PreciseMail Authentication Case Studies

Executive Summary

The rapid expansion of spam is requiring most sites to implement spam filtering solutions to keep users' email boxes from becoming clogged with junk mail. Early anti-spam solutions forced much of the administration related to anti-spam efforts onto the system administrator: retrieving messages that were incorrectly classified as spam; creating whitelists and blacklists for the entire site as well as individual users; and tweaking individual user's filtering settings to match the content of their legitimate email messages.

Modern anti-spam solutions give most of that control to the end user through a user interface, which improves the average user's anti-spam experience while freeing up the system administrator for more important tasks. Giving the power to alter spam filtering settings to end users also gives them the potential to abuse that power. While most users might not scan through their co-workers quarantined spam messages, the temptation to set up a blacklist entry that discards all email addressed to a person they dislike might be too great.

To prevent this type of abuse, users should have to authenticate themselves to the anti-spam solution using a user name and password. To avoid giving each user yet another user name and password they will inevitably forget, their email address and email password should be used.

In an ideal world, this would be a trivial matter of telling the anti-spam solution to authenticate users against a centralized authentication system. Unfortunately, most sites in the real world have a complex collection of email systems that have been forced on the system administrator by a mixture of budgetary policy, corporate acquisitions, and departmental mergers. The majority of sites are beginning to transition towards centralized authentication systems such as LDAP, but that process can take an extended period of time during which the anti-spam solution still needs to be able to authenticate end users. For the sake of simplicity, most spam filtering software only supports users who exist in an LDAP directory.

To help system administrators cope with complex collections of email server systems, PreciseMail Anti-Spam Gateway includes a plethora of authentication methods that can be mixed-and-matched together to fit a site's needs. The ability to simultaneously support multiple authentication methods is unique to PreciseMail. This whitepaper describes each of the authentication methods provided by PreciseMail Anti-Spam Gateway, and provides case studies of how several sites have combined the PreciseMail authentication methods to provide a seamless experience to their end users.

PreciseMail Authentication Methods

The authentication methods provided by PreciseMail Anti-Spam Gateway are:

SYSTEM

The `SYSTEM` authentication method checks user names and passwords against the local system password file (`SYSUAF` on VMS and `/etc/passwd` on UNIX). Use this method to authenticate users who have a login account on the same system that PreciseMail Anti-Spam Gateway is running on. The user portion of the email address used to sign in to PreciseMail (in other words, everything to the left of the @ sign in the address) must exactly match the user's login name on the system.

LDAP

The LDAP authentication method checks a user's credentials against a centralized authentication server. This method is ideal for sites that have begun or completed the transition to centralized authentication. The LDAP method is also the best choice for authenticating against email servers that are LDAP-based (Microsoft Exchange and the Sun Messaging Server are two such servers). A simple tag-expansion language is supported by the LDAP method that allows easy translation of email addresses into distinguished names (DNs). For more information about tag-expansion support, see the *PreciseMail Management Guide* for your platform.

PMAS

The PMAS authentication method checks users' passwords against the PreciseMail user database. Every user of PreciseMail has an entry in the user database, although the password field is usually left empty for most users. This authentication method is commonly used for internal Anti-Spam Gateway accounts (such as the pmas_admin user) and users that cannot be authenticated against any of the other authentication methods provided by PreciseMail.

POP3

The POP3 authentication method checks a user's credentials against a POP3 server. This method is an ideal choice if you need to authenticate users who do not have entries in a centralized authentication database. The POP3 method works by connecting to one or more specified POP3 servers and performing the authentication phase of a POP3 transaction. This authentication phase consists of exactly the same tasks that a mail client (such as Outlook, Netscape Mail, Eudora, or a webmail client) would perform when the user logged into the server to check their mail.

IMAP4

The IMAP4 authentication method operates in exactly the same way as the POP3 authentication method described above, except that it connects to an IMAP server and performs the authentication phase of an IMAP4 transaction. If possible, the POP3 method should be used in preference to the IMAP4 method since it generally requires fewer system resources on the email server. (Both the POP3 and IMAP4 methods require minimal overhead in PreciseMail.)

Authentication Procedure

The authentication system provided by PreciseMail is designed to let multiple authentication mechanisms co-exist in as simple an environment as possible. The system administrator doesn't have to maintain a database that explicitly lists which authentication methods must be used for which user, and users aren't required to know anything about their site's authentication mechanisms.

