FERMILAB-CONF-04-482-CD

FNAL Central Email Systems

Jack Schmidt, Al Lilianstrom, Ray Pasetes, and Kevin Hill

(Fermi National Accelerator Laboratory)

Introduction

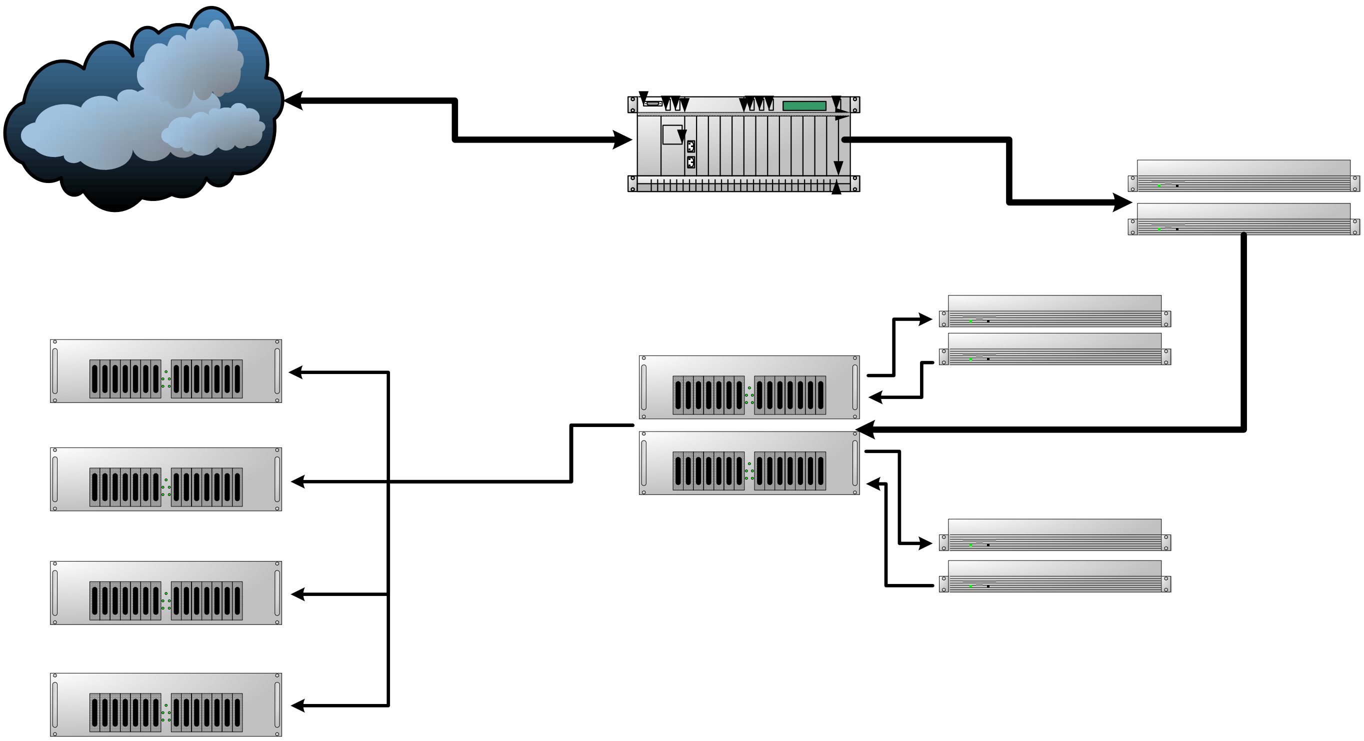
The FNAL Email System is the primary point of entry for email destined for an employee or user at Fermilab. This centrally supported system is designed for reliability and availability. It uses multiple layers of protection to help ensure that:

1) SPAM messages are tagged properly
2) All mail is inspected for viruses
3) Valid mail gets delivered

This system employs numerous redundant subsystems to accomplish these tasks

Hardware

SPAM Tagging	Dell 2650 (www.dell.com)
MTA	Sun E280 (www.sun.com)
LDAP	Sun Netra
Symantec AV	Dell 2650
IMAP	Sun E280 LSI FC SAN (www.lsilogic.com)
POP	Sun Netra LSI FC SAN
ListServ	Dell 2650



Services Software

The centrally supported services use commercial software. The ‘UNIX Servers’ represent the various UNIX and Linux machines that choose to receive mail.

