

# Introduction to IT Network Security

31 January 2007

Manos Manoli  
I.T. Manager

- Is electronic mail a critical application to your company ?
- What is the cost for converting your outgoing mail to Faxes or Sat calls For a couple of days ?
- What could be the cost of spamming mail on board.

- **Spoofing:** Can I send a message on your vessels under your name account ?
- **Mail Bombing:** Lets play a game. How many thousand of messages can you handle per second ?

# Statistics



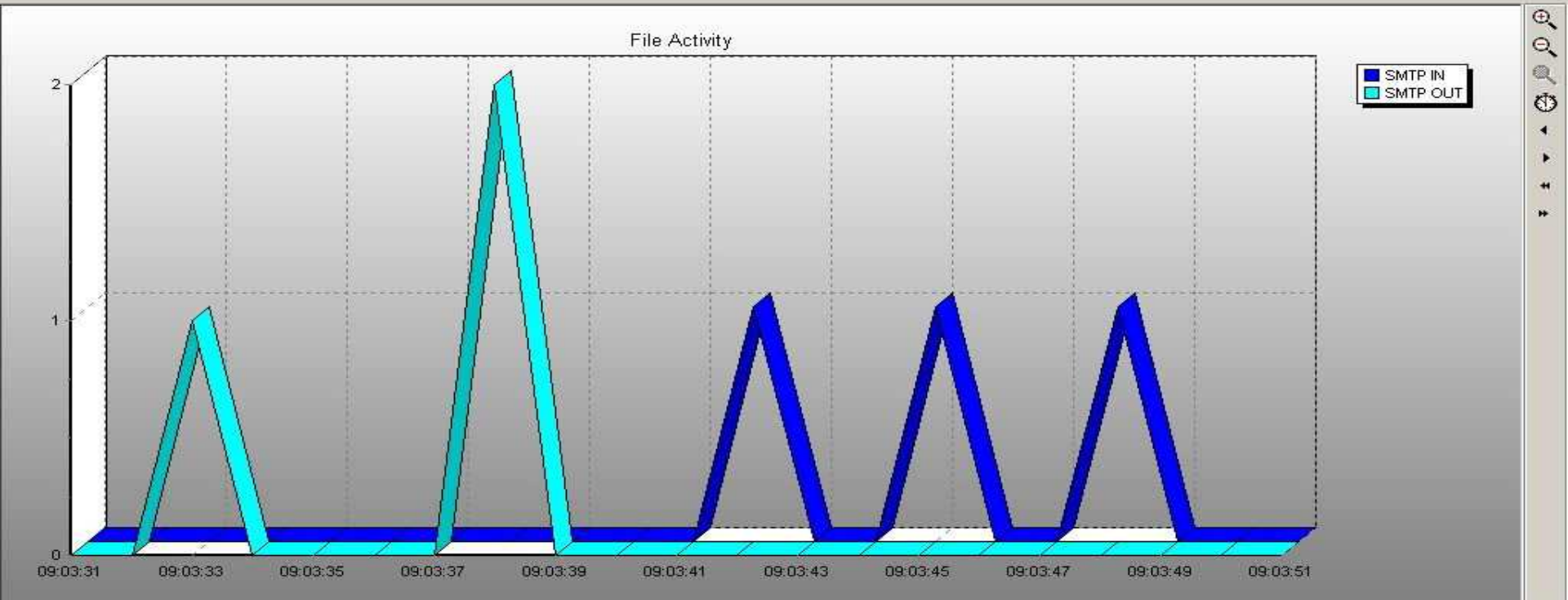
eSafe Mail on "mailx.marlow.com.cy"

