Lotus. software

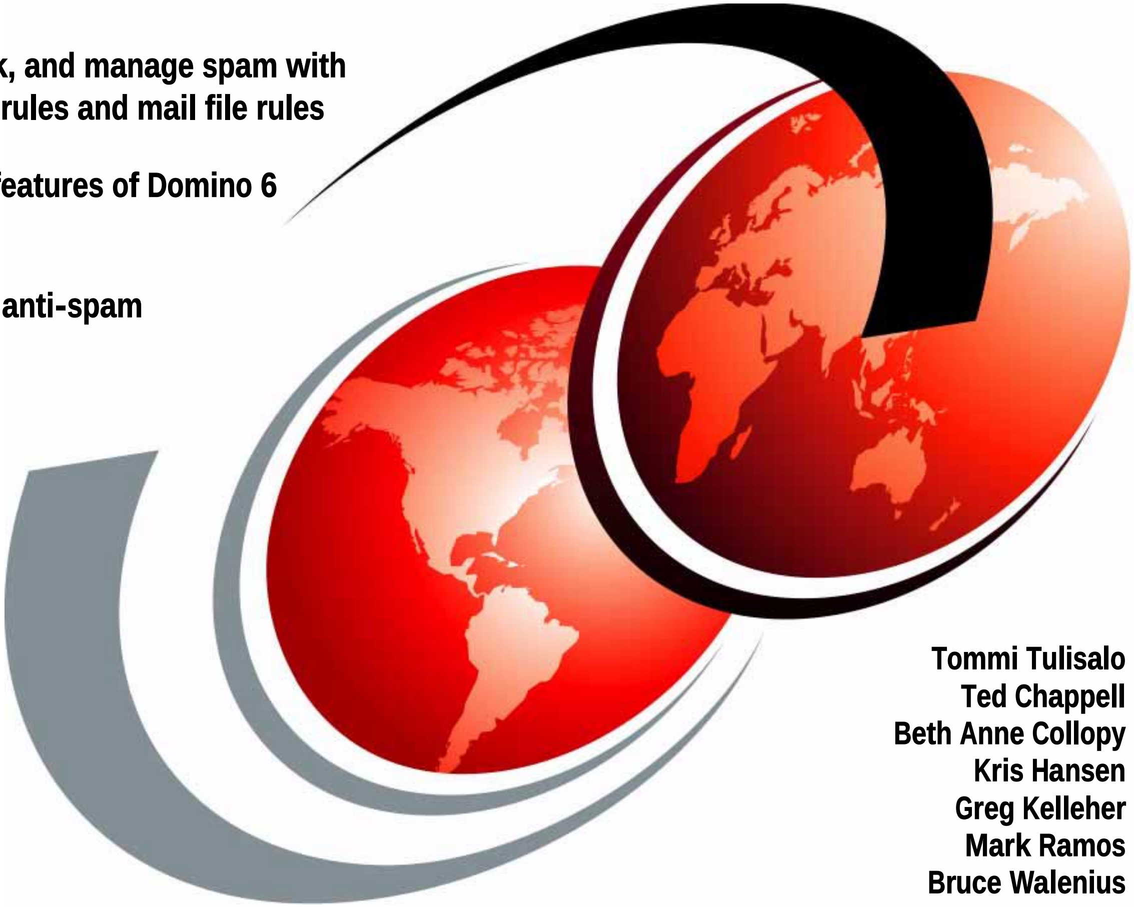
IBM

Lotus Domino 6 spam Survival Guide for IBM eserver™

Avoid, block, and manage spam with server mail rules and mail file rules

Anti-spam features of Domino 6

Third-party anti-spam products



Tommi Tulisalo
Ted Chappell
Beth Anne Collopy
Kris Hansen
Greg Kelleher
Mark Ramos
Bruce Walenius

Redbooks

ibm.com/redbooks

International Technical Support Organization

Lotus Domino 6 spam Survival Guide for IBM @server

January 2003

SG24-6930-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (January 2003)

This edition applies to IBM Lotus Notes 6.0 and IBM Lotus Domino 6.0.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation and/or Lotus Development Corporation in the United States, other countries, or both:

AIX®
AS/400®
Domino™
DB2®
IBM ®
IBM eServer™
IBM @server
iNotes™
iSeries™
Lotus Enterprise Integrator™
Lotus Notes®
Lotus®
Notes®
Perform™
QuickPlace™
Redbooks (logo)™
Redbooks™
S/390®

The following terms are trademarks of other companies:

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Preface

In this IBM Redbook we describe how you can use IBM Lotus Domino 6 to prevent and manage “spam.”

We begin by describing and categorizing spam, which is the commonly used term for unsolicited commercial e-mail. We discuss ways to prevent spam, outlining different techniques available to avoid and block spam.

We then explain how anti-spam control and management work can be divided between servers, between server tasks, and between administrators and end users. We also describe the anti-spam architecture of the Domino 6 messaging environment.

Anti-spam features of Domino 6 are presented in detail. They include the ability to control connections from spammers and the delivery of spam, and protecting against the use of your server as an open relay. We also discuss using mail file rules and server mail rules to prevent spam.

Finally, we highlight some of the business partner products available to further address the spam problem. These products fall into two categories: those that run on a Domino server, and those that operate as separate anti-spam servers and gateways. We include a number of examples of each type, along with references to help you obtain more information directly from them.

This redbook is written primarily for Lotus Domino administrators who want to prevent and manage spam in their environments. It is also useful as a basic introduction to the topic of spam.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Tommi Tulisalo is a project leader for the International Technical Support Organization at Cambridge, Massachusetts. He manages projects whose objective is to produce redbooks on all areas of Lotus Software products. Before joining the ITSO in 2001, he was an IT Architect for IBM Global Services in Finland, designing solutions for customers, often based on Lotus software.

Ted Chappell is a Managing Principal and co-founder of Eagle Technology Consultants LLC, an IBM Premier Business Partner, where he has worked for the past five years. Ted has ten years of experience in information technology working on various platforms. His most recent work includes the development of SpamEraser, Eagle Technology Consultants' anti-spam tool for Lotus Notes and Domino. Ted holds a BA degree in math and economics from Emory University in Atlanta, Georgia. Ted can be contacted via e-mail at tchappell@eagletc.com; his company's Web site is http://www.eagletc.com.

Beth Anne Collopy is a Senior Technical Instructor working in the Worldwide Product Introduction and Technical Support Organization within Lotus Software Group. Her primary responsibility is providing instructional training on Notes and Domino to individuals within the Lotus Customer Support Organization. She joined Lotus in 1997 and supported Domino Mail and Messaging until moving to the Performance and Learning Group in 2001 as a Instructor. Prior to joining Lotus, she worked as a Network Manager and as a Notes Administrator (beginning with Release 3).

Kris Hansen is a Chief Technology Officer at eWorld Enterprise Solutions, Inc. in Honolulu, Hawaii. He has nine years experience working with Lotus Domino infrastructure and development and is an IBM Certified Solutions Advisor, Solutions Designer, and a Certified Lotus Professional in Lotus Domino administration. His areas of expertise include systems architecture, messaging infrastructure, UNIX administration, Domino administration and development, and DB2 and WebSphere Application Server implementation on UNIX platforms.

Greg Kelleher is the product manager for Windows and Linux platforms at Lotus software.

Mark Ramos is a co-founder and the chief technologist of Granite Software. He was the primary developer of Granite's flagship product, ZMerge, a data integration tool and past winner of the Lotus Beacon Award. He developed the SNA APPN network driver for Lotus Notes/Domino and the Text Connector for Lotus Enterprise Integrator (LEI). He has over 20 years of IT experience, specializing in Notes API development. Most recently he directed the development of Granite's newest product, spamJam, an anti-spam product for Domino. More information about Granite Software can be obtained from their Web site: http://www.gsw.com

Bruce Walenius is a Critical Situation Manager for the Lotus Software Group; his geographic area of responsibility includes Europe, the Middle East, and Africa. Bruce has worked for IBM for ten years, all of it in the support organization. He started in 1993 as a software support specialist in Canada before transferring to Lotus France in 1998 to become first a Lotus Support Account Manager, and then the Critical Situation Manager for EMEA West and

EMEA South. He currently resides in Paris, France, and holds a degree from McGill University in Montreal, Canada.

A number of people have provided support and guidance. In particular we would like to thank **Jon Johnston**, Creative Business Solutions, for all his help in putting together the third party products chapter; and **Richard Schwartz**, RHS Consulting, for reviewing the redbook and making valuable suggestions regarding its content and structure.

Thanks to the following people for their contributions to this project:

Matt Chant, Mike Gagnon, Meredith Lovett, Brian Richards - IBM Westford Lab

Diana Ermini, Javier Izquierdo, Joseph John, Ted Niblett, Steven Preston, Jon Raslawski, Jeffrey Slone, Carol Sumner - Lotus Software

Dieter Stalder - STDI Consulting

Kristin Baker - Eagle Technology Consultants

Libby Schwartz - e-Pro Magazine

Andy Yett - Metal Logic

Anthony Barker - XM Technologies

Jeani Boots, Rolf Rennemo - Trend Micro

Jacquelyn Thrasivoulos - GROUP Software

Alison Chandler - ITSO Poughkeepsie

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an Internet note to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept HYJ Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

Introduction

The focus that Lotus has placed on spam prevention in Domino 6 is recognition of how important the issue is in e-mail communications today. A deliberate design goal of new Domino 6 features was to block the “front door,” that is, provide spam control and avoidance capabilities at the server and mail router rather than at the end-user mailbox. Why? Studies have shown that end-user managed spam costs 10 to 20 minutes of productivity per person per day on average. Other messaging clients/servers have not yet recognized this burden, and force users to constantly monitor and remove spam mail from their inboxes, or attempt to define filters to try to catch it. This is all reactive behavior. Domino 6, on the other hand, puts many tools at the server, reducing the risk that spam ever arrives in users’ inboxes.

In this chapter we provide an overview of spam, including a general definition, as well as a discussion of some of the categories of spam and the problems they can pose in an organization.

1.1 Definition of spam

What is *spam*? How do you know if you have been spammed? In a very broad sense, spam is the reception of unsolicited commercial e-mail. That does not mean that if you receive an unexpected e-mail from a friend that you have been spammed.

Spam is designed to flood the Internet with mass mailings, attempting to reach the largest audience possible. Most often spammers are merely trying to sell a dubious product, such as diplomas to unaccredited universities, get-rich-quick schemes, or discounts on prescription drugs. In a real world example, spam is the equivalent of receiving flyers, mailers, contest entries, and other such junk mail items routinely sent to thousands of households without the residents having explicitly requested them. The difference, for the average spammer, is not having to pay printing fees or postage, which makes spam infinitely less expensive than traditional junk mail.

A very important aspect of what constitutes spam is that spam has negative effects on those who receive it. Spam is the only form of advertising that is more expensive for its audience than for the advertiser. It is not simply a case of getting a few extra mail messages a day and taking a minute or two to delete them. Spam is not targeted at any specific group or person. It is sent to everyone. Therefore, it can be a very expensive nuisance. Consider the fact that service providers charge for time spent accessing the Internet. If you receive five spam messages a day, you will waste a minute or two deleting the messages. But what if you received 50 messages a day, or 100? What if everyone in your company received 50 messages a day? And without even considering the loss in man hours, what about storage costs?

Advertisers pay very small sums of money to acquire huge spamming lists and lists of e-mail addresses. These lists are gathered from various sources, often with questionable methods, and sold to anyone who wishes to send out spam. Advertisers then use these lists for spamming, trying to reach the broadest audience possible.

1.2 Categorizing spam

Spam generally falls into one of 6 categories:

- Advertisers trying to sell a product or service to as large an audience as possible.
- Mailings designed to cheat or mislead unsuspecting or gullible Internet mail recipients with incredible get-rich-quick schemes.

- Hoaxes. E-mail chain letters requiring you to perform an action or suffer serious consequences.
- Fake virus warnings, forged messages, or deceitful mail attempting to get the recipient to respond in a certain way.
- Mail trying to entice you to visit certain sites, often pornographic, or of very questionable nature.
- Malicious mail designed to interrupt regular Internet traffic or flood mailboxes or mail routers.

Each one of these categories of spam is trying to make the recipients react in a certain way, most often to their own detriment. Let's look at each one of the categories more closely:

- Advertisers trying to sell a product or service to as large an audience as possible.
  - This is the most common type of spam.
  - The idea is to reach as large an audience as possible. Statistics show that more than 99% of people who receive these types of offers delete them without opening them. However, if a spammer sends their message out to 1 million people, and only 1 out of 100 people actually read the message, the spammer is still reaching an audience of 10,000 prospective clients.
  - Some of the most widely distributed advertisement-type spam mailings include offers to reduce or enlarge various body parts, invitations to buy prescription drugs at discount prices, and offers to refinance your home loan.
- Mail designed to cheat or mislead unsuspecting or gullible Internet mail recipients with incredible get-rich-quick schemes.
  - There are many known examples of this type of scam. For example, someone is stuck in a war-torn country but has managed to secrete millions of dollars into a Swiss bank account, and only needs you to send them airfare and you will be entitled to a percentage of the treasure.
  - Another example of get-rich-quick spam is the pyramid mailer; “Just send 5 dollars to this person for this report, and move your name up one rung on the letter. Then send it out to as many people as you can.”.
  - Some other spam which falls into this category is not so obvious. For instance, a reputable-sounding investment firm believes a certain stock is hideously undervalued and urges you to buy it while it is low. The mail is made to look as professional and as serious as possible.

  All of these examples are messages which are designed to deceive the end user.
- Hoaxes: e-mail chain letters requiring you to perform an action or suffer serious consequences.

  - This type of spam is often referred to as a Virus Hoax or Mail Hoax.
  - This type of mail covers a very broad category from the “If you don't forward this to 5 people in 5 minutes, you will have 5 years of bad luck,” to the “Microsoft e-mail beta test will pay you 245 dollars per person to whom you forward this mail,” to “little Johnny is going to die but wants to be in the Guinness Book of World Records for having received the most e-mail before he passes.” This type of message plays on the recipient's gullibility.
  - Hoaxes are trying to trick you into sending out as many warnings as you can to as many people as you can.
  - If you are ever in doubt as to the authenticity of a suspicious mail, you can browse an extensive list of mail hoaxes by visiting this site:

    `http://hoaxbusters.ciac.org`

- Fake virus warnings, forged messages, or deceitful mail attempting to get the recipient to respond in a certain way.
  - Although similar to the previously described type, this spam can have more serious consequences. Often it derives from spammers posing as legitimate companies, for instance, “Microsoft Official Virus Warning” or some such thing. Microsoft, or any other reputable company, does not send out unsolicited virus warnings, nor unsolicited mail trying to get you to upgrade drivers on your operating system (do not confuse this with the Automatic Update feature of Windows Operating Systems). The spammer will tell you there is a new update to prevent a virus, and will try to get you to download an actual virus in its place.
  - Another common example is spammers posing as legitimate mail domains, often soliciting funds for a cause. For instance, the spammer may say that they are collecting money for disaster relief in the wake of the 9/11 tragedy, or trying to raise money to build a new wing for a cancer ward. Reputable charities do not use spam to solicit funds.
  - Another common example is a mail message leading an unsuspecting person to believe they have won a valuable prize, and asking them to “Simply call this number to claim your prize.” The number is often an overseas 809 area code, billed at extortionate rates per minute, with the goal of simply keeping you on hold for as long as possible.
  - A further example of a spam message designed to deceive, is the one arriving with a few names in the TO: field which very closely resemble your own mailing address, leading you to believe that a simple typo allowed you to be the lucky recipient of a fabulous offer. These spams may start something like “As requested, here is....”, or “Thanks for getting back to me, here is that site I was talking about......”. Do not be misled; if the mail was not solicited, don't answer it.

- Mail trying to entice you to visit certain sites, often pornographic, or of very questionable nature.
  - Mail of this nature is often directly to the point. “Wanna see more of me? Click here.” or “I can't believe it, you have to see this! Click here.” This type of spam is often paid for by the site in question. Advertising rates for big commercial sites are very high, for the simple reason that a great many people will see them.
  - If an unscrupulous site can demonstrate through an independent source that they have a very large hit rate, they will entice advertisers hoping to sell products or services via their site. The more people who innocently click on the link, the higher the hit counter will soar. Many spammers also take advantage of the fact that HTML mail can contain moving images. For instance, “Click on the Monkey to win $10,000” and when you click on the monkey then you are sent to the site the spammer intended.
- Malicious mail designed to interrupt regular Internet traffic or flood mailboxes or mail routers.
  - This last category is the type of spam the average person will be least likely to come across. It consists of malformed messages designed to disrupt mail services, often by attempting to crash SMTP routers. There are an infinite number of possible combinations of mail messages that a spammer can create. They can deliberately send empty attachments, bad headers, looping addresses, incorrect control characters within critical routing fields, or any of a myriad of other things to attempt to cause mail blockages.
  - Mail routing applications such as Lotus Domino have very robust SMTP defenses in place to avoid and prevent these types of attacks. Defensive code included in the product will reject malformed messages which could have provoked error conditions. Normally, mail needs to conform to a strict standard in order to be accepted. If not, the SMTP router will simply reject it. However, hackers, crackers, and malicious spammers are constantly changing the methods they use to attempt to disrupt services. Inevitably, an unprotected system will eventually fall prey to this type of message.

For more information about what constitutes spam, see the publicly available RFCs located here:

- RFC2505 (`http://www.ietf.org/rfc/rfc2505.txt?number=2505`)
- RFC2635 (`http://www.ietf.org/rfc/rfc2635.txt?number=2635`)

2

Preventing unwanted e-mail and spam

Many users and administrators will agree that unwanted e-mail and spam is a problem for them. Where they don't always agree is on what approach to take to circumvent this disruption.

One philosophy is to stop spam before it reaches the user; this avoids wasting the user's time dealing with rules or managing it at all. At the extreme end of this spectrum, the risk of having spam arrive in the user's mailbox outweighs the potential for false positives and the undelivered (real) mail associated with that - All mail is suspect and scrutinized by the server for point of origin and content. Any messages not measuring up are discarded.

Another philosophy is to let everything in and have the user sort out what is spam and what is real. The admin adopts a laissez-faire approach at the server level. Point of origin and content are not scrutinized, but the users are given tools to deal with unwanted mail.

Many environments use a blend of the two philosophies to achieve the optimum spam prevention for their organization, and what constitutes the best anti-spam campaign differs from one organization to another.

In this chapter we discuss some basic spam avoidance techniques, and how to select the right approach in your environment. One highly effective way for your users to not receive spam is to have them avoid having their e-mail addresses added to a spammer's list in the first place. We discuss how spammers usually accumulate these e-mail addresses and how you can help your users protect theirs.

2.1 Spam avoidance techniques

From a server point of view, the most efficient way to handle spam is not to have it delivered in the first place. This is why, as a Domino server administrator, it is in your best interest to help inform your users about how to avoid getting on spam lists in the first place. If they do this effectively it can save time administering spam rejection tools.

Most users, when confronted with spam, will not understand why they are getting it. Some users definitely get more spam than others, though, so we know that there is some user behavior that correlates to the amount of spam that they will receive. The best way to understand the behavior to avoid is to look at how most spammers get e-mail addresses in the first place.

2.1.1 Passive harvesting attacks

In this section we introduce some passive harvesting techniques that spammers use to obtain e-mail addresses. To learn about how to protect your Domino 6 server from harvesting attacks, see 4.5, "Protecting your Domino server from active address harvesting attacks" on page 62.

Web harvesting

Spammer Web robots or "bots" operate like Web search engine bots, except they look specifically for xxxx@domain.com patterns in the Web page text. When an e-mail address pattern is found they store it with other e-mail addresses for use in bulk mailing. You can defend against spammer Web-bots by obfuscating mail addresses when they are placed on Web pages. The best option for defense is placing e-mail addresses into graphics. Alternatively, you can hide them inside javascript, or simply provide human-recognizable alterations to the address that make it invalid for e-mailing, or make it more difficult for the Web-bot to recognize any e-mail address pattern.

Usenet harvesting

Spammer news-bots use a concept similar to that used by Web search engine bots. Spammers can subscribe to any usenet group. Then after downloading posts from a usenet group, the news-bots look for xxxx@domain.com patterns in posted message content and headers. When an e-mail address pattern is found they store it for use in bulk mailing. The best defense against spammer news-bots is to simply provide human-recognizable alterations to the address that make it more difficult for the news-bot to recognize any e-mail address pattern.

Listserv harvesting

Spammers develop programs that subscribe to list servers as any other user can, but they never send to the subscribed list. Instead they capture other list subscriber's e-mail addresses over time. The best defense against Listserv harvesting is to simply provide human-recognizable alterations to the sending and reply address to make them more difficult for an automated list-bot to recognize any e-mail address pattern.

2.1.2 Avoiding harvesting

Advise your users to avoid having their e-mail addresses harvested by employing the following techniques:

- Have a personal or “junk” account from a free provider that is used specifically for newsgroup or commercial Web site interaction.
- Do not post their address on newsgroups or public Web discussions.
- Avoid publishing their e-mail address in public “people finder” directories or Instant Messaging directories.
- Avoid using standard e-mail addresses for domain name registration contacts; instead, create accounts specifically to manage registration contact.
- Have users avoid using “e-invite” or “postcard” services with their organizational e-mail address: these services often sell or solicit to the e-mail addresses that they gather.
- Make sure that users know to read the privacy statements on Web sites that they provide information to.

Your public Internet site is also a target for address harvesting; here are some tips to make your Web site difficult for spammers to target:

- Do not create public directories available on the Internet without some form of protection from harvesters. Consider making this area a “sign in” area requiring some form of authorization, or confusing harvesters (as described in the next section).
- Be selective about which addresses are provided as contact points for the organization and try not to make them easy picking for spammers.
- Have public feedback mail delivered to a “mail in” mailbox so that spam doesn't clutter up a user's mailbox.

2.1.3 Confusing the harvesters

The e-mail harvesters are programs that gather e-mail addresses of a specific format. If the format of the address does not meet the criteria of the program it will not be gathered for spam usage.

Mailto tags

One area where you may want to employ this tactic is on your public Internet site. Harvesters are notorious for going after any address in a mailto: tag. One way to protect your addresses on the Web site is to write the mailto: tag with a hexadecimal e-mail address rather than an ASCII address. All browsers can understand these addresses while harvesting programs will not pick them up. Here is an example of an address converted to hexadecimal:

```
ASCII: <a href=mailto:me%40mydomain.dom>me@mydomain.dom</a>
Hex:  <a href= mailto:%6d%65%40%6d%79%64%6f%6d%61%69%6e%2e%64%6f%6d> Email
me</a>
```

Here is an example of a perl script that will convert ASCII addresses to hex:

```
#! /usr/bin/perl
# Little perl program to convert ascii email addresses to hex
# to avoid spam harvesting from mailto: tags

my $addr = shift                      or die "usage: $0 email\@address.dom\n";
$addr =~ s/(.)/ sprintf('%%%2x',ord($1)) /ge;
chomp($addr);
print "$addr\n";
```

Address obfuscation

If you are posting to a newsgroup or to a Web discussion board where you suspect that your address may be gathered, consider *munging*. Address munging involves changing your real e-mail address in a way that will make it unavailable for harvesting. Normally this involves adding a "NOSPAM" or some other text string that other people will know to remove before sending mail to that address. Harvesting programs are often not smart enough to distinguish between a munged address and a real address. An example of such an e-mail address is john.example@NOSPAMibm.com.

2.1.4 Inform Users

The more users know about the cause of their addresses being picked up by spammers, the greater the chance that they can avoid getting on the list.

Educating users about how to avoid giving their addresses to potential spam sources will help reduce the amount of spam that comes through your systems.

Have a mail policy

Have a mail policy that includes the sending of spam. While you are working very hard to stop spam from arriving, it's good to make sure that none of your users is a source of this type of mail. Make sure that users know what the rules are with e-mail and what constitutes productive use of e-mail in your environment. In some environments, inboxes are cluttered with jokes and other non-work related e-mail. If jokes are important to your organization, consider creating a discussion database for these types of messages; it can help to reduce the clutter.

Also consider using a discussion database or custom database for internal classified ads. Some users can find the ads and the subsequent threads that can follow the ads distracting in their inbox. If users want to be notified, you can use an agent that sends a daily summary of the new items that are in the database.

Users should never respond to spam

People that send spam are looking for a response. Advise your users of this and what the costs of spam are. Chances are, they are aware of it and dislike it as much as you do—but make sure that they know never to purchase anything from an unsolicited e-mail. A key reason that spam is a problem is that people continue to respond to it; if there were no buyers there would be no sellers. Make sure that your users are not adding to the problem by responding to the e-mail at all. This includes the “opt out” links that are often just used to verify whether or not a valid address has been found.

Ensure that your users understand that many unsolicited e-mail offers are hoaxes or confidence tricks. Some examples to note are the “Nigerian bank transfer” scam, and the “Timmy is trapped in the well” hoax. Explain to your users that if an offer or e-mail seems too good to be true, it's probably spam. And many “cries for help” or “secret recipes” are just scams to try and create e-mail chaos and generate more spam.

How to communicate with users about spam

Probably the best way to find out how spam impacts your users is to conduct a survey. Combine a survey with an information campaign: inform users about what spam is and how to avoid it while finding out whether it is a problem for them or not. Knowing how much of a problem spam is for your users will help you gauge how aggressive a stance to take on stamping it out.

Here is an example of a spam information message that you can modify and send to your users:

```
Dear users,
   The Information Systems department is interested in reducing the amount of
   unsolicited commercial e-mail (aka spam) delivered to our organization. We
   would also like to find out whether spam is a concern for you, as this will
   help us determine the best approach to take when configuring our systems to
   reject spam.

How to Avoid Spam
   The best way for us not to receive spam is to prevent our e-mail addresses
   from being gathered by those that send spam. Here are some ways that you
   can help:
   –  Never respond in any way to unsolicited commercial e-mail. Responding can
      make your address a target for more spam - this includes any “opt out”
      links which are often used just to verify that yours is a valid address.
   –  Avoid giving out your e-mail address on Web sites or discussions.
      Consider using a personal e-mail address or a free e-mail address for
      non-work-related correspondence.
   –  Disregard chain letters or other spam that encourages you to send
      messages to others.
   –  If you send mail to several external users, consider putting the
      addresses in the “bcc” field so that all of the addresses are not visible.

If you are careful and avoid having your address get on the spam lists you can
avoid having spam delivered to our organization.

Sincerely,

Your Domino Administrator
```

2.2 How to block spam

If spammers manage to get your users’ addresses, you may need to select an approach that configures your systems to block spam. As previously mentioned, there are two major philosophies when it comes to dealing with spam. The “gateway” approach forestalls spam by rejecting it based on either content or address origin when it reaches the organization's entry point. The “user” approach delivers all mail, even spam, and provides tools to the user so that the user can decide what is spam and what is mail. These approaches are not mutually exclusive, and the “right” approach depends entirely on your organization and your users. You will want to engage some server-based spam blocking techniques if you are looking to take an aggressive approach against spam.

