Managing inbound spam in Lotus Domino 6

Presented by the Lotus Developer Domain

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

Table of Contents

If you're viewing this document online, you can click any of the topics below to link directly to that section.

Section 1. Introduction

Should I take this tutorial?

This tutorial is for Domino/Notes administrators who want control over spam or junk mail. It covers many of the new features in Domino 6 for blocking and managing spam. This tutorial is focused on helping you get these anti-spam features up and running quickly.

You should be familiar with the following:

- Domino systems administration
- E-mail technology and Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)
- Transmission Control Protocol/Internet Protocol (TCP/IP)

What is this tutorial about?

Most e-mail users are familiar with spam or junk mail: Unsolicited e-mail that is usually sent in bulk to huge lists of e-mail addresses. At best spam is a nuisance; at worst it is a serious problem that can negatively impact an e-mail user's productivity and an e-mail system's performance.

Lotus Domino 6 is an excellent platform for electronic mail/messaging, as well as application development. As a messaging platform, Domino is one of the most powerful and flexible messaging products on the market. The anti-spam features of Domino 6 are one example of the sophisticated messaging capabilities of Domino.

Fighting spam is not an exact science. You'll find the most effective anti-spam weapons are the ones that change as fast as spam does, such as DNS blacklist filtering and verification of recipients against your directories. These features are automatically and dynamically maintained by external service providers and by your internal administrators. Anti-spam techniques that use rules that are too strict and can block legitimate mail, or require too much care and feeding to be effective, should be used with caution.

This tutorial focuses on using specific features of Domino 6 to control, block and manage spam. The most important and effective tools and techniques are covered first. We've included the specific configurations that will work against spam and point out the downsides, simply and concisely. This tutorial covers the following Domino server 6 anti-spam capabilities:

- Preventing open mail relays
- Using DNS blacklist filters
- Verifying inbound recipient names
- Verifying connecting host names
- Verifying sender's domain name
- Using server mail rules

Tools

In order to complete all the steps in this tutorial, you need to have the following applications installed:

- *Lotus Domino 6 Server*
- *Lotus Domino Administrator 6 client*
- *Lotus Notes 6 client*

About the author

Kenneth Adams, a *Studio B* author, has been in the Information Technology field for over 17 years and has been working with Lotus technologies for over 8 years. Ken is a Principal Certified Lotus Professional (PCLP), certified in both Lotus application development and systems engineering/administration, and certified in Lotus Domino Messaging Administration/Migration. His development experience includes Domino/Notes Designer, LotusScript, HTML, JavaScript, CSS and others. Ken also has a solid foundation in LAN/WAN technology having been network certified with a Master CNE (Certified Novell Engineer) and having many years experience in networking. Ken has worked with Domino & Notes since R2, and with practically every Lotus product including Sametime, QuickPlace, Discovery Server, Domino.Doc, Enterprise Integrator and more. Ken was a contributing author on the books *Special Edition: Using Lotus Domino/Notes R5* and *Professional Developer's Guide to Domino*. He can be reached at: *kadams@kennethadams.com*, or visit his Web site at: *http://kennethadams.com*.

Section 2. Preventing open mail relays

What is an open mail relay?

A mail server that accepts mail from any mail source outside the server's local domain and relays it to any external domain is called an open relay. If your mail servers act as open relays, any spam message relayed through one of your mail servers appears to originate from your Internet domain, making it look as if your organization is linked with the source of the spam.

Open relays are often targeted by Internet mass-mailers. These spammers use open relays as intermediaries between themselves and their target recipients. They use open relays to anonymously distribute huge quantities of mail.

This section shows you how to lock down your mail system to prevent opens relays. After you have locked down your mail system by preventing relaying, we will cover more advanced spam weapons such as DNS blacklist filtering and verification techniques later in this tutorial.

Why prevent open mail relays?

Leaving your mail servers open to use by anonymous third parties is generally considered irresponsible because spammers can easily exploit them. Not only does relaying spam reflect badly on your organization, but there are other more serious and costly consequences, including:

- **Blacklisting**: Your mail servers will get blacklisted if they are left open. Because DNS blacklist filtering is becoming a common method of blocking spam, your users will not be able to send mail to other mail systems that are protected by DNS blacklist filtering.
- **Degraded Performance**: Relaying mail consumes server resources and network bandwidth, reducing your system's ability to handle legitimate mail. As mail delivery slows, users, administrators, and help desk personnel are faced with service delays or even interruptions.

Technically speaking, preventing mail relays does not help you eliminate spam, but it is an absolutely critical first step in setting up an e-mail system and being a responsible e-mail citizen. The following panels will help you to verify that Domino is configured to prevent relays of all types.

Configuration Settings documents

Many of the settings covered in this tutorial are contained in one or more documents known as Configuration Settings documents. You can have several Configuration Settings documents -- one for each Domino server, for a group of servers, or for all servers. You can create as many documents as you need. If you'd like to learn more about how Configuration Settings documents work, see the Lotus Domino Administrator 6 Help (see Resources on page 27).

The Configuration Settings document or documents are stored in the Domino Directory database on the Domino server and are used by Domino servers to configure many functions, including mail routing, LDAP, iNotes Web access, IMAP, SNMP and more. Typically, Configuration Settings documents are created when you install Domino server, but if not, you must create them, which is explained in the next panel, Edit or create a Configuration Settings document on page 6 .

To check to see if you have a Configuration Settings document, you need to open the Server Configurations view of the Domino Directory. Depending on which you prefer, you can work with the Configuration Settings documents using the Lotus Domino Administrator client or the Lotus Notes client. Most of Lotus' own product documentation on administration topics is written based on using the Domino Administrator client. Most experienced Domino administrators who have been using Notes since R2 (such as old timers like me) use the Notes client for configuration tasks because it allows quicker and more direct access to many administration databases. The figures in this tutorial use the Notes client.