When PreciseMail is installed, the system administrator chooses which authentication methods should be used at the site, the order they should be used in, and options related to those methods. When a user authenticates to PreciseMail, each authentication method is tried in the order specified by the system administrator. If the user's authentication credentials are rejected by the first authentication method, the other specified methods are tried in order until either a successful authentication occurs or the list is exhausted.

For example, a site might be configured to authenticate against an LDAP server, two POP3 servers, and the system password database (in that order). The user `jane_doe@example.com`, whose account is on the second POP3 server, attempts to sign in to PreciseMail. The PreciseMail authentication module begins by trying to authenticate the user against the LDAP server. This attempt fails, since the LDAP server's directory doesn't contain an entry for the user. The PreciseMail authentication module next tries to authenticate her against the first POP3 server. This attempt fails as well, since the user doesn't exist on that POP3 server. Finally, an attempt is made to authenticate the user against the second POP3 server. This attempt succeeds, and `jane_doe@example.com` can access her quarantined spam messages and anti-spam settings.

This entire process is hidden from the end user - all `jane_doe` knows is that she entered her login information, clicked the "Login" button, and her personal start page was displayed in her web browser a fraction of a second later.

If `jane_doe` had accidentally mistyped her password, the PreciseMail authentication module would have tried to authenticate her against the LDAP server, both POP3 servers, and the system password database in turn. All of those authentication attempts would have failed, so PreciseMail would have displayed an error message to that effect and asked her to try again.

If an error had occurred during the authentication process (such as one of the POP3 servers being inaccessible), the PreciseMail authentication system would attempt to bypass it and continue trying to authenticate the user. If the first POP3 server (the one that doesn't contain the user's account) had crashed, `jane_doe` would have been logged into PreciseMail normally. If the second POP3 server (the one that does contain the user's account) had crashed, PreciseMail would have displayed an error message to the user as opposed to a "bad password" message.

While all of the authentication methods supported by PreciseMail are lightweight, external factors such as network latency and the workload of the systems containing the authentication information can slow authentication operations down significantly. The following suggestions can help prevent this from happening:

- Place the authentication method used the most often first in the list of authentication methods to try.
- Place authentication methods that depend on slow systems or network links near the end of the list.
- If a server you want to authenticate against supports both the POP3 and IMAP4 protocols, use the POP3 protocol to authenticate. POP requires fewer system resources than IMAP,

which will speed up the authentication session and reduce load on the server.

Authentication Aliasing

Sometimes email addresses don't have a corresponding user account. A common example of this would be the address of a site's Webmaster, such as `webmaster@example.com`. The real person who is responsible for the webmaster account might be Jane Doe, whose personal email address is `jane_doe@example.com`.

The PreciseMail administrator could resolve this problem by binding the `webmaster` account to the `jane_doe` account with an alias entry. This would have the effect of placing all quarantined mail for the webmaster account into `jane_doe`'s quarantine. Quarantined messages for the `webmaster` address would be accessible to `jane_doe` both through quarantine notification messages and the web-based user interface. The entry in the PreciseMail aliases file to accomplish this would look like:

```
webmaster@example.com   jane_doe@example.com
```

The problem with this approach is that it mixes messages quarantined for the Webmaster with messages quarantined for Jane Doe. A better solution is to place a third field on the alias line, which specifies an authentication alias. This alias field instructs PreciseMail to authenticate the account in the first field of the alias line using the authentication credentials of the account in the third field. To implement this solution for the webmaster example, the following line would be added to the PreciseMail alias file:

```
webmaster@example.com   webmaster@example.com   jane_doe@example.com
```

With the above alias entry in place, Jane Doe can check her personal quarantine by logging in as `jane_doe@example.com` (just like she always has). If she wants to check the messages that have been quarantined for the `webmaster` account, she can log in as `webmaster@example.com` and specify her personal password as the login password. In essence, this alias line has instructed PreciseMail to require Jane Doe's password for access to the webmaster account's quarantine area.

Six Case Studies

Following are six case studies that demonstrate how real-world sites have successfully used PreciseMail's flexible authentication system to provide a seamless anti-spam interface experience for their users.

