Using MDaemon AntiSpam for Spam Control

Alt-N Technologies, Ltd
2201 East Lamar Blvd, Suite 270
Arlington, TX 76006
Tel: (817) 525-2005

Contents

Abstract

To help stop Unsolicited Bulk Email (UBE), also known as spam, modern email servers must have configuration options to prevent unauthorized relaying of email messages. In addition, cost-effective and secure email servers should be able to detect and optionally block incoming spam before it reaches email account holders.

Fighting spam is important. More than 50% of all email messages are unsolicited and usually unwelcome. Spam costs enterprises and individuals billions of dollars each year by consuming time and resources while delivering content of limited, if any, value.

MDaemon includes the required options to stop unauthorized relaying, while permitting legitimate account holders to use the server from any location in the world.

In addition, MDaemon fights incoming spam through the use of black listing, white listing, heuristic pattern matching, Bayesian filtering and content filtering, plus domain and address blocking. These tools, plus others, make up the next phase in spam detection. Any email server without these types of tools is not serious about fighting the spam problem.

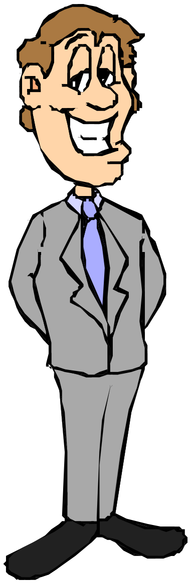
MDaemon offers these options in a package designed for both IT professional and email beginners.

So What's the Big Deal About Spam[1]?

A Sensible Method of Marketing

From a direct marketing point of view, sending introductory sales literature to bulk email lists makes good business sense. It is a very economical way of developing leads and it provides a service to the email recipients. To the sender, email canvassing is the electronic equivalent of cold call selling, only the return on investment is much higher.

So why are so many people upset about e-sales representatives making honest incomes?



The Junk Mail Analogy

Unsolicited email marketing, the senders say, is the e-commerce complement to direct sales literature arriving via old-style mail. Literally tons of unsolicited printed advertising travels through postal systems worldwide each day. These communications arrive addressed to individuals or current occupants. The parcels attempt to inform, entertain and persuade the recipients to buy, sell or donate. This unsolicited *junk mail* is a fact of life. Everyone more or less accepts it and just lives with it. While more than 95 percent of junk mail goes directly to the trash, as many as five in 100 recipients respond to the offers. To these buyers, junk mail is a welcome service. For the sellers, enough revenue comes from the buyers to make direct mail marketing remarkably profitable.

So what is the problem with taking the same approach with unsolicited email?

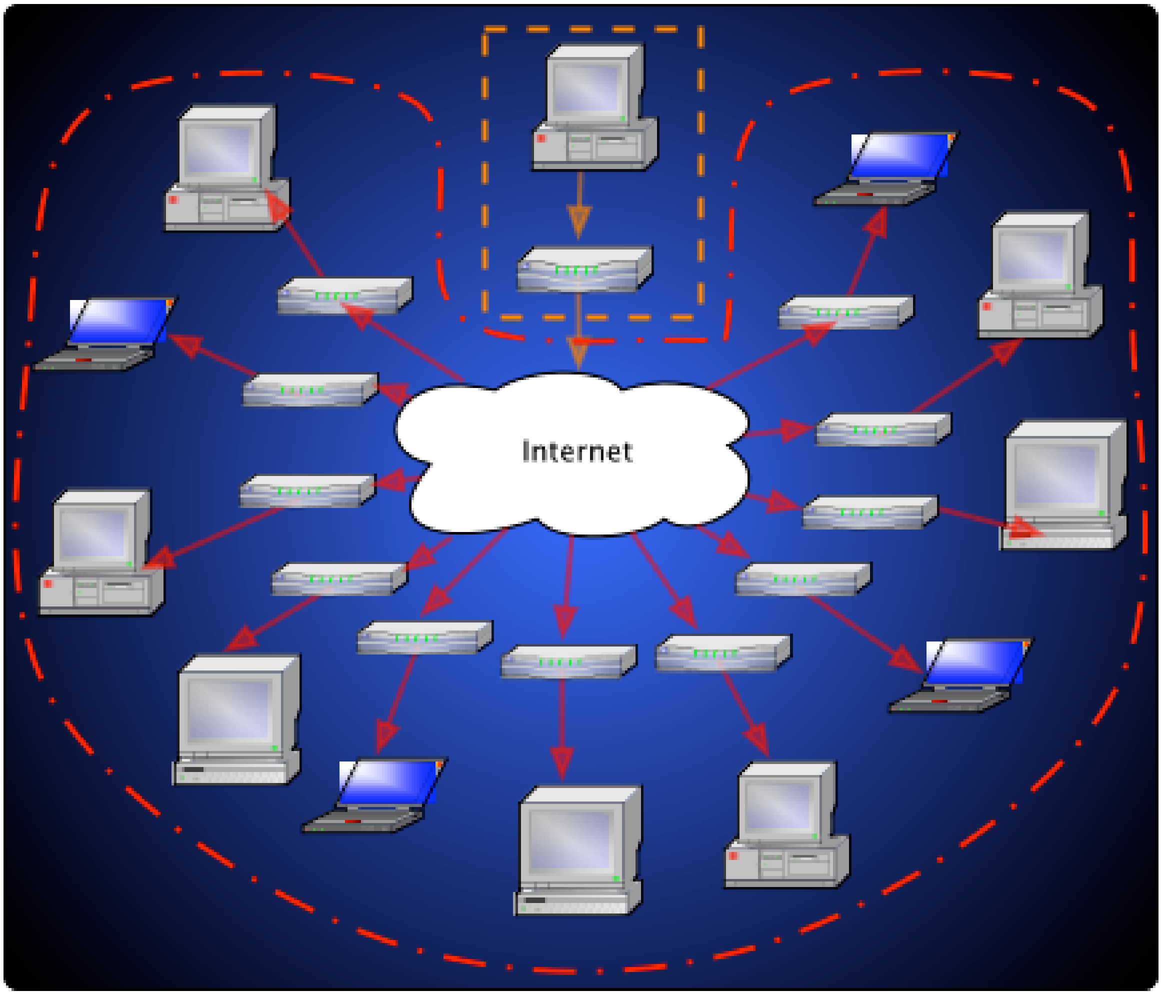
Why Junk Email Hurts the Internet

Traditional direct mail marketing pays its own way, plus a little bit of yours. The cash and risk for creating, printing and sending direct mail advertising comes from the senders. In addition, even though they pay low-cost bulk rates, senders spend enough with postal services to help keep other personal and business mail rates at lower levels. Without direct mail marketing, your personal and business letters would cost more to send, perhaps much more.

[1] SPAM is canned meat from Hormel Food Corporation. Hormel has taken a somewhat whimsical attitude towards the use of their trademarked named being used to describe a practice destructive to the Internet. For example, they say the name spam itself was adopted for unsolicited bulk email (UBE) because of a Monty Python skit. In the skit, a group of Vikings sing a chorus of "spam, spam, spam . . . " increasing louder, drowning out other conversation. The analogy applies because UBE is drowning out normal email on the Internet. When used in reference to UBE, "spam" should be used as any other lower-case word, to distinguish it from the meat product trademark, SPAM™. For more info, see Hormel's *SPAM and the Internet* web site: http://www.spam.com/ci/ci_in.htm.

By contrast, the cost of unsolicited direct email is almost free to the sender and quite expensive for everyone else. While senders still pay for creating their advertising, all other enterprises and users on the Internet support most of their e-trafficking costs. How can that be?

The illustration shows how direct email spreads its cost from one sender to thousands of receivers.

