

TLS versus policy-based S/MIME

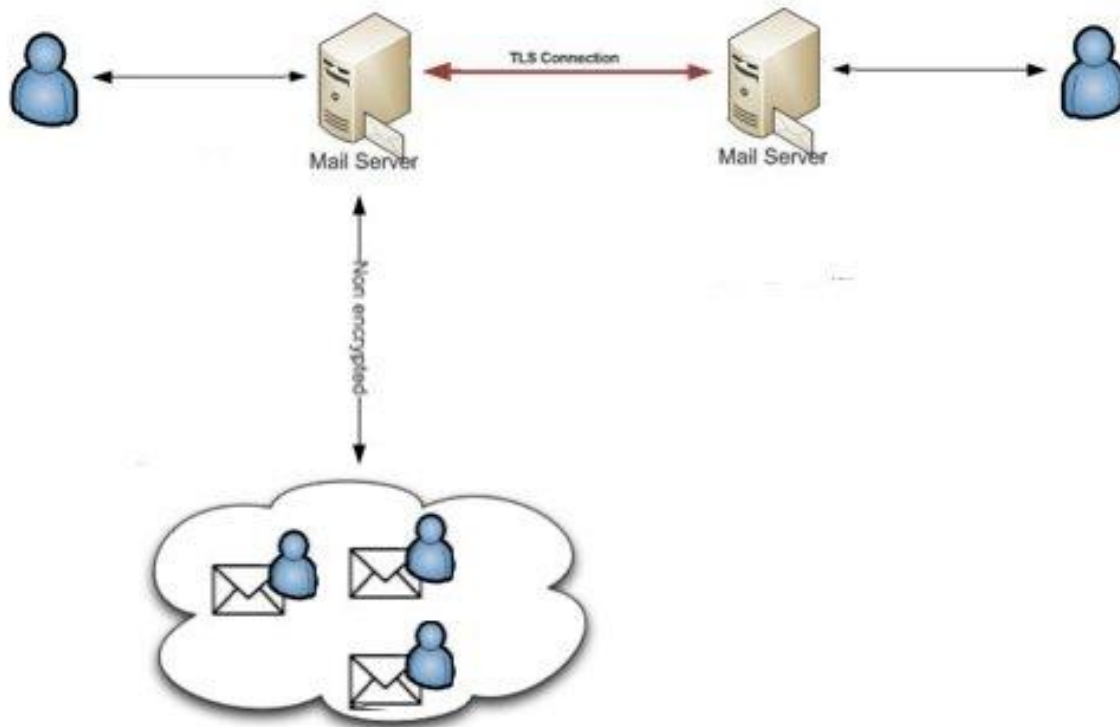
TLS is an effective encryption method when sharing confidential information with a single domain as it is the perfect tool to send confidential information between two enterprises where SSL certificates have been installed on both servers.

S/MIME is an effective encryption method when sharing confidential information outside of the TLS connection and over the Internet to customers, vendors, suppliers and others, that are not situated within the TLS domain.

TLS works well when combined with S/MIME.

How TLS Works

- An SSL certificate is installed on the senders and recipients email server
- A TLS relationship is established between the two servers to allow for encrypted delivery of messages
- Emails sent and received between the two servers are automatically encrypted
- Emails sent to any other address enters the public domain unencrypted



Definitions

TLS (Transport Layer Security) and **SSL** (Secure Socket Layer) are cryptographic protocols that provide secure communications over a network. TLS together with SSL ensure messages that traveling within the TLS are 100% protected.

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption used by Echoworx

Advantages of TLS

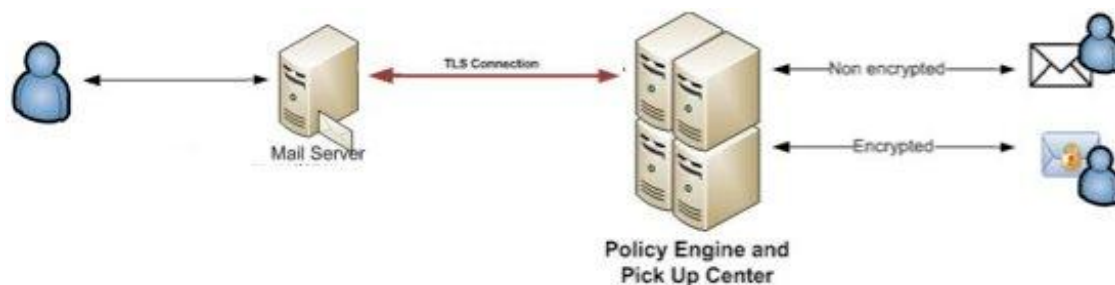
- Allows for seamless encryption between two servers
- No additional software is necessary for the sender or recipient to install
- It is easy to deploy and manage with a partner

Disadvantages of TLS

- Requires a predefined relationship between two servers
- Requires coordination between IT personnel to setup and maintain
- Email to domains without a predefined TLS relationship will remain unencrypted
- To send securely to all partners will require maintenance of several TLS connections
- TLS connections cannot be established with partners without their own email gateway such as Gmail, Hotmail, Yahoo

How Echoworx Policy Based Encryption with S/MIME works

- An SSL certificate is installed on the senders email server
- A TLS relationship is established between the senders email server and Echoworx
- The sender's emails are sent through the TLS connection to the Echoworx policy engine and pickup center
- The policy engine scans the message for confidential information
- If confidential data is found in the email or the attachment, the email is encrypted before it leaves the secure network and travels over the Internet



Advantages of Echoworx Policy Based Encryption

- Quick provisioning, as a single TLS connection is required for deployment
- Encryption is automatic based on policies defined by the organization
- No predefined relationship between the sender and recipient is required
- Delivery can be made to any email address in the world, including mobile devices
- X.509 signatures prove that the emails were sent encrypted for legal reasons
- Administrators can view detailed reports on the nature of confidential information being sent
- The organization defines their own encryption policies in conjunction with their compliance officer
- Recipients will create their encryption key in a onetime registration process
- Messages are removed from the pickup center at predefined intervals