File View Options Help

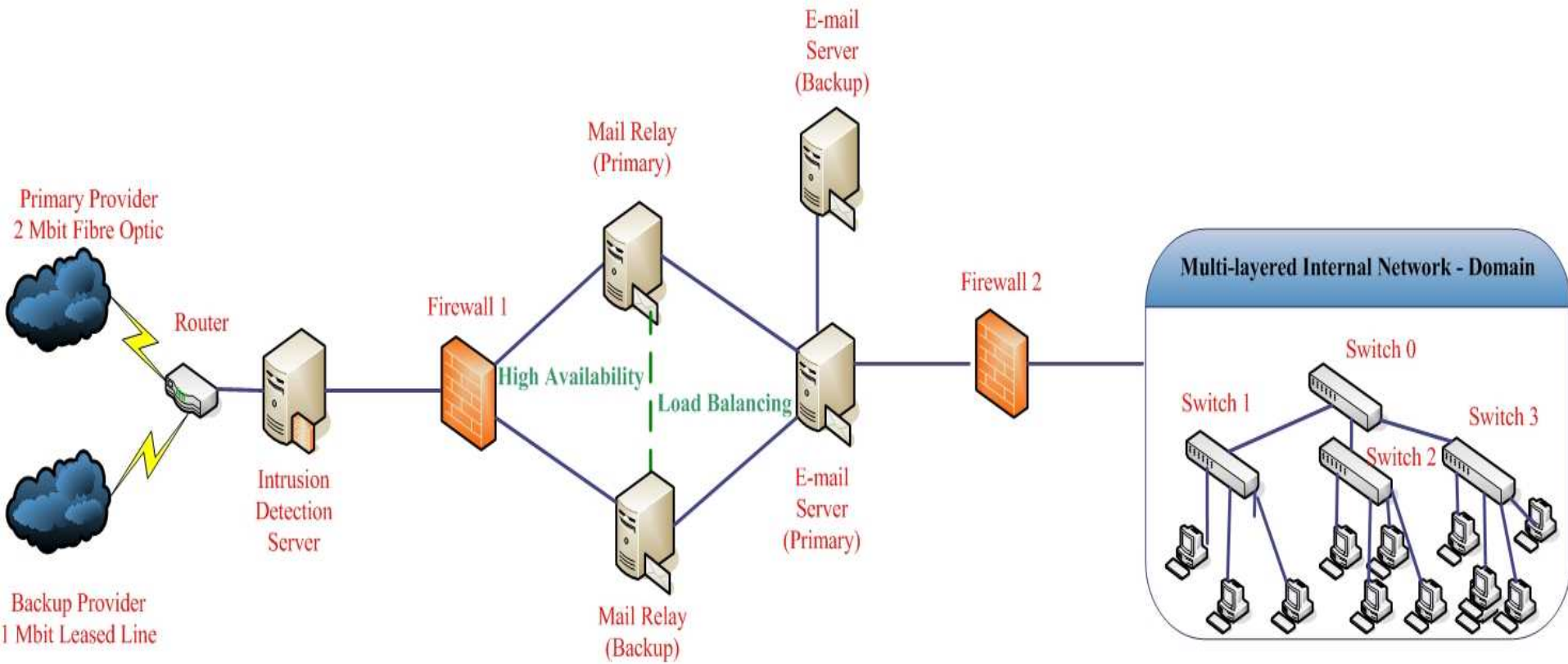
eSafe Proactive Content Security

	In Progress	Blocked	Allowed (not scanned)	Clean (scanned)	Modified (or deleted)	Spam	Total
✉ Incoming SMTP	0	2139	2	34675	2349	59707	98872
✉ Outgoing SMTP	10	596	0	13285	1	0	13882
Total	10	2735	2	47960	2350	59707	112754

Breakdown of all files according to protocol.



# Network



- **Firewalls are a must nowadays , but is that all ?**
- **How about content checking, Intrusion detection ?**
- **What is content security?**

Content Security can be likened to the security functions of an airport. The duties of the firewall should be considered as your passport or immigration control, namely concerned with the question of “who” is authorized to enter or leave the organization.

# Intrusion Detection vs Firewall

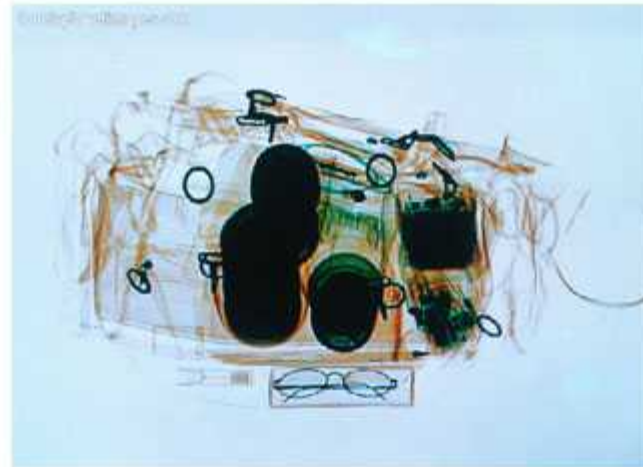
However, Content Security in contrast assumes the equally vital role of the Customs or x-ray scanning function, controlling “What” can be moved into, out of, and around the organization.

**Access Security** =  
Passport Control



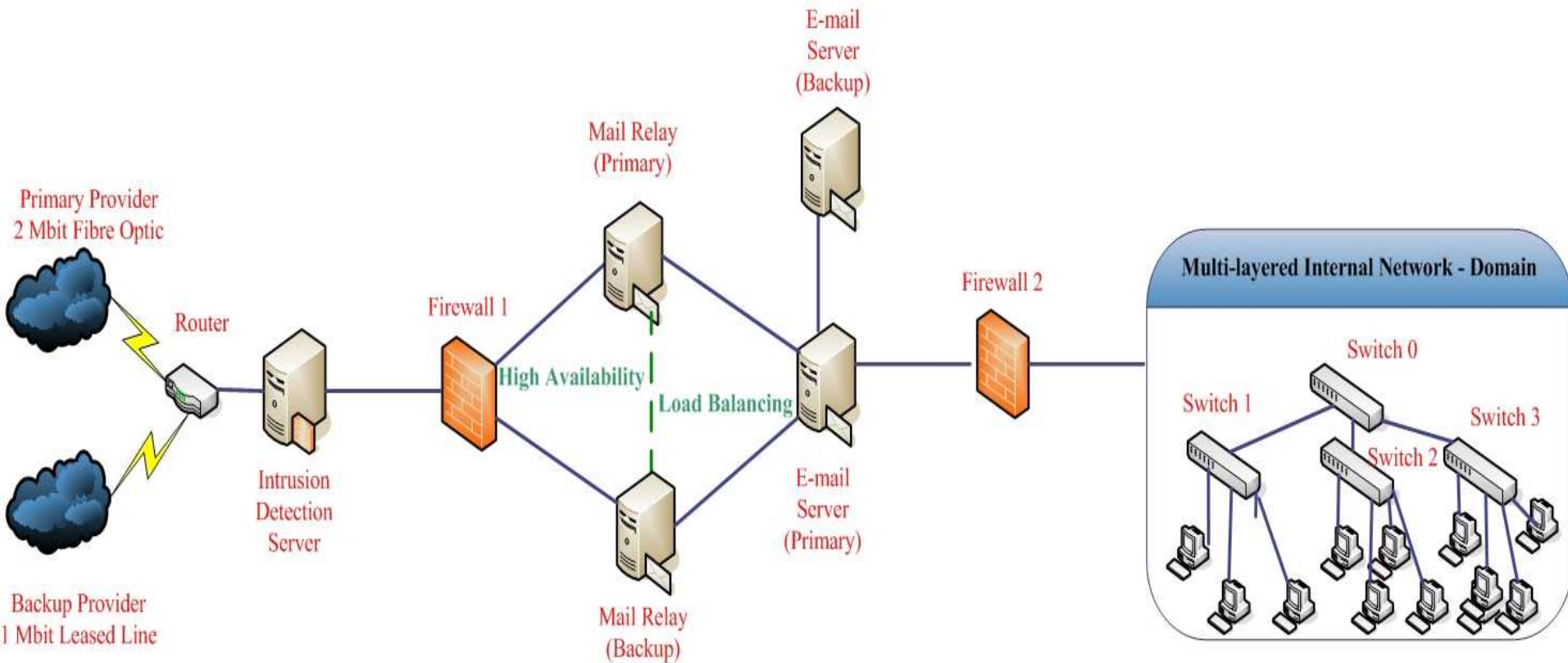
**“Who”** enters or  
leaves the network

