

Preventing Third Party Relaying In MS Exchange Server 5.5

Lee Derbyshire

Introduction

Unsolicited Commercial Email, or spam (as it has become more commonly known) seems to be with us to stay, in much the same way as the junk mail that lands on our doormat each morning. Most of the time we happily delete the daily tide of junk email that arrives in our inbox without giving much thought as to where it might have come from, or how it made its way to us. The fact is that each message must have started its brief life on a server somewhere, and unfortunately spammers rarely go to the trouble of providing their own server hardware, preferring instead to use other people's. Quite possibly yours.

It might seem strange that someone else could use your server to send email without even having a mailbox on your server, but there is nothing in the SMTP specification that specifically forbids this. Presumably, in the days when email was first conceived no-one thought it likely that anyone would want to take advantage of someone else's equipment in this way. In this day and age it is quite apparent that they do. In fact an entire industry, based on just this concept, seems to be developing quite rapidly.

So how do you know if it is possible for someone to use your server in this way? Very often the first thing you will know about it is a message from somebody like ORDB, ORBZ or Spamcop arriving in your Administrator Inbox telling you that your server is behaving as an open relay. This could quite possibly mean that someone has received some junk mail and was sufficiently provoked to find out it's source (i.e. your Exchange server) and submit the IP address for testing. Not only is this rather embarrassing, but it could mean that some of your emails will no longer reach the intended recipients, since some organizations refuse to accept emails originating from sources known to be open relays.

Fortunately, you can easily find out for yourself if your server is open to relaying. Then you can do something about it.

Procedure

The first thing you need to do is to find out if it is possible for someone to relay a message through your server. One way of doing this is from a telnet session to your Exchange server on port 25, which is the port used by the SMTP service. If you are testing from an MS Windows computer, type telnet in the Start menu and open a session as shown in figure 1. Of course, you'll need to supply the name of your own server instead of 'SRVR-1'.

Your version of the telnet may well look different to this, but they are all basically the same. It will make things much easier if you make sure that local echo is enabled, otherwise you won't be able to see what you are typing. Do this by selecting the appropriate menu option or (if you are using the CLI version) by typing in `set local_echo`.

Preventing Third Party Relaying In MS Exchange Server 5.5

Lee Derbyshire

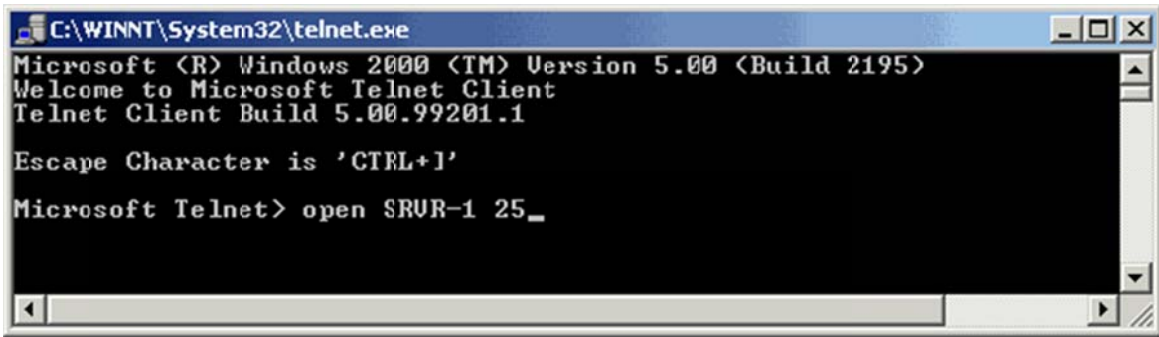


Fig. 1 - Opening a telnet session to your Exchange server.

If the connection is successful, you should see the banner shown on the first few lines of figure 2.

There are only two commands that you need to enter to find out if your server is an open relay. You need to pretend that you want to send a message to a different domain than your own email domain, and that it also *originates* from a different domain. This is done by entering a **mail from:** command followed by a **rcpt to:** command as shown in figure 2.

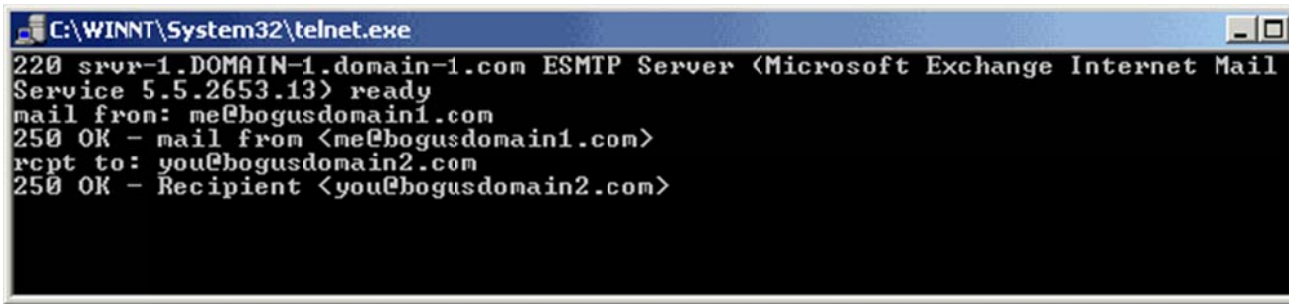


Fig. 2 - The Exchange server accepting the relay attempt.

