

Optimized Message Processing

Real-World Use-Cases for Intelligent Email Security, Policy Enforcement, Routing and Delivery in Complex Business Environments

INTRODUCTION

Today's typical email security software and appliance products fail to address the complex requirements of large multi-national businesses – why?

Typical Email Security Products:

- Are designed as “black-boxes” to simply scan, filter and block unwanted messages
- Lack the extensibility required for true intelligent message processing, routing and delivery
- Lack the necessary advanced message policy processing and enforcement capabilities for complex policy management and mail delivery

Large organizations with complex messaging requirements require solutions that not only scan and filter unwanted messages, but also solutions that provide advanced message processing and infrastructure for:

- Intelligent policy-driven message routing and delivery
- Highly accurate, bi-directional message policy enforcement
- Secure and extensible policy management and message routing

In order to address the complex messaging requirements of large organizations, an Optimized Message Processing infrastructure is required.

Sendmail has always been known for its trusted email delivery and its ability to handle complex routing for large enterprises. As messaging volumes continue to rise, the needs of enterprises have shifted from focusing on inbound threat protection to higher priorities of security, outbound content protection, and compliance. The real-world use-cases described in this tech-note make it clear that legacy spam and virus point products cannot handle the complex email infrastructure needs required for today's high volume and mission-critical messaging environments.

Now, more than ever, enterprises need to refresh and optimize their email architectures with bi-directional message processors capable of managing complex message policies, routing and message delivery.

The best way to understand how an Optimized Message Processing infrastructure can help solve complex messaging requirements is to see how it has enabled other businesses like yours to realize their own unique requirements.

The following section provides snippets of complex messaging routing and delivery use-cases from Sendmail's diverse customer base.

These use-cases are organized in the following format for quick reference:

Market:

Requirement:

Integration Points:

USE-CASES FOR COMPLEX, POLICY-DRIVEN MESSAGE ROUTING AND DELIVERY

Market: Biotech

Requirement: Policy-based message encryption for compliance and protection of sensitive data

Integration Points: Message Encryption, S/MIME encryption, LDAP directory

A large Biotech Company in California required certain messages to be encrypted based on a number of different message attributes. The Company had several concerns:

- Regulatory compliance with the disclosure of company financials and other sensitive executive level documents
- Concern for the rogue admin reading sensitive communication
- Compliance with electronic filing requirements with the FDA
- Recovery of encrypted data

Sophisticated policy-based message encryption and intelligent routing was the only viable way of ensuring that the correct encryption policies were applied to messages.

Using Sendmail's policy engine and integration with their LDAP directory, the policy sets make the determination as to what messages get routed through the encryption server for message encryption. LDAP lookups and deep content scanning are used to determine which messages need to be encrypted, for example:

- All executive email must be encrypted
- All documents marked confidential must be encrypted if they are leaving the organization
- Communications with the CBER and CDER at the FDA must be encrypted with S/MIME rather than their standard encryption solution. The policy determines which method is used for encryption.

The Biotech Company also has a special Sendmail Mailcenter Store deployment which lets users not enabled for encryption view messages.

Market: Healthcare

Requirement: Protect public health care information and ensure email delivery to registered health care workers only and to comply with government regulations.

Integration Points: Centralized government healthcare registration LDAP directory and TLS encryption over private network

Healthcare workers in a province of Canada must register with a provincial government organization that oversees the protection of the personal health information of the province's citizens. In order to ensure the privacy of that information, this governmental organization has built a private network based on Sendmail Sentrion MP Appliances. This Sentrion-based private network provides a secure email path between all privatized Canadian healthcare organizations—including the one discussed in this example—and the provincial government organization.

One particular large private healthcare provider in Toronto also uses Sendmail Sentrion Appliances to protect the public health information of its clients. Their Sentrion network prevents private information from being sent to recipients that are not registered healthcare workers in the province of Canada.

There are three general use-cases that Sentrion's policy management engine solves for the healthcare provider:

- If all recipients on an outgoing message are not registered within the government registration LDAP directory, then the message is assumed to not contain private health care information (e.g., one healthcare provider is not sending private patient information to another registered healthcare provider in the network) and the message is delivered through the standard internet connected MTA(s).