2.2.1 At the gateway

It is possible to subscribe to third party services or purchase network devices that aim to stop spam even before your mail server receives it. These services often act as a mail relay, and screen incoming mail for content or origin. Many ISPs and other service providers offer this as a service with a cost per megabyte of spam. Keep in mind that subscribing to these services may require a change to your mx (DNS mail delivery) records which, if not handled correctly, could cause a loss of mail during the transition. If you plan to use a third party or gateway device or service, be sure that you are aware of the technology that is used and the potential for false positives or friendly mail rejections. The ideal configuration rejects all spam while allowing all real mail through. Even if your organization employs some sort of spam gateway, it may also be a good idea to use other methods of spam rejection.

2.2.2 At the server

Stopping spam at the server and sending a rejection can be a very effective way of dealing with these messages. There are several configuration areas in Notes Domino 6 that can be set to help reject spam, both at the SMTP listener level and at the Domino router level. At the listener, the following options are available in Domino 6:

- Inbound Relay Control and Enforcement
- Inbound Intended Recipient Controls
- Disabled SMTP Routing to Groups
- Inbound Connection Controls
- Inbound Sender Controls

At the router, the server can be configured to deal with spam using server-based mail rules. These rules can be used to filter out specific recipient addresses or other specific criteria.

Inbound authorization settings can be used to reject known spam originators or known open relays. Open relays are servers that are configured to allow the sending of third party messages, including spam. You should always configure your server to not allow open relaying of mail to help fight spam. New in Notes Domino 6 are server mail rules and DNS blacklist support. Using server mail rules you can reject messages based on content (including recipient and originator.) If your server is configured with DNS blacklist lookups enabled, when a message arrives an external directory is consulted (much like a DNS lookup) and if the sender’s address is found in the directory, the message is considered spam. The spam can then be quarantined or rejected depending on your preference.

Also new in Domino 6 are intended recipient controls. With this restriction in place only users that exist in the Domino directory can receive mail.

The settings and components of Domino 6 spam prevention features are discussed in detail in Chapter 4, “Domino 6 Server anti-spam features” on page 29.

2.2.3 By the end user

Some administrators prefer to adopt a hands-off approach and have the gateway and server deliver all mail whether solicited or not. Users that want to reject mail are advised to use mail file rules to filter the signal from the noise. This can be an effective strategy where spam is not a serious problem and occurs only occasionally. Keep in mind that spam is a moving target, and originators’ addresses and the content often changes; user's mail rules can sometimes require frequent updates to stay on top of these changes.

Managing spam at the user level with Notes 6 involves creating mail file rules. These rules can be very targeted and aggressive since the user has the control here, and they can decide what they want to discard and what they want to retain. If they do create false positives, they can retrieve them or adjust the mail rules accordingly. Chapter 5, “Using mail file rules to prevent spam” on page 65 discusses this in detail.

2.2.4 Selecting the best approach

Spam may not be a big problem for you; maybe you have yet to receive an unsolicited e-mail message. Your users, however, may be wading through hundreds of useless messages a day. Consult your users and find out how much of a problem spam is for them. Consider sending out a survey to find out how many unsolicited e-mail messages they receive, how tolerant they are of false positives, and how willing they are to manage mail rules. If your users are fed up with spam and wish to make it a high priority, we recommend a server-based approach. If your users do not see spam as a major problem, are quite adept with Notes Mail rules, and are highly sensitive to false positives you may want to consider a user-centric solution. The best approach to employ in your anti-spam campaign is the one that fits for your organization.

After you have selected your approach and implemented your new configuration, re-evaluate the situation with another survey or follow-up with some of the key users. You may want to conduct this survey periodically to make sure that the approach that you have selected is still appropriate.

2.2.5 Managing the ongoing anti-spam campaign

Due to the nature of spam, there is no single configuration setting or secret notes.ini variable to toggle to have all spam delivery rejected. This is due to the constant change in the spam content, addresses, and the spammers themselves. The most effective way to keep your anti-spam configuration relevant is to monitor your results periodically and revise your configuration based on new information.

Determine how much time to allocate

Based on how much of a priority spam prevention is in your organization, and how much of a problem it is to users, you can decide how much time to assign to your anti-spam efforts.

If blocking spam is your top priority (this usually results from upper management receiving some particularly offensive spam) then you should plan to put aside some time daily or weekly to review how effective your configuration is. You may want to start out by monitoring your new configuration daily and tweaking the configuration based on the results. After a few days of this you can move to a weekly analysis. After several smooth weeks you might consider moving to a biweekly schedule. There are some tasks that you should perform infrequently to avoid impacting users. These tasks include surveys, user-based rule changes, and e-mail policy reviews.

How to analyze the effectiveness of your configuration

The daily or weekly tasks should include the following:

- Review the mail log and see how many rejections you are getting. (You can use log analysis to filter for “rejected.”) As these numbers increase your configuration is becoming more effective. Also scan these rejections for potential false positives.
- Scan the mail logs and look for mail with known “spam-like qualities” getting through. Things to look for include messages being sent to a large number of users, subjects such as “make money fast”, and known spam sender addresses. You may identify addresses or messages that your rules have missed.
- Talk with users that are known to receive large amounts of spam, or analyze the logs to see whether spam intended for them is being rejected.
- After reviewing your server rule hits, identify rules that are not being triggered and consider revising them. For those rules that are being triggered, look for ways to make them more effective and scan for false positives.

More infrequently, it's a good idea to review your overall spam approach to see if it is still appropriate. You might want to re-survey your users periodically to see if the situation has improved from their perspective.

It's also a good idea to occasionally appraise the technology landscape to see what the new approaches are to spam detection and prevention. There may be new Domino updates available or new techniques recommended to deter spam delivery.

2.2.6 Summary

The old saying “An ounce of prevention is worth a pound of cure” is especially prescient when related to spam. Users that avoid providing their e-mail address to spammers receive less spam. Web sites that are careful to make themselves a difficult target for harvesters also result in less unsolicited mail. With enough prevention effort, spam should be a rare occurrence. If it does arrive, there are several methods of handling it: gateway-based, server-based, and user-based. The right approach depends on the stance that your organization takes when dealing with spam and how much of a priority it is for you. A solid spam prevention configuration needs to be monitored and adjusted over time. Reserve some time every week to analyze the effectiveness of your anti-spam configuration, and periodically revisit your approach to ensure that it is still consistent with what is required. Overall, much can be done to avoid and reduce spam delivery.

3

Domino 6 anti-spam architecture

This chapter describes the components of the Domino messaging architecture that allow you to prevent and manage spam. As you begin using Domino to prevent spam, it is important to understand the messaging infrastructure and the components where it’s possible and appropriate to intercept spam.

Private Notes/Domino networks are well controlled and do not originate spam mail. The public and open nature of Internet e-mail has led to an explosion of spam, so for purposes of spam analysis, we focus on Internet-originated messages and how the Domino messaging components process those messages.

This chapter discusses:

- How anti-spam control and management work can be divided between servers.
- How the different anti-spam measures are divided between Domino server tasks.
- How the control over anti-spam measures is divided between the Domino administrator and the end-users.
- Common problems and recommended solutions.

3.1 The Domino messaging environment

While every Domino installation is different, and many do use a single Domino server to handle all tasks related to e-mail, a division of tasks between multiple servers is typical of most larger environments. Generally, there are a number of Domino servers on an internal network that users connect to in order to access their mail, and one or more external Domino servers that are responsible for connections to the Internet for inbound and outbound SMTP e-mail.

Some of the anti-spam features in Domino 6 must always be implemented on the external Domino servers that handle the actual SMTP connections, some must always be implemented on the internal servers, and some of the anti-spam features can be implemented on either the external or internal servers—or even on additional dedicated servers that are located “in between” the external servers and the internal servers in the network topology.

The features that must be implemented on the external servers are:

- DNS blacklist filtering
- Inbound relay control and enforcement
- Inbound intended recipient controls
- Inbound connection controls

The features that must be implemented on the internal servers are:

- User mail file rules

The features that may be implemented on either internal, external or other dedicated servers are:

- Inbound sender controls
- Disabled SMTP routing to groups
- Server mail rules

Figure 3-1 shows one such typical Domino network. A network such as the one depicted here is an ideal configuration for establishing control of spam via the Domino 6 anti-spam measures described in this redbook.

The implemented strategy to fight spam in the example Domino environment is to stop spam at the Domino server.

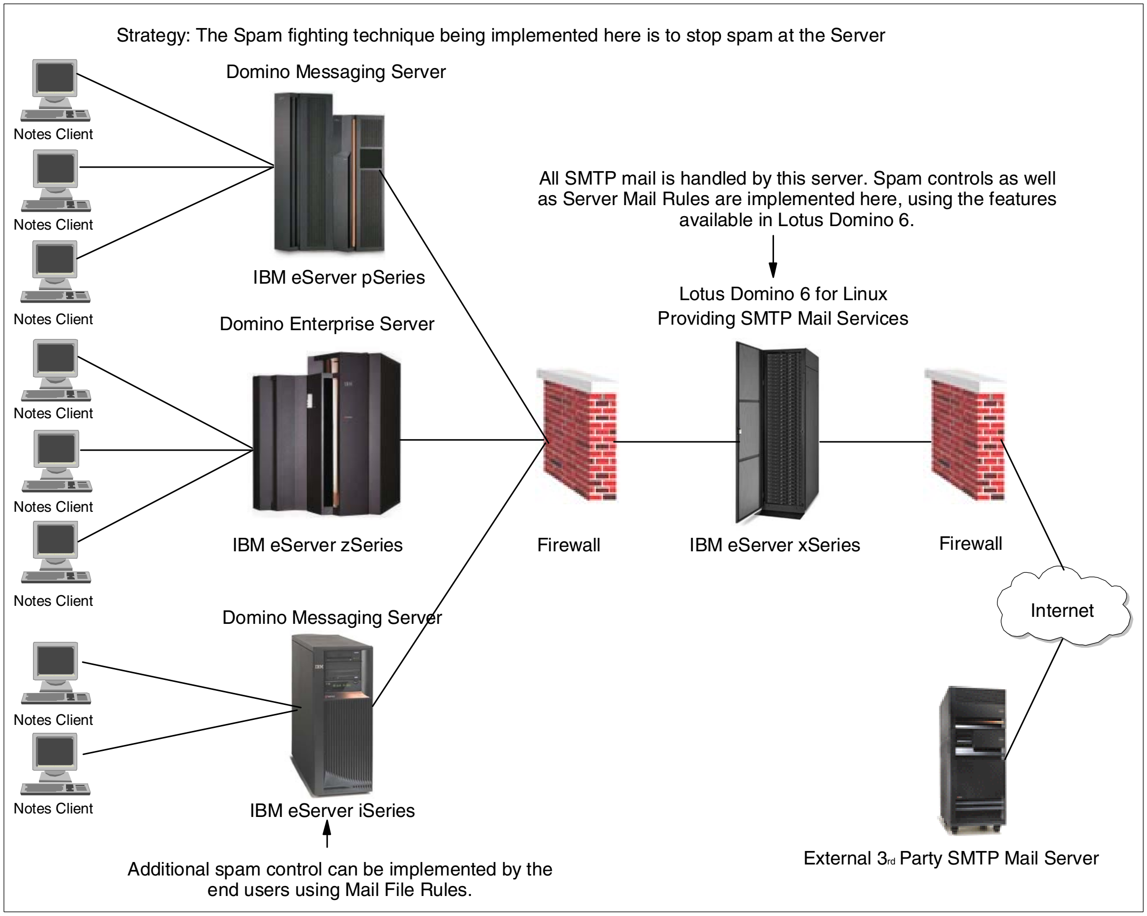

Strategy: The Spam fighting technique being implemented here is to stop spam at the Server
Domino Messaging Server
Notes Client
Notes Client
Notes Client
IBM eServer pSeries
All SMTP mail is handled by this server. Spam controls as well as Server Mail Rules are implemented here, using the features available in Lotus Domino 6.
Lotus Domino 6 for Linux Providing SMTP Mail Services
Domino Enterprise Server
Notes Client
Notes Client
Notes Client
IBM eServer zSeries
Firewall
IBM eServer xSeries
Firewall
Internet
Domino Messaging Server
Notes Client
Notes Client
IBM eServer iSeries
Additional spam control can be implemented by the end users using Mail File Rules.
External 3rd Party SMTP Mail Server

Figure 3-1 Fighting spam with a Domino 6 infrastructure

The server between the two firewalls, in the DMZ, is running Domino 6 for Linux. All SMTP mail is routed through this server and the anti-spam measures are enforced there. As the Domino version on the server is version 6, all the new anti-spam features can be utilized. Notice that not all the servers or clients in your environment have to be running Notes and Domino 6 to prevent and manage spam. Upgrade your SMTP mail server at the earliest possible stage of your upgrading project to take advantage of the new anti-spam features even before your other servers and clients are upgraded to Domino 6.

As a Domino administrator, you can implement mail rules on the server to protect against viruses and eliminate as much spam as you can. The end users of your organization can take further actions to manage spam by creating mail file rules.

End users can implement mail file rules to act on any spam that might have passed through the spam prevention measures configured on the server.

3.2 Domino 6 messaging components

In this section we describe the messaging components used by Domino 6 to help you control spam.

The Domino 6 anti-spam components are activated at three different points during the reception of an incoming message. Spam can be controlled by:

1. The SMTP Listener when incoming connections are established
2. The SMTP Server when messages are placed into MAIL.BOX
3. The Router when messages are moved from MAIL.BOX to individual mail files

Figure 3-2 is a graphical depiction of Domino 6 anti-spam messaging components.

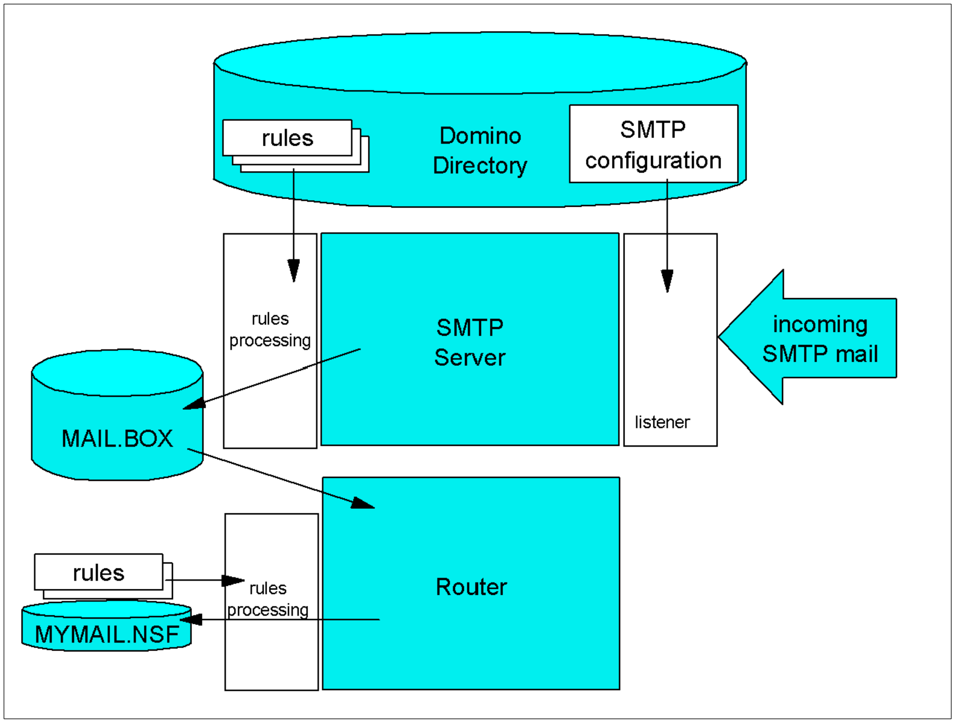


Figure 3-2 The Domino 6 messaging components

3.2.1 SMTP Listener/Server

Incoming SMTP messages are processed by the SMTP Listener task. This task is responsible for accepting incoming requests to communicate with the Domino SMTP server. The SMTP Listener task and the configuration settings that it uses are your first line of defense against spam. The features employed by the SMTP Listener task include:

- DNS blacklist filtering
- Inbound relay control and enforcement
- Inbound intended recipient controls
- Disabled SMTP routing to groups
- Inbound connection controls
- Inbound sender controls

For detailed discussion about the use of each of the listed feature, refer to Chapter 4, “Domino 6 Server anti-spam features” on page 29.

The SMTP Listener uses the configuration settings to determine if an incoming connection should be accepted. Once a connection is established, the SMTP Listener checks additional information in any incoming message and determines if the incoming message should be accepted. DNS blacklist filtering allows you to use an alternative vendor to validate the sending IP address against their database. If an originating IP address is determined to be a source of spam, the connection can be denied, or the incoming message can be tagged or logged. Even without blacklist processing, the incoming connection can be denied based on the originating IP address or name. Incoming messages can be processed and/or rejected based on origin e-mail address, IP address, or domain name.

Figure 3-3 and the list following the figure describe the sequence of configuration checking that occurs during the receipt of a message.

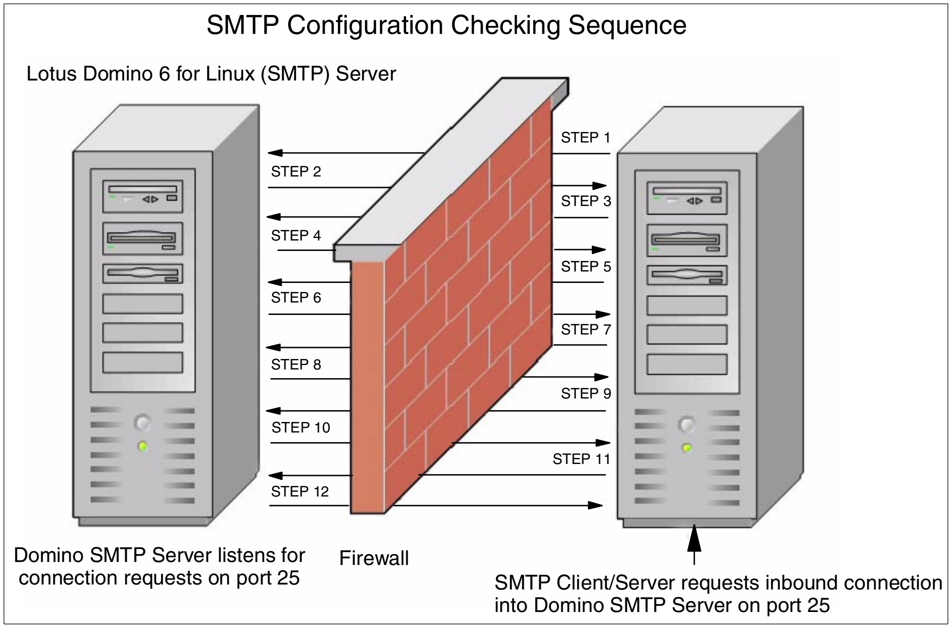

SMTP Configuration Checking Sequence
Lotus Domino 6 for Linux (SMTP) Server
STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6
STEP 7
STEP 8
STEP 9
STEP 10
STEP 11
STEP 12
Domino SMTP Server listens for connection requests on port 25
Firewall
SMTP Client/Server requests inbound connection into Domino SMTP Server on port 25

Figure 3-3 Communication sequence for incoming SMTP mail

The general communication sequence of incoming SMTP mail is as follows:

1. Originating SMTP server makes a connection request to Domino SMTP server on the TCP/IP port.
2. Domino SMTP server responds to the connection request and allows or denies connection based on SMTP Inbound Controls on Server Configuration document.
3. Originating SMTP server sends the MAIL FROM containing the sender's internet address.
4. Domino SMTP Listener checks Inbound Sender Controls, comparing contents of the MAIL FROM. If the maximum message size is enabled on the server and the client has provided the message size as a parameter on the mail from command, the inbound file size restrictions are performed (messages that are too large are rejected).
5. Originating SMTP server sends the RCPT TO containing the internet address of the intended recipient. (Note: Steps 5 and 6 are repeated for additional recipients.)
6. Domino SMTP Listener checks Inbound Intended Recipients Controls, comparing contents of the RCPT TO. If intended recipient is not a local user, it checks Inbound Relay Enforcement and Inbound Relay Controls, comparing contents to the RCPT TO.

7. Originating SMTP server sends the DATA command to initiate the transfer of the message contents.
8. Domino SMTP Listener acknowledges start of DATA.
9. Originating SMTP server sends END OF DATA to indicate data transfer is complete. Domino SMTP Listener checks any inbound file size restrictions. Server mail rules are run, but only “Don’t accept message” action is applied here.
10. Domino SMTP acknowledges END OF DATA and awaits disconnect or next message. (Note: Steps 3 through 10 are repeated for additional messages.)
11. Originating SMTP server sends QUIT, initiating close session sequence.
12. Domino SMTP acknowledges QUIT and closes connection.

The earlier in this sequence that you can detect and reject a spam message, the fewer server resources are wasted by the spam.

3.2.2 Router

Once a message has been received by the SMTP Listener, it is analyzed against the Server mail rules. The Server mail rules are evaluated against any incoming message as it is placed into the server MAIL.BOX. Server Mail rules are your second line of defense. Inbound controls can and should be used to block all mail to or from specific users and domains. The Server mail rules allow more flexibility and control by allowing you to specify additional conditions to be tested. You can also specify additional actions to be taken on the message other than just denying the delivery of it.

If a message passes all testing in the server rules, it is then processed by the router for forwarding to another Domino server (which might have a different set of rules), or for placement into an end-user mail file. The mail file rules are typically established by the end-user of the mail file. Mail file rules are evaluated for any incoming messages on the server, before delivering the message to the user’s mail file. Every Domino installation is different, and your particular circumstances will dictate where and how stringently you control incoming spam.

3.3 Domino 6 anti-spam configuration

The best defense against spam is knowing the options available to you as the administrator. Being able to identify what messages are considered spam, versus those that were unsolicited, will help in eliminating it. Spam comes in many forms, from Web hoaxes, chain letters, and unsolicited sales and marketing material for a product you’d never buy, to the most common, offensive adult-rated content. What is perceived to be offensive to one person may not be to another, and the amount of time an end user takes to delete this message varies from user to user. Identifying these spam messages and how you choose to act on them will vary from customer to customer. The features in Domino 6 will help you fight the battle to eliminate spam from your environment.

3.3.1 Server configuration features

This section introduces the anti-spam features that can be configured on a Domino 6 server by the Domino administrator. Enabling some or all of these features will have a performance impact on your Domino server.

Domino 6 has the ability to perform lookups to external sites, to determine if the connecting host is a known spamming site. This new feature, called *DNS Blacklist filters*, enables you to specify the name of one or more DNS blacklist sites (DNSBL) to check the validity of the incoming connection. DNS blacklist checking consists of utilizing an external source to conduct DNS queries to check if the inbound SMTP connection is coming from known sources of spam or hosts that permit third-party, open relaying.

Another new feature is *Verify that Local Domain recipients exist in the Domino Directory*. This feature verifies that mail received by your SMTP server is actually intended for a local user in your domain. When enabled, all messages received via SMTP are looked up based on the value of the RCPT TO field on the incoming message. If the recipient's address is not a local user, the message is not accepted and a Non Delivery notification is returned to the sender. This feature can help prevent messages sent to nonexistent users from accumulating in MAIL.BOX as dead mail. They are typically spam messages or messages intended for a user that has left the company.

Inbound connection controls allow you to specify how the Domino SMTP server will handle inbound connection requests and which hosts it will allow and deny connection to this server.

Inbound sender controls allow you to specify how the Domino SMTP server will process connections based on the sender address. You can deny and/or allow messages from specified addresses/domains.

Inbound relay controls were introduced in Domino Release 5. These options provide settings to control what servers can use your server as a relay and the destinations you'll allow mail hosts to relay messages to. Added to the product in Domino 6 are the *Inbound relay enforcement* options. These features allow you to further specify how anti-relay checking will occur. You can now enable anti-relay enforcement to apply to all external hosts, all hosts (internal or external), or not apply checking at all. You can exclude certain hostnames from this checking by specifying the hostname or IP address in an exclusion list. In previous versions of Domino, when you implemented Relay controls your POP or IMAP users were often prohibited from using Domino as a relay. Enhancements made in this area now allow you to provide your authenticated users with the ability to relay off the Domino server and not require relay control checking.

Although not documented to be a spam deterrent, a new notes.ini variable can be used to disable routing internet mail to groups. By enabling `RouterDisableMailToGroups=1`, Internet messages sent to a group defined in your Domino Directory will be failed.

Server Mail Rules are new to Domino 6. Similar to mail file rules implemented with the Notes client for a individual user in Release 5, server mail rules can be configured to act on specific messages upon entry into your Domino environment. You may choose to filter messages based on content, the number of attachments, the type of attachments, the number of recipients, and many other criteria. Messages containing questionable or offensive content can be examined and moved to a quarantine database for further analysis.

3.3.2 User configuration features

Mail file rules allow the individual end-user to isolate messages by sender address, domain, subject, or even by message body content. When creating anti-spam mail file rules with the Notes client, end users can be specific and even aggressive when defining the rules. End user can specify which actions are taken on the identified spam messages, whether they want to file the messages for further inspections and actions, or simple get rid of the unwanted messages.

Building anti-spam mail file rules should be seen as an additional measure in the overall solution to the spam problem. Although configured by the end users with their Notes client, mail file rules are enforced on the Domino server. Therefore, they do use some server processing power, and having a large number of mail file rules or several rules per user might have a performance impact on the server. Because of this, your anti-spam campaign needs to be well planned, and adequate direction on how to use mail file rules should be provided for the end users.

3.4 Common problems and solutions

A numbers of features are available to help you manage common messaging and e-mail problems. Each feature is particularly well suited to one or several specific kinds of problems. The correspondence between some common problems and the most appropriate features for solving them are shown in Table 3-1. Details for the techniques identified are in the following text.

Table 3-1 Some common problems and the features available to solve them

Problems	DNSBL Filters	Inbound intended recipient controls	Disable SMTP Mail to Groups	Inbound connection controls	Inbound sender controls	Server Mail Rules	Inbound Relay Controls	Inbound Relay enforcements	User Mail File Rules
Message received from a known spam domain.	X				X				X
A specific host is sending a large amount of spam to your server.				X					
A specific e-mail address is sending a large amount of spam to your server.					X				
External servers (spammers) are using your server as a relay.	X						X	X	
Messages are sent to users that are no longer with your company.		X			X				
Message received containing offensive content.						X			X
Internal servers/users are using your servers as a relay.							X	X	
Inbound messages are addressed to bogus users in your domain (more likely spam messages).		X			X				
Your domain has been blacklisted and can no longer send mail to other internet domains.							X		
A new virus has been identified and reported on the Web but it has not been incorporated into your vendor's anti-virus database. You want to stop these messages from coming into your domain.						X			
You suspect internal users are forwarding E-mail chain letters or Web hoaxes.						X			
Spammers are sending mail to public group names.			X						

Message received from a known spam domain.

- Inbound sender controls: Deny messages from this domain
- User mail file rules: Create a rule for this and don't accept mail from this domain.

