

ZL Unified Archive: Secure Messaging Technology

ZL TECHNOLOGIES, INC.
WHITE PAPER





Table of Contents

ZL Secure Messaging Technology..... 2

1. Overview of ZL System 2

2. Messaging Components.. 2

2.1 Mail Transfer Agent (MTA)..... 3

2.2 Mail Store..... 4

2.3 Listeners 4

 2.3.1 SMTP Listener 4

 2.3.2 SMTP Listener 4

 2.3.3 POP Listener..... 4

2.4 Webmail..... 5

3. Security..... 5

3.1 Staged Delivery and Large File Delivery 8

 3.1.1 The Staged Delivery Processes 9

3.2 Staged Delivery and Large File Delivery 10

3.3 Secure Portal Delivery 12

3.4 Secure Gateway TLS.. 13

Conclusion 14

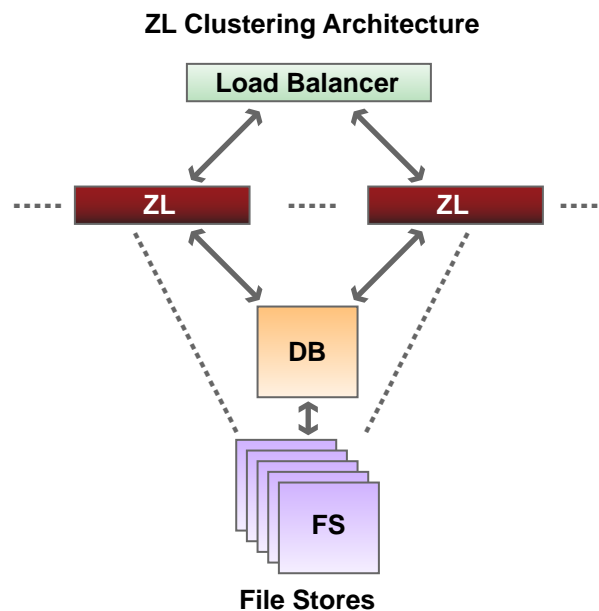
About ZL Technologies.. 14

ZL Secure Messaging Technology

ZL messaging solutions are designed to be highly scalable, reliable and flexible. Particular emphasis is given to security options, providing a broad-spectrum approach for corporate secure communications with multiple types of delivery and levels of security. This document focuses on the security aspects of ZL’s messaging solutions.

1. Overview of ZL System

The ZL messaging software is designed to run with J2EE Application Servers that minimally support Java Servlet and Java Server Pages (JSP). The software itself is written in 100% Java. All persistent information is stored in the Database and File System. ZL Servers can be clustered using a load balancer to provide scalability and transparent fail-over as the simple diagram below illustrates.



2. Messaging Components

Basic ZL Messaging servers are composed of the following main components:

- MTA
- Mail Store
- Listeners: SMTP / POP / IMAP
- Webmail

These components are written in modular fashion and thus one or more components can be easily disabled. This section discusses some of the more salient features and components.



2.1 Mail Transfer Agent (MTA)

The Mail Transfer Agent is built on top of the ZL Coordinator/Executor Architecture. This enables MTA processing to be distributed, and the number of executors controls how many MTA processing units are available in each processing unit. This distributed framework enables the ZL MTA to scale massively.

MTA mail-data and other state data are stored fundamentally in two different ways:

- *Mail-Queue* – Mail to be processed is stored in a file directory. The queue is comprised of 3 directories namely: queue, process, and done. Initially, all mails are kept in the queue directory. When the MTA begins to process, the mail is moved to the process directory. Once the mail is successfully processed, it is moved to the done directory. The advantage is zero database overhead, but the disadvantages include poor error handling and lack of visibility into mails when error occurs.
- *Database* - Mail to be processed is stored in the Database and File System. The actual mail is stored in the Vault (which has a database record pointing to a file on the file system) and additional database records to keep track of mail and recipient states. Advantages include very good exception error handling, excellent monitoring capabilities, but disadvantages include database overhead.

