



Security

Mail Marshall Content Filter

MailMarshal xSP is a hosted application that allows a company to enforce their limitations and restrictions for e-mail communications, otherwise known as an Acceptable Usage Policy (AUP)

Without an AUP in place, a company cannot control or reduce the occurrence of the following types of mail:

- Viruses
- Executable Files
- Video/Sound files
- Pornography / Spam
- Profanity
- Large files

If you do not control these types of non-work related mail, the company can suffer from:

- Increased Bandwidth usage, resulting in slower transmission of important messages
- Decreased productivity as employees send and receive large movies, jokes etc.
- Increased Legal Liability exposure as communications from the company containing profanity may be deemed to be acceptable mannerism from the company as a whole
- Exposure to Virus infections, Trojans etc. because Executable files are not blocked.

MailMarshal and your AUP

By enforcing your AUP, the following benefits are clear:

- Increased productivity
- Decreased bandwidth usage
- Reduced legal liability
- Reduced financial implications
- Defer delivery of large emails (ie wait until after hours to deliver these large messages, thereby freeing up bandwidth during the day)



Security

Mail Marshall Content Filter

MailMarshal allows a company to implement their AUP using plain English rules. There are only three steps required to implement each line of your AUP –

1. What users must be matched
2. What conditions must be matched
3. What action must be taken on the message

By combining these three items, as well as the ability to select multiple conditions, one can easily create rules that match your AUP.

For example, to block all incoming video files, a rule is created that:

1. Matches all users in your organization
2. Matches any message containing files of type Video (mpg, avi etc.)
3. Quarantines the message and sends a notification informing the sender and recipient that such messages are not allowed by the AUP

Should the message be work related, the administrator can easily release this message from the quarantine folder to be delivered to the intended recipient.



Security

Mail Marshall Content Filter

Key Features

- Full control of rules, security and mail by the customer
- Multiple Administrators per domain
- Individual security on mail handling (e.g. marketing manager can release mails for marketing department only)
- Web Based Console allows true remote capability (IE 5+ required for full functionality)
- Notifications of quarantined messages
- Pre-defined templates for rapid deployment
- 7 day "Quarantine" Folder
- Parking Folder for deferred delivery
- Graphical and Tabular reporting with drill-down capability to each individual message
- Full audit tracking of all changes and message release
- Inbound and Outbound Mail Scanning
- Virus Scanning
- Rule Summary for easy confirmation of policy implementation
- ASP Hosting gives maximum bandwidth reduction

Restrictions / Licensing

- A 30 day free trial is available
- Minimum of 1 month contract period.
- Each unique user in a domain requires a license
- "Maildrop" customers require licenses for each unique email address in their domain
- MailMarshal will reduce the number of Spam/Porn messages to your organization, not completely eliminate them. No product stops all spam/porn messages with zero false positives.

Technical Information

- MailMarshal requires that the MX record of the domain be changed to point to the MailMarshal Servers
- MailMarshal is a load-balanced solution to ensure redundancy and speed

Customer Responsibilities

- It is the responsibility of the customer to manage all the rules and quarantined messages of their domain.



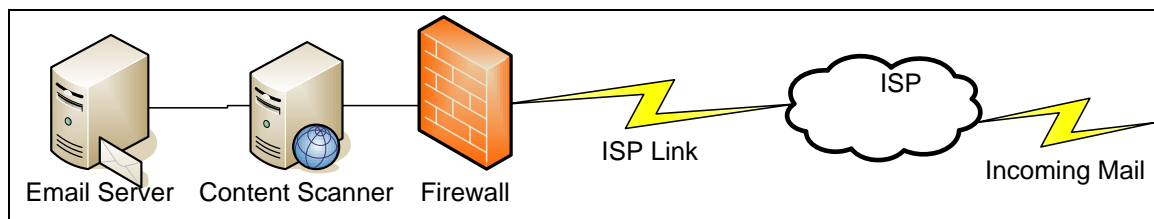
Security

Mail Marshall Content Filter

In-House Versus ASP Model

As seen in Figure 1, the traditional method of e-mail content scanning has been to dedicate an in-house server for this purpose. Whilst this ultimately provides greater control over the actual policies on the machine, there are many drawbacks to this solution as shown in Table 1. The biggest drawback is, of course, cost.