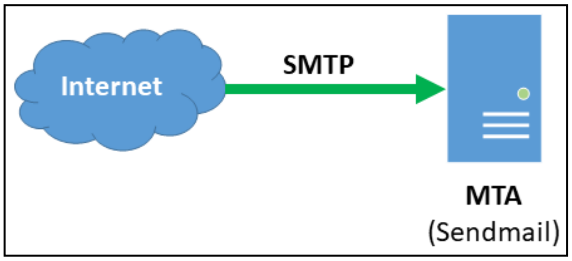
Sendmail with Local Users

This site uses a single system running Sendmail on Linux as their email server system. Each of their 500+ users has a local system account, so the `SYSTEM` authentication method is an obvious choice.

The site also enables the PMAS authentication method for usage by internal PreciseMail users, such as pmas_admin.

When a user supplies a set of valid credentials to access the user interface, the PreciseMail authentication system performs a quick check against the /etc/passwd file before allowing access. If invalid credentials are supplied, the authentication system will first check the /etc/passwd file. When that fails, the PreciseMail user database will be checked. If that fails, an error message will be displayed to the user.

The below diagram shows the network architecture for this site. Messages are received directly from the Internet by the email server (also known as a Mail Transfer Agent, or MTA), which is running Sendmail with PreciseMail. When a user attempts to log into the web interface, all authentication is performed locally on the MTA.



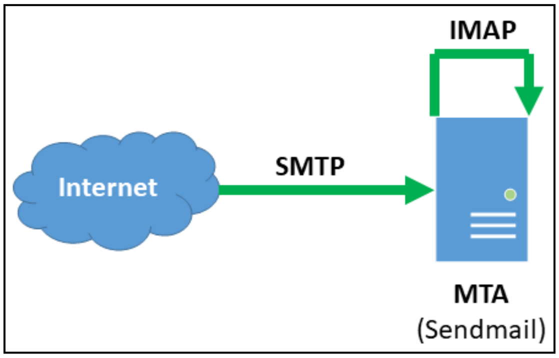
PMDF on Linux with Local and MessageStore Users

This site's email system consists of a single Linux system running PMDF. There are roughly 1,200 users on the system, whose mail is stored in the IMAP-optimized MessageStore. As a result, the system administrator has configured PreciseMail to use the IMAP authentication method. Like most sites, the administrator has also enabled the PMAS authentication method for administrative access. Because the vast majority of PreciseMail authentication attempts will be users accessing their quarantined mail or personal filtering settings, the system administrator has configured PreciseMail to try authentication against the IMAP server before it attempts authentication against the PreciseMail user database.

When a user attempts to authenticate themselves to the user interface, the PreciseMail authentication system opens a light-weight IMAP connection to the PMDF IMAP server (which is backed by the PMDF MessageStore). PreciseMail performs an IMAP login as specified in RFC 3501, Internet Message Access Protocol. If the authentication credentials are accepted by the IMAP server, PreciseMail grants the user access to the user interface.

If the IMAP server does not accept the user's authentication credentials, PreciseMail tries to authenticate against the PreciseMail user database. (This is what will happen if an administrative account, such as pmas_admin, is attempting to log in.) If this fails as well, an error message will be displayed to the user.

The below diagram shows the messaging system architecture for this site. Messages are received directly from the Internet by the email server, which is running PMDF. When a user attempts to log into the web interface, PreciseMail makes a quick IMAP connection to the PMDF IMAP server. If the IMAP server rejects the authentication credentials, PreciseMail checks the PreciseMail user database on the local system.