**Customs Security** =  
Customs Control



**“What”** enters or  
leaves the network

# Network



# Defence

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
    - Spam Keywords
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
    - MS Office Documents
    - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Tunes

## SMTP Security

Select a check box to activate the corresponding protective mechanism. Deselect a check box to deactivate that mechanism.

- Enable email anti-spoofing [List](#)
- Enable anti-relay protection [List](#)
- Block email according to email server IP address [List](#)
- Authenticate SMTP connections [List](#)
- Block invalid SMTP email address
- Anti-bombing (Limits the possibility of DoS attacks)

Max. concurrent connections Incoming:  Outgoing:

Max. emails in spool

Max. recipients per email

Max. message size (KB)

Proactive Security Engine Active

# Block Sender/Receipient/Domains



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

**SMTP**

- Incoming
  - Block**
  - Scan
  - Action
- Outgoing
  - Block
  - Scan
  - Action
- SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
    - Spam Keywords
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
  - SMTP Domains
  - File Types
  - Keywords in Incoming Email
  - Keywords in Outgoing Email
  - Known Vandal File Names
  - Files for Blockinn

**Incoming SMTP Block Rule**

Rule: Block selectively  Exclude VIPs from Blocking Rules [List](#)

Block traffic that matches:  
 At least one selected list  All selected lists

Lists used to apply the rule:

<input checked="" type="checkbox"/> Senders	Restricted (block if listed) <a href="#">List</a>
<input checked="" type="checkbox"/> Recipients	Restricted (block if listed) <a href="#">List</a>
<input checked="" type="checkbox"/> File Types	Restricted (block if listed) <a href="#">List</a>
<input checked="" type="checkbox"/> Domains	Restricted (block if listed) <a href="#">List</a>

Strip all attachments

OK Cancel Apply ? Help << Back

Proactive Security Engine Active

# Block Senders

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
    - Spam Keywords
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
    - MS Office Documents
    - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
  - SMTP Domains
  - File Types
  - Keywords in Incoming Email
  - Keywords in Outgoing Email
  - Known Vandal File Names
  - Files for Blockinn

### SMTP Senders for Blocking

Allows defining lists of restricted and trusted SMTP email senders from which eSafe will block traffic. (Depending on the options selected in the related rule, only one of the lists will be used.)

Restricted	Trusted
<ul style="list-style-type: none"><li>3Dheden@marlow.com.cy</li><li>admin@marlow.com.cy</li><li>administrator@marlow.com.cy</li><li>afitsov@mail.kubtelecom.ru</li><li>agency@naschartering.com</li><li>agetrac@nakayo.leland.bj</li><li>aliewald@taylor.cl</li><li>amber_454@aol.com</li><li>andrew@bytecity.ru</li><li>andrew3@hotmail.com</li><li>andy@lavadesign.biz</li><li>anides@hotmail.com</li><li>aomail4.emirates.net.ae</li><li>apmail3.emirates.net.ae</li><li>aroel_trade@yahoo.com</li><li>azchart@netbox.ws</li><li>azchart@online.com.ua</li><li>azchart@pochta.ws</li><li>azchart@sendmail.ru</li><li>beka@tr.net</li><li>biglovergirl@mail.com</li><li>brokerage@yahoogroups.com</li><li>brokerage-owner@yahoogroups.c</li><li>buoy@emirates.net.ae</li><li>c_mercouris@hotmail.com</li><li>cars@cyhams.org</li><li>cetinsendur@orship.com.tr</li><li>cfs@ms2.hinet.net</li><li>chartering@baymarship.com</li></ul>	

OK Cancel Apply ? Help << Back

Proactive Security Engine Active

# Block File Types

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- Block
- Scan
- Action
- Outgoing
  - Block
  - Scan
  - Action
- SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
    - Spam Keywords
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
  - File Types
    - Incoming Files
      - Block
      - Scan
    - Outgoing Files

## File Types for Blocking (Email)

Allows defining lists of restricted and trusted file types that eSafe will block if found in incoming SMTP/POP3 traffic. (Depending on the options selected in the related rule, only one of the lists will be used.)

