

WHITE  
PAPER

The Complete  
Internet Mail  
Solution



TABLE OF CONTENTS

**The Complete Internet Mail Solution**

Executive Summary . . . . .	2
Email: Landscape and Trends . . . . .	2
A New Paradigm in Email . . . . .	2
The Challenge: Expanding Requirements . . . . .	3
Controlling the Mail System . . . . .	3
Expanding the System's Capabilities . . . . .	3
Providing Reliable, Highly Available Service . . . . .	4
The Bottom Line Solving Real Business Problems . . . . .	4
New Requirements Demand a New Solution . . . . .	5
The Need For a New Solution . . . . .	5
Sendmail, Inc.: Grown Beyond its Roots . . . . .	5
Product Lines . . . . .	5
Products . . . . .	6
Internet Email – Common Elements . . . . .	6
The Fundamentals of Internet Email Architecture . . . . .	6
Message Routing and Delivery . . . . .	7
Message Storage and Access . . . . .	8
Extended Message Access . . . . .	8
System Services and Administration . . . . .	8
Hardware and Operating Environment . . . . .	9
Sendmail Mailcenter – A Comprehensive Solution . . . . .	9
Introducing Sendmail Mailcenter . . . . .	9
Email Routing and Delivery – The Sendmail Switch Product Line . . . . .	10
Message Routing and Delivery . . . . .	10
Securing Email Service . . . . .	10
Network and Data Security . . . . .	11
Email Policy Enforcement . . . . .	12
Email Storage and Access – Sendmail Advanced Message Server (SAMS) . . . . .	13
Sendmail Message Access Proxy . . . . .	13
IMAP Server . . . . .	13
POP Server . . . . .	14
Authentication . . . . .	14
Extended Message Access – Sendmail Mobile Message Server (SMMS) . . . . .	14
Webmail and Wireless Access . . . . .	14
System Administration . . . . .	16
Managing the MTA . . . . .	16
Managing the Message Store . . . . .	16
Sendmail – The Ideal Email Solution . . . . .	17
Planning for a Sendmail Deployment . . . . .	17
Conclusion: Comprehensive Email Solution . . . . .	19



**SENDMAIL®**  
THE FULL POWER OF EMAIL

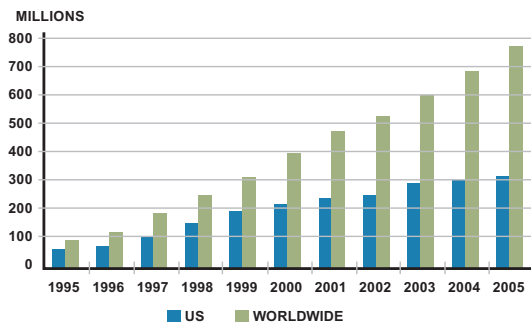


This white paper details the changing requirements for successful messaging systems, describes the elements of a distributed messaging architecture and presents the benefits of Sendmail's comprehensive email solutions. This document — intended for IT managers, system administrators, and CIOs — also examines the technical and business considerations in planning, sizing and deploying a Sendmail architecture.

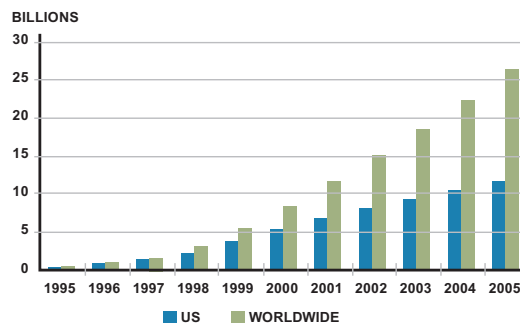
## Email: Landscape and Trends

### A New Paradigm in Email

The future of email is on the horizon — and with it, a new paradigm in messaging. That future will bring more of everything, from user accounts and message volumes to government regulations and security threats. In 2000, the worldwide number of emails sent on an average day hit the 10 billion mark; by 2005, this figure will more than triple to reach a staggering 35 billion. Along with this explosion in message volume and the correlative increase in active users of email, Internet messaging systems will face greater complexity and more rigorous demands at every level.



U.S. and Worldwide Email Mailboxes, 1995-2005 <sup>(1)</sup>

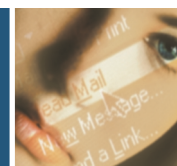


U.S. and Worldwide Email Volumes, 1995-2005 <sup>(1)</sup>

The rapid evolution of Internet messaging is driven by a complex set of forces:

- *The indispensable role now played by email in both business and personal life — such that many businesses would rather lose their phone service than lose their mail server*
- *The huge increase in the numbers of email accounts and messages sent*
- *Dramatic changes in message size and format, driven by the pervasive use of email to send practically anything to practically anyone, anywhere — from web pages and pictures to spreadsheets, slide presentations, audio, video and multimedia files*
- *Legislative, liability and security issues that require providers of messaging services to monitor and control the flow and content of messages with increasing precision*
- *The expectation by users that messages will be accessible and easily manageable anytime, anywhere, via any device*
- *An evolution in information technology that has made the Internet the common platform of choice, and made open standards the best way to leverage that platform*

<sup>(1)</sup> Source: "Email Usage Forecast and Analysis 2000 — 2005" Report # W23011, IDC, Sept. 2000



- *The drive to consolidate hardware while ensuring flexibility, scalability, manageability and quick, easy deployment of new or expanded services*
- *The bottom-line business requirement that messaging solutions be efficient and cost-effective, yet flexible, scalable, reliable and fast*

This rapid, multidimensional evolution means that messaging technologies must be chosen for their ability to meet tomorrow's requirements, not just today's. "Like a heavy rain, escalating email usage can be a blessing or a curse," observes Mark Levitt, research director for IDC's Collaborative Computing program, "depending on how prepared we and our environments are for it." A key element of that preparation is to understand the importance of the messaging architecture in meeting the challenges tomorrow's email systems will face.