If you receive the response **550 Relaying is prohibited**, you can breathe a sigh of relief since your server has just told you that it is secured against relaying. Unfortunately, in our example the server responded with **250 OK** which basically means 'go ahead and send as much junk as you like - I don't care'. We'd better do something about it.

The method described here relies on your Exchange server having either Service Pack 3 (or later) installed, or Service Pack 2, with the Post-SP2 Hotfix. If you have not applied the service packs you can only prevent relaying by making some changes to your system registry, and this method will not be described here. It also relies upon your not having deliberately specified IP addresses for relaying.

Close telnet by typing **quit** and start up the Exchange Administrator program. Expand the Directory tree in the left-hand window until you can see the Connections container. Click on the Connections container.

Preventing Third Party Relaying In MS Exchange Server 5.5

Lee Derbyshire

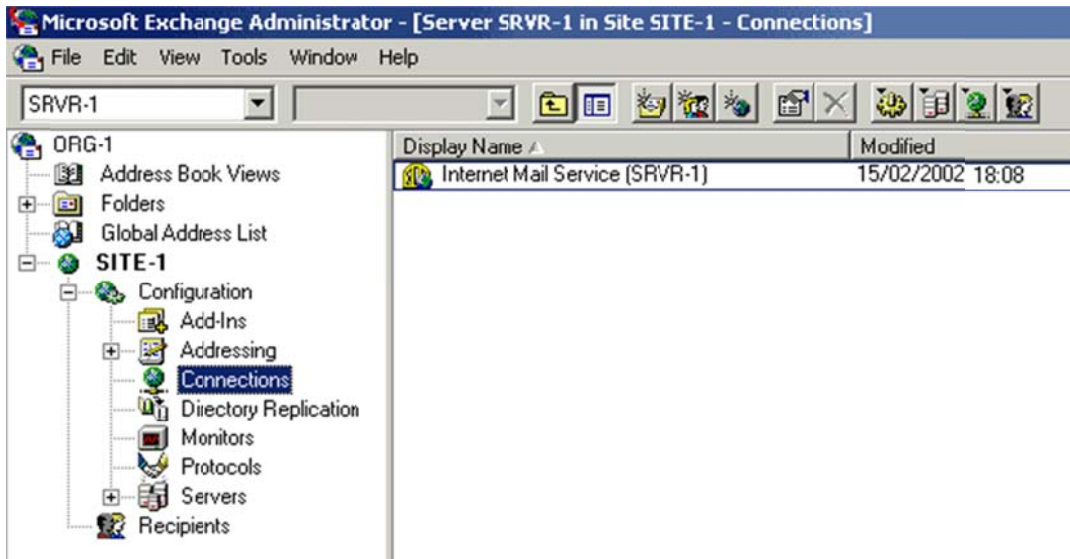


Fig. 3 - The IMC in the Connections container.

Double-click the Internet Mail Connector to open its property pages and then click on the 'Routing' tab to reveal the Routing property page shown in figure 4.



Fig. 4 - The Routing property page of the IMC.

Preventing Third Party Relaying In MS Exchange Server 5.5

Lee Derbyshire

It is quite tempting to select the option labelled 'Do not reroute incoming SMTP mail', since that sounds like what we are trying to do. Unfortunately this option does not work as well as you'd hope, since spammers have found ways of formatting email addresses that can bypass this configuration. What we actually have to do is play a small 'trick' on the IMC. Make sure that the 'Reroute...' option is selected and click on the 'Routing Restrictions...' button to reveal the dialog box shown in figure 5.

