

# Antirelay Configuration in Microsoft Exchange Server 5.5

Steve Friedl

In the "good old days", mail servers would happily forward mail to anybody who used them, and this was offered as a kind of service to the internet community at large: if your own mail server was having troubles, you could temporarily use your neighbor's mail server to route around it.

No more: those days are long gone.

Dirtball spammers but we repeat ourselves have come to "hijack" mail servers owned by others to do the hard work of delivering their trash, and this has caused enormous problems for the internet. Spammers routinely scan for these "open relays" and abuse them, and eventually this gets the mail server owner either flooded with bounced mail, put on a blacklist, or both. It's much like the bad guy sneaking a box of unstamped mail into your company's mail room: you pay the postage and send out the letters.

Securing a mail server to allow only authorized users to use is important, and this paper describes the process. Modern versions of Exchange (6, and 5.5 with the latest service packs) are not hard to secure, but some common principles are applied to all antirelay provisions.

The idea is that we tell the mail server which remote users are "trusted", and in practice this is the entire internal network. Since no *outside* users could ever connect from these *internal* IP addresses, they are "trusted".

Then, when Exchange receives a connection attempting to deliver mail, it looks at the "trusted" list: those on the list can send mail anywhere, but those not on the list can only deliver to the local machine. Others are told to get lost.

## Securing Microsoft Exchange Server 5.5

Even MS Exchange 5.5 with no service packs applied can be provisioned for antirelay, but this is quite difficult and requires editing the registry. We really, really recommend that you install some recent service packs. First run the Exchange administrator tool, often from the desktop.

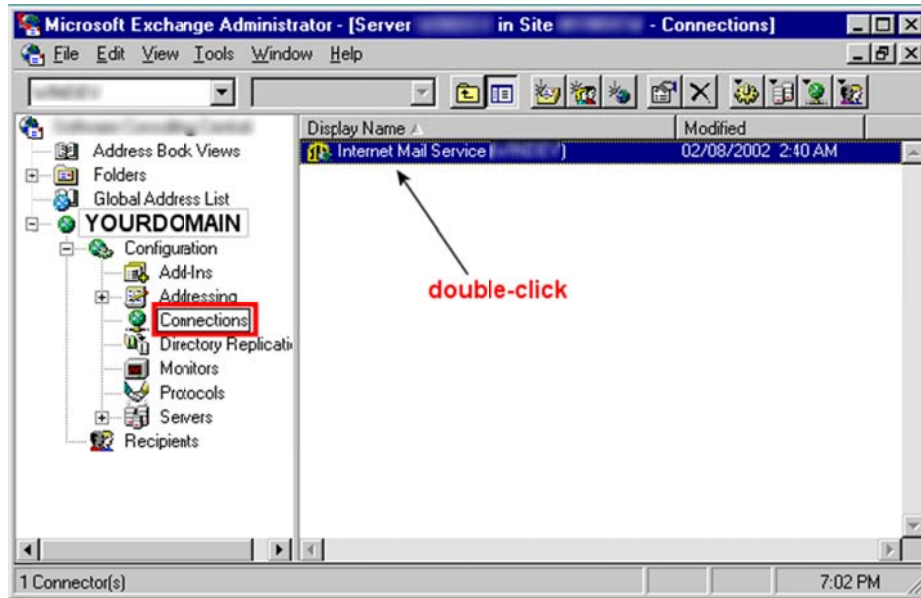


If not on the desktop, select Start -> Programs -> Microsoft Exchange -> Microsoft Exchange Administrator to launch this program.