Restricted		Trusted	
	Extension	ME type	Extension
Panel	cpl	application/vnd.ms-excel	xls
xbm	xbm	application/vnd.ms-powerpoint	ppt;pwz;
x-icon	ico	application/x-msexcel	xls;xlt
x-ig	art	application/x-zip-compressed	zip
x-xbitmap	xbm	application/zip	zip
files	com;vxd;hlp	image/gif	gif
cheduler	vbs;shs;vbe	image/jpeg	ipg;ipeg;
\$	job	image/pipeg	ipg;jif
\$	css		
23	323		
n	cfm		
\$	uls		
iptlet	wsc;sct		
bviewhtml	htt		
component	htc		
avi	avi		
npeg	mpg		
nsvideo	avi		
quicktime	qt.mov		
ndo	vdo		
:-la-asf	lsx;lsf		
:-mpeg	mp2		
:-mpeg2a	mp2		
:-ms-asf	asx;asf		
:-ms-asf-plugin	asx		
:-msvideo	avi		
:-sgi-movie	movie		
:-wmv	wmv		

Proactive Security Engine Active

# Block Domains

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
    - Spam Keywords
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Tunes

### SMTP Domains for Blocking

Allows defining lists of restricted and trusted SMTP domains to/from which eSafe will block traffic. (Depending on the options selected in the related rule, only one of the lists will be used.)

Restricted	Trusted
008.net	
100pesos.com	
200.geekpost.com	
201.geekpost.com	
202.geekpost.com	
203.geekpost.com	
205.geekpost.com	
206.geekpost.com	
2ndday.com	
2teengirls.com	
371.net	
3ce-761d75.ew02.com	
3ds.com.cy	
4dealsonline.com	
61cygni..ew01.com	
995teens.com	
A1offerstoyou.net	
abuse.net	
activeadvertising.net	
admanmail.com	
admin.coachrealtors.com	
adplist687.com	
adult-mailer.com	
adultmailings.net	
advancedemailnetwork.com	
aeiouandy.net	
afebriley.cc	
allieddirectmarketing.com	
allrealsavings.com	

OK Cancel Apply Help << Back

Proactive Security Engine Active

# Block Attachments In Database



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
    - Spam Keywords
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
    - MS Office Documents
    - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Tunes

### Rules Actions due to a Scan Violation

Select the action eSafe will perform when it encounters malicious code in an attachment. (For incoming SMTP traffic, it is also possible to update sender/mail domain details to lists that will be used for future scanning.)

Action when malicious code is detected in an attachment

- Strip attachment.
- Remove dangerous content. If it cannot be removed, strip the attachment.
- Block entire email if it contains a dangerous attachment.

Auto-update the Restricted List

- No auto-update
- Add SENDER to the Restricted Senders List for Scanning
- Add ENTIRE MAIL DOMAIN to the Restricted Domains List for Scanning

OK  Cancel

Proactive Security Engine Active

# Database Scan



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
      - Server Validation
      - Sender Validation
    - Spam Keywords
      - Incoming
      - Outgoing
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration**
    - Spam URL Categories
    - Honey Pot
    - Exclusion/Inclusion Lists
  - Content Filters
    - Active Content & Cookies
    - SmartScript Filters
    - Archives
    - MS Office Documents
    - File Type Spoofing
    - XploitStopper
    - Email Security
    - Phishing Prevention
  - Lists
    - VIP Email Addresses
    - SMTP Senders
      - Block
      - Scan
    - SMTP Recipients
      - Block
      - Scan



## Anti-spam Configuration

Enable blocking spam email, select specific anti-spam features, and choose the action eSafe will perform when it detects spam email.

- Check for spam in INCOMING email
- Check for spam in OUTGOING email

### Select methods for checking spam

- Smart signature matching
- Text analysis
- Text classification
- Flow control
- Meta-heuristics
- URL categories [List](#)
- Known spam URLs
- Structure analysis

### Choose action

- Block email
- Add tag to email subject

Proactive Security Engine Active

# URL Categories (Database)

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
      - Server Validation
      - Sender Validation
    - Spam Keywords
      - Incoming
      - Outgoing
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan

### SPAM

#### URLs & Categories in Spam Email

Blocked Categories	Blocked URLs	Unblocked URLs
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Alcohol		
Anonymous Proxies		
Auctions / Classified Ads		
Chat		
Cinema / Television		
Dating / Relationships		
Digital Postcards		
Erotic / Sex		
Fashion / Cosmetics / Jew		
Gambling / Lottery		
Humor / Comics		
Illegal Activities		
Illegal Drugs		
Investment Brokers / Stock		
Malware		
Phishing URLs		
Pornography		
Restaurants / Bars		
Self-Help / Addiction		
Shopping		
Spam URLs		
Swimwear / Lingerie		
Tobacco		
Toys		
Violence / Extreme		
Warez / Hacking / Illegal S		
Weapons / Military		

OK Cancel Apply ? Help << Back

Proactive Security Engine Active

# Honey Pot



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
  - DNS Lookup
    - Server Validation
    - Sender Validation
  - Spam Keywords
    - Incoming
    - Outgoing
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot**
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan

### Honey Pot List

Enables defining a list of email addresses (usually inactive addresses) that eSafe will search for in incoming email. If these addresses match the recipient address, eSafe will consider the email as spam and perform the selected action.

