What is Simple Mail Transfer Protocol: Uses and Best Practices

Simple Mail Transfer Protocol, or SMTP, acts as the backbone of email delivery across the internet. It moves your emails from your server to the recipient's server helping people communicate anywhere in the world. Knowing how SMTP works is important to use email to address security concerns.

How does SMTP Work?

Sending an email through SMTP might seem instant, but behind the scenes, there's a well-defined process that ensures your message reaches the right inbox. Here's how it works:

- ### Step 1: Establishing a Connection

  When you hit "Send," your email client—technically called a Mail User Agent (MUA)—connects to your outgoing mail server. This server, which handles the sending process, is known as the Mail Transfer Agent (MTA).

- ### Step 2: Transferring the Email

  Your email app passes along the necessary details—recipient address, subject line, message content—to the SMTP server for processing.

- ### Step 3: Identifying the Recipient's Domain

  The SMTP server extracts the domain from the recipient's email address to figure out where the message needs to go next.

- ### Step 4: Finding the Right Route

  Using DNS (Domain Name System), the SMTP server looks up the MX (Mail Exchange) records to find the mail server responsible for handling emails for the recipient's domain.

- ### Step 5: Delivering the Message

  Once it knows where to go, the sender's SMTP server connects to the recipient's mail server and hands over the email.

- ### Step 6: Inbox Placement

  The recipient's mail server accepts the message and places it into the intended inbox, where it becomes available for the user to open and read.

SMTP servers play the critical role of sending, routing, and relaying emails across networks. And in case you're wondering—SMTP uses TCP, not UDP. That's because email delivery needs reliable, ordered transmission, and TCP provides exactly that. SMTP typically operates over ports 25, 587, or 465, depending on the encryption and configuration used.

While SMTP handles email delivery efficiently, it wasn’t built with modern security in mind. Threat actors can exploit weak points in this flow—like DNS lookups or server handoffs. Fidelis Network® helps fill these gaps by monitoring SMTP traffic at every stage, giving organizations visibility into anomalies, protocol abuse, and lateral movement that traditional email security tools might miss.

Key Components of SMTP

SMTP depends on several main parts, and each one plays a role in how emails are sent. The SMTP client also called a mail user agent or a mail client, takes care of writing and sending messages. When you use programs like Apple Mail or Microsoft Outlook to send an email, the MUA reaches out to the SMTP server to deliver it.

SMTP servers work like digital post offices and handle sending, receiving, and forwarding email messages. These email servers also called mail transfer agents, play a key role in making sure that SMTP clients are sent to the right destinations. An SMTP email server makes this process possible.

The SMTP model includes several main parts like the user, the sender-SMTP or SMTP client, the receiver-SMTP or SMTP server, and the mail agents. These parts work together to make email communication flow.

9 out of 10 attacks are delivered by email, using phishing, macros and scripts, and social engineering.

- Monitors and analyzes SMTP traffic
- Quarantines messages that violate policy
- Detects threats withing mails and attachments

Download the Datasheet

Types of SMTP Servers

Outgoing Mail Servers (Mail Submission Agents – MSAs)

SMTP servers like these are the ones most people use . When you write an email in something like Gmail, Outlook, or Apple Mail and press “send,” your email client connects to an Outgoing Mail Server. This server’s main job is to take emails from Mail User Agents (your email app or software) and forward them to the right recipient’s server.

Here’s what stands out about Outgoing Mail Servers:

- **First Connection:** They act as the starting point for emails being sent.
- **Authentication Needed:** Most modern outgoing mail servers need a username and password to stop misuse and spam. This is why your email program gets set up with details from your email account.
- **Ports:** Port 587 is often used for sending emails with authentication, while port 465 is tied to SMTPS, which is an older method for secure connections. Port 25, another SMTP port, is reserved for server-to-server communication and is blocked for outgoing emails from regular users to curb spam problems.

