FAST.RELIABLE.SECURE.MESSAGING

How to Build an Effective Mail Server Defense

A multi-stage approach to securing your email communication

August, 21 2006

Author: Alin Dobre, Head of Customer Support, AXIGEN

GECAD Technologies

10A Dimitrie Pompei Blvd., BUCHAREST 2, ROMANIA

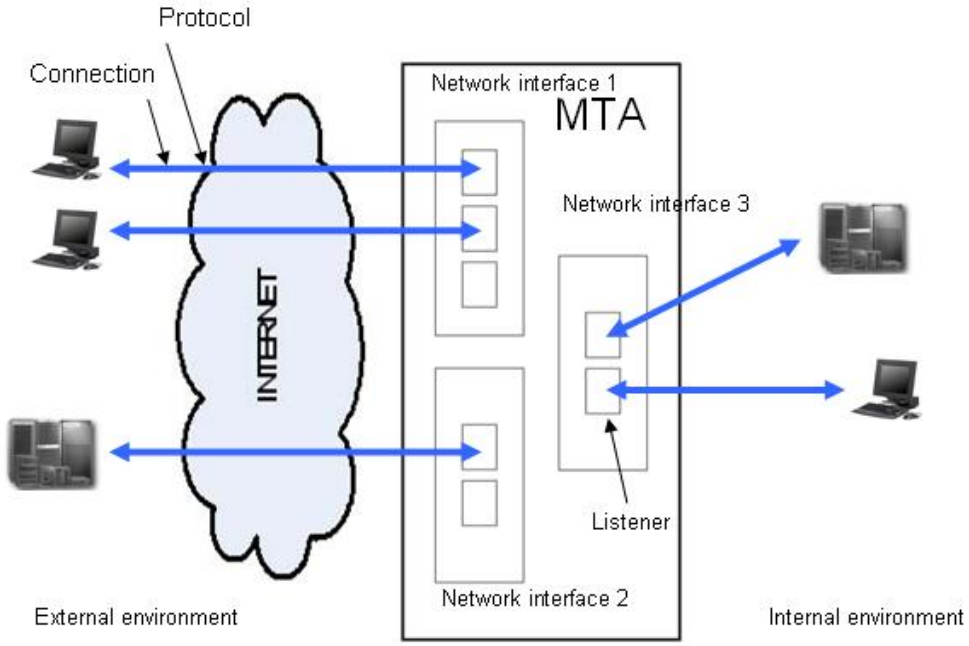
Tel.: +40 21 303 20 80

Fax: +40 21 303 20 81

http://www.axigen.com

When speaking of mail server-related security, one tends to limit the issue to message applied security measures, and even more to Antivirus and Antispam protection. This is however only one stage in the more complex process of securing your server. This article aims at identifying and explaining all security layers, highly important when choosing a certain mail server and consequently when configuring and using it.

We have chosen a multi-stage approach for your mail server securing procedure, each stage addressing one of the ***security layers*** we consider relevant: connection-related layer, protocol security, email control parameters (including Antivirus and Antispam applications), and the configuration and management layer (most likely to be affected by human errors).



Mail Server Environment Overview

The sections below describe security measures adapted to each layer of security:

1. Securing mail server connections

When using a newly installed mail server, administrators should first make sure they use secure connections. There are two main possibilities to secure connections: ***encryption*** and ***firewall-like rules***.

Encoding methods have continuously been developed as the Internet has become the preferred medium for data transfers. The most commonly used encryption methods are

SSL (Secure Sockets Layer) and ***TLS (Transport Layer Security)***. However, incorrect usage of encryption often leads to security breaches. Most common examples are web pages containing both secured and unsecured information or communications secured only after login via a plain login page.

Firewall-like rules enforced at server level are recommended to backup an existing Firewall or replace it when one is not available. They can impose limitations both on established connections and on hosted traffic. We recommend creating allow/deny rules both globally (applied to all protocols and listeners) and specifically for each listener in order to prevent attacks such as DOS (Denial of service).

2. Securing mail server protocols

After securing the first stage of an email transfer, the next action to take would be securing protocols.

The recommended steps are to use ***multiple listeners*** for each interface and correlate them with certain ***allow and deny rules***. Also, limiting the number of connection and authentication errors, the maximum number of commands or setting a time-out for your sessions can help protect your server from further DOS attacks.

To further enhance protocol security, we recommend ***client control rules***, based on the sender or receiver address and certain limitations regarding the number and size of email messages.

Authentication is also highly important at protocol level. By implementing several ***authentication methods***, either simple (plain, login, CRAM-MD5), or complex (GSSAPI, Kerberos), the mail server enhances communication security and is better equipped against attacks and unauthorized access.

Other efficient protocol level solutions are making sure your mail server is ***RFC compliant*** and preventing ***email looping*** (a very simple method would be setting a maximum numbers of “Received” headers per email).

3. Securing email control parameters

Apart from using different Antispam and Antivirus applications, there are further actions you should keep in mind where email control based security is concerned. One very handy option would be using ***gray lists***. Gray listing is basically a request to have the email resent, after temporarily rejecting the email. The server saves in a list the sender IP and the recipient and returns a temporary error. All valid servers will then resend the emails, unlike spamming scripts. Please note however that many servers cannot differentiate at this time between a temporary and a permanent error.