## The Challenge: Expanding Requirements

These challenges come at a time of heightened competition for enterprises and service providers — and, consequently, even more intense pressure on their IT departments to deliver more for less. This pressure translates to three key imperatives: the need to maximize control, both of the mail stream and of the messaging system itself; the need to accommodate rapid growth in capacity, services and infrastructure complexity without sacrificing performance and quality of service; and the need to provide highly reliable "always on" messaging to a user base whose expectations are rising dramatically over time. To meet these demands — while still turning a profit — requires sound strategy, robust technology and a messaging architecture that supports and incorporates both.

The demands on today's messaging systems — imposed by users and system administrators, legislators and regulators, spammers and virus writers, corporate executives and shareholders — are daunting:

### Controlling the Mail System

- *Network and data security – The system must protect against viruses, spam and intrusion while providing secure access to local and remote authorized users.*
- *Policy enforcement – The system must comply with regulations, protect confidential or sensitive data, and limit liability by enabling comprehensive, policy-based monitoring and control of data passing through the mail stream.*
- *System administration – Administrators need robust, usable interfaces and tools for installation and configuration; provisioning and migration; secure, delegated account and data management; monitoring and reporting; and backup and recovery.*

### Expanding the System's Capabilities

- *Scalability – The system must be highly scalable — scaling rapidly, incrementally and cost-effectively without degradation in performance, usability, or manageability.*
- *Access – Users expect anytime, anywhere message access from a diverse and growing collection of devices and interfaces, with a consistent view of messages from any device.*
- *Integration – The messaging architecture must be flexible and modular, using open standards and protocols to mediate between heterogeneous elements and provide open interfaces to integrate new technologies, networks and user bases.*



**Providing Reliable, Highly Available Service**

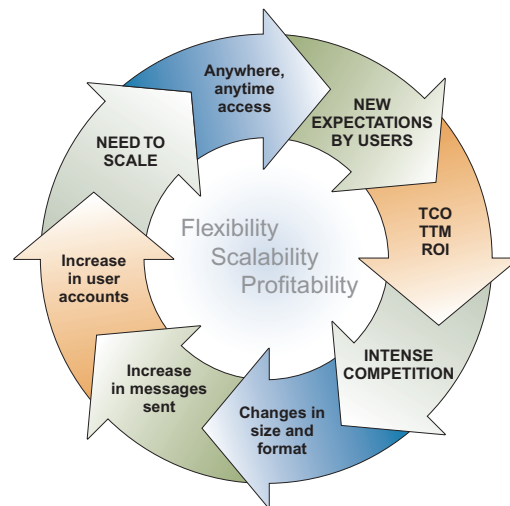
- *Uptime – Subscriber expectations and productivity demands make consistent, constant service a key requirement. "Five nines" (99.999 percent) availability may be overkill, but downtime — planned or not — should be nearly imperceptible to the user to avoid customer dissatisfaction, lost productivity and consequent churn.*
- *Message delivery – Data integrity is key, including reliable delivery of both message text and attachments. Email’s mission-critical role makes message loss intolerable to business users and unacceptable to service provider subscribers.*
- *Backup and recovery – In case of outages and failures, the system should fail gracefully, with robust backup and restore capabilities to prevent data loss and enable quick recovery with minimal downtime.*

**The Bottom Line: Solving Real Business Problems**

This new landscape and its expanding requirements demand an Internet messaging architecture and technologies that will provide a solid foundation for business success. Besides meeting technical requirements, the messaging system must also measure up to fundamental business metrics: time to market, customer satisfaction, efficiency, productivity and ROI — in short, profitability. Though not always foremost in a working system administrator’s thoughts, these measures remain the ultimate basis for measuring the success or failure of the technologies that the system administrator deploys and manages. Similarly, real-world business events such as mergers and acquisitions have a direct and dramatic impact on IT personnel, giving them a personal stake in deploying open, flexible, easily integrated systems whenever possible. And with executives (and the investors they represent) scrutinizing departmental P&L more closely than ever, efficient systems with a clear roadmap for growth make IT budgets easier to justify.

The one thing that continues to grow in this difficult economic climate is the volume of email. Gartner projects that for businesses, the number of mailboxes is growing at 40 percent per year, and that the size of the average message is also increasing by 40 percent annually — a combined increase of 275 percent in bytes per year.<sup>(2)</sup> If that hasn’t broken a company’s existing infrastructure already, it will within the next few years.

The bottom line for messaging system architects and administrators: the system must be conceived and deployed so that these overarching requirements of control, growth and reliability can be fully and continuously satisfied as the demands on the system change. To accomplish this (without periodically replacing the entire messaging infrastructure) requires an open, modular messaging architecture conceived to meet unforeseen needs — flexibly, scalably and cost-efficiently — and technologies designed and deployed to put those requirements into practice.



<sup>(2)</sup> Source: "Sizing the Email Mailbox: Less is More" Maurene Grey, GartnerGroup, Dec. 2000



## New Requirements Demand a New Solution

### The Need for a New Solution

In this rapidly evolving technology landscape, Sendmail believes that a successful email infrastructure must have certain characteristics:

- *A reliable, modular software architecture using open standards and protocols running on an equally reliable, manageable hardware and operating environment*
- *Architecture and technologies designed to address growth requirements, allow centralized management and meet unforeseen needs flexibly and effectively*
- *A system designed to address key business requirements — time to market, customer satisfaction, efficiency, productivity and ROI — for maximum cost-effectiveness*

This shared perspective is rooted in years of technological innovation and broad experience implementing real-world systems. On that basis, Sendmail offers customers a complete email solution that is scalable, flexible and high-performance.