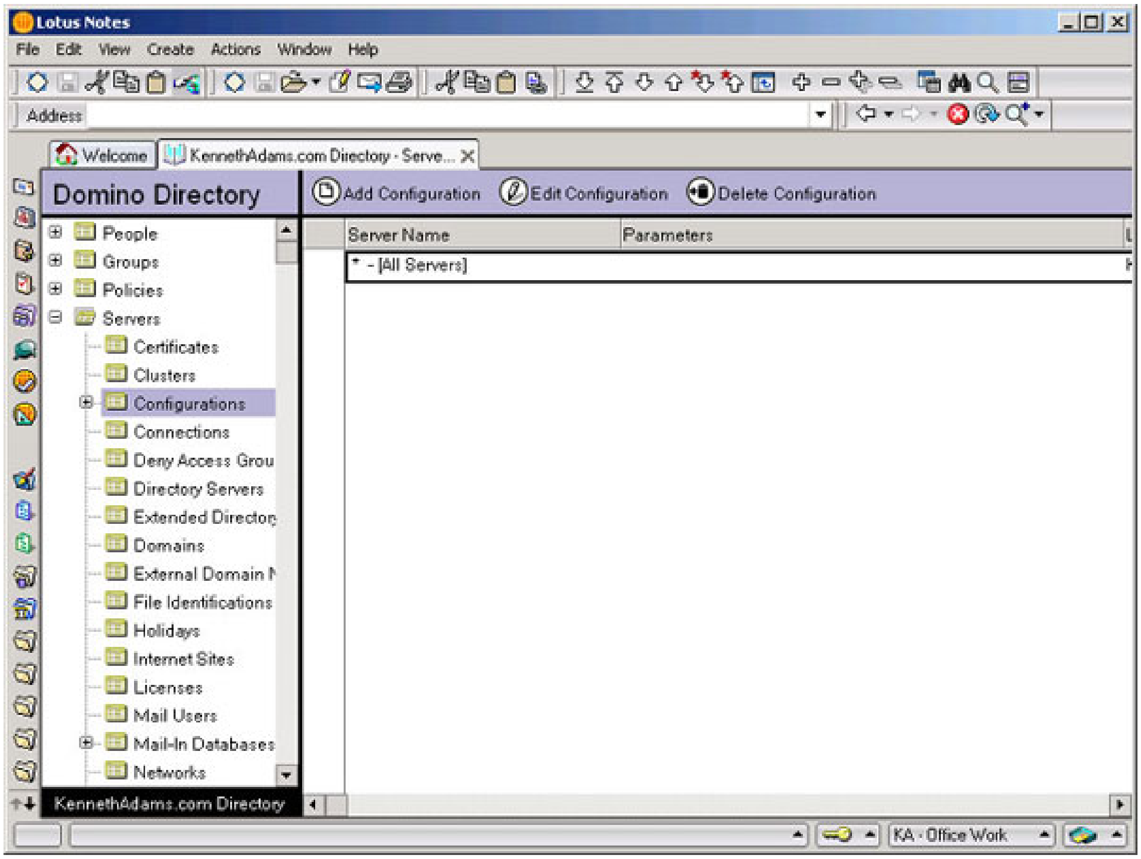
Follow these first few steps depending on which client you prefer.

From the Domino Administrator client:

1. Select a server.
2. Click the **Configuration** tab.
3. Expand the **Messaging** section.
4. Click **Configurations**.

From a Notes client (shown in the figure below):

1. Open the Domino Directory on the server.
2. Expand the Servers view list.
3. Select the Configurations view.



Server Name	Parameters
* - [All Servers]	

Edit or create a Configuration Settings document

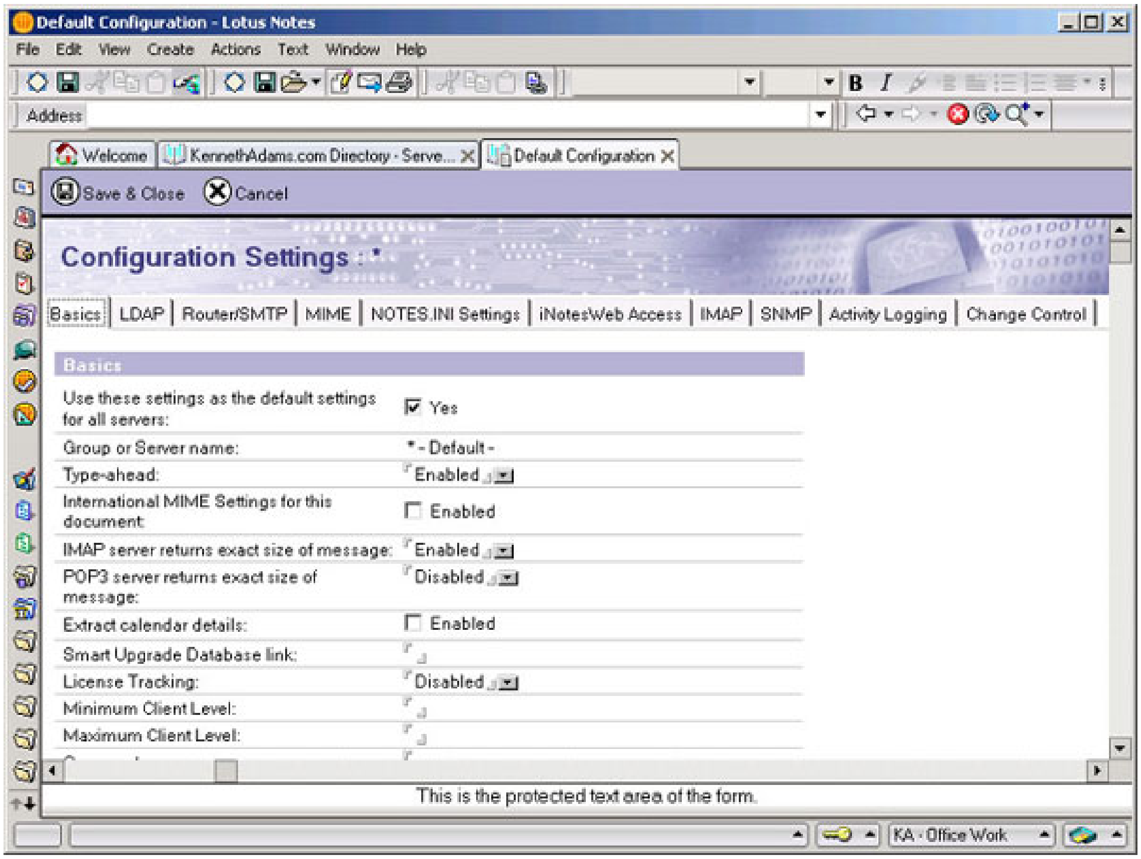
To edit an existing Configuration Settings document, do the following:

1. From the Configurations view, select the Configuration Settings document for the mail server or server group that you want to administer. If you are using one Configuration Settings document for all servers, select the default Configuration Settings document, which is displayed in the view as: `* - [All Servers]`.
2. Click **Edit Configuration**.

If a default Configuration Settings document does not exist, then you need to create one. To create a new Configuration Settings document:

1. From the Configurations view, shown in the figure below, click **Add Configuration**.
2. If you want this to be the default Configuration Settings document for all servers, select the Yes check box on the first field of the Basics tab, which is labeled `Use these settings as the default settings for all servers`.

3. If you want this to be a Configuration Settings document for one or more specific servers, then enter the server name of server group name in the `Group or Server name` field.


