

PROTECTING AND OPTIMIZING EXCHANGE ENVIRONMENTS:

Deploying a Secure Email Boundary to Optimize Enterprise
Messaging Networks.

November 2007

INTRODUCTION

In a recent survey conducted by Osterman Research, Messaging Security and Market Trends, 2005–2008, over 60 percent of respondents identified growth in email storage requirements and spam as the two “very serious” problems currently facing their enterprises.

Escalating volumes of spam and viruses, along with evolving threats like spyware and phishing, pose serious challenges to the security and stability of groupware networks. This barrage —spam, viruses, denial of service (DoS), dictionary-style attacks, and address harvesting —directed specifically at Exchange, places the email network, employee lists, customer relationship data, Active Directory (or any LDAP directory) and other corporate knowledge at risk. To keep the Exchange environment operating at maximum efficiency, administrators typically deploy additional servers dedicated to security processing, management, storage and quarantine. Given the certain growth in future email volumes, investing in additional servers is not a proactive strategy.

LOWER MESSAGING NETWORK OPERATING COSTS WITH A SECURE EMAIL BOUNDARY.

With a secure email boundary architecture in place, email security solutions can protect Microsoft Exchange, while enabling it to work more efficiently and reliably. The end result: a greater ROI on the messaging network.

For all their benefits, Exchange (or other Groupware) was designed prior to the explosion in Internet email and without anticipation of outside threats. Relying solely on the security capabilities of Exchange (Groupware) to protect the email network can seriously compromise security and significantly increase the server load, limiting the number of users each can support, and the storage costs to the organization.

Exchange and other groupware solutions represent a significant IT investment. These costs include licensing, user and administrative support, and processing and storage capacity. In all, IT departments are under constant pressure to keep groupware functioning seamlessly, while keeping their expenditures under control.

INTO ACTION: OUTLINING THE OPTIMAL SOLUTION FOR GROUPWARE OPTIMIZATION.

Secure email architectures aim to protect Exchange from constantly evolving threats transported by email, and to prevent the constant escalation of costs. To optimize the message processing network, many large enterprises are using an approach known as “The Secure Email Boundary.” This approach uses gateway components deployed in the DMZ to protect the enterprise email network from connection level attacks and most invalid and unwanted traffic.

Following are the key requirements for securing Exchange and increasing its ROI. They center on email gateway defense, and work to eliminate unwanted messages at the gateway prior to:

- Entry in the email network
- Scanning for spam or viruses
- Exposure to the Exchange Server
- Storage, quarantine or archival

With the following requirements in place, large enterprises benefit from a secure and optimized messaging infrastructure.

- High performance, high availability mail transfer agent (MTA) to withstand spikes in incoming connections
- SMTP connection control for detecting and regulating unwanted or suspect connections
- Flexible options for Anti-spam and Anti-virus filtering
- Secure, read-only, LDAP server optimized for messaging for connection and routing validation
- Authenticate sending domains to fight fraud, phishing and spoofing
- Clustering capabilities for load balancing and failover to enhance reliability

A ROBUST MAIL TRANSFER AGENT (MTA) TO MANAGE HIGH TRAFFIC AND ENSURE FAILOVER.

Enterprises with high message volumes run the risk of security issues, performance degradations, and lower availability if they deploy an unproven MTA (SMTP Gateway).

Groupware SMTP servers were designed to handle cleaner, internally-generated and routed email, which can be easily-overloaded by a variety of Internet-based attacks, malformed email, or email addressed to invalid or non-existent recipients.

To meet enterprise requirements the MTA must accommodate a wide range of security plug-ins such as anti-spam and anti-virus solutions, policy management and gateway defense solutions. This extensibility arms the enterprise with the flexibility to select from a broad range of anti-spam and anti-virus solutions, best-of-breed compliance and encryption engines, and quickly adopt innovative security technologies designed to deal with emerging threats.

The MTA must be capable of managing enterprise-level volume—including withstanding spikes in connections due to normal traffic variations and DoS attacks. The MTA must support high-availability clustering and configurations that reroute messages through alternate paths when necessary.

Lastly, to augment the MTA, and eliminate hard-coding of frequently changing routing configurations, optimal email environments incorporate directory-based routing, which enables more efficient routing decisions and routines.

CONNECTION CONTROL FOR MONITORING AND REGULATING THE CONNECTION.

