

WHITE  
PAPER

Protecting Your  
Email Network

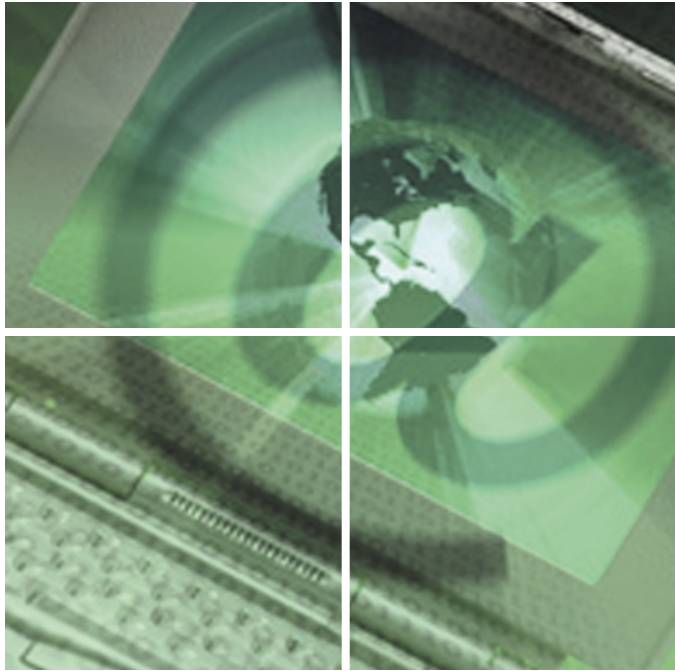


TABLE OF CONTENTS

Protecting Your Email Network

Executive Summary .....2

Risks of Relying on Groupware to Protect Internal Networks .....2

    Groupware Can Fail Under Increased Message Load .....3

    Relay Theft Exploits Company Resources .....3

    Denial of Service (DoS) Attacks May Disable the Network .....3

    Internal Information is Not Protected from the Internet .....3

    Heterogeneous Groupware Systems Can Cause Problems .....4

    Case in Point: Microsoft Exchange and Security .....4

Threats to Networks, Servers, and Content .....5

    Spam Puts Company Resources at Risk .....5

    Viruses Cause Data Loss and Cost Money .....5

    Single Points of Failure Can Disrupt Message Traffic .....5

    Unsecured Transmissions are Not Confidential .....6

    Unrestricted Content Can Cause Legal and Regulatory Problems .....6

Email Infrastructure Best Practices .....6

    Internet Gateway Server .....7

    Mail Hub .....7

    Local Email Server .....7

Sendmail Mailstream Manager .....7

    Mailstream Manager Overview .....7

    Mailstream Manager Components .....8

        Administration Console .....8

        Managed Switches .....8

        Anti-Spam Filter .....9

        Anti-Virus Filter .....9

        Policy Enforcement Filters .....9

        Directory Service .....9

Sendmail Mailstream Manager - Protecting Email Networks .....10

    Blocks Spam to Enhance Productivity .....10

    Protects Networks from Viruses Before They Enter the Organization .....10

    Blocks Relay Theft and DoS Attacks .....11

    Secures Internal Information from the Internet .....11

    Failover Protection Enhances the Reliability of Email Systems .....12

    Protects Information Sent Over the Internet .....12

    Facilitates Integration of Different Groupware Systems .....12

    Provides Control Over Content of Incoming and Outgoing Messages .....13

Business Benefits of Mailstream Manager .....13

    Maintains Reasonable Costs .....13

    Scales with Enterprise Needs in a Cost-Effective Manner .....14

    Centralized Management Saves Money on Administration .....14

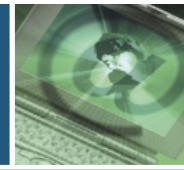
Conclusion .....14

Addendum .....15

    Advantages of Mailstream Manager Over Open Source *sendmail* .....15



**SENDMAIL**®  
THE FULL POWER OF EMAIL

**EXECUTIVE  
SUMMARY**

Businesses depend on email to communicate within their enterprises and with external customers, partners and suppliers. Gartner estimates that 40% of all business communications occur electronically. In just the past decade, email has replaced memos, faxes, dedicated document archiving systems, conferences and couriers as a communication device. Yet corporate email systems are vulnerable to threats that can interfere with their reliability.

Email systems are under constant attack from spammers and hackers who seek to steal bandwidth, capacity, or merely to disable the systems. Relay theft and denial of service attacks threaten network stability and can interrupt the flow of electronic communications. Security breaches, in which confidential information is compromised, present a potentially greater problem, although companies rarely speak about it because of embarrassment or to avoid negative publicity.