Default Configuration - Lotus Notes
File Edit View Create Actions Text Window Help
Address
Welcome
KennethAdams.com Directory - Serve...
Default Configuration
Save & Close
Cancel
Configuration Settings : *
Basics
LDAP
Router/SMTP
MIME
NOTES.INI Settings
iNotesWeb Access
IMAP
SNMP
Activity Logging
Change Control
This is the protected text area of the form.
KA - Office Work

Basics

Use these settings as the default settings for all servers:	☑ Yes
Group or Server name:	* - Default -
Type-ahead:	Enabled
International MIME Settings for this document:	□ Enabled
IMAP server returns exact size of message:	Enabled
POP3 server returns exact size of message:	Disabled
Extract calendar details:	□ Enabled
Smart Upgrade Database link:	
License Tracking:	Disabled
Minimum Client Level:	
Maximum Client Level:	

The next panel details the steps to prevent relaying with SMTP Inbound Controls.

Preventing all relaying with SMTP Inbound Controls

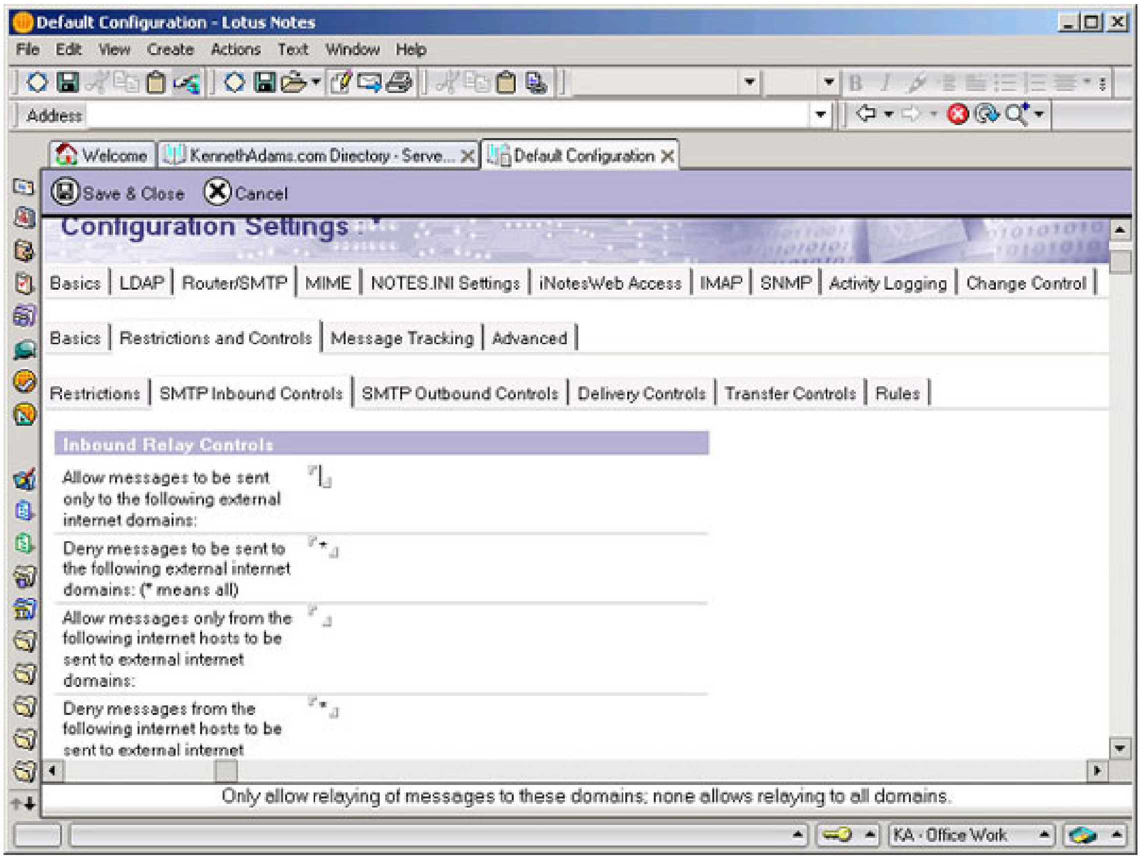
Preventing and controlling mail relays with Inbound Relay Controls is a feature that was supported in Domino R5. In Domino 6 it has been enhanced further with Inbound Relay Enforcement controls.

Preventing all relaying will completely stop mail relaying from any host for any reason. This is the safest way to configure your server. However, in large, sophisticated mail environments, you may wish to use relaying internally or externally for special purposes. If you have the need to relay, you should fully investigate your configuration requirements and options, and carefully configure them to meet your needs.

In order to prevent all relaying in Domino 6, you need to access the SMTP Inbound Controls tab section of your Configuration Settings documents. There are two main parts to this tab that contain fields whose values need to be set by the administrator. The first is the Inbound Relay Controls section covered here, and the second is the Inbound Relay Enforcement section covered next in Inbound Relay Enforcement section on page 8 .

To access the SMTP Inbound Controls tab, you need to first open any Configuration Settings documents for the server or servers and then select the **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls** tab.

The figure below shows the fields in the Inbound Relay Controls section of the SMTP Inbound Controls tab and the values needed to prevent all relays from your server. Once you have completed the fields, click **Save & Close**.


Default Configuration - Lotus Notes
File Edit View Create Actions Text Window Help
Address
Welcome
KennethAdams.com Directory - Serve...
Default Configuration
Save & Close
Cancel
Configuration Settings
Basics | LDAP | Router/SMTP | MIME | NOTES.INI Settings | iNotesWeb Access | IMAP | SNMP | Activity Logging | Change Control
Basics | Restrictions and Controls | Message Tracking | Advanced
Restrictions | SMTP Inbound Controls | SMTP Outbound Controls | Delivery Controls | Transfer Controls | Rules
KA - Office Work

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:

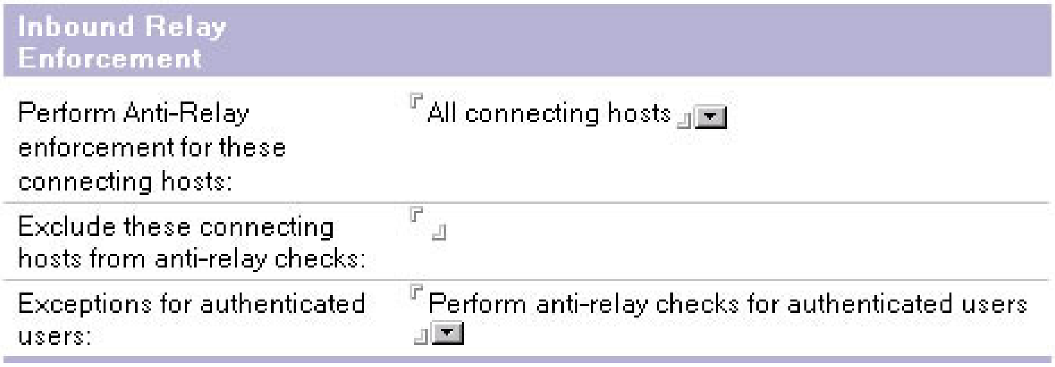
Deny messages from the following internet hosts to be sent to external internet *

Only allow relaying of messages to these domains; none allows relaying to all domains.