The standard attack profile for spammers is a mass-mail delivery, without message queuing. By rejecting connections with this profile, the number of messages entering the email network is dramatically reduced, typically by over 50%. By monitoring all the traffic connecting to an MTA and throttling back as needed, effective connection control protects the email network and Exchange environment from spam, viruses, and denial-of-service attacks. This reduction also helps reduce CPU-intensive content scanning, directory queries, generation and queuing of a bounce message, etc. The result is a massive reduction in network overhead, filtering servers, and number of backend mail stores.

Because nearly all malicious connections are rejected, resource usage is increased on the spammer's system (queuing) instead of the corporate Exchange environment. In most cases, spam servers are configured to "give up" on a receiving MTA if the connection is slow or repeatedly dropped, and move on to a different target.

With secure directory integration, connection control is further augmented by tapping into up-to-date directory data to reject invalid addresses, regardless of the connection profile. A connection generating messages that rapidly exceed a threshold of undeliverable addresses is likely being used for a dictionary-style attack or directory harvesting. Detecting and dropping such connections during the early stages of an attack (based on a configurable threshold) provides significant protection of sensitive address information and eliminates the load it would generate if allowed to reach the Exchange.

FLEXIBLE OPTIONS FOR ANTI-SPAM AND ANTI-VIRUS FILTERING.

Best practices dictate the use of multiple anti-virus solutions from different vendors. In addition, some enterprises elect to deploy different virus-scanning strategies (e.g., signature-based and distribution-based) to minimize the possibility of an outbreak prior to a release of a new virus signature for signature-based vendor solutions (so called zeroday anti-virus defense).

Scanning for viruses at the gateway lessens the volume of virus-laden messages that could affect end-user desktops and the mail server. Mailstore scanning on inter-user traffic, either on the same server or multiple mail servers, provides another tier to cleanse the environment from

potential threats. For the end user, scanning at the desktop for malware using delivery channels outside the control of the email environment is also critical.

Enterprises should look for an anti-spam engine that receives both periodic and micro-updates to deal with the real-time flow and patterns of spam on the Internet. In addition, it should support flexible policy enforcement to augment the functionality of the anti-spam engine. This gives the administrator the ability to block, delete and redirect specific messages based on patterns detected in their subject and/or message body.

With the right combination of connection control, anti-spam and anti-virus solutions at the gateway, most unwanted messages can be turned away before they are committed to resource-intensive Exchange processing and storage.

DIRECTORY-DRIVEN EMAIL SECURITY TO VALIDATE RECIPIENTS AND OPTIMIZE ROUTING.

Utilized throughout the entire email network, directory information is accessed to optimize capabilities such as: connection control, applying AS/AV and message routing.

By utilizing a high performance, messaging-specific, LDAP directory server, enterprises can leverage up-to-date directory data to optimize the key component parts of the messaging infrastructure. The result is a more secure network and less processing/storage/disk space used due to fewer unwanted messages and more precise routing between mail stores. Key requirements for using directories as part of email security include:

- A centralized, secure messaging-specific directory that is optimized for message processing
- Automated synchronization capability from multiple LDAP and non-LDAP data sources
- A secure, read-only, DMZ directory replica that is updated from the centralized directory and protected from DMZ attacks

FIGHT PHISHING, SPOOFING AND FRAUD WITH SENDER IDENTIFICATION.

After an email has survived the previous checks, it is now time to determine where they're really coming from. This should be simple, but unfortunately it isn't. This is due to the fact that the Internet email standard, SMTP, is a trusting protocol.

Senders can pretend to be anybody they want to be, and appear to send email from any domain they fancy.

There have been several approaches proposed to solve this problem, such as SPF, Microsoft's SenderID and Yahoo's DomainKeys. The approach that appears to have the most momentum is called DKIM, for DomainKeys Identified Mail. This is a cryptography-based authentication scheme in which the sending domain uses Domain Name Services to store the public key(s) of the outbound mail gateways which are authorized to send email on its behalf.

The matching private key(s) are used by the sending mail server to digitally sign each message, with the resulting signature pre-pended to the email as a special header. The receiving mail gateway can verify this digital signature using the public key retrieved from Domain Name Services. If the signature checks out then the email really comes from the domain indicated in the sender address.

An added benefit of this approach is if the signature checks out then you will also know that the email hasn't been tampered with in-transit. Depending on the type of communications processed by your organization, this side benefit may actually be as important as the first one.

DKIM was proposed by Yahoo! and Cisco, and the corresponding draft Internet standard written by Sendmail's Chief Science Officer, Eric Allman, was recently approved as an IETF standard.