- DNS blacklist filters: Check inbound connection and look-up host in DNS blacklist; log and reject message if determined to be from a known spamming site.

A specific host is sending a large amount of spam to your server.

- Inbound connection controls: Deny connection from this host.

A specific e-mail address is sending a large amount of spam to your server.

- Inbound sender controls: Deny messages from this address.

External servers (spammers) are using your server as a relay.

- Inbound relay controls: Close down your open relay, “Deny messages to be sent to the following external domains: *” and “Deny messages from the following internal hosts to be sent to external internet domains: *” (Note: * means all).
- Inbound relay enforcement: Change “Perform Anti-Relay enforcement for these connecting hosts,” to External hosts or All connecting hosts.
- DNS blacklist filters: Check inbound connection and look-up host in DNS blacklist; log and reject message if determined to be from a known spamming site.

Messages are sent to users that are no longer with your company.

- Inbound intended recipient controls: Enable “Verify that local domain recipients exist in the Domino Directory” to deny messages for recipients not listed in the Domino Directory, or list the e-mail address in the “Deny messages” field.

Messages are being received containing offensive content.

- Server mail rules: Create a rule to reject messages based on text of message, body or subject.
- User mail rules: Create a rule to reject messages based on text of message, body or subject.

Internal SMTP servers/users are using your Domino 6 server as a relay.

- Inbound relay controls: Close down your open relay, “Deny messages to be sent to the following external domains: *” and “Deny messages from the following internal hosts to be sent to external internet domains: *” (* means all).
- Inbound relay enforcement: Change “Perform Anti-Relay enforcement for these connecting hosts” to “All connecting hosts.”

Your domain has been blacklisted and can no longer send mail to other Internet domains.

- Inbound relay controls: Close down your open relay, “Deny messages to be sent to the following external domains: *” and “Deny messages from the following internal hosts to be sent to external internet domains: *” (* means all).
- Contact the Administrator of the DNS blacklist site where your domain is blacklisted and request your domain be removed from their list. This often requires that additional checks be conducted after you close down your relay.

Inbound messages are addressed to bogus (invalid) users in your domain (more likely spam).

- Inbound intended recipient controls: Enable “Verify that local domain recipients exist in the Domino Directory” to deny messages for recipients not listed in the Domino Directory.
- Inbound sender controls: If this continues, deny messages from this domain.

A new virus has been identified and reported on the Web but it has not been incorporated into your vendor’s anti-virus database. You want to stop these messages from coming into your domain.

- Server mail rules: Create a rule that moves messages with particular extension types (bat, exe, vbs, and so forth) to a quarantine database or do not accept these types of attachments.

You suspect that internal users are forwarding e-mail chain letters or Web hoaxes to other users.

- Server mail rules: Create a rule that acts on messages based on the contents of the messages believed to be the offending messages; move them to a database for further analysis.

Spammers are sending mail to your public group names.

- Disable the ability to route SMTP mail to your groups by enabling the server notes.ini variable `RouterDisableMailToGroups=1` on your inbound SMTP server. You can also use reader lists to control who can send mail to individual groups.

4

Domino 6 Server anti-spam features

This chapter describes the features available on the Domino 6 Server to assist with combating spam. We discuss in detail how to configure the new features, as well as features previously introduced in Domino Release 5.

We start by discussing how to detect spam messages.

Then we describe features that are available to control connections from spammers:

- DNS Blacklist filters
- Intended Recipient Controls
- Disabling Routing SMTP Mail to Groups
- Inbound Connection Controls
- Inbound Sender Controls

Next, we detail what can be done to control the delivery of spam with:

- Server Mail Rules

Finally, we discuss how to control use of your server as a relay, employing:

- Inbound Relay Controls
- Inbound Relay Enforcement

4.1 How to detect spam

As the Administrator, you will be tasked with determining what messages are spam. Working closely with your end users, you will get a good idea of the messages reaching the users' mail files.

But what about the messages that never make it to a user and wind up as, depending on the configuration of your system, DEAD or HELD mail in mail.box? Dead messages are messages that cannot route to the intended recipient and cannot route back to the sender. Held messages are undelivered messages held in mail.box instead of returning them to the sender. Often times, the address of the sender appears to contain a valid Internet address and the same with the name if the intended recipient. Viewing document properties, you can obtain valuable information about each specific message. Each message contains pertinent information about the sender, the intended recipient, the contents of the message and the hosts that routed this message. Using the information found in certain fields you can implement intended inbound recipient controls or even deny connections from certain hostnames or IP addresses.

4.1.1 Examining the message properties

By analyzing the properties of a message and reviewing several key fields, you can determine who the sender is, what servers processed this message, and who the intended recipient is. The fields to examine are:

- **From:** This is the address of the From: RFC822 header, if there was one added to the message. The From: address is often different than the SMTPOriginator on spam messages.
- **SMTPOriginator:** This is the address of the sender; it is built from the value of the MAIL FROM:
- **IntendedRecipient**: This is who the message was originally sent to; often times the address is invalid.
- **Recipients:** This is the address of whomever the message should be routed to.
- **Received:** This header contains routing information and the names/IP addresses of the SMTP servers that processed this message. All SMTP servers that process this message are required to place a received header on the message. It's not unusual to have a message that contains multiple received headers.

To get the document properties of a message:

1. View the documents in mail.box (or mail1.box, mail2.box, and so forth).

2. Select the document, right-click, and choose Document Properties. The individual fields are on the left and the value held in each field is on the right.

If you find that Dead mail or Held mail is accumulating in mail.box, determine whether the messages are for valid users by checking the IntendedRecipient field for each message.

You can use the value of the Received fields to determine the sending server's IP address or hostname. This is normally the last received field in the document. Received fields are read from bottom up, with the top received field being the one added by your Domino Server. The received fields also contain the time/date for each server processing the message. If you are being spammed by a particular IP address or hostname, you can use this information to place this host in the Deny connections from this host category.

If you have a large quantity of dead or held messages that appear to be invalid addresses in your domain, sent from the same domain, you may have been under a harvesting attack. Check the SMTPOriginator and From: fields to determine the sender of these messages. Keep in mind, most spam messages do not contain valid e-mail addresses and it's likely these headers will be different.

4.1.2 Separating legitimate e-mail from spam based on content

Often server mail rules are focused on the sources, the addresses and domains of incoming e-mail. There are some characteristics of spam mail that allow you to scan or search for items that can help you classify useful e-mail and eliminate spam e-mail. Some characteristics are easily discernible by simply viewing the message subject or content. Other characteristics can be identified by viewing the source information of incoming messages.

To learn more about how to separate e-mail from spam based on the content of the messages, see 5.1, "Distinguishing between spam and legitimate e-mail" on page 66.

4.2 Controlling connections from spammers

This section discusses which actions can be taken to control connections from spammers. The earlier you are able to stop spam messages from entering your environment, the more benefits you will gain. The features described in this section aim to stop spam at the Listener task. If you are able to stop spam there, you often avoid the whole message ever being transmitted over the networks, which will save network bandwidth and storage. Some of the anti-spam controls described here consume server system resources; therefore, they may have performance impacts. If spam is a major problem for your organization, the benefits of implementing controls here will outweigh the performance costs.

Note: For the features described in this section to work effectively, your Domino SMTP server has to be designated as a direct mail exchange server (MX server) on the Internet. If you relay messages from an internal SMTP server to your Domino server, the inbound connection will always be from the same internal server and the connection checking will always pass. In order for Inbound Connection controls or DNS Blacklist filters to work, the inbound connection to your SMTP server must be from an external sending IP address.

4.2.1 DNS Blacklist filters

DNS Blacklist (DNSBL) filters support allows you to configure the Domino 6 server to query an external DNS Blacklist site to be sure that the mail you are receiving is from a reputable source.

What is a DNSBL? Well, simply put, it is a list or database containing host names and IP addresses of known spamming sites or hosts that are susceptible to being used by a spammer. Hosts that allow relaying, also known as “Open Relays,” do not have any security imposed on their systems, allowing any user to send mail from their systems. These open relays leave their systems open and could be used by a spammer to flood the Internet with junk mail. Host names and IP addresses found in DNSBL databases are those of hosts that have failed to pass certain relay checking requirements, and therefore pose a high probability that they will be used by a spammer.

The sites that maintain DNSBL databases conduct tests against hosts that are believed to be open relays. When a host is found to be open, their hostname and IP address is added to the list until the system passes these relay checks. Often a host is placed on this list for being an open relay, without the host knowing that they were left open. If this happens, the owner of the host can work with the DNSBL site to verify that all open relay capabilities have been closed down.

DNSBL checking tends to vary from site to site. Some sites provide their service for free, while others charge a fee for their service. Contact your prospective DNSBL service provider to inquire on pricing.

Listed in Table 4-1 are several commercially available DNSBL service providers. We do not recommend one service provider over another. You should be aware that other services are available to you and you should contact individual blacklist providers to learn about their services and policies. We suggest you perform a Web search on DNS Blacklist sites to obtain listings of other providers since they may provide additional services you require.

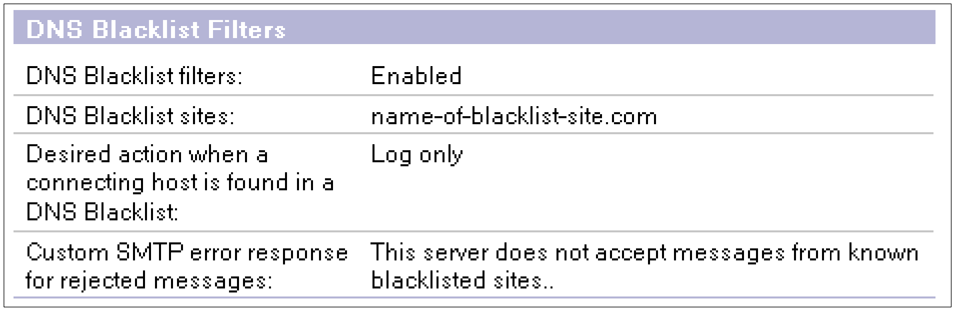
Table 4-1 Examples of DNSBL service providers

Service provider	**Web site URL**
Spamcop	`http://www.spamcop.com`
Mail Abuse Prevention Systems, LLC	`http://www.mail-abuse.org`
The Spamhaus Project	`http://www.spamhaus.org`
The Open Relay Database (ORDB)	`http://www.ordb.org`
OsiruSoft Research & Engineering	`http://www.osirusoft.org`

You can specify multiple sites to query, but be aware of the potential overhead of checking multiple databases. When utilizing multiple DNSBL sites, Domino will perform queries to all sites until a match has been found. If the connecting host is located in the first DNSBL site specified, the search is complete and remaining DNSBL sites will not be queried. The more DNSBL sites you use, the longer your queries could take.

Configuration of DNS Blacklist filters

1. In the Administration client click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the configurations settings document for the server you want to administer and click Edit Configuration.
4. Click the tabs in the following order: Router/SMTP → Restrictions and Controls → SMTP Inbound Controls and navigate down to DNS Blacklist Filters.
5. Double-click the document or click the Edit Server Configuration button to put the document in edit mode.



DNS Blacklist Filters

DNS Blacklist filters:	Enabled
DNS Blacklist sites:	name-of-blacklist-site.com
Desired action when a connecting host is found in a DNS Blacklist:	Log only
Custom SMTP error response for rejected messages:	This server does not accept messages from known blacklisted sites..

Figure 4-1 DNS Blacklist filters settings (Enabled)

6. Make the desired changes and click Save & Close.

> **Note:** You should consider creating a descriptive SMTP error message for rejected messages. Explain why you are not accepting this message and that if the message is *not* spam, suggest that the sender's organization contact organizations maintaining DNS blacklist sites to get off their blacklists. You might also consider listing the DNS blacklist sites your organization uses for checking connecting hosts for inbound SMTP mail.

DNS Blacklist filters are disabled by default. Figure 4-1 on page 34 depicts the field as it exists when it is Enabled. The additional 3 options will only be available when the feature is enabled.

The "DNS blacklist sites" field is used to specify the DNSBL site (or sites) that Domino will query. When you select sites to query, be aware that many DNSBL sites are fee-based and may require a subscription prior to utilizing their server. Contact the DNSBL site for more details.

When enabled, Domino will query the DNSBL sites that you've specified to determine if the connecting host name is listed in the database as a blacklisted site. If the host is not found in the first DNSBL site, Domino will then look to all subsequent DNSBL listed (if applicable). This feature is not enabled by default, but it is extremely useful in environments that have Domino as their SMTP server connected directly to the Internet.

This option will provide a level of checking for your inbound SMTP mail, as well as statistical reporting about where each of the blacklisted sites was found. Using the statistics available though Domino, you might want to make a business decision to implement tighter server mail rules, based on the sites found in the DNSBL.

The field “Desired action when a connecting host is found in a DNS Blacklist” has 3 possible options:

- `Log only`

  When Domino finds that a connecting host is on the blacklist, it accepts messages from the host and records the hostname and IP address of the connecting server and the name of the site where the server was listed.

- `Log and tag message`

  When Domino finds that a connecting host is on the blacklist, it accepts messages from the host, logs the host name and IP address of the connecting server, and the name of the site where the server was listed, and adds the Notes item $DNSBLSites to each accepted message.

- `Log and Reject message`

  When Domino finds that a connecting host is on the blacklist, it rejects the connection and returns a configurable error message to the host.

> **Note:** Domino uses IP version 4 (IPv4) addresses when querying DNS blacklist sites to find out if a connecting host is listed. If the connecting host has an IP version 6 (IPv6) address, Domino skips the DNSBL check for that host.

Using the Custom SMTP error message response for rejected messages, you can create your own error message. In the previous example, custom error handling is enabled and will result in a delivery failure report being returned with the text found in this field. If no custom error response is entered, the default error message will be “`Connection denied based on policy reason`.”

When utilizing the DNS Blacklist filters, you may wish to obtain additional statistics to determine which connections are being reported as found in the DNS Blacklist database. Domino does not enable these statistics by default.

To begin reporting the specifics on where these connections are coming from, and in what DNSBL these hosts were found, enable the following notes.ini variable on your SMTP server:

```
SMTPExpandDNSBLStats=1
```

SMTPExpandDNSBLStats:

Syntax: `SMTPExpandDNSBLStats=`*`value`*

Description: Use this setting to generate DNS Blacklist filter statistics for each connecting host found in a DNS blacklist site.

0 - Host-specific DNS Blacklist filter statistics are not generated by the SMTP server.
1 - SMTP server generates host-specific DNS Blacklist filter statistics which indicate the total number of hits per DNSBL site, per connecting host's IP address.

Applies to: Servers.

Default: In the absence of this setting, the SMTP task maintains statistics that track the total number of connecting hosts that were found on the combined DNSBL of all sites combined, as well as how many were found on the DNSBL of each configured site.

UI equivalent: None

These statistics are maintained by the SMTP Listener task and are cumulative while the SMTP task is running. Restarting the SMTP task or rebooting the Domino server will result in new statistics being recorded.

4.2.2 Inbound Intended Recipients Controls

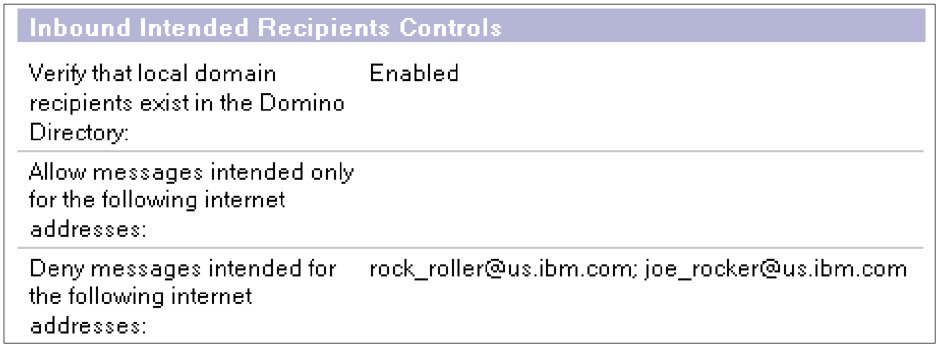
New to Domino 6 is the ability to verify that the intended local recipients actually exist in the Domino Directory prior to accepting a message inbound via SMTP. This is controlled using the “Verify that local domain recipients exist in the Domino Directory” field on the Inbound Intended Recipients Control section of the server configuration document. By enabling this feature, all messages received via SMTP will attempt to match the value of the RCPT TO envelope header to a user in the $Users view of the Domino Directory.

Configuration of Inbound Intended Recipient Controls

1. In the Administration client click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the configuration settings document for the server you want to administer and click Edit Configuration.

4. Click the tabs in the following order: Router/SMTP → Restrictions and Controls → SMTP Inbound Controls and navigate down to Inbound Intended Recipient Controls.

5. Double-click the document or click the Edit Server Configuration button to put the document in edit mode.



Inbound Intended Recipients Controls

Verify that local domain recipients exist in the Domino Directory:	Enabled
Allow messages intended only for the following internet addresses:	
Deny messages intended for the following internet addresses:	rock_roller@us.ibm.com; joe_rocker@us.ibm.com

Figure 4-2 Inbound Intended Recipients controls

6. Make the desired changes to the Inbound Intended Recipients Controls fields and click Save & Close. The fields have the following meanings:

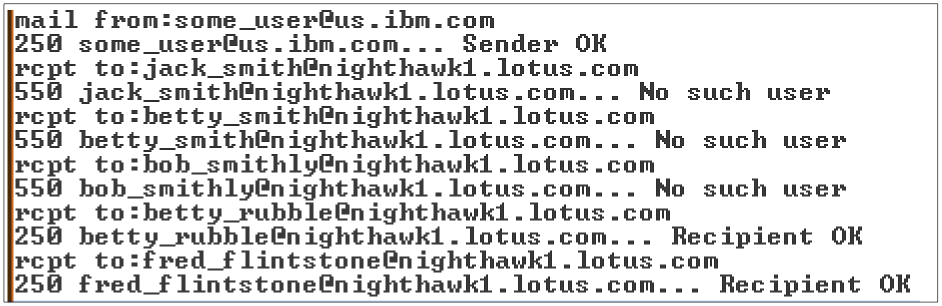
   – "Verify that local domain recipients exist in the Domino Directory."

     The default is disabled.

     When enabled: If the domain part of an address specified in an SMTP RCPT TO command matches one of the configured local Internet domains, the SMTP listener checks all configured directories to determine whether the specified recipient is a valid user. If all lookups complete successfully and no matching username is found, the SMTP server returns a 550 permanent failure response indicating that the user is unknown. Enabling this option has benefits in the areas of bandwidth, storage, and performance, as the body of the rejected message is never delivered.

     Enabling this option can help prevent messages sent to nonexistent users (for example, spam messages and messages intended for users who have left the organization) from accumulating in MAIL.BOX as dead mail.

Attention: If you choose to enable this option, you need to be aware that a spammer could obtain valid e-mail addresses for users on your Domino Server. This is due in part to the verification that takes place during the initial SMTP conversation. Attempting to guess valid e-mail addresses (of common names), a spammer has the potential to harvest addresses of your users.



```
mail from:some_user@us.ibm.com
250 some_user@us.ibm.com... Sender OK
rcpt to:jack_smith@nighthawk1.lotus.com
550 jack_smith@nighthawk1.lotus.com... No such user
rcpt to:betty_smith@nighthawk1.lotus.com
550 betty_smith@nighthawk1.lotus.com... No such user
rcpt to:bob_smithly@nighthawk1.lotus.com
550 bob_smithly@nighthawk1.lotus.com... No such user
rcpt to:betty_rubble@nighthawk1.lotus.com
250 betty_rubble@nighthawk1.lotus.com... Recipient OK
rcpt to:fred_flintstone@nighthawk1.lotus.com
250 fred_flintstone@nighthawk1.lotus.com... Recipient OK
```

Figure 4-3 Example of address verification on the Domino Server

> **Note:** When this setting is enabled, the server cannot relay mail to a smart host because Domino rejects messages addressed to local domain recipients who are not listed in the Domino Directory.

– “Allow messages intended only for the following internet addresses:”

If you enter addresses in this field, only those recipients can receive Internet mail. Domino denies mail for all other recipients.

– “Deny messages intended for the following internet addresses:”

If you enter addresses in this field, all addresses except those listed in this field can receive Internet mail. Domino denies mail for only the addresses in this field.

> **Tip:** If the server supports Local Part name lookups, users whose addresses are listed in the Deny field may still receive mail addressed to alternate Internet addresses. To prevent use of alternate addresses, complete the Internet address field in each user's Person document and allow users to receive inbound mail destined for their fullname addresses only. Refer to “Specifying how Domino looks up users in the Domino Directory” in the Admin Help file for information on restricting name lookups.

The Inbound Intended Recipient Controls are used to allow or deny mail from the Internet to be routed to particular users. If you have specific users that are not allowed to receive mail from the internet, you could add their explicit Internet address (e-mail address) to the “Deny messages intended for the following internet addresses” list. Likewise for those that you will allow to receive Internet mail.

Be aware that entries found in both the Allow and Deny fields will result in the user's messages being Denied. The Deny field take precedence over the Allow field.

The use of Group names in the allow and deny fields is acceptable; however, the group name must be the actual group name and not that of the groupnames internet address. Use the actual group name as it appears in the Group view in the Domino Directory.

> **Tip:** Domino 6 has a notes.ini variable that can be used to limit the number of recipients that can be included in a single message. If the number of recipients in an incoming STMP message exceeds the number of recipients you specified for the variable `SMTPMaxForRecipients=`, the message will be rejected.
>
> Use of this variable will limit the effectiveness of directory harvesting and will also eliminate spam messages which are sent to large numbers of users within your organization.

4.2.3 Disable routing mail to groups

New in Domino 6 is the ability to stop routing mail to groups. By enabling a Notes.ini variable, `RouterDisableMailToGroups=1`, the Router will no longer route any mail addressed to a group name. If the variable is not set, the router would normally allow mail addressed to a group name to be delivered to all the members of the group. This ini variable will mostly affect messages send to groups via SMTP, although all mail addressed to groups will be blocked regardless of the origin of the message.

Mail sent to groups by Notes users will be sent, because Notes client does a group expansion before sending the message off. By the time the router gets the message, it looks like it is sent to multiple, individual recipients, not groups. However, if internal users send mail to a group with a syntax (groups@localinternetdomain.com or group@notesdomain.com) that isn't expanded by the client, these messages will be rejected. Any other clients, even authenticated, can't send mail to groups. This includes iNotes Web Access users.

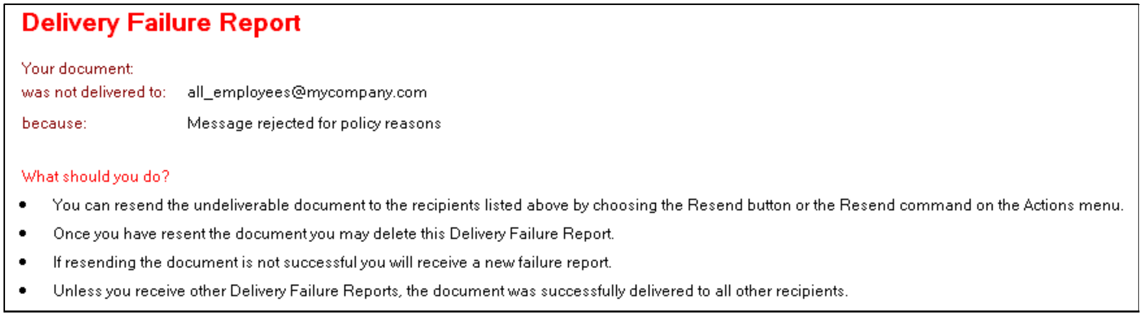
Tip: You can also restrict who can send mail to specific groups. Open the document properties of the group document and go to the Security tab. Uncheck the Use readers list of the document to determine who can send email to this group. This applies to messages sent from a Notes client as well as through SMTP. If a user who is not allowed to tries to send mail addressed to this group, they receive a non-delivery report indicating that the sender is not authorized to send mail to the specified recipient.

The following describes how group names are used normally when receiving an SMTP message addressed to a group.

A message is addressed to All_Employees@mycompany.com. The local part of the address, All_Employees, is the name of a group in my Domino Directory. This group contains a complete list of All Employees at my company.

1. A message is received via SMTP listener and deposited into MAIL.BOX.
2. The router performs a lookup to the $Users view to determine if the recipient is a valid user.
3. The recipient is found to be valid; it contains a group name.
4. The router needs to expand the group to determine who the members are who should receive this message.
5. Recipients field is added to the message, containing the members of the group (now expanded to the contents of the group).

Users or spammers attempting to send to any group name defined in your Domino Directory will now receive a delivery failure report, as shown Figure 4-4. The sender of the message will only be informed that the message was rejected for policy reasons.



Delivery Failure Report

Your document:
was not delivered to: all_employees@mycompany.com
because: Message rejected for policy reasons

What should you do?

- You can resend the undeliverable document to the recipients listed above by choosing the Resend button or the Resend command on the Actions menu.
- Once you have resent the document you may delete this Delivery Failure Report.
- If resending the document is not successful you will receive a new failure report.
- Unless you receive other Delivery Failure Reports, the document was successfully delivered to all other recipients.

Figure 4-4 Delivery failure report that is generated

4.2.4 Inbound connection controls

Inbound connection controls were introduced in Domino Release 5 and have remained unchanged in Domino 6. The inbound connection controls allow you to specify how the Domino SMTP server will handle inbound connection requests and which hosts it will allow/deny a connection to this server.

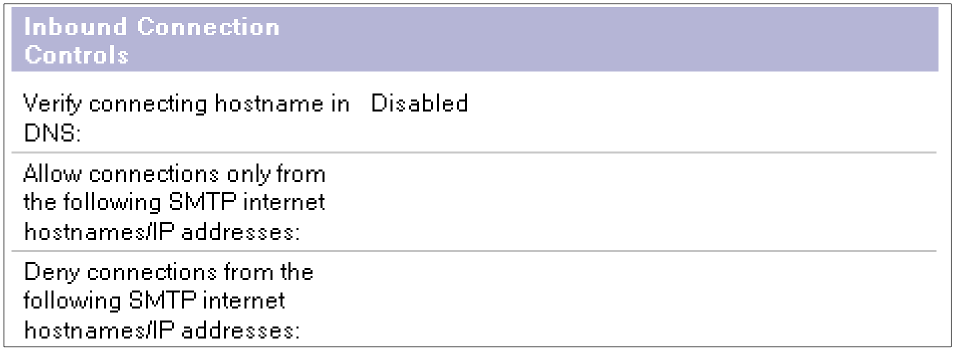
If you choose to enable “Verify connecting host name in DNS,” Domino SMTP server will attempt to verify the connecting host’s name to DNS. Domino will perform a reverse lookup to DNS that a PTR (pointer) DNS entry exists for the connecting IP address.

The remaining fields are used to specify the names or IP addresses of hosts that will be allowed/denied a connection to the Domino server. You can set “Allow connection” controls if you want to control the hosts that can be connected to this server. If the allow field contains entries, then only these hosts/IP addresses would be allowed to connect to the server. The opposite is true for the “Deny connections” field, where entries specify the hosts/IP addresses that will *not* be allowed a connection to the server.

