Transport Layer Security (TLS)

Frequently Asked Questions (FAQ)

Table of Content

1) Introduction

Most companies actively works to protect the privacy and data integrity of sensitive client information while it is in their possession and control to ensure confidentiality. In the course of providing services, they may exchange information with clients or their authorized representatives that is sensitive and confidential to the recipients.
In order to protect this information when sending via email, they will now encrypt email communication by using a security protocol called Transport Layer Security (TLS) when using Simple email Transfer Protocol (SMTP).

TLS, an acronym for **T**ransport **L**ayer **S**ecurity, is a feature of email servers that encrypts the transmission of electronic mail from one server to another. Sending unencrypted messages increases the risk that messages can be intercepted or altered. TLS security technology is designed to protect confidentiality and data integrity by encrypting email messages between servers and reduces this risk. TLS is an IETF (Internet Engineering Task Force) standard for communicating data securely and also is now supported on most commercial email / SMTP servers.

This guide provides details about TLS: what it is, how it works, why it is important, and how you can install this security protocol on your organization's Internet SMTP Gateway servers.

In total: 6 pages

2) What is Transport Layer Security (TLS)?

1. **What is TLS?**
TLS, an acronym for Transport Layer Security, it can be used as a feature of email servers designed to secure the transmission of electronic email from one server to another using encryption technology. TLS can reduce the risk of eavesdropping, tampering, and message forgery email communications. TLS is a security protocol from the Internet Engineering Task Force (IETF) that is based on the Secure Sockets Layer (SSL) 3.0 protocol developed by Netscape. The TLS protocol is made up of two layers. The TLS record protocol is designed to protect confidentiality by using symmetric data encryption. The TLS handshake protocol allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

2. **Is TLS something new?**
TLS is the successor to Secure Sockets Layer (SSL). SSL and TLS are frameworks that include cryptographic protocols which are intended to provide secure communications on the Internet. TLS is the widely recognized standard issued by the Internet Engineering Task Force (IETF) for securing transmitted data. It is now supported on most commercial email servers.

3. **Who is using TLS?**
Not least a growing number of industrial companies and financial institutions have implemented TLS or will be doing so. The general consensus among industrial companies and financial institutions is that there is a need to protect the information that they exchange via email from eavesdropping or tampering by third parties. Many industrial companies and financial institutions have already implemented TLS or they plan to convert to TLS by year-end 2011.

4. **Who does TLS work?**
When TLS is enabled on the email servers of both the sender and the receiver of the email, information exchanged between the servers is encrypted in a format that encodes plain text and attachments into non-readable form. Internet email servers use Simple email Transfer Protocol (SMTP) to send and receive messages. When sending encrypted messages, the email exchange works as follows:

   - Each company's Internet SMTP gateway is configured to enable TLS communications for SMTP traffic
   - When the sending party (client) connects to the receiving party (server), the sending party checks whether TLS services are offered
   - If the receiver offers TLS services, the sender initiates a TLS handshake. The server sends its TLS certificate to the client
   - If the sender trusts the certificate of the receiver, a TLS session encryption key is negotiated, the TLS session starts, and the SMTP message is transmitted

5. **Why is TLS so important?**
   Sending unencrypted messages increases the risk that messages can be intercepted or altered. TLS security technology automatically encrypts email messages between servers thereby reducing the risk of eavesdropping, interception, and alteration.

6. **What do I need to do to implement TLS on my Internet SMTP server?**
   Contact your internal or external IT technology support staff to find out if your organization has implemented support for TLS. If they have not, request that your IT technology staff implement TLS. Please reference the information regarding installing TLS on the following pages to engage the TLS protocol.

7. **Do I need to contact your company after I implement TLS on my Internet SMTP server to make it work?**
   No. You do not need to coordinate your implementation with our company. After you have enabled TLS on your email server, the server will automatically use TLS when exchanging messages with the company. But please give feedback when TLS is implemented or activated at your end.

8. **What will happen if I do not want to implement TLS?**
   Without TLS, you will still have the ability to receive and send emails with us. If your firm does not implement TLS, your emails exchanged with the company will not be secure, and will continue to use the unencrypted email transport protocols that have been in use. There is risk associated with sending confidential information via email through the Internet. If you choose not to secure or encrypt your emails to the company, we will not accept responsibility or liability for any unauthorized access to, or any loss, misuse or alteration of information exchanged between us.

   Depending on the criticality of the data/documents to exchange we may stop email exchange with your company because confidentiality is not assured via encrypted email data/document exchange. Or we have to find a more complex and expensive method to ensure email encryption.

3) Why Use Transport Layer Security (TLS)?

What are the benefits of using TLS?