SMTP Relay Servers (Mail Transfer Agents – MTAs)

SMTP Relay Servers often called Mail Transfer Agents or MTAs, play an essential role in moving emails between mail systems. After an email is sent out from an Outgoing Mail Server, it passes through an SMTP Relay Server. These servers ensure emails reach the right place by directing them from the sender's domain to the recipient's domain. They check the DNS to find MX (Mail Exchange) records that identify the target server.

Here are some key facts about SMTP Relay Servers:

- **Moving Emails Between Systems:** Their primary purpose is to shift emails between servers, like taking a message from Gmail and delivering it to Microsoft's system.
- **Robustness:** These systems handle large amounts of email traffic and make sure messages are delivered . They will often try resending emails if the receiving server is down.
- **Security Features:** They include tools such as SPF, DKIM, and DMARC. These tools help check if incoming messages are legitimate and stop spam or phishing attempts.
- **Often Internal:** Many large companies use their own SMTP relay servers within their network. This provides a way to track, secure, and control all outgoing emails before those emails leave their system.

Cloud-Based vs. Local SMTP Servers

The choice between using a cloud-based SMTP server (often provided by third-party services) and a local SMTP server (hosted within your own infrastructure) depends on various organizational needs and priorities.

Feature Cloud-Based SMTP Server Local SMTP Server

Setup

Quick and hassle-free. Just configure with provider credentials—no hardware needed. More complex. Requires hardware, installation, and network setup.

Scalability

Easily scales with changing email volumes. Flexible pricing plans available. Limited by infrastructure. Scaling often requires more servers or upgrades.

Control

Less control over infrastructure and policies. Customization may be restricted. Full control over setup, security, and storage.

Reliability

Generally high uptime with provider-managed redundancy and support. Depends on internal systems and IT capabilities. Prone to local issues.

Security

Strong security built-in, but data privacy depends on provider policies. Security fully in your hands. Offers more control over data location.

Cost

Pay-as-you-go model. Cost-effective for dynamic or large-scale needs. High upfront and ongoing costs—hardware, maintenance, and staff.

Best For

Most businesses, especially those needing fast setup and high deliverability. Organizations with strict data control or existing IT infrastructure.

To explain email security in SMTP, it's important to understand the specific weaknesses that attackers exploit and the layered defenses needed to close those gaps.

SMTP Attacks, Risks, and How to Strengthen Your Defenses

SMTP may be essential to email communication, but it comes with its share of vulnerabilities. Here's a breakdown of the most common threats and what organizations can do to mitigate them.

Common SMTP-Based Threats

Phishing Attacks

Scammers often send fake messages that look real. They try to trick people into giving private details like passwords or bank info.

Malware Spread

Hackers often use email to send harmful software. This includes things like viruses, ransomware, and tools that spy on users

Spoofing

Attackers fake the "from" address on emails so it looks like it's coming from someone trusted. They use this trick to send spam or phish for info.

Sending spam

Mass emails that are unwanted fill up inboxes and eat up network resources. Such attacks often

take advantage of SMTP servers that are either set up wrong or lack security.

Strengthening Email Security in SMTP

Organizations need to use multiple layers of security to protect against these risks. They should focus on things like encryption, authentication, and setting up servers.

Securing SMTP Communication

- **SMTP using TLS (Transport Layer Security):** This turns the connection into an encrypted and secure channel after starting the communication.
- **SMTP with SSL**, which stands for Secure Sockets Layer, is an older way to encrypt email communication. Most systems now use TLS instead. Both of these approaches work to keep email data safe while it is being sent. When people say “SMTP and TLS,” they are talking about using encryption systems to secure SMTP traffic.

Enabling Ways to Authenticate

- SPF stands for Sender Policy Framework. It checks if an email comes from an IP address that is allowed to send emails for a specific domain.
- DKIM, or DomainKeys Identified Mail uses a digital signature to verify that the message has not been altered.
- The DMARC system short for Domain-based Message Authentication, Reporting, and Conformance, builds on SPF and DKIM. It creates rules to decide what to do with emails that fail these checks.