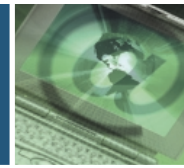
Groupware email products, which often contain confidential information such as employee lists, customer relationship data and other corporate knowledge, are especially vulnerable to security and management problems. Groupware is designed to facilitate individual productivity and collaboration, not to secure communications. Groupware also presents other challenges for system administrators. Integrating different groupware systems, especially common after corporate reorganizations, mergers or acquisitions, becomes difficult if the systems use different addressing formats. Without system integration and centralized management, managing the flow of mail in a heterogeneous environment is extremely complex and taxing to company resources required to maintain the systems.

Sendmail Mailstream Manager delivers the solid layer of security and control for enterprise or groupware-based email systems. Sendmail's enterprise products leverage the company's decades of experience to resolve the security issues most important to corporations. Today, 84 of the Fortune 100, including nine of the top ten, rely on Sendmail. Sendmail, Inc. has a dual mission — 1) to address the needs of corporations and service providers with a family of commercial infrastructure products and solutions for email, and, 2) to continue developing the popular open source sendmail message transfer agent and driving email related standards.

This paper discusses key problems surrounding email, groupware security and the technologies that contribute to a reliable and secure email system. It also explains why Sendmail Mailstream Manager is the best choice for protecting email and groupware systems.

## **Risks of Relying on Groupware to Protect Internal Networks**

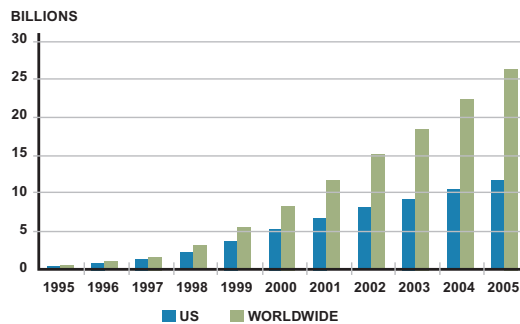
Groupware solutions, including Lotus Domino, Microsoft Exchange and Novell GroupWise, allow employees to collaborate on projects, improve teamwork and enhance their knowledge management capabilities. For all of its benefits, groupware was not designed with security as a top priority. Relying on groupware to protect the integrity of the enterprise mail system from Internet threats and to maintain the confidentiality of proprietary content seriously compromises network security.



## Groupware Can Fail Under Increased Message Load

Email has emerged as the mission-critical system for business communications and commerce. Its use has exploded in recent years (see Figure 1). This rapid growth places great loads on the servers and storage systems that handle email, not to mention the IT administrators expected to manage and administer them.

For handling nominal mail volumes, groupware systems perform as intended. However, a large increase in the number of messages, either incoming or outgoing, can cause problems if the groupware system does not contain robust mail queuing functions and the ability to throttle the flow of messages. This can result in mail delivery failures or even a groupware server that crashes, causing email loss and additional work for overloaded system administrators. The importance of the email network requires a bulletproof infrastructure that can grow with the company and its communications needs.



*Figure 1 - U.S. and Worldwide Email Volumes, 1995-2005*  
Source: IDC Email Forecasts and Trends

## Relay Theft Exploits Company Resources

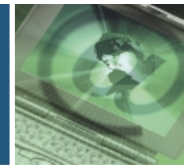
Spammers exploit groupware server vulnerabilities to relay enormous volumes of unsolicited bulk email, overloading the servers. Spammers find it much cheaper to steal bandwidth, cycles and disk capacity than to incur the message delivery costs themselves. When this occurs, legitimate company email can be bounced from the overloaded server and delivery can be delayed. A victimized company's system administrators must then clean up the bounced legitimate mail and deal with the bad publicity and angry users.

## Denial of Service (DoS) Attacks May Disable the Network

In some cases, Internet pirates are not looking to steal, but merely to vandalize. Denial of service attacks seek to crash a corporate server or render it unable to perform its function. They involve coordinated attacks by broadcasting machines that flood the target machine with useless traffic and usurp its capabilities. DoS attacks can disable your server or your network. DoS attacks do not usually result in the theft of information or other security loss, but depending on the nature of your enterprise, they can effectively disable your organization. These attacks are difficult to stop because the message traffic comes from many different machines. Groupware servers are not designed to recognize and prevent DoS attacks.

## Internal Information is Not Protected from the Internet

Groupware often concentrates a great deal of confidential information in a central location, making the protection of that information even more important. This information can include such critical data as user IDs, passwords, email addresses and internal server names. When a groupware server is exposed outside of the firewall, hackers can access this data. The recommended approach to keeping internal information secure is to separate groupware user



and directory information from a direct connection to the Internet. The benefit of this approach is that even if a hacker gets access to the gateway machine, it contains no user information, just the domain "company.com."