Note 1: Sentrion's extensible policy framework allows for easy integration with external LDAP directories, enabling more intelligent message processing and mail delivery.

- If all of the recipients are registered in the LDAP directory, then the message content is considered sensitive (e.g., one healthcare provider is sending private patient information to another registered provider) and the message is delivered over the private network using a TLS encrypted connection.
- If there is a mixed set of registered and non-registered recipients, the sender automatically receives a customized bounce message stating that non-Canadian Healthcare recipients have been removed from the message and will not receive the message; however the valid registered recipients (determined through the LDAP lookup) will receive the sensitive email.

Future policies will address messages that contain only non-registered recipients and sensitive private healthcare information is discovered within the message (found via Sentrion's deep content scanning of messages and attachments), the sender will receive a customized message stating the message was blocked from delivery.

Note 2: Sentrion's unique policy engine capabilities can perform this level of intelligent policy processing and mail routing "out of the box."

Market: ISP

Requirement: Route messages based on subscriber services

Integration Points: LDAP

One of the largest ISPs in Japan has roughly 1.5 million subscribers and uses Sendmail products for both their inbound and outbound gateways. Subscribers choose various e-mail filtering services such as Anti-virus, Anti-spam, email redirection, alert notifications via SMS and so on. The Sendmail installation at the inbound gateway routes incoming messages to the mail filtering servers whose roles vary depending on the services selected by mail recipients. There are numerous Sendmail servers at the inbound gateway, all of them centrally controlled by the data stored in the Sendmail Directory.

Market: Banking/Financial Services

Requirement: Custom mail routing for regulatory compliance; encryption metric reporting

Integration Points: Archive System, TLS encryption, Lotus Notes

Securities and Exchange Commission regulations dictate that, if requested, a registered broker must produce archived copies of all electronic mail (email) he has sent or received.

In order to comply with this regulation, a large Financial Services firm faced a dilemma. They did not want to place the entire burden of producing email archives on their internal Lotus Notes and Exchange mail systems, so they decided instead to design a solution that would allow the archives to be created while messages are in transit on their internal SMTP mail backbone, in real time. The Firm could have simply routed ALL of their inbound and outbound SMTP email through the system that actually produces the email archives, but, since only five to ten percent of their user population is comprised of brokers, routing ALL messages through the archive system would have created two interrelated problems. First, the email archive solution would have to have been capable of handling the email volume for their entire user population (100k + employees), even though it would only have been responsible for creating archives for an extremely small percentage of the email routed through the system. Second, routing ALL email through the archive solution would have added routing complexity and risk since ALL email would have to have traversed the archive system and any outages within the archive system could have impacted mail flow for the entire corporation. Therefore, The Firm had to figure out how to route ONLY SMTP email messages sent or received by brokers through the archive system.

Achieving this type of routing from an inbound perspective is accomplished through email address rewriting. For example, email messages sent to joe.user@thefirm.com are re-written to joe.user@cf.thefirm.com. As a result, the only thing The Firm has to do in order to selectively route broker email to the archiving solution is to assign them a different, unique, email address and subsequently place that information in the database. For example:

Scenario One (no archive is created)

- An inbound email message is sent to a Firm employee joe.user@thefirm.com who is NOT subject to SEC email archive regulations
- After routing through The Firm's internet-facing Sendmail MTA's the message is passed to another layer of internal Sendmail MTA's that "lookup" the RCPT TO: address joe.user@thefirm.com
- The policy rule set re-writes the RCPT TO: address from joe.user@thefirm.com to joe.user@notes.thefirm.com
- Next, the Sendmail system does a DNS lookup to determine where email destined for the notes.thefirm.com domain should route. DNS tells Sendmail to route the message, directly, to Lotus Notes.
- Note that the message did NOT route via the archive solution.