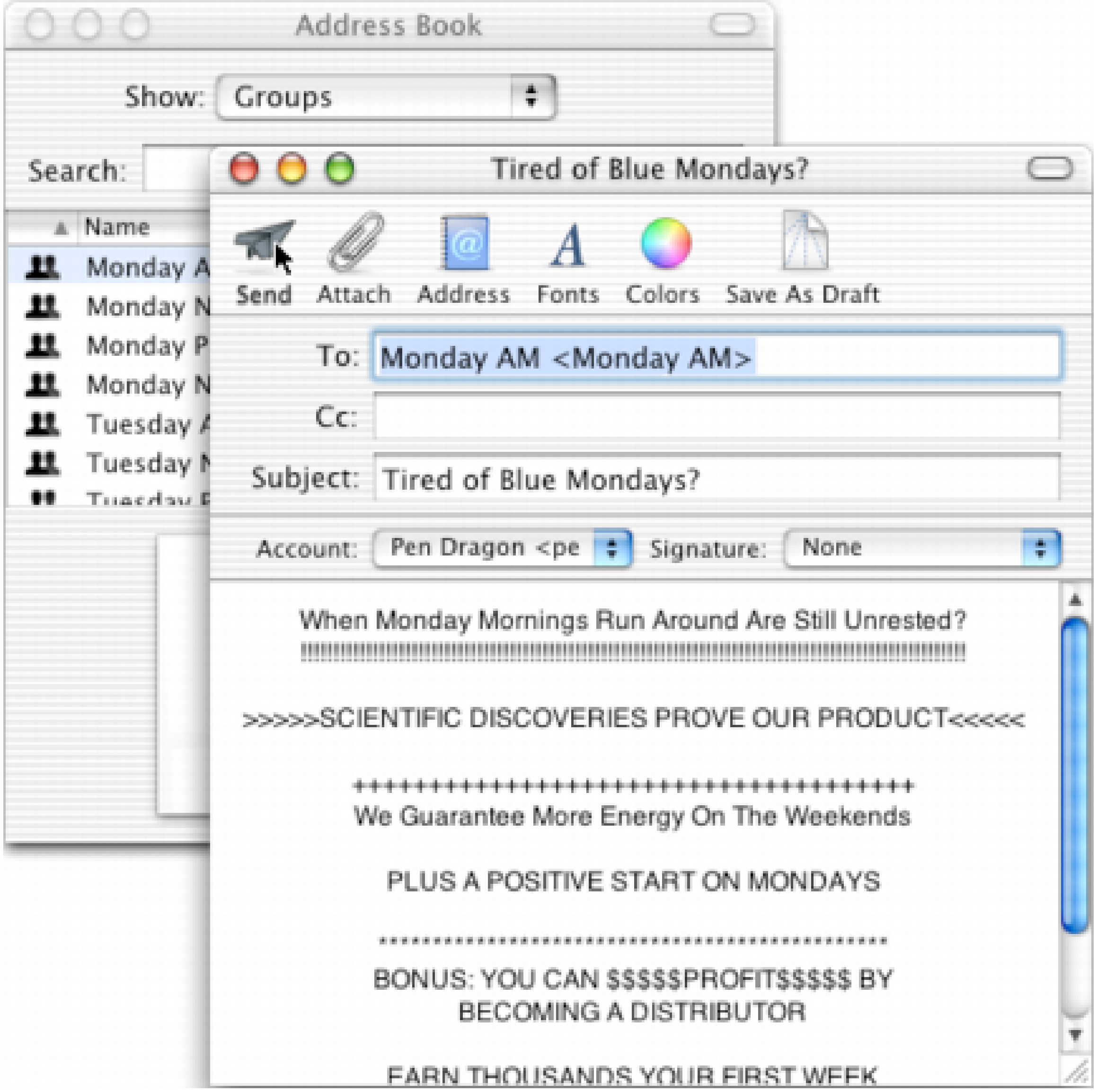


The message originator, highlighted in orange, sends a single email with 50, 100, 1,000 or more recipients, for example. This sender could be paying as little as $10 monthly for a dial up account. The one email goes from the sender to the email server and personal computer of each person on the “TO” list, highlighted in red.

As it multiplies and spreads out to the recipients, this one email consumes resources from many Internet carriers, service providers, businesses and customers. It expends bandwidth, router backplanes, computer processing time and disk space, plus the time of Internet workers and email patrons. When multiplied by millions of messages from thousands of spammers each day the cost of unsolicited bulk email becomes a burden for all but the senders.

Spamming remains popular with direct email advertisers because there are no incremental charges. Reaching one million people costs the same as targeting one individual. Printed advertising, by comparison, has incremental price boosts. Printing and mailing costs increase when the intended audience grows from 1,000 to one million.

Like the print advertisers, Internet carriers and service providers pay incrementally for what they use. The more bandwidth, hardware and personnel they require the more they pay. Some ISPs say as much as half the email they handle is resource-wasting spam. The price for handling this spam eventually gets passed along to the everyday customers who receive the unsolicited offerings.



To: Monday AM <Monday AM>

Cc:

Subject: Tired of Blue Mondays?

Account: Pen Dragon <pe

Signature: None

When Monday Mornings Run Around Are Still Unrested?
!!

>>>>>SCIENTIFIC DISCOVERIES PROVE OUR PRODUCT<<<<<

++
We Guarantee More Energy On The Weekends

PLUS A POSITIVE START ON MONDAYS

****

BONUS: YOU CAN $$$$$PROFITS$$$$$ BY
BECOMING A DISTRIBUTOR

EARN THOUSANDS YOUR FIRST WEEK

Other Problems with Spam

Success Through Resource Displacement

Spam exists because senders have a marketplace – a relatively small one, but profitable nonetheless. While direct mail marketing typically receives one to five percent response, email spammers sell to one in a thousand or one-tenth of one percent. Spammers can afford to sell in such weak markets by using the bandwidth and hardware of other people. They pass on the incremental expenses to Internet carriers, service providers and users. If spammers paid more, they would sell less and possibly disappear.

Various countries and states within countries have drafted legislation to make spamming more difficult, but few laws have passed. Besides, enforcement is difficult at best because of the international nature of the Internet. Being clever people, spammers can also be difficult to physically locate because all they need to operate is a notebook computer equipped with a modem. Moving around to avoid detection is no problem. So spamming and its related ills continue to grow.

Marginal Products

Very few reputable marketing companies use spam. Research indicates the majority of spam products and services consist of:

- Pyramid schemes, including chain letters
- Sex and pornographic materials
- Easy money strategies
- Spamming software and mailing lists
- Stock in "sure thing" business ventures
- Unbelievable health remedies
- Pirated software
- Pirated music

And the list goes on.

Stealth and Fraud

Not all spammers are cheats and frauds. For example, some natural health remedies do indeed have benefits. Also, some people make good, honest livings selling high quality products through multilevel marketing.

However, because so much spam offers questionable products and services, spammers frequently mask their intentions with deceptive subject lines, such as:

- Claim Your Lost Cash
- Build Your e-Commerce Site
- Here is Your Credit Report
- FBI Warning
- Restore Your Virility

Plus others unfit for quoting.

Also, spammers typically forge their return addresses to try and keep ISPs and others from finding their physical locations. Anyone can test this by replying to a spam message and seeing if it can be delivered. Honest people use their real return email addresses.

Spam as an Overwhelming Nuisance

For some service providers, spam can comprise up to half of the email they handle. If these quantities continue, spam could overthrow the value of email and ruin it as a useful way to communicate.

People who use email generally pay for the service. Even with free email accounts, the users “pay” by making themselves available to the advertisers sponsoring the service. In addition, almost everyone pays for their Internet connection. In all cases, spammers are using someone’s paid resources to deliver their messages, without permission.

Nearly 95 percent of people surveyed say they would stop spam if they could.

How Spammers Send Their Email

Spammers send their messages through SMTP mail servers the same as anyone else. Because of the nature of their work, spammers must sometimes use stealth to keep operating. To stay hidden they switch among servers from these sources:

- ISP Servers
- Local Servers
- Open Relay Servers
- Public Free Email Servers

ISP Servers

To operate regularly from an ISP requires cooperation from the service provider. This means the ISP looks to spammers as sources of revenue. In turn the marketers obtain high performance email service.

Local Servers

Some spammers run one or more email servers from their desktop or notebook computers. They can then connect to the Internet, send their messages, disconnect and be gone. Return mail is not required if the spam message routes users to a website, post office box or phone number.

Open Relay Servers

Some ISPs, organizations and businesses unknowingly provide spammers with free email services by allowing their SMTP servers to relay messages from any sender to any receiver. These are called open relay servers and were very common before the advent of spam. Having an open relay means neither the sender nor the receiver of a message must have an account on the server doing the relaying. To counteract this, several Internet organizations specialize in testing email servers and *black listing* those with open relays. Enterprises hoping to fight spam can use the lists to block all incoming email from open-relay servers. This helps pressure server administrators to close their open relays.

Free Email Servers

Some spammers employ the servers of free email providers to send spam. They do this by setting up an account, spamming several thousand people, abandoning the account and setting up another account. If caught in the act, spammers are often banned from the free service, but that is difficult to enforce.

Must You Surrender to Spam?

Can Spam be Moderated?

Many people, including some civil libertarians, believe spam should be legal and unregulated. These supporters say they like the diversity created by spam. It is part of the free market, they argue. Some in particular are concerned about the restraints on freedom of expression any restrictions might impose. They also question the potential for success of any legislation aimed at controlling a worldwide communications system.

These arguments, of course, ignore the increased networking capacities Internet carriers and ISPs must provide to handle the additional traffic generated by spam, plus the waste of the time for the email recipients.

Both people for and against spam have suggested several non-legislative methods to counteract spam:

- Deleting the offensive mail
- Opting Out or In for spam
- Filtering for content
- Blocking by sender, email server or ISP.

Deleting Spam

Deleting spam is just that. If you don’t like what you see, press the delete key. This is the primary recommendation from the spammers themselves. It’s good advice for most junk email. Yet, it does not stop spam. The spam still arrives and imposes its penalties on bandwidth, equipment, carriers, service providers and users.

Also what happens when you personally receive10 or 50 or 100 spams a day? What does this do to your email server and the hundreds of other people using email on that server? What does it do to your productivity, sorting through UBE to find personal email to you?

Opting In or Out

Opting in and *opting out* are options proposed by opponents and proponents of spam, respectively.

Spam foes say no one should receive bulk email unless they specifically seek it out. They propose *opting in*, where users sign up to receive periodic email from a vendor or organization. Spam supporters say this is overly restrictive and limits the ways they can contact new people. They suggest *opting out* as an alternative.

