Lotus Developer Domain
The Technical Resource for Lotus software
LDD Today

Level: Beginner
Works with: Notes/Domino
Updated: 01-Apr-2003

by
Dick
McCarrick

We've all received them—unwanted emails containing unsolicited advertisements, chain letters, offers too good to be true, or worse. Collectively these messages are known as spam mail, and they clutter your inbox, wasting your time and your computer's memory. Many people find they receive more spam than legitimate mail. And most of us have at one time or another deleted some important email while manually removing spam messages. Increasingly, dealing with this problem has become more than a mere annoyance—it's become a productivity issue. And recent surveys indicate it's rapidly getting worse with spam comprising an ever larger percentage of overall mail received.

Fortunately, Notes/Domino 6 includes several important features that help prevent spam mail from entering your organization and reaching your users. This article discusses these features. We start with an overview of spam and general techniques for preventing it. Then we examine in detail Notes/Domino 6 anti-spam features and how you can use these to help minimize the impact of unsolicited email in your environment.

This article assumes that you're an experienced Domino administrator or Notes user, familiar with general Notes/Domino features and terminology. For more information on Notes/Domino 6, see the **October 2002 Notes/Domino 6 special issue** of *LDD Today.*

Spam prevention primer

For many users, trying to explain exactly what comprises spam mail is an "I can't define it, but I know it when I see it" situation. This may work for humans, but computers need more specific rules, especially in a world where one person's spam is another's piece of vital information. Otherwise, you run the risk of "false positives," excluding mail messages your users need because they erroneously fall into your too-broad definition of spam.

There are several ways to prevent spam from reaching users. These include using an outside mail filtering service, dealing with spam internally at the server and/or user level, and (best of all) avoiding becoming a target in the first place.

Third-party services

Many organizations use a third-party mail filtering service. This prevents unwanted mail from ever reaching your servers and internal corporate network, which helps keep these free for real work. This method can be especially appealing for administrators who may not have the time or inclination to manage an ongoing enterprise-level anti-spam campaign. On the downside, using an outside service obviously costs money. It also gives you less direct control, which can result in legitimate mail being classified as spam and mistakenly discarded before you ever get to see it (or conversely, mail you don't want getting through to your users).

Blocking spam at the server and user level

So even if you use a third-party mail filtering service, you may still want to implement internal anti-spam measures. These can be server-based or user-based. Rejecting spam at the server helps prevent mail clutter and lets your users focus on more productive matters. Domino 6 offers a number of server options for avoiding spam, including

© Copyright IBM

server mail rules, relay controls, and DNS blacklists. You can also allow your Notes mail users to manage their own anti-spam efforts through Notes functionality such as mail file rules. The next sections of this article discuss these and other Notes/Domino 6 anti-spam features.

Preventing spam at the server level avoids users having to do this themselves. But as with third-party services, stopping spam at the server is usually a "broad brush" technique, sometimes eliminating desired mail along with the unwanted. User-based prevention allows users to customize their individual mail files to accommodate their personal definitions of spam, thus helping minimize the possibility of rejecting legitimate email. But many administrators may not want their users making anti-spam decisions on their own. Plus, the load on your servers could be greater because they will still have to handle the incoming spam traffic. Therefore, relying solely on user level blocking is usually only recommended for those lucky environments where spam is not a major problem.

Harvesting
Of course, it can be argued the most effective way of preventing unwanted messages is for spammers to never discover your email address. Unless you're prepared to swear off email for life, it's probably impossible to completely prevent this from happening—there seems to be an infinite number of spammers, and the tricks they invent to find you are varied and numerous. Nevertheless, there are actions users can take to minimize their exposure. Spammers often use a process called "harvesting" to collect email addresses. Harvesting can take several forms, including obtaining addresses from Web page traffic, user groups, subscriber lists, and so on. There are a number of ways users can minimize the chances of this happening to them. We discuss these later in this article.