### **Heterogeneous Groupware Systems Can Cause Problems**

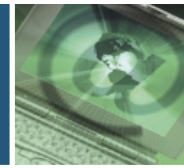
Enterprises today frequently undergo reorganization, mergers, acquisitions or major IT upgrade initiatives. These situations often result in the addition of groupware servers to an existing environment. Combining diverse groupware solutions presents technical and logistical challenges. Different groupware packages use different directory systems that don't easily integrate with each other, leading to message delivery problems. For example, when an organization is running both Exchange and Lotus, messages must first be routed to one groupware directory and then the other, until the user information is located. This can cause a message to take extra serial 'hops' to its final internal destination. In addition, heterogeneous groupware environments can lead to message delivery problems, as each system may speak its own dialect of a standard protocol. Email servers that centralize all user information and leverage Internet standards such as SMTP, POP, IMAP and LDAP can smooth the integration process.

### **Case in Point: Microsoft Exchange and Security**

Microsoft Exchange 2000 requires several different components to function: a Windows 2000 Server, Internet Information Service (IIS), Active Directory and Outlook 2000. Since Exchange 2000 does not have its own SMTP service it uses the Windows 2000 SMTP service included with IIS, which installs by default on the Windows 2000 operating system. Companies that run this SMTP service, referred to as the "SMTP connector" by Microsoft, risk being compromised due to numerous security holes in the Windows 2000 Server. In the last two years, Microsoft has issued over 95 security alerts specific to Windows 2000 and 25 alerts on Microsoft Exchange.

These alerts include Microsoft Security Bulletin MS01-037, which states an "Authentication Error in SMTP Service Could Allow Mail Relaying." The Microsoft recommendation for this flaw reads, "Best practices recommend disabling unneeded services. If the SMTP service has been disabled the vulnerability could not be exploited." Security Bulletin MS02-012 declares "Malformed Data Transfer Request can Cause Windows SMTP Service to Fail" and recommends customers either apply the patch, or disable the SMTP service entirely.

A system administrator must keep abreast of the multiple security issues related to each Microsoft software component, especially when it's exposed to the Internet. There are hundreds of web pages in Microsoft's TechNet, Security and Knowledge Base websites devoted to the recommended best security practices for the three components required to run Microsoft Exchange. This translates to a significant amount of time spent researching and applying software patch updates to all servers in an Exchange mail environment. When you factor in the frequency at which administrators must update the software for each server, the sheer cost of resources devoted to Microsoft security concerns alone can be substantial to an enterprise.



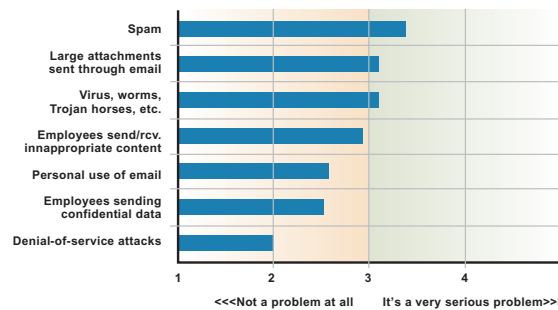
## Threats to Networks, Servers, and Content

In addition to email issues related to groupware, the Internet holds a variety of risks to smooth mail delivery, including spam and viruses. Human error, in the form of poorly designed networks or inappropriate email policies, can also interrupt internal and external communications.

### Spam Puts Company Resources at Risk

Unsolicited bulk mail, or "spam," is a growing problem for companies and service providers. An April 21, 2002, article in the San Jose Mercury News states that as much as 40 percent of all commercial email today is spam. Beyond the annoyance of get-rich-quick schemes, bogus offers and pornography, unsolicited email places a burden on the email network and can even bring down a mail server. It also hurts end user productivity, requiring the user to spend time identifying and deleting spam. In addition, it puts companies at legal risk if it exposes employees to illegal or "objectionable" content. Fighting spam is an ongoing battle as spammers change their methods and even their names to elude countermeasures.

Research shows that spam is a top concern threatening corporate email systems



Source: Osterman Research

### Viruses Cause Data Loss and Cost Money

Viruses are perhaps the most destructive external threat to corporate email networks. Virus writers exploit networked communications to transmit viruses via Internet mail. According to the Ferris Insight Bulletin, November 2001, 90% of all viruses are spread by email. Recent outbreaks, such as the "Melissa," "Lovebug," and "Klez" viruses, have received widespread media exposure. These malicious attacks can cause data loss, system crashes, diminished corporate credibility and considerable expenses, both in terms of increased IT costs and lost productivity. In fact, McAfee claims that viruses cost businesses \$13.2 billion in 2002 alone. The most important aspect of anti-virus technology is the capability to recognize new viruses before they can enter the email system. Once identified, the system can block the offending message, strip the virus from it and quarantine or forward the content to the proper authorities for analysis or prosecution.

### Single Points of Failure Can Disrupt Message Traffic

As with any system, email networks are only as strong as their weakest component. Each component must have full redundancy to prevent a network, hardware or software failure from bringing down the entire email infrastructure and causing message loss. Planned outages, such as maintenance, hardware or software upgrades, can also disrupt message

traffic if the system does not have the correct multi-layer architecture. The most reliable enterprise email systems include failover protection — an alternate email server that can transparently pick up the workload to avoid losing any messages — as well as offsite queuing, message storage and backup capabilities.

