Domino Messaging Restrictions and Controls

by
Craig
Lordan

Level: Beginner
Works with: Domino 5.0
Updated: 11/01/99

Inside this article:

Related links:

Notes spam mail filtering: Introduction
Notes Mail Rules
AntiSpamFilter agent article
AntiSpamFilter agent download
Domino 5 Administration Help

Get the PDF:

This article is second in our series this month on Notes spam mail filtering. In this article, we learn about how to use Domino messaging restrictions and controls to filter Internet spam mail.

Restricting Internet spam mail routing prevents users and organizations from receiving unwanted or inappropriate mail, and reduces the load of unwanted mail on your system. To filter or deny Internet spam mail, you can set these restrictions:

- Verify and restrict who can send Internet e-mail to your users
- Restrict who can receive Internet e-mail in your organization
- Verify and restrict inbound connections
- Control inbound relay access

All the features discussed in this article require a Domino R5 server and the Domino Administrator R5 client. This article also assumes that you are familiar with Domino Administrator.

Configuration Settings document

You set all mail restrictions and controls in the Configuration Settings document. You will need to create one if you haven't done so already. You can use one Configuration Settings document for one specific server, a group of servers, or all the servers in your domain.

1. In Domino Administrator, click the Configuration tab.
2. Expand the Messaging view and click Configurations. Alternatively, you can expand the Server view and click Configurations.
3. Click Add Configuration or choose Actions - Add Configuration.
4. In the Group or Server Name on the Basics tab, enter one server name, an existing server group name, or an asterisk (*) for all servers in the domain.
5. Click Save and Close.
6. You can then use this Configuration Settings document for all the mail restrictions and controls discussed in this article.

Tip: Once you have created a Configuration Settings document, you can use the Messaging Settings document as a shortcut to the Router/SMTP tab in the Configuration Settings document -- they are the same thing.

Filtering spam based on domain

You can use Domino's Inbound Sender Controls to filter spam mail by specifying Internet domains that are allowed to or denied from sending messages to your organization.

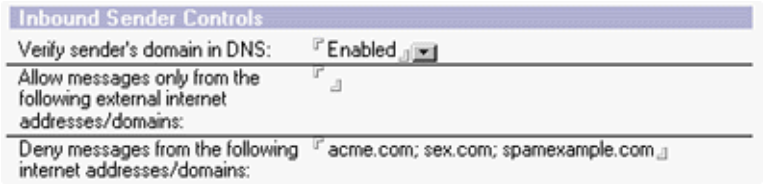
You can also use DNS (Domain Name Service) to ensure the Internet domain exists. If DNS cannot verify the message's domain, the message is denied.

Be aware, though, that not all sending domains have a direct connection to the Internet, so you may be filtering out legitimate mail.

Complete the following fields on the Router/SMTP - Restrictions and Controls - SMTP Inbound Controls tab in the Configuration Settings document.

Field	What to enter
Verify sender's domain in DNS	Disabled is the default. Choose Enabled to check the sending domain in DNS to verify that the sender's domain exists, and deny the message if the domain cannot be verified.
Allow messages only from the following external Internet addresses/domains	Internet domains from which the server will accept messages. By allowing only certain domains, all others are denied. For example, if you enter **lotus.com**, only messages from that domain are allowed. All other are denied.
Deny messages from the following Internet addresses/domains	Internet addresses from which the server will not accept messages. This is typically where you would enter known spamming or inappropriate domains, such as pornography domains or other unwanted commercial sites.

The following graphic shows an example of how you might fill in these fields:



Filtering based on address

Through the Inbound Intended Recipients Controls, Domino allows you to filter incoming messages based on the intended receiver's address. This is especially useful if you want to restrict certain individuals from receiving any Internet e-mail, either because your organization has policies restricting Internet use, or because sometimes individuals subscribe to Internet mailing lists that generate hundreds or thousands of messages per day.

This feature is also useful if Internet mail is coincidentally addressed to people or groups that should not be receiving *any* Internet messages whatsoever. For example, if you have an internal Notes group named "Everyone," you can block inbound messages to "everyone@acme.com."

Complete the following fields on the Router/SMTP - Restrictions and Controls - SMTP Inbound Controls tab in the Configuration Settings document.

Field	What to enter
Allow messages intended only for the following Internet addresses	Internet addresses that are within the local Internet domain and that are allowed to receive mail from the Internet. 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	Internet addresses within the local Internet domain that are prohibited from receiving mail

following Internet addresses	from the Internet. If you enter addresses in this field, all recipients *except* those listed in this field can receive Internet mail.

