XGEN Plus™

Worlds Most Advanced E-Mail Server

Security Features

Table of Contents

1. Introduction

E-mail is an integral part of the working of any organization. Email has allowed organizations to expand globally, through which you can easily interact with another individual in any part of the world with a single mouse click. True that a single click hooks you up with anyone in the globe; but if that click is made on the wrong place, you could be possibly giving out an open invitation to viruses, scams and other security threats to contaminate your mailbox. This is the reason email security is becoming a priority for all organizations, and they are ready to part with huge amounts to get email security.

Scope of email security can never be defined in a single line or a single paragraph. The job of email security package starts right from the beginning i.e. right from auditing and tracking of mails into and out of the organization. They also aim at reducing the risk of losing any mail data and retaining corporate knowledge. Not to forget, it should also ensure a disaster-recover plan in place to recover data from backups and archives in case of need. Another key aspect of the management of mail flow security is the protection of the business from malicious or unlawful attacks. And this list continues with the increasing scope of email security. That's why, however effective your email security system may be, you always have to be cautious while handling your emails.

For secure and effective email management, organizations must take a proactive approach and invest wisely in a comprehensive solution. And this is what exactly the hightlight for XGenPlus email solution is. XgenPlus email solution comes with in-built security features that promise to bring a much-more secured email management experience for you and your organization.

2. XGenPlus – Security Features

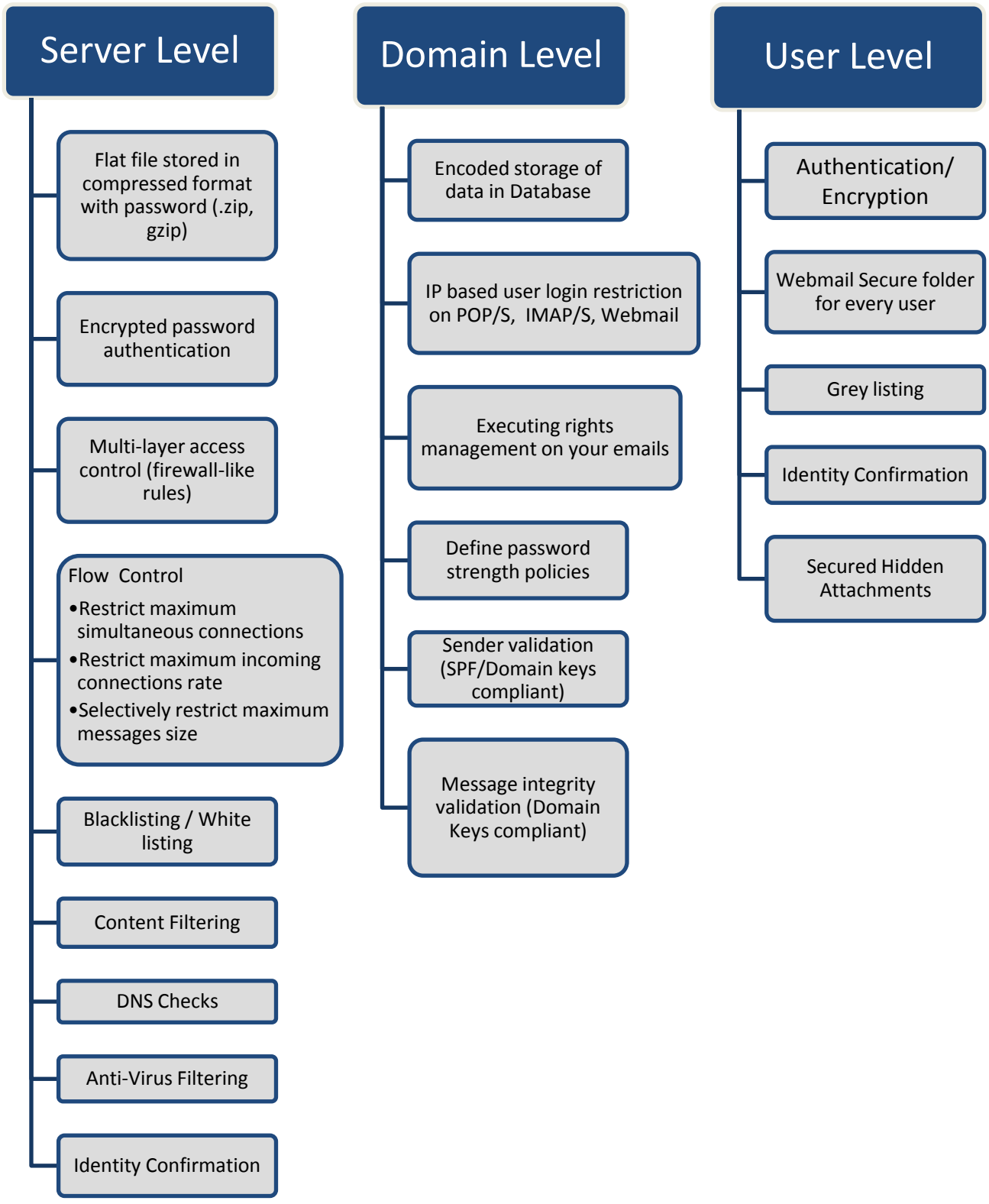
XgenPlus offers a secure email management solution that incorporates tight security at all levels of email management – be it mail flow, storage and user access. Along with a virus-free and spam-free email solution, these security features also offer the complete protection of your data. Thus, XgenPlus can be used to handle even the most confidential data without any worries. Its security, encryption, validation and protection techniques make sure your data is safe and is in the right hands.