Figure 1: The traditional in-house Model



In-House Advantages and Disadvantages

Item	Advantages	Disadvantages
Cost	Software and Hardware are 100% owned	Large upfront cost for hardware Large upfront cost for software Maintenance contract required every year Salary of in-house personnel to administer service
Flexibility	Full control of policies	
Bandwidth	Outbound email content is blocked locally, even though it may only account for a low percent of the total traffic.	All inbound email content must be transferred over the link to the ISP before being content scanned
Support	Deal directly with vendor	Often a dispute between vendor and ISP when email is not working
Administration	Local administration Can view real time activity	Cannot administer outside your corporate network unless firewall is opened or vpn tunnels created

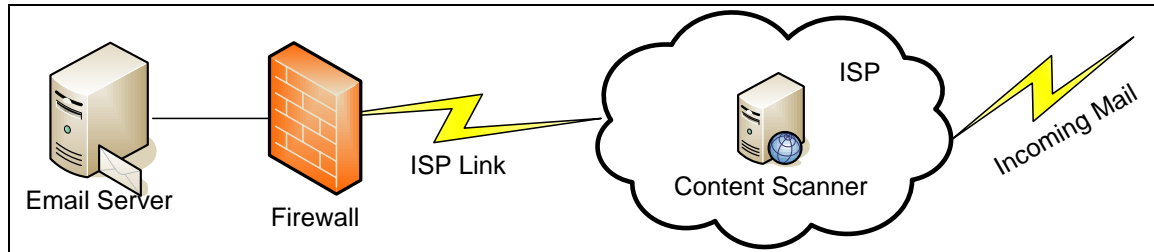


Security

Mail Marshall Content Filter

Figure 2 shows how the ASP model moves this content scanner to a centralized environment, giving the benefits shown in Table 2

Figure 2: The outsourced ASP Model



ASP Model Advantages and Disadvantages

Item	Advantages	Disadvantages
Cost	<ul style="list-style-type: none"> Fixed monthly cost No upfront costs for hardware or software No dedicated in-house personnel required No maintenance contracts Reduced costs due to lesser bandwidth requirements 	
Flexibility	Upgrades are handled by the ISP	Limitation of type of policies that can be configured
Bandwidth	Inbound traffic is content scanned and blocked before being transferred over the link to the ISP, resulting in significant reduction in traffic	Outbound content must still travel over the link before being scanned. This however is overcome by the fact that the user will stop trying to mail banned content.
Support	ISP handles support for the entire offering	
Administration	<ul style="list-style-type: none"> Can administer settings and mail, view reports using a standard web browser from any location Can view inbound queue Full Audit Log 	



Security

Mail Marshall Content Filter

Sample Reports

The report below is from a live customer – it shows the total mail delivered and blocked by the service over a one-month period.

One can see that even though, by number, only 13.75% of the messages have been stopped, this constitutes to more than 30% of the total size of the mail, or roughly 1.5GB of 4.9GB.

This represents a bandwidth reduction of over 30%.

Category	Messages	Percent	Size	Percent
Message Parked	7	0.01%	80,068.6 KB	1.61%
Sound	83	0.09%	78,289.2 KB	1.57%
Executable	104	0.11%	65,165.4 KB	1.31%
Virus Inbound	110	0.12%	13,743.3 KB	0.28%
Invalid Address	120	0.13%	360,919.6 KB	7.25%
Error Unpacking Message	165	0.18%	1,188.7 KB	0.02%
Pornography	263	0.29%	1,926.9 KB	0.04%
Video	287	0.31%	684,888.4 KB	13.76%
Connection Failed	2,816	3.08%	189,394.8 KB	3.80%
Junk/Spam	8,706	9.53%	61,035.8 KB	1.23%
Normal Mail	78,695	86.15%	3,441,696.1 KB	69.14%
Totals	91,342	100.00%	4,977,958.2 KB	100.00%



Security

Mail Marshall Content Filter

Graphically, this is represented as follows

