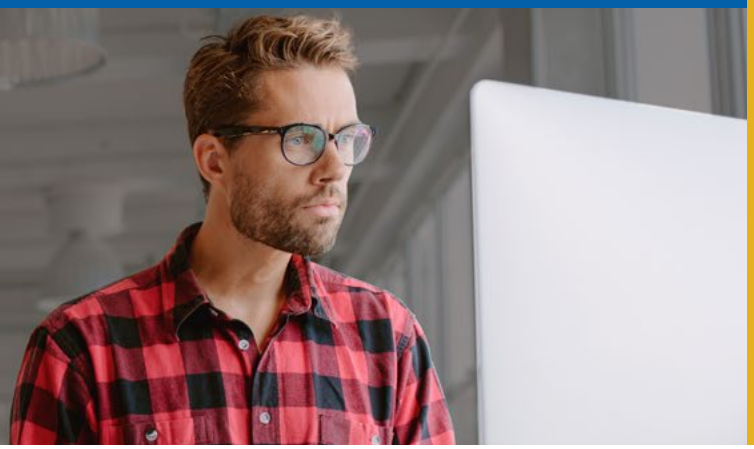
zix

Superior TLS through ZixGateway®

Overcoming TLS Limitations & Enhancing Email Security



Who uses Zix?

14,500+ customers including:

- All Federal Financial Institutions Examination Council (FFIEC) regulators
- The U.S. Securities and Exchange Commission (SEC)
- 30% of U.S. banks
- 1,200+ U.S. hospitals
- 30+ Blue Cross Blue Shield (BCBS) organizations

Benefits:

- Appropriately enables TLS securely and reliably
- Enables secure, bi-directional delivery
- Mitigates MITM attack opportunities of TLS

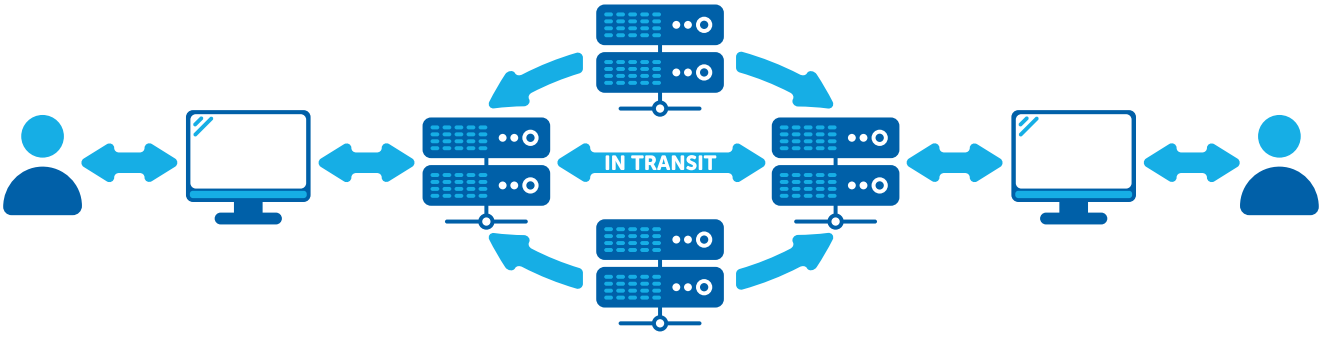
Features:

- Policy management of TLS
- Integration of TLS into Best Method of Delivery
- Message-level and transport-level encryption
- Certificate authentication and encryption level settings

Email exchange is the essence of business communications enabling efficient, real-time exchange of information. Protecting sensitive data from the time the sender presses "Send" to the display of email contents on the recipient's device requires a comprehensive approach to safeguard against the inherent vulnerabilities of basic email exchange. As an alternative to secure message-level encryption, some organizations attempt to reduce the risks of unsecure email by implementing Transport Layer Security (TLS) for protecting email while in-transit, often without realizing TLS does not guarantee secure bi-directional email exchange and can be vulnerable to Man-in-the-Middle (MITM) attacks.