XgenPlus follows a layered approach for security of its email management solution. This layered approach ensures effective email management, policy enforcement, auditing, archiving and data recovery. Whilst each one of these components should be addressed separately, they must be viewed as part of a total security agenda.

Based on this layered approach, XgenPlus security features can be divided into the following categories:

- Server Level Features
- Domain level Features
- User Level Features

All security features have been categorically listed below:



3. Server Level Features

These features provide the security layer at server level and have been described below in detail.

Flat file stored in compressed format with password (.zip, gzip)

- Flat files stored in the database are not in the plain text. All flat files are compressed and password-protected while storing in the database. This ensures extra security of data in flat files

Encrypted password authentication

- User Password is not saved as plain text in the database. User password is encrypted and stored in the database. It is not saved as plain text in the database. Hence, anyone having access to database can also not see user's password, thus, ensuring extra security for password as well

Restrict maximum simultaneous connections

- Restrict the total number of simultaneous connections that a service may accept, the maximum number of simultaneous connection accepted from the same IP address in order to avoid attacks from a single IP.Additionally, privileged IP address groups (trusted servers) may have different connection limits policies

Restrict maximum incoming connections rate

- Restrict the total number of connection per time unit that a service may accept, the maximum number of connection per time unit accepted from the same IP address in order to avoid attacks from a single IP. Additionally, privileged IP address groups (trusted servers) may have different connection rate limits policies

Selectively restrict maximum messages size

- The server can be configured to accept different maximum messages sizes based on sender/sender domain, recipient/recipient domain, remote IP address, connection security, authentication level and other message or connection related parameters, ensuring a flexible protection for the queue and the storage (privileged users may have extended rights)

Content Filtering

- Spamassassin, Baysian, Keyword and type of attachment based contenet filtering is available to the administrator to use. Separate module called spamjadoo is available with XgenPlus for this purpose

DNSBL, DBL/RHSBL

- Administrators validate sender IPs against a selected list of DNSBLs (DNS Blacklists) and DBL/RHSBL in order to block emails; at the same time, they can also choose to skip this validation for custom defined IP Ranges

DNS Checks

- Additional validations that can be run to reject spam are by checking the originating domain for MX entries and the originating IP for a reverse DNS entry

Anti-Virus Filtering

- XgenPlus's Advanced Filtering System allows the system administrator to define a set of filters and priorities at server, domain or user level, offering unparalleled flexibility to setup company security policies

Anti-Impersonation

- Enforce user authentication on message submission and verify that the sender header matches the authentication credentials preventing impersonation attempts from local accounts.
- Message and connection parameters for security policies (message size, anti-impersonation, SPF, access control, email address blacklisting / white listing, DNS checks, open relay blocking, etc):
  - Originating host's IP, ports, greeting
  - Originator's email address, domain or username
  - Recipient email address, routing information
  - Message size, headers, number of recipients
  - Connection security level (SSL / non-SSL)
  - Authentication information
  - Session statistics (total mails sent, total size)
  - SPF interrogation result