### *Sendmail, Inc.: Grown Beyond Its Roots*

Sendmail, Inc. builds powerful and secure email systems for large enterprises and service providers that depend on email to run their business. Founded by *sendmail* author Eric Allman, the company is deeply committed to open Internet standards and is a principal driver in the continuing progress of Internet messaging architecture and technology — through its technological innovations, its worldwide user base, and its deep involvement in the IETF standards process.

Sendmail has played a central role in the evolution of email and the Internet from the very beginning. The *sendmail* Mail Transfer Agent (MTA), the de facto standard implementation of the Simple Mail Transfer Protocol (SMTP), has been the foundation of Internet messaging for more than 20 years and still powers more than 60 percent of the Internet's mail domains. Recently honored by the Smithsonian Institution for its contributions to the advancement of information technology, Sendmail, Inc. remains a leading contributor to the ongoing evolution of email and the Internet. Today, 84 percent of the Fortune 100 — including nine of the top ten corporations on the list — rely on Sendmail, Inc.

Sendmail, Inc. has built a strong business by delivering a comprehensive suite of email solutions; routing, storage and access servers products; consulting services, and support offerings that build on its unique expertise in Internet email. Today, Sendmail products include:

### *Product Lines*

- *Sendmail Mailstream Manager — Ensures the reliable and secure flow of business-critical email inside an organization and across the Internet while enabling content policy controls and creating a predictable model to scale the system. Email is scanned for viruses, spam and other malicious code, filtered against policy enforcement policies and transmitted through secure channels to its destination—all controlled from a central administration system.*
- *Sendmail Mailcenter — Combines all the components necessary to deploy a complete email system of any size.*
- *Sendmail High Volume Mail — A high performance, fault-tolerant email messaging system for businesses that send large volumes of unique messages to opt-in subscribers.*

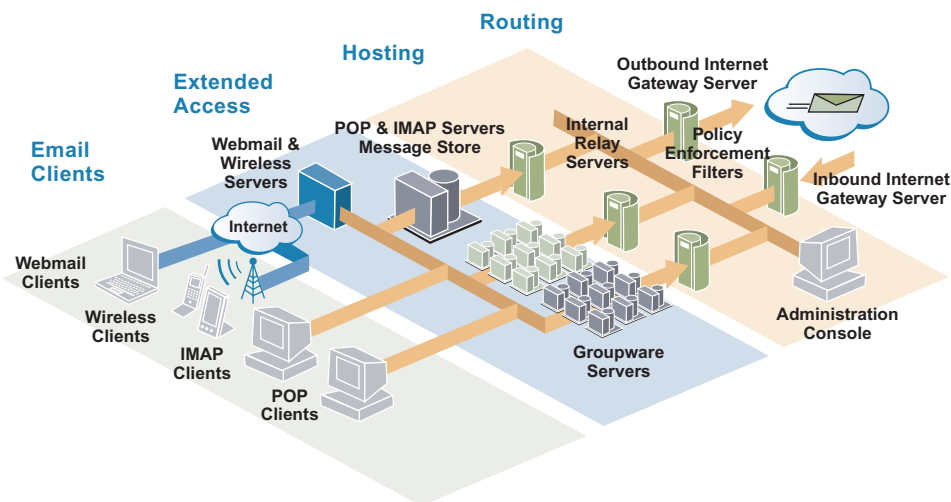
## Products

- *Sendmail Switch* — Provides the email infrastructure for routing and managing Internet mail, enabling configuration, deployment, management and monitoring of a multi-node mail traffic topology from a single central console.
- *Sendmail Advanced Anti-Spam Filter* — the only intelligent spam filtering solution that allows your organization to proactively monitor, manage and, if necessary, filter unauthorized inbound, outbound and intra-company email.
- *Sendmail Anti-Virus Filter* — Screens incoming and/or outgoing mail for viruses at the server level using McAfee's Olympus engine.
- *Sendmail Policy Enforcement Filters* — Attachment Filter, Message Copier and Message Appender provide precise control of incoming and outgoing content and the ability to limit message size.
- *Sendmail Advanced Message Server* — A high-performance mailbox hosting and POP/IMAP access server made infinitely scalable by the inclusion of a robust, secure message access proxy.
- *Sendmail Mobile Message Server* — Provides Webmail and wireless access.

## Internet Email — Common Elements

### The Fundamentals of Internet Email Architecture

The essential task of a messaging system is straightforward: to enable users to send and receive email, dispatching their outbound messages and placing their inbound messages in a mailbox message store where recipients can retrieve them. In practice, this three-part process (message data sent, stored and retrieved) translates to a set of tasks reflecting the complex, sometimes conflicting demands on the system — which must be flexible and open to accommodate the evolving realities of Internet mail and the varied needs of users, administrators and profit-minded executives, yet also provide tight control so that both message data and the network itself can be secured and monitored.



Distributed Messaging Architecture - Common Elements



The functional elements of a messaging system fall into three basic categories:

- *Message routing and delivery (including security and policy enforcement)*
- *Message hosting (message storage and POP and IMAP mailbox access)*
- *Extended message access (Webmail and wireless access to mail accounts)*

In addition, the underlying hardware and operating environment (whether the system is distributed across multiple machines or consolidated on one large-scale machine) is a crucial aspect of the messaging system.

## **Message Routing and Delivery**

*Routing Servers* — Email travels between servers (in this context, a server is a software application or daemon with a specific function in the architecture) via the Simple Mail Transfer Protocol (SMTP), a store-and-forward protocol that operates reliably even across high-latency networks or intermittent sender-recipient connections. Routing MTAs fulfill several roles:

*Inbound Gateway Server* — The inbound gateway server (or boundary server) is the system's front door, welcoming "friendly" correspondence while protecting against external threats. Situated either on the firewall or in a DMZ connected to the firewall, but isolated from the internal network, it has two main tasks: (1) to examine inbound messages against specified criteria (to eliminate security threats or policy infringements) and take action as appropriate (such as rejecting spam); and (2) to hand off accepted messages to the internal relay host for routing to their destinations.