Linux Proxy for an ISP's Custom Email Software

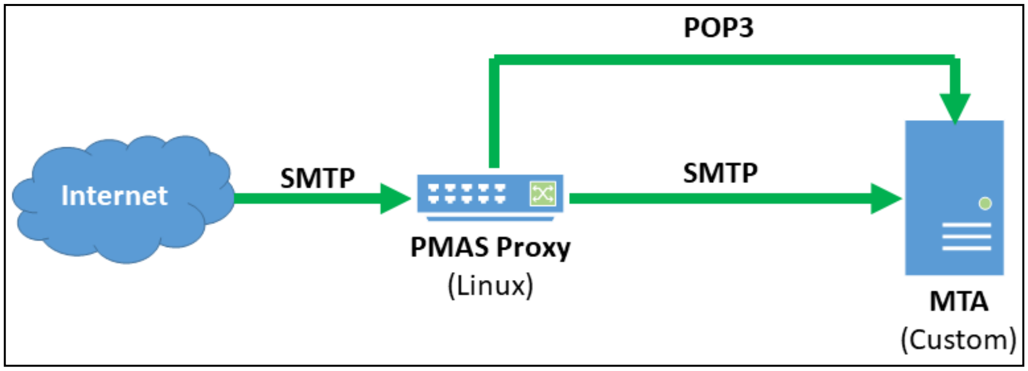
Like many Internet Service Providers (ISPs), the site in this case study has developed custom email server software to handle its specific requirements. Each of the ISP's users is allowed to have up to five different email addresses, each of which is protected by PreciseMail. As a result, PreciseMail provides email security for between 350,000 and 500,000 accounts depending on usage. Because the ISPs email servers are already heavily loaded, placing a PreciseMail pass-through proxy in front of them was a logical choice. Using the proxy doesn't add any additional overhead to the existing email servers - in fact, it significantly decreases system load by keeping messages identified as spam off of the actual email servers.

Currently, the ISP only allows its customers to access their email through either a custom web interface or the POP3 protocol. PreciseMail's support of the POP3 protocol for user authentication made it a drop-in solution. Like most sites, the ISP's system administrators enabled the `PMAS` authentication method for administrative access in addition to the `POP3` authentication method. The ISP's long-range planning calls for IMAP support to be gradually phased-in over the next several years. When this project begins, all the system administrators have to do is tell PreciseMail to begin using the `IMAP` authentication method in addition to the `POP3` authentication method. The ISP's users won't notice any change in the way they use PreciseMail.

With the current POP3 system, the ISP's users connect to a web server running the PreciseMail user interface on the proxy system. When users provide an email address and password to login to the user interface, PreciseMail makes a lightweight POP3 connection from the proxy system to the main email server. If the main email system accepts the authentication credentials, the user is granted access to the PreciseMail user interface. If the main email system rejects the authentication credentials, PreciseMail attempts to authenticate the user against the user database located on the proxy system (this is how the `pmas_admin` user is authenticated). If a match cannot be found in the PreciseMail user database, an error message is displayed to the user.

The below diagram shows how the PreciseMail pass-through proxy is integrated into the ISP's mail system. Incoming messages from the Internet are accepted by the PreciseMail proxy system, which checks with the main email server to make sure they're addressed to a valid recipient. If PreciseMail determines that a message is not spam, it is passed straight through to the main email server. If PreciseMail identifies the message as spam, it is held on the proxy system.

When a user logs in to the PreciseMail user interface on the proxy, a quick POP3 connection is made to the mail server. If the mail server reports back that the authentication credentials are invalid, PreciseMail checks the user database on the proxy system.



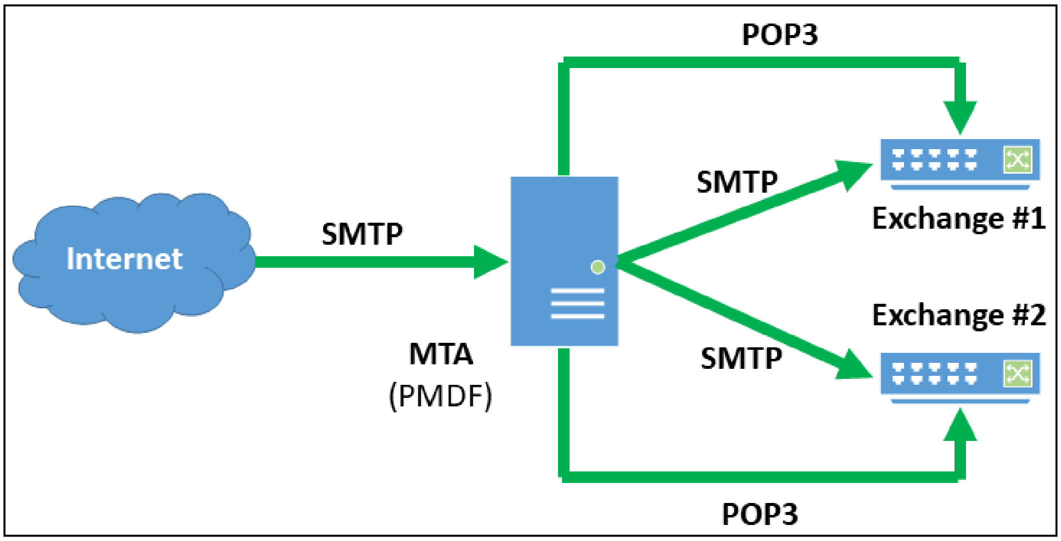
OpenVMS PMDF Gateway for Two Exchange Systems

