

# Re: Open Relays

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.admin/2007-01/msg00014.html>

---

- *From:* "Kevin Longley" <[kwlongley@xxxxxxxxxxxxxxxx](mailto:kwlongley@xxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 2 Jan 2007 16:23:36 -0500
- 

This url may help

<http://support.microsoft.com/kb/895853/en-us>

"news.zen.co.uk" <[test@xxxxxxxx](mailto:test@xxxxxxxx)> wrote in message  
[news:4599170a\\$0\\$32020\\$fa0fcedb@xxxxxxxxxxxxxxxx](mailto:news:4599170a$0$32020$fa0fcedb@xxxxxxxxxxxxxxxx)

Hi All

Recently one of my clients has been blacklisted via  
<http://www.spamhaus.org/> and I am currently trying to ascertain the cause  
of the problem.

I have ensured that all clients have the latest AV definitions and have  
performed a full system scan on all machines including the Exchange server  
and everything is "clean". I have also ran various spywhere detection  
utilities and again everything is "clean".

My next step was to test for open relays. On the majority of the websites  
which test for open relays the result was that the Exchange server was not  
configured as an open relay (which I expected). However on several of the  
sites it claimed that the machine was an open relay. Please find below  
the result of the test (I have removed the real IP address)

Relay test 1

RSET

<<< 250 2.0.0 Resetting

MAIL FROM:

<[spamtest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:spamtest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>

<<< 250 2.1.0 spamtest@xx OK

RCPT TO:

<[relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>

Re: Open Relays

<<< 550 5.7.1 Unable to relay for relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
Relay test 2

RSET

<<< 250 2.0.0 Resetting

MAIL FROM:

<spamtest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

<<< 250 2.1.0 spamtest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx OK

RCPT TO:

relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

<<< 550 5.7.1 Unable to relay for relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
Relay test 3

RSET

<<< 250 2.0.0 Resetting

MAIL FROM: <spamtest>

<<< 250 2.1.0 spamtest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx OK

RCPT TO:

<relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

<<< 550 5.7.1 Unable to relay for relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
Relay test 4

RSET

<<< 250 2.0.0 Resetting

MAIL FROM: <>

<<< 250 2.1.0 <>....Sender OK

RCPT TO:

<relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

<<< 550 5.7.1 Unable to relay for relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
Relay test 5

RSET

<<< 250 2.0.0 Resetting



Re: Open Relays

RCPT TO:

<relaytest%antispam-ufrj.pads.ufrj.br@[80.177.41.226]>

<<< 550 5.7.1 Unable to relay for  
relaytest%antispam-ufrj.pads.ufrj.br@[80.177.41.226]  
Relay test 9

RSET

<<< 250 2.0.0 Resetting

MAIL FROM:

<spamtest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

<<< 250 2.1.0 spamtest@xx OK

RCPT TO:

<"relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx">

<<< 250 2.1.5 "relaytest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"@saturnvisuals.com

As you can see all of the tests failed except test 9. I would be grateful if you could please confirm if this is normal or is the server acting as an open relay.

TIA

Craig