Scenario Two (archive is created)

- An inbound email message is sent to a Firm employee john.broker@thefirm.com who IS subject to SEC email archive regulation
- After routing through the Firm's internet-facing Sendmail MTA's the message is passed to another layer of internal Sendmail MTA's that "lookup" the RCPT TO: address john.broker@thefirm.com
- The policy rule set re-writes the RCPT TO: address from john.broker@thefirm.com to john.broker@cf.thefirm.com
- Next, the Sendmail system does a DNS lookup to figure out where email destined for the cf.thefirm.com domain should route. DNS tells Sendmail to route the message to the archive solution
- The archive system accepts the message, produces a copy and then routes the message to Notes

It is also important to note that the re-writing rules ONLY work on the message envelope address, not the message header address. SMTP messages are routed on the basis of the envelope, but the header is what you see in your email client. As a result, even though the policy rule set is rewriting addresses and accomplishing the type of routing The Firm needed, the address displayed to end users were NOT changed.

The capability to handle the above message policy and routing is available "out of the box" in Sentrion Appliances. However, accomplishing the type of selective routing detailed above for OUTBOUND mail was more difficult. Why? Email messages are routed on the basis on the RCPT TO: address in the envelope. Therefore, the solution has to distinguish between a message sent by a broker to external.user@gmail.com that MUST be archived and an email message sent by a non-broker to the same external address, which doesn't need to be archived.

The only thing that distinguishes the broker-originated outbound message in the above example from a non-broker-originated message is the MAIL FROM: address. All Non-brokers have a @notes.thefirm.com address while all brokers have a @cf.thefirm.com address. Unfortunately, this distinction doesn't help because messages are routed on the basis of the RCPT TO: address NOT the MAIL FROM: address. So, The Firm consulted with Sendmail and asked if a custom policy rule set that could route a message on the basis on the MAIL FROM:, instead of the RCPT TO: could be created.

Note: The extensibility and power of the Sendmail Sentrion Appliance policy and routing capabilities enabled The Firm to extend the system to satisfy this very complex requirement. For example:

Scenario One (no archive is created)

- An outbound email message is sent by a non-broker Firm employee external.user@gmail.com from The Firm's internal Lotus Notes system. Notes hands the message to a layer of Sendmail systems running the custom "Sender Routing" policy rule set
- Upon receipt of the message the Sendmail system processes the custom policy rule set which checks the domain part of the MAIL FROM: address in the envelope. If the address is @notes.thefirm.com the system routes the message on the basis of the domain part of the RCPT TO: @gmail.com because the Sendmail policy system does NOT have a sender routing rule for the @notes.thefirm.com domain. The message is passed (up) to The Firm's outbound mail servers and delivered to the intended Gmail recipient
- Note that the message did NOT route via the Archive solution

Scenario Two (archive is created)

- An outbound email message is sent by The Firm's Broker to external.user@gmail.com from The Firm's internal Lotus Notes system. Notes hands the message to a layer of Sendmail servers running the custom "Sender Routing" policy rule set.
- Upon receipt of the message, the Sendmail MTA, as a function of the Sender Routing rule, checks the domain part of the MAIL FROM: address in the envelope. Since the domain part in this example is @cf.thefirm.com the Sendmail MTA DOES have a sender routing rule for the @cf.thefirm.com domain, and the MTA routes the message to the Archive system
- Upon receipt of the message the Archive system makes a copy of the message and, since it is NOT running any custom rules, routes the message to the internet on the basis of domain portion of the RCPT TO: @gmail.com
- Note that the message DID route via the Archive solution.

Enhanced TLS Policy Rule Set Requirement:

The Firm also had an additional requirement to better track TLS encryption metrics to produce more meaningful TLS encryption reports for management.

TLS encryption activities are logged via 'syslog', but the entries in the logs are not sufficient.

The Firm consulted with Sendmail to see if a custom policy rule set to add information to the "stock" TLS log file entries could be created.

Ultimately, the enhanced TLS logging allowed The Firm to produce the following metrics:

Outbound Metrics

- Number of individual messages sent, successfully, via TLS.
- Percentage of messages being sent via TLS, as opposed to clear text.
- Number (and Name) of the Domains The Firm is communicating with via TLS
- Percentage of Domains being sent via TLS
- Top 10 Domains, based on message volume, where TLS is NOT being utilized.