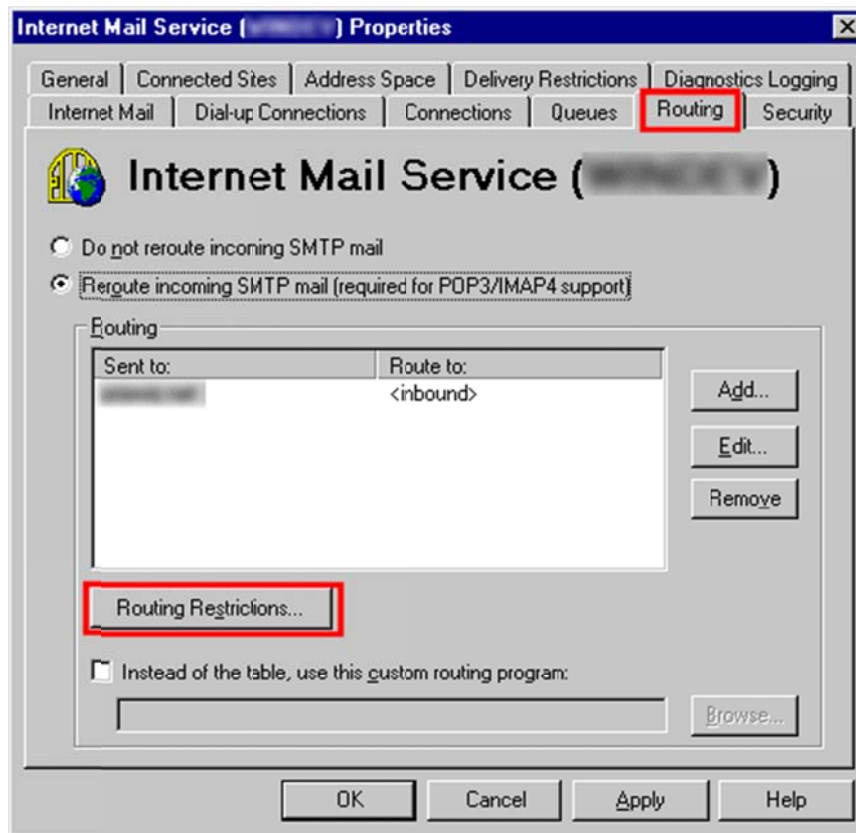
Navigate down the tree to Connections in the Configuration section. Once selected, Internet Mail Service appears in the right-side pane. Double-click this.

# Antirelay Configuration in Microsoft Exchange Server 5.5

Steve Friedl



Click the **Routing** tab and click the **Routing Restrictions...** button:

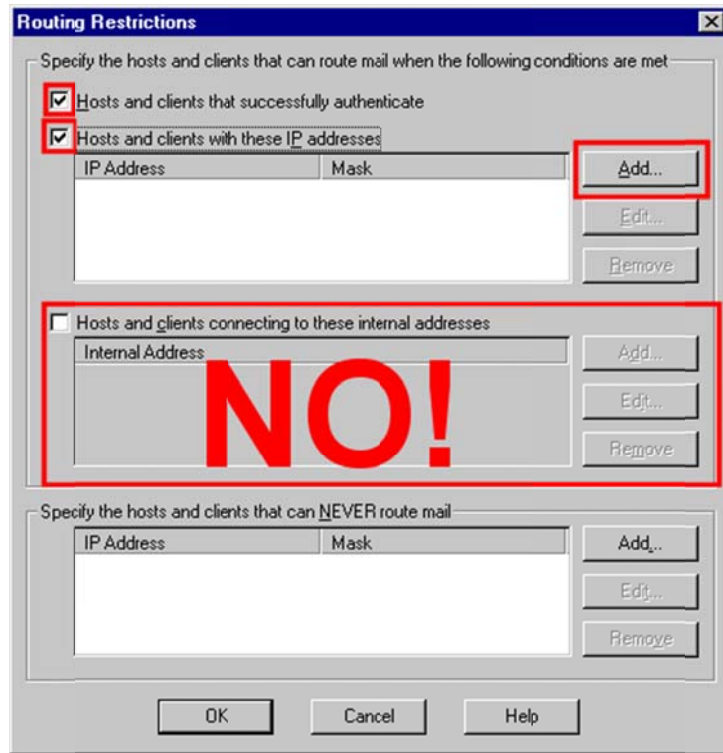


We don't believe there is any harm in allowing **"Hosts and clients that successfully authenticate"**, as this is probably only internal Exchange client users. Also check **"Hosts and**

