Emailing in China

The basics of Email delivery

To understand how email processing in China works, we need a basic understanding of how an email is sent. I will use examples to demonstrate what is happening.

1) Email between two people on a company email server

    a) The email is created on their local PC, mobile, etc. When sent, a copy is kept on their local device and sent to the company email server.
    b) The recipient downloads the email to their device using local software. A copy of the email is usually stored on the local drive.

    The other way is to write and read the email directly in the email service, typically using a browser. This is often called Webmail. Only a copy of the email is held on the company server.

    All company email servers use an SSL certificate, so emails cannot be read as they travel across the Internet between staff on the same company email service.

    Copies of the email are stored on the company email service and on the local drive, unless Webmail has been used.

    In this case, the business can manage and control email security.

2) Sending emails outside the company server

    a) The email is created on their local PC, mobile, etc. When sent, a copy is kept on their local device and sent to the company email server as before.
    b) The company's Email server then forwards the email with TLS encryption (like an SSL certificate) so that the next hop cannot read the email.
    c) The next hop can be directed to another company email server, and therefore, the email can't be read until it is delivered to this company email server. Once the email has been delivered, a copy is stored on the new company email server and can be read by the recipient. The number of copies of the email stored is increasing.

d) Sometimes, the next is not directly to the recipient's email server but to an email relay server. This could be within the network-provided data centre, within a country board, within a cloud service, etc. While the email could still be using TLS encryption between Email servers, it can still be stored and read in the email replay server
e) In summary, third parties can store, open, and read email if they can access the public internet.

Email security

Email can be sent securely. There are two approaches to achieving this;

- An enclosed email service.

  Only emails can be sent or received by staff within the system.

  Emails are contained only within the closed services. This can be extended so that remote users can view and write emails with copies on local drives. Users must connect to the centre point via a secure connection (VPN, SSL, or TLS).

  Large companies and governments often use this. It is expensive to build and run. It is very secure as long as all staff use it correctly. You may be in the news from time to time about local government officials sending emails through public email services rather than the secure government platform. Anyone can read emails if you do not use a secure email service.

- End-to-End Encryption (ETEE)

  This is an encryption protocol for hiding the contents of emails as they pass over the public internet and through email servers.

  ETEE Tools, such as PGP (Pretty Good Privacy) or S/MIME, ensure that only the sender and recipient can read the email content.

  For this to work, ETEE needs to be supported by and allowed on the network(s) where you send and receive email.

  China's networks and email services do not support ETEE.

Use of Email in China

Many people use their private email and messaging accounts for business, not a company email address. This type of email is free to set up and use.

For many Chinese businesses, this is a low-cost option. The same applies outside China, where we can use third-party email services like Gmail.

This often means verifying who works for which company can be confusing.

Free Chinese email services allow you to set up and use them. These services will enable you to use your domain name, such as QQ mail.

Most overseas public email services, like Gmail, are blocked in China. However, if your business operates a dedicated Email service, it may not be blocked. Please check by testing your Email service from within China.

If you run an office in China, we strongly advise you to instruct all staff to use the company email system for all published information. This will ensure a professional image.

Since EtEE is not available in China, you need to assume third parties can read Emails. For most business communications, this is not important. When sending confidential business emails from China, use your webmail service to send content directly to your company's email system.

Chinese firewall

- The Chinese firewall controls internet access, and certain websites, services, and platforms are blocked or restricted. This can impact email communication, especially if the services you use are among the blocked ones.
- When travelling to China for business or opening an office, etc., check with local contacts to ensure your email service is available there.
- You can create a QQ email account and forward your email to this account while in China.

Use of Local Email Providers

- In China, local providers like QQ Mail (by Tencent) and 163 Mail (by NetEase) are commonly used. These providers are more reliable for communications within China since they are not subject to the same restrictions as foreign providers.

VPNs and Workarounds

- A Virtual Private Network (VPN) will allow you to access content directly with our overseas services.
- Using VPNs in China is legal for personal use, but VPN providers must be government-approved. Some 5-star VPN services in China are licensed to use VPNs. Unapproved VPN services may not work reliably or could lead to penalties.

Performance and Delays

- Even if emails are not blocked, they can be significantly delayed due to the slow internet speeds in China.
- Large attachments or emails with embedded media (videos, for example) will be very slow to download from overseas Email services.

Alternative Communication Tools

- WeChat, including messaging and email-like functionalities, is widely used for personal and professional communication in China. WeChat may be a good alternative for informal or quick communications, although it's also subject to government monitoring.
- Aliyun Mail (Alibaba) is another email platform commonly used in China that may be more efficient for business communication than international email services.