### Unsecured Transmissions are Not Confidential

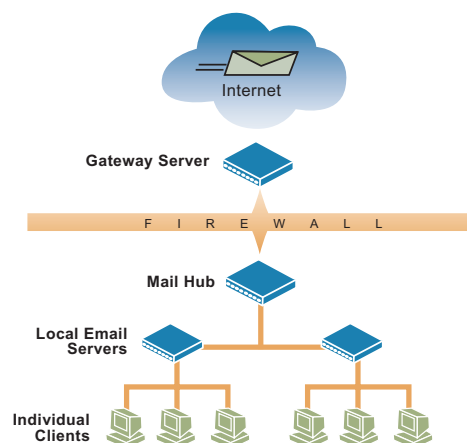
Hackers can read unsecured electronic communications, just as anyone can read a postcard sent through the regular mail. To keep confidential information safe, companies can secure their messages using authentication and/or encryption. User authentication occurs via passwords or X.509 certificates. Once a user is authenticated, the email channel can be encrypted for the secure transmission of messages. TLS (Transport Layer Security) uses digital signatures to authenticate the parties to an email exchange, and then encrypts the SMTP session that follows. TLS encryption ensures privacy between authenticated servers and/or clients and prevents anyone from tampering with the contents of the message while it is in transit. Many companies use both authentication and encryption together to further protect their email communications.

### Unrestricted Content Can Cause Legal and Regulatory Problems

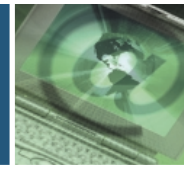
Beyond spam and viruses, unauthorized incoming or outgoing message content can cause legal, regulatory or public relations problems. Having an email management policy, along with automated implementation mechanisms, helps resolve this issue. Policies typically address corporate confidentiality, security, archiving and disclosure requirements. To ensure consistency across the enterprise or department, content management policies should work at the server level rather than trying to manage every desktop or portable system. Policy enforcement filter products include filtering attachments to block certain types of files, setting size limits, adding boilerplate text to outgoing mail or automatically creating archival copies of certain types of messages to meet the requirements of regulatory bodies such as the SEC or NYSE.

## Email Infrastructure Best Practices

Corporate email systems often contain a mixture of new and legacy components distributed throughout the enterprise, including interconnected message transfer agents (MTAs), groupware servers and various security hardware and software. An MTA is a highly specialized program that delivers mail and transports it between machines; much like the post office delivers conventional mail. MTAs perform specific functions, depending on their configuration and physical location in the email network. MTA roles vary from performing security and filtering functions at the firewall or network perimeter



*Figure 2 - Corporate email systems generally contain these components*



(gateway server), to maintaining centralized user and account information (mail hub), to distributing mail efficiently among heterogeneous groupware systems (local email servers).

Although every corporate email system is unique, most share several common elements dictated by the functional requirements of moving mail into, out of, and within the enterprise (see Figure 2 on previous page). Efficient management of the email flow among all the MTAs helps maintain a reliable system that meets the business' needs.

### **Internet Gateway Server**

The Internet gateway server acts as the first line of defense against Internet threats. It typically sits at the corporate firewall, or just inside the firewall, but remains isolated from the internal network. It assures the availability of the email system and the security of internal resources.

The main role of the gateway server is to filter messages and hand off the accepted ones to the mail hub for routing. Gateway servers may perform filtering functions on incoming and/or outgoing mail. Administrators can configure them to block spam or viruses, or perform specialized email content filtering.

### **Mail Hub**

The mail hub ensures efficient message routing within the organization. The advantage of using a mail hub is that it integrates two or more departmental mail systems from different vendors, relieving departmental email systems from the complex task of managing address resolution. Another benefit of using mail hubs is that they enable group — or department-specific filtering and policy management enforcement.

Mail hubs also increase the availability of the email system as a whole by providing redundant capacity for handling mail. They improve the reliability of departmental email systems by queuing spikes in volume that might overwhelm a groupware server. In addition, mail hubs that run Sendmail Mailstream Manager software can help to balance the email traffic load, further enhancing system performance. Scaling a corporate email system becomes easier using mail hubs; just add more mail hubs as the number of separate departmental systems increases.

### **Local Email Server**

The local email server receives messages from the mail hub and processes them for delivery to their recipients using standard Internet mail protocols. The local server is often used in configurations where the message stream needs some additional processing, such as implementing content filters. Groupware servers often perform the role of a local email server, if a separate server does not exist.