If an entry is found in both the allow and deny fields, the address in the deny field will take precedence over the entry in the allow field.

Configuration of inbound connection controls

1. In the Administration client click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the Configurations Settings document for the server you want to administer and click Edit Configuration.
4. Click the tabs in the following order: Router/SMTP → Restrictions and Controls → SMTP Inbound Controls; navigate down to Inbound Connection Controls.
5. Double-click the document or click the Edit Server Configuration button to put the document in edit mode.



Inbound Connection Controls	
Verify connecting hostname in DNS:	Disabled
Allow connections only from the following SMTP internet hostnames/IP addresses:	
Deny connections from the following SMTP internet hostnames/IP addresses:	

Figure 4-5 Inbound connection controls

6. Make the desired changes to the Inbound Connection Controls and click Save & Close.

Enabling “Verify connecting hostname in DNS” will result in increased connection times. When enabled, Domino will attempt to find a PTR record in DNS for each host that attempts to establish a connection with Domino. If no PTR record is located in DNS, the connection will be denied. Be aware that PTR records are *not* a required DNS record. Domino potentially could reject connections from valid hosts with this feature enabled.

Using the “Allow connections only from...” or “Deny connections from the following SMTP internet hostnames/IP addresses” fields can be used to control the hosts that are allowed or denied a connection to this Domino server via SMTP. Hostnames and IP addresses are allowed in these fields. If you choose to use IP addresses, be sure to enter them in brackets, for example: [192.168.10.17].

Entering hostnames or IP addresses in the “Allow connections only from the following SMTP internet hostnames/IP addresses:” field will allow *only* these hosts to connect to the Domino server. All other hosts are denied.

For example, if abc.com was entered in the Allow field, only hosts belonging to the abc.com domain would be allowed to connect to the Domino server.

If you enter a hostname/IP address in both the Allow and Deny fields, the Deny entries will take precedence over the Allow entries.

4.2.5 Inbound sender controls

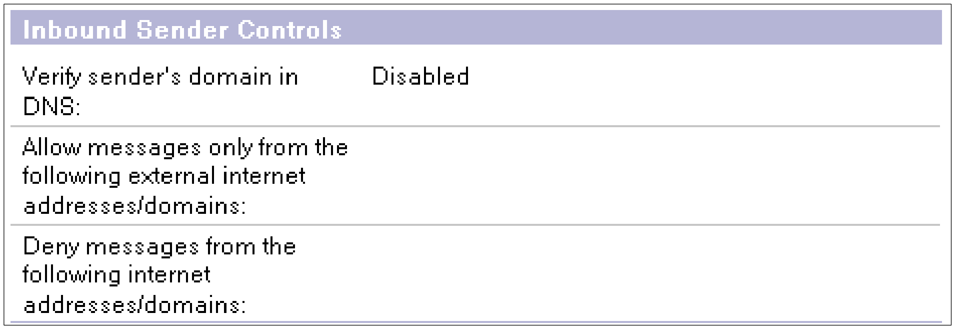
Inbound sender controls were introduced in Domino Release 5 and have remained unchanged in Domino 6. The inbound sender controls allow you to specify how the Domino SMTP server will process connections based on the sender address.

“Verify sender’s domain in DNS,” when enabled, instructs the Domino SMTP server to verify the sender address (using the contents of the MAIL FROM field in the message header) to confirm that the sender’s domain name actually exists. Domino will attempt to verify the address in DNS (searching for an MX or A record) and if found, will accept the message from the sender. If the sender’s domain name can not be located, Domino will reject messages from this host.

The “Allow messages only from...” and “Deny messages from the following internet addresses/domains” settings work very similar to most of the other Allow/Deny fields. These will allow you to specify the names/addresses of the external hosts that you will accept or reject mail from.

Configuration of inbound sender controls

1. In the Administration client click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the Configurations Settings document for the server you want to administer and click Edit Configuration.
4. Click the tabs in the following order: Router/SMTP → Restrictions and Controls → SMTP Inbound Controls; navigate down to Inbound Sender Controls.
5. Double-click the document or click the Edit Server Configuration button to put the document in edit mode.



Inbound Sender Controls

Verify sender's domain in DNS:	Disabled
Allow messages only from the following external internet addresses/domains:	
Deny messages from the following internet addresses/domains:	

Figure 4-6 Inbound sender controls

6. Make the desired changes to the Inbound Sender Controls and click Save & Close.

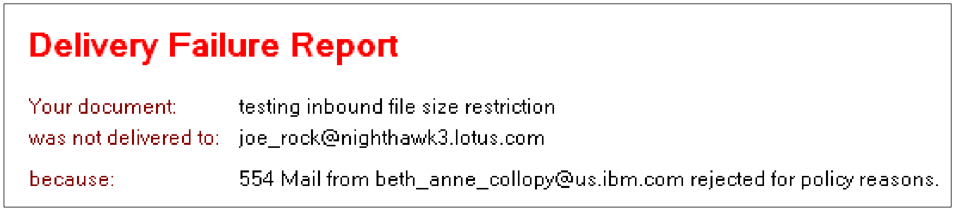
You can stop mail from entering your environment by using the Deny messages from the following internet addresses/domains field. If your company has domain names that it will *not* accept mail from, you could add these domain names here.

You can also deny mail from certain individuals by adding their explicit internet address to the Deny field. If you want only specific users to send mail into your server, you could utilize the "Allow messages only from the following internet addresses/domains" field.

Allowing or denying addresses using the inbound sender controls works very similarly to using Server Mail rules. To determine which method is best for your environment, consider the following differences:

- If you deny messages from certain Internet addresses or domains using the inbound sender controls, the sending server will receive a 554 SMTP response and will not be allowed to transfer the message. The message is never accepted by the Domino server, nor is it written to mail.box.

  The delivery failure report that's generated when a message is denied using inbound sender controls is shown in Figure 4-7. Notice the failure reason provides an SMTP Reply code, 554 along with the reason for the failure, "Mail from <E-mail address> rejected for policy reasons."



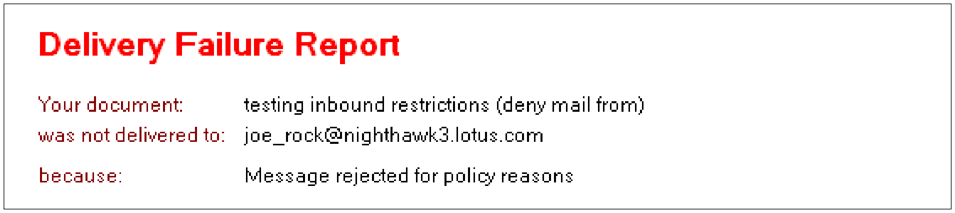
Delivery Failure Report

Your document: testing inbound file size restriction
was not delivered to: joe_rock@nighthawk3.lotus.com

because: 554 Mail from beth_anne_collopy@us.ibm.com rejected for policy reasons.

Figure 4-7 Delivery Failure Report with 554 SMTP response code

- If you deny messages from certain Internet addresses or domains using a server mail rule, (with the don't deliver message action), as the administrator, you can choose either to send an NDR (Non-Delivery Report) or to silently delete the message. The delivery failure report in Figure 4-8 was generated using a server mail rule. Notice that the reason for failure only indicates "Message rejected for policy reasons," but does not make note of the sender's address.



Delivery Failure Report

Your document: testing inbound restrictions (deny mail from)
was not delivered to: joe_rock@nighthawk3.lotus.com

because: Message rejected for policy reasons

Figure 4-8 Delivery Failure Report for messages denied using a Server rule

As you can see from the two delivery failure reports, messages failed using the inbound sender controls provided more detail to the sender regarding why the message was failed. Either method of denial will work with a sender's internet address; the method you choose is up to you.

Tip: We recommend that you block mail from unwanted sender addresses and domains by using inbound sender controls instead of server mail rules. They will perform better and will prevent any data from being transferred at all in many cases.

4.3 Controlling delivery of spam

Not all spam can be stopped on the Listener before it is placed in the mail.box. Domino 6 Server offers tools to further control the delivery of mail messages in your Domino environment. You can control which messages are delivered to end-user's mail files.

4.3.1 Server mail rules

Server mail rules allow you centrally control the messages that are routed into your environment. After a message is placed into a mail.box by the SMTP server, server mail rules are applied by the router before delivering messages any further. It is most powerful to deny messages from know spam sources by using inbound sender controls, since then the messages are stopped at the listener. The power of the server mail rules lies in the possibility of using different conditions and factors against which the messages should be checked. You configure server mail rules to prevent spam messages from ever reaching your end-users.

Enabling server mail rules should be thoroughly planned prior to implementation. Each rule that is created will act on messages received by the server. Server mail rules will affect *all* messages sent to the server, including messages sent from a

Notes client and messages received from other Domino servers, as well as those from the Internet.

Server mail rules are configured and stored on the server configuration document in the Domino directory. Server mail rules will be registered as monitors for all MAIL.BOX files in use on the server.

Server mail rules can use the message header, the body of the message, or even the form which a mail message is using to determine whether to act on it. The combination of conditions and actions is large; this offers you absolute control over which messages are delivered in your environment. With these rules you can filter out known spam senders, messages that contain questionable content, or even prevent your own users from sending out a message to a large number of recipients.

Enabling and implementing server mail rules can have a performance impact on your server, but if spam is a major problem in your organization, benefits will outweigh the costs.

Configuration of server mail rules

1. In the Administration client, click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the configuration settings document for the server you want to administer and click Edit Configuration.
4. Click the tabs in the following order: Router/SMTP → Restrictions and Controls → Rules.

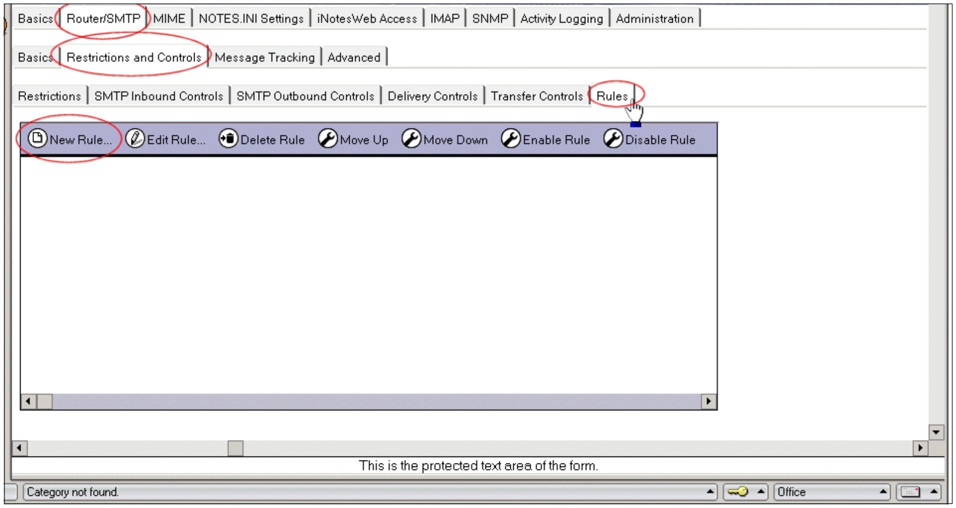
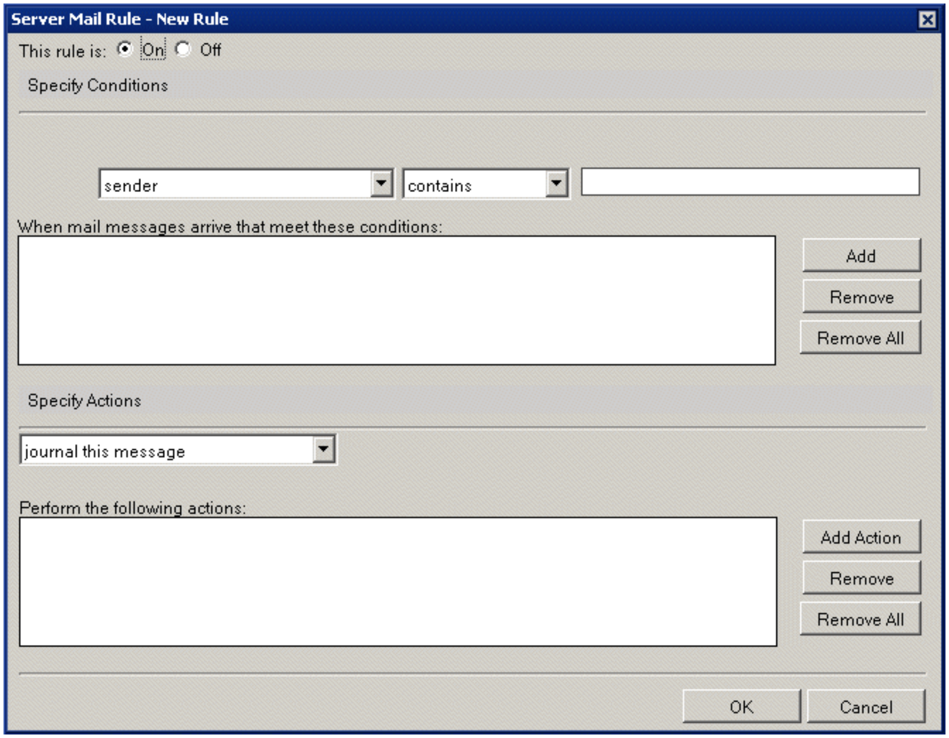


Figure 4-9   Where to set up server mail rules

5. Double-click the document or click the Edit Server Configuration button to put the document into edit mode.
6. Click New Rule to create a new rule document.



Server Mail Rule - New Rule

This rule is: ● On ○ Off

Specify Conditions

sender | contains

When mail messages arrive that meet these conditions:

Specify Actions

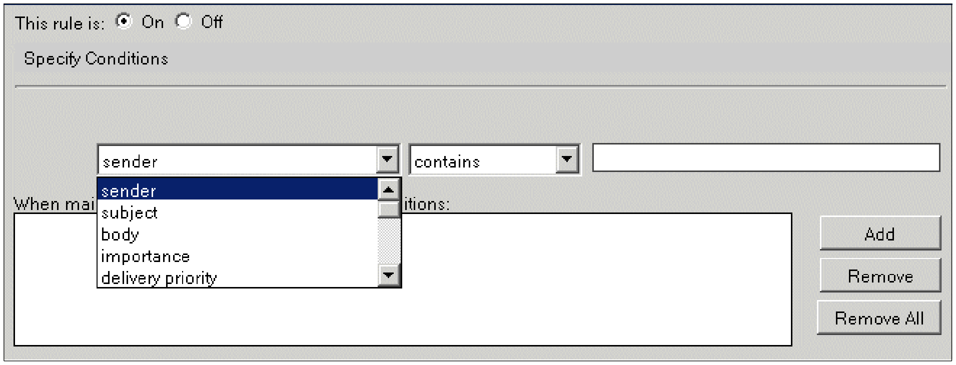
journal this message

Perform the following actions:

Figure 4-10 New server mail rule

7. Note that the default setting is for this rule to be turned on once you save it.
8. In the Conditions section of the new server mail rule, specify the ways of identifying the mail that you want the rule to act upon.
   a. First choose a field for the rule to look at:
      - Sender
      - Subject
      - Body
      - Importance
      - Delivery priority
      - To
      - CC
      - BCC
      - To or CC
      - Body or subject
      - Internet domain
      - Size (in bytes)
      - All documents

- Any attachment name
- Number of attachments
- Form
- Recipient count
- Any recipient



This rule is: ● On ○ Off

Specify Conditions

sender | contains

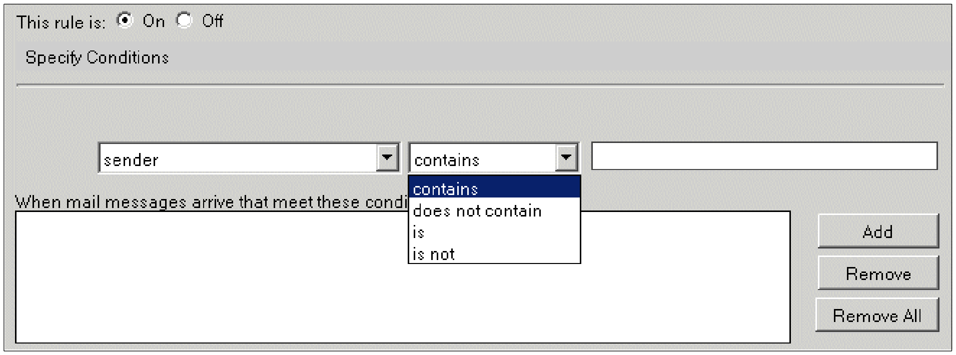
sender
subject
body
importance
delivery priority

When mai itions:

Figure 4-11 Choose the field to be examined by the rule

b. Each field can be tested for the following conditions:

- contains / does not contain
- is / is not



This rule is: ● On ○ Off

Specify Conditions

sender | contains

contains
does not contain
is
is not

When mail messages arrive that meet these condi

Figure 4-12 Specify the criteria for the field

c. Fields with numeric logic can be tested for the following conditions:

- is less than / is greater than
- is / is not

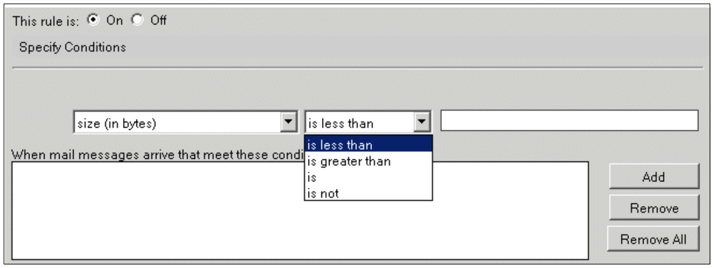
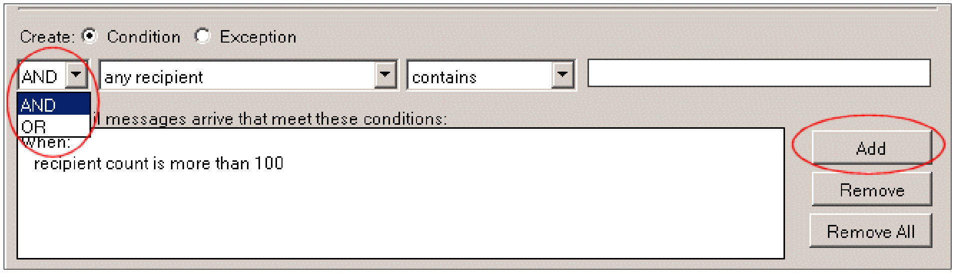


Figure 4-13 Numeric test

9. Click the Add button to enter the condition into the rule. Note that you can add more conditions and that they will be related to the previous condition in one of two ways: AND / OR.


Create: ● Condition ○ Exception
AND
any recipient
contains
AND
OR
l messages arrive that meet these conditions:
Add
Remove
Remove All

When:
recipient count is more than 100

Figure 4-14 Add the condition

10. Move to the Specify Actions section of the Server Mail Rule dialog box. There are five possible actions; only one action per rule can be selected.

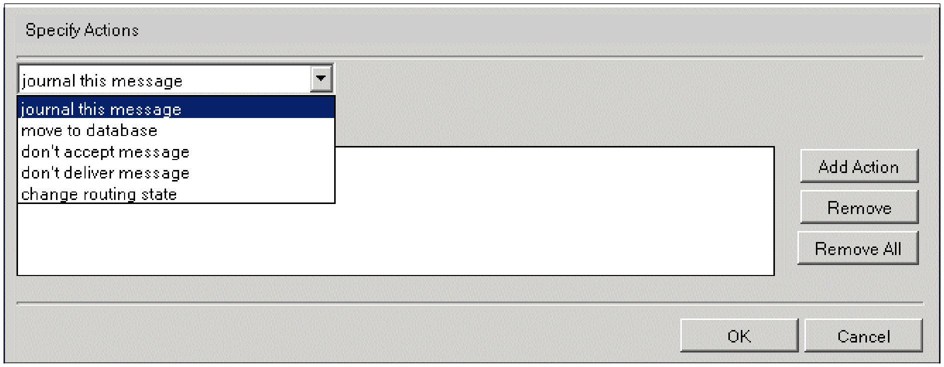
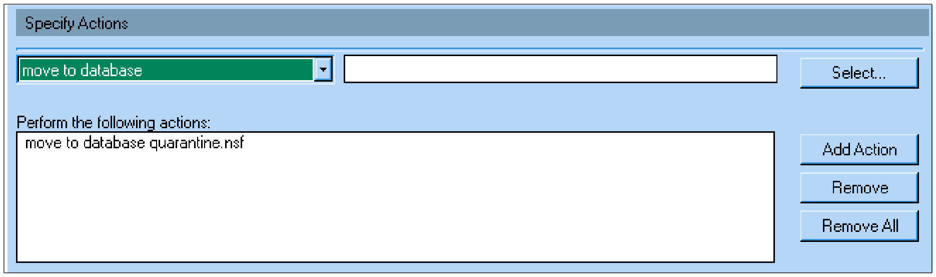


Figure 4-15 Specify action

- **journal this message**
  This is used in conjunction with mail journaling. For more details on mail

journaling, see the redbook *Upgrading to Notes and Domino 6*, SG24-6889, and the Domino 6 Administrator Help.

– **move to database**
You can create a graveyard or quarantine database for suspicious messages. Be sure to specify the server on which you are creating the rules prior to selecting the database. The router assumes a relative path from the data directory of the server.


Specify Actions

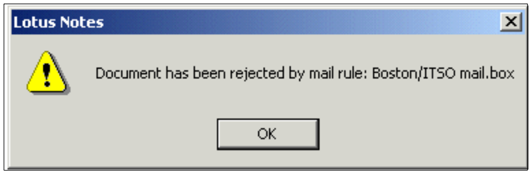
move to database

Perform the following actions:
move to database quarantine.nsf

Figure 4-16 Move to database

Tip: Use the normal mail template (mail6.ntf) or the mail journaling template (mailjrn.ntf) to create a quarantine database.

– **don't accept message**
An internal Notes sender receives an immediate dialog box that the message has been rejected. The message never leaves the user's mail file. For an SMTP message the router informs the connecting SMTP system that it will not accept the message.


Lotus Notes

Document has been rejected by mail rule: Boston/ITSO mail.box

Figure 4-17 Immediate rejection notice

– **don't deliver message**
For an incoming SMTP message the Domino Server informs the connecting SMTP system that it will not accept the message.

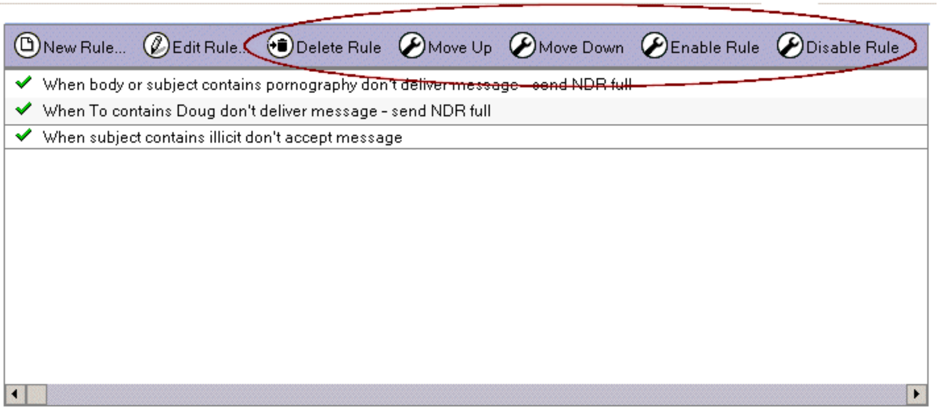
An internal Notes sender receives an immediate dialog box that the message has been rejected. The message never leaves the user's mail file.

- **change routing state**
  Domino accepts the message but its routing state in mail.box is changed to held.

11. Once you have finished creating the rule click OK to close the New Rule dialog box.
12. Click Save & Close to save the server configuration document. The rule will not be recognized until the server configuration document has been saved and the router has recognized the new rules.

> **Tip:** You can force the router to read the new rules by entering this command at the console:
>
> ```
> set rules
> ```
>
> The router will respond with the number of system filters it has recognized.

13. You can manage the server rules with the buttons on the Rules tab of the server configuration document, as shown in Figure 4-18. You can delete, prioritize, enable, and disable the server mail rules.



✓ When body or subject contains pornography don't deliver message - send NDR full
✓ When To contains Doug don't deliver message - send NDR full
✓ When subject contains illicit don't accept message

Figure 4-18 Manage server mail rules

Usually, server mail rules are created to isolate or deny certain types of messages from reaching your end users. Messages containing offensive material are a good reason to implement a server mail rule. These messages could be moved to a database for further analysis or they could even be deleted and never seen by your end users. Messages containing an inordinate number of recipients or attachments can be moved to a database or held in mail.box pending further analysis.

Table 4-2 outlines various types of rules and provides suggestions on the action to take on these messages. Initially, you may want to use the “Move to Database” or “Change Routing State” actions more frequently than the “Don’t accept message” or the “Don’t deliver message”. There is no way to recover messages that were rejected using “Don’t accept message” or deleted using “Don’t deliver message” actions.

Table 4-2 Examples of Server Mail Rules

Rule conditions to meet	**Action to perform when met**
When any attachment name contains *name of attachment* or *extension type*	Move to database quarantine.nsf, or change routing state to mark as held
When Internet domain contains *name of domain*	Move to database quarantine.nsf, don’t accept message, or change routing state to mark as held
When recipient count is greater than *number of recipients*	Move to database quarantine.nsf or change routing state to mark as held
When subject contains dvd OR subject contains money OR subject contains tv OR subject contains music OR subject contains cd OR subject contains credit OR subject contains phone OR subject contains movie Except when: Subject does not contain free	Move to database quarantine.nsf, don’t accept message, or change routing state to mark as held
When subject contains XXX AND subject contains child OR subject contains XXX AND subject contains adult OR body contains XXX AND body contains child OR body contains XXX AND body contains adult OR subject contains XXX AND body contains child OR subject contains XXX AND body contains adult OR body contains XXX AND subject contains child OR body contains XXX AND subject contains adult	Move to database quarantine.nsf, don’t accept message, or change routing state to mark as held
When number of attachments is greater than *number of attachments*	Move to database quarantine.nsf or change routing state to mark as held
When To contains *recipient address 1* OR To contains *recipient address 2*	Move to database quarantine.nsf or change routing state to mark as held
When Sender contains *spammer name1* OR Sender contains *spammer name2*	Move to database quarantine.nsf or don’t accept message. Inbound sender controls could be used for this, denying mail from these senders.

Most of the server rules in the table contain simple evaluations and simple actions. When creating rules, keep the evaluation conditions simple. Rules will be executed on messages that meet the criteria specified including Notes messages sent to another Notes user, not just SMTP messages.

Be aware of the performance implications that could be imposed on your server when using rules. Rules should be monitored frequently when first implemented. You may need to refine the conditions or change the action performed on messages. Using the “Move to Database” action, you can further examine the contents of the messages acted upon and refine rules, as needed.