Under opting out, spammers are free to send email to anyone anytime. To protect people who do not want to receive the mail, they include a link or reply address to say, “No more mail, please.” Some spammers include bogus opt-out addresses or use the replies just to see if an email address is active. Others may honor a request for no more unsolicited email, but then sell the active email address to additional spammers.

Filtering and Blocking, Including Heuristic and Bayesian Tools

Filtering means checking both incoming and outgoing mail for objectionable content and then keeping it from coming or going.

Blocking can also eliminate emails based on sender names or IP addresses or both, for example.

While filtering works fine, email must be regularly monitored to check for new filtering needs. Filtering can work at both the server and client levels. Filtering catches spam after it arrives at the email server or client.

Blocking can be set up manually or by using one of the open relay server lists.

Two new filtering methods have recently become available for enterprises serious about stopping spam. These are heuristic spam detection and Bayesian filtering.

Hueristic Spam Detection

Heuristic spam detection uses feature-matching rules, gained through experience, to identify spam. Through detailed analysis of incoming email based on carefully designed rules, heuristic filtering assigns a numerical value or “score” to each message. This “score” is used to determine whether the message is likely to be spam or not. Through years of “learning” what spam (and non-spam) messages typically look like, the default set of rules -- and therefore the scores assigned by them -- have become very reliable and effective in detecting what is and what is not spam.

Bayesian Filtering

As a spam-fighting tool, Bayesian filtering ”learns” to detect junk mail and legitimate mail by analyzing the header, subject and content of received messages known for sure to be either spam or non-spam. The Bayesian process assigns a spam-probability to each word, domain name, HTML code or other ”token” in each message. Bayesian filtering then uses this data to determine if new incoming messages are likely spam or non-spam. Because Bayesian filtering analyzes messages received at each email server, the ”token” probabilities are site-specific.

As part of the Bayesian process, MDaemon has tools for setting up separate folders to receive copies of messages known to be spam and known to be legitimate mail. Bayesian filtering obtains its data by analyzing the messages in these folders. During its initial setup, Bayesian filtering should have 200 or more messages of each type for its first analysis. By regularly adding new known spam and non-spam into the Bayesian system, spam filtering ”learns” to be more reliable in distinguishing between the two over time for each email server.

MDaemon uses the Bayesian results to further refine the ”scores” it assigns to messages.

MDaemon's AntiSpam Tools

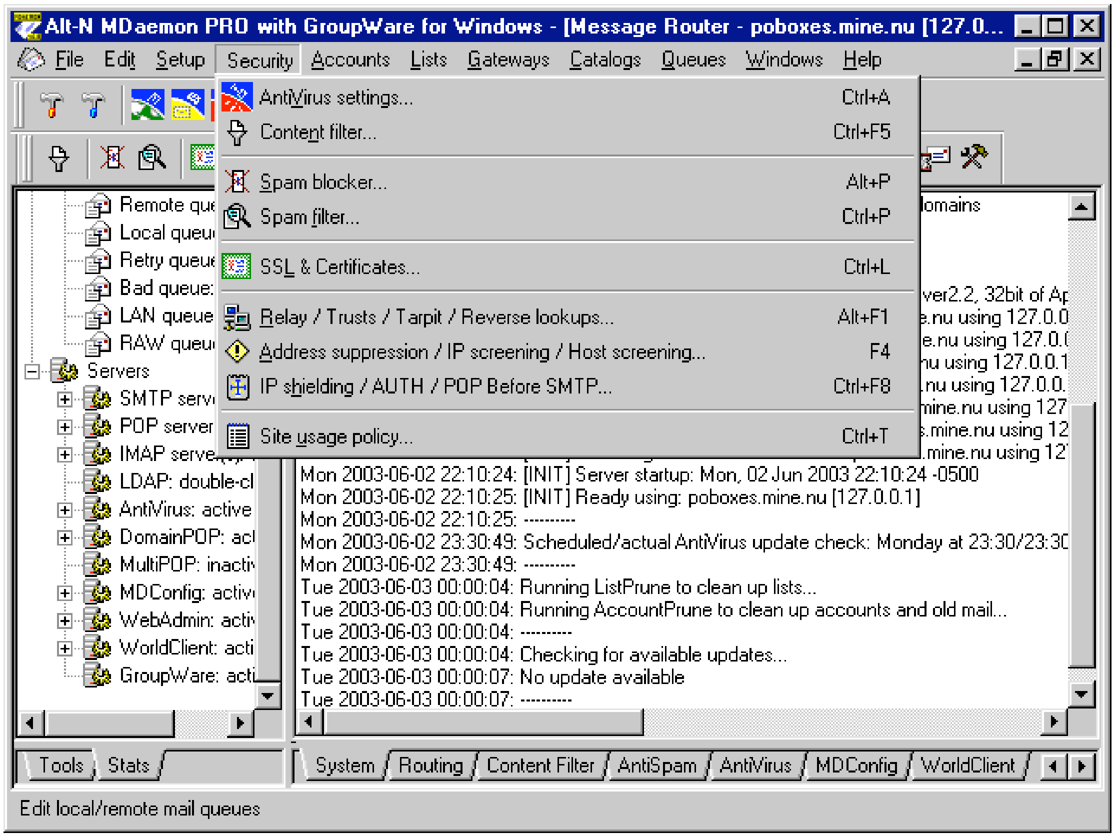
Pluses and Minuses for Server Spam Tools

Using email server tools to fight spam raises controversy among those for and against spam.

Supporters of spam say if you don't want the email, filter it out and block the source IP addresses. Spamming antagonists say these tools do not work well enough and simply allow the spammers to continue by working around the restraints. In addition, by the time spam reaches an email server it has already used most of the bandwidth and router resources, the opponents say.

While the critics' comments are partly true, filters and blocking both work against spam. Using some of these tools requires checking logs to see if the filters and blocks are still accomplishing their purposes. Others run pretty much unattended.

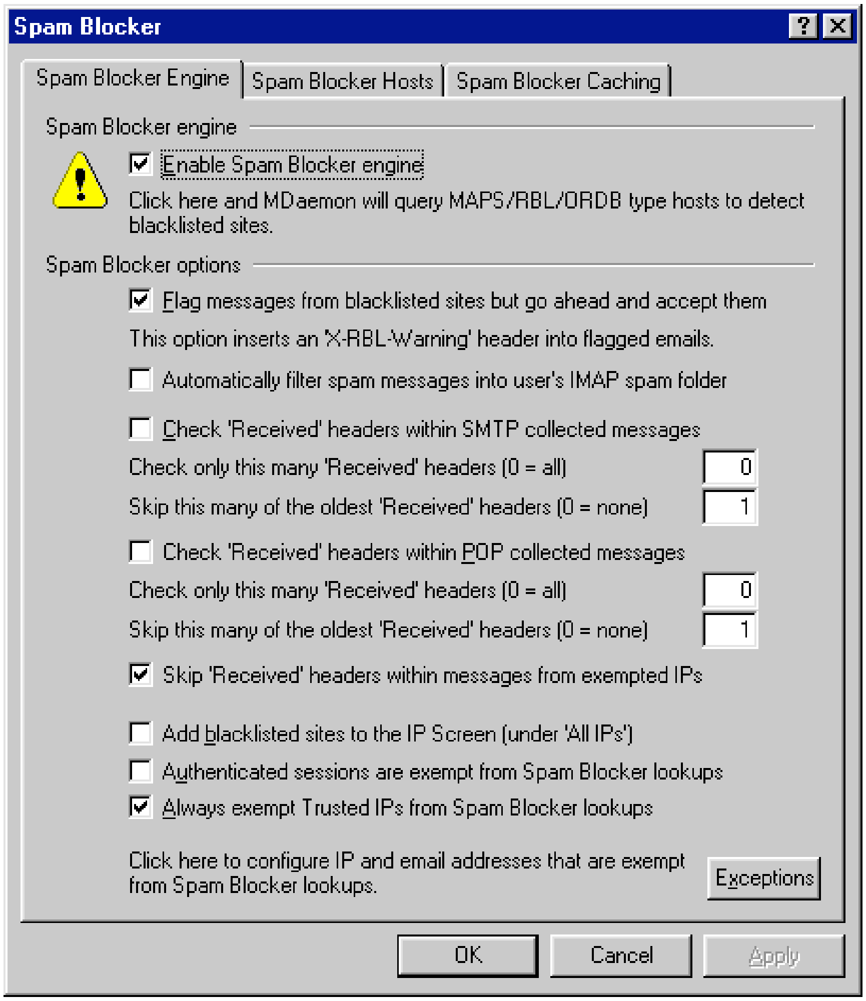
For MDaemon, most of the antispam commands are available through the Security menu.