---

## **Sendmail Mailstream Manager**

### **Mailstream Manager Overview**

Sendmail Mailstream Manager protects enterprise and service provider email systems by providing a secure boundary around the entire email architecture and enabling a flexible

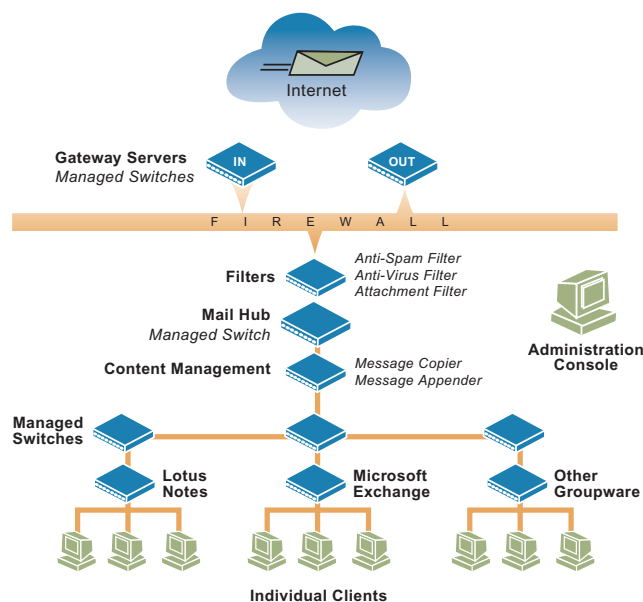
email infrastructure to control message flow. Mailstream Manager sits in front of and works seamlessly with existing email solutions to ensure reliable message delivery. It combines a set of key components to protect against security threats, enables flexible control of email and implements email policies.

Mailstream Manager provides an open framework that supports a variety of email architecture designs, making it suitable for the diverse needs of different companies. It starts with intelligently deploying email servers at the email gateway to control the flow of email and create a barrier against potential hackers, spammers and viruses. It improves overall network security, enables content policy controls and creates a predictable model from which to scale the email infrastructure.

### Mailstream Manager Components

Sendmail Mailstream Manager contains several components that perform specific functions and work closely together to deliver a mission-critical email infrastructure solution (see Figure 3).

- Administration Console
- Managed Switches
- Anti-Spam Filter
- Anti-Virus Filter
- Policy Enforcement Filters
- Directory Service



**Figure 3 - Sendmail Mailstream Manager Components Work Closely Together**

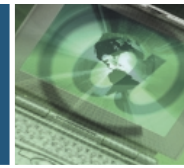
### Administration Console

The Administration Console controls all the Managed Switch MTAs in an enterprise from a single, secure remote console. It allows IT managers or system administrators to view the configuration and activity of every Managed Switch MTA in the network and make changes remotely through an intuitive GUI.

The Administration Console provides comprehensive activity logs, automated alerts and notifications and management reports. In addition, it simplifies scaling the email network by allowing IT staff to add, configure, deploy and manage additional mail routing servers. Email systems without centralized management require administrators to configure each MTA individually, wasting time and introducing opportunities for errors.

### Managed Switches

Message transfer agents are the heart of every email system. They route messages through the network until they reach their final destination. Besides basic routing functionality,



Managed Switches efficiently handle encryption and filtering of both incoming and outgoing mail based on the configurations set through the Administration Console.

To ensure the email is delivered to the proper recipient(s), Managed Switch performs directory lookups, address rewriting and aliasing to interpret, resolve or rewrite the address. It can use DNS Mail Exchange records, as well as LDAP directories for both message routing and user authentication. Managed Switches support all Internet email standards (see Sidebar).

To ensure reliable message delivery, Managed Switch writes a copy of the incoming message to disk before sending an acknowledgement back to the sender. With some other MTAs, including groupware, the mail server acknowledges receipt as soon as it receives the message. If a problem occurs that disrupts the groupware server or its memory, the message will be lost and the recipient will never receive it.

### **Anti-Spam Filter**

The best way to deal with spam is to remove it as soon as possible to minimize the costs of handling it. Sendmail Anti-Spam Filter is 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. It goes well beyond traditional static keyword or block lists by creating a lexicon – or dictionary – of common spam characteristics. The anti-spam engine is trained with tens of thousands of messages – spam and legitimate email – to identify and inventory what is spam and what isn't, increasing accuracy and reducing false positives. Once a message passes through the gateway server, the Anti-Spam Filter scans the header, message body and attachments to eliminate unsolicited email. Messages that meet the threshold spam criteria can then be destroyed, redirected, quarantined, blocked or tagged, depending on customer preference.

### **Anti-Virus Filter**

As with spam, viruses are best handled before they enter the enterprise. The Sendmail Anti-Virus Filter examines email as soon as it passes through the Internet gateway. By scanning at the server level, it eliminates viruses before they reach client systems, or even other MTAs, dramatically reducing the risk of desktop infection and the costs of cleanup. System administrators have a choice of automated virus updates, pull-type manual updates or a combination of the two approaches. The filter can check incoming and/or outgoing mail for viruses.

### **Policy Enforcement Filters**

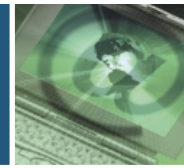
Sendmail Policy Enforcement Filters allow companies to enforce policies regarding the messages that flow through their email systems. The Attachment Filter, Message Copier and Message Appender provide administrators precise control of incoming and outgoing content and the ability to limit message size.