IMAP	Solaris 9 (www.sun.com) Sun Java Enterprise Server Mail Server
POP	Solaris 8 iPlanet Messaging Server
ListServ	Windows Server 2003 (www.microsoft.com) ListServ (www.lsoft.com)

Gateway Software

A combination of commercial and open source software is used to build what we consider the gateway system

SPAM Tagging	Fermi Linux LTS 3.01 (www-oss.fnal.gov/projects/fermilinux/) PostFix (www.postfix.org) Spam Assassin (www.spamassassin.org)
MTA	Solaris 9 (www.sun.com) SunONE Messaging Server Sophos AntiVirus (www.sophos.com)
LDAP	Solaris 9 SunONE Directory Server
Symantec AV	Windows Server 2000 (www.microsoft.com) Symantec NAV for Gateways (www.symantec.com)

Bord

FNAL Central Email Systems

Jack Schmidt, Al Lilianstrom, Ray Pasetes, and Kevin Hill

(Fermi National Accelerator Laboratory)

Incoming Mail

Mail that is destined for a user at Fermilab can only enter the site through a small number of dedicated machines. The border router is configured to only allow incoming SMTP connections to these machines. All other attempts are rejected. By imposing this restriction all incoming mail can be evaluated by software designed to check the mail for SPAM indicators, for viral content using two different applications, and then deliver it as quickly as possible to the end user: on either one of the centrally supported servers or a personal Linux/UNIX machine.

Mail that originates outside of Fermilab and addressed to Fermilab users should be addressed to *user*@fnal.gov. If the mail is addressed to *user*@machine.fnal.gov the external machine will first attempt to connect directly to machine.fnal.gov. When that fails a MX record is used to discover that the mail gateway system is the way in and it is then accepted for delivery.

SPAM Tagging

All incoming mail is routed through the SPAM tagging subsystem. Based on a combination of PostFix and SpamAssassin the mail is evaluated as potential SPAM using the rules defined inside SpamAssassin and the responses from DNS queries sent to public access RBLs (Real Time Blackhole Lists). Any mail that passes through SpamAssassin has X-Headers added to the message to shows its ‘score’. If the message is determined to be SPAM then a X-SPAM-Flag header is added with its value set to Yes. This flag can then be used by any client that supports filtering of messages based on headers to folder the mail for later reading rather than have a cluttered Inbox.

While not 100% effective user response has been very positive.

MTA

Once the mail has been processed by the SPAM tagging system it is handed off to the MTA. At this point the delivery destination is determined by a LDAP lookup and then the message is checked with Sophos AntiVirus. Sophos stops approximately 95 to 98 percent of the viruses that get to Fermilab via email. Any message that is determined to have viral content is not delivered. It is removed from processing. Neither the sender or the intended recipient is notified.

The Sophos definitions are updated two ways: The first is via cron every other hour. The second is triggered by email from Sophos that a new definition is available.

The MTA is also used as the SMTP server for the desktop clients and as an authenticated SMTP server for users who travel to allow relaying of mail.

The MTA processes an average of 800,000 to 1,200,000 messages per week.

Symantec AV

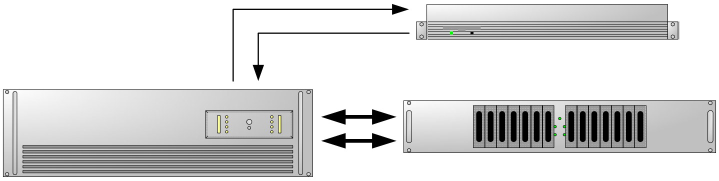
As mentioned in the MTA section Sophos is approximately 95 to 98 percent effective in removing viral content. In previous implementations of our IMAP and POP services we used Symantec AntiVirus for Gateways on the IMAP or POP server to catch any viruses that made it past Sophos. As we changed the design of the IMAP services we decided to implement Symantec AV as a service for all mail that comes through the gateways.

This implementation has resulted in nearly all viruses being caught before they reach the users mailbox. The Symantec definitions are updated every other hour via a scheduled job.

After being scanned the mail is returned to the MTA for delivery to the destination mailbox or list.

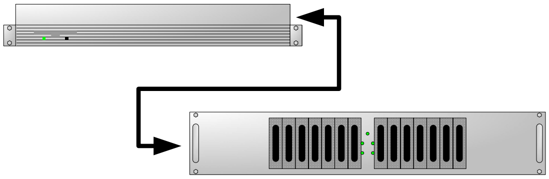
IMAP Services

IMAP is the preferred way for users at Fermilab to receive mail. It is a centrally managed and supported service. Users are not restricted to a particular client and a webmail interface is available for those who travel. All user information is stored in redundant LDAP servers and the users mail resides on storage available via two different paths. Users can request higher quotas for mail retention. Server side filters are also supported to help organize mail. We currently have approximately 3000 users with over 150GB of mail



POP Services

POP is still used at Fermilab but the number of active accounts is dwindling. User s are not restricted in the client that is used. Quotas are strictly enforced and a webmail interface is not available.



ListServ

ListServ is used to manage over two thousand mailing lists used at Fermilab by our users and collaborators around the world. For lists that are archived a web interface is available to view the archives. Once created the lists are managed by the list owners.

ListServ processes over 24,000 list messages weekly. These messages are distributed to over 325,000 email addresses.

UNIX/Linux Servers

There is no restriction on users receiving mail on their personal UNIX/Linux desktop. Many users do this and are very happy with managing their own server.