Hello,

When connecting using TLS to an unresponsive SMTP server, Net::SMTP can hang until 10 minutes.

The issue is here, we should have a read timeout:

```ruby
def tlsconnect(s)
  verified = false
  s = ssl_socket(s, @ssl_context)
  logging "TLS connection started"
  s.sync_close = true
  s.connect
  if @ssl_context.verify_mode != OpenSSL::SSL::VERIFY_NONE
    s.post_connection_check(@address)
  end
  verified = true
  s
  ensure
    s.close unless verified
end
```

To workaround the issue for the moment I used:

```ruby
module Net
class SMTP
  alias :original_tlsconnect :tlsconnect

  def tlsconnect(s)
    Timeout.timeout(@read_timeout, Net::ReadTimeout) { original_tlsconnect(s) }
  end
end
```

Here the steps to reproduce the bug:

```ruby
smtp = Net::SMTP.new('mail.example.com', 465)
smtp.read_timeout = 3
smtp.enable_tls
smtp.start('localhost.localdomain', 'medecins@example.com', '********') {}
```

Sorry for the credentials I can't provide this publicly, after testing with one failing server you will be able to see that the read timeout is ignored.

By failing server I mean an SMTPS server where you are able to open a connection but you can't read on the socket.

Working case:

```ruby
smtp = Net::SMTP.new('mail.example.com', 465)
smtp.read_timeout = 3
smtp.start('localhost.localdomain', 'medecins@example.com', '********') {}
```

Without TLS it's ok!
If you have any questions, suggestions just ask, if I can help.

Related issues:
Is duplicate of Ruby master - Bug #12678: No way to set a timeout for TLS han... Closed

Revision 87cacf7e - 08/09/2017 08:10 AM - usa (Usaku NAKAMURA)
merge revision(s) 56576,56623: [Backport #12678] [Backport #13429]

* lib/net/smtp.rb (tlsconnect): support timeout for TLS handshake.
  [ruby-core:76893] [Bug #12678]

* lib/net/protocol.rb (ssl_socket_connect): new method to implement
timeout for TLS handshake.

* lib/net/http.rb (connect): use Net::Protocol#ssl_socket_connect.

* test/net/smtp/test_smtp.rb (test_tls_connect, test_tls_connect):
  use Socket.tcp_server_sockets in case localhost is resolved to ::1.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@59533 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 59533 - 08/09/2017 08:10 AM - usa (Usaku NAKAMURA)
merge revision(s) 56576,56623: [Backport #12678] [Backport #13429]

* lib/net/smtp.rb (tlsconnect): support timeout for TLS handshake.
  [ruby-core:76893] [Bug #12678]

* lib/net/protocol.rb (ssl_socket_connect): new method to implement
timeout for TLS handshake.

* lib/net/http.rb (connect): use Net::Protocol#ssl_socket_connect.

* test/net/smtp/test_smtp.rb (test_tls_connect, test_tls_connect):
  use Socket.tcp_server_sockets in case localhost is resolved to ::1.

History
#1 - 05/19/2017 07:37 AM - shugo (Shugo Maeda)
- Is duplicate of Bug #12678: No way to set a timeout for TLS handshake when using Net::SMTP added

#2 - 05/19/2017 07:42 AM - shugo (Shugo Maeda)
- Assignee set to usa (Usaku NAKAMURA)

keysen (Jérémy Carlier) wrote:

  When connecting using TLS to an unresponsive SMTP server, Net::SMTP can hang until 10 minutes.

In Ruby 2.4, open_timeout affects TLS handshake.
I'm not sure whether it should be backported to 2.3.

What do you think, usa-san?

#3 - 07/14/2017 08:34 AM - hsbt (Hiroshi SHIBATA)
- Status changed from Open to Assigned

#4 - 07/18/2017 12:34 PM - usa (Usaku NAKAMURA)
- Status changed from Assigned to Closed
- Backport changed from 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: DONE

Ok, I'll backport this later.

#5 - 08/09/2017 08:19 AM - usa (Usaku NAKAMURA)
- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: DONE to 2.2: UNKNOWN, 2.3: DONE, 2.4: DONE