

Re: IS MY SERVER A RELAY?

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2006-10/msg03530.html>

- *From:* "GC Postmaster" <Blake.Whitney@xxxxxxxxxx>
 - *Date:* 26 Oct 2006 13:38:01 -0700
-

That's the way I understood things should work. What I'm saying is that this isn't happening. Servers whose IP address is not in our relay list are able to send mail through our exchange smtp server and they are also not authenticating. My desktop computer's ip address is not in the allow relay and even i could telnet over port 25 to the exchange server and send mail that way.

I was hoping based on my posted settings someone would see something wrong with our config and I'd be able to fix it. We only want the situation described, but right now it seems not to be the case.

Ed Crowley [MVP] wrote:

The IP addresses listed in your list are authorized to relay. All other IP addresses must authenticate to do so. Does that answer your question?

—

Ed Crowley

MVP – Exchange

"Protecting the world from PSTs and brick backups!"

"GC Postmaster" <Blake.Whitney@xxxxxxxxxx> wrote in message
<news:1161890388.917695.113540@xx>

This is fine. The real question I'm trying to answer here is why servers are able to send mail via our exchange server whose IP address is not in the relay list. This should not be.

Our users are using authentication to send messages. Just not programs that send e-mail alerts from other servers. Those servers have been given access via IP address.

Ed Crowley [MVP] wrote:

Most Exchange users mostly MAPI clients so the need to relay is generally limited. When there is such a need, such as with Entourage

Re: IS MY SERVER A RELAY?

or Eudora clients, the best practice is to require authentication instead of allowing relay by IP address.

—
Ed Crowley
MVP – Exchange
"Protecting the world from PSTs and brick backups!"

"GC Postmaster" <gc_postmaster@xxxxxxxxxxxxxxxxxxxx>
wrote in message
news:eKtB9UH%23GHA.4524@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Leif,

The messages are destined for both offsite users and internal users. Shouldn't we be able to make it so you can't send to either unless your ip address is in that list or your username is in the allow users who authenticate list?

Is it normal to allow any internal computer to relay through exchange if the rcpt to or mailfrom address is a mydomain.com address?

Thanks.

"Leif Pedersen [MVP]"
<Leif.pedersenNO-SPAM@xxxxxxxx>
wrote in message
news:%23oYMkPH%23GHA.1128@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

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>

Re: IS MY SERVER A RELAY?

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

Re: IS MY SERVER A RELAY?

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

Re: IS MY SERVER A RELAY?

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
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

Re: IS MY SERVER A RELAY?

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

Re: IS MY SERVER A RELAY?

"allow all
computers
which
successfully
authenticate..."
checkbox 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"

Re: IS MY SERVER A RELAY?

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.

Re: IS MY SERVER A RELAY?