Inbound Relay Enforcement section

The figure below shows the fields in the Inbound Relay Enforcement section of the

SMTP Inbound Controls tab and the values needed to prevent all relays from your server:



Inbound Relay Enforcement

Perform Anti-Relay enforcement for these connecting hosts:	All connecting hosts
Exclude these connecting hosts from anti-relay checks:	
Exceptions for authenticated users:	Perform anti-relay checks for authenticated users

Once you've completed the fields in this tab, update the routing configuration using the following command at the server console:

```
Tell Router Update Config
```

The next section looks at DNS blacklist filters and how they can be used to combat spam.

Section 3. Using DNS blacklist filters

DNS blacklist filters overview

DNS blacklist filters are a new and powerful feature in Domino 6 and one of the more effective weapons against spam. With the DNS blacklist filters enabled, Domino will check inbound mail to see whether it originates from a mail server that is listed in one or more DNS blacklists (DNSBLs).

DNSBLs are databases that keep records of Internet SMTP mail hosts that are known sources of spam or permit open mail relaying. DNSBLs are maintained by many sources, both free and fee-based, and their effectiveness varies, so you may need to experiment with different DNSBLs to see how effective they are in your environment.

This section first gives some background on what DNS blacklists are before moving on to show you how DNS blacklist filters work and how to enable and monitor blacklist filters.

Selecting DNS blacklists to use

There are a number of free, publicly-available services along with numerous private paid subscription services that maintain DNS blacklists. Each blacklist service will use its own policies and methods for adding mail servers to its blacklist.

The more restrictive blacklist sites will add mail servers to their blacklist as soon as they fail an automated test, regardless of whether the server is verified as a source of spam. Other less restrictive sites will blacklist a mail server only if the server acts as a host to known spammers or if its system administrator fails to close the server to relaying after a specified period.

It is possible (and even likely) that any DNSBL might cause legitimate mail to be rejected. This is known as a false positive. It is best to assume that false positives will occur. Fighting spam is not an exact science and it's inevitable that legitimate mail will be blacklisted at some point.

You should search the Internet to find sites that provide DNS blacklist services. A good place to start is the Lotus Developer Domain discussion forums (see Resources on page 27). In the discussion forums, you can get an idea of which services other Domino administrators have used and what their experiences have been with them.

When evaluating a DNSBL service you should review the services policies and methods for selecting mail servers to be blacklisted. Consider how restrictive the

DNSBL's policies are and compare them to your own organization's views and tolerances to determine whether the service might be a good match. Consider what your user's reactions might be to false positives and how many they might tolerate before determining the service is too restrictive.

Specifying the DNS blacklist sites to check

You can specify one or more sites that the Domino server's SMTP task will use to identify whether a connecting host is a "known" open mail relay or spam source. You must specify sites that support IP-based DNS blacklist queries.

In order to minimize the impact on performance, you should limit the number of DNSBL sites by selecting only a few to use. Remember that Domino will perform a DNS lookup on each DNSBL site for each SMTP mail connection. Once Domino finds a match for a connecting host in one of the blacklists, it does not continue checking the lists. This is so the server's work is kept to the minimum necessary to get the job done.

Performance considerations

When Domino checks a DNS blacklist, it performs DNS queries over the network. If the DNS query goes over the Internet, it could take a significant amount of time to resolve DNS queries and therefore slow the processing of blacklist filters on inbound messages. In a high volume mail environment, this can present a serious bottleneck on inbound mail.

When using a free public blacklist service, the network latency of DNS queries made over the Internet can result in slowed blacklist filtering performance. With a private service that allows DNS zone transfer, Domino can perform the required DNS lookups to a local DNS host that you set up with a copy of the DNS blacklist. With a zone transfer, the contents of the DNS zone file at the DNSBL service provider are copied to a DNS server in your local network. DNS queries for blacklist filtering can then be completed on the local network without going over the Internet, thereby improving the performance of blacklist filtering.

How DNS blacklist filters work

When DNS blacklist filters are enabled on a Domino server, every incoming SMTP mail connection is checked against one or more DNSBLs. Domino performs a DNS query against the blacklists at the DNSBL sites specified. If a connecting SMTP mail host is found on the blacklist, Domino can do any of the following:

- Log the message
- Log and tag the message
- Log and reject the message

The next panel takes a look at these actions in more depth.

Choosing and using filter actions

Below are some of the actions that Domino can take if a connecting SMTP mail host is found on a DNS blacklist.

Log the message

When logging the message, Domino reports the event to the server console and records it in an entry to the Mail Routing Events view of the server's Log database. The messages provide the host name and IP address of the server and the name of the blacklist site where the server was listed.

Log and tag the message

When tagging messages, Domino adds a special field named $DNSBLSite to messages received from hosts found on a blacklist. The value of the $DNSBLSite field is the first blacklist site found listing the host.

You can use the $DNSBLSite field to provide custom handling of messages received from hosts listed in a blacklist. For example, you can check for the presence of the field through the use of simple formula language in an agent in the user's mail files and provide conditional handling of messages, such as moving or copying the messages to a folder or another database. You can design views in user's mail files that display messages with the $DNSBLSite field in them and sort and total messages by its value.

Log and reject the message

When a message is rejected, an e-mail is returned to the sender with a message that can be customized. For example, your message might read "Your host 127.0.0.2 was found in the DNS Blacklist at blackholes.mail-abuse.org". Once a message is rejected it cannot be retrieved and the recipient will never be aware that the message was ever sent, so this action is potentially dangerous if a blacklist you are using lists legitimate mail servers.

It is strongly recommended that you use a Custom SMTP error response for rejected messages. In the event that a legitimate e-mail is rejected, you want the sender to have as much information about why as possible.

A note of caution on using DNS blacklist filtering

If you want to experiment with DNS blacklist filtering, or want to test a DNSBL service, use the log only or log and tag actions. You can use the log and statistics to see what effect the filtering might have on your mail. If you'd like to create your own agents to handle messages, then use the log and tag action and create your agents.

If you're ready to cut the amount of spam you receive, and have confidence in your DNSBL service, then use the reject action and keep an eye out for reports of false positives.

Enabling DNS blacklist filters

Enabling DNS blacklist filters requires only a few settings. These settings are controlled via a Configuration Settings document.

To enable DNS blacklist filtering:

1. Open the Configuration Settings document for the server or servers. See Configuration Settings documents on page 5 for information on opening Configuration Settings documents.
2. Select the **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls** tab.
3. Complete the fields under the DNS Blacklist Filters section (shown in the figure below), and then click **Save & Close**.