Stopping spam with the Domino 6 server

As mentioned earlier, Domino 6 offers several features designed to block unsolicited mail at the server and to prevent it from reaching your users. These include:

- Server mail rules
- DNS blacklist filters
- Relay controls and enforcement
- Other Domino mail restrictions

The following sections present brief overviews of these. For detailed information on these and other Domino 6 features designed to help you control spam mail in your organization, see the **Domino 6 Administrator help**.

Server mail rules
Server mail rules are an important component of Domino spam control functionality. Server mail rules were first introduced in R5. (See the *Iris Today* article "**Notes spam mail filtering: Notes mail rules**.") In Domino 6, server mail rules have been significantly enhanced to run on MAIL.BOX and to process all messages on the server.

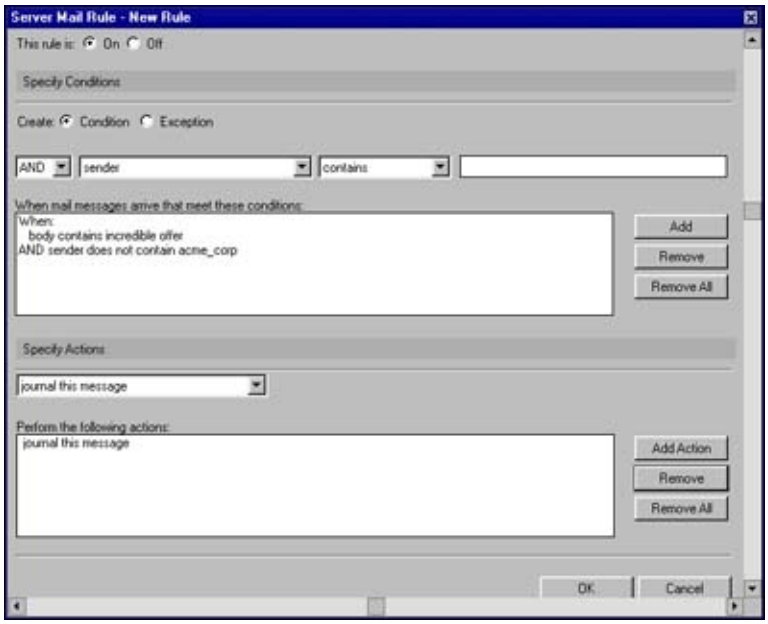
With server mail rules, you can create content filtering for a server that specifies actions to take on certain messages. When a new message meeting the condition you define arrives in MAIL.BOX, Domino automatically performs the designated action. Server mail rules can use the content of the header or body of the message (or even its form) to determine whether or not to act on it. The large number of possible combinations of conditions and actions gives you a great deal of control over which messages you allow into your mail environment.

You can instruct the server to automatically:

- Refuse to accept or deliver a message
- Move it to a "graveyard" or "quarantine" database
- Journal the message
- Change the routing state of a message

You create server mail rules through the Server Configuration document in the Domino Directory. Open the Configuration document and go to the Router/SMTP - Restrictions and Controls - Rules tab. You can define up to 100 rules for your server. Mail rules consist of two parts. The first contains the conditions the mail message needs to meet to be considered spam. The second contains the actions the server performs when a message arrives meeting these conditions. This screen displays the options available when you create a server mail rule:

© Copyright IBM



With server mail rules, you can have your server automatically handle mail in a variety of situations. You can create rules to block spam mail or to intercept messages with suspicious content (for instance, anything with subjects containing words such as "incredible offer" or "free prize," or mail originating from a known source of spam).

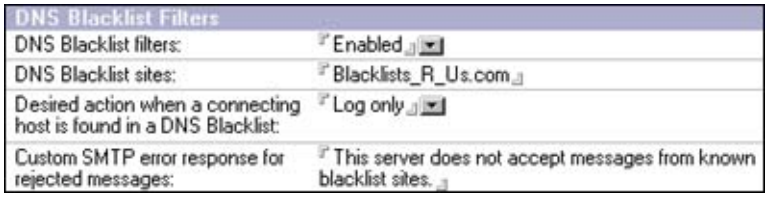
Note that server mail rules do involve some performance considerations. Server mail rules affect all messages sent to the server, and therefore, could have some impact on response time. After implementing server mail rules, you should monitor them frequently, refining conditions or changing actions as necessary. For more information on Domino 6 server performance with mail rules, see the *LDD Today* Performance Perspectives column "**Domino 6 server mail rules**." However, most sites should find whatever performance impact they may encounter more than offset by the fact mail rules save disk space, reduce network traffic, and help users avoid wasting time with spam mail.