FAILOVER PROTECTION TO ENHANCE EXCHANGE RELIABILITY.

Most groupware systems, such as Microsoft Exchange and Lotus Notes, are preconfigured to bounce mail if they do not receive an immediate confirmation after recipient mail server failures. Rather than queue such messages on the groupware email server and load it with delivery re-tries, the optimal solution must possess the capability to queue and store messages in a separate MTA for delivery until the mail environment becomes available or the redundant environment is ready for routing.

This architecture can include optional onsite and offsite failover MTA servers. In case of an internal or external failure, an alternate MTA can accept and queue email for delivery so that the system does not lose any messages. When the regular email system resumes operation, recipients receive mail from the queue. With the right solution in

place, during an outage, customers, business partners and even internal users are unlikely to ever see a message bounce.

SENDMAIL: THE COMPLETE ARCHITECTURE FOR SECURING AND OPTIMIZING EXCHANGE.

Over half of the Fortune 1000, including seven of the top ten, relies on Sendmail to design and implement their email security. This expertise is why the largest corporate email networks trust Sendmail to support hundreds of thousands of their end users.

Sendmail customers typically see a 50% reduction in unwanted messages at the gateway. A company that drops 50% of unwanted messages prior to spam and virus scanning, followed by a further elimination or quarantine of suspected spam, is primed to dramatically reduce the email reaching its Exchange (groupware) servers, sometimes by 75-80% of total mail volume. The results are a parallel reduction in the number of groupware servers required or an increase in the number of users supported by each server.

Often this results in savings of hundreds of thousands of dollars per year. The larger the enterprise, the greater the savings.

With Sendmail, Exchange environments gain:

Connection regulation and management

- Reduces invalid/unwanted connections by 50 percent
- Validates address queries more efficiently and accurately by leveraging directories
- Eliminates unnecessary queuing and generation of bounce messages

Dependable, accurate, and optimized routing

- Enhances regulation of mail flow and mail server traffic
- Improves routing accuracy through directory integration
- Provides dependable network redundancy and failover protection

Flexible approaches to protect against spam and viruses

- Captures 99 percent of spam and virus traffic with multiple AS & AV engines

- Filters and scans at the mail store and gateway levels
- Extends AS/AV filtering with additional cascading policies

Sendmail provides a complete solution for securing Exchange or any other groupware network. It supports all Internet-based mail protocols, including SMTP, POP and IMAP. It interacts with directories such as Microsoft Active Directory, Lotus Domino, Novell eDirectory, Netscape iPlanet/Sun One/Fedora Directory Server, Open LDAP, and any other standards-compliant LDAP v3 directory server. In addition, Sendmail runs on most of the major operating platforms.

SENDMAIL DELIVERS APPLIANCES AND SOFTWARE TO MEET ANY ENTERPRISE REQUIREMENT.

Sendmail Sentrion™ MP is the first high-performance appliance that offers all-in-one protection for both inbound and outbound messages – obsolescing single-purpose Messaging Gateways that only protect companies from inbound threats, or only manage company policies related to outbound messaging. With Sentrion MP, organizations can dramatically reduce the cost and complexity of securing and managing corporate email by enabling both inbound and outbound message protection in a single appliance – without degrading message processing performance.

Sentrion MP is a Purpose-built, High-Performance Message Processing Appliance for:

- **Gateway Management:** Bi-directional message encryption and sophisticated connection controls prior to inbound processing
- **Email Authentication:** Authenticates all incoming and digitally signs all outgoing messages with DomainKeys Identified Mail (DKIM), and other authentication mechanisms to certify email senders
- **Inbound Message Processing:** Spam, virus and malware protection after Gateway processing
- **Outbound Data Leak Prevention:** Highly accurate, in-line content monitoring and enforcement to prevent data loss and compliance breaches
- **Intra-company Message Management:** Enforces acceptable use policies. Front-ends and protects Microsoft Exchange environments

Policy applications can be added to Sentrion MP to monitor and enforce outbound messages for:

- Corporate governance
- Regulatory compliance
- Privacy violations
- Data leak prevention

Sentrion leverages directory-driven email security, providing comprehensive integration with Active Directory and other corporate directories. With all of this functionality and performance packed into a hardened system, the Sentrion appliance is designed to easily secure and optimize groupware networks of any size.