Alt-N MDaemon PRO with GroupWare for Windows - [Message Router - poboxes.mine.nu [127.0...
File Edit Setup Security Accounts Lists Gateways Catalogs Queues Windows Help
AntiVirus settings... Ctrl+A
Content filter... Ctrl+F5
Spam blocker... Alt+P
Spam filter... Ctrl+P
SSL & Certificates... Ctrl+L
Relay / Trusts / Tarpit / Reverse lookups... Alt+F1
Address suppression / IP screening / Host screening... F4
IP shielding / AUTH / POP Before SMTP... Ctrl+F8
Site usage policy... Ctrl+T
Remote que
Local queu
Retry queue
Bad queue:
LAN queue
RAW queu
Servers
SMTP serv
POP server
IMAP serve
LDAP: double-cl
AntiVirus: active
DomainPOP: ac
MultiPOP: inacti
MDConfig: activ
WebAdmin: acti
WorldClient: acti
GroupWare: acti
omains
ver2.2, 32bit of Ap
e.nu using 127.0.0
e.nu using 127.0.(
nu using 127.0.0.1
.nu using 127.0.0.
nine.nu using 127
.mine.nu using 12
.mine.nu using 12
Tools Stats
System Routing Content Filter AntiSpam AntiVirus MDConfig WorldClient
Edit local/remote mail queues

```
Mon 2003-06-02 22:10:24: [INIT] Server startup: Mon, 02 Jun 2003 22:10:24 -0500
Mon 2003-06-02 22:10:25: [INIT] Ready using: poboxes.mine.nu [127.0.0.1]
Mon 2003-06-02 22:10:25: ---------
Mon 2003-06-02 23:30:49: Scheduled/actual AntiVirus update check: Monday at 23:30/23:30
Mon 2003-06-02 23:30:49: ---------
Tue 2003-06-03 00:00:04: Running ListPrune to clean up lists...
Tue 2003-06-03 00:00:04: Running AccountPrune to clean up accounts and old mail...
Tue 2003-06-03 00:00:04: ---------
Tue 2003-06-03 00:00:04: Checking for available updates...
Tue 2003-06-03 00:00:07: No update available
Tue 2003-06-03 00:00:07: ---------
```

Spam Blocking

Spam blocking can be configured to use the black lists containing the IP addresses of spamming servers or open relays or both. When enabled, this function matches the IP addresses of incoming email to the addresses in the black lists. If they match, the messages can be delivered, isolated or deleted. The inbound SMTP session can also be immediately terminated when the sending server is on a blacklist, refusing the email. The dialog contains input areas for specifying which black lists to use.



Spam Blocker engine

☑ Enable Spam Blocker engine

Click here and MDaemon will query MAPS/RBL/ORDB type hosts to detect blacklisted sites.

Spam Blocker options

☑ Flag messages from blacklisted sites but go ahead and accept them

This option inserts an 'X-RBL-Warning' header into flagged emails.

□ Automatically filter spam messages into user's IMAP spam folder

□ Check 'Received' headers within SMTP collected messages

Check only this many 'Received' headers (0 = all) 0

Skip this many of the oldest 'Received' headers (0 = none) 1

□ Check 'Received' headers within POP collected messages

Check only this many 'Received' headers (0 = all) 0

Skip this many of the oldest 'Received' headers (0 = none) 1

☑ Skip 'Received' headers within messages from exempted IPs

□ Add blacklisted sites to the IP Screen (under 'All IPs')

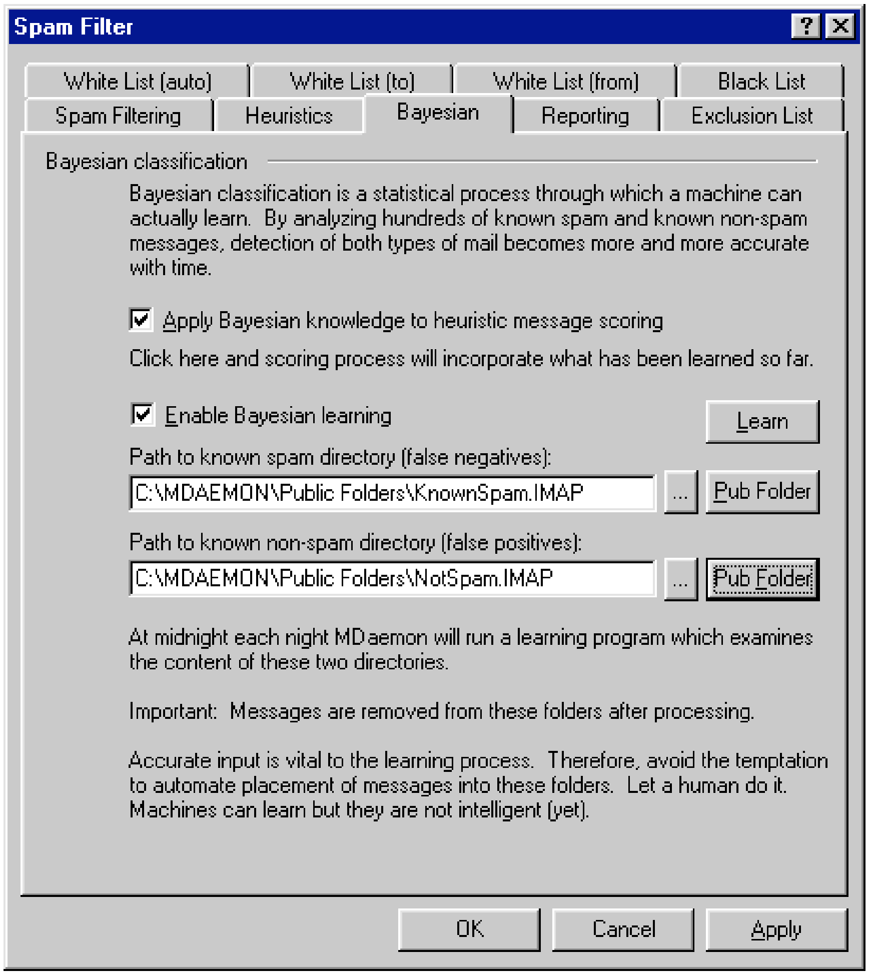
□ Authenticated sessions are exempt from Spam Blocker lookups

☑ Always exempt Trusted IPs from Spam Blocker lookups

Click here to configure IP and email addresses that are exempt from Spam Blocker lookups.

Spam Filtering

Spam filtering involves setting up heuristic and Bayesian tools, plus white listed sites, black listed sites and sites excluded from any processing. Spam filtering works for incoming and outgoing messages. Recent experience shows Bayesian filtering to be particularly effective at blocking spam while allowing legitimate mail through.



Bayesian classification

Bayesian classification is a statistical process through which a machine can actually learn. By analyzing hundreds of known spam and known non-spam messages, detection of both types of mail becomes more and more accurate with time.

☑ Apply Bayesian knowledge to heuristic message scoring

Click here and scoring process will incorporate what has been learned so far.

☑ Enable Bayesian learning

Path to known spam directory (false negatives):
C:\MDAEMON\Public Folders\KnownSpam.IMAP

Path to known non-spam directory (false positives):
C:\MDAEMON\Public Folders\NotSpam.IMAP

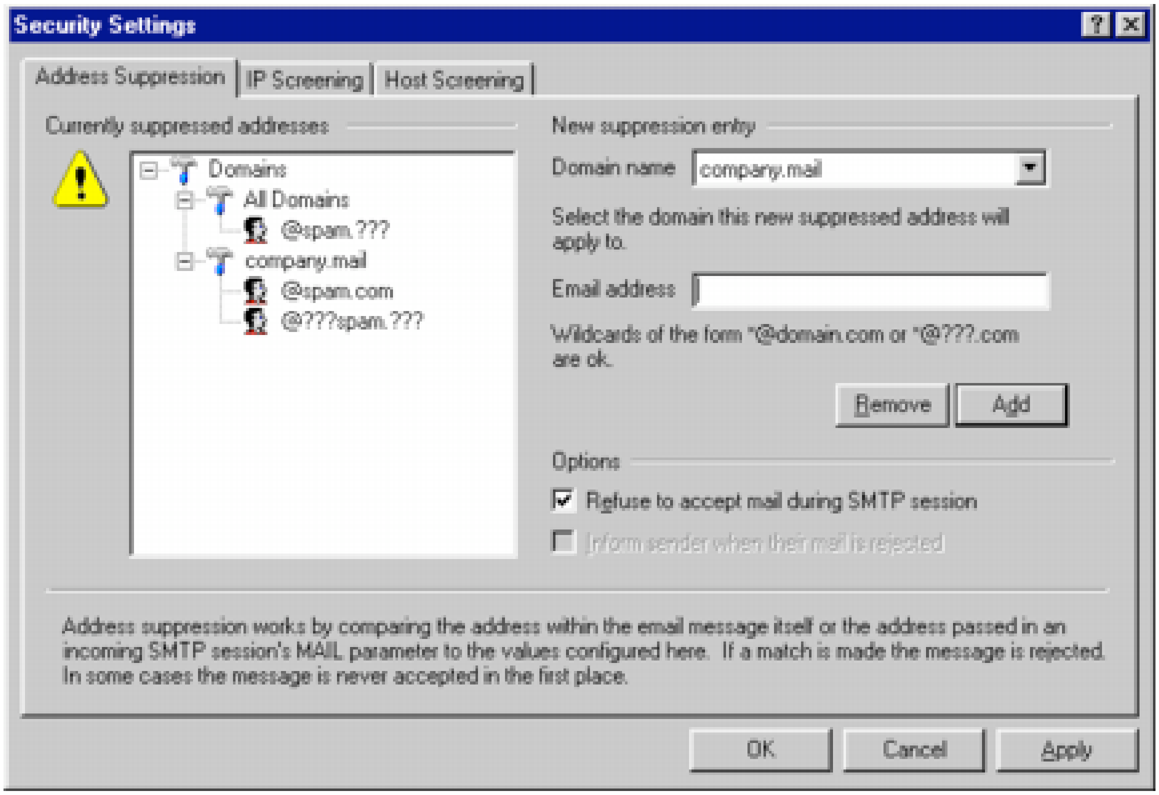
At midnight each night MDaemon will run a learning program which examines the content of these two directories.

