

A New Standard in Encrypted Email

A discussion on push, pull and
transparent delivery

By ZixCorp

November 2010

Email enhances our daily business life. It enables efficient, real-time communication, unites businesses through a ubiquitous platform and improves collaboration with colleagues and business partners. Email continues to dominate business communication with more than 883 million workers worldwide using email for business.

According to a May 2010 Osterman Research survey, the typical business user spends 146 minutes, or 30 percent, of an eight-hour day on email. This time is greater than the combined time spent on the telephone (54 minutes), instant messaging (23 minutes) or social media (18 minutes). Email will remain the primary means of communication in business for many years, with the number of emails sent and received projected to only increase from 133 to 160 messages sent and received daily, according to a 2009 Wall Street Research Report.

As email is leveraged to communicate, collaborate and exchange sensitive information, business users need to be aware and understand the risks of unsecure email.

Email: Inherently insecure

The transmission of a message in an unencrypted email is often times compared to the delivery of a message on a postcard. In fact, the email may produce greater exposure than the postcard due to the methodology used to deliver an email message. The action of sending an email involves storing of the message on several servers; often times the server maintains a cached copy for some period of time. IT staff have an opportunity to obtain the message through traffic monitors or packet sniffers as the messages traverse their machines or as it's copied to the server.

Breaches on the rise

In addition, we all read stories or headlines about the volume of data breaches rising; we hear about the damage those breaches can inflict and the costs associated with remediation. A recent Ponemon Institute report listed the cost of a single data breach as \$6.75 million.

When you blend increased threats with an ever increasing use of email then the decision to encrypt email becomes obvious. ZixCorp understands this fact; we've helped thousands of organizations in their efforts to manage risk and secure their email traffic. Whether your organization is concerned about email privacy because of the need to maintain customer trust or the need to avoid regulatory fines and lawsuits, it is important for you to understand the different methods of securing email communications. This paper examines the different methods of encrypting email communication with an emphasis on the need for transparent email encryption.

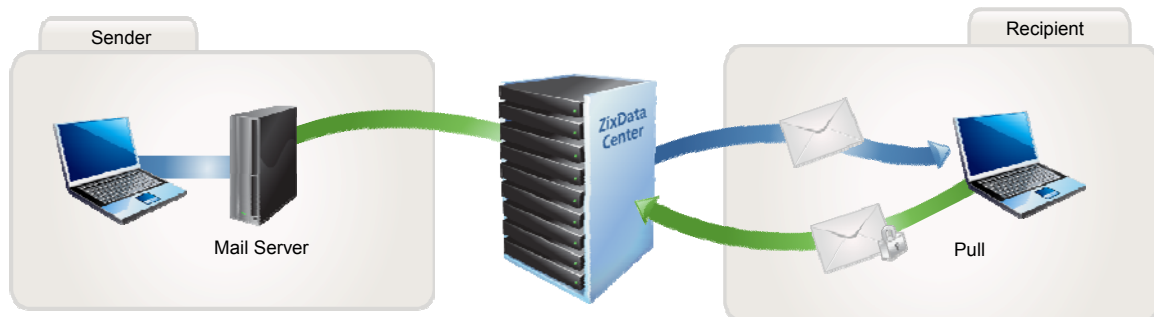
Approaches to email encryption delivery

It's important to understand which mechanisms are available for delivering encrypted email to the intended recipient. Different types of recipients will have different preferences regarding how they receive secure email messages, and the solution you chose should meet the needs of your email recipients. Conventional email encryption solutions are focused on the sender; the typical means of sending an encrypted message involve desktop to desktop or “push” delivery; secure portal or “pull” delivery; or training users to trigger encryption through use of a keyword or phrase in the subject line.