Though, it is possible to use the *Mail-Queue* or the *Database* to handle mails, ZL uses a *Hybrid* scheme whereby the MTA is extremely reliable and serviceable with very little database overhead. The hybrid approach first uses the *Mail-Queue* for all incoming mail. If the mail cannot be processed in the first attempt (e.g. Unable to contact destination SMTP servers), the mail is moved from the *Queue* to the *Database*. Thus the database overhead is incurred only in situations where good visibility or error handling is required.

The MTA processing is extremely flexible due to the ZL MTA Handler Architecture. The type of processing performed is specified in terms of chained-handler. The handling of mails can be defined as 3 steps:

- *Pre-Processing Handler* – (This handler itself can nest multiple handlers). Performed once for the entire mail, this is used to perform operations that are common to all recipients (e.g. Virus Scanning).
- *Recipients Handler* – (This handler typically nests a set of sub-handlers). Processing is done on a per-recipient basis and the handler could be different for different recipients. This enables processing of mail differently for different recipients (e.g., Mail addressed to Internal user may go through SPAM check, Folder Filter Rules and the act of storing the mails. Mail addressed to external users may go through digital signing).



- *Post Processing Handler* – This is done once all recipients in the mail are DONE (with or without errors) and handlers typically perform Post Actions (e.g., Mail done with errors send an undeliverable error Message).

Additional processes can be quickly and easily added as new business or customer requirements are created. Thus, the MTA is very scalable, reliable and flexible.

2.2 Mail Store

ZL Mail Store uses a combination of the Database and File System to provide an extremely scalable, flexible and serviceable mail store. Meta Information of the Mail such as the Subject, From Address, To Address, Sent Date, virtual path of the actual mail, size, etc. are stored in the Database. The actual mail is stored as a Single File on the File System, making the Store resistant to data corruption and flexible enough to store data in multiple formats, geographic locations, or copies based on policy. Also, the stored mails in the file system can be optionally encrypted with provisions to perform Escrow Decryption. More details on the Mail Store can be found from the ZL Mail Server white paper and other technical documents.

2.3 Listeners

ZL servers provide support for a variety of protocols and one or more instances of these protocols may be enabled on the same runtime. Supported Mail Protocols include SMTP, POP3, and IMAP4.

2.3.1 SMTP Listener

The SMTP listener supports SMTP Protocol as defined by RFC 821, 2821. In addition the SMTP listener supports: Message-SIZE RFC 1870, Authenticated SMTP (RFC 2554), Secure SMTP over TLS (RFC 2487). Connection pooling of Sessions enables quick session initialization. Tight integration of SMTP Listener with ZL MTA reduces end-to-end mail processing latency.

2.3.2 SMTP Listener

POP listeners support POP3 protocol as defined by RFC 1939 and RFC 2449 to access user mails in the mail store. In addition Secure POP over TLS (RFC 2595) is supported. As in the SMTP listener, connection pooling and tight integration to the mail store enhances the responsiveness of the POP3 listener.

2.3.3 POP Listener

IMAP listeners support IMAP4 protocol as defined by RFC 2060 and RFC 2177 to access user mails in the mail store. Secure IMAP over TLS (RFC 2595) is supported as well.



2.4 Webmail

Webmail is a web-application built on top of the ZL web infrastructure. Webmail enables users to perform mail activities using a standard browser. Some salient features of Webmail are:

- Ability for a Single Runtime Instance of the Server to Serve multiple UI's to multiple devices in multiple languages based on states such as Domain, Language, Device and Account Type;
- Secure Staged Delivery Based Emails that provides Security, Tracking, Revoking, Expiration and Shredding;
- Server-side SMIME that offers a Client-less Secure Email with Non-Repudiation, Tamper Proofing, and Transport Security;
- Patent Pending Z-Vite Technology that enable sharing of Folders with anyone (that has an email address) with varying privileges (read, delete, create sub folders), timed access;
- ZL Synchronization technology to enable mail stored in Legacy Email systems with secure web and wireless access using standard protocols IMAP and POP3;
- Ability to seamlessly integrate other application such as Calendar, Net Storage, Issues Tracker, Z-Groups or Discussion Groups; and
- Cross Scripting Attack Proof.