4.4 Controlling use of your server as a relay

Spammers try to distribute their spam messages to as large an audience as possible, and they try to cover their tracks by any means. One of their methods is relaying mail through third party servers to disguise the origin of the messages. The third party server hardly ever has anything to do with the message content.

Your server may end up on a DNS Blacklist through no direct fault of your system. This can happen if you have a relay open (you allow anyone relaying mail off your server) and a spammer has used your server for relaying spam messages.

You need to close your relay and control who can relay mail off your server. This section describes how you can to do it.

4.4.1 Inbound relay controls

Inbound relay controls provide settings to control which servers can use your server as a relay, and the destinations you’ll allow mail hosts to relay messages to.

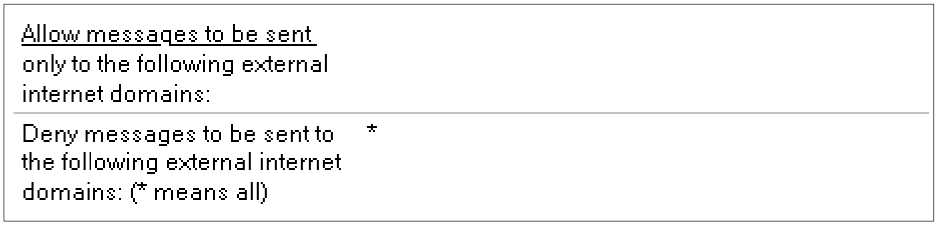
The inbound relay controls settings are where relay restrictions for your Domino SMTP Server are set. When you initially set up your Domino R5 Server, no relay restrictions are applied. All hosts are allowed to relay off this server and all destinations will be allowed to be relayed to. Notice that this has been changed in Domino 6: when you set up you Domino 6 Server, relaying is denied by default.

Using Allow and Deny destination lists, these controls determine the relay destinations to which a server can or cannot send mail and the sources from which the server can and cannot accept relays.

The wording of the field names tends to cause confusion in what setting is for what functionality. There are four fields on the server configuration document dealing specifically with the inbound relay controls.

You will find the inbound relay controls on the server configuration document. Select Router/SMTP → Restrictions and Controls → SMTP Inbound Controls.

These two fields shown in Figure 4-19 determine the names of the hosts that this Domino Server will relay mail to (Destination).



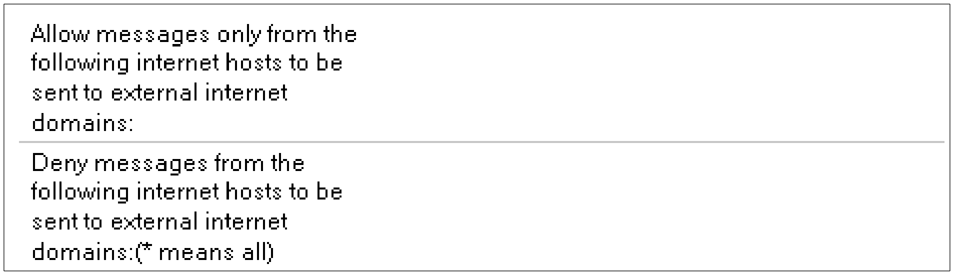
Allow messages to be sent only to the following external internet domains:	
Deny messages to be sent to the following external internet domains: (* means all)	*

Figure 4-19 Inbound relay controls (Destination host settings)

These fields are used to explicitly enter the name of those hosts that you want this server to relay to, or those that you specifically want to prohibit. When an entry is placed in the Allow field, only the hosts listed in this field will be allowed to be relayed to, all others will be denied. When you place an entry in the deny field, only those domains listed will be denied, all other domains are allowed. If entries exist in both the allow and the deny fields, the entries in the Deny field will take precedence over the same entries in the Allow field.

Important: Because you configure the valid relay *destinations* separately from the valid relay *sources*, conflicts between the two sets of restrictions can occur. When such conflicts occur, Lotus Domino requires instructions for resolving the conflict. In Lotus Domino 5, Deny entries took precedence over Allow entries; in Lotus Domino 6, Allow entries take precedence over Deny entries.

The next two fields deal with the connecting hosts (Source). These are used to specify the hosts that this Domino server will relay mail for.



Allow messages only from the following internet hosts to be sent to external internet domains:	
Deny messages from the following internet hosts to be sent to external internet domains:(* means all)	

Figure 4-20 Inbound relay controls (Source Host settings)

You may find that you have certain hosts that are allowed to relay off this Domino server. You could then add these hosts (name or IP address) to the “Allow messages only from the following internet hosts to be sent to external internet domains” field. Only hosts that are explicitly added to the Allow field will be able to use this server as a relay.

Internal hosts (those within the same Internet domain) are exempt from relay checking by default. Any host determined to be part of your local internet domain will be allowed to relay off this Domino server, regardless of the setting described.

In Domino Release 5, in order to restrict internal as well as external hosts from relaying, you would need to set the notes.ini variable `SMTPAllHostsExternal=1`. This variable treated all connecting hosts as external hosts and all hosts were subject to relay checking. This allowed Administrators to close down the relay capability within Domino for all hosts, including internal hosts. If it was determined that an internal host needed to relay though the Domino server, this host could be placed in the “Allow messages only from the following internet domain to be routed to external internet domains” field.

Conflicts between the destination and source restrictions

Domino 6 handles the conflict that can occur between the destination and source fields differently than R5 did. In Lotus Domino 5, Deny entries took precedence over Allow entries; in Lotus Domino 6, Allow entries take precedence over Deny entries.

For example, let’s say that you allow relays from the following host and deny them to the following domain:

```
Allow from hosts: 9.95.91.51
Deny to domains:  yahoo.com
```

On a Domino 5 server, because the Deny entry takes precedence, the named host, 9.95.91.51, cannot relay to denied destinations. In the example, the Domino 5 server cannot relay to any address in the yahoo.com domain.

On a Domino 6 server, in the event of a conflict between entries, Allow entries take precedence. By giving a specific host “Allow” access, you allow that host to relay to any destination. In the example, the host 9.95.91.51 can relay to the yahoo.com domain even though the domain is explicitly denied as a relay destination.

Similarly, the following configuration denies relays from a specified host and allows them to a specified domain:

```
Deny from hosts:  myhost.iris.com
Allow to domains:  hotmail.com
```

On a Domino 5 server, the Deny entry takes precedence, so that the named host, myhost.iris.com, is not a valid relay source. The named host cannot relay to any domain, even to allowed domains.

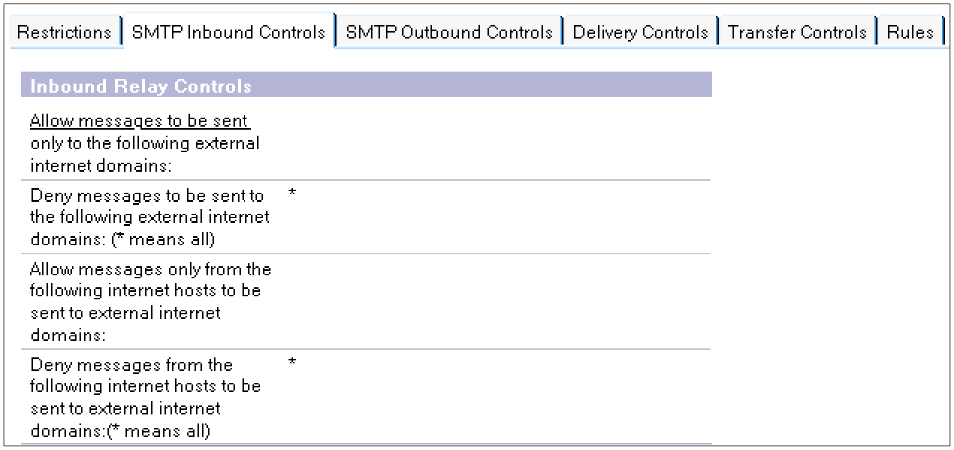
On a Domino 6 server, the Allow entry takes precedence. In the preceding example, myhost.iris.com is allowed to relay to hotmail.com, but not to any other destination.

> **Tip:** When you upgrade a Domino 5 SMTP mail server, you have the option to *not* accept this change if you do not want to reconfigure your upgraded mail servers. Lotus Domino 6 provides the NOTES.INI setting `SMTPRelayAllowHostsandDomains` to allow the server to follow the Domino 5 behavior. Set this value to 1 to allow the Deny entries to take precedence. The default value for this setting is 0.
>
> ```
> SMTPRelayAllowHostsandDomains=1
> ```

Enhancements to Domino 6, specifically the inbound relay enforcements, can further restrict the relay capabilities of internal host. More information regarding these enhancements can be found in 4.4.2, “Inbound relay enforcement” on page 59.

Configuration of inbound relay controls

1. In the Administration client click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the configurations settings document for the server you want to administer and click Edit Configuration.
4. Click the tabs in the following order: Router/SMTP → Restrictions and Controls → SMTP Inbound Controls; navigate down to Inbound Relay Controls.
5. Double-click the document or click the Edit Server Configuration button to put the document in edit mode.



Inbound Relay Controls

Allow messages to be sent only to the following external internet domains:	
Deny messages to be sent to the following external internet domains: (* means all)	*
Allow messages only from the following internet hosts to be sent to external internet domains:	
Deny messages from the following internet hosts to be sent to external internet domains:(* means all)	*

Figure 4-21 Inbound relay controls

6. Make the desired changes to the inbound relay control fields and click Save & Close.

The server configuration document in Figure 4-21 depicts a server that does not allow any relaying to occur. By specifying an asterisk (*) in either or both of the Deny fields, Domino will not relay any mail for external hosts and will not allow any users to use this server as a relay.

If you find that your domain is being reported as an open relay, you would want to close down the capability. The settings shown are the correct representation of a closed relay.

The following two tables show the results of some sample inbound relay configurations, and some that should be avoided.

Table 4-3 Sample inbound relay configurations

Allow to	Deny to	Allow from	Deny from	Result of inbound relay setting
	*			No hosts will be allowed to relay mail through the Domino server
	*	abc.com		abc.com can relay to any destination. All other hosts will not be allowed to relay any mail
xyz.com			*	All hosts will be allowed to relay messages to xyz.com, but not to any other domain.

Table 4-4 Avoid these inbound relay configurations

Allow to	Deny to	Allow from	Deny from	Result of inbound relay setting
	xyz.com		abc.com	All hosts, except abc.com can relay mail to any destination. abc.com can relay to any destination, except xyz.com.
	xyz.com		*	All hosts can relay mail to any destination except xyz.com
	xyz.com	abc.com		All hosts can relay mail to any destination.
	*		abc.com	All hosts, except abc.com, can relay mail to any destination
xyz.com			abc.com	All hosts, except abc.com, can relay mail to any host. abc.com can relay mail to xyz.com

4.4.2 Inbound relay enforcement

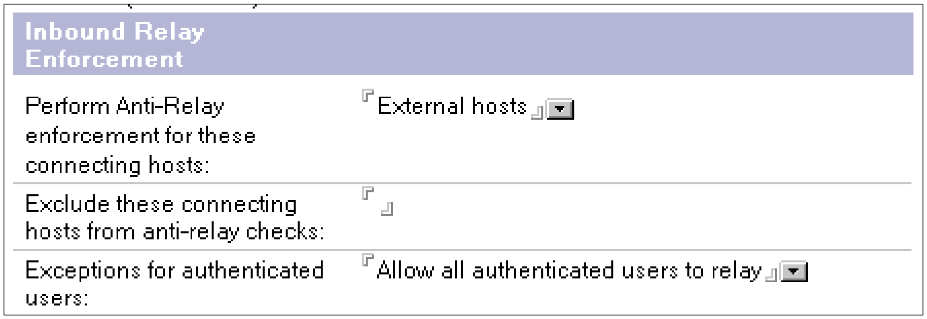
New to Domino 6 are the inbound relay enforcement configurations. These options allow tighter control over the hosts that are allowed to relay off your Domino server. You can choose whether the Domino server performs relay checking for all hosts, external hosts only, or disable relay checking all together.

Enabling anti-relay enforcement allows you to further exclude certain hosts from being checked against your inbound relay controls options. You could choose to perform checking on all hosts and yet, exclude certain hosts (whether external or internal) from being checked by explicitly entering these hostnames or IP addresses in the “Exclude these connecting hosts from anti-relay checks.” Domino 6 enables “Anti-relay enforcement checking for all External Hosts” by default. If you choose not to make adjustments to the default settings, you can rest assured that your server will perform inbound relay checking for external hosts.

Using the “Exceptions for authenticated users” field, you can choose to allow or deny your POP or IMAP users to relay. This new field allows authenticated users to use the Domino server as a relay for messages to the Internet. POP or IMAP users have to configure their mail client to authenticate again with Domino SMTP Server. Name and password authentication must be enabled on the Domino Server. After the SMTP Listener task determines the user has been authenticated, it treats the connection as if it originated from a local user and exempts it from inbound relay controls. This is especially helpful when a POP or IMAP user accesses the Domino server by way of an Internet Service Provider. Domino would normally treat this inbound connection as a remote connection, perform anti-relay checks, and fail the relay attempt due to the address not being recognized as local.

Configuration of inbound relay enforcement

1. In the Administration client click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the configurations settings document for the server you want to administer and click Edit Configuration.
4. Click the tabs in the following order: Router/SMTP → Restrictions and Controls → SMTP Inbound Controls; navigate down to Inbound Relay Enforcement.
5. Double-click the document or click the Edit Server Configuration button to put the document in edit mode.



Inbound Relay Enforcement

Perform Anti-Relay enforcement for these connecting hosts:	External hosts
Exclude these connecting hosts from anti-relay checks:	
Exceptions for authenticated users:	Allow all authenticated users to relay

Figure 4-22 Inbound relay enforcement configuration

6. Make the desired changes to the inbound relay enforcement fields and click Save & Close.

This section has 3 fields:

- "Perform Anti-Relay enforcement for these connecting hosts:"

  Specifies the connections for which the server enforces the inbound relay controls. Choose one:

  – *External hosts (default)* - The server applies the inbound relay controls only to hosts that connect to it from outside the local Internet domain. Hosts in the local Internet domain are exempt from anti-relay restrictions. The local Internet domain is defined by either a Global Domain document, if one exists, or as the Internet domain of the host server.

  – *All connecting hosts* - The server applies the inbound relay controls to all hosts attempting to relay mail to external Internet domains.

  – *None* - The server ignores the settings in the inbound relay controls. All hosts can always relay.

By default the inbound relay controls are enabled for external hosts. If the connecting host's IP address resolves to a name in one of the local Internet domains, the host is considered internal. IP addresses that resolve to host names outside the local Internet domains or that do not have DNS entries are considered external. You can change this so that all or no hosts are subject to the inbound relay controls.

- "Exceptions for authenticated users:"

  Specifies whether users who supply login credentials when connecting to the server are exempt from enforcement of the inbound relay controls. Choose one:

  – *Perform anti-relay checks for authenticated users* - The server does not allow exceptions for authenticated users. Authenticated users are subject to the same enforcement as non-authenticated users.

  – *Allow all authenticated users to relay* - Users who log in with a valid name and password are exempt from the applicable inbound relay controls. Use this to enable relaying by POP3 or IMAP users who connect to the network from ISP accounts outside the local Internet domain.

  This field provides an exception mechanism so that POP3 and IMAP users will be able to send internet e-mail through this server.

- "Exclude these connecting hosts from anti-relay checks:"

  You create an exceptions list containing the IP addresses or host names of hosts that relay to any permitted domain. For each specified exception, the inbound relay controls will not be enforced. Enter the IP addresses or host names of hosts to be exempted from the restrictions specified in the Inbound relay controls section.

  – Enter IP addresses or host names of specific servers that should be able to relay messages through this server.

  – IP addresses are entered in brackets. Wildcards can be used to indicate all addresses in one subnet. Also ranges of addresses can be specified.

  ```
  [156.16.25.1]
  [156.16.25.*]
  [156.16.25.128-255]
  apps1.lotus.com
  ```

  Note: You can use wildcards to represent an entire subnet address, but not to represent values in a range. For example, [127.*.0.1] is valid; [123.123.12-*.123] is not. If you want to specify a range, you can do it by entering, for example [127.0.0.128-255].

  – Set the previous field to "All connecting hosts" and enter IP addresses or host names of internal servers that are allowed to relay in order to prevent unauthorized use of your SMTP servers by internal departments.

4.5 Protecting your Domino server from active address harvesting attacks

In this section we introduce some of the active address harvesting attack types that spammers use to obtain email addresses, and we give recommendations and instructions on how you can protect your Domino 6 server from these attacks.

4.5.1 SMTP harvesting attacks

The most insidious types of attacks can occur when spammers attempt to use your SMTP mail server's directory against you. Spammers may use a “name” dictionary to send random name combinations as recipients of SMTP mail to your mail server. They then harvest responses to these “dictionary” mailings to build a list of valid e-mail addresses that can be sold or targeted for more spam in the future.

For example, in its default setting, the Domino SMTP task attempts to return mail that is undeliverable to the sender with a delivery failure message. When Domino operates in this mode, the spammer can use returned information to “cleanse” their dictionary of bad addresses by tracking subject, sender, and recipient information. Addresses for which the spammer receives non-delivery reports can be removed from their spamming list; other addresses are maintained as valid spam targets. This is called an SMTP Harvesting attack.

4.5.2 Spam mail bombing

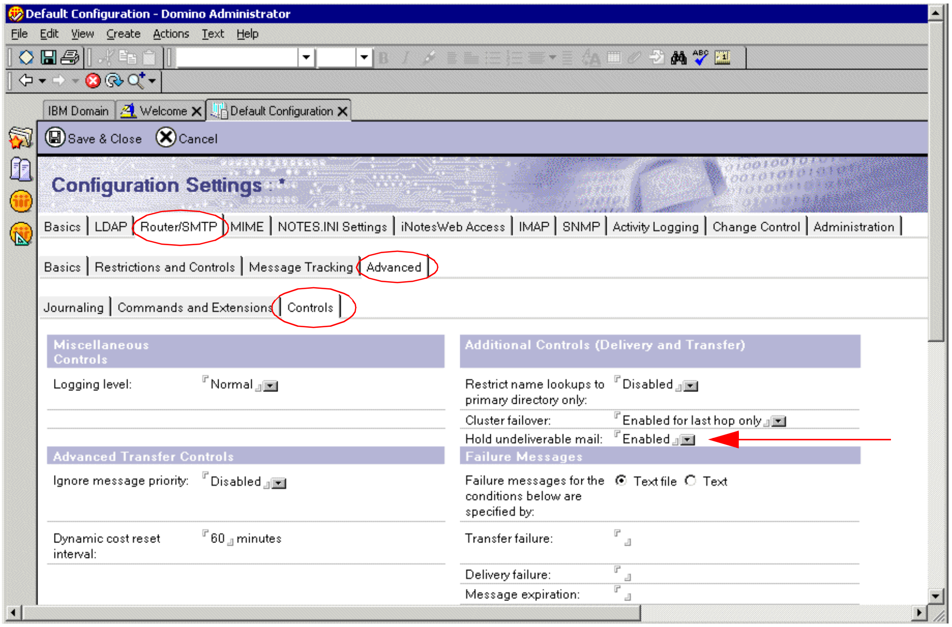
In many cases the spammer is merely hoping that their e-mail address dictionary will happen to have some valid addresses. In this case the spammer does not usually provide valid return delivery information. This type of attack is known as spam mail bombing. It represents a Denial of Service (DoS) attack because it keeps your Domino SMTP server busy handling invalid e-mail addresses. Indeed, this type of DoS attack consumes CPU and disk space as well, since invalid e-mail that cannot be returned by Domino is marked as DEAD mail and accumulates in the mail.box file.

4.5.3 Direct SMTP RCPT TO harvesting

Another variation of a harvesting attack occurs when a connecting e-mail sender tests the response of the SMTP server to the “RCPT TO” command. Spammers can use this automated technique to very quickly test thousands of addresses without sending any e-mail. Spammers test the SMTP server response to the RCPT TO command and when the response is “positive” for a good address, the spammer marks the e-mail address as a valid target for spam. This type of attack simulates the transmission of an e-mail with a large list of recipients. This harvesting technique is especially effective for spammers when you configure Domino 6 to validate recipient addresses during transport by enabling the “Verify that Local Domain Recipients exist in the Domino Directory” setting in Inbound Intended Recipient Controls. For this reason, we *do not* recommend enabling this setting since it can assist spammers in targeting your domain for spam. However, if you must use the setting, you can reduce the effectiveness of this type of address harvesting by using the Domino 6 ini setting `SMTPMaxForRecipients`. The SMTPMaxForRecipients setting will not stop harvesting, but may slow it down or reduce it. The intention of the SMTPMaxForRecipients ini setting is to prevent messages with large lists of recipients, but it has the useful side effect of making it a little more difficult for spammers to harvest addresses.

4.5.4 Defending against active attacks

We recommend that you configure Domino to hold undeliverable mail. This can be done from the Configuration Settings document, under Router/SMTP → Advanced → Controls. Change the value of the field “Hold undeliverable mail” to Enabled. The field is located in the Additional Controls (Delivery and Transfer) section shown in Figure 4-23.


Default Configuration - Domino Administrator
File Edit View Create Actions Text Help
IBM Domain
Welcome
Default Configuration
Save & Close
Cancel
Configuration Settings
Basics | LDAP | Router/SMTP | MIME | NOTES.INI Settings | iNotes Web Access | IMAP | SNMP | Activity Logging | Change Control | Administration
Basics | Restrictions and Controls | Message Tracking | Advanced
Journaling | Commands and Extensions | Controls

Miscellaneous Controls

Logging level: Normal

Advanced Transfer Controls

Ignore message priority: Disabled

Dynamic cost reset interval: 60 minutes

Additional Controls (Delivery and Transfer)

Restrict name lookups to primary directory only: Disabled

Cluster failover: Enabled for last hop only

Hold undeliverable mail: Enabled

Failure Messages

Failure messages for the conditions below are specified by: ● Text file ○ Text

Transfer failure:

Delivery failure:

Message expiration:

Figure 4-23 Undeliverable mail setting

When the Domino SMTP task operates in this mode, undeliverable mail is always held in the mail.box file. This setting prevents spammers from gleaning valid addresses, by process of elimination, from all the returned non-delivery reports. However, the undelivered messages can still accumulate in the mail.box file.

Note: In both types of attacks (Harvesting or DoS) it is likely that the attack will create a substantial load on your mail server with errant spam mail messages (in either HELD or DEAD state), so you should monitor your mail.box closely. We recommend building a new view in mail.box that isolates mail with the following select formula:

```
SELECT RoutingState = "HOLD":"DEAD" & @Contains(FailureReason;"not listed in
public")
```

and a column that displays the field “IntendedRecipient.” If this new view contains more than a few messages where the IntendedRecipient is an invalid address in your domain, then you may have been (or may still be!) the target of an e-mail harvesting attack.

By studying the content of these messages you can adjust your Inbound Connection controls to defend against such attacks. Look carefully at the Received fields in the problem messages. If the messages appear to come from the same IP address or range of IP addresses, you may want to deny connections from those particular IP address. However, you should be aware that spammers often roam the internet looking for open relay servers from which to send their spam, so the IP connections that you observe in the messages may not show a pattern. Also, even though you may use a DSN Blacklist service, the lists can lag behind as new open relays open up all the time.

Even with these anti-spam measures in place, it is always a good idea to monitor your mail.box for dead and held messages. Typically these messages are just spam junk and can be deleted, but occasionally you may see a true addressing error: a slight misspelling of a true recipient in your mail system, for example.

We think the best combination is to use the “Hold undeliverable mail” setting combined with active monitoring of mail.box for repeat offending IP addresses. When you use “Hold undeliverable mail,” Domino always accepts mail, preventing all types of active harvesting. Active monitoring of mail.box is required to prevent the negative impact of spam mail bombing and the accumulation of large amounts of bogus undeliverable spam mail.

5

Using mail file rules to prevent spam

This chapter describes actions that can be taken by the end user to further address the spam problem.

As an administrator, you can enable many anti-spam features at the Domino 6 server, and that’s where stopping spam is most effective. If the spam messages reach the end user’s mail file, part of the damage is already done. However, given that server-based anti-spam measures must address broader spam indicators, not all spam can be blocked at the server. Your end users can build anti-spam mail file rules that are much more specific and aggressive.

Building anti-spam mail file rules should be seen as an additional measure in the overall solution to the spam problem. Mail file rules are enforced on the Domino server, so they do use some server processing power. Having a large number of mail file rules, especially rules that scan the body of e-mail messages, might cause performance issues. Because of this, there needs to be some thought and direction given to how the end users set the rules up.

In this chapter, we describe how to coach your users to design and set up effective mail file rules, how to implement anti-spam rules, and how to monitor and evaluate the rules once they are in place.

5.1 Distinguishing between spam and legitimate e-mail

In this section we look into some characteristics of spam mail content. There are characteristics of spam mail that allow you to scan or search for items that can help you classify useful e-mail and eliminate spam e-mail. Some common features of spam are easily discernible by simply viewing the message subject or content. Others can be deduced by taking note of the source of incoming messages.

Viewing the page source of e-mail messages

The Notes 6 client allows you to view source information in a mail message by opening the message in the client and then selecting View → Show → Page Source from the Notes 6 client menu. This feature will show the “raw” content of the message as received by the SMTP server. The receiving SMTP server has to be Domino version 6.

> **Note:** Page source is available for messages sent from the Internet. You cannot view the page source of a message that was sent to you from your own Domino domain.

Example 5-1 shows the page source information for a sample spam e-mail message.

