

## Re: Exchange question

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-11/0083.html>

---

**From:** Thor (*thor\_at\_hammerofgod.com*)

**Date:** 11/14/03

To: "Tom Burns" <tburns@torcausa.com>, <focus-ms@securityfocus.com>  
Date: Fri, 14 Nov 2003 08:32:25 -0800

>One thing that was brought up is that NDR's can be used to relay (the  
>spammer uses NDR's to forward the message content by using the mail  
>from: email@address.com) I think that we will be seeing more of this  
>type of relaying going on- it sends a message back to the address in the  
>from block.  
>  
>Anyone setup a double SMTP setup in there network? Ie. exchange only  
>receives messages from the 2nd SMTP that is out on the net and the 2nd  
>server relays the message internally from the outside?

I've got a similar setup to what you describe above (with ISA and SMTP filtering thrown in the mix) but that won't keep the NDR's from being sent back. Unless I miss something in your setup... One would basically use smart host delivery for all mail, or depending on the gateway features, DNS for some domains and smarthost for others, but the NDR would go out unless you have an option not to send one.

For exchange, you can turn this off by going into SysMan, Global Settings, Internet Message Formats, select the properties of the default rule, and clear "allow non-delivery reports."

NDR's had a place, but these days, I really question their effectiveness any more. Most don't resolve to a valid email (spam) and even in the case of a spammer using the NDR to deliver the message, the email body is in the form of an EML attachment, which would have to be manually opened. I just turn it off when I can.

That being said, I have not seen a way to turn off NDR's altogether via the standard IIS SMTP service. If anyone has a reg hack for that, it would be great. Since Win2k3 now has a pop3 service (a bit ghetto, but quite functional) it is easy to set up and configure a pretty cool mail solution right out of the box. however, one is only using the SMTP service, and you just can't turn NDR's off (that I know of.)

t

SecurityFocus Microsoft: Re: Exchange question

---

Network with over 10,000 of the brightest minds in information security at the largest, most highly-anticipated industry event of the year. Don't miss RSA Conference 2004! Choose from over 200 class sessions and see demos from more than 250 industry vendors. If your job touches security, you need to be here. Learn more or register at [http://www.securityfocus.com/sponsor/RSA\\_focus-ms\\_031027](http://www.securityfocus.com/sponsor/RSA_focus-ms_031027) and use priority code SF4.

---