3. Security

ZL utilizes non-PKI-based security protocols. Non-PKI-based security solutions feature delivery-to-any recipient methods with zero to limited client footprint on the recipient machine. This includes the following methods:

- Staged Pull Delivery
- Secure Large File Delivery
- JS Push
- Secure Portal, and
- Gateway TLS

These methods use a combination of strong encryption, 128-bit SSL (Secure Socket Layer) for session handling, and a variety of encryption military strength encryption algorithms (including but not limited to AES (FIPS 197), 3DES/DES (FIPS 46-3); FIPS 140-1/FIPS 140-2 Crypto libraries, Blowfish, etc.) for message and file storage. Secure large file delivery is also very useful for overcoming message size restrictions of traditional email systems, enabling delivery of files over 250MBs in size.

Ultimately, hybrid methods that combine two-factor systems, biometrics or smart card interfaces, can be added through ZL's APIs.

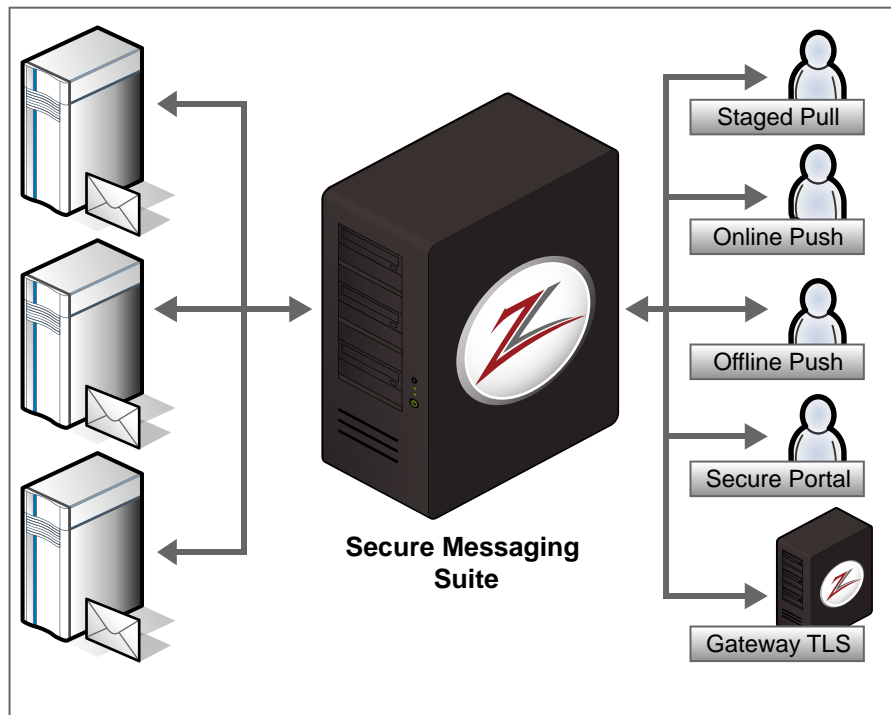


As such, ZL delivers a comprehensive platform of technology that provides a range of solutions for different customers satisfying requirements for:

1. Non-PKI
2. Client-based and Client-less
3. Push delivery and Staged Pull delivery
4. Internal and External recipients

Together, these methods are classified into:

- Staged Pull Delivery
- Large File Delivery
- JS Push (Online Authentication mode or Offline Authentication)
- Secure Portal
- Gateway TLS



ZL Secure Messaging Engine

	Client Free	External/Internal	No PKI Required	Server-side No Desktop
Staged Pull	✓	✓	✓	✓
Online Push	✓	✓	✓	✓
Offline Push	✗	✓	✓	✓
Secure Portal	✓	✓	✓	✓
Gateway TLS	✓	✗	✓	✓