### **Directory Service**

Sendmail Directory Service is an email-centric user directory. It contains the user information needed by each Mailstream Manager component, and provides users with a single administration interface for their personal mail system preferences, such as password changes or vacation notices.

#### Sendmail Mailstream Manager Supports Internet Email Standards

- SMTP
- MIME
- HTML
- LDAP
- S/MIME
- TLS



## Components in Typical Mailstream Manager Implementation

### Server

- Internet Gateway Servers
- Anti-Virus Gateway Server
- Anti-Spam Gateway Server
- Mail Hub Server
- Directory Server
- Administration Console

### Software

- Sendmail Managed Switch
- Sendmail Anti-Virus Filter
- Sendmail Anti-Spam Filter
- Sendmail Managed Switch
- Sendmail Directory Service
- Sendmail Administration Console

(Actual configuration will depend on customer requirements.)

## Sendmail Mailstream Manager - Protecting Email Networks

Sendmail Mailstream Manager instantly adds security, reliability and performance to groupware email systems. It enables IT managers to easily monitor the entire email network through a secure, remote console, gaining visibility on its operation. System administrators can change the settings on any Managed Switch and immediately view the results, adding real-time control capabilities to better run their networks. This section addresses the advantages of using Sendmail Mailstream Manager to protect corporate email systems.

### Blocks Spam to Enhance Productivity

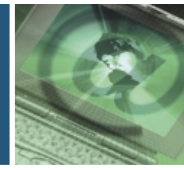
Mailstream Manager provides robust features to identify, block and remove spam before it enters the internal email network. It uses a powerful anti-spam scanning engine together with flexible anti-spam rule sets to identify objectionable content. System administrators and IT managers can update the criteria based on new rules or even examples of the types of messages they want to block.

Headers often contain enough information to identify spam. Mailstream Manager requires fully qualified domain names for sender addresses outside the network. It can also limit the maximum size and number of recipients per message to screen out bulk mailings. In addition, Mailstream Manager uses customized pattern matching to identify a common phrase or address in the header to catch suspect messages.

Mailstream Manager provides a multi-layered defense against spam. Messages not caught by header identification can be caught through keyword scanning on the message body and email attachment. A more comprehensive full text analysis examines the message content based on the context, proximity and frequency of trigger words. In addition, the filter searches common attachment formats for features common to spam.

### Protects Networks from Viruses Before They Enter the Organization

Mailstream Manager integrates leading anti-virus technology from McAfee to scan email at the gateway and remove viruses before they damage internal systems. Depending only on client-side virus scanning, as some companies do, means that the virus can penetrate



the email network and damage systems with inadequate or outdated protection. Centralized management, flexible configurations and automatic virus definition updates streamline administration and enable local or remote policy enforcement via a secure, web-based, central console. A strong anti-virus policy reduces the risk and cost of business interruption.

In addition to preventing virus-related down time, blocking viruses at the gateway saves companies money on hardware costs. With groupware servers, such as Microsoft Exchange, a company needs to purchase additional servers to maintain system performance while running processor-intensive anti-virus scans. For example, consider an enterprise of 5,000 users with an average of 300 users on each Microsoft Exchange server. This company can save up to \$250,000 in hardware and administration costs in the first year by deploying Sendmail Anti-Virus on gateway servers rather than installing and running an anti-virus filter on each separate Exchange server. The larger the enterprise, the greater the savings.

A 5,000 user company can save up to  
\$250,000 in hardware and administrative  
costs in the first year with Sendmail Anti-Virus Filter.

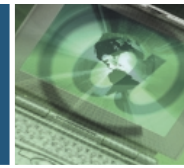
### **Blocks Relay Theft and DoS Attacks**

Mailstream Manager features gateway mail servers that sit at the firewall to control gateway ports and machines. It only allows authenticated users to relay messages from outside the firewall, based on specific lists of domains, hosts and users that are allowed to send mail. In addition to a default setting that blocks promiscuous relaying, Mailstream Manager supports spammer and hacker blacklists to prevent unauthorized users from relaying messages and provides a defense against denial of service attacks. For maximum protection from unauthorized use, Mailstream Manager uses password — or certificate-based authentication combined with TLS (Transport Layer Security) encryption — to allow only approved users to send email.

### **Secures Internal Information from the Internet**

Some older versions of groupware feature directories that contain confidential user information. When these groupware servers are exposed outside the firewall, hackers can access this data. The Mailstream Manager architecture separates groupware user and directory information from direct connection to the Internet, keeping internal information internal. Mailstream Manager also rewrites email addresses on outbound mail to hide internal network and user log-in information, further protecting confidential user information.