Tips for Emailing to and from China

- Avoid sensitive topics in your emails, especially anything political or related to the Chinese government.
- If you communicate frequently with contacts in China, consider using local email services like QQ Mail to ensure better reliability.
- If you use a VPN to access foreign email services, ensure it's reliable and up-to-date, as China frequently blocks VPN traffic.
- For important or time-sensitive emails, test the connection beforehand and be prepared for potential delays.
- Use plain text and avoid large attachments to reduce the chance of emails being flagged or delayed.

By being mindful of these challenges and adapting your communication methods, you can ensure more reliable email exchanges with contacts in China.

Using your company email server with an SSL certificate for emailing to and from China can offer some advantages, but there are also important considerations. Here's a breakdown of how this setup would work, along with its pros and cons:

Benefits of Using Your Email Server with SSL

- **Increased Control** - Hosting your email server gives you complete control over how emails are sent, received, and stored. This can help avoid potential issues with third-party email providers being blocked or monitored in China.
- **SSL Encryption for Security** -An SSL certificate encrypts emails in transit, ensuring encrypted data is sent between your email server and clients (in China and elsewhere). This helps protect sensitive information from being intercepted.
- **Avoiding Service Blocks** - Using your server with a custom domain prevents you from relying on blocked services like Gmail or Outlook. If Chinese censors don't specifically target your server, this could provide a more reliable communication method.
- **Compliance with International Standards** - Having an SSL-enabled server means ensuring it meets international security standards, which may be required for certain business transactions or communication with global partners.

Challenges with Running Your Email Server in China

- **The Chinese Firewalls** - While using your email server might help avoid issues with blocked third-party services, your server's IP address could still be subject to censorship or throttling if flagged by the Great Firewall. Some domains or IP addresses could be added to blocklists, causing emails to be delayed or undelivered.
- **SSL Alone May Not Be Enough** - While an SSL certificate encrypts your email traffic, this doesn't make the content invisible to the Chinese government if they intercept or monitor the traffic. SSL only protects emails in transit, but it doesn't hide the existence of the email or its metadata (like sender, recipient, and timestamp).
- **Server Location Matters** - Chinese Firewalls may still slow down or block your email server's connection if it is outside China. Hosting servers in China may improve performance but pose compliance challenges (such as complying with local laws on data storage and content monitoring).
- **Compliance with Chinese Regulations** - If you host your email server in China, you must comply with strict data localisation and cybersecurity regulations. For instance, China's Cybersecurity Law mandates that certain types of data must be stored on servers physically located within China. This could involve government inspections or compliance with local data privacy laws, which may not align with privacy expectations in other countries.
- **Potential IP Blocklisting** - If the Chinese government or ISPs flag your server's IP for any reason (e.g., perceived misuse, hosting politically sensitive content, etc.), your emails may be blocked or delayed. Setting up a reliable email server requires careful monitoring to prevent IP addresses from being blocked.

Best Practices for Using Your Email Server

- Use a Trusted SSL Certificate Provider - Ensure you use a well-known SSL certificate authority (CA) recognised globally and by Chinese ISPs. Avoid lesser-known or untrusted SSL CAs, as Chinese services may not recognise or trust them, which could cause connection issues. Note:- Let's Encrypt is available and widely used in China
- Consider Server Location - If most of your email recipients are in China, consider using a server in a nearby region (e.g., Hong Kong, Singapore) or even hosting a server in China through a local provider. This can reduce latency and the risk of email delays caused by the Chinese Firewall.
- DNS and SPF Records -Ensure your DNS settings, including SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC records, are correctly configured to avoid having your emails marked as spam by Chinese ISPs.
- Monitor Server for Censorship - Regularly check if Chinese ISPs or the Great Firewall have blocked or flagged your server's IP. You can use services that monitor whether your email server can reliably send and receive emails from Chinese domains.
- Use Plain Text Emails - Simplify your emails using plain text rather than HTML formatting, particularly if you communicate with contacts in China. This can help reduce the risk that your emails will be flagged as spam or for surveillance.
- Be Aware of Content Sensitivity -Even though your server has an SSL certificate, you should still be cautious about the content of your emails. Discussing politically sensitive topics or specific keywords could still raise red flags with Chinese authorities, regardless of encryption.

Using VPN or Encryption Tools

- While SSL encrypts emails in transit, some users may also consider using VPNs or end-to-end encryption services (like PGP encryption) for additional privacy. However, using VPNs in China is heavily regulated, and encrypting email content with PGP might raise suspicion, as the government monitors encrypted communications.

Conclusion

Using your email server with an SSL certificate for emailing to and from China can offer more control and security. Still, it's not a guaranteed solution to bypass all the challenges posed by Chinese firewalls:

- Optimise server settings and DNS records,
- Monitor your server's performance, and
- Remain cautious about the content of your emails.

Additionally, encryption should be balanced with understanding the local laws and restrictions on internet usage in China.