Inbound Metrics

- Number of Messages Received via TLS
- Percentage of Messages Received via TLS, as opposed to Clear Text
- Number (and Name) of external Domains taking advantage of The Firm's TLS Services
- Top 10 Domains, based on message volume, where TLS is NOT being utilized.

Market: County Government

Requirement: Messaging metrics for HIPAA compliance

Integration Points: Voltage Encryption

An Association of Counties (each state in the U.S. has an Association of Counties) had two distinct messaging requirements: they needed to ascertain metrics regarding HIPAA compliance in email sent by their employees and to encrypt only messages sent out by their Human Resources department. Sendmail extensible policy and routing capabilities allowed the Association to meet both requirements.

The Association's Human Resources Department requires all messages sent by anyone in the HR department to be encrypted. The Association uses an optional Sentrion encryption application powered by Voltage IBE to realize this requirement. Their Sentrion's are configured to always encrypt messages sent by anyone in their Human Resources department based on their specific email address. Additional policy rules have also been created to encrypt messages sent to specific external addresses, such as mail sent to a "large health care provider."

The Association also knew that some email messages being sent by their employees were subject to HIPAA regulations, but they didn't know how many; nor did they know what specific type of HIPAA information their employees were sending. Before making a decision about how to best bring the Association into compliance, their legal team wanted to know more about what was being sent.

Through the use of Sendmail's policy capabilities, the Association was able to produce reports that tracked how many messages containing information subject to HIPAA regulations were being sent and, more importantly, how much and what type of HIPAA information was contained within each message. This was achieved by associating all HIPAA terms and phrases with a score in Sendmail's policy engine. Multiple reports were created to give management very precise reports on HIPAA compliance. The first report was for email messages with a low score (0-100), the second report for messages that had a moderate amount of information (101-500) and a third report for messages that contained a significant amount of HIPAA information (501 to 10000).

Right now, the Association's legal team is actively reviewing the reports generated by Sendmail's policy engine. These reports will help them gain a more complete understanding of the kind of HIPAA information being sent via email and how they can best bring the Association into compliance.

Market: Banking/Financial Services

Requirement: Integrate e-mail traffic from three different legacy groupware systems with full redundancy; perform gateway scanning and content inspection for corporate compliance.

Integration Points: LDAP, Lotus Notes, MS Exchange and Oracle CS

A large Japanese Bank has three different legacy groupware systems: Lotus Notes, MS Exchange and Oracle CS. In order to integrate email traffic from these different systems, the bank built a fully redundant e-mail gateway with Sendmail products. The gateway also performs various filtering services such as: Anti-virus, Anti-spam, archiving, and deep message content inspection for corporate compliance.

The Sendmail policy engine achieves the integration of the three systems by passing incoming messages through the custom bank policy, which queries an LDAP directory to determine where the message should be routed. Based on the results of the policy processing, the message is delivered to the appropriate back-end mail store. Separate divisions at the bank run each of the three back-end mail stores, so they have completely different rules and policy requirements based on a company-wide corporate compliance structure. A single Sendmail cluster handles all three policy sets. The servers in the cluster are also deployed in a redundant, disaster-safe fashion, i.e. they are in two geographically different locations.

Market: Diversified Manufacturing

Requirement: Secure email routing between partners

Integration Points: Private network; domain and address email lists

A very large diversified U.S. manufacturing company communicates with hundreds of business partners on a daily basis. The company particularly needs to protect the confidentiality of its email communications with one of their largest business partners, a division of the parent company.

The specific requirements for this use-case are:

- Messages sent by employees to the Business Partner are routed through a private connection (not via Internet)
- Messages sent by employees of the Business Partner to Internet addresses are only allowed to be delivered if the sender is authorized to send Internet emails
- Messages received from the Internet for the Manufacturing Company employees will only be delivered to their destination if the recipient is authorized to receive Internet emails
- Messages sent to the Internet by authorized Manufacturing Company employees need to have the sender domain name rewritten into a “friendly name”

This specialized policy-based routing is accomplished using Sendmail policy rule sets which, in the customer's legacy environment, use existing email address and domain lists rather than a directory service.