This site houses all of its users' email accounts on two Microsoft Exchange systems that sit behind an email firewall running PMDF on VMS. The site is involved in an industry that is highly regulated by the US government, so the email firewall is responsible for enforcing email policies in addition to scanning all incoming email for spam and viruses. The system administrator has decided to have PreciseMail use the POP3 authentication method against both of the Exchange servers to allow users access to PreciseMail's web interface. Like most sites, the system administrator has enabled the PMAS authentication method for administrative access to the web interface.

When a user logs into the PreciseMail web interface, the authentication system opens a POP3 connection to each of the Exchange servers in turn. PreciseMail performs a POP3 login as specified in RFC 1939, Post Office Protocol. If the authentication credentials are accepted by either of the Exchange servers, the user is granted access to PreciseMail's web interface.

If neither of the Exchange servers accepts the user's authentication credentials, PreciseMail tries to authenticate the user against the PreciseMail user database. (This is the authentication path taken by administrative users at this site.) If this fails as well, an error message will be displayed to the user.

The below diagram shows the messaging system architecture for this site. Every message from the Internet passes through the PMDF email firewall, where it is checked for spam, viruses, and policy compliance. If the message is deemed legitimate, it's passed on the Exchange server that holds the user account to which it is addressed. When a user attempts to login to the web interface, PreciseMail makes a quick POP3 connection to each of the Exchange servers. If both Exchange servers tell PreciseMail the authentication credentials are invalid, PreciseMail checks the PreciseMail user database on the PMDF system before displaying an error message to the user.