# Antirelay Configuration in Microsoft Exchange Server 5.5

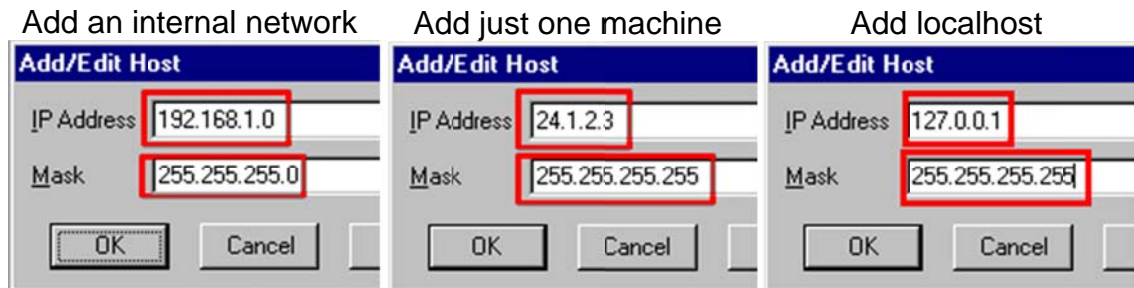
Steve Friedl

clients with these IP addresses", then click the **Add** button to add some hosts. We'll see the details on this in the next section.



**DO NOT** check "Host and clients connecting to these internal addresses", unless you have more than one Ethernet card and one of them is solely connected to the internal network. If you have only one Ethernet card and you check this box, you will relay every piece of trash that gets anywhere near your network.

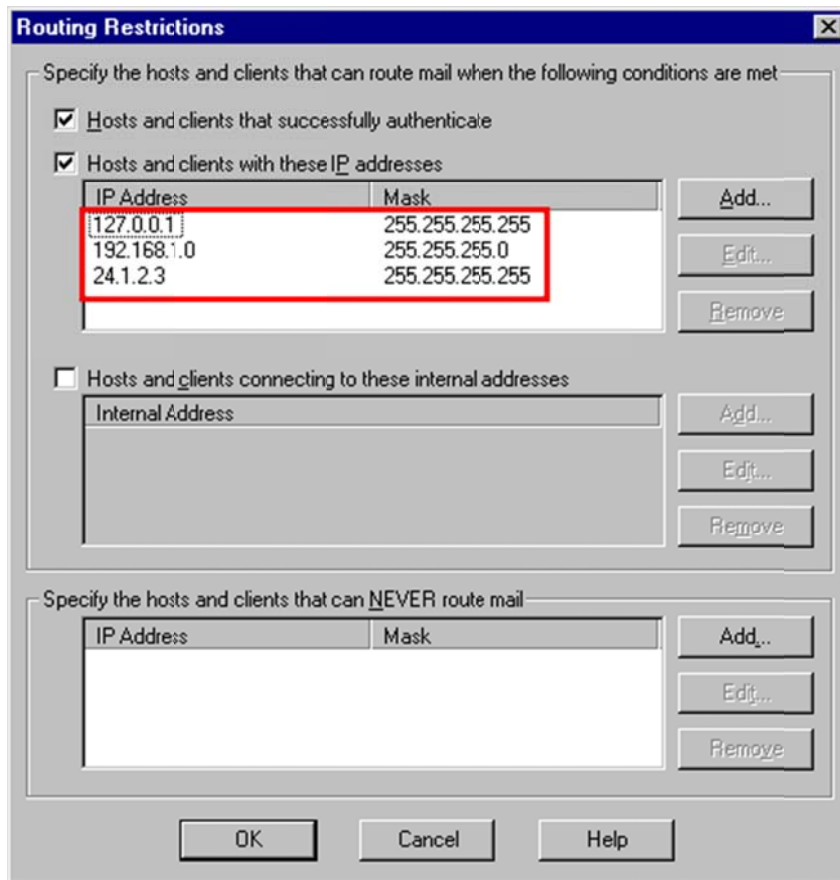
For each "trusted" IP address or range, add it. Add as many as are required, and include all @I[internal] networks, plus any external trusted machines (say, a cable modem user at home). We also have found that it's probably wise to add **localhost** as well.



The resulting dialog box ought to look something like this. Click **OK** to dismiss this and the rest of the dialog boxes.

# Antirelay Configuration in Microsoft Exchange Server 5.5

Steve Friedl



The Internet Mail Service has to be restarted, and there doesn't seem to be a way to do this from the Exchange Administrator. So we must use standard NT administration techniques.

From the lower left, click **Start**, then **Settings**, then **Control Panel**, then double click on **Services**. Scroll the services window until **Microsoft Exchange Internet Mail Service** is visible, then click **Stop** (and confirm if asked). The service takes a moment to stop, then click **Start**.