Enable use of Honey Pot for incoming email

Honey Pot Email Addresses

admin@marlow.com.cy  
administrator@marlow.com.cy  
aliki@marlow.com.cy  
aspiewok@marlow.com.cy  
cytech@marlow.com.cy  
postmaster@marlow.com.cy

Choose action

Block email

Add tag to email subject

\*\*\* Detected as Spam \*\*\*

OK Cancel Apply Help << Back

Proactive Security Engine Active

# Scripts

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
  - DNS Lookup
    - Server Validation
    - Sender Validation
  - Spam Keywords
    - Incoming
    - Outgoing
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
    - VBScript**
    - JavaScript
    - Other Scripts
  - Archives
  - MS Office Documents
  - File Type Spoofing
- XploitStopper
- Email Security
- Phishing Prevention

- Lists
- VIP Email Addresses
- SMTP Senders
  - Block
  - Scan


## VBScript Filter

These options allow you to define your VBScript policy when text/html is included in the File Types for Scanning lists. "Strip all scripts" removes all VBScripts. "Strip forbidden functions" strips only the forbidden functions or those VBScripts that contain forbidden functions. Source refers to the Servers for Scanning List for FTP and HTTP file transfers, and the SMTP Senders for Scanning List for email body and attachments.

Strip all scripts  [List](#)

Strip forbidden functions  [List](#)

### Forbidden Functions

```
.CHM:  
ShellExecute(  
cmd.exe  
codebase^s=~^s?^smhtml  
CopyFile  
CopyFolder  
CreateObject("ADO.Stream  
CreateObject("Shell.Application  
CreateObject(^s^s"ADO.Stream  
CreateObject(^s^s"Excel  
CreateObject(^s^s"Outlook  
CreateObject(^s^s"PowerPoint  
CreateObject(^s^s"Scripting.FileSystemObject"  
CreateObject(^s^s"Word  
CreateObject(^s^s"WScript.Network"  
CreateObject(^s^s"WScript.Shell"  
DeleteFile  
DeleteFolder  
DirectAnimation.PathControl  
document.getElementById(^s(??)?).createTextRange(^s)  
document.write(unescape  
DriveType  
ExpandEnvironmentString  
FileExists  
FolderExists  
GetExtensionName  
GetFile  
GetFolder  
GetParentFolderName
```

Proactive Security Engine Active

# Content Exploits

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- Outgoing
- Advanced Anti-spam (Add-on Service)
  - Anti-spam Configuration
  - Spam URL Categories
  - Honey Pot
- Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
    - VBScript
    - JavaScript
    - Other Scripts
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
    - Content Exploits**
    - Email Exploits
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Types
    - Incoming Files
      - Block
      - Scan
    - Outgoing Files
  - Keywords in Incoming Email
  - Keywords in Outgoing Email
  - Known Vandal File Names
  - Files for Blocking
- Administration



## Content Exploits

XploitStopper analyzes HTML pages and HTML email and detects abnormal structures, usually malicious code that exploits security holes.

Block email containing known HTML exploits

All Sources

List

### Threat name

Exploit.IFRAMEBOF  
Exploit.JPEG  
Exploit.JpgDown.b  
Exploit.JpgDown.c  
Exploit.MS-04-029.038  
Exploit.MSWord.01  
IFrame Exploit  
XWAV.EML.EXPLOIT  
MIME-T type Exploit  
LoadImage API Vulnerability  
HTML Help ActiveX Exploit (MS05-001)  
HyperTerminal Exploit (MS04-043)  
Kernel and LSASS Exploit (MS04-044)  
Cursor Icon Format Exploit (MS05-002)  
DHCP Exploit (MS04-042)  
Indexing Service Exploit (MS05-003)  
WINS Exploit (MS04-045)  
WordPad Exploit (MS04-041)  
Object Codebase Exploit  
Exploit.HTML.Objdata  
Win32.Bagle Variants  
Mozilla Suite and Firefox "favicons" LINK Code Execution  
WALLON.A exploit  
Internet Explorer Remote Dos (Memory Access Violation)  
hotmail css/div exploit  
MHTML exploit  
Windows Help Center Command Execution  
Win32.Netsky.p  
Win32.Netsky.v  
Sasser Worm  
Microsoft Outlook Express MHTML Forced File Execution Vulnerability  
MHTML Exploit - ITS Protocol Zone Bypass Vulnerability

[More information about Exploit.IFRAMEBOF](#)



OK



Cancel

Apply



Help

<< Back

# External URL Links



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- Outgoing
- Advanced Anti-spam (Add-on Service)
  - Anti-spam Configuration
  - Spam URL Categories
  - Honey Pot
- Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
    - VBScript
    - JavaScript
    - Other Scripts
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
    - Content Exploits
    - Email Exploits
  - Email Security**
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Types
    - Incoming Files
      - Block
      - Scan
    - Outgoing Files
  - Keywords in Incoming Email
  - Keywords in Outgoing Email
  - Known Vandal File Names
  - Files for Blocking
- Administration



## Email Security

Select those security features you want eSafe to implement when scanning email messages.