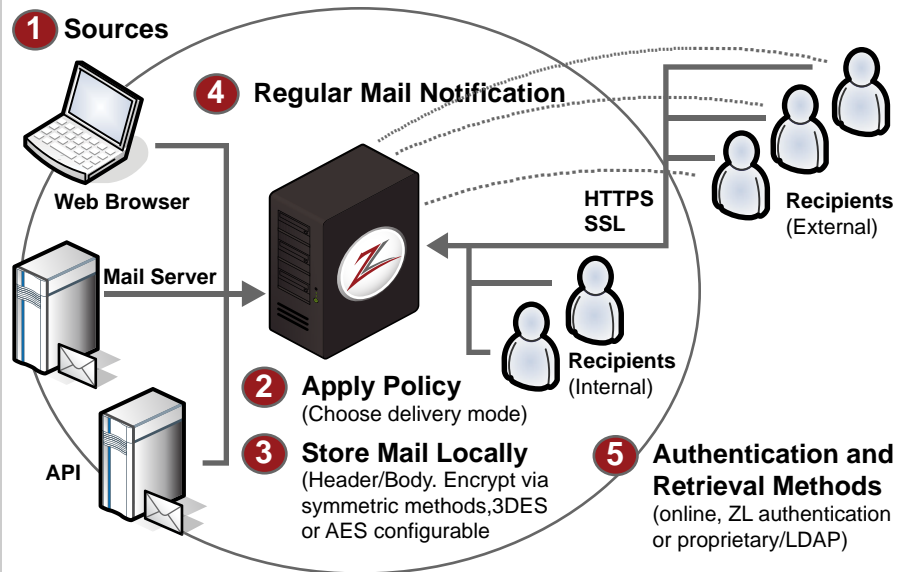
The table below gives a comparison of ZL's full spectrum of secure delivery solutions.

NON-PKI Methods	JS Push (Online/Offline)	Secure Portal	Staged Pull	Large File	Gateway TLS
Simplicity	High	High	High	High	High
Delivery to Any Recipient	Yes	Yes	Yes	Yes	No (other TLS gateways)
Secure Reply (Two-Way)	Yes	Yes (also initiate new)	Yes	Yes	Yes
Security Level	High	High	High	High	High
Client Required	No (Yes for Offline)	No	No	No	No
Attachments	Any	Any	Any	Any (supports > 250MB)	High
Client Certificate	No	No	No	No	No (gateway level certificate)
Sender PKI	No	No	No	No	No
Recipient PKI	No	No	No	No	No
Password	Yes	Yes	Yes	Yes	No
Non-Repudiation	Low	Low	Low	Low	Medium (to gateway level)
Authentication	Low/High	High	High	High	Low
Authorization	Medium	Medium	Medium	Medium	Medium
Audit Trail/ Tracking	Medium	High	High	High	Low
Revocation	No/Yes	Yes	Yes	Yes	No



3.1 Staged Delivery and Large File Delivery

ZL Secure Staged Delivery Process



The ZL Secure Staged Delivery system is a solution whereby a URL linked to a secured message or file is distributed via a notification email to the recipient. ZL's email notification can take the form of simple text, rich HTML, or even multimedia content.

The benefits of Secure Staged Delivery include the ability to send a secure message or document to ANY web-based device irrespective of client and without the need to download or install additional software. This means that a secure email can be sent to any email address in the world on any device, be it PC, PDA, or wireless cellphone. Moreover, Secure Staged Delivery is server-based and enables the sender to track access to the message and even control rights to the message data after the notification has been sent. ZL also provides automatic housekeeping rules to manage the retention of staged messages and files so that the gateway automatically deletes unneeded files on a regular basis.

Access to the actual message is secured via 128-bit SSL and communication between members of the same system is automatically secured. For secure communications to external email addresses, several passive and active methods for ensuring user identity are provided. Passive restrictions are set by corporate policy and include: allowed access only for a particular corporate IP address or domain name or a specific user IP address. Active restrictions include the addition of a challenge question, which requires a passphrase of variable length to open the document. This passphrase can be pre-arranged or can be alluded to by the sender in an optional hint, which only the recipient can understand and decipher.



Passphrases can be set by corporate policy to any length (e.g. 15, 30, 45 characters, etc.). The longer the passphrase, the more secure the symmetric key. Individual passphrases can be set for each message or file if so desired.

On a corporate basis, such as healthcare organizations sending secured messages and files to their members, passphrases can be derived from the current customer database using existing PIN numbers, user account information, etc. so that the recipient and user automatically knows the passphrase utilized. It is important to note that any message or file that is sent between members of the same system using the ZL Data Exchange, is automatically secured at 128-bit SSL without the need for a passphrase. All data can be stored in encrypted form so that even if a firewall or network is breached, the data remains inviolate.