The gateway server plays a crucial role in both network and data security (service availability, virus and spam control, authentication and encryption) and policy enforcement.

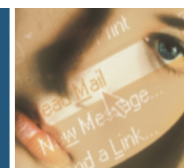
*Internal Relay Host* — A relay host (or smart host) receives messages from other SMTP servers and resolves each recipient's address using various internal and external resources. The smart host queries them to match the current email address against the DNS (for domain names) and LDAP (for addresses and host domains, alias lists and other internal tables that map or expand the current address).

Because the smart host is often aware of user accounts, it should not be directly exposed to the Internet. Both gateway servers and smart hosts are typically deployed to avoid jeopardizing user account information.

*Outbound Gateway Server* — Besides handling outbound SMTP traffic, the outbound gateway server may monitor those messages to ensure that nothing — proprietary or sensitive information, or texts requiring disclaimers — leaves in violation of policy.

*Fallback MTA* — A fallback MTA handles SMTP traffic (inbound or outbound) that cannot be passed on to its next destination immediately — for instance, if the MTA designated in a DNS MX (Mail Exchange) record is temporarily offline — to ensure service availability and avoid tying up outbound SMTP servers.

*Filters* — Monitoring message envelopes, headers and/or bodies for elements matching specified profiles; filters are used to block spam, viruses and other malicious code; to modify message text (by appending a disclaimer, for instance) and to archive messages.



## Message Storage and Access

*Storage and Access Server* — The hosting server is the core of the messaging system, where messages are received, stored and retrieved. It has six main functions:

- To receive inbound messages and inject them into the message store
- To store message data securely, reliably and efficiently
- To authenticate users prior to message store access
- To provide local and remote message access via POP and IMAP, the two main Internet standard protocols for email retrieval
  - IMAP (Internet Mail Access Protocol) mail is generally stored in server-side folders. Messages are retrieved in pieces (letting users scan message headers before downloading bodies and attachments) and synchronized to client-side folders as users request.
  - POP (Post Office Protocol) mail is usually stored in client-side folders after being downloaded from the user's server-side inbox. Messages are retrieved in whole (in the order received) as the user checks their email, and then typically deleted from the server.
- To securely delegate administrative capabilities to site and domain administrators
- To securely delegate message, folder and account management capabilities to users

*Access Proxy Server* — A multiplexing access proxy mechanism enhances scalability and security without introducing new complexity to clients — for instance, allowing multiple back end message stores while giving clients a single, consistent front-end destination server — enabling seamless integration and seamless transitions for provisioning, migration and back-end updates and upgrades.

## Extended Message Access

*Extended Access Servers* — Webmail (HTTP) and wireless (WAP) email access servers provide anytime, anywhere message access and give users a consistent, synchronized view of their messages from multiple client devices. Webmail is also a lightweight and cost-efficient way for an organization to extend email service to workers whose day isn't spent in front of a desktop computer — for instance, using kiosks to provide Webmail to workers in a retail setting or on the factory floor.

## System Services and Administration

*Other Services* — The messaging system will generally also leverage other services internal or external to the system, such as DNS (an Internet service that translates domain names into corresponding IP addresses) and LDAP (Lightweight Directory Access Protocol, an open Internet standard protocol that enables almost any application on any platform to obtain directory information, such as email addresses and public keys, from an LDAP server).

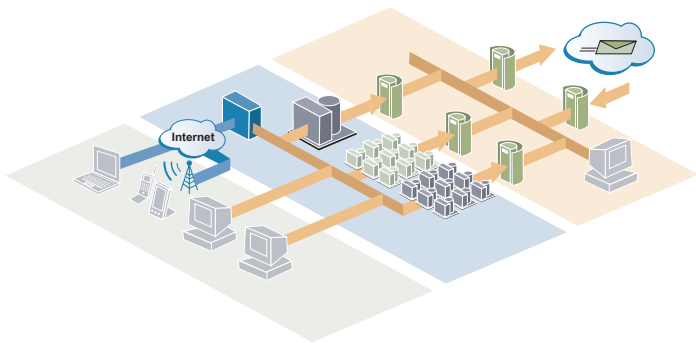
*System Management* — The architecture must also provide for ongoing management of the messaging system. Administrators need robust, usable interfaces and tools to install and configure messaging components; for secure, delegated account and data management; for provisioning and migration; and for backup and recovery. Administrative interfaces should allow for secure, simplified, centralized management of MTAs, including gateway servers, smart hosts and other internal routers. Interfaces for the message store and access servers should simplify management of accounts and other data, and should be self-contained, extensible and modular to underlying interfaces for increased flexibility.



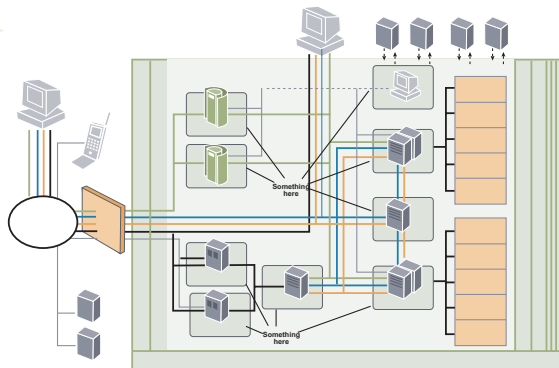
## Hardware and Operating Environment

*Computing Platform* — The hardware and operating environment are key considerations in planning and implementing a messaging architecture. The platform choice has a profound effect on performance, availability, scalability, security and manageability — not to mention such fundamental business considerations as cost-efficiency, user experience and deployment time.

*Distributed Versus Consolidated Environments* — The functional elements of a messaging architecture — MTAs, hosting servers, directory servers and so on — have traditionally been deployed across multiple servers in a networked environment. The number of servers deployed in a distributed networked environment will depend on scalability and provisioning issues, security concerns, administrative and business requirements and similar considerations.