Market: Government

Requirement: Protect overall domain reputation

Integration Points: External database

A branch of the Federal government uses separate mail domains for each of its 100 offices, as well as for a number of branch organizations. For a variety of purposes, the offices occasionally send out large volumes of email to their constituents through the same set of outbound SMTP servers. If, for whatever reason, one of these mailings triggered a blacklist, the whole set of legislative branch domains had been affected.

To solve this issue without an additional investment in hardware (i.e. to physically separate each office's outbound SMTP server), the legislative branch implemented custom Sendmail policy rule sets. These rule sets segregate each individual office's outbound email to a separate virtual IP on the same set of physical SMTP servers.

By leveraging Sendmail's intelligent policy and routing capabilities, which didn't require the purchase of additional hardware or maintenance contracts, this government agency was able to save significant amounts of tax payer money.

The Sendmail policy rule set queries the sending IP address information and then performs a database lookup to locate the appropriate outbound IP address for that incoming IP (office). Outbound email that does not match one of the defined sender domains is sent on the server's default IP, and also triggers a notification to the mail administrator.

Note: Again, the flexibility of being able to leverage “external systems” to help perform policy processing enables organizations to make more intelligent message routing and delivery decisions.

With this sophisticated policy and routing configuration, even if a particular office should get blacklisted, it won't affect the other subdomains.

Market: Leading professional societies for the engineering and technology community

Requirement: Email address re-writing and integration with hybrid email infrastructure

Integration Points: Off-site AV/AS service

This Institution provides a global knowledge network to facilitate the exchange of knowledge and ideas and promotes the positive role of Science, Engineering and Technology in the world. They have more than 150,000 members in 127 countries and has European, North American and Asian-Pacific offices. The Institution provides members with an email aliasing service that creates a virtual mailbox at the Institution's domain; this allows members to include a valuable and prestigious mailbox in their professional title.

Sendmail Sentrion Appliances deployed at the gateway accept Internet mails for both internal staff and members. Sentrion policies determine if the email is from a member or internal staff. If it is from a member, the policy processes an alias re-write for the member email and then routes the message back to the Internet for delivery to their final ISP mailboxes.

Internal staff emails are routed and delivered to their Microsoft Exchange servers. This approach has the added benefit of providing recipient validation by accepting only emails that are valid and exist in the aliases database.

In addition, the Institution uses policies to add disclaimers to messages depending on the source of outgoing emails. For example, staff users have a disclaimer automatically added to their outgoing email, while member email does not. A second policy handles email notifications when inbound emails are destined for employees who are no longer with the organization.

Additionally, the Institution chose a hybrid email security approach of outsourcing their basic anti-virus and anti-spam function to Message Labs and using Sentrion's for their core messaging infrastructure. Two Sentrion's replaced what six legacy systems used to do in addition to managing the traffic between Message Labs and the use-case described above.

Market: IT Solutions and Services

Requirement: Support a "Lifetime Email Address" with global routing and delivery

Integration Points: External aliases database

This large well known IT Solutions and Services Company provides IT know-how in the area of software development, services and solutions. Their ability to offer their industry and business expertise from a single source gives them a unique position in the market. The company has 43,000 employees spread across the following business groups:

- Business Innovation Center, Switzerland
- Development Innovations and Projects, Greece
- Program and System Engineering, Austria
- Business Services, Germany
- Information Systems Ltd., India

The Company supports a concept of a "Lifetime Email Address" that follows employees and clients wherever they go no matter where they are located -- either on their own premises or at on-site locations engaged in long-term customer projects.

The Company's UK organization uses Sentrion Appliances for their Internet-facing gateways. This is part of a larger gateway backbone that links into the central WAN at the Business Services group in Germany. The UK gateway is primarily used to route email for internal UK staff and clients. A combination of policy rule sets and aliases databases facilitates the solution to their requirements. Although the gateway services around 20-30k staff + clients users, the aliases database-mapping contains in excess of 560,000 entries.

In addition, the Company's UK IT group provides outsourced relay services for a number of high value small Banks.