DNS blacklist filters

An important new spam prevention feature introduced in Domino 6 is DNS blacklist filtering. DNS blacklists are databases that keep a record of Internet SMTP hosts that are possible sources of spam or that permit third-party, open relaying. (Open relays leave systems accessible and could be used by a spammer to flood the Internet with junk mail. We talk more about relaying later in this article.) When you enable blacklist filters, for each incoming SMTP connection Domino performs a DNS query against the blacklists at the specified sites. If a connecting host is found on the list, you can instruct Domino to report the event in a console message and log entry, to add a special Notes item to flag the message, or to reject the message altogether.

There are a number of publicly available (and private, paid subscription) services that maintain DNS blacklists. Each blacklist service has its own set of criteria for adding servers to its list, some more restrictive than others. You should be fully acquainted with the criteria of each blacklist service you use to determine what mail will and will not get through to your site to ensure that messages being rejected are in fact unwanted.

DNS blacklist filtering is configured and enabled in the Router/SMTP - Restrictions and Controls - SMTP Inbound Controls tab of the Configuration Settings document:



© Copyright IBM

This tab includes fields for:
- Enabling DNS blacklist filters
- Selecting blacklist sites
- Defining the action the server should take when it receives email from a blacklisted sender
- Creating a custom SMTP error response for rejected messages

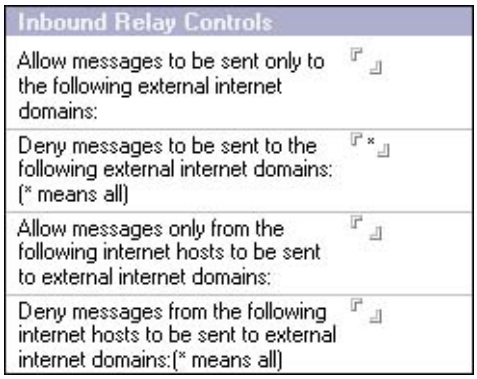
As with server mail rules, using DNS blacklist filters places some additional demand on servers. To help minimize this impact, Domino performs blacklist checks only on hosts subject to relay checks, as defined in the SMTP Inbound Controls tab of the Configuration Settings document. Hosts authorized to relay are exempt from blacklist checks. For messages sent from all other hosts, the server must contact each blacklist site listed in the Configuration Settings document and determine if the host is included. In addition, relay controls (described in the next section) require a reverse DNS lookup. This is performed when the inbound connection is first accepted. Additional DNS queries are then performed for each DNS blacklist site specified in the Server Configuration document. This requires both time (especially if you select a large number of blacklists to check) and additional server workload. The more sites specified, the longer it can take to perform the lookups and the greater the risk that a timeout will occur. Therefore, we recommend limiting the number of enabled DNS blacklist sites to one or two to prevent the connecting host from timing out.

Again, we recommend you monitor your site closely after enabling DNS blacklist filters both to check the efficacy of your selected blacklist sites and to gage server performance.

Relay control and enforcement
One of the more ingenious (or devious) techniques used by spammers is to relay mail through a third-party server to disguise the origin of the message. This is undesirable for several reasons. First, it thwarts anti-spam measures because it appears that the mail is being sent by a trusted host. Second, it can place additional overhead on your server as it passes messages from one host to another, often without your knowledge. Worst of all, it can make your site look like a spammer—you could even end up on somebody's blacklist! This can happen if your server has a relay open that allows anyone to relay mail through it.