Important: Messages are removed from these folders after processing.

Accurate input is vital to the learning process. Therefore, avoid the temptation to automate placement of messages into these folders. Let a human do it. Machines can learn but they are not intelligent (yet).

Address Suppression

MDaemon uses address suppression to prohibit specified addresses from sending mail to a server. Each address can apply to all domains or to any single domain. Addresses can use wildcards. Examples include: @spam.com, b*@spam.org, or @spam.???. This is useful for prohibiting access by specific individuals or groups.



Currently suppressed addresses

- Domains
  - All Domains
    - @spam.???
  - company.mail
    - @spam.com
    - @???spam.???

New suppression entry

Domain name: company.mail

Select the domain this new suppressed address will apply to.

Email address:

Wildcards of the form *@domain.com or *@???.com are ok.

Options

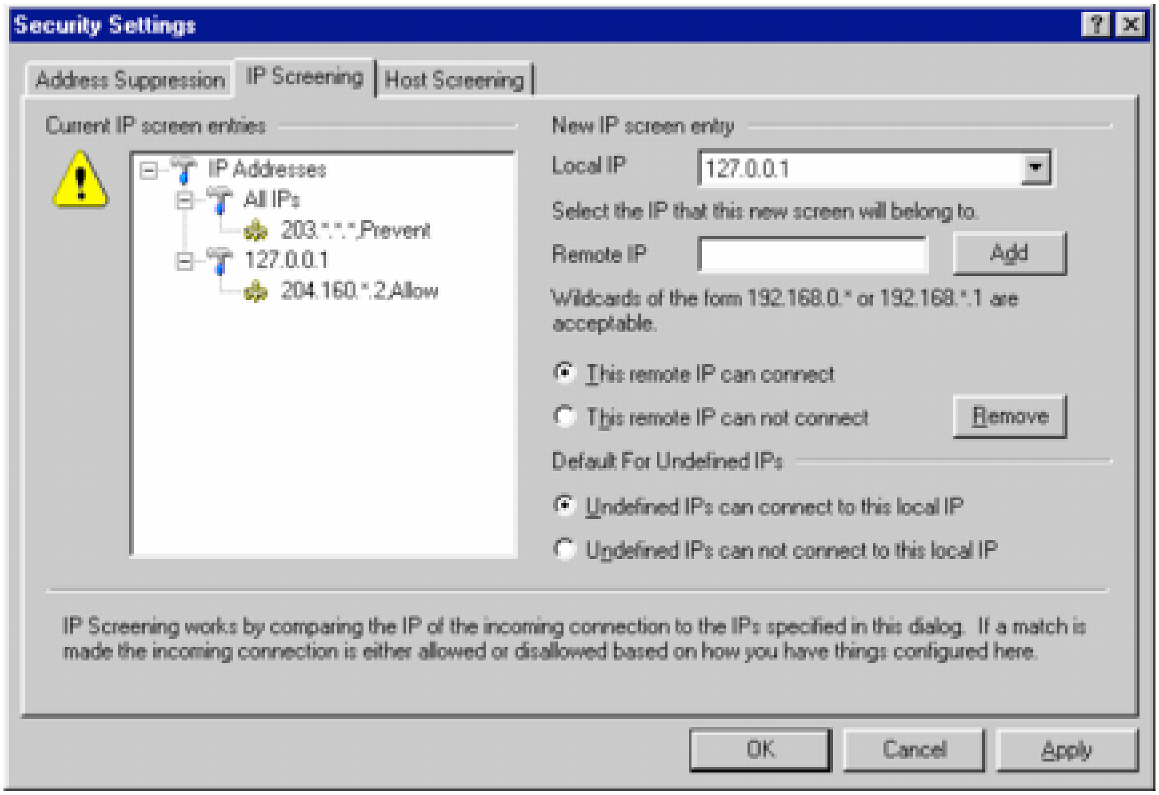
☑ Refuse to accept mail during SMTP session

☐ Inform sender when their mail is rejected

Address suppression works by comparing the address within the email message itself or the address passed in an incoming SMTP session's MAIL parameter to the values configured here. If a match is made the message is rejected. In some cases the message is never accepted in the first place.

IP Screening

IP screening sets permissions for attaching to the server from specific addresses and address ranges. Wildcards apply. Examples are: `203.*.*.5`, `203.*.*.*` and `203.120.14.*`. This is useful for enabling and prohibiting access from IP address ranges.



- IP Addresses
  - All IPs
    - 203.*.*.*.Prevent
  - 127.0.0.1
    - 204.160.*.2.Allow

Local IP: 127.0.0.1

Select the IP that this new screen will belong to.

Remote IP:

Wildcards of the form 192.168.0.* or 192.168.*.1 are acceptable.

● This remote IP can connect

○ This remote IP can not connect

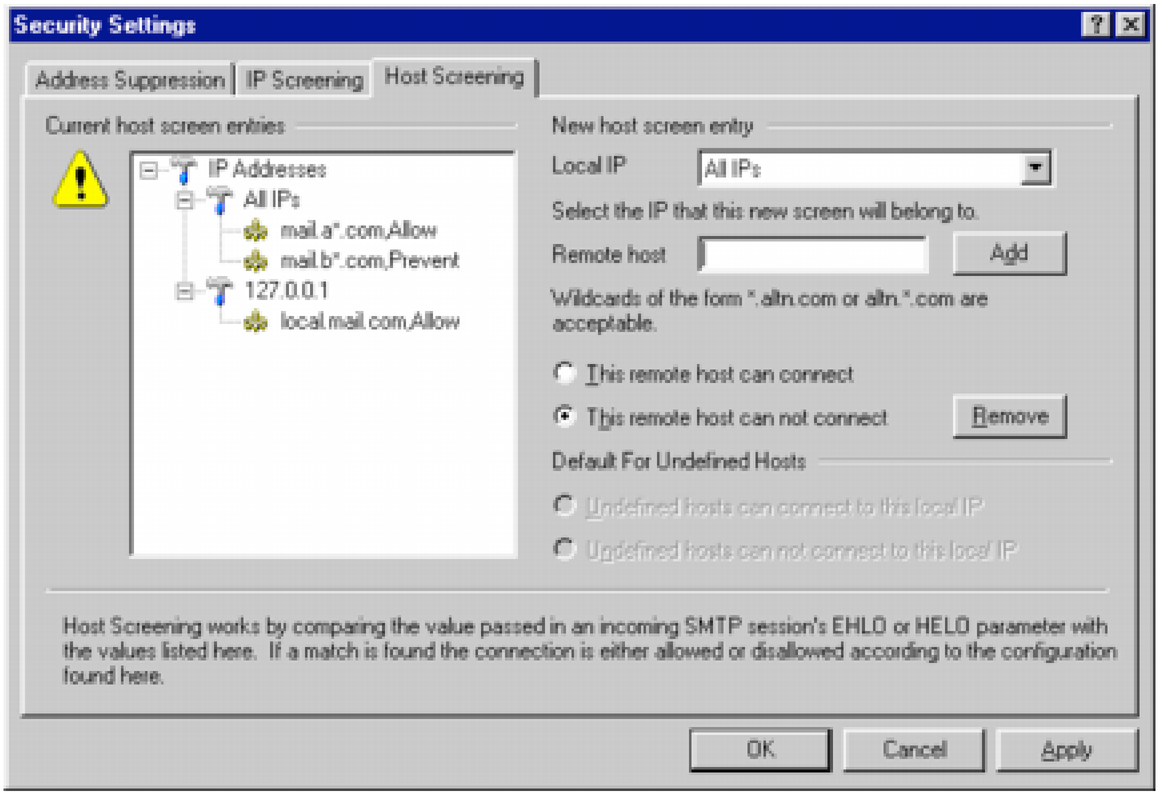
● Undefined IPs can connect to this local IP

○ Undefined IPs can not connect to this local IP

IP Screening works by comparing the IP of the incoming connection to the IPs specified in this dialog. If a match is made the incoming connection is either allowed or disallowed based on how you have things configured here.

Host Screening

Host screening determines whether an SMTP session can connect to the local server. Permission can be granted or denied by host name. Wildcards apply. Examples include: `mail.a*.com`, `*.altn.*` and `company.com`. This is useful for enabling and prohibiting SMTP host access by DNS name.



mail.a*.com,Allow
mail.b*.com,Prevent
local.mail.com,Allow

Local IP: All IPs

Select the IP that this new screen will belong to.

Remote host:

Wildcards of the form *.altn.com or altn.*.com are acceptable.