Below are a list of fields and the appropriate values for the DNS Blacklist Filters section of the SMTP Inbound Controls tab:

DNS Blacklist filters

- Enabled

DNS Blacklist sites

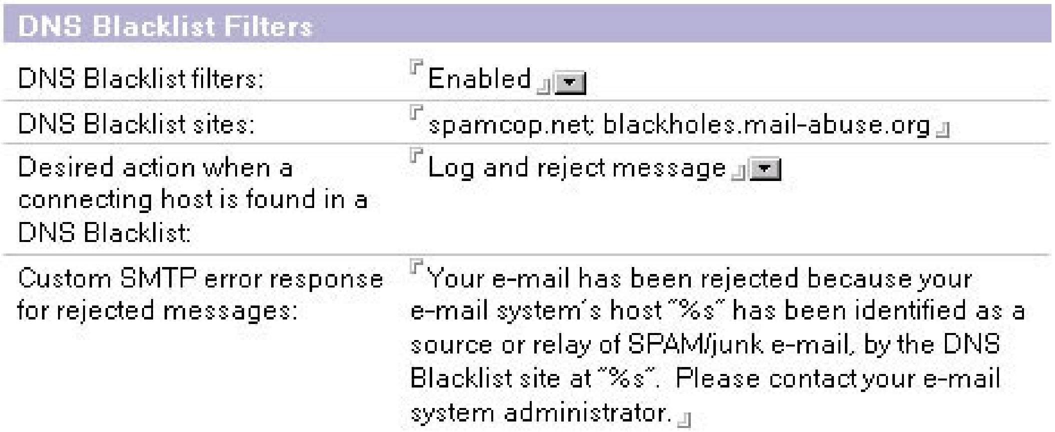
- Specify the DNSBL sites to check. List them in the order you wish them to be checked.

Desired action when connecting host is found in a DNS Blacklist

- Log
- Log and tag message
- Log and reject message

Custom SMTP error response for rejected messages

- Provide customized error message. See Changing the default error message for rejected e-mails on page 14 for an example.



DNS Blacklist Filters	
DNS Blacklist filters:	Enabled
DNS Blacklist sites:	spamcop.net; blackholes.mail-abuse.org
Desired action when a connecting host is found in a DNS Blacklist:	Log and reject message
Custom SMTP error response for rejected messages:	Your e-mail has been rejected because your e-mail system's host "%s" has been identified as a source or relay of SPAM/junk e-mail, by the DNS Blacklist site at "%s". Please contact your e-mail system administrator.

Once you have completed these steps, reload the SMTP task or update the SMTP configuration to put the changes into effect:

```
Tell SMTP update config
```

Changing the default error message for rejected e-mails

When rejecting a message from a blacklisted host, Domino returns to it a default SMTP response, which includes the remote host's IP address and the blacklist site that listed the host. For example:

```
Your host 127.0.0.2 was found in the DNS Blacklist at
bl.spamcop.net
```

You can customize this response in the `Custom SMTP error response for rejected messages` field in the Configuration Settings document. The text of a customized response can include the string format specifier `"%s"` to represent a rejected host's IP address and the DNSBL blacklist site where the host was found. When the message is created, Domino replaces the first occurrence of "%s" with the address of the rejected host, and the second with the DNS blacklist site.

In the event that a legitimate e-mail is rejected, it is important to provide the sender of the e-mail with a descriptive and useful response. Here is an example of a more descriptive message that you would enter in the `Custom SMTP error response for rejected messages` field.

```
Your e-mail has been rejected because your e-mail system's
host "%s" has been identified as a source or relay of spam/junk e-mail,
by the DNS Blacklist site at "%s".  Please contact your e-mail system
administrator.
```

Hosts that are exempt from blacklist checks

The Domino Server performs DNS blacklist checks only on hosts that are subject to relay checks, which is specified in the SMTP Inbound Relay restrictions.

Any host that is authorized to relay is exempt from blacklist checks. This is done in order to avoid unnecessary DNS lookups, which would result in slower performance.

DNS blacklist filtering statistics and logging

Being able to monitor activity and statistics is important if you need to troubleshoot a problem, view activity related to a specific DNSBL, or measure the activity. There are two ways to monitor DNS blacklist filtering activity: through the activity log and filtering statistics.

Filtering activity is logged when a match of an inbound mail server is found in the DNS blacklist. The activity is logged in the "Mail routing events" view of the server's activity log (`log.nsf`).

The Domino server's SMTP server task maintains statistics that track the total number of connecting hosts that were found on all DNSBL sites combined, as well as how many were found on the DNSBL of each configured site. These statistics are cumulative for the life of the SMTP server task and are lost when the task stops, is restarted, or the configuration is updated.

You can view the statistics from the Domino Administrator or by using the `SHOW STAT SMTP` command from the server console. If you have configured Statistics Collection for your Domino server, the statistics will be collected and stored in the Statistics

Reporting database at the intervals you defined. For details on statistics, see the "Monitoring the Domino system" section of Lotus Domino Administrator 6 Help (see Resources on page 27).

You can further expand the statistics to learn the number of times a given IP address is found on one of the configured DNSBLs. To collect the expanded information, you set the variable `SMTPExpandDNSBLStats` in the `NOTES.INI` file on the server. Because of the large numbers generated by the expanded set of statistics, Domino does not record the expanded statistics by default. In order to generate the expanded or Host specific DNS blacklist filter statistics, the default `SMTPExpandDNSBLStats` variable must be set to 1. This variable is set to 0 by default.

You can edit this setting by shutting down the Domino server and editing the `NOTES.INI` file directly on the server, or you can use the following server console commands to set the variable without shutting down the server:

```
Set config SMTPExpandDNSBLStats=1
Tell SMTP Update Config
```

Section 4. Verifying inbound recipient names

Verification overview

Although Domino R5 supported allow and deny of specific addresses on inbound mail, Domino 6 has a new feature to check recipients against the Domino Directory known as verifying inbound recipient names, a simple verification technique designed to keep incorrectly addressed e-mail out of your system. Because spammers sometimes use outdated e-mail addresses or generic e-mail addresses to try to get through to someone, this verification is sometimes successful at blocking spam.

How it works

You can restrict inbound mail based on a verification of the existence of the recipient's name in the Domino Directory. Using this restriction can prevent spam that is sent to users that do not exist or who have left the organization.

This verification occurs at the point that the message first enters the mail system via SMTP. The SMTP listener checks the recipient's names via the SMTP command `RCPT TO`. The name is compared against the Domino Directory before the message is accepted.

If no matching user name is found, the SMTP server returns a 550 permanent failure response to the sending SMTP server, indicating that the user is unknown, for example: `550 bad_user@yourdomain.com ... No such user`.

Using the new Domino 6 feature to verify inbound recipients against the Domino Directory can be an effective way to block some spam. You should only use allow and deny of specific addresses when you know a specific address is an ongoing problem.