*Traditional Distributed Messaging Architecture in a Networked Environment*



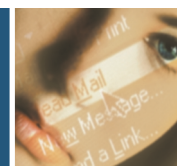
*Consolidated Messaging Architecture on a Single Large-Scale Server*

An alternative approach is to consolidate the entire messaging architecture on a single piece of hardware. Such an approach transposes the functional elements of the messaging system — message routing, message hosting and extended access — to a collection of virtual servers residing on one high-capacity server and communicating via internal system buses.

## Sendmail Mailcenter — A Comprehensive Solution

### Introducing Sendmail Mailcenter

Sendmail Mailcenter addresses the new messaging landscape, providing unprecedented levels of scalability, flexibility, reliability and control even as it reduces cost and administrative complexity. Sendmail Mailcenter is pre-configured and performance-matched so that you



receive a well-integrated, scalable, easily managed solution that provides the functionality you need.

In the Sendmail Mailcenter, the functional categories of message routing (including security and policy enforcement), message hosting and extended access are represented by Sendmail's software products. What follows is a quick survey of features for Sendmail in each of these functional areas.

### **Email Routing and Delivery — The Sendmail Switch Product Line**

The following section describes the features and advantages of Sendmail Switch. The Sendmail Switch product line includes the Multi Switch Administration Console, Sendmail Switch Administration Console and the versatile, flexible Sendmail Managed Switch MTA.

Sendmail Switch has six main functions:

- *Exposing SMTP service, while securing the port and the server itself*
- *Managing relay and communication privileges passing through the Internet gateway*
- *Managing message content passing through the Internet gateway*
- *Accepting responsibility for message delivery (queuing messages to be delivered)*
- *Interpreting, resolving and rewriting addresses*
- *Evaluating each message and delivering it to its next destination*

These tasks fall into three general categories: message routing, security and policy enforcement.

#### ***Message Routing and Delivery***

Sendmail Switch provides all of the routing functions discussed above — receiving messages, resolving the domain names and routing them toward their destinations, invoking forward and vacation files as required.

In addition, Sendmail Switch handles address rewriting. The interpretation, resolution, and (where necessary) rewriting of email addresses entails support for virtual hosting, aliasing, masquerading and directory lookups — generally involving DNS Mail Exchange (MX) records, as well as the use of LDAP directories for both message routing and user authentication.

Sendmail Switch's multiple queues provide a significant performance and scalability advantage. Its efficiency, reliability, security and liberal acceptance of mail from other systems — combined with its scrupulous adherence to open standards upon handoff — make it a complementary product to groupware applications. In fact, it often provides a standards-based "glue" for integrating diverse elements of a heterogeneous messaging environment.

#### ***Securing Email Service***

Sendmail Switch at the Internet gateway provides both network and data security (spam control, virus control, authentication and encryption) and policy enforcement.



### *Network and Data Security*

Sendmail Switch at the gateway is the messaging system's front line against external threats. Leading the list:

*Spam.* Sendmail blocks spam at the gateway, as well as minimizing the impact on the hosting server of legitimate multi-recipient mailings. Sendmail Switch has many ways to identify and exclude spam based on header info, including:

- *Flexible, powerful, anti-spam rule sets*
- *Requiring fully qualified domain names for sender addresses outside the network*
- *Limiting the maximum size and number of recipients per message*
- *Customized pattern matching to identify a common phrase or address in the header so as to catch suspect messages*

These and many other anti-spam features are easy to configure and tune using the Sendmail Multi Switch Administration Console.

*Unauthorized relaying.* Sendmail Switch lets legitimate users relay outbound messages from outside the firewall while preventing unauthorized use. Spammers view every open relay as an invitation to hijack the unwary mail server — stealing bandwidth, cycles and disk space, incurring no delivery cost, and leaving system administrators to clean up the bounced mail that can lead to blacklisting, bad press and furious users. Sendmail Switch offers features to keep spammers out while letting legitimate roaming users relay email through their primary servers:

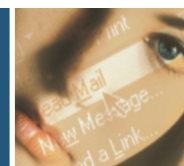
- *It turns off "promiscuous relaying" (relaying without limitation) by default*
- *It invokes an anti-spam access database and lookups for DNS-based blacklisting of known spammer sites*
- *It invokes specific lists of domains, hosts and users allowed to use the relay (sending capability) services and blocks spammers from "stealing" that service*
- *Finely tuned access database lookups allow very specific anti-spam checks, such as allowing mail relaying to a specified site without allowing relaying from that site*

*Unauthorized access.* Sendmail provides a flexible, secure authentication framework, as well as granular control of folder access permissions in the message store. Sendmail leverages a complex subset of capabilities to carry out these tasks, including:

- *Transport Layer Security (TLS) authentication and encryption to enable a secure channel of communication for only those privileged to use it*
- *SMTP AUTH username and password authentication prior to sending mail*

TLS and SMTP authentication make life easier for mobile users and administrators and tougher for spammers. SMTP AUTH adds an authentication step to the mail exchange process, providing a powerful way to control relaying with maximum flexibility. By enabling relaying based on the submitting user instead of the submitting host, it helps roaming users submitting mail from untrusted sites, while giving system administrators even tighter control. TLS, the new Internet standard for authenticating and encrypting transmissions across open networks (and successor to Secure Sockets Layer, or SSL), uses digital signatures to authenticate the parties to an email exchange, then encrypts the SMTP session that follows, enabling encrypted server-to-server communication.

Sendmail Switch offers features to keep spammers out while letting legitimate roaming users relay mail.



*Network intrusion.* Sendmail Switch blocks attempts by intruders to get special permissions or elevate their privileges via the mail system.

