

Re: How should I select these options?

Re: How should I select these options?

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2008-07/msg01136.html>

- *From:* John <John@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 20 Jul 2008 14:46:00 -0700
-

Rich,

Thank you!

Basically, I am trying to do is that I want our users to send secured emails to xyz.com. Also, we should be able to receive the secured emails from xyz.com.

What do you recommend on my settings to make this work?

I will check the logs tomorrow due to limited access to the server now.

I really appreciate your effort and time.

"Rich Matheisen [MVP]" wrote:

On Sat, 19 Jul 2008 15:45:00 -0700, John
<John@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Sorry about my confusion. I did install the certificates on the frontend server's default and second secured SMTP server otherwise they can not send emails to us. xyz.com can send emails to me but I still can not send emails to them. I got NDR immediately after I click sending in the outlook from my system administrator,

Okay, then what do you see when you do this?

```
telnet <their-smtp-server> 25
EHLO
```

Re: How should I select these options?

The following recipient(s) cannot be reached:

Partner email address on 7/18/2008 6:38 PM
The recipient could not be processed because it would violate the security policy in force <my.exchangebackendserver.local #5.7.0 smtp;530 5.7.0 Must issue a STARTTLS command first>

And in your front-end server's SMTP protocol log you see what? Do you see a connection from the IP address of your 2nd (TLS) SMTP VS to their SMTP gateway server? What commands were sent and what responses were received?

Then later, I installed the certificates on the backend server's SMTP default SMTP server, but still with no luck. I can not send emails to them.

How many SMTP servers they have is of no concern to you. You only have to know that when you send to their domain that you use TLS (and that it goes to the 2nd VS for delivery). Get rid of those smart hosts in your SMTP Connector (and never put them into the SMTP VS).

should I put each of their MX record IP in the smart hosts for the secured SMTP connector?

Nope. Just their domain name.

you mean on the General tab of second SMTP secure connector, what should I choose a) Forward all mail through this connector to the following smart hosts b) Use DNS to route to each address space on this connector?

You should select "Use DNS . . ." On the "Address Space" tab you should have "xyz.com".

What, exactly, are your requirements? Do you care if xyz.com sends you

Re: How should I select these options?

Re: How should I select these options?

email using TLS? I wouldn't. Leave the responsibility with them to use TLS. All you have to do is make sure you offer the STARTTLS keyword.

If you don't care, then you really don't need two SMTP Virtual Servers. You can secure the connection between your server and their server when /you/ send them mail simply by checking the "TLS encryption" box on the "Advanced Security..." button on the "Advanced" tab of the SMTP Connector.

The link below is overly complicated for what I think you really need. You don't have to use smart hosts to deliver mail to xyz.com. And I don't think you have to be worried if the sender can't control their own security needs by /not/ sending mail to you if your server doesn't offer STARTTLS.

Rich Matheisen
MCSE+I, Exchange MVP