Example 5-1 Page source of a sample spam e-mail message

```
Received: from a3mail.lotus.com ([9.xx.xx.xx])
          by cammail01.lotus.com (Lotus Domino Release 6.0)
          with ESMTP id 2002110613302032-41715 ;
          Wed, 6 Nov 2002 13:30:20 -0500
Received: from internet1.lotus.com ([9.xx.xx.xx])
          by a3mail.lotus.com (Lotus Domino Release 6.0)
          with ESMTP id 2002110613301828-376177 ;
          Wed, 6 Nov 2002 13:30:18 -0500
Received: from lotus2.lotus.com (lotus2.lotus.com [129.42.250.42])
          by internet1.lotus.com (8.12.6/8.12.6) with ESMTP id gA6IUGBF027827
           (version=TLSv1/SSLv3 cipher=EDH-RSA-DES-CBC3-SHA bits=168 verify=FAIL);
          Wed, 6 Nov 2002 13:30:16 -0500 (EST)
Received: from yahoo.ca ([213.86.167.33])
          by lotus2.lotus.com (8.12.6/8.12.6) with SMTP id gA6IWe0r019429;
          Wed, 6 Nov 2002 13:32:44 -0500 (EST)
To: joe_user@lotus.com /* This is the recipient of the e-mail message */
Subject: Awseome way to make money.
Importance: Normal
Message-Id: <2H46BI3VP6.3E2V0E.beth_anne_collopy@yahoo.ca>
Date: Wed, 06 Nov 2002 13:32:33 -0500
X-MSMail-Priority: Normal
```

```
Reply-To: joe_user@yahoo.ca
From: beth_anne_collopy@yahoo.ca /* FROM: field */
Received: from yahoo.ca by RTKVQCG94P7.yahoo.ca /* This is the host that sent the message. */
with SMTP for joe_user@lotus.com; Wed, 06 Nov 2002 13:32:33 -0500
X-MIMETrack: Itemize by SMTP Server on A3MAIL/CAM/H/Lotus(Release 6.0|September 26, 2002) at
 11/06/2002 01:30:18 PM,
         Serialize by Router on A3MAIL/CAM/H/Lotus(Release 6.0|September 26, 2002) at
 11/06/2002 01:30:21 PM,
         Serialize complete at 11/06/2002 01:30:21 PM,
         Itemize by SMTP Server on CAMMAIL01/CAM/M/Lotus(Release 6.0|September 26, 2002) at
 11/06/2002 13:30:20,
         Serialize by Notes Client on Beth Anne Collopy/North Reading/IBM(Release
 6.0|September 26, 2002) at 11/20/2002 05:30:46 PM,
         Serialize complete at 11/20/2002 05:30:46 PM
Bcc:Beth_Anne_Collopy/North_Reading/IBM%LOTUS/* The message is also sent to Beth Anne Collopy*/
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset=iso-8859-1

/* Most of the content of the e-mail message has been omitted, we left the last paragraph in,
as it demonstrates how the spammer is trying to act as a legitimate party sending e-mails */
/* Notice, the following paragraph includes an IP address in "to be removed from this list" and
they site some U.S. Federal Law! */

IMPORTANT: You may remove yourself from this mailing by utilizing our automated removal system
at http://210.192.108.35/remove.html. This message is in full compliance with U.S. Federal
requirements for commercial e-mail under bill s.1618 Title 111, Section 301, Paragraph (a) (2)
(c) passed by the 105th U.S. Congress and cannot be considered spam since it includes a remove
mechanism.
```

From the page source display you can determine if message header information is deliberately misleading or has been “faked”. Examples are:

- Missing the “From” address.
- Multiple recipients with the same name or similar alpha spelling. For example, tommi@us.ibm.com, tommi@emaildomain.com, tommichaels@lmxxop.com
- Different source domain/IP than the sender. This is not always spam, but it is suspicious.
- Opt-out or remove instructions in the body with IP-numbered URLs.

  For example: http://123.21.92.12/remove.html

You can also view the Received header values. The Received values typically show Internet address information from various SMTP hosts that have processed the message. If you notice that particular internet addresses or domains have been involved in sending you multiple spam messages, you should consider either creating a mail file rule for yourself or look at possibly blocking the address or domain at the server. With the information from the page source display you can take notice of specific patterns that may identify messages that are likely to be spam.

5.2 Mail file rules

Server-based anti-spam measures address broad spam indicators; they can't address every individual problem. The mail file rules allow the individual end user to isolate messages by sender address, domain, subject, or even by message body content. When creating anti-spam mail file rules with your Notes client, you, as an end user, can be specific and aggressive when defining the rules.

> **Attention:** Even though the mail file rules are created and managed on the Notes client for individual end users, they are evaluated and enforced on the Domino server. There's no way to run mail file rules in the Notes Client.

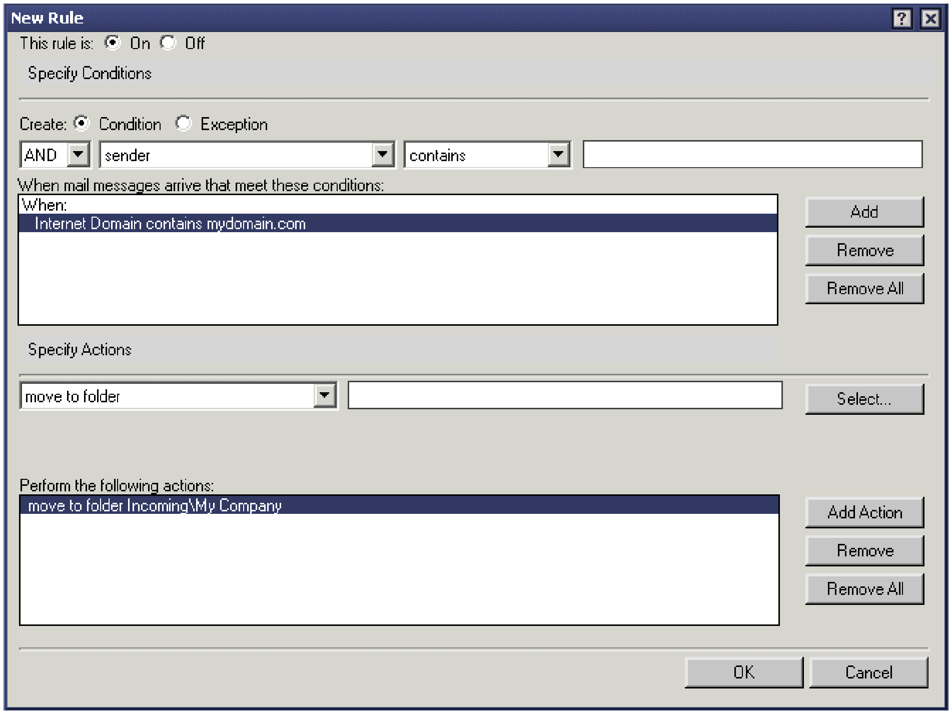
Mail file rules are used to control incoming e-mail messages. In addition to helping prevent spam, mail file rules can be used to manage your legitimate e-mail messages. In this section, we concentrate on anti-spam mail file rule development.

5.2.1 Setting up mail file rules

Use the following steps to manage your mail file rules:

1. Open your mail file. The Views and Folders list is displayed on the left.
2. Select Tools → Rules under the Views and Folders list to open the Rules view.
3. Click the New Rule button to begin building an anti-spam rule.

The Rule dialog box is the primary interface for developing your anti-spam rules. Figure 5-1 on page 69 shows the New Rule dialog.


New Rule

This rule is: ● On ○ Off

Specify Conditions

Create: ● Condition ○ Exception

AND ▾ sender ▾ contains ▾

When mail messages arrive that meet these conditions:

When:
Internet Domain contains mydomain.com

Specify Actions

move to folder ▾

Perform the following actions:

move to folder Incoming\My Company

Figure 5-1 Notes 6 new rule dialog

If you need help creating rules, beyond what is provided in this book, review the Lotus Notes 6 Help section, “Filtering new mail using rules.”

Specifying rule conditions

Under “Specify Conditions,” select a part of each message to check (such as *sender* or *subject*), select a state (such as *contains* or *is*), and enter the criteria to check for (such as the name of a certain person or a certain word). Don't use quotation marks for the criteria you enter.

As an example, you could select *sender* and *contains*, and then enter Alice to filter all messages sent to you by Alice French, Alice Stearns, and anyone else named Alice. Or you could select *Size (in bytes)* and *is greater than*, and then enter 2000 to filter all messages sent to you that are greater than 2000 bytes.

Note: The *contains* condition works on partial words, and is not case sensitive. For example, you could select *sender* and *contains*, and then enter Al or al to filter all messages sent to you by anyone named Al, Alice, Alex, or Alicia. Conversely, the *is* condition works on exact matches. You would have to use the exact e-mail address if using the *is* condition.

Tip: The *all documents* condition, new in Lotus Notes 6, lets you perform an action on all messages that arrive in your mail while the rule is enabled. For example, you might select *all documents* and specify sending a copy to myassistant@mycompany.com while you are out of the office. Be aware that you can create a mail sending loop if you improperly forward mail to an e-mail account that concurrently forwards mail to you.

Specifying rule actions

Once you have set the conditions for a rule you must select an action or actions to take for messages that meet your selected criteria. Under “Specify Actions,” select one of the following:

- Move to folder
- Copy to folder
- Send copy to
- Set expiration date
- Change importance to
- Delete

Depending on which action you have selected, you must complete the process by doing one of the following:

- If you selected *Move to folder* or *Copy to folder*, click Select and select a folder. You can also create a folder from this dialog box if no folders have yet been created in the mail file.
- If you selected *Send copy to*, select whether you want the forwarded copies to contain the full message or the message headers only. The headers are the subject, the addresses, and the date and time at the beginning of the message; they don't include the rich-text content of the message. Then enter the recipients' addresses, separated by commas, or click Address to select addresses from an address book.
- If you selected *Set expire date*, enter a number and select days, weeks, months, or years.
- If you selected *Change importance to*, select an importance level.

You can combine multiple actions for a single rule. For example, you can copy the message to a folder and change the importance. Note that if you select *Delete* as the action, you cannot add any other actions to that rule.

The client mail rules give individual users the opportunity to detect and isolate objectionable e-mail content. By isolating likely spam e-mail, the user can make an informed judgement about each specific e-mail message. The e-mail from known spammers and most offensive emails can be deleted using the more restrictive rules, yet other e-mails can be recovered without extensive restore procedures. In this way spam can be dealt with quickly without losing control of your e-mail.

5.2.2 Developing anti-spam mail file rules

In order to develop rules for your e-mail, you should first determine what type of rules you want to create and how restrictive you want to be. By creating rules that eliminate e-mail from known spamming sources and rules that file suspicious e-mail based on content, you can start to rid your inbox of most of the unwanted mail. You can also set up rules for acceptable mail from known acceptable addresses and domains that can be sequenced before any content checking takes place. This will ensure that e-mail from those sources will not be filed in your suspicious folder as a false-positive.

As an administrator, you should also look to incorporate rules that users may have in their individual mail files that would eliminate spam for the whole organization if implemented as server mail rules. Since some users want to receive mail that other users don't, however, the mail file rules are an effective way to alleviate conflicts over which domains and addresses to block at an organizational level.

In our examples we include several types of rules, in the following order:

- Denying e-mail from certain addresses
- Denying e-mail from certain domains
- Denying self-mail (spoofed "from" your own address)
- Filing e-mail with unacceptable subject content
- Filing e-mail with unacceptable body content
- Filing acceptable addresses and domains

Table 5-1 shows the different types of rules, listed with the relative effectiveness of each as an anti-spam method and the general performance cost. This may help you in deciding which types of rules to create and how many of each type:

Table 5-1 Types of mail file rules with effectiveness and performance cost

Type of rule	Overall Anti-Spam Effectiveness			Performance Cost		
	Very	Medium	Less	High	Medium	Low
Address Blocking		X				X
Domain Blocking	X					X
Self-mail		X				X
Subject Content		X			X	
Body Content	X			X		
Filing Acceptable Mail			X		X	

> **Note:** In our examples we have used several folders and we are using rules to direct e-mail and spam e-mail into them. You don't have to use this same method to handle your mail. For example, you could use just a single folder for all mail you suspect to be spam without filing anything else automatically. You could send suspicious e-mail to another mail-in database, set an expiry date on the messages, or delete all of the suspicious e-mail. Pick the style that suits you best. Be careful when setting up rules that delete any mail, as deleted e-mail messages cannot be recovered.

The anti-spam rule building technique that we show in this section is oriented toward the isolation and reduction of spam. This technique requires some review of the contents of various folders in the user's mail file. The folders used in this example are:

- **Incoming\Suspicious** - This folder is used to hold e-mail that our rules have determined to be suspicious and likely to be spam.
- **Incoming\My Customers** - This folder is used to hold incoming mail messages that our rules have determined to be from known customers and vendors.

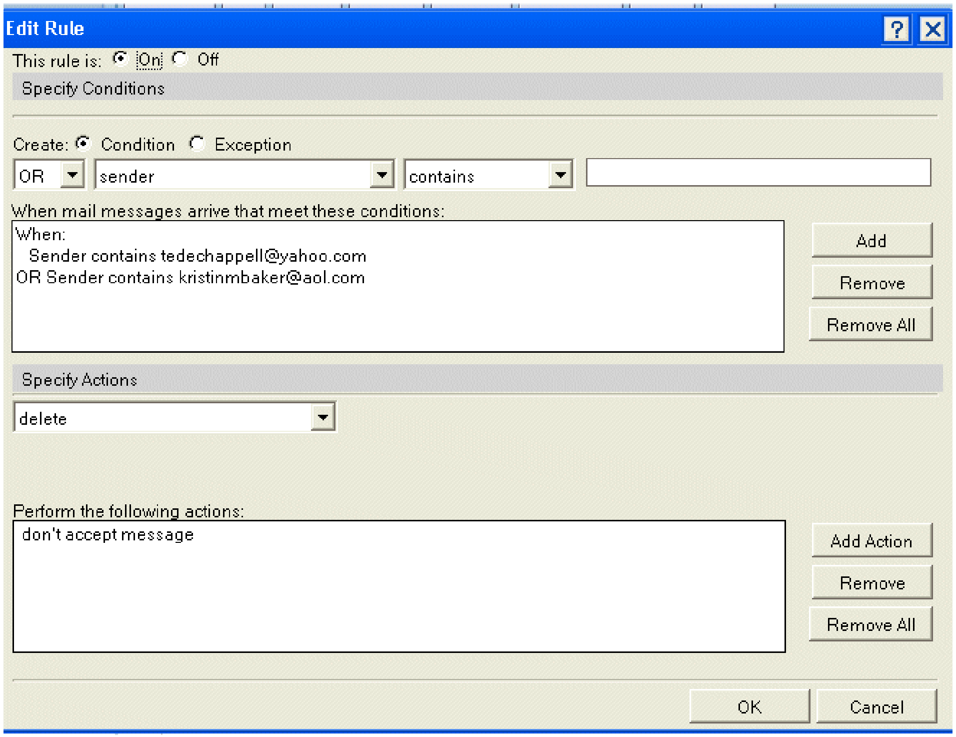
As a normal consequence of receiving e-mail, all users make an initial assessment of their inbound e-mail. However, as users develop anti-spam rules, they must make a qualitative analysis of the e-mails as they relate to the established mail rules. A user employing the technique in our example on their own mail file would have to periodically review all of the Incoming folders. The user must review the content of the Suspicious folder for false positives, that is, desired e-mails that were initially determined to be spam. At other times, the user must assess whether more stringent criteria are required to filter out more spam.

If a user established a rule that was too broad, for example, that user would undoubtedly receive e-mail that was incorrectly categorized as suspicious. On discovery of false positives, the user must make adjustments to the mail file rules to avoid such invalid categorizations in the future.

Similarly, if a user was receiving uncategorized (regular inbox) e-mail that appeared to be spam, those e-mail messages should be reviewed for characteristics that might be used to categorize them as spam so that they are deleted or placed in the suspicious folder in the future.

Denying mail from certain addresses

Some spammers use certain e-mail addresses from which to send their spam, and sometimes they send mail from domains which the organization or individual may not want to block entirely. For example, some spammers use public domain e-mail sites to create and send their spam. A lot of times these spammers change addresses frequently, but sometimes they use the same addresses repeatedly. To deny mail from these addresses you can create a mail file rule that denies mail based on the sender.



This rule is: ● On ○ Off

Specify Conditions

Create: ● Condition ○ Exception

OR | sender | contains

When mail messages arrive that meet these conditions:

When:
Sender contains tedechappell@yahoo.com
OR Sender contains kristinmbaker@aol.com

Specify Actions

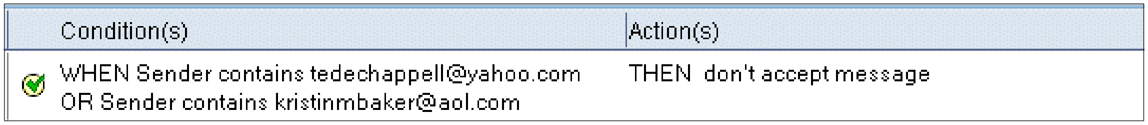
delete

Perform the following actions:

don't accept message

Figure 5-2 Rule denying mail from specific addresses

Note that the chosen action, when creating the mail rule, is *Delete,* but the displayed action, in the Mail rules view, is *Don’t accept message*. You should be judicious in your use of the delete action because messages are not archived: they are deleted and cannot be recovered. Once you click OK and save the rule it will appear in your rules view, as shown in Figure 5-3.

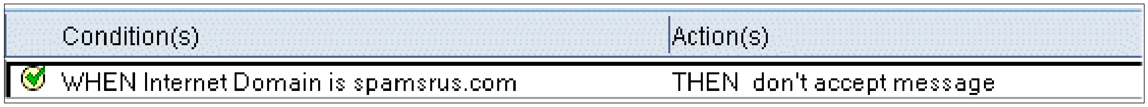


Condition(s)	Action(s)
✓ WHEN Sender contains tedechappell@yahoo.com OR Sender contains kristinmbaker@aol.com	THEN don't accept message

Figure 5-3 Rule denying mail from specific addresses as listed in rules view

Denying mail from certain domains

Since most spammers use public e-mail service domain names, you may want to add rules that exclude e-mail from one or more public e-mail service domains. For example, if you have determined that all e-mail you receive from domain spamsrus.com is spam mail, you could add a rule that automatically denies all mail from domain spamsrus.com.



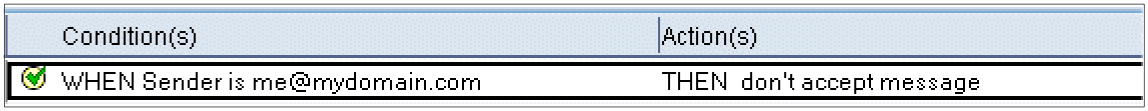
Condition(s)	Action(s)
✓ WHEN Internet Domain is spamsrus.com	THEN don't accept message

Figure 5-4 Deleting all mail from spamsrus.com

If you decide at a future time that you want to accept e-mail from a specific address at spamsrus.com, but not from anyone else there, then you could add an acceptable address rule for that address and move it above the denying rule.

Denying self-mail

The next rule is used to avoid a fairly common spam technique that we call self-mail. Self-mail is e-mail sent by a spammer where the *from* address appears to be the same as the destination address. Self-mailed e-mail from the Internet is almost always spam. Do not confuse internet mail with Notes mail. The *from* address for Notes mail is always the full Notes e-mail address, not the Internet e-mail address. In this way we can deny self-mail from the Internet without eliminating the ability of users to send Notes mail to themselves, which is fairly common. Figure 5-5 shows a self-mail rule that deletes these e-mails.



Condition(s)	Action(s)
✓ WHEN Sender is me@mydomain.com	THEN don't accept message

Figure 5-5 Self-mail Rule

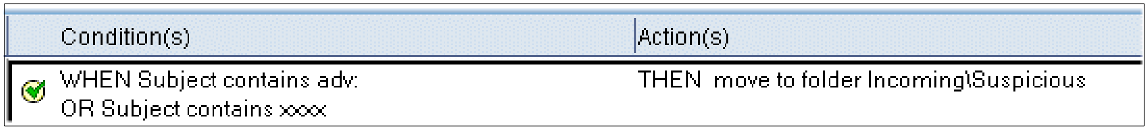
Scanning for text content

Mail rules also allow you to scan the subject or body fields for content that can help you determine the disposition of an incoming e-mail. For example, if you are always interested in e-mail about *Spacely Sprockets*, you can create a mail rule that scans for Spacely Sprockets in the subject and body fields and places that e-mail message into a Spacely Sprockets folder. Similarly, you can scan for certain words and phrases that are characteristic of spam mail. For example, many spam mail messages are solicitations for purchase of products or services at a discount. Given the nature of this type of message, you can create a mail rule that scans for text *% off*. Then, if the % off text is found in a message it can be redirected to the Suspicious folder.

You should be deliberate in your consideration of what text phrases constitute spam, and on what action to take for suspected spam messages. Some language (profanity, for example) can be indicative of spam, but might also be present in an e-mail from an unsatisfied customer. These issues must always be considered when putting mail rules in place because “false positives” (desired e-mail that has been classified as spam) can result.

Filing mail with unacceptable subject content

As a new feature in Notes 6, the number of unread items in your e-mail show next to names of the folders they are in. For example, if you have 2 unread documents in your Incoming/Suspicious mail folder, then the folder name will appear in bold with (2) next to it. When this feature is coupled with rules that file incoming e-mail into folders automatically, you can easily tell where your new unread mail is. In the following figure we have created just such a rule that files mail with unacceptable words in the subject.



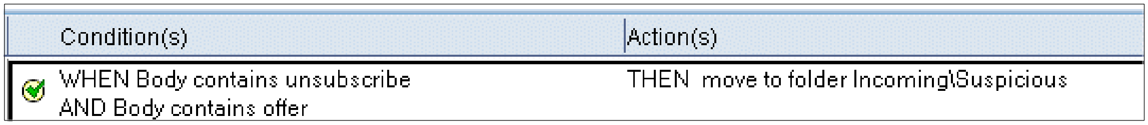
	Condition(s)	Action(s)
✓	WHEN Subject contains adv: OR Subject contains xxxx	THEN move to folder Incoming\Suspicious

Figure 5-6   Subject scanning rule

In Figure 5-6 we show a rule that scans for specific words in the subject of incoming e-mail; if the subject contains these words the mail is filed in the Incoming\Suspicious folder. When using the *Contains* action, remember that it is not case sensitive and it is not matching on whole words. For example, if scanning for *adv*, then words like *Advice* or *Advertising* would also cause a match. In this example, we’re scanning for Adv: or xxxx.

Filing mail with unacceptable body content

To scan the body of incoming e-mail, we choose the rule condition *When body contains*. This type of rule uses up the most processing power on the server, and should be created with that in mind. Having a lot of rules that scan the body of e-mails can cause server performance problems. It is recommended that you create only a few rules of this type for your mail, so you should be creative in setting them up. By looking at the spam you have received in the past and examining what the body of those e-mails contains, you can come up with some very accurate rules that will catch most of the spam you receive. It is also recommended that you file mail that matches on a scan of the body content unless you are certain your rule is going to catch only spam.



	Condition(s)	Action(s)
✓	WHEN Body contains unsubscribe AND Body contains offer	THEN move to folder Incoming\Suspicious

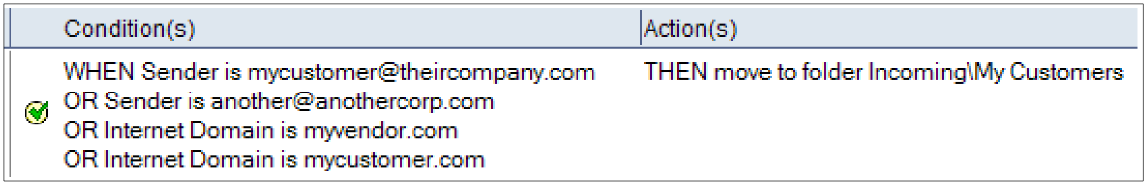
Figure 5-7 Body scanning rule

In the example in Figure 5-7 we are scanning the body of incoming mail to see if it contains the words *unsubscribe* and *offer*. If an e-mail contains both of these words, the rule files it in our Incoming\Suspicious folder.

Filing e-mail from acceptable addresses and domains

As you develop your mail rules, keep in mind that acceptable addresses and domains might be used by spammers to deceive you into thinking that their spam e-mail is legitimate. You should consider your selection of acceptable addresses and domains carefully. Remember also that public e-mail service domains seem to be the preferred method of spoofing e-mail.

Figure 5-8 shows a rule to accept e-mail from specific addresses and domains.



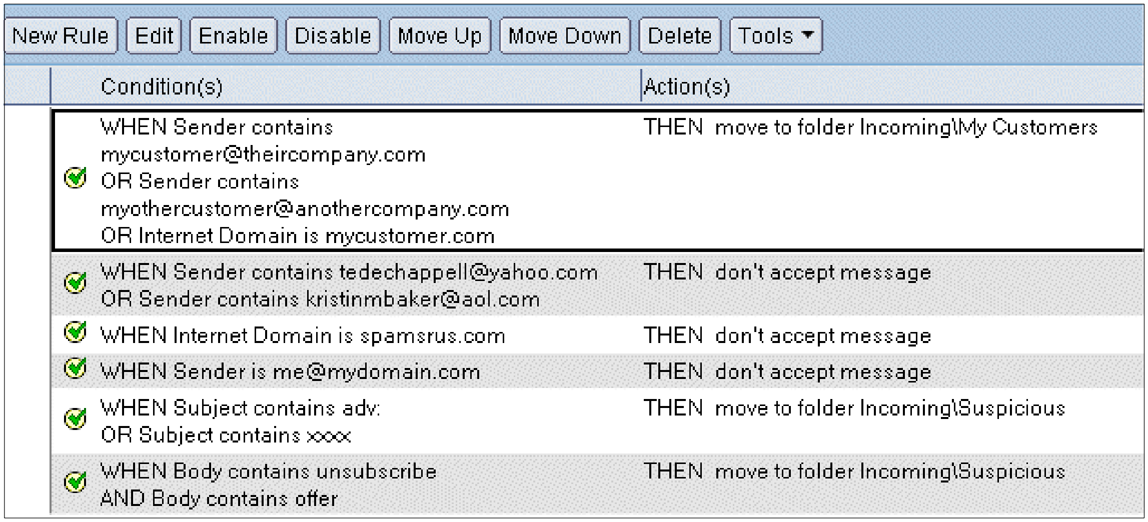
	Condition(s)	Action(s)
✓	WHEN Sender is mycustomer@theircompany.com OR Sender is another@anothercorp.com OR Internet Domain is myvendor.com OR Internet Domain is mycustomer.com	THEN move to folder Incoming\My Customers

Figure 5-8 Acceptable customers and vendors rule

In rules for filing e-mail, we recommend that you *do not* specifically file mail from the domains of public e-mail services. Instead we recommend that you only file e-mail from *full e-mail addresses* of legitimate senders within those e-mail domains. Be aware that bulk emailers are seldom legitimate business concerns, so they may create spoofed e-mail which appears to come from legitimate sources. With these ideas in mind, try to build your initial rules such that the accepted e-mail addresses and domains indicate genuine e-mail from known sources.

5.2.3 Viewing mail rules and the evaluation sequence

Once you have created the rules for your mail file, you need to look at the whole set and place them in the right sequence. Figure 5-9 shows our sample rules and their sequence in the mail file rules view. *Move Up* and *Move Down* action buttons at the top of the rules view can be used to change the sequence.



	Condition(s)	Action(s)
✓	WHEN Sender contains mycustomer@theircompany.com OR Sender contains myothercustomer@anothercompany.com OR Internet Domain is mycustomer.com	THEN move to folder Incoming\My Customers
✓	WHEN Sender contains tedechappell@yahoo.com OR Sender contains kristinmbaker@aol.com	THEN don't accept message
✓	WHEN Internet Domain is spamsrus.com	THEN don't accept message
✓	WHEN Sender is me@mydomain.com	THEN don't accept message
✓	WHEN Subject contains adv: OR Subject contains xxxx	THEN move to folder Incoming\Suspicious
✓	WHEN Body contains unsubscribe AND Body contains offer	THEN move to folder Incoming\Suspicious

Figure 5-9 Rules view showing rules in the evaluation sequence

Based on these rules, the mail that you know you want will end up in the folder My Customers. Mail that is definitely spam will be denied and mail that is likely to be spam will end up in the Suspicious folder. Typically, you will want any rules that file acceptable mail into folders to be first and rules that scan the body of messages to be last, since these take up the most processing time.