Note: With this complex mix of email policy and routing requirements, the company needed a solution that was extensible, reliable and secure. Sendmail was the only company they trusted to provide an Optimized Messaging Infrastructure to address their requirements.

Market: Banking/Financial Services

Requirement: Consolidate multiple email domains and message stores after merger without impacting established brand names

Integration Points: Lotus Notes, Microsoft Exchange, iPlanet, and LDAP

When two major U.S. banking firms merged each of them had a number of different email domains. This Bank required the consolidation of all the different message stores (Lotus Notes, Microsoft Exchange, iPlanet, among others) associated with the different domains. However, the Bank did not want this consolidation effort to impact the well-known, branded domain names.

Sendmail Sentrion Appliances successfully address this complex routing requirement. Multiple Sentrion's are used with the Bank's LDAP directory-syncing functionality and intelligent policy-processing engine to collate each user's message store and their various email addresses, including their primary externally-known brand email address.

Sentrion's intelligent policy and routing components were configured to deliver all outbound email to the correct external gateways, and route all internal email to the correct mailstores. Sentrion policies also determine which messages should be routed over internal private networks and which messages require routing to their email archive service.

Market: Financial Services

Requirement: Remove and save to local disk email attachments of certain sizes when sent to specific users

Integration Points: Custom user database list

This large US-based Financial Services firm required the automatic removal of large email attachments sent to certain sets of users. Some users were allowed to receive attachments up to 25 MB while others could receive message attachments up to 50 MB.

Policies were set up in Sendmail's policy engine to determine:

- If the message has an attachment
- The size of the attachment
- Who the recipient is via a lookup in the custom user list

Based on the results of the policy processing, attachments are stripped from the message and saved to a local disk. The email message is then delivered to the recipient with a custom pre-pended notification and a link for the recipient to retrieve the file (original attachment) over HTTP instead of receiving it in email.

Market: Systems Integration

Requirement: Integrate hybrid messaging infrastructure; re-route messages sent directly to internal MTA's to hosted anti-spam service

Integration Points: Postini (Google) hosted anti-spam service

This Systems Integrator uses a hybrid messaging approach using the Postini/Google hosted anti-spam solution for basic filtering and Sendmail for its critical messaging infrastructure. The organization will only accept email that comes from Postini servers however, some internal applications, and even some users, were sending email directly to internal MTA's (using the IP addresses of the MTA's). The Integrator did not want to drop or deny this email; they wanted a policy which would re-route mail that was sent directly to MTA's to Postini for appropriate filtering. The Sendmail solution was able to support a custom policy that would determine if a message came from Postini, if not, the policy would route the message to Postini for spam scanning.

Market: Utilities

Requirement: Replace failing Sophos and Trend Micro systems

Integration Points: Replicate and improve policies from legacy Trend system

This well known North American utilities provider had been using Sophos Pure Message and Trend Micro for their spam and virus protection. However, the Utility had complex requirements that those systems were not effectively managing. This use-case illustrates one example of the successful realization of those requirements through Sendmail's flexible policy engine and complex routing capabilities.

The utility provider has a policy that only certain users are allowed to receive attachments in email messages. The legacy system could only implement an "all or nothing" attachment policy – if a message with an attachment with multiple recipients was sent and one of those recipients was on the "not allowed to receive attachment" list, the attachment would be stripped from the message and none of the recipients would receive the attachment.

Sendmail's highly flexible policy management capabilities enabled the utility provider to implement a much more robust and user friendly attachment filter policy. The Sendmail solution solved the problem by implementing a policy which used envelope-splitting to apply individual policies to each recipient of the message. Envelope-splitting within a policy enables individual users who are allowed to receive attachments to receive them even if there are recipients listed which are not allowed to receive attachments. This provides them much needed flexibility and fine grained control over their attachment filtering policies. All Sophos PureMessage word lists and Trend Micro policies were easily migrated to the new Sendmail solution, including this important attachment filtering policy.

Note: Envelope-splitting is a unique and very powerful function of Sentrion's policy engine.

