

RE: what will happen to outbound TLS connection if receiver's cert has expired?

## RE: what will happen to outbound TLS connection if receiver's cert has expired?

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.general/2005-05/msg00275.html>

---

- *From:* [Kenwood@xxxxxxxxxxxxxxxxxxxxxx](mailto:Kenwood@xxxxxxxxxxxxxxxxxxxxxx) (Kenny Wood)
  - *Date:* Sat, 21 May 2005 18:15:17 GMT
- 

Hello Kehboon,

To answer your questions:

1. Not sure, I will have to research if we have a grace period or cache.
2. Not all servers will fail if a certificate is invalid, this is dependant on their configuration.
3. TLS is certificate based (<http://www.faqs.org/rfcs/rfc2246.html>)
4. Turning off certificate validation would partially defeat the purpose of TLS. TLS is not only meant to encrypt the data, but also to be assured that the server you are communicating with is the one you intended to be communicating with. If you turn off certificate validation, how would you know if someone was performing a man in the middle attack on you?
5. You either set TLS on the virtual server or only had ONE connector, Try creating two connectors and giving the TLS connector a higher priority.
6. It should have failed DURING the TLS negotiation.
7. Google.

Thank you for your post.

Kenny Wood  
CISSP, MCSE (+S, +M)  
PSS Security  
Microsoft Corporation  
--

This posting is provided "AS IS" with no warranties, and confers no rights. Use of included script samples are subject to the terms specified at <http://www.microsoft.com/info/copyright.htm>

Note: For the benefit of the community-at-large, all responses to this message are best directed to the newsgroup/thread from which they originated.

RE: what will happen to outbound TLS connection if receiver's cert has expired?

RE: what will happen to outbound TLS connection if receiver's cert has expired?

-----  
| From: "Confused by TLS" <kehboon.lim@xxxxxxxxxxxxxxxx>  
| Newsgroups: microsoft.public.exchange2000.connectivity,microsoft.public.exchange2000.general  
| Subject: what will happen to outbound TLS connection if receiver's cert has expired?  
| Date: 17 May 2005 09:26:03 -0700  
| Organization: <http://groups.google.com>  
| Lines: 54  
| Message-ID: <1116347163.928962.72890@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
| NNTP-Posting-Host: 203.95.78.129  
| Mime-Version: 1.0  
| Content-Type: text/plain; charset="iso-8859-1"  
| X-Trace: posting.google.com 1116347170 14526 127.0.0.1 (17 May 2005 16:26:10 GMT)  
| X-Complaints-To: groups-abuse@xxxxxxxxxxx  
| NNTP-Posting-Date: Tue, 17 May 2005 16:26:10 +0000 (UTC)  
| User-Agent: G2/0.2  
| Complaints-To: groups-abuse@xxxxxxxxxxx  
| Injection-Info: f14g2000cwb.googlegroups.com; posting-host=203.95.78.129;  
| posting-account=H-56vgwAAACrkrMfaSA4hkwZBH5kvUZJ  
| Path:  
TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!newsfeed00.sul.t-online.de!t-online.de!news.glorb.com!post  
f14g2000cwb.googlegroups.com!not-for-mail  
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.exchange2000.general:12649  
microsoft.public.exchange2000.connectivity:3322  
| X-Tomcat-NG: microsoft.public.exchange2000.general

| Hi all

| After the cert used by sendmail (8.12.11 on Redhat Enterprise Linux 3)  
| has expired for 4 hours, all TLS connections from certain servers fail  
| with the following entries in the /var/log/maillog file:

| May 17 21:06:44 mail Receive[15172]: STARTTLS=server, relay=[sender's  
| IP], version=TLSv1/SSLv3, verify=NO, cipher=RC4-MD5, bits=128/128  
| May 17 21:06:45 mail Receive[15172]: j4HD6gGQ015172: [sender's IP] did  
| not issue MAIL/EXPN/VRFY/ETRN during connection to MTA

| Before a cert was created, these exchange servers can send mail to the  
| sendmail through non-TLS session only. After assigning a new cert, the  
| connections from those servers are back to normal.

| The senders are running exchange 2000 & exchange 2003.

| My questions:

- | 1. Why the connections fails four hours later, not immediately.  
| Between the time at which the cert expired and the time at which the  
| first failed connection appeared, there were a lot of successful  
| connections from those servers.
- | 2. Why the expired certs don't affect the TLS connections between the  
| sendmail and other servers, be it inbound TLS or outbound TLS?

RE: what will happen to outbound TLS connection if receiver's cert has expired?

RE: what will happen to outbound TLS connection if receiver's cert has expired?

| 3. How does certs come into the picture of TLS connection?

| My understanding of TLS connection is that cert is not required for  
| TLS.

| 4. Could it be the exchange's configuration issue?

| Is it possible that the exchange servers are configured in such way  
| that it needs certs for TLS connection to work? e.g. for  
| authentication. Is possible for exchange to have outbound TLS  
| connection to sendmail no matter sendmail's cert has expired or not?

| 5. Why the exchange servers didn't fall back to non-TLS connection?

| 6. I guess the connections were dropped by exchange servers after the  
| TLS handshake, not during the TLS handshake. Is it so?

| 7. where and how can I look for more information for troubleshooting?

| The following error message appear in the eventlog of one of the  
| exchange server:

| Source: Schannel

| Event ID: 36871

| Description: A fatal error occurred while creating an SSL server  
| credential.

| Thanks,  
|  
|

- 
- Prev by Date: [\*\*\*Re: Backup\*\*\*](#)
  - Next by Date: [\*\*\*Exchange ActiveSync error\*\*\*](#)
  - Previous by thread: [\*\*\*Recipient groups in GAL\*\*\*](#)
  - Next by thread: [\*\*\*Exchange ActiveSync error\*\*\*](#)
  - Index(es):
    - ◆ [\*\*\*Date\*\*\*](#)
    - ◆ [\*\*\*Thread\*\*\*](#)