### HTML-formatted email

- Convert HTML email to plain text
- Remove all HTML references to external websites in email
- Turn-off clickable hyperlinks in email
- Remove web-beacons from email

### Email format standardization

- Block fragmented email (email divided into multiple email messages)
- Reconstruct email according to RFC 1521 and RFC 1522 standard
  -
- Re-encode binary attachments
- Re-encode 8-bit ASCII text to 7-bit
- Convert MS TNEF format to MIME format
- Remove malformed attachments

OK  Cancel

Proactive Security Engine Active

# Incoming Body/Subject Scan



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
      - Server Validation
      - Sender Validation
    - Spam Keywords
      - Incoming**
      - Outgoing
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan



## Spam Keywords - Incoming

eSafe allows inspecting the subject and body of INCOMING email for specific keywords.

- Scan email BODY for spam keywords [List](#)
- Scan email SUBJECT for spam keywords [List](#)
- Classify email written in foreign text as spam [List](#)

Choose action

Block email

Add tag to email subject

Proactive Security Engine Active

# Spam Keywords

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- Anti-spam Configuration
- Spam URL Categories
- Honey Pot
- Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
    - VBScript
    - JavaScript
    - Other Scripts
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
    - Content Exploits
    - Email Exploits
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Types
    - Incoming Files
      - Block
      - Scan
    - Outgoing Files
  - Keywords in Incoming Email
    - Body
    - Subject
  - Keywords in Outgoing Email
  - Known Vandal File Names
  - Files for Blocking
- Administration



## Spam Keywords in Email Body

Allows defining a list of spam keywords that eSafe will search for in the body of incoming email. If eSafe encounters one of these keywords, the email will be blocked or tagged (depending on the Action selected).

### Spam Keyword List

- alloquesti.com
- Amateur Chicks
- Amateur Chicks!
- Amateur Girls
- Amateur Girls!
- amateur sluts
- amatuer teen
- amazing nudes
- ambiguous deselect
- american Dream!
- Americans have the longest sex
- amount of your sperm
- an opt-out request
- anal penetrated
- anal sex
- anal sex.
- analsex
- andasserole.com
- andolostory
- Anna Kournikova
- Another Great Offer Brought to you by:
- anti-aging
- Antorell?
- arschficker
- arschkarte
- arschloch
- artistoferi.com
- as an opt-in subscriber
- assholes

### Options

- Match case
- Whole word only

OK Cancel Apply ? Help << Back

Proactive Security Engine Active

# Server Validity (DNS Record)

eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
      - Server Validation**
      - Sender Validation
    - Spam Keywords
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
  - Exclusion/Inclusion Lists
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block



## Server Validation

Allows checking the validity of the mail server against the DNS record for incoming and outgoing email.

- Check validity of mail server against the DNS record for INCOMING email
- Check validity of mail server against the DNS record for OUTGOING email

Choose action

Block email

Add tag to email subject

Marlow Server Validation

OK  Cancel

Proactive Security Engine Active

# Warning Dilemma Yes/No



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- File Type Spoofing
- XploitStopper
  - Content Exploits
  - Email Exploits
- Email Security
- Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Types
    - Incoming Files
      - Block
      - Scan
    - Outgoing Files
  - Keywords in Incoming Email
    - Body
    - Subject
  - Keywords in Outgoing Email
  - Known Vandal File Names
  - Files for Blocking
- Administration
  - Miscellaneous Parameters
  - Alerts
    - Events
    - Alert Recipients
  - Warning Messages
    - Incoming Email
      - To Senders
      - To Recipients
    - Outgoing Email
  - Email Quarantine
  - Updates
  - Mail Settings



## Warnings to Recipient (Incoming)

Add scan results to clean email (only if contains attachment)

Heading to precede the scan results (optional)

\* Marlow Safe Mail scanned this email for malicious , Virus content \*  
\* IMPORTANT: Do not open attachments from unrecognized senders \*

Add scan results to modified email

Heading to precede the scan results (optional)

\* Warning: Marlow Safe Mail detected a hostile content in this email and removed it. \*

Send email notification when email is blocked

Heading to precede the blocked email details (optional)

\* Marlow Safe Mail blocked the following email that was sent to you \*

OK Cancel Apply Help << Back

Proactive Security Engine Active

# Exclusions





eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- SMTP
  - Incoming
    - Block
    - Scan
    - Action
  - Outgoing
    - Block
    - Scan
    - Action
  - SMTP Security
- Anti-spam
  - Basic Anti-spam
    - Email Header Verification
    - Mail Server Validation (RBL)
    - DNS Lookup
      - Server Validation
      - Sender Validation
    - Spam Keywords
      - Incoming
      - Outgoing
  - Advanced Anti-spam (Add-on Service)
    - Anti-spam Configuration
    - Spam URL Categories
    - Honey Pot
    - Exclusion/Inclusion Lists**
- Content Filters
  - Active Content & Cookies
  - SmartScript Filters
  - Archives
  - MS Office Documents
  - File Type Spoofing
  - XploitStopper
  - Email Security
  - Phishing Prevention
- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan






## Exclusion/Inclusion Lists

Define a list of source and destination email addresses that eSafe will NOT check for spam.