3.1.1 The Staged Delivery Processes

Steps involved in composing an email (Standard/Staged Pull)

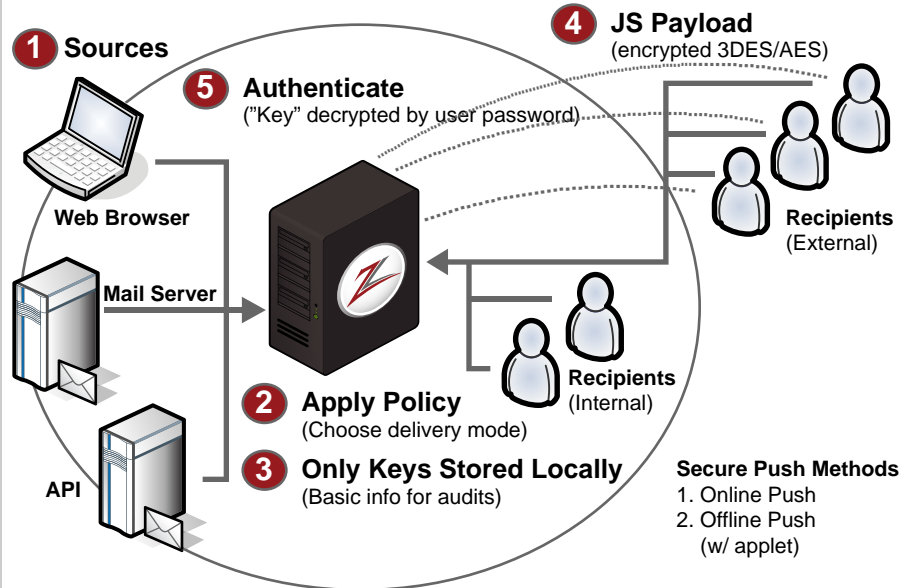
1. Sender logs on to the ZL server over secure socket layer (SSL) using desktop, WAP or other email clients such as Microsoft Outlook etc. Link with Outlook can be through client side plug-in, secure stationery, or server-side content filtering of To, From, Subject, Size, or other customer set parameters.
2. The user composes a message as they normally would with attachments and personal signature, etc.
3. Then if they so wish, they can also add a alphanumeric passphrase currently up to 30 characters in length. This will be the passphrase required by the receiving party to open the message. The message is then encrypted with the hashed value of the password and stored securely on the server.
4. A rich HTML form or plain text notification will reach the recipient. No sensitive data from the message is contained in the notification; therefore no information is exposed on the Internet. The user then types into the web form or page the passphrase requested, and is presented the secure email message and any attachments associated with the email.
5. Additionally, for complete two-way communication between the sender with ZL and the receiver, which may not have ZL technology, ZL provides a Secure Reply mechanism into every mail delivered to a non-ZL email system. This enables the recipient to securely respond back to the sender in a completely secure fashion.

Note: Any communication between two ZL users (e.g. ZL sender(s) and ZL recipient(s)) shall occur securely, end-to-end without the need for password or client software because message traffic is then passing through a closed, encrypted system. This is important to note for groups, businesses, or teams using the same ZL system.



3.2 Staged Delivery and Large File Delivery

ZL Secure Push Delivery Process



The other set of non-PKI based delivery systems are collectively called Push Delivery mechanisms because they push content out to the Internet and to the recipient. ZL provides several mechanisms for Push Delivery and continues to develop alternatives for greater flexibility and function.

The overall benefits of ZL's push delivery systems are that they provide automatic offline viewing. They need not be downloaded or stored because the entire payload is carried within the initial pushed package. Furthermore, authentication of the user is contained in hash form within the payload itself. Therefore, an individual who has POP'd their email into their mail client and is reading or responding to mail offline will have full ability to read the push delivered mail and its attachments.

The first mechanism, termed JS Push, exists in two forms: Offline Authentication Mode and Online Authentication Mode.

Both are 100% web-based and deliver the email message and file attachments as a complete payload, which is stored in the recipient's inbox. Neither require clients of any kind, nor any type of download such as applet or plug-in for receipt and decryption.*

This method is ideal for secure statement deliveries and basic emails. Attachments associated with the message can be any type. To read JS Push messages, users simply need to open the file and type in a simple passphrase.