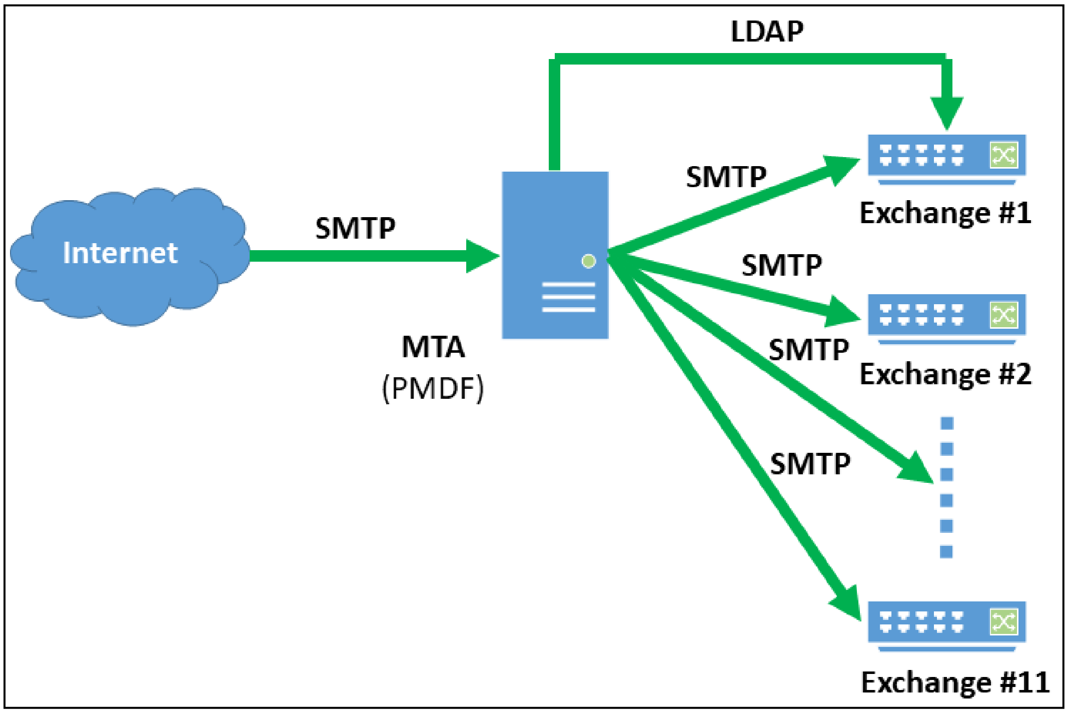


Linux Sendmail Gateway for 11 Exchange 2012 Systems

This site uses 11 different Microsoft Exchange 2012 servers to host email accounts for its 5,500 users. Each major department has its own subdomain and its own Exchange server. All of the Exchange servers consult a single instance of ActiveDirectory running on one of the Exchange servers for user information. PreciseMail Anti-Spam Gateway directly supports ActiveDirectory with the LDAP authentication method, which the system administrator at this site has chosen to use. The system administrator has also enabled the PMAS authentication method for use by PreciseMail's administrative users.

The below diagram shows how PreciseMail Anti-Spam Gateway integrates into this site's email infrastructure. Since there are a large number of email systems PreciseMail needs to scan email for, placing the pass-through proxy version in front of all of the systems was the most efficient choice. The site chose to use the Linux version of the PreciseMail pass-through proxy, since that allowed them to run it on the same type of system as their Exchange servers. Using a common system type simplifies maintenance, reduces the inventory of spare parts that must be kept on hand in case of hardware failure, and allows all of the systems to fit into the same rack in the corporate data center.

Every message from the Internet is scanned by the PreciseMail proxy on its way to the Exchange server that holds the account for the message recipient. If PreciseMail determines that the message is spam or contains a virus, it quarantines the message on the proxy system and prevents it from ever reaching the Exchange systems. When a user attempts to login to the PreciseMail web interface, PreciseMail performs an LDAP query against the ActiveDirectory server running on one of the backend Exchange systems. If the ActiveDirectory server tells PreciseMail that the user's credentials are invalid, PreciseMail checks the user database on the proxy system to determine if the user is supplying a valid password for one of the administrative users. If all of the authentication checks fail, the PreciseMail web interface displays an error message to the user.



Sun Messaging Servers Serving as Local Message Stores and Gateways for Lotus Notes

The final case study covers a site that is currently engaged in a very gradual transition from two legacy Lotus Notes systems to two Sun Messaging Server systems. The transition was approximately 75% complete when they chose PreciseMail to protect their email users. A key consideration in the site's decision to use PreciseMail was that it provided the flexibility to support all of their email systems both during and after the transition period.

When the transition is complete, all mail sent to the site will pass through the primary Sun Messaging Server system. Message scanning for spam and viruses will take place on this primary system. If the primary system determines that a message does not contain harmful content, it will transfer the message to the secondary system where the user mailboxes are located. During the transition period, the primary system sends mail for non-migrated users to the legacy Lotus Notes systems.