○ This remote host can connect

● This remote host can not connect

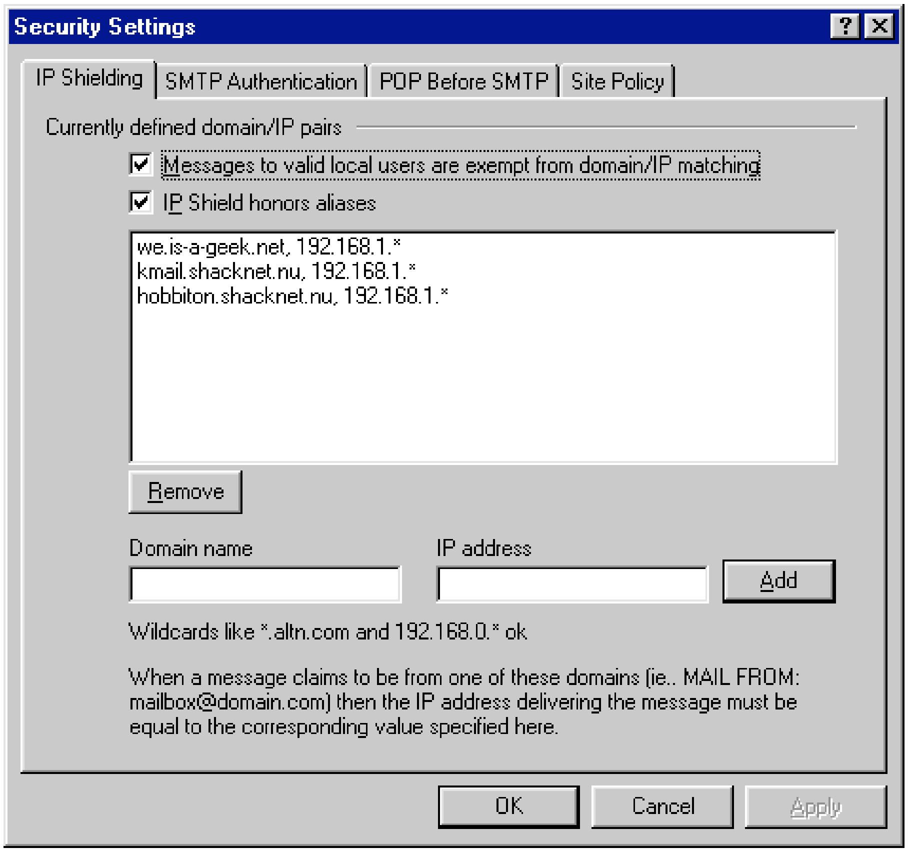
○ Undefined hosts can connect to this local IP

○ Undefined hosts can not connect to this local IP

Host Screening works by comparing the value passed in an incoming SMTP session's EHLO or HELO parameter with the values listed here. If a match is found the connection is either allowed or disallowed according to the configuration found here.

IP Shielding

IP Shielding sets up a list of email domain names and their corresponding IP address ranges. When an SMTP request comes from one of these domain names, MDaemon checks to make sure the corresponding IP address matches. This is useful for blocking mail from forged addresses.



Currently defined domain/IP pairs

☑ Messages to valid local users are exempt from domain/IP matching

☑ IP Shield honors aliases

```
we.is-a-geek.net, 192.168.1.*
kmail.shacknet.nu, 192.168.1.*
hobbiton.shacknet.nu, 192.168.1.*
```

Domain name

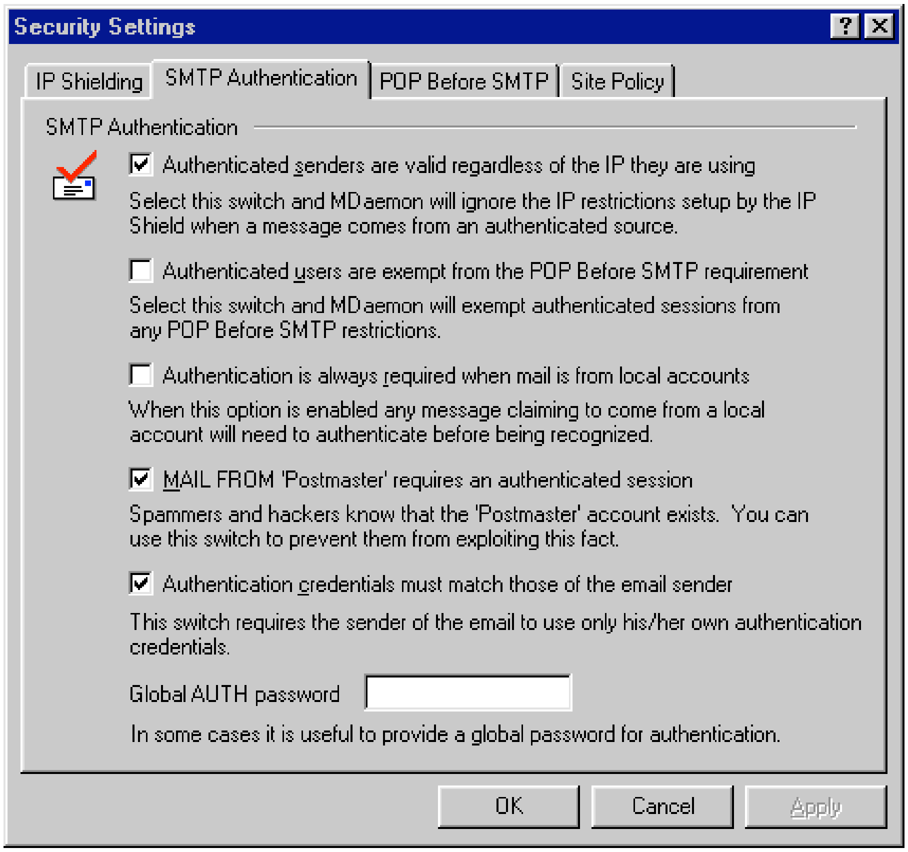
IP address

Wildcards like *.altn.com and 192.168.0.* ok

When a message claims to be from one of these domains (ie.. MAIL FROM: mailbox@domain.com) then the IP address delivering the message must be equal to the corresponding value specified here.

SMTP Authentication

SMTP Authentication enables local users to connect remotely, without regard for their IP address. Another setting in this command overrides *POP before SMTP* for authorized users. This is also the command for setting up required authorization for relaying email from the server postmaster address, an often overlooked security problem.



☑ Authenticated senders are valid regardless of the IP they are using

Select this switch and MDaemon will ignore the IP restrictions setup by the IP Shield when a message comes from an authenticated source.

☐ Authenticated users are exempt from the POP Before SMTP requirement

Select this switch and MDaemon will exempt authenticated sessions from any POP Before SMTP restrictions.

☐ Authentication is always required when mail is from local accounts

When this option is enabled any message claiming to come from a local account will need to authenticate before being recognized.

☑ MAIL FROM 'Postmaster' requires an authenticated session

Spammers and hackers know that the 'Postmaster' account exists. You can use this switch to prevent them from exploiting this fact.

☑ Authentication credentials must match those of the email sender

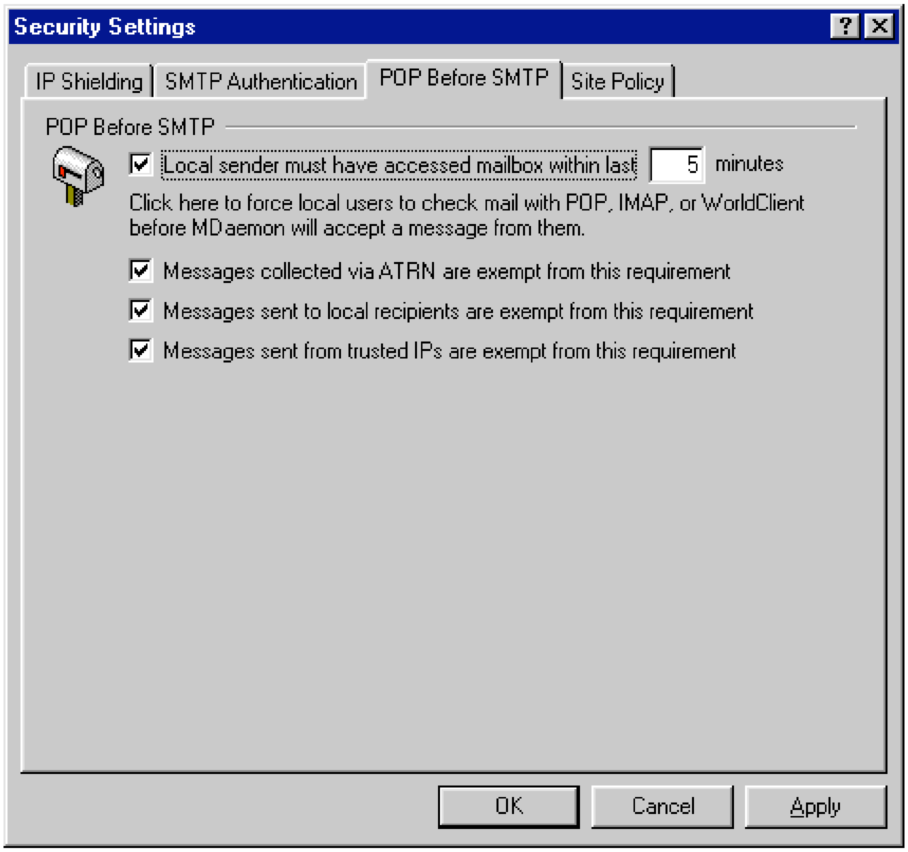
This switch requires the sender of the email to use only his/her own authentication credentials.

