

Re: Exchange spam relay problem?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-08/msg00068.html>

- *From:* Jim <Jim@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 2 Aug 2006 17:35:02 -0700
-

Chris,

I am having the same problem your having with our server. AOL has put our domain on the 24hour blocked list, but the 24hrs have turned into weeks now. When I enabled SMTP logging, there are connections going to domains that my users haven't email to. Have you resolved this issue with your domain?

"Chris" wrote:

Hi Les,

I did check the queue names as you suggested – and yes – all the queues with retry status did hold goofy non-existing domains. But when I disabled the outbound mail (on the "Queues" display) for an hour or two outside office hours where no one were using the system, I got a very high number of real domains as well, some of them with up to 62 different recipients within the queue.

This made me try the dnsreport.com on my domain [my domain], and according to that tool, I have a number of issues with the mail setup:

1. The mailserver does not accept mail in the domain literal format (user@[0.0.0.0]) which actually seems to be in non compliance with RFC 1123 5.2.17. How do I correct this?
2. The domain does not have a SPF-record. I guess that is something that should be fixed on the DNS servers?
3. The OpenRelay test did not show anything, but a more thorough test at www.abuse.net/relay.html did raise a serious question mark in the Relay test 6:

RSET

Re: Exchange spam relay problem?

<<<250 2.0.0 Resetting

MAIL FROM : <spamtest@[my domain]>

<<<250 2.1.0 spamtest@[my domain] . Sender OK

RCPT TO:securitytest%abuse.net@[my domain]

<<<250 2.1.5 securitytest%abuse.net@[my domain]

Does Exchange see this as originating from within the domain [my domain] or what is going on? If so, how do I fix this?

Regards Chris

"Les Connor [SBS Community Member – SBS MVP]" <les.connor@xxxxxxxxxxxx> wrote in message news:%23nrGme0jGHA.4264@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Take a look at the domain names and see if any of them are domains you do – or want to do – business with. Try them on dnsreport.com. The reason they're in the queue is because they're not reachable, they don't exist, they're bogus, they're wasting your cpu cycles and internet bandwidth.

Les Connor [SBS Community Member – SBS MVP]

SBS Rocks !

"Tell me and I'll forget. Show me and I'll remember. Involve me and I'll understand." – Confucius

"Chris" <chr0081@xxxxxxxxxxxx> wrote in message news:ehYm3bnjGHA.3496@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi Les
Thanks for your help – I just hope you are right about the contents in the queues :-)
Regards Chris

"Les Connor [SBS Community Member – SBS MVP]" <les.connor@xxxxxxxxxxxx>

Re: Exchange spam relay problem?

wrote in message

news:eOXgRKmjGHA.1552@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Whoops, I meant many of us had Exchange SP1 installed prior to SBS SP1.

Install SBS SP1 and then Exchange SP2.

--

Les Connor [SBS Community Member – SBS MVP]

SBS Rocks !

"Tell me and I'll forget. Show me and I'll remember. Involve me and I'll understand." – Confucius

"Chris" <chr0081@xxxxxxxxxxx> wrote in message

[news:e2z\\$Q8ZjGHA.3572@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:e2z$Q8ZjGHA.3572@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi Les,

Thanks for your reply and the explanation which certainly reduces the probability of ending on a blackhole list. Is there by the way some tools one could use to read the rejected messages in the SMTP connector queues – just to make sure it is Non Delivery Reports?

Finally – is it possible to apply Exchange SP2 in a SBS environment without first upgrading SBS to SP1? – And is it advisable?

Best regards

Chris

"Les Connor [SBS Community Member – SBS MVP]"

Re: Exchange spam relay problem?

<les.connor@xxxxxxxxxxxx>

wrote in message

news:ONBaglYjGHA.4284@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi Chris,

These outgoing queues are almost certainly as a result of email being sent to your domain, but addressed to non-existent users (email addresses). Exchange then attempts to send a Non Delivery Report to the sender, but the originating sender's email address is bogus, therefore the queues build up and the email is re-tried until the time-out limit.

To protect yourself from this "NDR Attack", you can take these steps:

Re: Exchange spam relay problem?

- a) Apply Exchange SP2
- b) Enable Active Directory Filter – which sets your server to reject email that doesn't match an existing valid email address in your domain.
- c) Enable Intelligent Message Filter – which helps reduce the amount of spam that is sent to valid email addresses.

The instructions for AD Filter and IMF can be found in the Exchange on-line help system, and also by google search for those terms against this newsgroup.

--

Les Connor
[SBS

Re: Exchange spam relay problem?

Community
Member –
SBS MVP]

SBS Rocks
!

"Tell me
and I'll
forget.
Show me
and I'll
remember.
Involve me
and
I'll
understand."
– Confucius

"Chris"
<chr0081@xxxxxxxxxxxx>
wrote in
message
news:ejqKfaljGHA.2188@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi,
I
just
noticed
21
new
relayed
messages
arriving
around
noon
for
different
recipients,
all
under
domain
earthlink.net.
They
all
arrived
within
2
seconds.
No

Re: Exchange spam relay problem?

entries
were
created
in
the
application
log
even
though
SMTP
Protocol
Maximum
logging
is
still
enabled.
I
really
would
appreciate
some
help
before
the
server
ends
on
a
blockhole
list.
Thanks
in
advance
Chris

"Chris"
<chr0081@xxxxxxxxxxxx>
wrote
in
message
news:%23MfA2fBjGHA.1640@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi,
The
sender
address
is
to
the
best
of

Re: Exchange spam relay problem?

my
knowledge
always
Postmaster@<domain>
Regards
Chris

"ketanbhut"
<ketanbhut@xxxxxxxx>
wrote
in
message
news:1149893063.044238.173620@xxxxxxxxxxxxxxxx

hey
chris,
could
you
confirm
the
sender
address
?
is
it
unique
(postmaster)

Chris
wrote:

Hi,

I
think
I
may
have
a
mail
relay
spam
issue
on
a
server.
What
complicates
the

Re: Exchange spam relay problem?

situation
is
that
all
settlings
to
the
best
of
my
judgment
seems
to
be
in
accordance
with
Article
ID
324958
rev
9.0,
December
28,
2005
("How
to
block
open
SMTP
relaying
and
clean
up
Exchange
Server
SMTP
queues
in
Windows
Small
Business
Server").

The
symptoms
are
a
large

Re: Exchange spam relay problem?

number
of
strange
SMTP
connector
queues
–
especially
if
I
try
to
disable
outbound
mail
during
the
night
hours
(where
no
one
is
supposed
to
use
the
system).
Max
increase
between
01:00–03:00
AM.

The
system
is
running
SBS2003
without
SP1
but
else
fully
patched.
Exchange
is
SP1,
also

Re: Exchange spam relay problem?

fully
patched.
Server
is
multihomed
with
Basic
Firewall
activated
and
further
a
3COM
Secure
Gateway
between
the
server
and
the
internet
with
only
port
25
open.
POP3
is
not
being
used.

Selecting
SMTP
Protocol
Maximum
Logging
level
did
not
reveal
much
apart
from
a
number
of
7010
events

Re: Exchange spam relay problem?

(Invalid address, Unable to relay; Need to authenticate first). The number of 7010 events though is much lower than the number of strange queues, so the queues can most likely not just be the reject messages.

So please – how should I proceed to discover what is really

Re: Exchange spam relay problem?

going
on
–
and
eventually
fix
the
problem?

Chris