Setting Up a Secure SMTP Server

- Block open relays to stop any unauthorized access.
- Use strict server policies and limit access as needed.
- Keep systems updated with the newest security fixes.

A secured SMTP server goes beyond just sending emails. It plays a crucial role in defending against phishing, spoofing, malware, and other threats that spread through email. Following these steps allows organizations to build trust, stay compliant, and keep operations running.

Securing SMTP at the configuration level is one piece of the puzzle. To fully protect against misuse and advanced threats, you need contextual awareness of what’s happening on the network. Fidelis Network® brings that visibility, helping you enforce email policies and respond faster to suspicious or malicious activity over SMTP.

Best Practices to Keep SMTP Secure and Efficient

To keep email communication both effective and safe, try following these important steps:

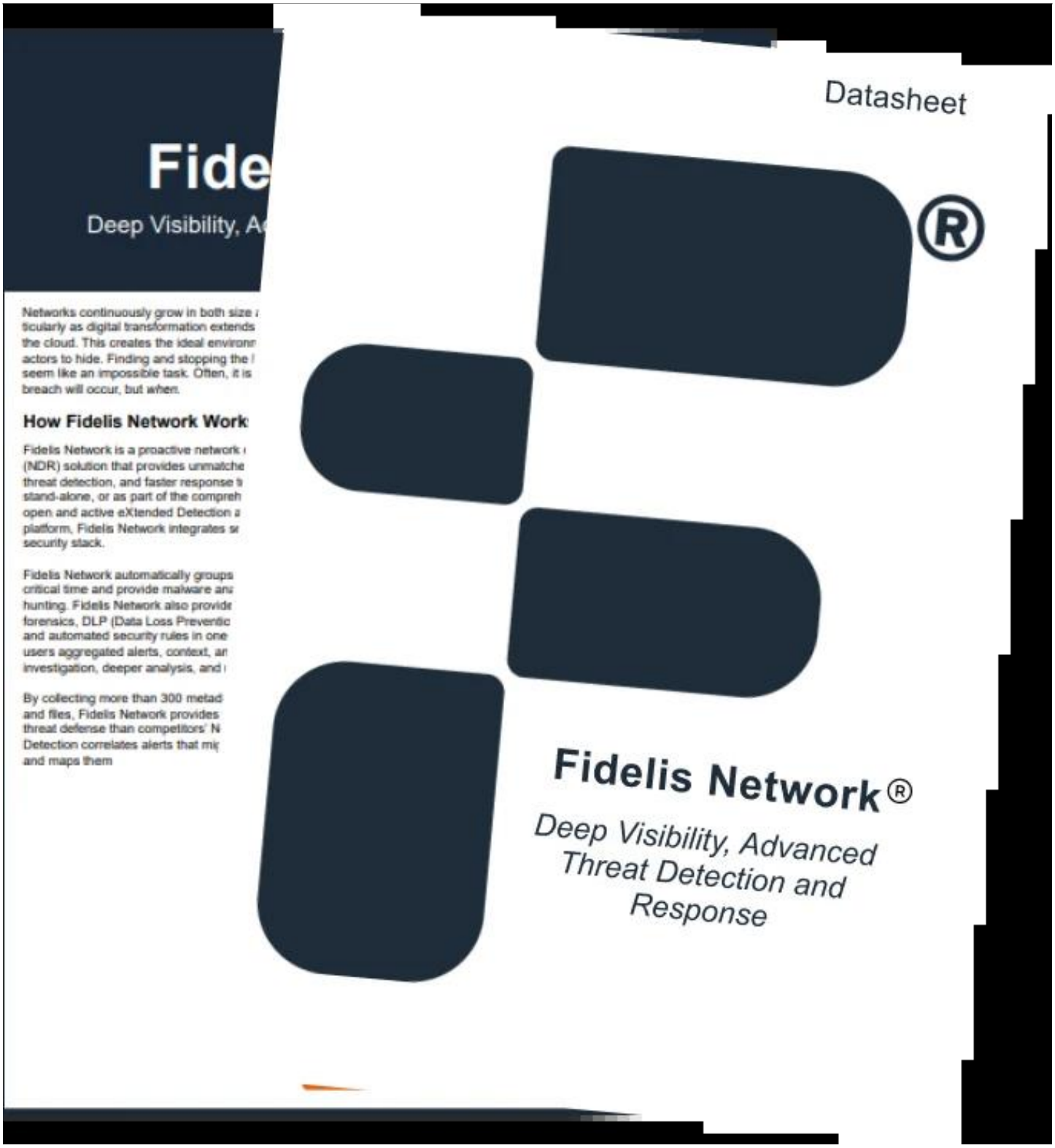
- **Use the Right SMTP Ports and Authentication**: Pick port 587 to submit emails with authentication or go with port 465 for encrypted SMTPS. Avoid port 25 since ISPs often block it to reduce spam issues.