Push versus Pull

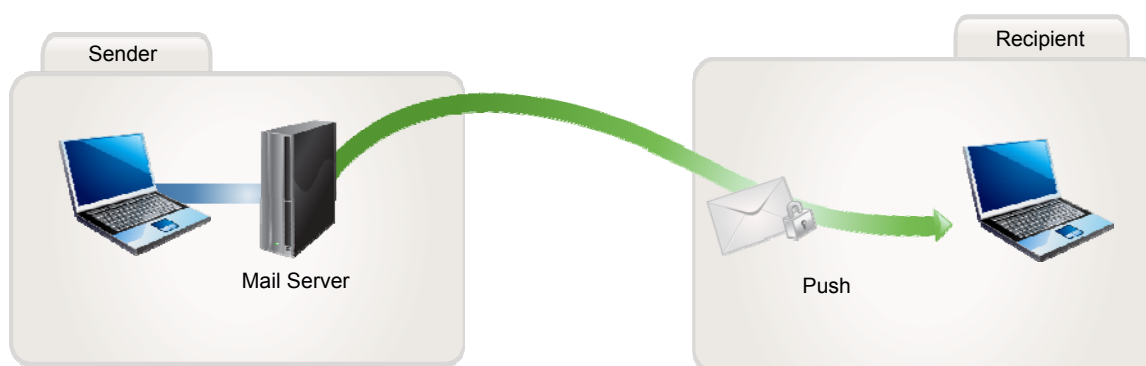
In the world of email encryption, push and pull are industry terms that refer to the different technologies used for delivering encrypted email to users who do not have email encryption capabilities. Pull refers to the concept of a secure portal where users can pull encrypted email from a secure Web site. The pull method can also be thought of as pulling users back to a Web portal.

Pull Method



With pull technology, the secure portal provides a way to deliver the encrypted message to users without requiring users to install any client software. Users receive a notification message with a link to the secure portal. When users click on the link, they are taken to the portal, where they are authenticated (typically with a password), and the messages are decrypted and presented to them via their Web browsers. Most secure portals allow users to download attachments and reply to or forward the message. Some secure portals will also allow users to compose or originate new messages, thus providing full two-way secure communication. In addition, most secure portals can be branded to match the company's Web site, although some require considerable work on the part of the customer.

Push Method



Push refers to the ability to push the encrypted email directly to user email inboxes. Similar to the pull technology, push does not require users to install any client software to read the encrypted message. In this model, users receive an email message with an attachment. The attachment is an HTML file that contains the encrypted message. When users double click on the attachment, it launches their Web browsers where they are authenticated (typically with a password) and the message is displayed. From there, users can save attachments, as well as reply to and forward the message. In addition, most solutions provide the capability to add branding to the email.

The pull approach is ideal when organizations already have a portal that provides a variety of services and secure communications can be added as one of these services. The push approach is ideal for organizations that want to have secure messages delivered to users just like any other email message. Both push and pull provide companies with a way to send email securely to users who do not have an encryption solution.

While these methodologies may prove valuable in certain circumstances, the methodology that's least disruptive is known as transparent email encryption.

Transparent Email Encryption

What is transparent email encryption?

trans·par·ent: (of a process) operating in such a way as to not be perceived by users.

Transparent email encryption from ZixCorp embeds security while maximizing convenience for both sender and receiver. Conventional email encryption solutions often introduce an added burden on receivers, requiring additional user authentication. ZixCorp designed its solution to alleviate the receiver's burden, by delivering encrypted email automatically and transparently.

ZixCorp delivers fully transparent delivery to *ZixGateway*TM customers who send email to other ZixGateway customers. By fully transparent, we mean the sender simply sends his/her message; it is automatically scanned by the ZixGateway appliance, encrypted and sent. The receiver's ZixGateway appliance scans the inbound message, decrypts and delivers to the recipient's inbox. The sender and receiver enjoy the benefit of encrypted email delivery without any extra actions. The only means of knowing the message was sent securely is a simple footer at the bottom of the message.