The following graphic shows an example of how you might fill in these fields:

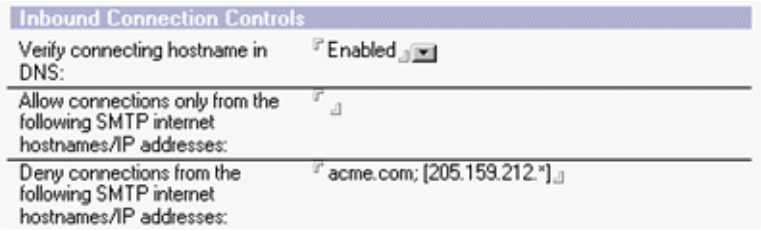
Restricting inbound SMTP connections

Some users and organizations may attempt to send bulk spam mail to your site. You can use Inbound Connection Controls to prevent Domino from accepting unwanted mail and keep your servers from redistributing it.

Complete the following fields on the Router/SMTP - Restrictions and Controls - SMTP Inbound Controls tab in the Configuration Settings document. If you enter an IP address, use brackets -- for example, [205.159.212.144]. You can use an asterisk in an IP address, but only for an entire octet -- for example, [205.159.212.*].

Field	What to enter
Verify connecting host name in DNS	Disabled is the default. Choose Enabled to check the IP address of the connecting host in DNS to verify that the sender's domain exists. If the IP address does not correspond to a valid host name, Domino accepts the connection but does not allow the host to transfer mail.
Allow connections only from the following SMTP Internet hostnames/IP addresses	The host names and/or IP addresses that are allowed to connect to this server. Only those servers matching these entries can connect to your server over SMTP. For example, if you enter lotus.com; ibm.com, Domino accepts only connections from servers with host names ending in lotus.com or ibm.com. Domino rejects all other connection requests.
Deny connections from the following SMTP Internet host names/IP addresses	The host names and/or IP addresses that are not allowed to connect to this server. All servers except those matching entries in this field can connect to your server over SMTP. For example, if you enter [205.159.212.144], Domino accepts connections from all servers except the server with this IP address.

The following graphic shows an example of how you might fill in these fields:



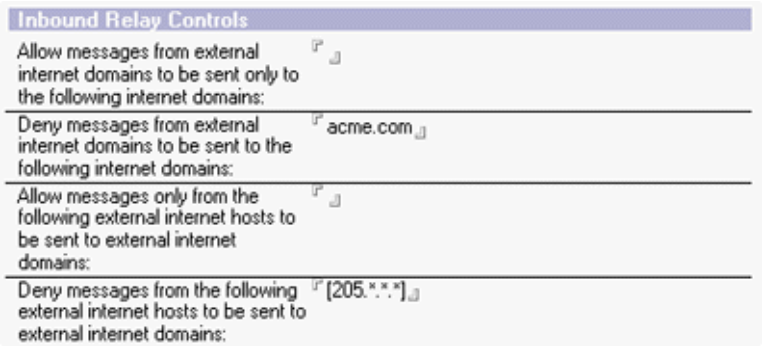
Preventing relay of spam mail

By sending a spam message through your system when it is actually destined for another system, your system appears to be the spamming domain if the destination server does a DNS lookup. You can prevent this by using Inbound Relay Controls to specify which incoming messages from hosts outside the local Internet domain are accepted for recipients outside the local Internet domain. Setting this kind of restriction prevents people from trying to use your messaging system as a spam mail relay.

Complete the following fields on the Router/SMTP - Restrictions and Controls - SMTP Inbound Controls tab in the Configuration Settings document. If you enter an IP address, use brackets -- for example, [205.159.212.144]. You can use an asterisk in an IP address, but only for an entire octet -- for example, [205.159.212.*].

Field	What to enter
Allow messages from external Internet domains to be sent only to the following Internet domains	Internet domains to which Domino will relay messages. For example, if you enter acme.com, Domino relays messages to acme.com only.
Deny messages from external Internet domains to be sent to the following Internet domains	Internet domains to which Domino will not relay messages. For example, if you enter acme.com, Domino does not relay any messages to acme.com.
Allow messages only from the following external Internet hosts to be sent to external Internet domains	Internet host names and/or IP addresses from which Domino will relay messages. For example, if you enter acme.com, Domino relays messages from acme.com only.
Deny messages from the following external Internet hosts to be sent to external Internet domains	Internet host names and/or IP addresses from which Domino will not relay messages. For example, if you enter acme.com, Domino does not relay any messages from acme.com.

The following graphic shows an example of how you might fill in these fields:



"Allow message" versus "Deny message"

In all of the restrictions and controls described above, there are "Allow message" and "Deny message" fields. These fields are mutually exclusive -- that is, if you enter anything in a "Deny message" field, it will ignore the

corresponding "Allow message" field.

Other Domino messaging restrictions and controls

Obviously, Domino has many other messaging restrictions and controls besides the spam mail filtering features we covered in this article. For example, you can also set restrictions on mail sent to and received from other Notes domains.

For full details and instructions on these features, and on all the features discussed in this article, see the chapter "Customizing the Domino Mail System" in **Domino 5 Administration Help**.