

Exchange 2003 incoming SMTP network level problem

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.connectivity/2004-12/0385.html>

From: Carol Chisholm (*carol.lists_at_smalldomain.ch*)

Date: 12/25/04

Date: Sat, 25 Dec 2004 18:37:32 +0100

This one will probably only be solved with a packet sniffer, but perhaps someone has already solved this one.

A new Exchange 2003 server does not receive SMTP data from certain mail hosts when connected to an ADSL connection.

This same server same server receives the SMTP data from all mail hosts when connected to a cable modem provided by a closely related ISP.

Now for the gory details.

I built a new exchange server and connected it to a firewall and an ADSL modem. It did not get mail from some hosts.

First I changed the ADSL modem. (Zyxel 623ME and a 650R). no progress.

Then I changed the firewall (Sonicwall TZ170). No better

Then I built a new Exchange server. No better.

Then I moved the server to another building. Problem solved. (However the server cannot stay in the other building for ever, I need it back in it's owner's offices).

It works fine with the cable connection, and erratically with the ADSL connection.

The "erratic" means:

- some hosts can send mail to it all the time (notably all other versions of Exchange
- other hosts can't send it mail when sent with software (some Unix hosts)
- these difficult hosts can however always send it SMTP mail when they send "manually" with a user typing in telnet x.x.x.x 25, ehlo....

(Of course this slowed the diagnosis greatly because everyone tests SMTP manually, and it works fine. I have had a hard time getting help from ISPs because they tell me there is nothing wrong with my server.)

microsoft.public.exchange.connectivity: Exchange 2003 incoming SMTP network level problem

In the Exchange SMTP log I see a connection, and EHLO and then *no* DATA, BDAT or any kind of data transfer. Eventually there is a timeout. At the other end the sending host sees a connection, no refusal, no data transfer and then a timeout.

There are no blacklist and no spam filters.

The two ISPs (cable and ASDL) are related and have very similar setups.

The firewalls are the same on both sites (Sonicwall TZ170s). I have swapped the firewall hardware between sites.

The modems are obviously different but both are configured as bridges, and not doing anything clever. I have tried two different models of ADSL modem: both Zyxel, a 623ME and a 650R.

The server is the same, a new HP Proliant.

I'm thinking this is related to the version of sendmail the sending ISPs are using (but no-one will tell me that top secret information) and to a network level problem somewhere. However it is a rather daunting task to diagnose, so I'm looking for help.

Happy Christmas.