Mailstream Manager contains its own email-specific user profile environment. This user profile connects to groupware directories such as Microsoft's Active Directory using a one way synch. Having a separate directory for email information prevents Active Directory from taking too many "hits," thus improving Active Directory's performance. As Active Directory also contains non-email specific user information, this allows Active Directory to spend its time on non-email specific tasks.



### **Failover Protection Enhances the Reliability of Email Systems**

Mailstream Manager's multi-layer and modular architecture allows user organizations to run redundant hardware to prevent a single component failure from immobilizing the entire network. The Mailstream Manager architecture includes optional onsite and offsite failover servers. This assures that in case of an internal or external failure, an alternate email server can accept and queue email for delivery, so the system does not lose any messages. When the regular email system resumes operation, recipients will receive mail from the queue. During an outage, customers, business partners and even internal users will never see a message bounce. Many groupware systems such as Microsoft Exchange and Lotus Notes are pre-configured to bounce mail if they do not receive an immediate confirmation.

### **Protects Information Sent Over the Internet**

Mailstream Manager protects a company's valuable data and keeps proprietary information safe. It supports Transport Layer Security (TLS), the Internet standard for authenticating and encrypting transmissions across open networks (and the successor to Secure Sockets Layer, or SSL). TLS uses digital signatures to authenticate the parties to an email exchange, then encrypts the SMTP session that follows, enabling secure server-to-server communication.

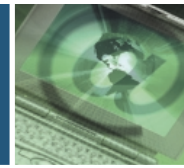
TLS encryption secures server-to-server email transmission by encrypting the email channel. Securing the email channel means that only the email session is encrypted – an improvement over scrambling the entire message. When the entire message is scrambled, virus scanners cannot scan the message. With Mailstream Manager's TLS encryption, virus scanners can review the email but prying eyes cannot see the message.

TLS encryption protects email traffic between company sites, partners, customers and even internal servers. It just requires one X.509 certificate for each server. Client to server communication for email 'sends' can be encrypted with Mailstream Manager via TLS, as long as the client has a valid X.509 certificate. Mailstream Manager also works with IMAP servers that support TLS to provide a secure environment for receiving email. This means that with TLS, a user can safely send and receive email from a hotel room, home or other remote location.

### **Facilitates Integration of Different Groupware Systems**

Mailstream Manager provides a standards-based glue for integrating heterogeneous groupware messaging environments and reconciling different interpretations of standard protocols such as SMTP, POP, IMAP and LDAP. Mailstream Manager also features a centralized, email-specific user directory for email transactions, consolidating user information from different groupware or email systems to create a more efficient and secure network. A centralized directory prevents messages from taking extra time to reach their destination by providing a one-stop-shop for user information, instead of requiring the message to serially search different groupware directories.

When companies add groupware servers to an existing environment, messages can take extra time to reach their destinations. Mail destined for an internal user might go through a server outside the firewall before it reaches its final destination. This means that the system



consumes more resources for a simple transmission and the message is unnecessarily exposed to the Internet. The Mailstream Manager architecture prevents email destined for internal users from being exposed to the Internet by accepting messages and resolving delivery to the correct groupware server.

### **Provides Control Over Content of Incoming and Outgoing Messages**

Managing the flow of email in and out of a corporate network goes beyond controlling external threats. It is important to ensure that outgoing messages do not contain confidential information or other content that could embarrass the company, create a potential liability or violate regulatory policies. Mailstream Manager offers several policy enforcement functions:

- 1) Sendmail Attachment Filter determines what file types or sizes may or may not be transmitted through the corporate email system. It allows companies to block or discard unwanted MIME attachments by scanning email messages by file extension, file name, MIME type and subtype, or by the sender's email address. Size limits prevent bulky attachments from clogging or slowing the network. Options allow the system to amend an attachment, replace an attachment, modify the message header and/or redirect the message to an alternate mailbox for review.
- 2) Sendmail Message Copier delivers a complete range of options for copying incoming or outgoing messages, routing them to a recipient, file or analysis program, and then delivering the message to its intended destination. Administrators may set policies to copy and archive all or selected messages that match specific criteria to a designated location or to sample messages for offensive content that could result in potential liability. These choices give IT managers the power and flexibility to monitor and manage email traffic to fulfill internal policies or external compliance requirements. Some of the configurable options include filtering based on specific content criteria, sender or destination. Message Copier stores the entire message, including blind copy (BCC) recipients.
- 3) Sendmail Message Appender processes inbound or outbound email to add text messages to the bottom or top of the message in MIME style or simply append or prepend. It inserts corporate information, standard disclaimers, or targeted advertisements based on sender or recipient and message size. It can also modify header information to eliminate sensitive security information from them. The administration console provides complete control over what occurs on the email network.