Offline and Online authentication forms of JS Push are similar in every aspect, except that Online JS Push provides higher security and authenticates the recipient against an authentication list at the time of reading.



The second mechanism, termed JS Push Online and Offline actually pushes the data to the recipient. In the online delivery mode, users should be online so that additional authentication can take place when the email is opened. In the offline delivery mode, which occurs when a user is on an airplane or any other situation that restricts access to the Internet, a one time transparent download of a small agent occurs in the background for the recipient. Once downloaded, the user's system is able to locally decrypt any email file sent in this manner, perform offline reading, and receive any type of attachment.

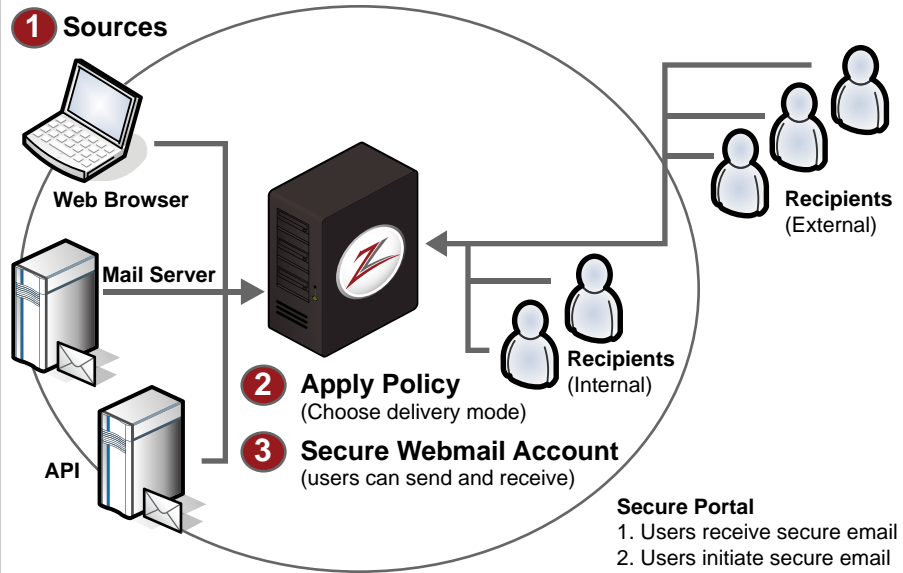
**[Note regarding competing "no download" technology claims: Some competing technologies claim "no downloads" or clients required for their secure messaging systems, yet require Java applets to install or ActiveX to be present to decrypt messages. ZL does not utilize these methods since they do not work with all systems.*

Specifically, Java applets are not supported by all browsers or operating systems and take time to download. For example, a Windows XP recipient would be unable to use Java applets, so any method requiring applets would not automatically work for all Windows XP users. ActiveX is not supported by Unix or Macintosh-based systems. Consequently, these users would not be able to decrypt messages encrypted by such systems.

It is important to specifically and explicitly understand what claims different companies are making, and recognize the limitations of their solutions. ZL focuses on open standard, common technologies. This means standard email client and standard web browser. No additional software is required to support ZL secure messaging.]

3.3 Secure Portal Delivery

ZL Secure Portal Process



- Secure Portal**
1. Users receive secure email
 2. Users initiate secure email
 3. Secure web UI, no client
 4. Users have secure inbox
 5. Branding, look & feel

ZL's third basic method of delivery was designed around web technologies and focused on the need for users to not only be able to reply to secure emails sent to them, but to also enable users to initiate and compose new messages for other individuals. One challenge was providing this type of functionality without the need for installing a desktop client or plug-in.

To accomplish this, ZL developed the Secure Portal solution. The Secure Portal is simply a secure webmail portal, which can be made to have the same look and feel of the existing enterprise portal.

Typically, the solution is used for augmenting an existing customer or partner portal; providing the added functionality of a secure webmail system, and enabling users to initiate new emails to specific recipients within the organization that they have dealings with.

Secure Portal provides a complete Inbox, Sent Items folder, Compose page, and other standard email options. It can be transformed into a closed system, such that users can only send to specific users within the network and not outside the network (e.g. recipients outside the system, for which the bank or company have no relationship).