Setting relay controls
Fortunately, Domino 6 offers many options for controlling mail relaying on your servers. These let you restrict relay access to only authenticated external hosts by:
- Allowing/denying messages to be sent to selected external Internet domains
- Allowing/denying messages from selected Internet hosts to be sent to external Internet domains

Relay controls are defined in the Configuration Settings document's Router/SMTP - Restrictions and Controls - SMTP Inbound Controls tab:



In R5, when you initially set up your Domino server, no relay restrictions were applied; all hosts were allowed to relay through the server and all destinations could be relayed to. In Domino 6, relaying is denied by default. You can then use the options shown in the preceding illustration to determine the relay destinations to which your server can or cannot send mail, and the sources from which the server can and cannot accept relays.

Inbound relay enforcement
Another new Domino 6 anti-spam feature is inbound relay enforcement. This set of options gives you additional control over the hosts allowed to relay through your Domino server. You can instruct Domino to perform relay checking for all hosts, external hosts only, or disable all relay checking. This lets you further exclude specific hosts

© Copyright IBM

from being checked against your inbound relay controls options. (See the preceding section.)

You can exempt hosts from relay enforcement based on:

- *Domain location*
  Domino by default enforces relay controls for hosts outside the local Internet domain only. You can enforce stricter control by applying these controls to all connecting hosts. You can also relax enforcement to stop Domino from performing relay checks, although we do not recommend doing this. In particular MX hosts should not disable relay controls because this casues an open relay condition, making it possible for spammers to abuse your server and potentially result in your server being blacklisted.

  You can extend enforcement by applying relay restrictions to both internal and external hosts. This gives you more secure and controlled routing. In addition, you can enable relay enforcement for internal hosts if your site includes a Domino SMTP server receiving mail from a firewall server.

- *Authentication status*
  Domino by default applies relay controls to authenticated SMTP sessions. You can exempt all authenticated users from relay checks.

- *Host name or IP address*
  All external hosts are by default subject to relay controls. You can specify a list of IP addresses or host names exempt from relay checks.

Other Domino 6 anti-spamming features
In addition to mail rules, DNS blacklists, and relay controls, Domino 6 offers other functionality that can be useful in your battle against spam mail.

Restricting users from receiving Internet mail
The Configuration Settings document includes three options that let you specify the users for whom the server accepts mail sent over SMTP connections. One option enables the server to verify the intended recipient exists before accepting a message. The other two let you specify the Internet addresses that can and cannot receive mail:

- *Verify that local domain recipients exist in the Domino Directory*
  This new Domino 6 feature performs real-time lookups against configured Domino Directories during the actual SMTP conversation. If the local domain recipient does not exist in the directory, the message is rejected during transfer and is not stored in the mailbox. This saves administrators from having to delete thousands of dead messages per day for each SMTP server. There is no additional performance cost for nonexistent users, as the router would perform these lookups anyway. The only cost is the additional lookups performed for valid users. Unfortunately, this feature also allows spammers to validate harvested addresses because they get to see which messages are rejected and which are not.

- *Allow messages intended only for the following Internet addresses* and *Deny messages intended for the following Internet addresses*
  These two options allow you to explicitly specify Internet addresses that can and cannot receive mail. Use this option judiciously, however. You don't want to prevent Internet mail from reaching users who need it. Also, maintaining the names on the allow/deny lists may require a significant amount of attention.

Mail journaling
Mail journaling (introduced in Domino 6) isn't an anti-spam feature, but it can be useful in monitoring spam traffic. Journaling captures some or all messages handled by the router and saves copies of selected messages to the Domino Mail Journaling database (MAILJRN.NSF). Used in conjunction with mail rules, journaling lets you capture questionable emails and copy them to a secure place for examination.