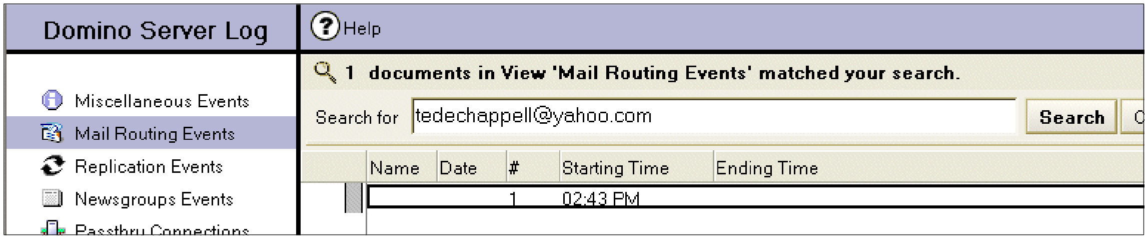
Attention: All rules are always evaluated with every message. This means that the rule execution is not stopped if one or more rules are applied to a message. Consider an example where a message is received from an acceptable address and a rule files it to a folder. Another rule with the action *Don't accept message*, which is later in the evaluation sequence, then finds unacceptable words in the subject. The message is deleted.

Plan your rules appropriately and use the *Don't accept message* action very carefully.

5.2.4 Monitoring mail file rules

Depending on the type of mail rules you set up, monitoring their success and effectiveness can be as simple as looking at what is in your different folders, or as difficult as searching the notes logs and interpreting whether or not a spammer tried to send you something.

If you are using a mail file rule that doesn't accept mail from a certain address or domain, then to tell if it is working, you would need to search the Domino Server Log database on your mail server in the view Mail Routing Events. To make your search easier, you may want to Full-Text Index the database. From the View menu, select Search This View to access the search bar and enter the address you want to search for.



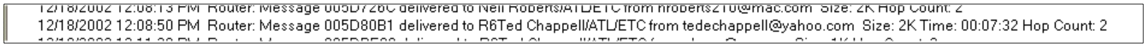
1 documents in View 'Mail Routing Events' matched your search.

Search for: tedechappell@yahoo.com

Name	Date	#	Starting Time	Ending Time
		1	02:43 PM	

Figure 5-10 Searching the Domino Server Log - Mail Routing Events

In Figure 5-10 we are searching for an address that we are denying mail from in a mail file rule. Since we have not received mail from this address since setting up the rule, we are searching to see if the spammer has tried to send us any e-mail since that time. The log entry itself is show in Figure 5-11.



```
12/18/2002 12:08:13 PM  Router: Message 005D726C delivered to Neil Roberts/ATL/ETC from nroberts210@mac.com  Size: 2K Hop Count: 2
12/18/2002 12:08:50 PM  Router: Message 005D80B1 delivered to R6Ted Chappell/ATL/ETC from tedechappell@yahoo.com  Size: 2K Time: 00:07:32 Hop Count: 2
```

Figure 5-11 Mail Routing Events log entry

Since we didn’t receive this e-mail, whose attempted delivery to us is shown in the log, we know our mail file rule worked and deleted the e-mail.

If you are using mail file rules that file e-mails into folders, such as Incoming\Suspicious, you can examine what is in the folders to see if the rules are working the way you want them to. You can also see if there are any false positives where you have rules that are scanning the subject or body of e-mails.

Build your rules carefully

When developing mail file rules, it is imperative that you take into account all mail that you receive. Classifying messages as spam when they are not will, at best, cause a nuisance, and at worst will cause missed or lost business.

Select your text phrases carefully. Scanning for text that is too broad in scope can cause false positives. For example, at first glance it may seem appropriate to scan for the text *sex*. However, there are words—like *sextuplets* and *Essex*—that contain that same text, but that may not be indicative of spam messages. It is also important to understand the nature of your organization when building rules. For example, in a hospital, anatomical terms for body parts may be completely acceptable within medical or research departments, but could be used to screen out spam in the accounting department.

As you gain more experience in setting up your mail file rules, and further analyze the nature of the spam mail that you receive, you can refine your rules to more effectively eliminate spam.

6

Third party anti-spam products

This chapter introduces some of the third party products available to help you in addressing the spam problem. We have divided the products into two categories:

- Anti-spam products that run on a Domino server
- Separate anti-spam server and gateway products and services

6.1 Anti-spam products for Notes and Domino

This section introduces some third party anti-spam products that operate in a Notes/Domino environment. These products add features to the anti-spam functionality provided by Notes/Domino.

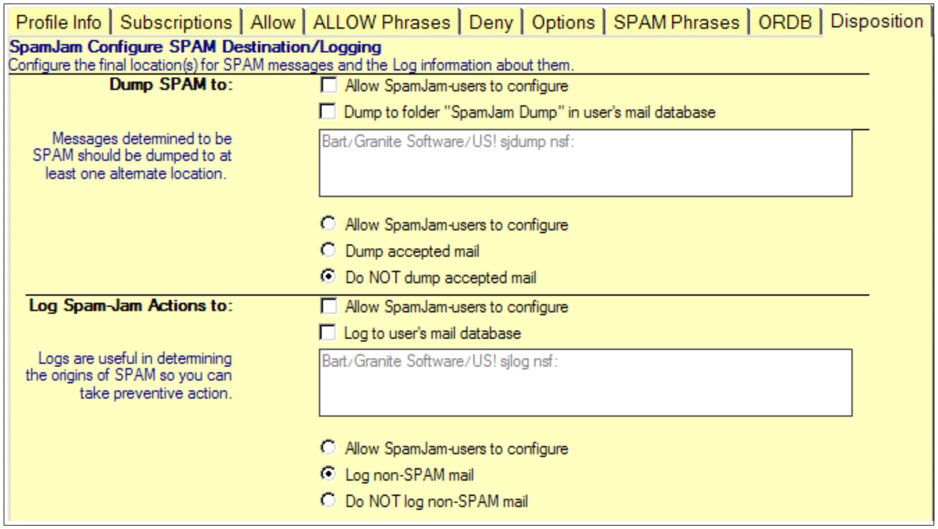
6.1.1 spamJam for Lotus Notes and Domino

spamJam for Lotus Notes and Domino is an adaptable filter designed to help administrators and end users detect and prevent spam. spamJam combines the best attributes of a centrally administered configuration with the flexibility of end user rule definition. End user message recovery is simple and immediately effective. This combined spamJam approach produces a system that administrators and users can trust to evaluate e-mail effectively, without the danger of losing or delaying important e-mail.

Configuring spamJam

spamJam allows mail administrators to define spam filters at the corporate level to prevent true spam, like pornography, while allowing individual users to define their own individual levels of spam control. For example, one user may want to see an unsolicited industry newsletter, while another may not.

Administrators define the initial Master configuration and then the user takes over from there. The user can decide to leave their Master configuration as is, or define additional anti-spam criteria. Master configurations can be designated for “levels of aggressiveness,” so administrators and users can apply spam controls that are more or less lenient, depending upon their specific spam problems. This also reduces the possibility of incorrectly categorizing desired e-mail as spam (false positives). In addition, once user configurations are defined, any changes to the corporate Master anti-spam configuration automatically update their corresponding user configurations.



SpamJam Configure SPAM Destination/Logging

Configure the final location(s) for SPAM messages and the Log information about them.

Dump SPAM to:

Messages determined to be SPAM should be dumped to at least one alternate location.

□ Allow SpamJam-users to configure

□ Dump to folder "SpamJam Dump" in user's mail database

Bart/Granite Software/US! sjdump nsf:

○ Allow SpamJam-users to configure

○ Dump accepted mail

● Do NOT dump accepted mail

Log Spam-Jam Actions to:

Logs are useful in determining the origins of SPAM so you can take preventive action.

□ Allow SpamJam-users to configure

□ Log to user's mail database

Bart/Granite Software/US! sjlog nsf:

○ Allow SpamJam-users to configure

● Log non-SPAM mail

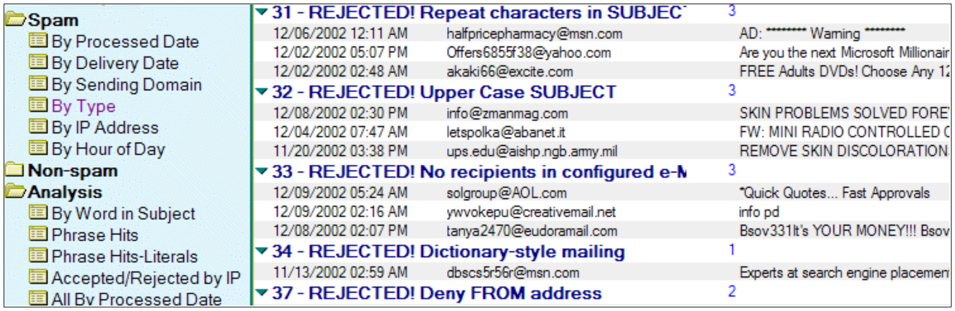
○ Do NOT log non-SPAM mail

Figure 6-1 Spam destination and logging configuration

Figure 6-1 shows a few of the configuration options available to administrators and users. In particular, it shows the Disposition tab from within a spamJam Master Configuration. The Disposition settings allow administrators to configure how spamJam will handle mail that has been determined to be spam.

Dump and log databases

With spamJam, administrators track and view spam via log and dump databases. The log database contains a listing of all incoming mail (spam and non-spam) and provides spam analysis features.



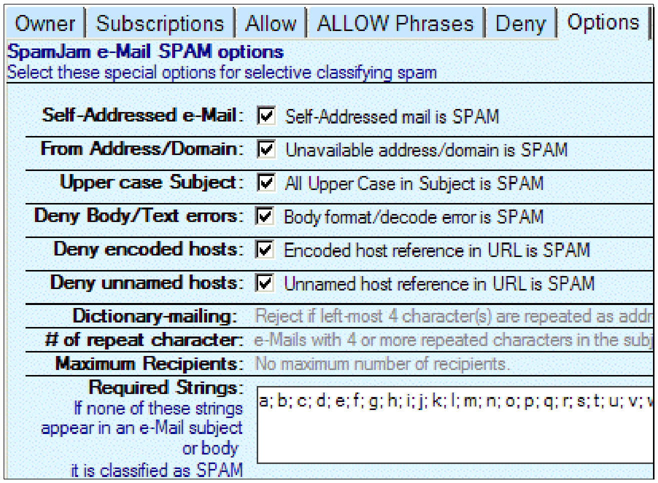
```
▼ 31 - REJECTED! Repeat characters in SUBJEC      3
   12/06/2002 12:11 AM   halfpricephamacy@msn.com          AD: ******** Waming ********
   12/02/2002 05:07 PM   Offers6855f38@yahoo.com           Are you the next Microsoft Millionair
   12/02/2002 02:48 AM   akaki66@excite.com                FREE Adults DVDs! Choose Any 12
▼ 32 - REJECTED! Upper Case SUBJECT               3
   12/08/2002 02:30 PM   info@zmanmag.com                  SKIN PROBLEMS SOLVED FORE
   12/04/2002 07:47 AM   letspolka@abanet.it               FW: MINI RADIO CONTROLLED C
   11/20/2002 03:38 PM   ups.edu@aishp.ngb.amy.mil         REMOVE SKIN DISCOLORATION
▼ 33 - REJECTED! No recipients in configured e-M  3
   12/09/2002 05:24 AM   solgroup@AOL.com                  *Quick Quotes... Fast Approvals
   12/09/2002 02:16 AM   ywvokepu@creativemail.net         info pd
   12/08/2002 02:07 PM   tanya2470@eudoramail.com          Bsov331It's YOUR MONEY!!! Bsov
▼ 34 - REJECTED! Dictionary-style mailing         1
   11/13/2002 02:59 AM   dbscs5r56r@msn.com                Experts at search engine placemen
▼ 37 - REJECTED! Deny FROM address                2
```

Figure 6-2 A view of a spamJam log database showing rejected messages

The log database (see Figure 6-2) contains a listing of the user's spam, from which any rejected e-mail can be recovered to the user's mail file. The spam messages are categorized by the reason they were rejected. Alternatively, spam can be simply redirected to an alternate folder within the user's mail file. The administrator's view of log and dump databases displays information for all users in the system, while the individual user access to log and dump databases shows only spam information for that particular user. End users see an immediate reduction in spam, but also know they can review all filtered messages at any time.

End-users have full control

spamJam gives users the benefits of a full-featured anti-spam filter without affecting the resources of operations staff. Users don't have to call mail administrators to adjust individual rules or to recover desired messages. Depending on the various levels of Master configurations, end-users have a wide array of spam classification options that they can control according to their level of technical expertise. These options include Allow/Exception settings (for domains, addresses, and subjects), Deny settings (domains, addresses, content filtering, and open relay), and much more. Figure 6-3 shows a small portion of the configuration options that can be set by the end-user or the administrator.



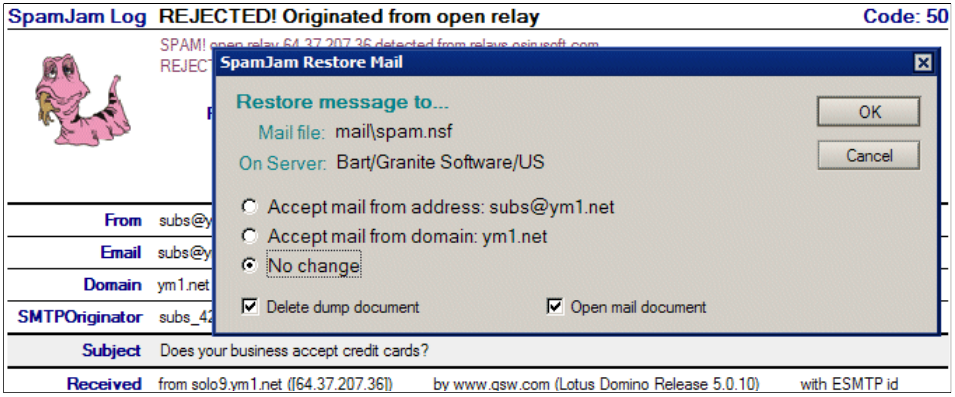
SpamJam e-Mail SPAM options

Select these special options for selective classifying spam

Self-Addressed e-Mail:	☑ Self-Addressed mail is SPAM
From Address/Domain:	☑ Unavailable address/domain is SPAM
Upper case Subject:	☑ All Upper Case in Subject is SPAM
Deny Body/Text errors:	☑ Body format/decode error is SPAM
Deny encoded hosts:	☑ Encoded host reference in URL is SPAM
Deny unnamed hosts:	☑ Unnamed host reference in URL is SPAM
Dictionary-mailing:	Reject if left-most 4 character(s) are repeated as addr
# of repeat character:	e-Mails with 4 or more repeated characters in the subj
Maximum Recipients:	No maximum number of recipients.
Required Strings: If none of these strings appear in an e-Mail subject or body it is classified as SPAM	a; b; c; d; e; f; g; h; i; j; k; l; m; n; o; p; q; r; s; t; u; v; v

Figure 6-3 A portion of the spamJam spam classification options

When users review their spamJam log, they can restore e-mail messages directly to their own mail file without the requirement for administrative approval or intervention. Users simply click a button to restore the message and are presented with options (see Figure 6-4 on page 85) to subsequently accept mail from the sending domain or address.



SpamJam Log REJECTED! Originated from open relay Code: 50

SPAM! open relay 64.37.207.36 detected from relays.osirusoft.com
REJECT

SpamJam Restore Mail

Restore message to...
Mail file: mail\spam.nsf
On Server: Bart/Granite Software/US

○ Accept mail from address: subs@ym1.net
○ Accept mail from domain: ym1.net
● No change

☑ Delete dump document ☑ Open mail document

From subs@y
Email subs@y
Domain ym1.net
SMTPOriginator subs_42
Subject Does your business accept credit cards?
Received from solo9.ym1.net ([64.37.207.36]) by www.gsw.com (Lotus Domino Release 5.0.10) with ESMTP id

Figure 6-4 Restoring a message to the user's mail file

spamJam benefits existing Domino environments

The continuing increase of undesired e-mail plagues many end users and frustrates system administrators because of its unpredictability. spamJam gives end-users and administrators relief from the deluge of spam while providing peace of mind with full recoverability, all within their familiar Domino environment.

All spamJam configuration and operational controls are within the Domino infrastructure. There is no need for separate relay servers or new and separate user interfaces. Users and administrators don't have to leave their familiar Notes client to configure spamJam or to review or recover intercepted spam messages.

spamJam runs in Domino R5 and Domino 6 environments and is supported on all Domino server platforms. For more detailed information or for an evaluation copy of spamJam for Lotus Notes and Domino, visit the Granite Software Web site at:

```
http://www.gsw.com
```

6.1.2 SpamEraser for Lotus Notes and Domino 6

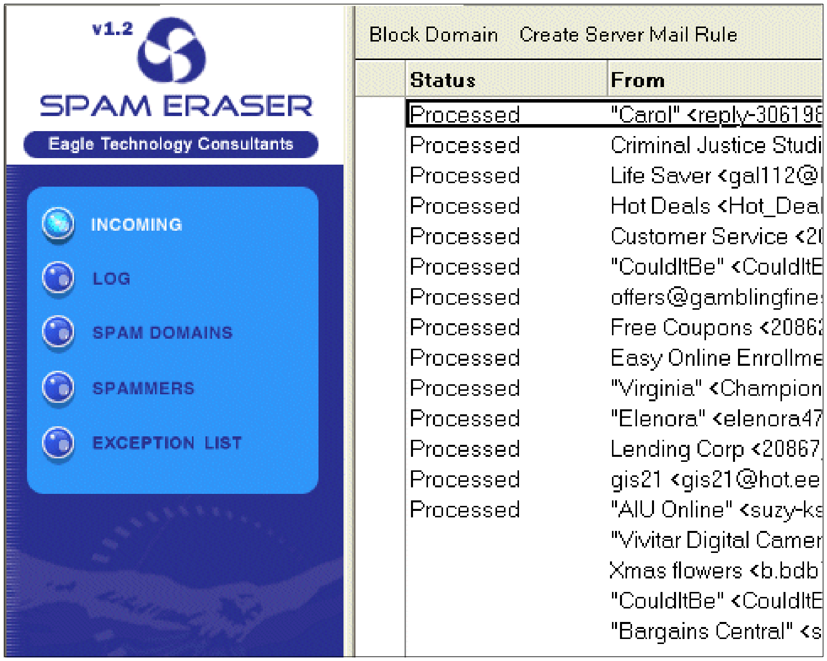
SpamEraser for Lotus Notes and Domino 6, from Eagle Technology Consultants, LLC, automates the process of blocking unwanted e-mail addresses and domains. It allows all of the users in an organization to contribute to the blocking lists. SpamEraser reduces the amount of storage space needed for e-mail by deleting the unwanted messages, and the newest version leverages the content filtering features contained in Lotus Notes 6. SpamEraser helps keep viruses out of an organization by keeping a log and blocking known spamming sources. Additionally, SpamEraser leverages the Spamhaus block list to give organizations an immediate return on their investment by blocking those known spammers immediately.

SpamEraser can be set up in three different configurations:

- Individual user configuration - Users have their own block list that they control.
- Group user configuration - A group of users contribute to a shared block list that is managed by an administrator.
- Enterprise configuration - Enterprise mode is set up with one block list for the entire organization; the list is centrally controlled by an administrator. Users can contribute to the blocking lists.

SpamEraser integrates with the Server Configuration document and allows you to automatically append addresses and domains to the fields in the Server Configuration. This is done by an administrator on the SMTP server, so appropriate administration privileges to the server are required.

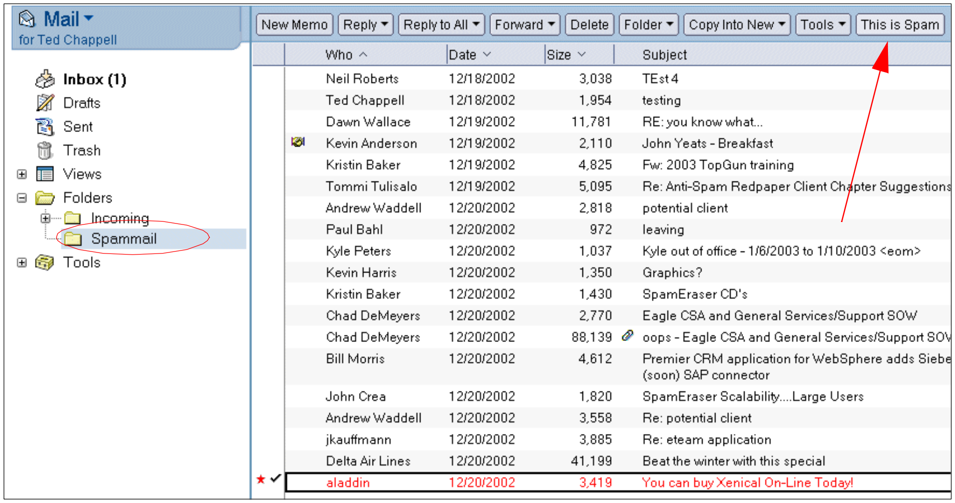
SpamEraser works through a series of Domino agents which check the block list for all incoming mail and delete them if they are from someone on the list or from a domain that is in the SpamDomains list.



Status	From
Processed	"Carol" <reply-306198
Processed	Criminal Justice Studi
Processed	Life Saver <gal112@I
Processed	Hot Deals <Hot_Deal
Processed	Customer Service <2(
Processed	"CouldItBe" <CouldItE
Processed	offers@gamblingfine
Processed	Free Coupons <20862
Processed	Easy Online Enrollme
Processed	"Virginia" <Champion
Processed	"Elenora" <elenora47
Processed	Lending Corp <20867
Processed	gis21 <gis21@hot.ee
Processed	"AIU Online" <suzy-ks
	"Vivitar Digital Camer
	Xmas flowers <b.bdb
	"CouldItBe" <CouldItE
	"Bargains Central" <s

Figure 6-5 Incoming mail queue

With the Individual or Group configurations, the mail enters the organization but never reaches the recipient if it is from a known spammer. Each user blocks spam mail by clicking a “This is Spam” button or by dragging the message to the Spam folder in their mail files. The “This is Spam” button and the SpamMail folder are visible in Figure 6-6.

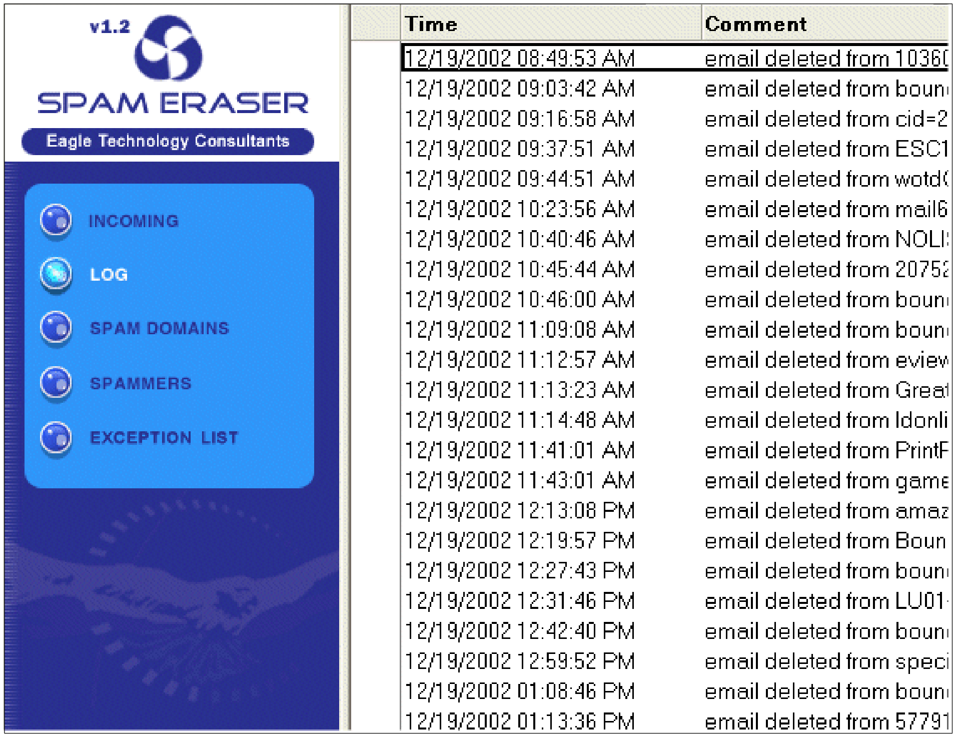


Who	Date	Size	Subject
Neil Roberts	12/18/2002	3,038	TEst 4
Ted Chappell	12/18/2002	1,954	testing
Dawn Wallace	12/19/2002	11,781	RE: you know what...
Kevin Anderson	12/19/2002	2,110	John Yeats - Breakfast
Kristin Baker	12/19/2002	4,825	Fw: 2003 TopGun training
Tommi Tulisalo	12/19/2002	5,095	Re: Anti-Spam Redpaper Client Chapter Suggestions
Andrew Waddell	12/20/2002	2,818	potential client
Paul Bahl	12/20/2002	972	leaving
Kyle Peters	12/20/2002	1,037	Kyle out of office - 1/6/2003 to 1/10/2003 <eom>
Kevin Harris	12/20/2002	1,350	Graphics?
Kristin Baker	12/20/2002	1,430	SpamEraser CD's
Chad DeMeyers	12/20/2002	2,770	Eagle CSA and General Services/Support SOW
Chad DeMeyers	12/20/2002	88,139	oops - Eagle CSA and General Services/Support SOV
Bill Morris	12/20/2002	4,612	Premier CRM application for WebSphere adds Siebe (soon) SAP connector
John Crea	12/20/2002	1,820	SpamEraser Scalability....Large Users
Andrew Waddell	12/20/2002	3,558	Re: potential client
jkauffmann	12/20/2002	3,885	Re: eteam application
Delta Air Lines	12/20/2002	41,199	Beat the winter with this special
aladdin	12/20/2002	3,419	You can buy Xenical On-Line Today!

Figure 6-6 “This is Spam” button in the mail file

In order to prevent messages from mistakenly being construed as spam, the application also features an Exception List functionality, which is basically the opposite of a block list, allowing users to manage a list of addresses and/or domains they never want to block.

Whenever SpamEraser acts on a incoming message, this is recorded on the log that SpamEraser maintains. Figure 6-7 on page 88 shows a log view that contains several entries for messages that were rejected by SpamEraser.



