a machine whose ip address was in this list, that I wouldn't be able to telnet over port 25 to this server.

ii. the "allow all computers which successfully authenticate..."

check box is not checked.

USERS BUTTON

this lists the same two accounts described above.

3. Messages Tab

a. the first two check boxes are cleared. the next two have 50 and 640000 as their setting, respectively.

b. the setting for sending copies of NDRs is filled in with an address.

c. there is nothing in the "forward all mail with unresolved..."

4. Delivery Tab

a. the intervals are all set up.

b. Outbound security

i. the "anonymous access" radio button is selected.

ii. tls encryption is not checked.

c. Outbound Connections tab

i. the limit number of connections to is set to 1000

ii. the limit number of connections per domain is set to 100

iii. tcp port is 25

b. Advanced tab

i. the max hop count is 30

ii. the FQDN is set up

iii. it is not performing reverse DNS lookups.

Anyone who can help would be greatly appreciated!

Peace.