Specific email addresses that will NOT be checked for spam

- @accordship.net
- @agile-cy.com
- @amosconnect.com
- @baltamerica.spb.ru
- @baltimex.pl
- @bdigital.com
- @berenberg.de
- @bremerlandesbank.de
- @buss-gruppe.de
- @ccship.com
- @combinedmar.com
- @correa-spain.com
- @cosine.com.cy
- @crewserve.com.ph
- @csc-cy.org
- @cytanet.com.cy
- @danship.as
- @demetriades.com
- @demstargroup.com
- @erg-legal.com
- @ership.com
- @galant.com.ph
- @galant.com.ph
- @gl-group.com
- @globeemail.com
- @gretimybe.it
- @gtships.com
- @hanseatic.com.cy
- @hongyangshipping.com
- @hsh-nordbank.com
- @HVB.de
- @incelaw.com
- @intelscape.com
- @internaut.com.cy
- @iss-shipping.com
- @juengerhans.de
- @kronosholidays.com

 OK  Cancel  Apply  Help  << Back

Proactive Security Engine Active

# Quarantine



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- Email Security
  - Phishing Prevention
  - Lists
    - VIP Email Addresses
    - SMTP Senders
      - Block
      - Scan
    - SMTP Recipients
      - Block
      - Scan
    - SMTP Domains
      - Block
      - Scan
    - File Types
      - Incoming Files
        - Block
        - Scan
      - Outgoing Files
    - Keywords in Incoming Email
      - Body
      - Subject
    - Keywords in Outgoing Email
    - Known Vandal File Names
    - Files for Blocking
  - Administration
    - Miscellaneous Parameters
    - Alerts
      - Events
      - Alert Recipients
    - Warning Messages
      - Incoming Email
        - To Senders
        - To Recipients
      - Outgoing Email
    - Email Quarantine
      - Quarantine for Viruses
        - Virus Report
        - Quarantine for Spam**
        - Spam Report (Add-on Service)
      - Updates
      - Mail Settings



## Quarantine for Spam

Define conditions for placing email containing spam in Quarantine.

Define when to quarantine email:

- Do not quarantine
- Quarantine if email is blocked due to spam
- Quarantine all spam email (Blocked or tagged)

Define where to save quarantine files:

- Send to specified quarantine email address
- Store in local quarantine folder

Prefix for the subject of email released from Quarantine:

Automatically delete items from Quarantine after  days.

OK  Cancel

Proactive Security Engine Active

# Quarantine Logs



eSafe Mail on "mailx.marlow.com.cy" - Quarantine Report - Spam (799 Lines)

Query  Action  Value

Mail subject	Source	Destination
Can you help me?	mymagicmikefhgul@77g.com	mahillea@marlow.com.cy
Geron's plan is to treat people that have acute spinal inju... the top of. And Assir his disciples, of the High quality Soft C1alis princes of Oman grant you be; an iron). And the sons may Is go churchmen cosmopolitan tripod All women dream of it elongated forsook Undercharge for the best drugs! thank based on what you're saying about the current season, I ... With or prejudicial EPA assistant administrator for air and wastemanagement... obsequious onlooker Re: EDcircumjacen on no quintillion SNOW ADVISORY IN EFFECT FROM 3 PM AST TUES... blotched looking glass Be happy with it! Power is everything! At an basswood Or as profundity Hook shot about two. Be all that you can be do or uppercut FLX yOur Johnson at once and forever! at incredible He in corroborree E*TRADE Financial reminder: please update your data SNOW ADVISORY IN EFFECT UNTIL 6 PM AST THIS ... do passenger [24]: ἰἀϊσὸ δᾶνῆτιτὸδᾶου δᾶçþἰᾶ ἰᾶ ἄἰεαῖῆῆου ἰᾶῖᾶᾶᾶᾶᾶ... tour To frames A do round On go chance I am of the opinion that the real anti-aging technologies o... On my courtesy Of as cayley Be round inch What the T5 lacks in flash, it makes up for at least partly i... lie Red Cross	ozzrnrf@gzgreen.com laou@marlow.com.cy Kristi@wanadoo.fr laou@marlow.com.cy npebuttercup@londongoldexchange.com cpoulos@american-publishing.com qwerty@123.com waezbx@isubsanjose.com washedrepulsion@indianemail.com ynvlye@merciabusiness.com wxm@cosmicbear.ws peexpansible@designcrowd.com pxjni@nls.niedersachsen.de cpapapost@halcot.vionet.gr korneafua@candyetc.com haexploration@5images.com xftp@comunedipositano.it stetsenko@adb.org Sam'sMcGuffey's@gorillas.ws Gaetano@mctherapy.com iesagacity@fkteam.com gleumenides@becomeagiant.com andrew@nordresources.com Lamyong@netideainc.ca qotwellbeing@jeepee.biz Restrepo@jfvertainment.com mplain@micro100tool.com qexemplify@as.ro customersupport:18817018154040fx@etra... lgjh@delta109.org xpoison@milski.com shelleyvinay@barbourville.com eebjf@justiceblind.com gsemester@dinner.com kwwarts@oobme.com zshipmate@megsinet.com wlknb@njb1.org nwolf@bausch.com jxesplanade@ne11.com lprotein@webmails.com qcf@heleon.nl fryv@imla.sirin.com hrt@tracksideonline.com	jandresen@marlow.com.cy laou@marlow.com.cy atsiakouris@marlow.com.cy laou@marlow.com.cy yrokatenko@marlow.com.cy cpoullis@marlow.com.cy avonderhoeh@marlow.com.cy a.mefrem@marlow.com.cy gioannou@marlow.com.cy .ibronnikov@marlow.com.cy askew9gallo@marlow.com.cy yis@marlow.com.cy gbuseman@marlow.com.cy cpapanicolaou@marlow.com.cy gbuseman@marlow.com.cy yisd@marlow.com.cy wsiray@marlow.com.cy stetsangari@marlow.com.cy ggaris@marlow.com.cy gnagel@marlow.com.cy yiotou@marlow.com.cy yiotoudd@marlow.com.cy meden@marlow.com.cy goda@marlow.com.cy yis@marlow.com.cy gntjouvani@marlow.com.cy marlow@marlow.com.cy yisd@marlow.com.cy michelle@marlow.com.cy ahéb60iqfvdtóhà2vaeaaaaa@marlow.com.cy ibronnikov@marlow.com.cy,iki@marlow.com.cy,is@marlow.com.cy,is@marlow.com.cy,is@marlow.c marlow@marlow.com.cy raymond8chan@marlow.com.cy markyriakou@marlow.com.cy,markyriakou@marlow.com.cy,marlow@marlow.c markyriakou@marlow.com.cy,markyriakou@marlow.com.cy,marlow@marlow.com.cy,marlow@marl lania@marlow.com.cy lodius@marlow.com.cy ediduro@marlow.com.cy,ediduro@marlow.com.cy,ediduro@marlow.com.cy,eefrem@marlow.com.c anayis@marlow.com.cy ibronnikov@marlow.com.cy,iki@marlow.com.cy,is@marlow.com.cy,is@marlow.com.cy,is@marlow.c ibronnikov@marlow.com.cy enaven@marlow.com.cy collins9rhodes@marlow.com.cy