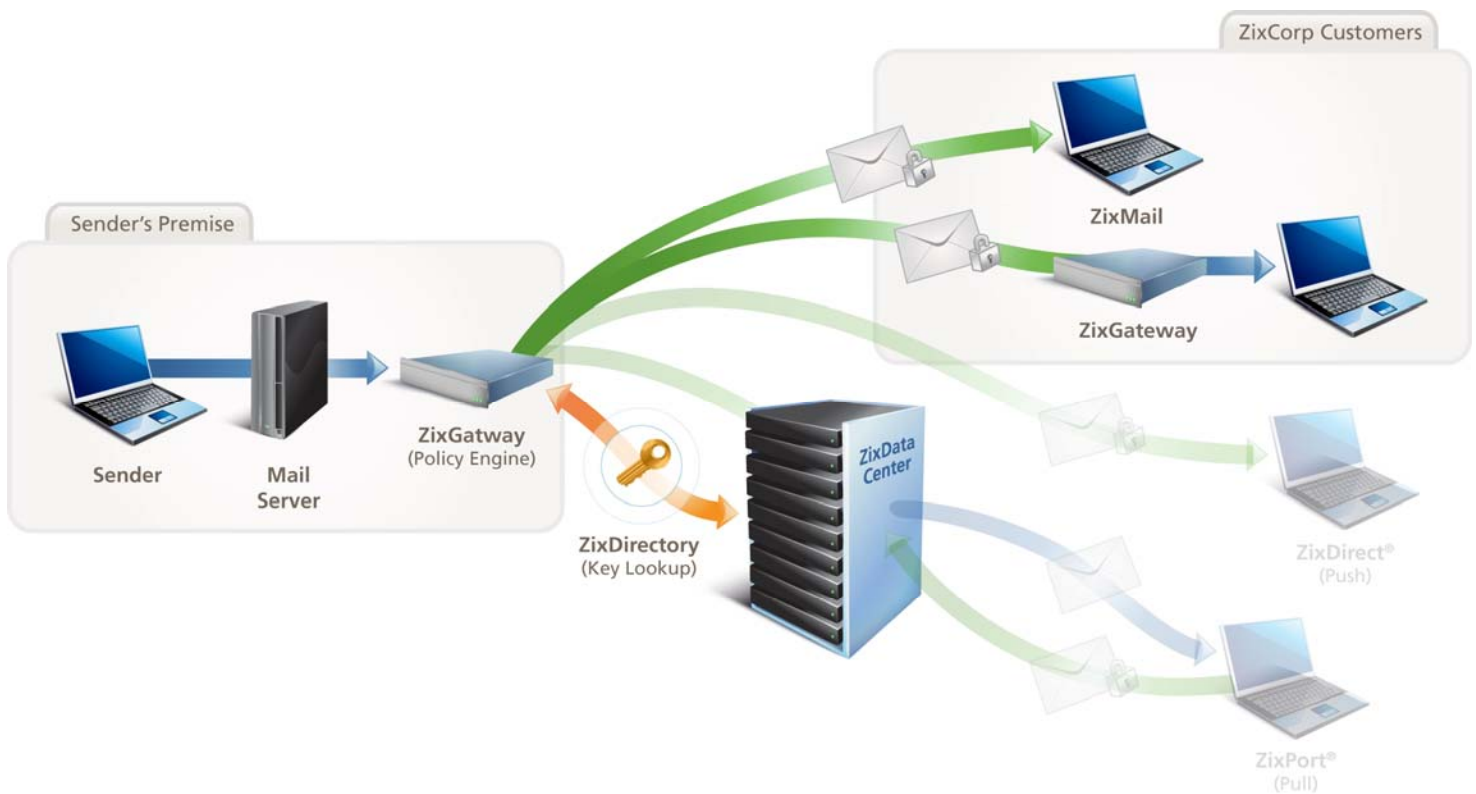
A critical component of delivering this capability is effective encryption key management. ZixCorp's method of simplifying key management is through use of the *ZixDirectory*SM, our key management solution in the cloud.

Key management: Simplified through ZixDirectory

An email encryption solution can be difficult to setup and maintain, because it requires the exchange and maintenance of encryption keys and digital certificates for each organization or user. Over time, as certificates expire, the encrypted email connection can fail and cause mission critical email to be dropped or sent in the clear, neither of which is desirable.

The advantage of *ZixCorp*[®] Email Encryption Services is the centralized key server, called ZixDirectory. ZixDirectory is the largest email encryption directory in the world, enabling seamless secure communication among its millions of members, including many of the nation's most influential institutions. Each ZixCorp customer has a public key that is hosted in the directory, and each customer has access to the public keys of all other customers. When communicating with other ZixCorp customers, email encryption is completely automatic and transparent. Whereas most public key infrastructure (PKI) systems work fine within the confines of a single corporation, they do nothing to aid in key exchange between organizations. The ZixDirectory is the only directory which enables key exchange between organizations; it is a continually available, highly secure encryption and signing key broker. It provides global key distribution as a low-cost service.

How does it work?



ZixCorp installs ZixGateway at the perimeter of an enterprise. The enterprise administrator uses ZixCorp's policy manager and pre-defined Lexicons to create his/her own encryption policies.

ZixGateway has several modes of delivery which are triggered by an organization's encryption policy. The ZixGateway protocol is a secure gateway-to-gateway protocol. If the sending ZixGateway server determines that the recipient of the email message is also served by a ZixGateway, then the message is encrypted using the recipient ZixGateway server's public key, signed-on *on behalf of* the original sender and addressed with *attention-to* the recipient. The unique capability of ZixGateway to digitally sign messages *on-behalf-of* and with *attention-to* ensures that though the ZixGateway solution is transparent to the end-user, it still uses full strength public key cryptography.