Global AUTH password

In some cases it is useful to provide a global password for authentication.

POP Before SMTP

The settings for this command can be used to force users to check their mail before sending messages through the SMTP server. Overrides are available for ATRN connections, authorized users and trusted IP addresses.



☑ Local sender must have accessed mailbox within last 5 minutes

Click here to force local users to check mail with POP, IMAP, or WorldClient before MDaemon will accept a message from them.

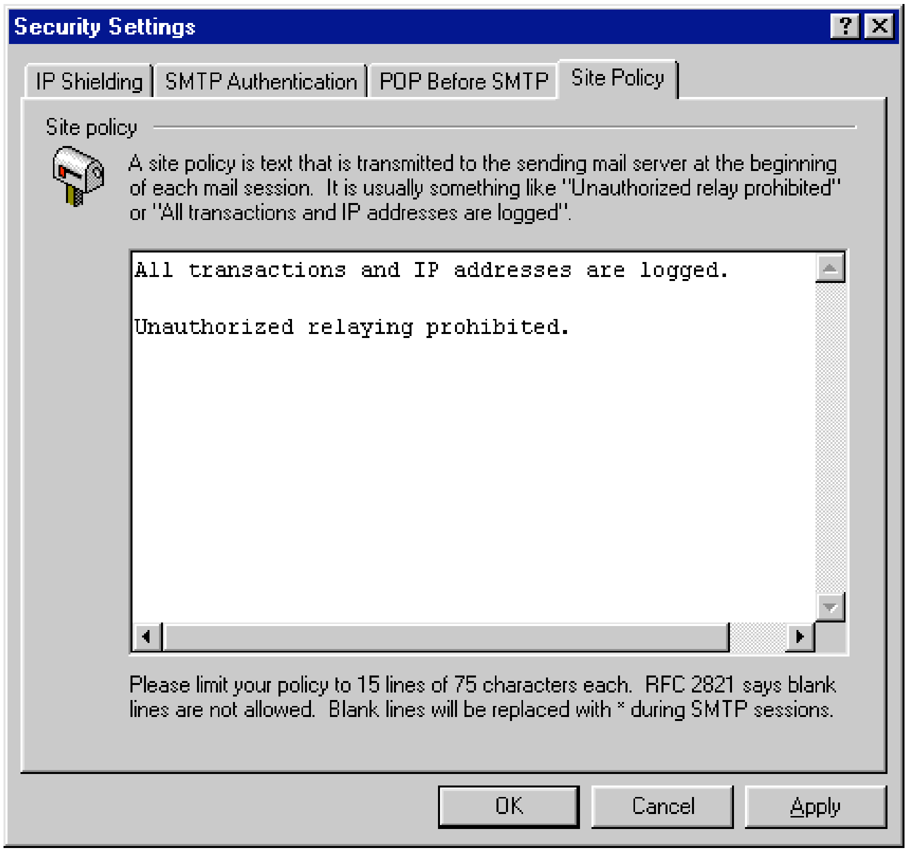
☑ Messages collected via ATRN are exempt from this requirement

☑ Messages sent to local recipients are exempt from this requirement

☑ Messages sent from trusted IPs are exempt from this requirement

Site Policy

A site policy consists of a text message transmitted to the sending email server at the beginning of each email session. The policy itself does not filter or block spam but it can let the sender know you are watching the use of your email server. Typical content might say “Unauthorized relay prohibited!” or “All transactions and IP addresses are logged.”



A site policy is text that is transmitted to the sending mail server at the beginning of each mail session. It is usually something like "Unauthorized relay prohibited" or "All transactions and IP addresses are logged".

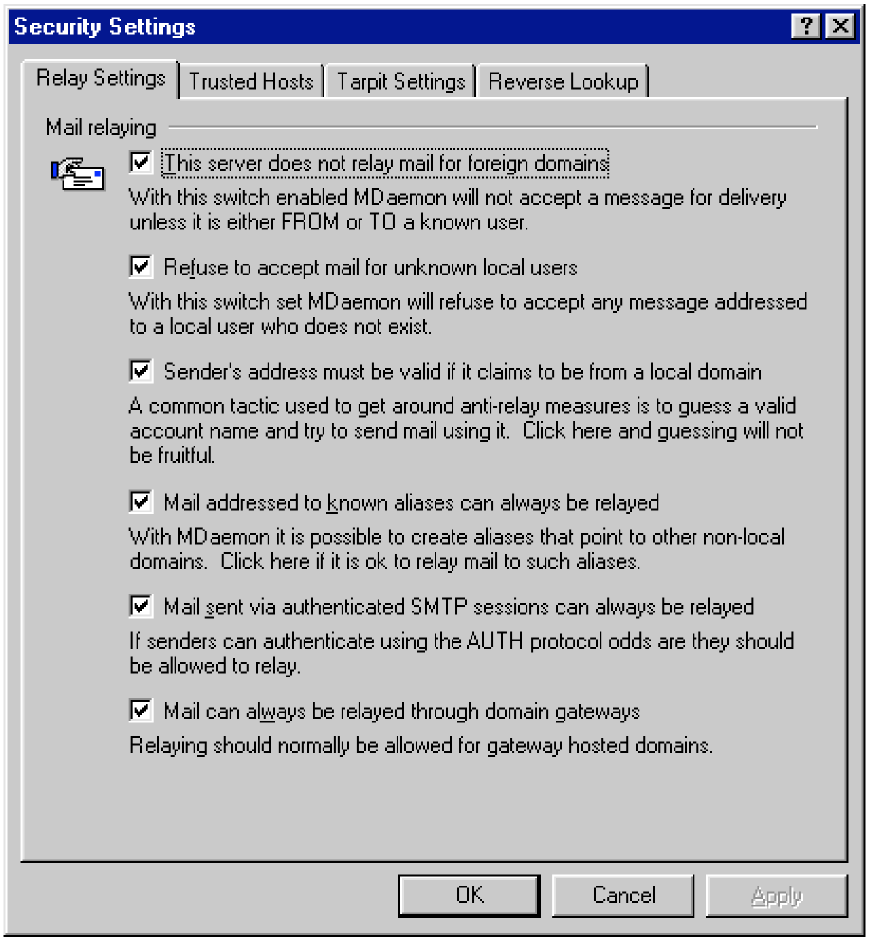
```
All transactions and IP addresses are logged.

Unauthorized relaying prohibited.
```

Please limit your policy to 15 lines of 75 characters each. RFC 2821 says blank lines are not allowed. Blank lines will be replaced with * during SMTP sessions.

Relay Blocking

Relay settings are for making sure your server is not operating as an open relay. Exceptions to the rule are available for authorized accounts and trusted IP addresses.



☑ This server does not relay mail for foreign domains
With this switch enabled MDaemon will not accept a message for delivery unless it is either FROM or TO a known user.

☑ Refuse to accept mail for unknown local users
With this switch set MDaemon will refuse to accept any message addressed to a local user who does not exist.

☑ Sender's address must be valid if it claims to be from a local domain
A common tactic used to get around anti-relay measures is to guess a valid account name and try to send mail using it. Click here and guessing will not be fruitful.

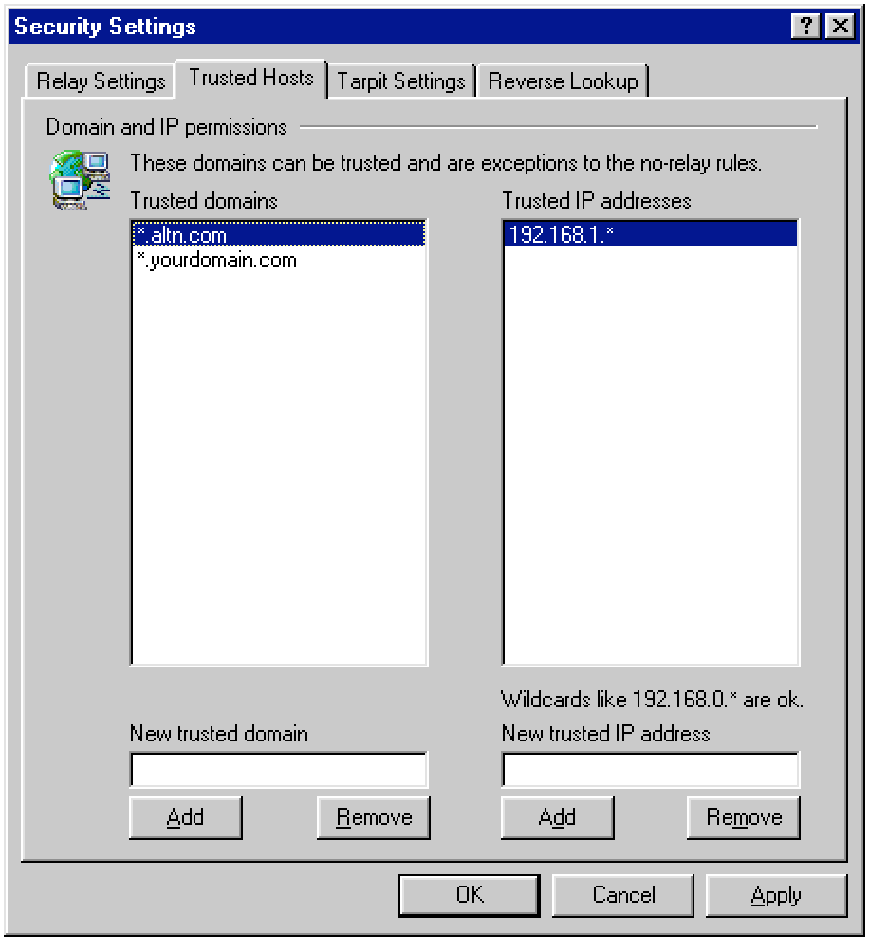
☑ Mail addressed to known aliases can always be relayed
With MDaemon it is possible to create aliases that point to other non-local domains. Click here if it is ok to relay mail to such aliases.