Multi-layer access control (firewall-like rules)

- Stopping spammers and preventing DOS attacks is one of the most important tasks of a mail server and the sooner the problem is identified in the mail stream, the better. This is why XGEN Plus has a Firewall module called spamjadoo at the application (TCP listener) level that allows the administrator(s) to control connectivity parameters.
- Furthermore, Administrators may define IP sets that have specific sets of such rules, applied with different priorities or IP sets whose connections are denied

Blacklisting/ White-listing

- Permanently reject emails coming from untrusted senders - can be defined globally by the administrator (server level) and further refined by the users according to their personal needs (WebMail interface)
- Administrators can also define Whitelists in order to permanently accept emails coming from trusted sources (such as business partners or remote offices)

4. Domain Level Features

Domain level features are the ones that can be incorporated at domain level and have been discussed below in detail.

Encoded storage of data in Database

- No plain text data storage in the database. All data is stored in the encoded format in the database. Encoded format ensures the protection of your data even from the administrators. Thus, get complete mailbox security from insiders as well as outsiders

IP based user login restriction on POP/S, IMAP/S, Webmail

- Worried about getting your account hacked by others? Want to ensure no one else logs in to your account? Set IP ranges for your account login and be free from all worries. Setting IP range makes sure that no one else is able to login to your account from external IP range

Executing rights management on your emails

- You can manage rights of your email in recipient's inbox while sending emails. By executing rights, you can restrict the recipient from deleting, forwarding, printing or replying to your emails. These rights can be executed across all domains on the same server

Define password strength policies

- Define and set password strengthening policies for your domain. E.g. set minimum password length, required sets of characters, mandatory alphanumeric characters etc. for the password. This restricts the users from setting simple and vulnerable passwords

Sender validation (SPF/Domain keys compliant)

- XGEN Plus implements a standard-based SPF verification module for sender validation (if the remote domain is properly configured with SPF information)

Message integrity validation (Domain Keys compliant)

- The messages' integrity may be checked if the originating server used Domain Keys to sign them; locally-originated messages may be signed by XGEN Plus to allow validation by Domain Keys-compliant remote servers

5. User Level Features

User level features cover the security features that can be configured on user level and have been discussed below in detail.

Authentication/Encryption

XGEN Plus server supports authentication, meaning it can be instructed to accept connections /messages only from authenticated entities. CRAM-MD5, LOGIN, PLAIN methods, in the same order, are available for client authentication thus, reducing the risk of unauthorized connections.

Xgen Plus supports SSL enabled connections. SSL-enabled connections are the connections that support Secure Socket Layer Security. SSL (Secure Socket Layer) is a standard providing encryption and authentication service that can be negotiated during the start up phase of many Internet protocols, including SMTP, POP3 and IMAP, and used for general communication authentication and encryption over TCP/IP networks. XGEN Plus supports SSL-enabled connections, providing advanced SSL parameters for TCP Listener configuration available for all its TCP Services (SMTP, IMAP, POP3, WebMail, CLI and WebAdmin)

Webmail Secure folder for every user

Secure your important emails in a separate password-protected folder. Keep password different from login password for Secure Folder. Separate password ensures double password protection for secured folder

Grey listing

This feature enables XGEN Plus to automatically reject messages from unknown senders / IPs with a temporary error message. Unlike legitimate email servers, most spam sources will not try to resend the emails in question, thus reducing the amount of spam received by the XGEN Plus server

Identity Confirmation

Identity Confirmation is basically the implementation of a Challenge/Response-based antispam method. It enables users to effectively block unwanted messages from reaching their inbox by intercepting incoming emails and requiring new/unknown senders to confirm their identity, while allowing legitimate communications to come through

6. How Important Security is?

As email becomes more prevalent in the market, the importance of email security becomes more significant. Managing large, active stores of information takes time and effort in order to avoid failures – failures that can impact the users and therefore the business, leading to lost productivity. XgenPlus is a perfect blend of Email Management System and Email security solution.

Robust, reliable and highly secured, XgenPlus is apt for all your business needs. For more details regarding XgenPlus, please visit www.xgen.in.