### ***Email Policy Enforcement***

Sendmail Switch at the Internet gateway also plays a crucial role in policy enforcement: anti-virus protection, protecting confidential or sensitive data, complying with government regulations, limiting exposure to legal liability and securing transmission of sensitive information over the public Internet. Such policy implementations can entail:

- *Anti-virus scanning of inbound and outbound messages to detect and cleanse MIME attachments and uuencoded message bodies*
- *Scanning inbound and outbound messages for specific attachment types*
- *Copying and archiving messages, globally or selectively (for instance, by department), for periodic review by compliance officers or outside regulatory agencies (for example, to comply with SEC requirements)*
- *Appending disclaimers to messages to protect against potential liability*
- *Blocking proprietary, confidential and sensitive data before it leaves the network*
- *Blocking outbound messages that breach policies, such as spam or pornography*

Such tasks — along with security functions like spam control and virus scanning — require a comprehensive and efficient approach to monitoring, evaluating and acting on the data that flows through the messaging system. Sendmail's Policy Enforcement Filters — leveraging a multithreaded API built into the Sendmail MTA — provide that approach.

The Sendmail Policy Enforcement API enables an external process to act on messages as they flow through the MTA, providing a safe, flexible way to monitor and filter SMTP traffic within a Sendmail process without altering the executable. This alleviates the heavy SMTP transaction cost inflicted when messages pass between the MTA and a succession of external applications, such as virus filters or archiving software. The API delivers connection, envelope and header information simultaneously to each plug-in, and then passes the message body through each application. This multitasking approach improves architectural scalability and diminishes the performance degradation that traditional systems incur when processing each message sequentially through each filter. The result is faster delivery and fewer applications to manage — a solution marrying speed and robustness with flexibility and automation. Available Sendmail policy enforcement plug-ins include:

- *Anti-Spam Filtering* — *Scans the header, message body and attachments to eliminate unsolicited email*
- *Attachment Filtering* — *Blocks or discards unwanted MIME attachments by scanning email messages by file extension, file name, MIME type and subtype, or by sender's email address incoming messages*
- *Anti-Virus Filtering* — *Utilizes the McAfee Olympus virus scanning engine to detect and cleanse MIME attachments and uuencoded message bodies*
- *Message Copying* — *Scans SMTP-based traffic passing through the MTA, copying messages that match specified criteria to a designated location*
- *Message Appender* — *Adds a disclaimer or other text (as simple text or MIME-encoded) to messages matching a specified profile, often to limit liability*



The Sendmail Policy Enforcement API is an open API, enabling development of third-party and custom applications, both proprietary and open source.

### **Email Storage and Access — Sendmail Advanced Message Server (SAMS)**

The architecture and component technologies of Sendmail Advanced Message Server (SAMS) are specifically designed to support rapid growth while maintaining consistent user experience, performance and reliability.

SAMS scales comfortably to hundreds of thousands of users and supports millions of users. The sophisticated indexing and caching capabilities of SAMS' fast, multithreaded POP and IMAP access servers optimize performance and maximize concurrency.

SAMS' partitionable message store can be spread easily across multiple disks and disk arrays, and storage can be added as needed, making the system easy to scale as requirements increase. SAMS' online storage reconfiguration lets administrators add capacity without downtime; dynamic data updates allow administrators to add users without downtime. Performance can be enhanced by adding cache and/or solid-state RAID and by tuning the storage configuration.

The message store's streamlined database is optimized for messaging, eliminating the unnecessary overhead imposed when a general-purpose SQL database is used to store message data. If a message is sent to multiple recipients, only one instance of that message resides in the message store, minimizing disk usage and the effects of large recipient lists on the server. Similarly, multiple-recipient messages are cached on first access to avoid I/O bottlenecks. More generally, the system's efficient design allows for consolidation of resources and maximizes performance.

SAMS provides full support for secure hosting of multiple (virtual) domains, and message store administration can be fully delegated by role (site administrator, domain administrator, end user) and by domain.

Highlights of each hosting component are listed below:

#### *Sendmail Message Access Proxy*

Sendmail Message Access Proxy is a scalable, high-performance POP and IMAP proxy server used to multiplex several back-end message stores into one logical front-end server. The proxy server extends Sendmail's hosting capacity horizontally across multiple virtual servers to support millions of users.

At its simplest, a proxy session is a pass-through connection where message retrieval occurs between a back-end message store and a mail client (MUA). The proxy can also be deployed across multiple virtual servers on the front end. Where multiple instances of the proxy are deployed, any instance of the proxy can communicate with any instance of the message store.

#### *IMAP Server*

The fast, highly scalable IMAP4 server — along with the message store itself — is the heart of Sendmail Advanced Message Server. It fully implements the IMAP4rev1 spec, giving

Sendmail Advanced Message Server scales comfortably to hundreds of thousands of users and supports millions of users.



users and administrators fine-grained control over mailboxes and messages in the message store. Key capabilities include:

- *Sophisticated indexing and caching capabilities that provide rapid message access, reduce network bandwidth load and optimize use of memory and CPU*
- *Partial body fetches to give users fine-grained control over message downloads across network or dialup connections (letting them view message headers without downloading bodies and attachments, or download only selected attachments in any sequence desired), reducing bandwidth load and speeding remote access*
- *Unique message identifiers that persist across sessions, letting clients resynchronize message state information from a previous session or from a different device*
- *Complete MIME support to ensure correct handling of complex messages — including bodies and headers in non-US character sets (crucial for global organizations) and non-textual message bodies (such as audio, video, images and HTML) with inline graphics*
- *Delegated folder management to let users and permitted administrators manage IMAP folders, creating, deleting, moving and modifying them as desired*
- *Hierarchical folders, allowing users and groups to embed multiple subfolders within a folder and enabling user groups to organize information intelligibly for fast, easy retrieval or review*

### **POP Server**

Sendmail Advanced Message Server's fast, standards-conformant POP3 server uses the same high-performance message database as the IMAP server, ensuring quick, reliable downloads. It supports all POP3-standard functionality (RFC 1939) as well as the full suite of POP3 extensions, including integration of the Internet-standard SASL authentication framework.