- **Secure Emails with Strong Authentication and Encryption**: Protect outgoing mail by using user authentication along with TLS or SSL encryption. This ensures your credentials and email data stay safe during transmission.

- **Check Server Logs and Keep an Eye on Performance:** Watch SMTP server logs for suspicious behavior, errors, or signs of attacks. Also, track performance to keep email delivery smooth and reliable.

- **Keep Software Up to Date:** Update your SMTP server software, operating system, and security patches. This helps close security loopholes and shields your system from potential SMTP threats.

- **Pick Trustworthy SMTP Service Providers:** Go with services that deliver emails well, offer strong security tools like SPF, DKIM, and DMARC, and provide solid support to ensure emails are sent.



Conclusion

SMTP remains a foundational part of email communication, but without proper security measures, it can also become an entry point for serious threats like phishing, spoofing, and malware. From securing SMTP with encryption and authentication protocols to choosing the right server setup, every layer plays a role in safeguarding your communication infrastructure.

But beyond configuration and best practices, what organizations truly need is visibility and a clear view of how email traffic is moving across the network and where threats might be hiding.

That’s where Fidelis Network® comes in. It delivers deep, real-time inspection of SMTP traffic, helping detect hidden threats, enforce policy, and stop suspicious activity before it escalates. Whether it’s identifying phishing attempts, blocking data exfiltration via email, or mapping out attacker behavior, Fidelis Network provides the advanced detection and response capabilities required to secure email at the network level.

By combining best practices with advanced network detection, you don’t just send emails you secure them.

Frequently Ask Questions

What is SMTP?

SMTP (Simple Mail Transfer Protocol) is the internet standard protocol used for sending and receiving email messages. It acts as a set of communication guidelines that allow software and servers to exchange email.`

What are SMTP settings?

SMTP settings typically include the SMTP server address (e.g., smtp.example.com), the port number (e.g., 25, 587, or 465), and often authentication requirements (username and password).

When is SMTP used?

SMTP is used whenever an email is sent from an email client to an email server, or from one email server to another. It’s the protocol for outbound mail.

Why is SMTP used?

SMTP is used because it provides a standardized, reliable, and efficient way for email systems to transfer messages across the internet, ensuring that emails reach their intended recipients.

How do I find the SMTP server for my email?

To find the SMTP server for your email, use the command prompt or terminal to type: `nslookup -type=mx yourdomain.com`, replacing “yourdomain.com” with your email domain. This will display the MX records, which include the SMTP server address.

What is the Simple Mail Transfer Protocol?

The Simple Mail Transfer Protocol (SMTP) is a standard Internet protocol used for sending and receiving email messages. It is utilized by mail servers and message transfer agents for email communication.

How does SMTP work?

SMTP functions by establishing a connection between an email client and the mail server to transfer email data, verify the recipient’s domain, and then closing the connection upon successful transmission.

What are some common SMTP commands used in email

communication?

Common SMTP commands include DATA for defining email content, HELO for identifying the sender’s domain, and RSET for resetting the SMTP process. Understanding these commands is essential for effective email communication.