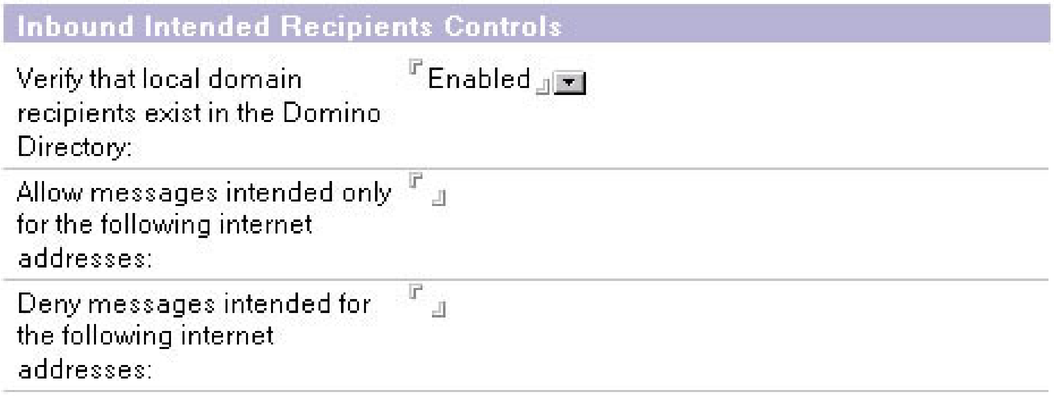
Enabling verify inbound recipient names

To enable the verification of inbound recipient names:

1. Open the Configuration Settings document for the server or servers. See Configuration Settings documents on page 5 for information on opening Configuration Settings documents.
2. Select the **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls**

tab.

3. Under the Inbound Intended Recipients Controls section, set `Verify that local domain recipients exist in the Domino Directory` to Enabled, as shown in the figure below, and then click **Save & Close**:



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:	

Once you are done, update the routing configuration using the following command at the server console:

```
Tell SMTP Update Config
```

The next section shows two more advanced verification techniques.

Section 5. Verifying host names and sender's domain name

Verifying host names and sender's domain name overview

In this section we'll look at two advanced verification methods: verifying the connecting host name and verifying the sender's domain name.

Verifying the connecting host name and verifying the sender's domain name may successfully block some spam, but it increases the likelihood that legitimate e-mail may be blocked as well if a legitimate organization has not been thorough about setting up their DNS records.

First we'll look at configuring the Domino server to verify the sender's domain name.

How verifying sender's domain name works

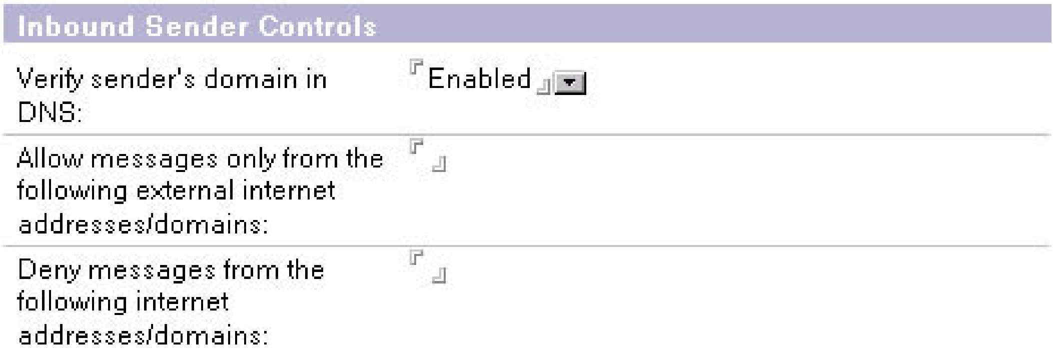
You can configure the Domino server to verify that the sender's domain exists before accepting mail. This control can prevent spam from sources that use fictitious sender addresses or from sources that send from domains that have no way to return mail to them. This verification of the sender's domain is accomplished by checking DNS for a mail exchanger (MX), canonical name (CNAME), or address (A) record that matches the domain portion of the address in the `MAIL FROM` command received from the sending SMTP host. If a match cannot be found, then the inbound message from the host is rejected.

Essentially this verification test checks for the existence of evidence that an organization has a mail server and/or a Web site or some other host on the Internet. If a message fails this verification, it is recorded in the server's log (`log.nsf`). Since MX records are required for a domain to receive mail, and an organization that sends mail is likely to want to receive it, this test is likely to be valid in most situations. However, it is possible that a legitimate organization might use a domain for only sending news or other mail and not for receiving mail or other services. In this scenario, they would not need any of these DNS records, which would cause this verification to fail.

Enabling Verifying sender's domain name

To enable the verification of the sender's domain name:

1. Open the Configuration Settings document for the server or servers (See Configuration Settings documents on page 5).
2. Select the **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls** tab.
3. Under the Inbound Sender Controls section, set the `Verify sender's domain in DNS` field to Enabled, and then click **Save & Close**.



Inbound Sender Controls

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

Once complete, update the routing configuration using the following command at the server console:

```
Tell SMTP Update Config
```

Next, we'll look at configuring the Domino server to the name of the connecting host.

Verifying connecting host names overview

Verifying the connecting host name is a feature that existed in Domino R5 and remains the same in Domino 6. This verification is dependent on DNS records being set up thoroughly to provide maximum DNS functionality. Unfortunately, no strict standards exist for setting up DNS, and commonly used services like mail and Web will function even if DNS records are not complete in every detail.

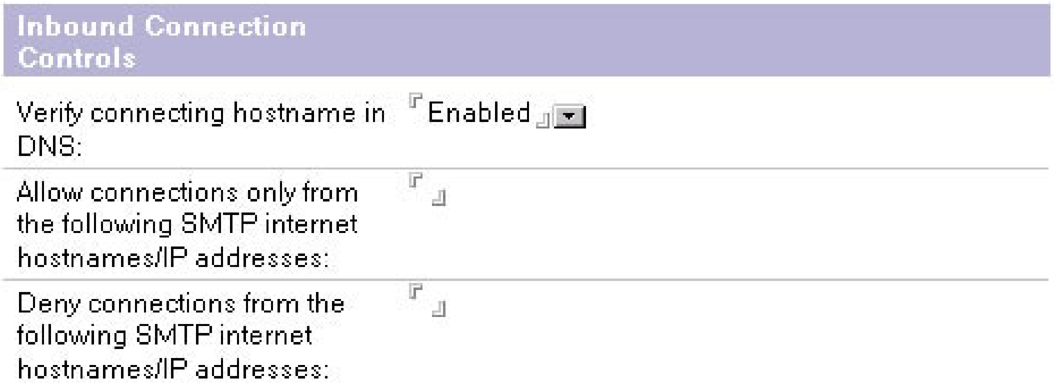
Domino can verify the name of the connecting host in an attempt to verify that the address of the server sending the message matches the address of the host name on record. This is accomplished by performing a reverse DNS lookup of the IP address. The Domino server checks DNS for a pointer (PTR) record that matches the IP address of the connecting server to a host name. If a match cannot be found, then the transfer of the message is not allowed.