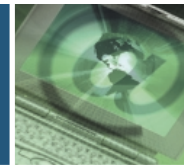
#### **Mailstream Manager Runs on All Major Platforms**

- Solaris 2.6, 7, 8
- Windows NT, 2000
- Red Hat Linux 7.0, 7.1
- Red Hat Advanced Server
- IBM AIX 4.3.3, 5.1
- SuSE Enterprise Linux 7.0

## **Business Benefits of Mailstream Manager**

### **Maintains Reasonable Costs**

Mailstream Manager uses dedicated servers, each of which performs a specific function in the overall email delivery process. As most of the functions are input/output intensive, it allows companies to run the required servers on very cost-effective hardware. Enterprises can use their fast processors and huge memory machines to run compute-intensive tasks, rather than delivering email. Because Mailstream Manager offloads the tasks of filtering and



content management from the groupware servers, it effectively increases the capacity of those servers. This allows more groupware users on each server and thus decreases the overall number of machines required for groupware functions.

### **Scales with Enterprise Needs in a Cost-Effective Manner**

Mailstream Manager features a modular architecture that allows for predictable, cost-effective scalability. Companies can expand their email network to support growing numbers of users and increasing message loads. In addition, they can add incremental servers to maximize uptime and eliminate single points of failure. Mailstream Manager can scale to accommodate millions of messages per hour.

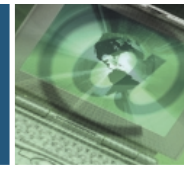
### **Centralized Management Saves Money on Administration**

Mailstream Manager allows IT administrators to focus on tasks other than managing the email system, which can be time consuming and complex. It provides a "locked down" administration console that centralizes critical system management tasks, improves security and control and eliminates duplicated efforts among several departments. Functionality includes overseeing mail queues, aggregating traffic reports, automating email traffic alert notifications, monitoring specific health attributes and providing statistical reports for each SMTP router. One key benefit of the console is that it allows administrators to configure and manage each server in Mailstream Manager through a secure (SSL) web interface, allowing access while traveling, from home, or from any location with an Internet connection. In addition, it allows a single administrator to manage email networks in several sites.

Enterprises need a secure solution to protect their email networks from Internet-based threats and equipment failure. Isolating groupware servers from the Internet with a security strategy that pushes defenses to the network edge forms the foundation of such an approach. A flexible, scalable, resilient architecture assures mail delivery regardless of traffic conditions and provides low and predictable maintenance and expansion costs. Centralized management is essential to monitor such an infrastructure and control the flow of information throughout an organization.

Sendmail, Inc. has packaged over 20 years of email experience into a set of architectural guidelines to help organizations design reliable, secure and scalable high-performance email infrastructures. Sendmail Mailstream Manager delivers an intelligent mail infrastructure that includes integrated security functions, comprehensive system and content management tools, and a wide range of professional services for designing, migrating, optimizing and customizing Sendmail commercial software. Its efficiency, reliability, security and liberal acceptance of email from other systems, combined with its scrupulous adherence to open standards, make it an ideal complement to groupware applications. With Mailstream Manager, IT managers can seamlessly integrate diverse email systems and offer their users a secure email environment with full confidence that their messages will reach their destination.

## CONCLUSION



### **Advantages of Mailstream Manager Over Open Source *sendmail***

Sendmail's Mailstream Manager is an enterprise solution based on open source *sendmail*. It runs in front of groupware to improve security, efficiency and reliability. Mailstream Manager leverages the *sendmail* technology that has been proven across the Internet over the past 20 years and the expertise gained in over 700 customer implementations worldwide. In addition to the core MTA functionality, it adds functions important to system administrators, with a focus on providing a secure, robust, scalable, cost-effective end-to-end email solution.

### **Mailstream Manager Adds Key Features to Open Source *sendmail* Including:**

- *Centralized management of all MTAs through a user-friendly GUI*
- *Anti-spam features*
- *Anti-virus protection*
- *Secure transmission via TLS*
- *Policy enforcement filters*
- *Top-tier customer support with leading *sendmail* experts*

Sendmail's Mailstream Manager represents a proven solution that works with the main groupware solutions - Lotus Domino, Microsoft Exchange and Novell GroupWise - and supports all the Internet-based mail protocols such as SMTP, POP and IMAP. Mailstream Manager runs on all major hardware platforms. Sendmail's professional services group provides 24x7 mission-critical technical support, along with decades of expertise to help companies design, migrate, optimize and customize their Sendmail commercial solutions.

### **Open Source *sendmail* - Setting The Standard Since 1981**

Most companies already use a form of Sendmail technology as part of their email infrastructure. Open source *sendmail*, developed in 1981 by Sendmail, Inc.'s co-founder and CTO, Eric Allman, is a flexible, powerful, highly configurable mail transfer agent (MTA). It is the dominant implementation of SMTP, the Simple Mail Transfer Protocol (RFC 821).

*sendmail* open source powers the majority of Internet mail domains worldwide. Through over twenty years of development, use and testing, *sendmail* has become the Internet's standard for message transfer. The *sendmail* standard is so pervasive that even competitors use open source *sendmail* as the foundation for their MTA products.



WHITE  
PAPER

Protecting Your  
Email Network



**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)

© 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.