Zix's superior TLS enables you to integrate TLS directly into ZixGateway® and the Zix Best Method of Delivery℠ (BMOD) as an optional delivery method within your policy controls. You can identify that sending via TLS is appropriate by policy, specifying required certificate authentication and encryption levels mitigating MITM attack opportunities that could compromise the security of sensitive email contents.

No other solution can provide the security, simplicity, control, transparency, visibility and branding that is delivered through Zix.



Understanding TLS Limitations

A successfully negotiated TLS session provides an encrypted tunnel for protecting the email while in transit between two mail servers. TLS is frequently described as "best effort" or "opportunistic." If TLS is not available or cannot be successfully negotiated for some reason, the session "fails open" and the email is sent in the clear, making it vulnerable to eavesdroppers. Some mail servers attempt to implement safeguards by requiring TLS be successfully established, thus mandating TLS, or email delivery fails resulting in bounced email.

Mandating or forcing TLS with certificate validation and strong encryption is the safer TLS method but requires that both parties agree on the level of authentication and encryption and that TLS be set-up correctly on both mail servers to ensure a successful handshake, authentication and secure email delivery. Manual effort to set-up bidirectional TLS with every domain and the associated on-going maintenance can be costly and for most organizations is an option reserved only for key customers and partners.

When depending on TLS, additional security considerations include:

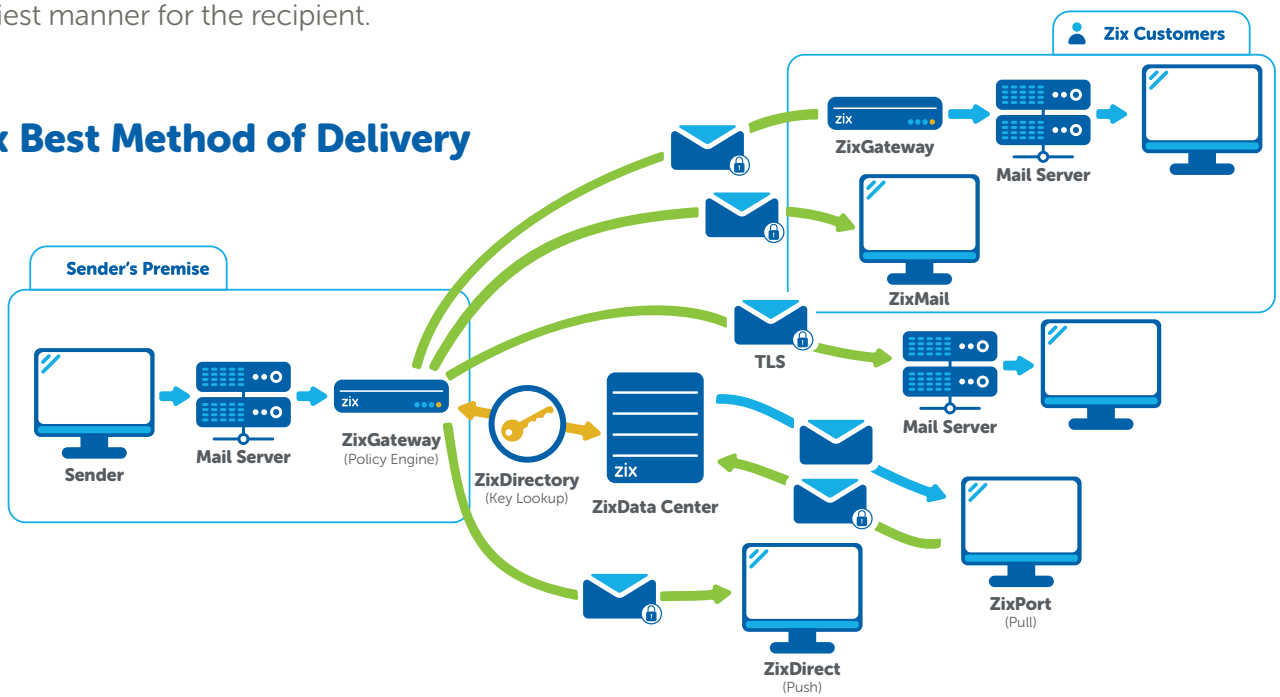
- No guarantee that messages are sent securely
- No guarantee of secure reply messages
- No failover to another secure transfer method when TLS is not available
- No reporting in support of auditing for compliance and/or awareness
- No reporting capabilities that email did or did not transfer securely