Because Internet SMTP hosts are not required to have PTR records in DNS, this setting may reject legitimate mail. Therefore, you should use this setting with caution.

Enabling verifying connecting host names

To enable the verification of the connecting host names, follow these steps:

- Open the Configuration Settings document for the server or servers. See Configuration Settings documents on page 5 .
- Select the **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls** tab.
- Under the Inbound Connection Controls section, set the `Verify connecting host in DNS` field to Enable, as shown in the figure, and then click **Save & Close**:



Inbound Connection Controls

Verify connecting hostname in DNS:	Enabled
Allow connections only from the following SMTP internet hostnames/IP addresses:	
Deny connections from the following SMTP internet hostnames/IP addresses:	

Once this is complete, update the routing configuration using the following command at the server console:

```
Tell SMTP Update Config
```

The next section looks at using server mail rules to battle spam.

Section 6. Using server mail rules

Mail rules overview

Mail rules allow you to create content filtering rules that define actions to take on certain messages based on their content. For example, you could reject mail that contains certain words or is from a specific domain.

Server mail rules are configured by the Domino administrator and are stored in the Domino Directory. User level mail rules are also supported and are stored in user's mail files and configured by each individual user. This section will focus specifically on server mail rules.

Mail rules are not designed specifically for battling spam but are more of a general purpose tool for handling mail. Mail rules are one of the least effective means of controlling spam. Due to the huge volume of spam being generated, and the endless sources and methods used to send it, it's extremely difficult, if not impossible, to filter out spam based on rules that you must maintain yourself. However, there may be specific situations where mail rules might prove useful to you.

In this section we will cover some of the basics about mail rules. Before using mail rules on a production server, it is recommended that you fully review the Lotus Administrator documentation on this subject (see Resources on page 27) and make sure you understand the capabilities and limitations of mail rules.

About server mail rules

Server mail rules allow you to create content filtering rules for a server that define actions to take on certain messages. When a new message that meets a specified rule condition is deposited in the server's MAIL.BOX, Domino automatically performs the designated rule action. Rule conditions are based on content in the messages. Available actions include journaling the message, moving it to a database, rejecting the message, silently deleting the message, returning a non-delivery report, or changing the routing state of a message.

You can specify only one action for each rule. Rule conditions are based on content in the message headers or in the message body.

Mail rules can be used for a number of purposes.

- You can reject some spam or intercept messages with questionable content. For example, you can use a rule that rejects mail with subjects like "get rich quick" or that comes from a known spam source.

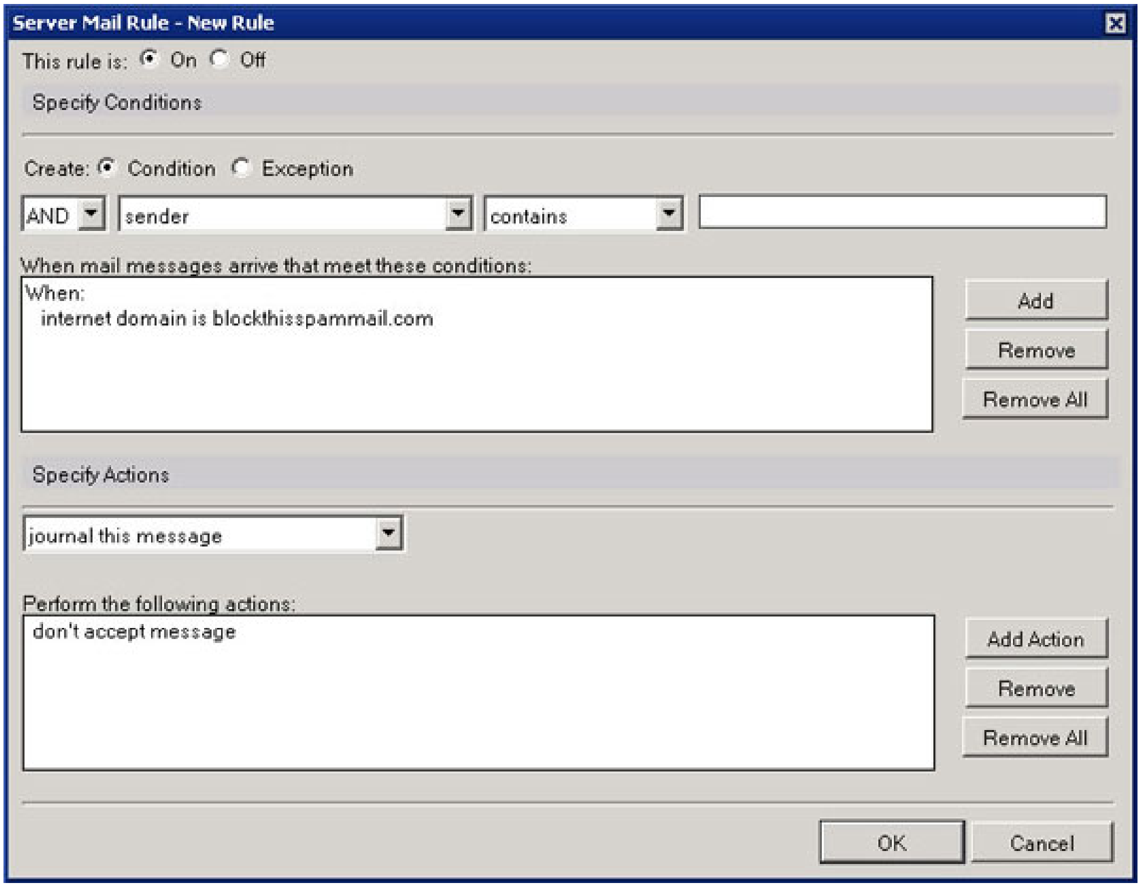
- You can reject mail with attachments of certain file types (EXE, VBS, VBE, SCR, etc.).
- You can journal all messages or messages that match a specific condition to provide a record for regulatory or other purposes.

Creating a mail rule

In this example, we will create a simple mail rule that will reject messages from a specific domain called *blockthisspammail.com* that is a known source of spam. (*blockthisspammail.com* is used for example only and is not an actual domain name or known source of spam.)

To create a mail rule:

1. Open the Configuration Settings document for the server or servers. See Configuration Settings documents on page 5 for details.
2. Select the **Router/SMTP=>Restrictions and Controls=>Rules** tab.
3. Click **New Rule**.
4. In the Specify Conditions section of the New Rule dialog box, set the condition to `internet domain is blockthisspammail.com`.
5. Click **Add**. The new condition is displayed in the `When mail messages arrive that meet these conditions` field.
6. In the Specify Actions section specify the action to perform as **don't accept message**, and click **Add Action**.
7. To save the rule, click **OK**.
8. Click **Save & Close**.



