

## Re: Secure SMTP virtual server from spam mail

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2007-10/msg00460.html>

---

- *From:* "Elton Seng Yan Thung" <[sengy01@xxxxxxxxxxxxx](mailto:sengy01@xxxxxxxxxxxxx)>
  - *Date:* Thu, 4 Oct 2007 08:41:48 +0800
- 

The ports are SMTP, POP3, IMAP, HTTP and HTTPS. We didn't publish FE as our MX at public but plubish it as web server for mobile users to access OWA. So that is the only reference and we can't affort to remove it.

We really have to stop the spam mail from passing through FE, any wish to get helps from all of you.

thousand thanks

"Betelgeuse" <[betelgeuse@xxxxxxxxxxxxx](mailto:betelgeuse@xxxxxxxxxxxxx)> wrote in message [news:ut3aS9bBIHA.3900@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ut3aS9bBIHA.3900@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

What ports are open on the FE to the world?  
What are you advertising for MX in SMTP? If there is any reference to the FE, I would remove it and see what happens...

"Elton Seng Yan Thung" <[sengy01@xxxxxxxxxxxxx](mailto:sengy01@xxxxxxxxxxxxx)> wrote in message [news:OwTKI8WBIHA.4656@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OwTKI8WBIHA.4656@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

- Our Exchange 2003 system work with the following configuration.
1. Clustered BE at Internal network service all internal users using outlook(mapi),
  2. 2 FE at DMZ works in NLB mode with the following role as RPCover HTTPS, OWA\OMA\PUSH MAIL, SMTP\POP\IMAP4 for mobile users outside the LAN. The FE server is also the Local bridge head.
  3. All incoming and outgoing email to through a smart host for Anti spam and anti virus filtering. The smarthost is a linux with send mail installed. The smarthost is also our public MX server. (We call it linux here)

With the above configuration, we though we are free from spam mail. However we discover recently a lot of spam mail coming via FE server instead of linux. Since the email coming direct to FE, it didn't go through Linux for filtering. We have tried the follow way to block but failed.

## Re: Secure SMTP virtual server from spam mail

1. At SMTP Connector, configure BE and all FE as local bridgeheads. Forward all mail through this connector to Linux. However the incoming mail pass through FE still go to mailbox direct.
2. At FE – protocol – SMTP – Access – relay, we restrict allow relay only list of computers, remove "allow all computers which successful authenticate to relay, regardless of the list above". With this setting, I believe we managed to stop the FE from becoming open relay however it doesn't stop spam mail from pass through it.
3. At FE – Protocol–SMTP– ACCESS–Authentication, We remove anonymous access and grant permission to all mobile users. We believe by doing so we can stop spam mail from passing through FE. However all mobile users are not able to send email from their outlook express (POP3\SMTP\IMAP4).

At the moment, We can't force our mobile users to migrate their mail client to Activesyn or RPCoverHTTPS. Hence we have to maintain SMTP virtual server at FE. We really need to stop the spam mail from passing through our FE otherwise the investment of Anti spam\virus Linux will be failed.

We wish to get some advices from you. Please help.

thanks a lot