Email over TLS provides the following advantages compared to traditional (unencrypted) email:

- Protection. Email servers can be configured to enforce TLS encryption between named parties and confidential information can be exchanged with low risk of eavesdropping or interception to ensure confidentiality.
- Every email sent and received is encrypted. When TLS is enforced, no individual review or decision is required to determine whether or not to encrypt an email based on the criticality of the email's content.
- Email encryption is transparent to both the sender and the receiver. Both parties send and read emails the same way as they do today.
- TLS is globally accepted and currently available on most, if not all, email servers.
- Industry Standard. There is a growing trend among industrial companies and financial institutions to use TLS. These companies and institutions have already implemented TLS or they plan to convert to TLS by year-end 2011.
- Email can be easily inspected for viruses and other malware types. With SMTP over TLS, encryption terminates at partner's email gateways. This means that after messages move inside a company's DMZ firewall, they can be treated just like regular SMTP (email) traffic. Messages can be inspected, scanned and analyzed for malicious content to comply with corporate security policies. This is in sharp contrast to PGP- or S/MIME-style encryption schemes, in which messages are decrypted only at the point of receipt (the end users).
- Reduced cost. When company-to-company encryption over TLS is in place, tactical person-to-person systems (PGP or S/MIME) for encrypting messages are no longer needed. In addition, companies need only create private TLS certificate or purchase TLS certificates for servers, rather than large numbers of enterprise PGP or S/MIME certificates for all clients or all user. There typically is no out-of-pocket cost to implement TLS, although there is some effort to set up and test TLS on the server, as there is no need to purchase any software.
- No overhead for end-users. Because no special software (PGP or S/MIME) is installed on client machines, TLS encryption is "always on" for compliant partners; the process is completely transparent to end users.
- Rapid deployment. Workstations nor Server do require any additional configuration; only the Internet SMTP Gateway Server need to be configured.
- The configuration process is also straightforward. Time to value is measured in days and weeks, not months and years.

4) Installing Transport Layer Security (TLS)

What do I need to do to install TLS on my Internet SMTP Gateway servers?

To implement TLS encryption for SMTP, you will need to:

(1) Generate or renew a TLS certificate for your SMTP Gateway server
Note: These certificates are similar to the SSL certificates used on web servers.

(2) Install the TLS certificate on your SMTP Gateway server

(3) Enable the TLS capability on the SMTP Gateway server

(4) Send test email to the recipient and verify that the test was successful by examining email headers
Note: It is generally advisable to implement and test TLS email services on a test domain (or test host first, before configuring production servers.

Step (1): Generate or Renew TLS/SSL Certificates
In order to encrypt email traffic using TLS, the email server must use a valid certificate. Certificates need to be generated or renewed on a recurring basis, depending on the validity period of the certificates. Most companies specify a validity period of one or two years. The process for obtaining a TLS certificate for use with SMTP is identical to the one used to obtain a web server SSL certificate. Most companies are familiar with how to do this, and generally have their own preferred processes and solutions for doing so, using OpenSSL (create private TLS certificate) or VeriSign for example.
Instructions for using these solutions are straightforward and need not be repeated here. The steps that follow assume you have successfully generated public/private key pairs and obtained a new certificate from your firm's preferred Certificate Authority.
Note: Certificate renewal is extremely important to ensure that email continues to flow normally. If your certificate expires, pending emails may be rejected by some domains. Your firm should have a process in place to ensure that you have sufficient advance warning of impending certificate expirations. Contact your internal technology support staff to find out if your organization has implemented support for TLS. If they have not, request that your technology staff implement TLS.

Step (2): Install the certificate on your Internet SMTP Gateway servers
After you have created a TLS certificate, the email server must be configured to use it for encryption, and for authentication with other domains. If you are operating a Microsoft SMTP server (such as the one provided with Exchange or the Windows server platform), the certificate can generally be imported from the Windows certificate registry into the SMTP server using a GUI interface. On UNIX and Linux based systems, the SMTP applications need to be configured to point to the location of the public/private keys and the certificate, generally from the command line or via a configuration file.
See the instructions for installing TLS certificates for specific SMTP server solutions in your product's documentation or online help material.

Step (3): Enable TLS policy on your Internet SMTP Gateway server
Most TLS encryption services for SMTP servers can be configured to support different classes of email service on an opportunistic or a per-domain basis. For example, policies can ensure that that for particular domains, your TLS-capable SMTP servers will:

a) Always send/receive emails in plain text

b) Use TLS if available, otherwise fall back to plain-text

c) Always use TLS; if not available, refuse email

d) Always use TLS, and verify certificate CN match with the other party's fully-qualified domain name; otherwise, refuse email

   Note: To verify certificate you can't use private certificates.

Not all servers support every option. You should refer to the appropriate documentation for your email gateway software on configuring specific SMTP server solutions to enforce TLS policies.

It is good with us to have previously listed policy b) enabled.

Step (4): Test TLS over SMTP

Once the SMTP server has been configured, you can verify that TLS was used by examining the message header in a message from a domain that has enabled TLS.

The "raw" message header should look similar to the following:

Received: from email.example.edu (IDENT:smmsp@email.example.edu [10.0.0.11]) by example.org (8.12.1/8.12.1) with ESMTP id fBA0M7gU038106 **(using TLSv1/SSLv3 with cipher EDH-RSA-DESCBC3-SHA (168 bits) verified FAIL)** for <user@example.org>; Sun, 9 Dec 2001 16:22:10 -0800 (PST)

Received: from grue.example.edu (sender@grue.example.edu [10.0.0.13])
(authenticated bits=0) by email.example.edu (8.12.1/8.12.1) with ESMTP id fBA0M3rD003797
(version=TLSv1/SSLv3 cipher=RC4-MD5 bits=128 verify=NOT) for <user@example.org>; Sun, 9 Dec 2001 16:22:07 -0800

Sender: sender@example.edu

Message-ID: <3C14002A.FAB442A3@example.edu>

Date: Sun, 09 Dec 2001 16:22:02 -0800

From: Sender <sender@example.edu>

To: user@example.org

Subject: test

5) References

References to TLS Email encryption can be easily found by search in the Internet (e. Wikipedia).