### **Authentication**

Sendmail Advanced Message Server's message store supports a wide selection of runtime-configurable authentication methods. An internal database supports the Internet-standard SASL authentication framework (including CRAM-MD5, DIGEST-MD5 and PLAIN). An authentication server (authproxyd) uses a plug-in architecture to provide non-SASL authentication (including Kerberos v4, ANONYMOUS and GSSAPI) for POP and IMAP clients that don't understand SASL. Authproxyd can be configured to migrate users automatically from an insecure mechanism to a more secure one; it also enhances security by isolating all code requiring superuser privileges into a single process. In addition, Sendmail Advanced Message Server provides full support for LDAP-based authentication.

Once users have authenticated, Access Control Lists (ACLs) permit or restrict access to messages and folders in the message store based on the user's level of authorization, giving site and domain administrators flexible, effective control of folder accesses for varied operations.

### **Extended Message Access — Sendmail Mobile Message Server (SMMS)**

#### **Webmail and Wireless Access**

Sendmail Mobile Message Server (SMMS) extends Sendmail Advanced Message Server's POP and IMAP access to web browsers and wireless devices, providing POP and IMAP messaging via a web-based interface. Users can read, compose, save, delete, forward and



reply to messages from wherever they happen to be, plus IMAP support gives users a consistent view of messages from multiple access devices. Since Webmail and wireless components run on the server side, there's no client software to install, minimizing configuration and support overhead. Besides giving users anytime, anywhere access, SMMS provides an ideal way for an organization to extend email service to workers, customers and affiliates with limited access (or no access at all) to a desktop computer — for instance, using kiosks to provide Webmail to workers in a retail setting or on the factory floor.

The SMMS architecture itself maximizes scalability, reliability and availability. Its components scale across multiple virtual servers and processors using a "switchboard" load balancing architecture that scales to support even the largest installations, and there's no hard limit to the number of user interfaces per installation. SMMS runs on the same virtual server as the web server, passing HTML, email and the UI to the user's browser via HTTP. Since communications with the message store use standard protocols (POP3, IMAP4, SMTP), SMMS doesn't need to run on the same virtual server as the message store, and can easily expand service on one virtual server or across several virtual servers as the number of users grows. The benefits of this horizontal scalability include:

- *Internal load balancing* — Users are automatically routed to virtual servers with the lightest user load, enhancing speed of access and system scalability.
- *Fault tolerance* — If a software process crashes, user session information is handed off for rerouting to another virtual server, allowing uninterrupted service.
- *Failover* — Session information persists across virtual servers. In case of failure, the session is passed to another virtual server for uninterrupted service.

The flexible, templated Webmail interface is easily customized for branded services, banner advertising and third-party features (such as calendars and search). SMMS can retrieve individualized configuration parameters for each user, based on an external LDAP database, or, if preferred, define parameters consistently for all users — enabling finely targeted customization of the UI. Support for multiple domains and for multiple UIs and languages makes it easy to present distinct domains with different corporate looks and feels and to internationalize the UI for specific domains and users.

Administrative features are designed for flexibility and low overhead. Text configuration files enable manual control of critical processes and daemons, and SMMS incorporates a "heartbeat" monitor for critical processes. Full LDAP integration, including a central LDAP directory, enables lookup of a user's mail "home" (useful in large installations with multiple message stores) and lookups into a corporate directory (essentially a "white pages" function for the enterprise).

Sendmail Mobile Message Server's wireless capability allows message access from any wireless browser that supports the Wireless Access Protocol (WAP). No additional equipment is needed for wireless access — the administrator simply copies an additional set of files during configuration.

Sendmail Mobile  
Message Server  
gives users  
anywhere, anytime  
access to email.



## System Administration

The Sendmail Multi Switch Administration Console allows administrators to oversee their email operation easily. A browser-based user interface provides access to all messaging services over secure TLS-encrypted sessions.

### *Managing the MTA*

The Sendmail Multi Switch Administration Console centralizes monitoring of multiple instances of the Sendmail Switch Managed MTA, storage of MTA data and generation of aggregate reports for MTA clusters. The administration console provides queue control, a granular reporting system and system monitoring tools. In addition, it includes straight-forward but extremely flexible interfaces and tools to facilitate setup, configuration, migration and testing — speeding deployment and enabling administrators to scale the system rapidly as increased demand requires.

This centralized management and administration architecture:

- *Reduces the cost of system administration and management*
- *Reduces support cost through downtime prevention*
- *Eases consolidation of information and provides clear, comprehensive data for performance tuning*
- *Alerts administrators to potential performance bottlenecks before problems arise*

In addition, robust TLS-based security features allow administrators to monitor the messaging network in a secure environment that won't compromise critical information.

### *Managing the Message Store*

Sendmail Advanced Message Server gives administrators powerful management tools that are easy to use and easy to delegate, using a browser-based interface to manage common tasks in the message store. Any modern browser provides fully secure remote access to all needed administration tasks, including:

- *Creating and deleting users of all administrative levels (and all associated data)*
- *Adding, deleting and administering domains*
- *Suspending and enabling users*
- *Adding, removing, or modifying user rights*
- *Setting or modifying account quota limits*
- *Viewing and editing quota usage and IMAP folder properties*
- *Creating shared mailboxes*
- *Altering user and administrator levels*
- *Allowing end users to create passwords*

SAMS' web interface allows secure delegation of domain and account management tasks — both by domain (or subdomain) and by role — to enhance the administrative scalability of very large or complex sites. For instance, management of each virtual domain hosted in a given message store can be securely delegated to its own domain administrators — to whom other domains hosted on the same server will be invisible and inaccessible — while retaining

A secure administration console centralizes the management of mail flow through multiple Sendmail Switches.



overall site management authority for site administrators (who have access to all domains hosted across the messaging system).

