



Security

Mail Marshall Content Filter

MailMarshal 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 (i.e. wait until after hours to deliver these large messages, thereby freeing up bandwidth during the day)

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



Security

Mail Marshall Content Filter

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:

4. Matches all users in your organization
5. Matches any message containing files of type Video (mpg, avi etc.)
6. 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.

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



Security

Mail Marshall Content Filter

MWEB Business offers 3 flavours of the Mail Marshal Product:

Service Options	Description
Basic	<p>Spam and AV – for pre-filtering against inbound email threats, blocking all viruses and around 98% of spam. Consists of:</p> <ul style="list-style-type: none"> • Anti-Spam • 1 x Anti-Virus Scanners (MacAfee) • + 5 template rules <ul style="list-style-type: none"> ○ Block executables ○ Block Audio and Video ○ Block Image Files ○ Block Bad Language ○ Relay large messages after hours
Intermediate	<p>As above and customizable with more control over defining up to 10 rules for blocking selected content, for example by file types, images, abuse / race / hate email. Consists of:</p> <ul style="list-style-type: none"> • Anti-Spam • 1 x Anti-Virus Scanners (MacAfee and/or Norman) • Adds optional rules for the Customer to select suggested rules <ul style="list-style-type: none"> ○ Block executables ○ Block Audio and Video ○ Block Image Files ○ Block greater than 10Mb email ○ Block email with more than 50 Recipients ○ Block Bad Language ○ Block Racist / Hate Content ○ Block Invalid Recipients (Customer must provide their own whitelist) ○ AntiSpam advanced - URL censor ○ Relay large messages after hours • Includes the ability to define user group exclusions for any of these rules. • Customer has the ability to display the rule selections in the End User console
Advanced	<p>Fully loaded Content Security functionality plus the ability to custom define policy with up to 30 end user defined rules, and with spyware functionality built in. Consists of:</p> <ul style="list-style-type: none"> • Full Anti-Spam • 1 x Anti-Virus Scanners (MacAfee and/or Norman) • Adds optional rules for the Customer to select suggested rules <ul style="list-style-type: none"> ○ Block executables ○ Block Audio and Video

Copyright © 2009 MWEB Business.

All rights reserved worldwide. These Product Terms and its contents are confidential trade secrets of MWEB Business. Unauthorised duplication or dissemination of these Product Terms or any of its contents is a violation of applicable laws.

Version 01/030306



Security

Mail Marshall Content Filter

- Block Image Files
- Block greater than 10Mb email
- Block email with more than 50 Recipients
- Block Bad Language
- AntiSpam advanced - URL censor
- Spam Quarantine Management (SQM)
- Block Racist / Hate Content
- Block Invalid Recipients (Customer must provide their own blacklist)
- Generic Disclaimer Stamp on Outbound email
- Includes the ability to define user group exclusions for any of these rules.
- Customer has the ability to display the rule selections in the End User console
- Ability to define new policies
- Opens up full Policy Wizard functionality in the End Customer console for the Customer to define whatever policy they wish.
- No limit on additional rules over the basic defined rules above.

Restrictions / Licensing

- 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.



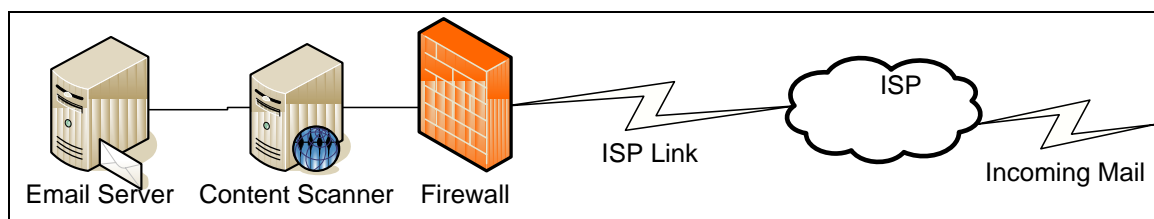
Security

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	In-house personnel to administer the service
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

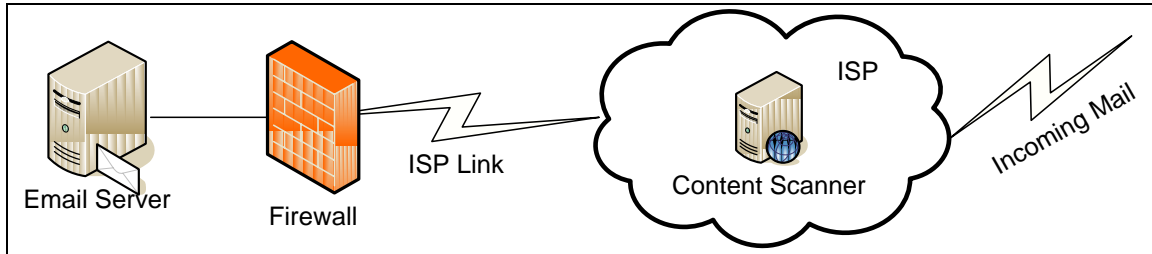
Figure 2 shows how the ASP model moves this content scanner to a centralized environment, giving the benefits shown in Table 2



Security

Mail Marshall Content Filter

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	<ul style="list-style-type: none"> Upgrades are handled by the ISP 	<ul style="list-style-type: none"> Limitation of type of policies that can be configured
Bandwidth	<ul style="list-style-type: none"> Inbound traffic is content scanned and blocked before being transferred over the link to the ISP, resulting in significant reduction in traffic 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	