Host control is another easy way to ensure only valid emails are further processed by your email server. Two well known methods are ***SPF (Sender Policy Framework)*** and ***DNS based black hole lists***. SPF records are public details published by domains within DNS servers. Usually they point to and confirm the real addresses of domains. By using SPF checks, you can successfully prevent spam and back-scatter emails.

Black lists may be either public (free of charge) or private and usually contain IP addresses of open-relay servers, open proxies and ISPs with no spam filtering. Your server needs to be set up such as to request such lists and not to accept connections initiated by IP addresses included in them. If one of your servers gets erroneously listed, to be removed from such a list, you might need to fill an online form, contact the list administrators or, in more severe situations, change your IP.

A more complex authentication method is ***DKIM (Domain Keys Identified Mail Signature)***. Implemented by Yahoo and supported by Google, Cisco, Sendmail, PGP, DKIM has considerable chances of becoming the standard authentication method. The email header contains an encrypted signature and is in its turn encrypted, pointing to an encrypted key, published on DNS servers by the sending domain. The server processing the email will use this key to decode the email body. If the decryption is successful, then the email is valid.

Relay rules can sometimes make the difference between a secured server and an unsecured one. Our first recommendation is to never accept open relaying, as it can easily get you black listed. Therefore you should implement a few relay rules, based on sender address/recipient address, or relay for authenticated users only. When selecting your mail server, you should make sure it has the following features: it allows creating relay rules, domain authentication is configurable, the sending interface is customizable, it supports SSL/TSL and different authentication methods and extensions.

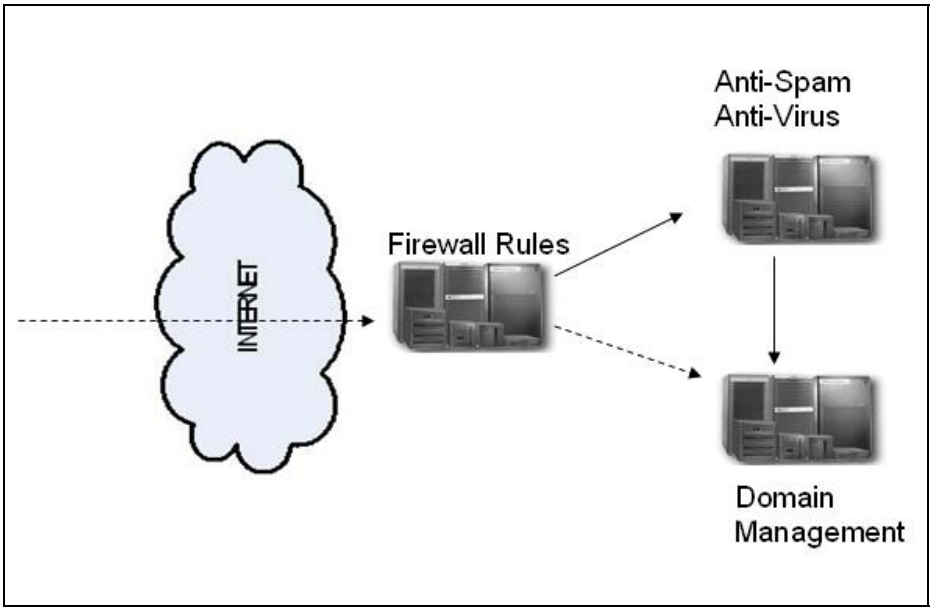
4. Secure configuration and administration

Configuration and administration are not commonly regarded as a security layer. However, the configurability features offered by the server and the actual configuration made by the user play a key part in securing your MTA. Firstly, the administrator should get acquainted to the solution, all its features and all its flaws, if any. The ***server executable file*** needs to support programming with no memory leaks, dropping root privileges (on Unices systems only), and blocking all access requests except those for public files.

Access to the ***configuration file*** should be granted to the administrator only. Further more, the file should always be very specific, easy to understand and to modify, while all default values should be secure. For example, a default value allowing open relay would represent a major security flaw.

Alternate administration modules (web interface, command line interface) should be provided for modifying the server configuration. It is also highly important that all connections to these modules are made through SSL. To make sure you securely access these modules, we recommend using a mail server with **proprietary HTTP server** and **HTML-based scripting language**.

Our most complete security recommendation is implementing a "***smart-hosting***" system. Such a system consists of several mail servers installed on different machines, each performing a specific task. The server offering the best connection and protocol security should be focused on firewall protection. The second one should run email control parameters (including Antispam and Antivirus applications). The third one should be mainly focused on domain management. However, smart hosting might require more hardware and software resources than those available within your system.



Smart Hosting

Conclusions

The most important aspect you should keep in mind is that there is no full proof security; therefore an optimal protection should substitute perfection. At each security layer, there are possible flaws and breaches. The solution is to choose the best possible configuration and adapt it to your network's needs and topology.

If you have any further questions or comments regarding the content of this article, feel free to email the AXIGEN support team.