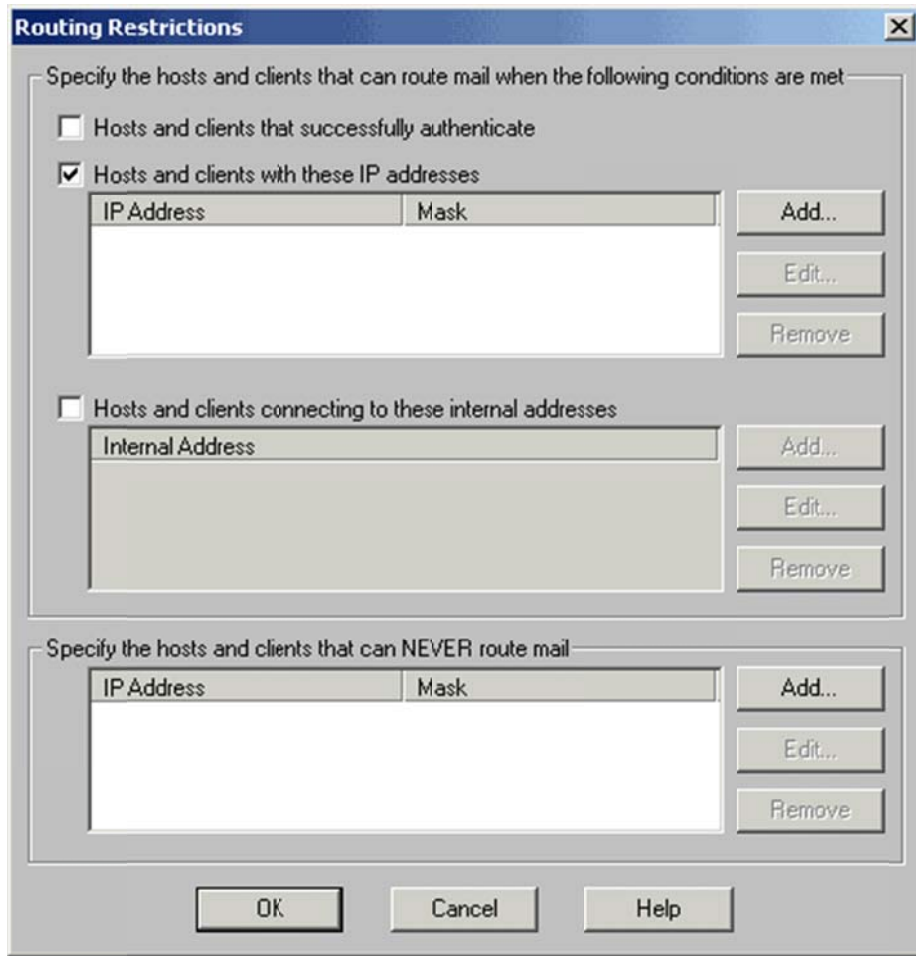


Fig. 5 - The Routing Restrictions property page of the IMC.

The trick that we are going to play on the IMC is this; we select the option labelled 'Hosts and clients with these IP addresses' *but leave the table empty* as shown above. This configuration is not documented, but luckily for us it changes the behaviour of the IMC in the way that we require.

Click the 'OK' buttons to close the IMC property pages altogether. Note that you will need to stop and restart the MS Internet Mail service using the Services applet in the Windows NT Control Panel before the new configuration is activated.

Preventing Third Party Relaying In MS Exchange Server 5.5

Lee Derbyshire

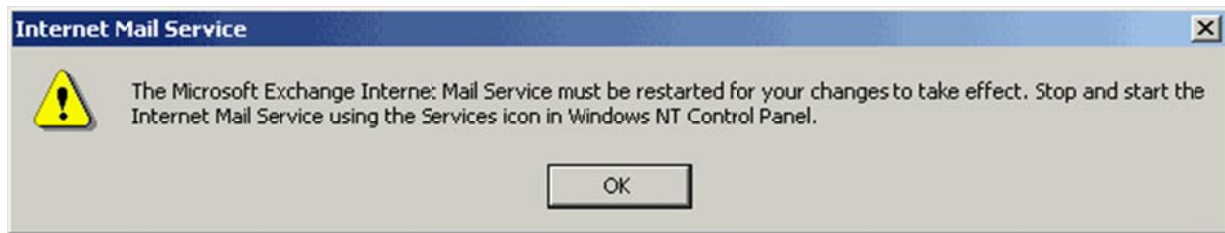


Fig. 6 - The IMC restart warning message.

Having restarted the IMC, we can now use the telnet utility once more to test our new configuration.

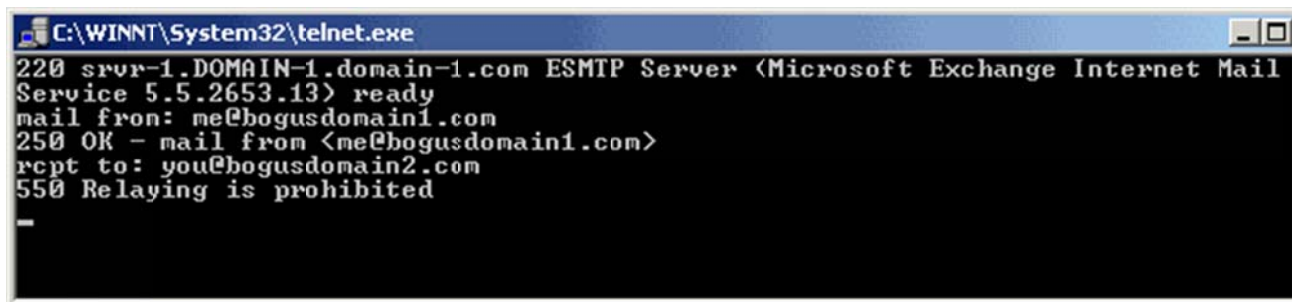


Fig. 7 - The Exchange server rejecting the relay attempt.

Hopefully, this time you will see the response **550 Relaying is prohibited** as shown in figure 7. If so, you can be sure that your server is now secure against third party relaying. Of course, it is a good idea to make sure that you look out for new system vulnerabilities. It is possible that one day the spammers will find a way to circumvent this configuration. They can be very determined.