☑ Mail sent via authenticated SMTP sessions can always be relayed
If senders can authenticate using the AUTH protocol odds are they should be allowed to relay.

☑ Mail can always be relayed through domain gateways
Relaying should normally be allowed for gateway hosted domains.

Trusted Hosts

Trusted hosts are exempt from relay blocking.



These domains can be trusted and are exceptions to the no-relay rules.

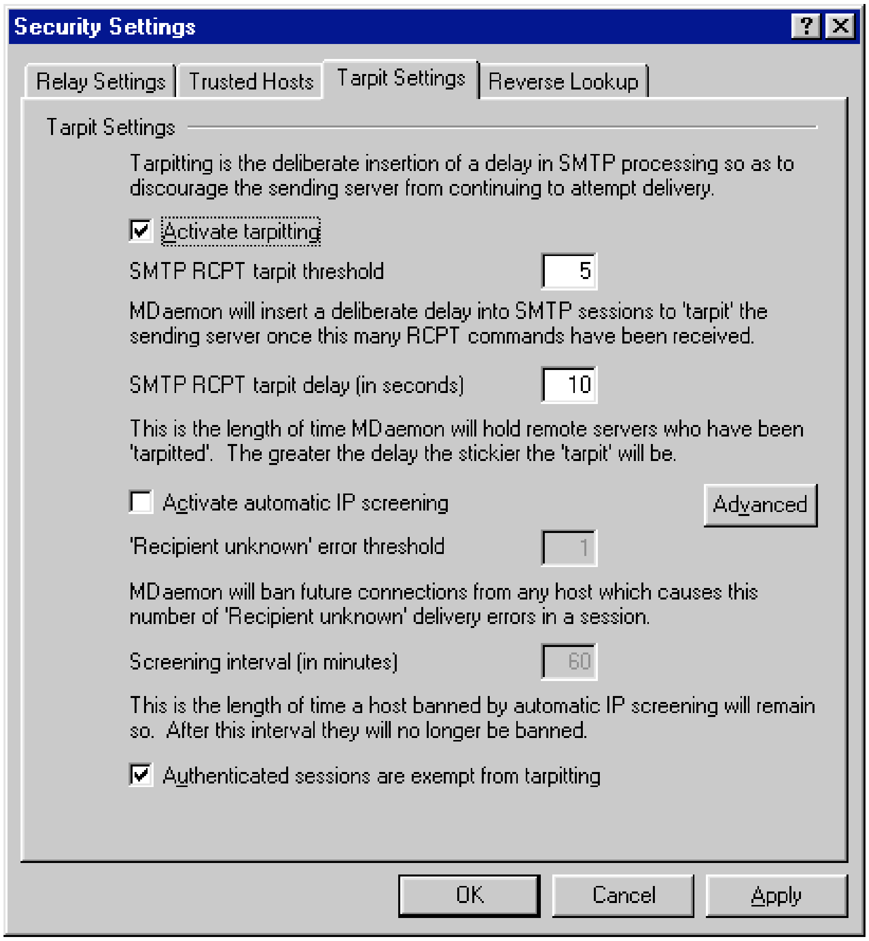
Trusted domains: *.altn.com, *.yourdomain.com

Trusted IP addresses: 192.168.1.*

Wildcards like 192.168.0.* are ok.

Tarpitting

Tarpitting consists of a deliberate delay inserted into SMTP processing if the sending server contacts MDaemon repeatedly during a user-specified number of seconds. Rapid successive contact is often the result of someone attempting to relay through your server or send spam to your user accounts.



Tarpit Settings

Tarpitting is the deliberate insertion of a delay in SMTP processing so as to discourage the sending server from continuing to attempt delivery.

☑ Activate tarpitting

SMTP RCPT tarpit threshold: 5

MDaemon will insert a deliberate delay into SMTP sessions to 'tarpit' the sending server once this many RCPT commands have been received.

SMTP RCPT tarpit delay (in seconds): 10

This is the length of time MDaemon will hold remote servers who have been 'tarpitted'. The greater the delay the stickier the 'tarpit' will be.

☐ Activate automatic IP screening

'Recipient unknown' error threshold: 1

MDaemon will ban future connections from any host which causes this number of 'Recipient unknown' delivery errors in a session.

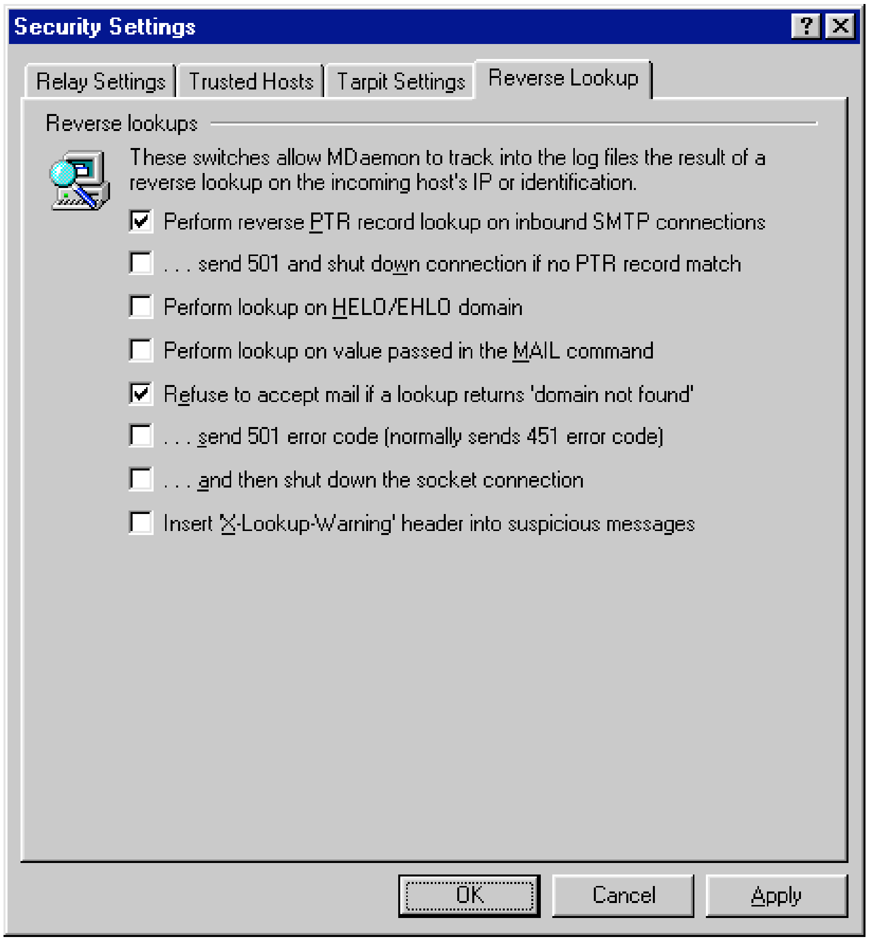
Screening interval (in minutes): 60

This is the length of time a host banned by automatic IP screening will remain so. After this interval they will no longer be banned.

☑ Authenticated sessions are exempt from tarpitting

Reverse Lookup

Reverse lookup is one way of detecting forged IP addresses and domain names in incoming mail. This command enables MDaemon to compare MX records to incoming mail. If the records do not match the information in the email, MDaemon can refuse the connection.



Reverse lookups

These switches allow MDaemon to track into the log files the result of a reverse lookup on the incoming host's IP or identification.

☑ Perform reverse PTR record lookup on inbound SMTP connections

☐ . . . send 501 and shut down connection if no PTR record match

☐ Perform lookup on HELO/EHLO domain

☐ Perform lookup on value passed in the MAIL command

☑ Refuse to accept mail if a lookup returns 'domain not found'

☐ . . . send 501 error code (normally sends 451 error code)

☐ . . . and then shut down the socket connection

☐ Insert 'X-Lookup-Warning' header into suspicious messages

Conclusion

MDaemon, through its various security tools, can limit who can access the email server. While these tools use system resources, including time, they provide strong counter-measures to spam and potential security problem. A server set up to resist spam is also typically secure from other types of attacks.