Troubleshooting TLS connections in email

Thursday, October 5th, 2006

So you set up your MS Exchange Server 2003 to use TLS connections for a specific domain[1], and when you try and send email to that domain, it gets stuck in the queue. If you look in the Exchange System Manager, under Queues, you see those emails just sitting there with a status of "retry" and clicking on the affected queue shows "`The remote SMTP service does not support TLS.`"

As you can guess, this happened to me recently. Using Ethereal on the affected server, I did a network packet capture while sending an email from an internal client to the required domain (them.com):

```
220 Mail1.them.com ESMTP

yourserver> EHLO mail.myserver.com

Response: 250-Mail1.them.com
Response: 250-8BITMIME\r\n
Response: 250 SIZE 20971520\r\n
```

You can do the same thing by doing a `telnet mail.them.com 25` to open a manual connection to their mailserver. Once you get the 220, go ahead and type `EHLO yourserver.com` and you will get a list of responses. **The main thing to note is the presence or absence of the line `250 STARTTLS` among the list.**

So you see, because Exchange does not see `STARTTLS` listed, it does not believe the remote SMTP service can handle TLS transactions, so it closes the connection.

This particular case was strange because both of our servers had successfully used TLS connections in the past. Even more strange, I could get the `STARTTLS` response when telnetting from an outside server but not when connecting from our company's mail server. The problem in this case turned out to be the firewall on the other end - they happened to be using IronPort. This firewall checks every incoming IP address and assigns it a score, then uses different policies based on the score. They had neglected to allow TLS in one of these policies and our server's IP address happened to be scored high enough by the firewall to fall into that policy.

[1] http://support.microsoft.com/kb/829721/en-us