How Domino puts it together
A thorough, detailed examination of how Domino uses the data you enter into the Configuration Settings document to prevent spam is beyond the scope of this article. However, it may be useful to take a quick look at how this works. Domino 6 inbound relay controls, DNS blacklist filters, and inbound connection controls allow or deny mail based on who sent the message. To do this, the server must identify the connecting host's IP address, host name, and Internet domain. Domino obtains this information from two places:

- *The IP stack*
  When a host connects to Domino's SMTP service, the host passes its IP address to Domino's IP stack. The SMTP service reads the IP address directly from this stack.
- *The Domain Name Service (DNS)*
  For Domino to obtain host name and domain information, it must access the DNS and locate the PTR record for the connecting host. (PTR records resolve IP addresses to host names.) When requesting the PTR record,

© Copyright IBM

> Domino's SMTP listener performs a reverse lookup to the DNS. This lookup returns a host name from which Domino obtains the domain name of the connecting host and compares this to the list of local Internet domains in the Global domain document. Domino considers hosts from domains listed in the Local primary Internet domain or Alternate Internet domain aliases fields as part of the local Internet domain. Other hosts are defined as external hosts. If no Global Domain document exists, Domino parses the Fully Qualified Internet Hostname specified in the Server document.

For more information on how Domino 6 processes anti-spam information, see the **Domino 6 Administrator help**. You can also consult the IBM Redbook, **Lotus Domino 6 spam Survival Guide for IBM eserver**.

User-based spam prevention

As we mentioned in the previous section, server-based spam locking will typically form a critical component of your overall anti-spam strategy. However, the Domino server by necessity defines spam in broad and general terms. To prevent "throwing out the baby with the bath water" and rejecting too many legitimate messages, most administrators must be careful not to be overly restrictive in their use of server mail rules, DNS blacklist filters, and other server functionality. As a result, a certain percentage of unwanted mail often manages to slip through, especially as spammers evolve new methods for circumventing blocking measures. So even though your site employs server-level spam prevention (and perhaps even a third-party filtering service), it's probably wise to also implement spam blocking at the user level as a final barrier for spammers.

The primary way to do this is through Notes mail file rules. These allow users to isolate email by sender address, domain, subject, or message content. This helps control incoming email messages and is also useful for managing your legitimate email. Note that although mail file rules are created and managed on the Notes client, they are evaluated and enforced on the Domino server. Mail file rules do not run on the Notes client.

To create a mail file rule, open your mail database and click Tools - Rules in the navigation pane:

Click the New Rule button to display the New Rule dialog box. (This is the same as the Server Mail Rules dialog box shown in the previous section.) Notes mail file rules are similar to server mail rules in that they specify certain conditions that identify a message as possible spam and actions you want performed when a message arrives meeting these conditions (although these rules apply only to individual mail files).

Specifying conditions

The Specify Conditions section of the New Rule dialog box defines:

- The part of each message to check, for example the sender or subject field
- The state, such as *contains* or *is*
- The criteria to check, for instance, a particular name or word

Specifying rule actions

After you define the rule conditions, you select the actions to take for messages that meet these conditions. Options include:

- Move to folder

© Copyright IBM

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

You can select multiple actions (unless, of course, you choose Delete). By isolating likely spam email to this level of specificity, you can control how you want each email handled. The most objectionable email can be deleted, while other questionable messages can be examined and recovered as appropriate. This lets individual users use their personal judgement and taste to define exactly what they consider spam mail, and what they want done with it, to a level difficult or impractical if done at the server.

As with server-based mail rules, you should monitor the success of your Notes mail file rules after you implement them. For example, if you want mail from particular hosts to be deleted, you may have no idea how well these rules are working unless you examine the server log and see whether or not these hosts are in fact attempting to spam you. Also note that all rules are evaluated with every message; rule processing continues even if one or more rules are applied to a message. Therefore, we suggest you plan your rules appropriately and carefully.

For more information on Notes 6 mail file rule features, refer to the IBM Redbook, **Lotus Domino 6 spam Survival Guide for IBM eserver**. Also see the **Notes 6 Client help**.

Avoiding harvesting

As we noted at the beginning of this article, spammers often obtain email addresses through various methods collectively called harvesting. It may be virtually impossible to make your users completely invisible to harvesting, but Domino does offer features that can at least make life more difficult for the spammers.