With Zix, you get a solution that appropriately enables TLS securely and reliably to meet your secure communication business requirements, while allowing you to overcome these limitations.

A Superior Solution

Zix delivers superior support for TLS by integrating it directly into ZixGateway encryption policies, enabling the addition of TLS as a secure delivery option with specific certificate authentication and encryption level requirements. When an email is sent, the message is scanned for sensitive content with the robust and customizable content filters available in ZixGateway. When security is required, the Zix Best Method of Delivery ensures that email messages containing private or sensitive information are delivered in the most secure, easiest manner for the recipient.

Zix Best Method of Delivery



By integrating TLS into ZixGateway encryption policies and the Zix Best Method of Delivery, you benefit from these exclusive features:

Secure, bidirectional delivery – The Zix Best Method of Delivery allows you to select delivery methods that support bi-directional security, when required, choosing the most secure and transparent delivery method available for each message. Zix S/MIME provides secure message-level delivery and bidirectional transparency, enabling the decryption of the message at the gateway and delivering it to the recipient without need for a password or extra steps. When TLS encryption option is indicated and can be successfully established with receiving mail server, the email can be delivered securely through TLS delivery. Other Zix Best Method of Delivery options that include secure bidirectional delivery are ZixMail®, ZixPort® and ZixDirect™.

Simple configuration and maintenance – By making TLS a part of the ZixGateway policies, TLS can be added as a delivery method by simply checking a box. By replacing the need for individual TLS configurations, ZixGateway allows your organization to skip the cost and time typically associated with each connection. Certificate authentication and encryption level requirements are configurable by policy and domain/host.

Increased delivery control with failover – No longer is TLS an all-or-nothing method. By making TLS a part of the ZixGateway policies, TLS is used only where appropriate. If a TLS connection is not available or cannot meet minimum authentication and encryption requirements, Zix provides a fallback secure delivery method.

Dashboard and detailed reporting – ZixGateway offers superior visibility for compliance officers through the ZixReporting Dashboard. The dashboard provides reports that show how each message was delivered, including TLS encrypted email, and to whom it was delivered.

Security branding – Embedded at the top of each TLS message is a "Secured by Zix" banner, providing confidence to your email recipients that the email and its sensitive content were delivered securely.

Zix Email Encryption	TLS	TLS with Zix
Secure, bidirectional delivery		✓
Simple configuration and maintenance		✓
Increased delivery control with failover		✓
Dashboard and detailed reporting		✓
Security branding for confidence and awareness		✓

About Zix

Zix is a trusted leader in email data protection. Zix offers industry-leading email encryption, a unique email data loss prevention (DLP) solution, and an innovative bring your own device (BYOD) email solution to meet your company's data protection and compliance needs. Zix is trusted by the nation's most influential institutions in healthcare, finance and government for easy-to-use secure email solutions. For more information, visit www.zixcorp.com

Secure, Reliable Email Encryption

Zix Email Encryption is the most secure, reliable and easy-to-use solution. It eliminates the inherent risks and limitations of TLS. If your organization is considering TLS as an additional component to your security strategy, leverage the benefits of "safe" TLS support through ZixGateway.

Phone 866-257-4949
sales@zixcorp.com
www.zixcorp.com