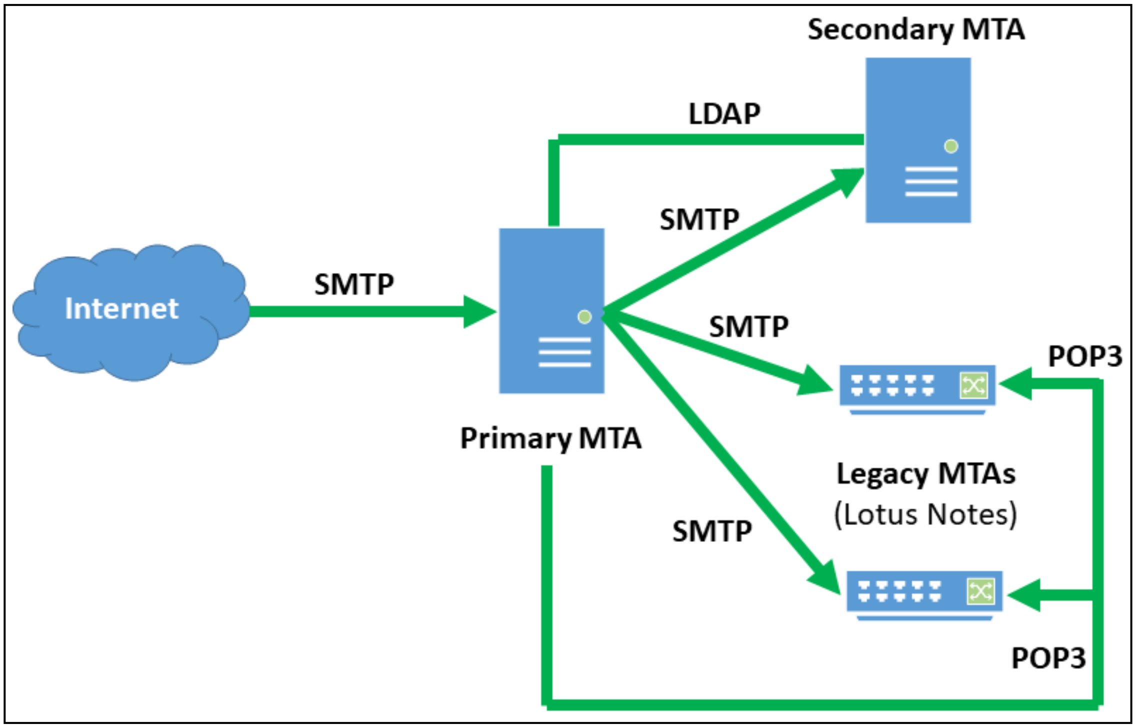
PreciseMail must be able to authenticate users of the two legacy Lotus Notes systems in addition to the new Sun Messaging Server systems. Lotus Notes supports the POP3 protocol, so the site's administrator has chosen to use that authentication method for users whose accounts are still located on the legacy systems. The Sun Messaging Server product is tightly tied to an LDAP server, which contains authentication information for every user on the system. While the system administrator could choose to use the `IMAP4` authentication method to authenticate users against the Sun

Messaging Server's IMAP server, the LDAP authentication method is much faster and requires fewer system resources.

The site's administrator has chosen to order the authentication methods so that PreciseMail tries to authenticate users against the LDAP server before attempting to authenticate them against the two Lotus Notes systems. This makes the login process fast for the growing majority of the site's users who have been migrated to the new Sun Messaging Server systems. If the LDAP authentication fails, then authentication using the POP3 method is attempted against each of the Lotus Notes systems. Once every user has been migrated away from the legacy Lotus Notes systems, the system administrator will remove the POP3 authentication method from the PreciseMail configuration.

The below diagram shows the messaging system architecture for this site during its transition. All incoming email from the Internet is routed through the primary Sun Messaging Server system. Messages addressed to users who have already been migrated to the new system are passed on to the secondary Sun Messaging Server system, which houses the users' Inboxes. Messages destined for users who have not yet been migrated to the new systems are sent to whichever Lotus Notes system the user account resides on.

When a user attempts to login to the web interface, PreciseMail queries the LDAP server used by the Sun Messaging Server systems. If the LDAP server tells PreciseMail that a user's authentication credentials are invalid, a POP3 connection is opened to each of the legacy Lotus Notes systems. If the LDAP server and both of the Lotus Notes servers reject a user's authentication credentials, the web-based interface will display an error message.



About PreciseMail Anti-Spam Gateway

PreciseMail Anti-Spam Gateway is an enterprise software solution that eliminates spam, phishing and virus threats at the Internet gateway or mail server. It has a proven 98% spam detection accuracy rate out-of-the-box without filtering legitimate messages. PreciseMail Anti-Spam Gateway has a highly sophisticated filtering engine is based on a combination of proven heuristic, DNS blacklisting, and Bayesian artificial intelligence technologies, which automatically learn how to separate spam messages from legitimate email. As a result, PreciseMail Anti-Spam Gateway can determine whether email is spam instead of passively reacting to known spammers by creating rules that block them after a spam attack occurs.

About Process Software

Process Software has been a premier supplier of communications software solutions to mission critical environments for twenty years. We were early innovators of email software and anti-spam technology. Process Software has a proven track record of success with thousands of customers, including many Global 2000 and Fortune 1000 companies.

PROCESS™
SOFTWARE

U.S.A.: (800) 722-7770 • International: (508 879-6994 • Fax: (508) 879-0042
E-mail: info@process.com • Web: http://www.process.com/