Market: Defense Contractor

Requirement: Ability to execute multiple types of message actions on any given policy; create highly custom policies

Integration Points: LDAP

This large defense contractor has 80,000 users and receives up to 14 million email messages per day. Sendmail messaging infrastructure manages a large percentage of this email traffic, which has a number of complex policy and routing requirements.

For instance, different departments require custom policies that rely on LDAP for intelligent message routing and address rewriting for different business units. The Defense Contractor also has complex policy requirements that require the option to execute any number of message actions depending on the results of the policy processing--such as: add a recipient, annotate the message, log the event, or textize the message.

Another of their complex policy processing needs requires the Sendmail policy engine to interface with external systems so that they can make more intelligent decisions on message policies, routing and delivery.

The Sendmail messaging infrastructure also gives the Defense Contractor the flexibility to control bandwidth and network usage.

Market: Healthcare

Requirement: Tracking of all customer service emails in corporate database without affecting flow of email

Integration Points: Corporate IBM DB2 database

This large well known healthcare organization uses a set of predefined customer service email addresses such as generalinquiries@lhco.com and customerservice@lhco.com, etc. For tracking and follow-up purposes all of these email addresses have to be stored in a corporate IBM/DB2 database.

All messages sent to any of the customer service email address are processed by the Sendmail policy engine which has custom rule sets to:

- Identify email messages based on the presence of one of the customer service addresses as a recipient
- Parse the messages into their individual components (envelope, headers, body, attachments)
- Inserts the data into the DB2 database which is hosted on a remote server

Market: ISP

Requirement: Reduce overwhelming message traffic due to non-delivery reports (DSNs)

Integration Points: IronPort

A large European internet service provider offers a range of services including internet hosting and managed storage among many others to more than 25 organizations, funds and programs of the United Nations.

This organization currently uses IronPort filtering products at the gateway with multiple Sendmail products internally to handle reliable mail routing and delivery. However, the IronPort product was unable to address a problem they were having with heavy inbound mail traffic due to DSNs, which was caused by an accidental internal virus outbreak.

The power and flexibility of Sendmail's email policy, routing and delivery products enabled the organization to quickly and easily address the problem that could not be handled by the IronPort appliance, which was deployed for basic email filtering.

Market: Entertainment

Requirement: Segment message traffic and delivery priority; custom attachment filtering

Integration Points: LDAP

This media giant has over 135,000 employees and dozens of subsidiaries and business units. As a result, they require a very complex messaging infrastructure. This use-case is one of many examples of how they rely on Sendmail to manage, segregate and prioritize high volumes of messages.

- In addition to using port 25 for their MTA communications, the company uses other ports to keep email traffic segregated based on origination and destination or class of traffic. Segmentation is also controlled by the presence of multiple IP addresses on a single server, which bind to a Sendmail MTA with a specific service or path
- Policies sets determine and enforce that messages destined to the Internet be segregated into specific outbound queues. Each of these messages is assigned to a unique IP address based on destination groupings defined in an LDAP directory (business partner, large ISP, etc). After one delivery attempt, messages are moved into segregated low priority queues for future attempts
- Messages destined to internal destinations are segregated into specific queues based on destination groupings / route tree as defined in LDAP
- Policies leverage LDAP to control the ability for users to send/receive to certain designations

Content and attachment filtering is performed based on values found in LDAP per organizational unit or user. Customized attachment rejection notices are generated as needed and sent back to the sender.

Market: Online Content Provider

Requirement: Manage bounced and undeliverable email

Integration Points: Opt-in mailing databases

This online content provider sends thousands of email-based newsletters and special offers to their opt-in customers. Given the size of their opt-in distribution lists, many email addresses become invalid over time. The company was having trouble managing their bounces and opt-in database.

The company needed to keep track of which email addresses were bouncing so they could update their opt-in lists and reduce the amount of non-delivery spam reports they were receiving. They knew that Sendmail Sentrion Message Processors could manage this complex, high-volume bounce management problem. The solution was to create custom policies based on sample non-delivery reports

Now, upon reception of a bounced message, Sendmail Sentrion's are configured to process the non-delivery report, and to extract the [To:] addresses that generated the bounce. These addresses are then exported to a tab-delimited file which the company integrated into their automated system to update their opt-in mail lists. The customer had requirements to deliver the tab-delimited file in a number of different ways, including via SCP, copied to an NFS share, or saved locally. Sentrion was able to handle these custom requirements with ease.