For example, spammers often use techniques that rely on a great deal of rote processing and guesswork to determine email addresses. These often result in a high number of wrongly addressed, undeliverable messages. By saving and examining undeliverable mail received at your site, you may for example discover many of these are coming from a single source. If these messages all contain the same content, and that content is unsolicited and undesired, you've discovered another spammer—and another host to avoid in the future.

You can also advise your users how to avoid having their email addresses harvested by doing one or more of the following:

- Refrain from standard email addresses for domain name registration contacts. Instead, create special accounts to manage registration.
- Maintain a “junk” account from a free provider to use specifically for newsgroup or commercial Web site interaction.
- Don't use organizational addresses when dealing with “e-invite” or “postcard” services. (In fact, it's probably wise never to do this unless the correspondence is strictly business-related.)
- Set up a mail-in mailbox for public feedback mail (which attracts spammers like flies, trust us).
- Avoid posting addresses on newsgroups or public Web discussions.
- Don't publish addresses in public directories.

These and similar measures can help deal with spam the best way possible: preventing it from being sent to you in the first place.

Planning your anti-spam campaign

The previous sections examined Notes and Domino features designed to help you battle spam mail. However, even the best functionality is of limited use if not carefully and logically deployed. So to help you use these features effectively, this section touches upon a few things to consider when planning your anti-spam campaign.

Choosing a strategy

Before deciding which features are most useful for your site, talk to your users to determine how big a problem unsolicited email is for them. Do they receive many spam messages? Would getting rid of it be worth the risk of the occasional real message getting rejected? Would they mind managing their own mail file rules? The answers could determine whether you choose a server-based approach, user level measures, or both. And whatever techniques you choose initially, be sure to perform monitoring and follow-up to ensure your strategy is working.

Informing users

An educated user is usually the one least troubled by unsolicited mail. Users who know how to avoid the risk of harvesting help reduce the amount of spam that comes through your systems. It also helps to have a corporate

© Copyright IBM

anti-spam policy to motivate all users to take this problem seriously and do all they can to help minimize it. Advise your users about the costs of spam and how it prevents them (and your organization) from being as productive as possible.

Building Notes mail file rules
When developing Notes mail file rules, consider all mail you receive. Minimize the risk of false positives because deleting even one critical email may not be worth preventing 100 spam messages from getting through. As you become more experienced with Notes mail file rules, re-examine and refine them to fit your needs.

Managing your ongoing anti-spam effort
Unfortunately, there's no single way to eliminate all possible spam, other than shutting down your network completely. So most sites will find themselves picking and choosing from all available options, then carefully keeping an eye on the results to determine whether they're effective or need tweaking to keep up with the latest spamming trends. This will take time and effort and needs to be carefully tracked. If you find yourself expending too much work and cost, you may decide to hire a third-party service to manage spam blocking for you. Also, stay current with all the latest anti-spamming technology as it gets developed. New Notes/Domino updates may become available to help thwart spam delivery.

Down with spam!

Spam mail, like viruses and hackers, is probably an inevitable consequence of the age of telecommunications. However, this doesn't mean that you're powerless to do anything about it. In this article, we looked at several important spam protection features in Notes/Domino 6, how they work, and how you can use them to help keep your email environment free from clutter. We hope you found this useful.

No one spam prevention method is perfect, but by using Notes/Domino 6 anti-spamming features to your advantage, your users should find spam a rarer occurrence. The best strategy for your site depends on the choices you and your users make. Be sure to monitor the effectiveness of your strategy, and adjust it as needed. Set aside regular time to review how well your anti-spam measures are working and remain open to changing these if necessary.

Of course, every new spam blocking measure seems to eventually result in a counter measure invented by the spammers. (If only this energy were channeled towards more productive goals.) The Notes/Domino team is well aware of this and working hard to stay ahead of the spammer community. As new spam protection features and methods are perfected and released, we'll be covering them in future articles to help you—and your users—deal with this ever-increasing problem.

© Copyright IBM