Time	Comment
12/19/2002 08:49:53 AM	email deleted from 1036
12/19/2002 09:03:42 AM	email deleted from boun
12/19/2002 09:16:58 AM	email deleted from cid=2
12/19/2002 09:37:51 AM	email deleted from ESC1
12/19/2002 09:44:51 AM	email deleted from wotd
12/19/2002 10:23:56 AM	email deleted from mail6
12/19/2002 10:40:46 AM	email deleted from NOLI
12/19/2002 10:45:44 AM	email deleted from 2075
12/19/2002 10:46:00 AM	email deleted from boun
12/19/2002 11:09:08 AM	email deleted from boun
12/19/2002 11:12:57 AM	email deleted from eview
12/19/2002 11:13:23 AM	email deleted from Great
12/19/2002 11:14:48 AM	email deleted from Idonli
12/19/2002 11:41:01 AM	email deleted from PrintF
12/19/2002 11:43:01 AM	email deleted from game
12/19/2002 12:13:08 PM	email deleted from amaz
12/19/2002 12:19:57 PM	email deleted from Boun
12/19/2002 12:27:43 PM	email deleted from boun
12/19/2002 12:31:46 PM	email deleted from LU01
12/19/2002 12:42:40 PM	email deleted from boun
12/19/2002 12:59:52 PM	email deleted from speci
12/19/2002 01:08:46 PM	email deleted from boun
12/19/2002 01:13:36 PM	email deleted from 57791

Figure 6-7 The log view of SpamEraser

For more detailed information about SpamEraser for Lotus Notes and Domino 6, visit the Web pages of Eagle Technology Consultants, LLC at:

```
http://www.eagletc.com
```

6.1.3 iQ.Suite

GROUP Technologies offers a suite of products, the iQ.Suite, for e-mail security and organization. A number of products are available for Microsoft Exchange and Lotus Domino servers. The securiQ product line contains the following e-mail security-related products:

- securiQ.Wall - Anti-spam and content filtering
- securiQ.Xblock - Image scanning and filtering
- securiQ.Crypt - Encryption/decryption
- securiQ.Watchdog - Anti-virus protection and attachment control
- securiQ.Trailer - Legal disclaimers
- securiQ.Safe - E-mail recording and archiving

securiQ.Wall

The securiQ.Wall product protects companies from spam and prevents spreading of sensitive information. Some of the features include:

- Protection from spam, junk mail, and advertising mailshots.

  It blocks unsolicited e-mail by checking sender, recipient, and mail content.

- Protection of enterprise-critical information.

  This is accomplished by preventing the unauthorized sending of confidential information using lexical analysis procedures. The analysis is applied to the full e-mail and/or e-mail file attachments.

- Blocking of e-mail to undesirable recipients (competitors, freemail services, and so forth).

  Specific e-mail communication channels can be blocked. This is achieved by checking predefined sender/recipient combinations. Information can be selectively channelled in this way.

- Comprehensive protection of Groupware databases.

  This feature protects e-mail traffic and all Groupware databases. In addition to real-time scanning, scheduled protection mechanisms are available to support this.

- Server-based protection of encrypted e-mail.

  When used in conjunction with securiQ.Crypt, securiQ.Wall offers centralized content checking for encrypted inbound and outbound e-mail.

- Flexible tailoring in line with enterprise e-mail.

  The flexible setup controls can quickly be tailored to suit the rules of your enterprise. Different security mechanisms can be employed for different areas of the enterprise.

6.1.4 ScanMail for Lotus Notes with eManager

Trend Micro ScanMail for Lotus Notes (SMLN), version 2.6, scans e-mail, Domino databases, and add-on Lotus products, like SameTime and QuickPlace, to detect and remove hidden viruses. ScanMail provides comprehensive, rule-based content filtering of e-mail and attachments, as well as a spam filter with automatic updates. It also offers centralized management through support of Trend Micro Control Manager 2.5. With Control Manager, administrators can easily configure, monitor, and deploy scan engine and pattern file updates. ScanMail delivers effective virus protection and content security to safeguard against the loss of confidential information, minimize server congestion, and maintain productivity. SMLN is available for Windows 2000, Solaris, AIX, S/390, AS/400, RedHat, and SuSE Intel compatible Linux.

Key features of ScanMail for Lotus Notes:

- Virus elimination and alerts
- Efficient database and replication scanning
- High-performance scanning and scalability
- Flexible configuration and management
- Trend Micro eManager support – content filtering
- Trend Micro enterprise protection strategy support
- E-mail and file type blocking to enforce security policies

Principle of spam filtering in ScanMail for Lotus Notes

eManager is an optional module that provides spam and content filtering. In ScanMail for Lotus Notes, eManager is integrated in e-mail filter rules. E-mail filter rules let the administrator define policy-based rules for e-mail content filtering and mail and bandwidth management.

The spam filtering is based on a spam rule database with filter rules to identify the spam mail. These rules are used by the content filter of eManager and are applied to headers, subject, and content of e-mail. TrendLab has a Web of personal and corporate mailboxes around the world where they collect spam. A team continuously updates the spam database, just like the pattern file for the virus solution. The fingerprints they create are frequently published, and automatically downloaded and deployed in your ScanMail installation, freeing up administrator time from dealing with the time-consuming issue of creating rules.

Configuring rules for spam filtering

You can create one or more rules that will activate filtering. Figure 6-8 shows the ScanMail view from which you can create filter rules.

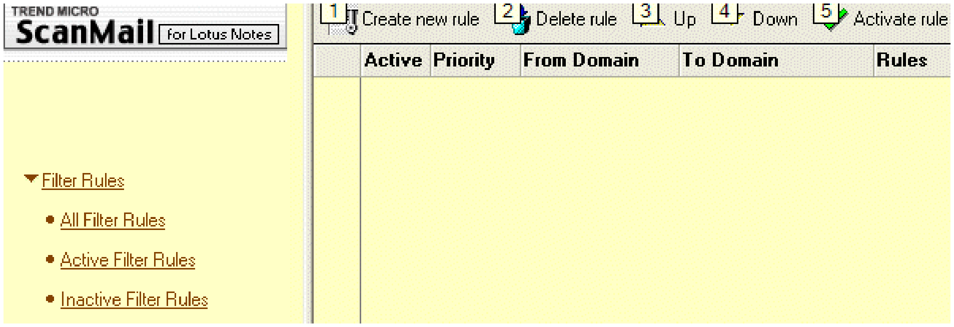
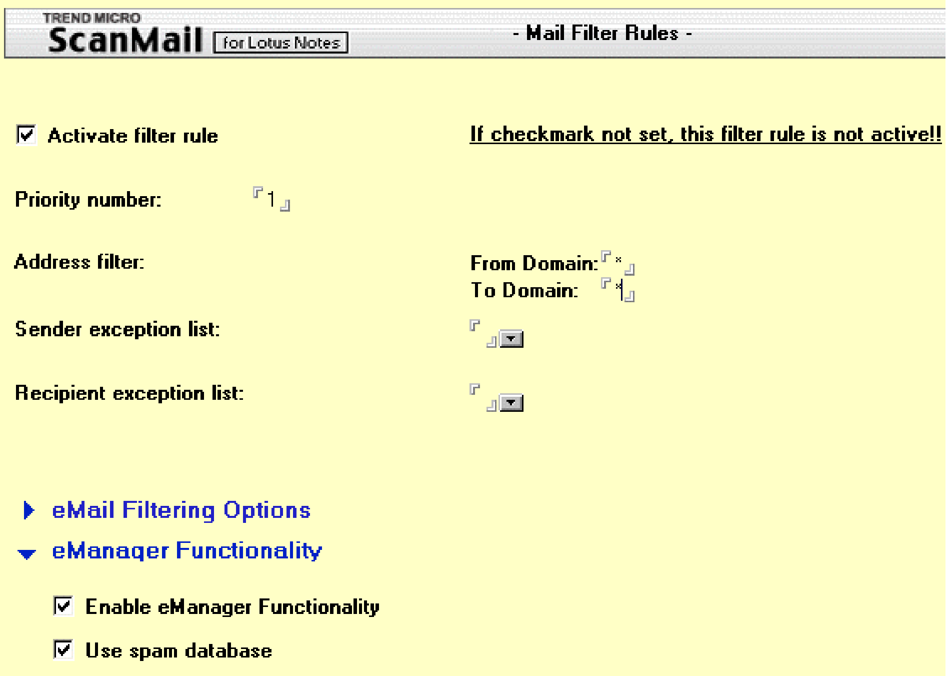


Figure 6-8 Filter Rules configuration

The configuration screen for a spam rule is shown in Figure 6-9. It illustrates how simple the creation and prioritization of rules is with this tool. The administrator can optionally choose to quarantine the blocked e-mail, and notifications can also be enabled for testing purposes.



☑ Activate filter rule

If checkmark not set, this filter rule is not active!!

Priority number: 1

Address filter: From Domain: * To Domain: *

Sender exception list:

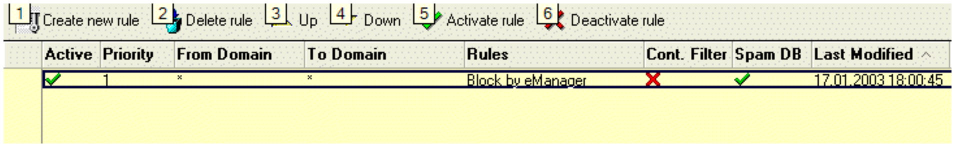
Recipient exception list:

☑ Enable eManager Functionality

☑ Use spam database

Figure 6-9 Mail filter rule configuration

After you save the new rule, it will be listed in the view, as shown in Figure 6-10.



Active	Priority	From Domain	To Domain	Rules	Cont. Filter	Spam DB	Last Modified
✓	1	*	*	Block by eManager	✗	✓	17.01.2003 18:00:45

Figure 6-10 Mail filter rules view

To find out more about ScanMail for Lotus Notes and eManager, see the Trend Micro Web site at:

http://www.trendmicro.com/en/products/email/smln/evaluate/overview.htm

6.1.5 XM SpamStop

XM SpamStop from XM Technologies Inc. integrates with Domino 6 and provides inbound messaging content security with over 300 built-in algorithms, including blacklists, malformed header checks, whitelists, auto whitelists, and message signatures. A smart application, SpamStop continually updates itself to counter the ever-changing, but simple methods of spammers to get their junk mail to you.

Based on customer project experiences with SpamStop, XM Technologies has organized their offering to address what they have identified as key challenges in anti-spam implementations, as follows:

- DNS Blacklists are not 100% effective.

  DNS Blacklists do not cover hotmail, yahoo, and other big ISPs, since it is impossible to do global blocking against them. As well, many small companies can inadvertently end up on a DNS Blacklist and have problems removing themselves.

- Users have differing requirements.

  SpamStop allows a company to have per-user or per-department settings to accommodate different languages, non-western characters, special department circumstances, and so forth.

- Stopping messages before they get to the user is often most effective.

  SpamStop allows for a simple workflow where no one is forced to read unwanted or inappropriate e-mail content; it can be stopped at the server before ever going to a user’s bulk mail or spam folder.

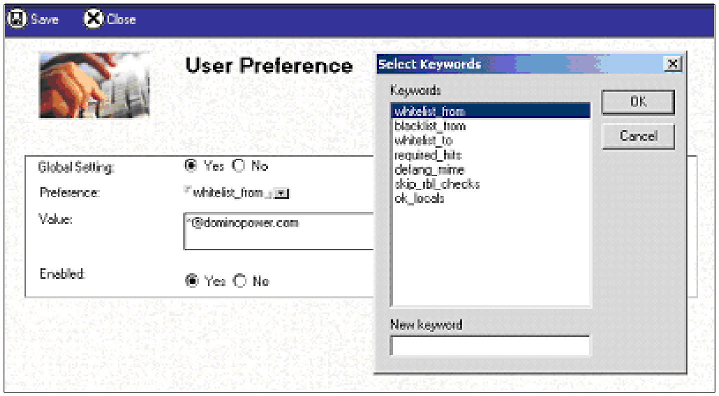
- Management is unwilling to spend the necessary funds.

  Spam is a low profile problem in many companies—unless a senior manager is receiving it. Licensing of SpamStop is based on a flat per-server fee plus monthly maintenance, making it easy to make a business case to management.

SpamStop incorporates the following key features:

- Uses an adjustable scoring system of 1 to 100
- Allows for user-specific or global settings
- Does between 10 and 300 built-in checks
- Checks DNS Blacklist (2-20 servers)
- Uses and automatically creates Whitelists
- Checks Blacklists
- Checks allowed language formats
- Workflow system deals with spam management or allows it to flow to the user
- Checks message signatures (known spam)

Figure 6-11 through Figure 6-13 show some sample screens from the SpamStop product.



Global Setting: ● Yes ○ No

Preference: whitelist_from

Value: @dominopower.com

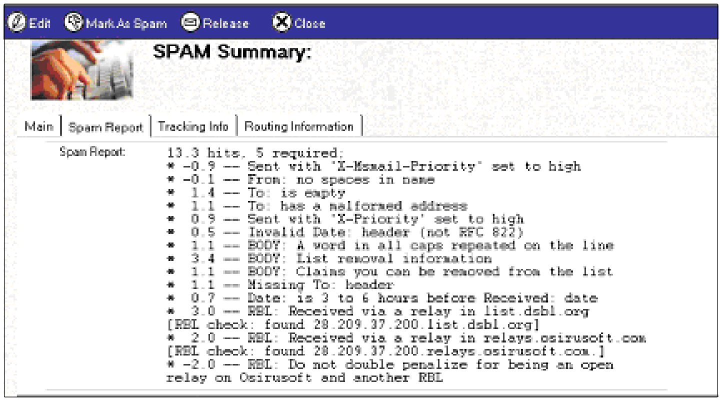
Enabled: ● Yes ○ No

Keywords

- whitelist_from
- blacklist_from
- whitelist_to
- required_hits
- defang_mime
- skip_rbl_checks
- ok_locals

New keyword

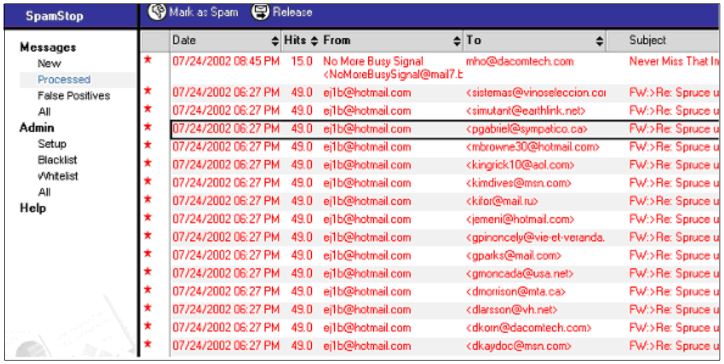
Figure 6-11 User customizable



Spam Report:

```
13.3 hits, 5 required;
* -0.9 -- Sent with 'X-Msmail-Priority' set to high
* -0.1 -- From: no spaces in name
*  1.4 -- To: is empty
*  1.1 -- To: has a malformed address
*  0.9 -- Sent with 'X-Priority' set to high
*  0.5 -- Invalid Date: header (not RFC 822)
*  1.1 -- BODY: A word in all caps repeated on the line
*  3.4 -- BODY: List removal information
*  1.1 -- BODY: Claims you can be removed from the list
*  1.1 -- Missing To: header
*  0.7 -- Date: is 3 to 6 hours before Received: date
*  3.0 -- RBL: Received via a relay in list.dsbl.org
[RBL check: found 28.209.37.200.list.dsbl.org]
*  2.0 -- RBL: Received via a relay in relays.osirusoft.com
[RBL check: found 28.209.37.200.relays.osirusoft.com.]
* -2.0 -- RBL: Do not double penalize for being an open
relay on Osirusoft and another RBL
```

Figure 6-12 Uses over 300 checks with point system



	Date	Hits	From	To	Subject
★	07/24/2002 08:45 PM	15.0	No More Busy Signal <NoMoreBusySignal@mail7.b	mho@dacomtech.com	Never Miss That In
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<sistemas@vinoseleccion.coi	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<simutant@earthlink.net>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<pgabriel@sympatico.ca>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<mbrowne30@hotmail.com>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<kingrick10@aol.com>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<kimdives@msn.com>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<kifor@mail.ru>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<jemeni@hotmail.com>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<gpinoncely@vie-et-veranda.	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<gparks@mail.com>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<gmoncada@usa.net>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<dmorrison@mta.ca>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<dlarsson@vh.net>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<dkorn@dacomtech.com>	FW:>Re: Spruce u
★	07/24/2002 06:27 PM	49.0	ej1b@hotmail.com	<dkaydoc@msn.com>	FW:>Re: Spruce u

Figure 6-13 Workflow allows for spam management

6.1.6 Other anti-spam products for Notes and Domino

This section lists other anti-spam products for Notes and Domino that we were aware of at the time of writing. For more information, see the individual company Web sites.

- CS MIMEsweeper for Domino from Clearswift Ltd

  `http://www.mimesweeper.com/products/msw/domino/default.asp`

- GFI MailEssentials for Exchange/SMTP 7 from GFI Software Ltd

  `http://www.gfi.com/mes/index.html`

- GroupShield for Domino from Network Associates (McAfee)

  `http://www.mcafeeb2b.com/products/groupshield-domino/default.asp`

6.2 Anti-spam server and gateway products and services

This section covers anti-spam products that are separate server products or operate on the gateway. By using these products you can further address the spam problem. Anti-spam server and gateway products aim to prevent spam messages ever entering the company's e-mail system. Often the vendors of these products offer content filtering, connection management, and other related functionality as a service. Some vendors also provide products and services that prevent directory harvesting and denial of service attacks, as well as virus protection.

6.2.1 BrightMail Anti-Spam 4.0 from BrightMail, Inc.

BrightMail Anti-Spam 4.0 provides options for Internet Service Providers and enterprises that wish to install an on-premises server to handle local inbound scanning for viruses and spam mail.

BrightMail hosts dummy e-mail accounts throughout the world that receive spam messages. Suspected spam messages are analyzed for content by BrightMail's Logistics and Operations Center (BLOC); if they are determined to be spam, they are added to BrightMail's anti-spam database. The Anti-spam Enterprise on-premise server functions as a client in a client-server environment with the on-premise server installed at your site acting as client to the BLOC. The BLOC provides updates to your on-premise server, downloading the anti-spam database on a scheduled basis.

BrightMail's on-premise product acts as a “gateway” product, meaning that it operates in front of your Lotus Domino servers. It can intercept and scan messages before they enter into your Domino system. Inbound message attachments are first scanned for viruses, then they are processed by the anti-spam filter module. If the message is determined to be spam, it is moved into a separate junk mail folder. If not, the message is then passed on to the custom message filter, and if not blocked during this process, it is delivered to the end user as a valid e-mail message.

Administrators can create custom filters using a script language called “sieve.” Commands are available for complete control of inbound messages, including generating replies, filing messages, redirection to a different e-mail address, and acceptance or discarding of messages. Custom rules can be configured to handle attachments and can act on attachments based on attachment type and size. More information can be found on the BrightMail Web site at:

http://www.brightmail.com/enterprise-as.html

6.2.2 ActiveState PureMessage

PureMessage from ActiveState is a comprehensive e-mail filtering system for spam protection, virus protection, and corporate policy enforcement. Configurable filters provide full control over the security and usage of any corporate e-mail system at the gateway level, protecting against productivity loss, network downtime, and vulnerability of informational assets caused by unsolicited or malicious e-mail.

PureMessage spam filter

The PureMessage spam filter safely identifies spam using a sophisticated suite of heuristics, spam directories, and spam signatures. According to ActiveState, customers experience over 80% spam filtering immediately upon installation, increasing to accuracy levels in excess of 95% after basic filter tuning. To maintain effectiveness against the evolving tactics of spammers, PureMessage includes regular updates to the tests developed by the ActiveState anti-spam response team. The result is an inbox clear of unsolicited e-mail.

The PureMessage system promotes end user productivity, protects against liability caused by circulation of offensive materials, increases network efficiency, and increases server security by protecting against denial of service and directory harvest attacks. Flexible configuration options allow organizations to uniquely define their spam identification and handling policies (for example delete, quarantine, and archive).

How PureMessage spam filtering works

E-mail enters an organization via the Internet and is received by PureMessage through its integrated mail transfer agent. E-mail is then filtered through a comprehensive series of positive/negative tests to determine a spam probability rating. Positive tests identify characteristics of legitimate messages, while negative tests identify characteristics of spam messages. When combined, they yield extremely efficient spam identification. Following are examples of the types of tests conducted to identify the probability that a message is spam:

- Basic keywords and phrases in the e-mail message, like AMAZING or casino
- Malformed headers or addresses in the e-mail message header, such as missing headers, invalid date, suspicious list of recipients, recipients commonality ratio, forged “Received” headers
- Pornography rules - approximately 40 positive and negative tests to prevent false positives
- HTML form use in e-mail body
- Usual spam claims and unsubscribe URLs, such as “to be removed..”, “we do not send...”, “http://...?remove=...”
- Complex text patterns for common spam content, such as (?:You (?:were sent|have received|are receiving)|You're receiving).{0,15}(?:message|e-?mail)s? because - if you (?:(?:want|wish|care|prefer) not to |(?:don't|do not) (?:want|wish|care) to)(?:be contacted again|receive (any)?\s*(?:more|future|further) (?:e?-?mail|messages?|offers|solicitations))
- Foreign character sets detected in headers and body
- Spam phrase identification. Count the ratio of frequent spam phrase occurrences, such as “credit card,” “loan you,” “multi level” and compare it with threshold value
- Unique identifiers, tags in the message/subject
- Suspicious text formats, for example a gap in text ("G E T R I C H F A S T"), lines of yelling (BUY NOW!!!)
- Nigerian scam, multiple patterns

  The Nigerian scam always mutates, and can be detected by pattern matching only.

- Network checks such as no MX record for sender's domain
- Realtime Blacklist checks, 10 RBL systems supported

  RBL tests don't uniquely identify a message as spam. They act as a contributing test to the probability that a given message is spam.

- Distributed checksum checks

  Razor network check supported. Provides peer-based identification of spam messages.

6.2.3 Trend Micro Inc. products

Spam Prevention Service software

Spam Prevention Service software from Trend Micro is a on-site anti-spam application designed for the enterprise. It resides at the gateway, where it monitors incoming SMTP e-mail and identifies spam with a 90% to 95% accuracy rate, according to Trend Micro Inc.

The Spam Prevention Service software is scalable, works with all common Message Transfer Agents, and supports Windows 2000, .Net, Solaris, Red Hat Linux, and SuSE Linux.

In conjunction with Trend Micro ScanMail Lotus Notes and/or Trend Micro InterScan Messaging Security Suite, the Spam Prevention Service provides comprehensive protection against blended virus, spam, and content security threats.

InterScan Messaging Security Suite

InterScan™ Messaging Security Suite provides comprehensive virus protection, flexible policy-based content filtering, and easy-to-use management tools to help monitor and control SMTP and POP3 traffic at the messaging gateway. It helps safeguard against the loss of intellectual property and confidential information, minimizes server congestion, and helps maintain employee productivity. InterScan Messaging Security leverages Trend Micro Control Manager™, a platform-independent management tool, for centralized updating, consolidated reporting, and remote configuration capabilities.

Key features include:

- High-performance virus protection
- Customizable policy-based management
- Content filtering which protects both network and business integrity
- Trend Micro enterprise protection strategy support
- Advanced mail handling
- Denial of service protection

More information can be obtained from Trend Micro’s Web site at:

`http://www.trendmicro.com`

6.2.4 Other anti-spam server or gateway products and services

- Postini Perimeter Manager from Postini Corporation

  `http://www.postini.com/services/corporations.html`
- EasyLink MailWatch from EasyLink Services Corporation

  `http://www.easylink.com/services_north_america/1_5_boundary.cfm`
- SkyScan AS from MessageLabs

  `http://www.messagelabs.com/page.asp?id=568`

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information on ordering these publications, see "How to get IBM Redbooks" on page 100.

- *Upgrading to Notes & Domino 6,* SG24-6889
- *Lotus Domino 6 for Linux,* SG24-6835
- *Lotus Domino 6 for iSeries Implementation*, SG24-6592
- *Lotus Domino R5 for Sun Solaris 8*, SG24-5969

Referenced Web sites

These Web sites are also relevant as further information sources:

- Lotus Developer Domain:

  `http://www.lotus.com/ldd`

  Especially articles:

  "Notes spam mail filtering: Mail file rules" by Graig Lordan

  "Notes spam mail filtering: Domino Messaging Restrictions and Controls" by Graig Lordan
- Hoaxbusters, CIAC Hoax Pages. Lists and categorizes many hoax and chain mail messages and more. If you receive a suspicious mail message, you can search this site to see if it is a hoax.

  `http://hoaxbusters.ciac.org`
- Urban Legends lists hoaxes and chain mails as well as many urban legends and stories.

  `http://www.urbanlegends.about.com`
- Granite Software, Inc. Creator of spamJam for Lotus Notes and Domino:

  `http://www.gsw.com`

- Eagle Technology Consultants, LLC. Creator of SpamEraser for Lotus Notes and Domino 6:

  `http://www.eagletc.com`

- Spamcop - DNS Blacklist service provider:

  `http://www.spamcop.com`

- Mail Abuse Prevention Systems, LLC - DNS Blacklist service provider:

  `http://www.mail-abuse.org`

- The Spamhaus Project - DNS Blacklist service provider:

  `http://www.spamhaus.org`

- The Open Relay Database (ORDB) - DNS Blacklist service provider:

  `http://www.ordb.org`

- OsiruSoft Research & Engineering - DNS Blacklist service provider:

  `http://www.osirusoft.org`

How to get IBM Redbooks

You can order hardcopy Redbooks, as well as view, download, or search for Redbooks at the following Web site:

ibm.com/redbooks

You can also download additional materials (code samples or diskette/CD-ROM images) from that site.

IBM Redbooks collections

Redbooks are also available on CD-ROMs. Click the CD-ROMs button on the Redbooks Web site for information about all the CD-ROMs offered, as well as updates and formats.

Index

IBM Redbooks

Lotus Domino 6 spam Survival Guide for IBM eServer

(0.2”spine)
0.17”<->0.473”
90<->249 pages

Lotus Domino 6 spam Survival Guide for IBM eserver™

Avoid, block, and manage spam with server mail rules and mail file rules

Anti-spam features of Domino 6

Third-party anti-spam products

In this IBM Redbook we describe how you can use IBM Lotus Domino 6 to prevent and manage "spam."

We begin by describing and categorizing spam, which is the commonly used term for unsolicited commercial e-mail. We discuss ways to prevent spam, outlining different techniques available to avoid and block spam.

We then explain how anti-spam control and management work can be divided between servers, between server tasks, and between administrators and end users. We also describe the anti-spam architecture of the Domino 6 messaging environment.

Anti-spam features of Domino 6 are presented in detail. They include the ability to control connections from spammers and the delivery of spam, and protecting against the use of your server as an open relay. We also discuss using mail file rules and server mail rules to prevent spam.

Finally, we highlight some of the business partner products available to further address the spam problem. These products fall into two categories: those that run on a Domino server, and those that operate as separate anti-spam servers and gateways. We include a number of examples of each type, along with references to help you obtain more information directly from them.

This redbook is written primarily for Lotus Domino administrators who want to prevent and manage spam in their environments. It is also useful as a basic introduction to the topic of spam.

SG24-6930-00 ISBN 0738429457