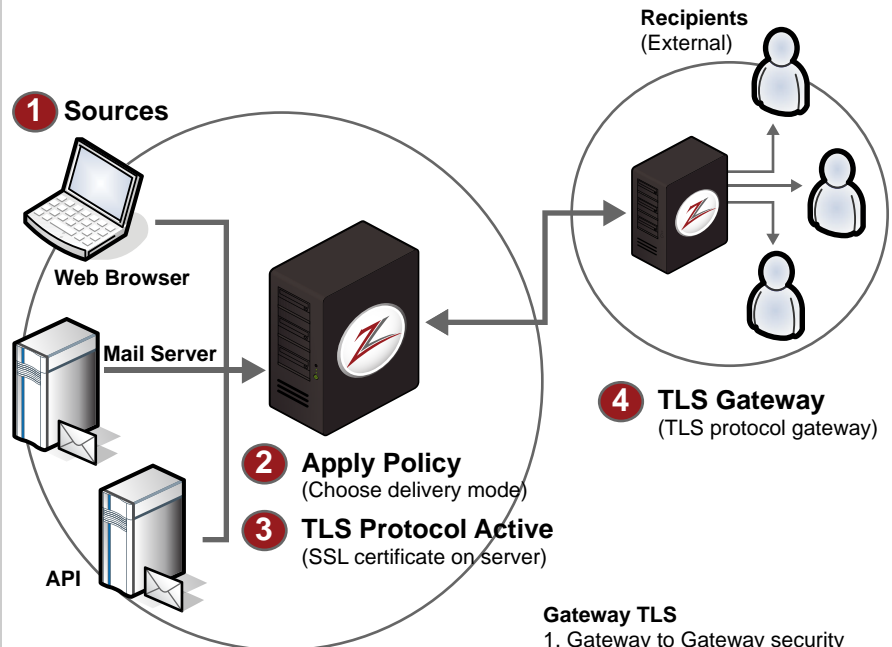
Users can also audit their secure emails, revoke existing mails, and view all secure emails and associated attachments within their Inbox.

Firms may assign an automated purging of the accounts on a regular basis (e.g. 30, 60, 90, 120 days)



3.4 Secure Gateway TLS

ZL Secure Gateway TLS Process



- Gateway TLS**
1. Gateway to Gateway security
 2. No client for either side
 3. Assumes sufficient LAN security

ZL's fourth basic method of delivery, Gateway TLS, protects messages traveling between networks that support TLS (transport layer security) by leveraging the same technology that protects web clients when visiting secure websites.

Not designed for point-to-point security, Gateway TLS delivers effective security around the concept of trusted networks. Firms can communicate via the ZL Gateway TLS server to another TLS gateway ensuring that mail passing between them is encrypted by a secure pipe.

Once inside the network, the mail is delivered via standard protocols in plain text. As such, this is not a technology designed for point-to-point security, but rather securing messages between trusted partners.

TLS is an open standard that is widely available and adopted by many firms. The ZL TLS server will attempt to handshake with external servers to initiate a TLS session if possible. If not, it will send via an alternative methodology or via plain text depending upon the policy.



Conclusion

The ZL Gateway provides a flexible way to conduct secure communications for a wide variety of internal uses as well as external customers, vendors, or partners. Depending upon the particular requirements of the group, one of the four solutions is typically favored and this is decided through business logic and an intelligent server. This flexibility to address a complete range of secure messaging channels is what is required in the demanding requirements of today's IT firms and differentiates the ZL secure messaging solution from the many point solutions in the marketplace.

About ZL Technologies Inc.

Established in 1999, ZL Technologies, Inc. (ZL) provides cutting-edge enterprise software solutions for email archiving, regulatory compliance, litigation support, corporate governance, content management, file archiving, and secure email. ZL's flagship product, the Unified Archive, offers comprehensive email and file archiving and management for companies using Lotus Notes/Domino, Microsoft Exchange, Bloomberg, and others. The suite provides a highly flexible framework that is fully scalable, enabling organizations of all sizes to meet legal discovery, compliance, and storage management requirements. With a proven track record and an impressive list of clients, including Walgreens, Bank of New York Mellon, Pacific Life, and Morgan Keegan, among other top global institutions, ZL has emerged as the premier provider of email archiving and compliance solutions. For more information, please visit www.ZLTI.com