Server Mail Rule - 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 is blockthisspammail.com

Specify Actions

journal this message

Perform the following actions:

don't accept message

The change takes affect after the next Router configuration update. To put the new setting into effect immediately, reload the routing configuration using the following command at the server console:

```
Set Rules
```

Section 7. Blocking mail from yourself

Blocking mail from yourself overview

One method used by spammers is to send the spam so that the from address looks like it came from your own mail address or domain. Forging an address like this is known as *spoofing*.

You can block mail that is from your own domain or your personal e-mail address in several different ways. You can block mail at the server using the deny control of Inbound Sender Controls or using server mail rules. You can also do the blocking in the user's mail file with mail rules.

WARNING: The rational behind blocking mail from yourself is that any mail coming to you from outside your mail server that claims to be from you is a forgery. On the surface, it seems like a reasonable assumption, but it's not always true and can sometimes block legitimate mail, as explained in Blocking mail from yourself can block legitimate mail on page 25 .

Blocking mail from yourself can block legitimate mail

Because there are many legitimate uses for spoofing mail to make it appear to come from you, it is likely that you will block legitimate mail with this technique. A very common legitimate use of spoofing mail addresses is done by Web sites that send mail on your behalf. They usually do this when you request that a message be sent to someone from their Web site, such as a link to a page on the site or news. Sending the message with your e-mail address in the from field makes it clear that the e-mail was initiated by you, and allows the recipient to use reply to respond directly to you.

IBM's Lotus QuickPlace uses this technique to send notifications via e-mail. If you use the Notify feature of QuickPlace, it will spoof your e-mail address to make it look like the e-mail came from you. Technically speaking, it *is* coming from you: it's being created and sent by QuickPlace software at your request.

If you block mail from your own e-mail address and send a QuickPlace notification to yourself, or more likely cc: yourself on a notification to someone else, it will get blocked. Worse is if you block spoofed mail for your entire domain. You could potentially block mail from any of your users in all of the QuickPlaces on that server.

How to block mail from yourself (or anyone)

If you still wish to block mail from yourself, there are several ways this can be done. You can also use the same techniques to block mail from any address or domain. There are three different ways to block mail with Domino:

1. At the server -- using the deny control of Inbound Sender Controls
2. At the server-- using server mail rules
3. At the user's mail file -- using mail rules in the user's mail file.

The most efficient method is to use Inbound Sender Controls because it rejects the mail before it completely enters the server. Inbound Sender Controls are enforced in real time as mail is being sent from the sender mail server into the Domino server. Mail rules in the user's mail file are the least efficient because they are not processed until after the mail is routed through servers and delivered to the user's mail file.

To block mail using Inbound Sender Controls:

1. Open and edit the Configuration Settings document for the server or servers. See Configuration Settings documents on page 5 for details.
2. Select the **Router/SMTP=>Restrictions and Controls=>SMTP Inbound Controls** tab.
3. Navigate to the Inbound Sender Controls section.
4. Enter the domains and addresses to block in the `Deny messages from the following Internet addresses/domains` field, and then click **Save & Close**.

To block mail using server mail rules, follow the steps in Creating a mail rule on page 23 using the conditions to match the domain or address that you wish to act on and the action you wish taken.

To block using mail rules in the user's mail file, refer to the Notes 6 Help for details on created mail rules in Notes mail (see Resources on page 27). Notes mail rules are similar to server mail rules and can be found in your Notes mail under **Tools=>Rules**. Use the conditions to match the domain or address that you wish to act on and the action you wish taken.

Section 8. Summary

Tutorial summary

In the battle against spam, there is no perfect weapon or magic bullet. Instead, there is a growing arsenal of weapons that must be used correctly and with awareness of their strengths and weaknesses. There are many weapons to choose from, and there will be many more added as technology advances. But if you start with Lotus Domino 6, you will have one of the best weapons of all.

This tutorial covered many techniques available to Domino administrators to battle spam mail, including:

- Making sure your mail server isn't used by spammers to relay spam mail
- Using third party maintained DNS blacklists that can filter out spam
- Using several techniques to verify various aspects of mail in an attempt to identify and filter out spam
- Using mail rules and other types of restrictions to combat spam

Resources

General Notes/Domino resources

- Some of the information contained in this tutorial, and additional details, can be found in Lotus Domino Administrator 6 Help. You can view the *Lotus Domino Administrator 6 Help* with a Web browser, without having to download it first.
- The Lotus Developer Domain's *Notes/Domino Product Pages* contain numerous resources on Notes and Domino, including links to articles, documentation and trial downloads.
- *Lotus Domino 6 Server and Administrator Documentation* is available from Lotus Developer Domain.

Spam-related resources and articles

- See the IBM Redbook, *Lotus Domino 6 Spam Survival Guide for IBM eServer*, for thorough and up-to-date coverage of all of the issues surrounding spam and how it can be managed with Domino 6.
- Read this Lotus Developer Domain *mail filtering article* covering various techniques on battling spam with the Notes client.
- For an IBM developerWorks article that looks at SpamAssassin, an open source tool

for combating spam, see *Stamp out spam with SpamAssassin*.

- See the IBM developerWorks article, *Spam filtering techniques*, which covers six approaches to eliminating spam.
- The *Notes/Domino 6 forum* contains a wealth of information on spam and other mail-related topics.
- The Lotus Developer Domain's *Sandbox* has a number of downloads available on spam and junkmail, including several add-ons and code samples of anti-Spam tools and some Lotusphere presentations.
- Search the forum for *DNS blacklist recommendations*.
- You can find many spam-related Web sites from *Yahoo's directory*.

Feedback

Please send us your feedback on this tutorial. We look forward to hearing from you!

Colophon

This tutorial was written entirely in XML, using the developerWorks Toot-O-Matic tutorial generator. The open source Toot-O-Matic tool is an XSLT stylesheet and several XSLT extension functions that convert an XML file into a number of HTML pages, a zip file, JPEG heading graphics, and two PDF files. Our ability to generate multiple text and binary formats from a single source file illustrates the power and flexibility of XML. (It also saves our production team a great deal of time and effort.)

You can get the source code for the Toot-O-Matic at www6.software.ibm.com/dl/devworks/dw-tootomatic-p. The tutorial Building tutorials with the Toot-O-Matic demonstrates how to use the Toot-O-Matic to create your own tutorials. developerWorks also hosts a forum devoted to the Toot-O-Matic; it's available at www-105.ibm.com/developerworks/xml_df.nsf/AllViewTemplate?OpenForm&RestrictToCategory=11. We'd love to know what you think about the tool.