An extensive, easily customized toolset is available at the command prompt. Administration tools are self-contained (so no additional software is required), fully extensible (so tools can be integrated into existing site account maintenance mechanisms) and modular to underlying interfaces (so components can be replaced where needed).

Other administrative capabilities include:

*Mailbox Quota Management* – Quotas limit the disk space a user's messages can occupy, helping administrators manage system storage. Per user message quantities can also carry a quota, which is handy for low-capacity access devices like phones and PDAs.

*Bulk User Creation and Deletion* – The utilities provided allow quick creation of authentication and user accounts and quotas, as well as automatic batch creation of new users from external database records (HR records, for instance).

*LDAP* – Sendmail fully supports LDAP for authentication and routing and enables LDAP-based integration with external provisioning and authentication systems.

*Virtual domains* – Sendmail's hosting server supports multiple virtual domains with secure, delegated administration, making site management efficient and scalable.

### **Sendmail — The Ideal Email Solution**

Sendmail's modular architecture and basis in open Internet standards and protocols provide the flexibility to incorporate new technologies and meet unforeseen needs without compromising an organization's existing investment.

To obtain detailed recommendations for deploying Sendmail in your specific environment, contact a Sendmail sales representative.

---

## **Planning for a Sendmail Deployment**

To understand how best to deploy Sendmail, it is important to define what is needed from the messaging system, both now and over time. A few points to keep in mind while planning a messaging system are:

- *While the raw number of users does matter, sizing is not just a question of how many users must be supported, but of what they do and when: to measure the users' impact on the messaging system, it is important to profile the users behavior.*
- *Mail systems are ultimately better measured by the number of concurrent connections they support, not the number of mailboxes the system can accommodate.*
- *System configuration has an enormous impact on messaging performance — and, of course, user profiles influence system configuration choices.*

Profiling users is of paramount importance to properly identify and evaluate messaging requirements. It is essential to know both what user profiles the messaging system must support and what proportion of the users will fit into each of these profiles.



For example, questions should be asked about:

- *Access* — Will users use POP, IMAP, Webmail, wireless, or a combination of these?
- *Storage* — Will messages be stored on the server (typical for IMAP) or downloaded and then deleted (typical for POP)? What quotas will apply in each case?
- *Connection type* — Will users maintain a more or less constant connection to the server (typical for IMAP) or connect only intermittently (typical for POP)?

Other questions to consider when planning a messaging installation:

- *Numbers of users* — How many users of each type (user profile) will there be initially?
- *Message size and volume* — How many inbound and outbound messages will there be within a given interval? How big will they be on average? What extremes of message size and bandwidth rate must the system support?
- *Bursty traffic* — How much will message volume and concurrency vary over time? How intense will the peaks be?
- *Migration and provisioning* — What mail system (mailbox format) will existing users be migrating from? How will new users be created (e.g., from HR records)?
- *Growth curve* — What are the scalability targets? How many users are expected, and when? How will that growth be distributed among the various user profiles?
- *Profile migration* — To what extent are users expected to move from one usage profile to another (for instance, ISP subscribers upgrading from POP to IMAP or adding wireless message access, or a subset of employees switching from Webmail-only to IMAP)?
- *Security requirements* — What requirements exist with respect to spam blocking? Virus filtering? Control relaying?
- *Policy requirements* — What sort of policy enforcement capabilities are required, and at what points in the mail stream should they be implemented?
- *Message type* — Are there requirements related to particular MIME types or character sets? Will different MIME-type restrictions apply to different classes of user profiles? Will certain users or domains require support for non-US ASCII characters?
- *Prototyping* — Will a subset of users "test drive" the messaging system before its implementation for the entire user base?



## Comprehensive Email Solution

Sendmail offers an email solution that meets the needs of enterprises and service providers for new levels of control, scalability, flexibility and reliability.

Sendmail Mailcenter provides unprecedented control of the mail stream and of the messaging system, protecting against spam, viruses and intrusion while giving legitimate users secure message access. Sendmail's Policy Enforcement Filters, leveraging the unique API built into the Sendmail MTA, allow comprehensive policy-based control of data passing through the system to limit liability, scan for viruses, protect sensitive data and enable regulatory compliance and policy enforcement. Powerful, intuitive interfaces and tools make installation, configuration and account and data management easy and secure, lowering administrative costs and speeding deployment.

Sendmail Mailcenter is designed for fast, flexible growth, scaling to millions of users at extremely high levels of concurrency — quickly, cost-effectively and without degradation in performance, usability or manageability. Mobile messaging capabilities give users any-time, anywhere access from a diverse collection of devices and interfaces, with a consistent view of messages from any device. Sendmail's standards-based, modular architecture allows flexible integration of heterogeneous messaging environments (including groupware applications) and enables rapid assimilation of new technologies, networks and user bases.

Finally, Sendmail Mailcenter provides reliable, highly available service. Online storage reconfiguration and backup, dynamic data updates, a partitionable message store and powerful technologies keep downtime to a minimum. In the event of failure, robust backup and restore capabilities prevent data loss and enable quick recovery.

## CONCLUSION



WHITE  
PAPER

The Complete  
Internet Mail  
Solution



**SENDMAIL**®  
THE FULL POWER OF EMAIL

**Sendmail, Inc.**  
6425 Christie Avenue, 4<sup>th</sup> Floor  
Emeryville, CA 94608

510 594 5400  
[www.sendmail.com](http://www.sendmail.com)  
[sales@sendmail.com](mailto:sales@sendmail.com)

© 2002 Sendmail, Inc. All rights reserved. Sendmail and the Sendmail logo are registered trademarks of Sendmail, Inc. All other trademarks or service marks are the property of their respective companies.