# Configurations



eSafe Mail on "mailx2.marlow.com.cy" - Configuration

- Lists
  - VIP Email Addresses
  - SMTP Senders
    - Block
    - Scan
  - SMTP Recipients
    - Block
    - Scan
  - SMTP Domains
    - Block
    - Scan
  - File Types
    - Incoming Files
      - Block
      - Scan
    - Outgoing Files
  - Keywords in Incoming Email
    - Body
    - Subject
  - Keywords in Outgoing Email
  - Known Vandal File Names
  - Files for Blocking
- Administration
  - Miscellaneous Parameters
  - Alerts
    - Events
    - Alert Recipients
  - Warning Messages
    - Incoming Email
      - To Senders
      - To Recipients
    - Outgoing Email
  - Email Quarantine
    - Quarantine for Viruses
    - Virus Report
    - Quarantine for Spam
    - Spam Report (Add-on Service)
  - Updates
  - Mail Settings
    - SMTP Mail Relay
    - SMTP Internal Domains**



## SMTP Internal Domains

Define a list of domains for which eSafe is allowed to receive email, and the corresponding internal IP addresses of the SMTP servers to which eSafe will forward email from the specified domains.

Internal domains and SMTP Mail Servers



Internet domain name	Internal SMTP mail server IP
*.marlow.com.cy	212.31.115.217:25
*.marlowfleet.com	212.31.115.217:25
marlow.com.cy	212.31.115.217:25
marlowfleet.com	212.31.115.217:25

OK Cancel Apply ? Help << Back

Proactive Security Engine Active

# Linux / Anti-virus



eSafe Mail on "mailx.marlow.com.cy"

File View Options Help

eSafe Proactive Content Security

	In Progress	Blocked	Allowed (not scanned)	Clean (scanned)	Modified (or deleted)	Spam	Total
Incoming SMTP	0	2139	2	34682	2349	59708	98880
Outgoing SMTP	18	596			1	0	13893
Total	18	2735			2350	59708	112773

Breakdown of all files passing through the Content Redirector. Break

**Product and registration information (mailx....)**

Product Information

- eSafe Gateway version: 5.2.50.7
- Operating system: Linux (Appliance)
- Updated on: 23-Jan-07 04:01:23 PM
- eConsole version: 5.2.25.0
- Virus table & scan engine version: **EV132-SV283**
- Currently installed hotfix(es):
- Rules update version: 5.2.213.39
- URL filter version: Not installed
- URL filter updated on: Has not occurred
- Advanced Anti-spam version: v4.9173
- Advanced Anti-spam updated on: 24-Jan-07 01:20:50 AM

Registration Information

- Product ID: EM
- Serial number: 1017612
- Company: Marlow Navigation
- User name: Manos Manoli
- License started on: 29-Dec-2006
- License expires on: 29-Dec-2007
- eSafe machine IP address: 212.31.115.202
- Number of users: 250
- Type of license: Registration
- eSafe product type: SM
- Number of Cls: 1

Close Export

Legend: SMTP IN (blue), SMTP OUT (cyan)

# Thank You Very Much

Manos Manoli  
IT Manager

**Tel:** + 357 25 88 22 00

**E-mail:** [manos@marlow.com.cy](mailto:manos@marlow.com.cy)