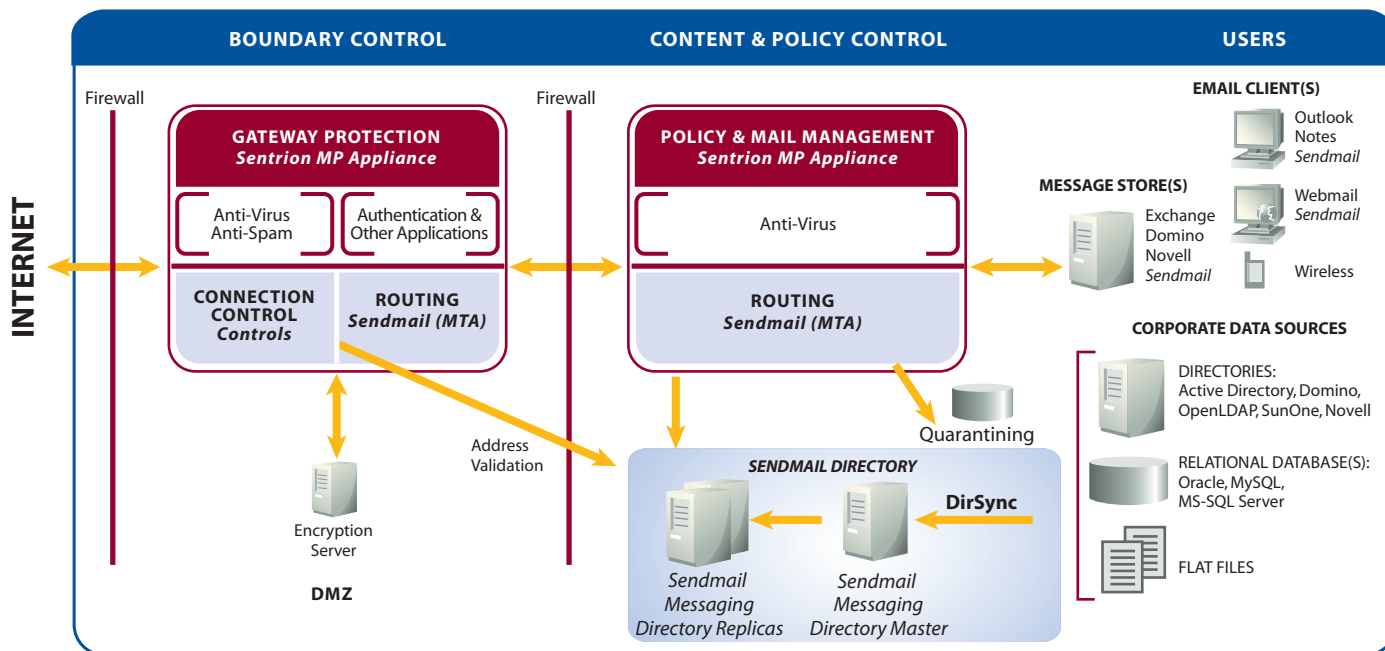
A PARTNER YOU CAN TRUST.

Over 60% of the world's email traffic runs through a Sendmail MTA. This experience combined with the knowledge gained at over 1,000 enterprise implementations, provides Sendmail with the industry's most comprehensive knowledge base for designing, optimizing and protecting any email or Exchange environment.

To learn how Sendmail can protect and optimize your Exchange or other groupware environment please contact us.

ABOUT SENDMAIL, INC.

Sendmail is the leading global provider of trusted messaging. With 25 years of leadership delivering innovative messaging technology, Sendmail ensures the protection and trust of employee and customer communications. Sendmail technology, driven by the industry's most powerful and flexible policy engine, provides protection where 80% of security and compliance violations occur – within inbound and outbound messaging. Large enterprises in 33 countries, and the majority of the Fortune 1000 trust Sendmail to shield users from unwanted messages, defend the messaging infrastructure, stop data and privacy leaks and effectively manage messaging to maintain brand and shareholder value and support regulatory compliance. Sendmail is headquartered in Emeryville, CA with offices and distributors in Europe, Asia and North America. For more information call 1-87-SENDMAIL.



This diagram illustrates how Sendmail solutions form to create a secure email boundary that can protect groupware, while enabling it to work more efficiently and reliably delivering ROI on the messaging processing network.

Sendmail, Inc.
 6475 Christie Avenue,
 Emeryville, CA 94608
 Tel: +1 888 594 3150
 Fax: +1 510 594 5429
www.sendmail.com