As the last mail transfer agent (MTA) to handle outgoing email and the first to handle incoming email, ZixGateway is far-removed from the end-user's awareness. In fact, it has little impact on any of your current email technologies. ZixGateway has no effect on your choice of email client, mail servers, virus checkers or content filters. The only step needed is to reconfigure your email pipeline to include ZixGateway as the segment of the pipeline immediately adjacent to the network perimeter. Email flows unimpeded and unaltered through your trusted intranet e.g., your

mail servers and virus checkers. Only when it nears the network perimeter does it pass through the ZixGateway appliance and become encrypted.

The Benefits of Automation/Transparency

Like any security policy or technology, email encryption is only beneficial when executed correctly. If users are not applying email encryption appropriately, then the security benefits are not maximized and the potential of a breach rises.

With automatic scanning and encryption capabilities, gateways leverage email encryption for optimal security and:

- Relieve user burden of knowing when and what to encrypt
- Eliminate human error
- Remove the need for training users on updated policies based on new regulations or company preferences
- Alleviate the stress of unintentional internal threats

As a result, gateways are the preferred method of email encryption for senders. Similarly, transparency will become the preferred method of email encryption for recipients.

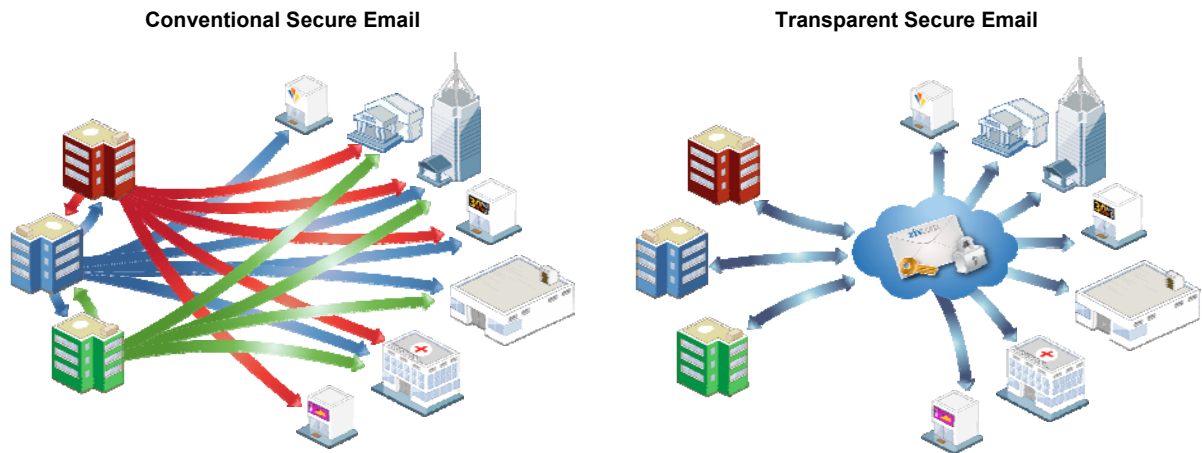
Designed with your most important relationships in mind, ZixCorp transparent email encryption sets a new standard for simplicity and ease of use. Other solutions require users to authenticate upon receipt of a message. This may seem like a small point, but it rapidly becomes an issue when you consider the amount of daily email received by the average user and the number of senders delivering messages.

Hundreds of emails sent by multiple senders mean multiple new passwords. When thinking about the multiple passwords you use daily for your business and personal life, the number quickly stacks up, due to:

- computer and desktop encryption log-ins
- social media passwords
- online banking
- online bill pay for your mortgage, car, insurance, electricity and cable
- online newspapers and magazines

How much time is wasted trying to remember which password applies to which log-in? How much time is wasted waiting for email reminders or temporary passwords? How frustrating can the delay and interruption become? And, using fewer passwords only jeopardizes the strength of your secure information and email encryption.

The Result



Transparent email encryption is the only solution that maximizes the strength of email encryption and enhances the recipient experience by eliminating email encryption passwords and saving time and frustration. ZixCorp Email Encryption Services automatically provide transparent email encryption between ZixCorp customers and offers the flexibility to choose between push or pull for all other recipients.