HOW DO SENDMAIL PRODUCTS ADDRESS THESE COMPLEX REQUIREMENTS?

With 25 years' experience in Internet messaging, Sendmail is able to provide solutions for the worlds most complex messaging challenges. This is accomplished by giving our customers the most powerful and flexible Message Processor and Policy Management solutions available on the market today.

Sentrion Appliances

Sentrion Message Processors provide all-in-one high-performance Message Processing with 360° protection for clean, secure, compliant and authenticated messaging.

Sentrion is a purpose-built, policy-centric and high-performance Message Processing Appliance for:

- Gateway Management with intelligent message routing and delivery
- Inbound Protection against spam, viruses and other malware
- Email Authentication to prevent phishing and fraud
- Outbound Data Leak Prevention for compliance and content protection
- Intra-company Message Management and routing.

Base configurations include:

- Enterprise-grade high-performance 64-bit architecture
- High-performance industry standard MTA and intelligent connection controls
- Centralized policy management with highly accurate and intelligent policy engine
- Email Authentication
- Role-based Access Control and User Interface
- Message Quarantine

Highly Accurate and Intelligent Policy Engine

As noted throughout this tech-note, the Sendmail policy engine is one of the key components of Sentrion Appliances – it is what enables our customers to solve very complex messaging problems. So why is Sendmail's policy engine so different than other policy engines? The answer to this question would require a long and extensive whitepaper, but above and beyond the unprecedented amount of flexibility available through the standard policy interface, the extensibility of the policy engine is critical.

Extensibility – The Sentrion eXtensible eXpression Language (XXL)

"...I imagine how Sentrion can make logical calculations and perform real-time updates to external databases and applications based on a policy triggered from an SMTP email. How about when our help desk responds to a business customer, we encrypt the message, but just prior to the encryption we add a copy of the original customer email and our response into a CRM, help desk, finance, healthcare, or other application. And being able to query an external system (versus building word lists) in real time to make a decision on whether to encrypt, drop, quarantine, alert, or bounce an email is incredible! The possibilities seem endless with XXL. I can't wait to dig deeper."

- Sendmail customer commenting on Sentrion's policy engine extensibility

Limitless Policy Conditions and Actions

A number of the use-cases in this tech-note discussed the power of Sentrion's policy engine. In addition to taking advantage of XXL, the ability for the Sentrion policy engine to specify any number of different policy conditions and actions, per policy, is required to achieve the complex routing and delivery requirements outlined. The chart below provides some out-of-the-box example policy conditions and actions provided with Sentrion.

Policy Conditions	Policy Actions
<p>Specifies the conditions under which the specified message actions will be applied to messages</p> <ul style="list-style-type: none"> • Any attached file • Any attached or embedded file • Any MIME body part • Any recipient • Address • Address (list) • Anti-Abuse Shield (spam) • Anti-Abuse Shield (virus) • Directory Attribute • GLBA Lexicon Score • Header • HIPAA Lexicon Score • Message Contains HTML Script • Message Content Type • Message HTML Tag Match • Message Property • Message Text Match (list) • Policy Comment • Priority • Random Sample • Raw Message Text • Recipient Count • Sender ID Status • Sender Type • Size 	<p>Specifies one or more message actions to perform if the message conditions specified are met</p> <ul style="list-style-type: none"> • Add Header • Add Recipient • Annotate Message • Increment Policy Counter • Log Event • Policy Comment • Remove Header • Remove Message HTML Script • Rewrite Header • Rewrite Raw Message Text • Send Notification Message • Set Disposition Set Header • Set Message Property • Set Status acceptance • Stop Policy Processing • Textize Message



Also available as a virtual appliance with Sentrion MPV

ABOUT SENDMAIL

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.

CONTACT US

For more information or to setup a demonstration, contact us at sales@sendmail.com, or phone 877-363-6245. Also ask us about our 360° Messaging Assessment Program.

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