Transport Layer Security (TLS)

Definition: Transport Layer Security (**TLS**) is a protocol that provides security for communication over the Internet. TLS encrypts segments of network connections, in order to provide confidentiality when communicating via the Internet.

How Does TLS Work?

A TLS session begins with a handshake. The client first sends the server a hello message that lists the client's supported capabilities. The server responds back with its own hello message, with its choice of one of the available listed capabilities, to ensure the client and the server will be able to speak the same language.

The server then sends its certificate, which contains its public key, and may request a certificate from the client if client authentication is required. The client checks to see if it's a valid certificate, and sends its own back if necessary.

The client then sends a random number that has been encrypted with the server's public key. After this number is decrypted by the server, the client and server will have a common key that can be used to the send and receive data that only the pair of them can understand. Both the client and server then send messages notifying the other that all further communication will be encrypted and both send final messages that are actually encrypted, ending the handshake and allowing encrypted data exchange to begin.

While this may seem like a lengthy process, a TLS/SSL handshake in most cases takes less than a second.

***Note: In the case of email servers communicating via TLS, both systems are actually servers.**

Does My Organization Need To Use TLS?

Whether you need to use TLS/SSL depends on your organization's activities. For organizations involved in health services or payment processing, using a security protocol such as TLS/SSL to encrypt network communications may be a federal or commercial requirement. For other organizations, using TLS/SSL might simply be a good idea

How TLS Increases Email Security

TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

How To Implement TLS

TLS implementation varies greatly depending on the server it is to be installed on, please see instructions pertaining to your software/hardware vendor. A common step that would apply to all implementations would be to acquire a digital certificate for each server. These certificates may be from a Certificate Authority, or self-signed.

For further information, please view the following links:

http://www.techsoup.org/learningcenter/networks/page11959.cfm

http://www.networkworld.com/newsletters/gwm/0329gw1.html