

Limit sending and receiving mail in Exchange 2007

The article will introduce some methods to perform the above management tasks for the mail system or for the entire network.

Network Administration - Suppose we have a mail system called MExchange.org and a user called Anderson Patricio.

In this article we will perform the management of this user's ability to send and receive mail in the system, and we will also perform the following basic tasks:

1. *Block all out-of-system mail sent to users.*
2. *Block all mail sent out of the system.*
3. *Allows users to send a certain amount of mail to an out-of-network user.*
4. *Only allow users to receive mail from a specific domain.*

The main purpose of the article is to learn some methods to perform the above management tasks for the mail system or for the entire network. You can combine these tasks together to meet the specific requirements of each system.

Manage incoming mail traffic of users

There are several methods of managing the amount of mail sent to a certain user. We can create Transport Rules, configuration for Recipient Filtering, mailbox level changes, .

The first method we use is to use Transport Rules. This tool allows us to create a Rule that returns a NDR to the sender, for example, in case the user is not allowed to receive mail sent from the Internet. To do so, please do the following:

1. Open the **Exchange Management Console** .
2. Expand **Organization Configuration** .
3. Click on **Hub Transport** .
4. Select the **Transport Rules** tab.
5. In **Toolbox Actions** , click **New Transport Rule** .
6. On the **Introduction** page, enter a name for the Rule and then click **Next** .
7. On the **Conditions** page, select the **From users inside or outside the organization** section and the **Sent to people** section . In the Step 2 box you can specify the value of the previously selected items. However, to do this, make sure that the Outside value is selected for the first link and the second link when you add the user mailbox to the list that cannot receive mail from the Internet. When done, click **Next** .
8. In the **Actions** page, select the option **Send bounce message to sender with enhanced status code** , then change the content of the mail and status code.

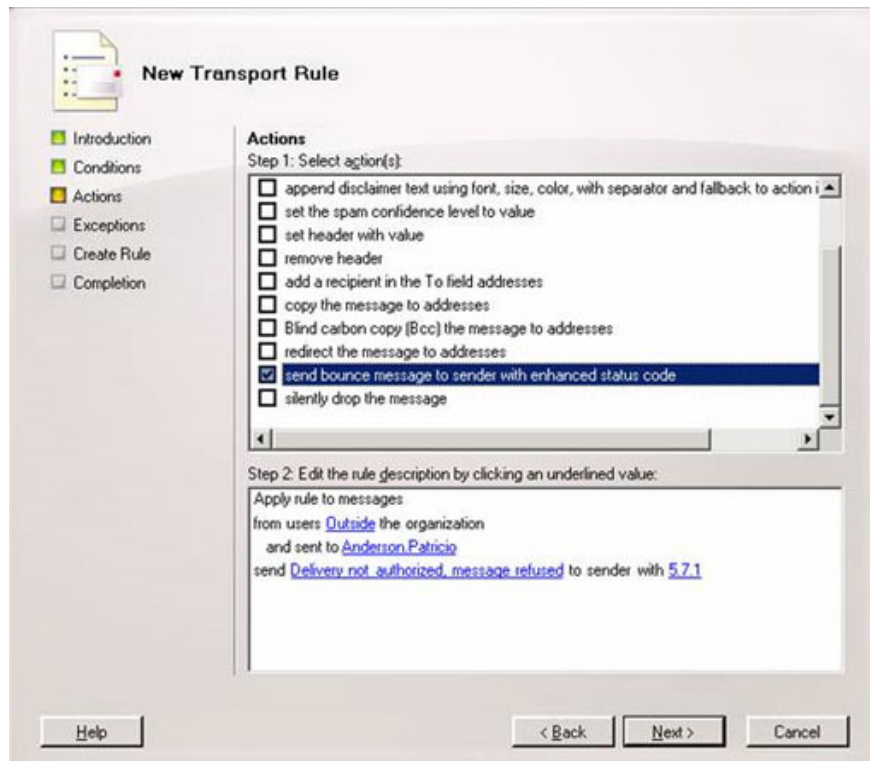


Figure 1: Configure the new rule on the Actions page.

1. On the **Exceptions** page, click the **Next** , **New** and **Finish** buttons.

The second method we can use is to use **Recipient Filtering Anti-spam Agent** . It has been enabled by default on an Edge Transport server, but if you are using the **Hub Transport Role** to receive mail from the Internet you need to enable **Anti-Spam Transport Agent** .

Alternatively, we can perform the configuration for the **Recipient Filtering** similar to the steps above. Next we will examine changes in a **Hub Transport** .

1. Open the **Exchange Management Console** .
2. Expand **Organization Configuration** .
3. Click on **Hub Transport** .
4. Select the **Anti-spam** tab.
5. Double-click the **Recipient Filtering** .
6. Select the **Blocked Recipients** tab.
7. Click the box to select **Block the following recipients** and enter the mail account of the internal user you want to block incoming mail from the Internet (Figure 2).

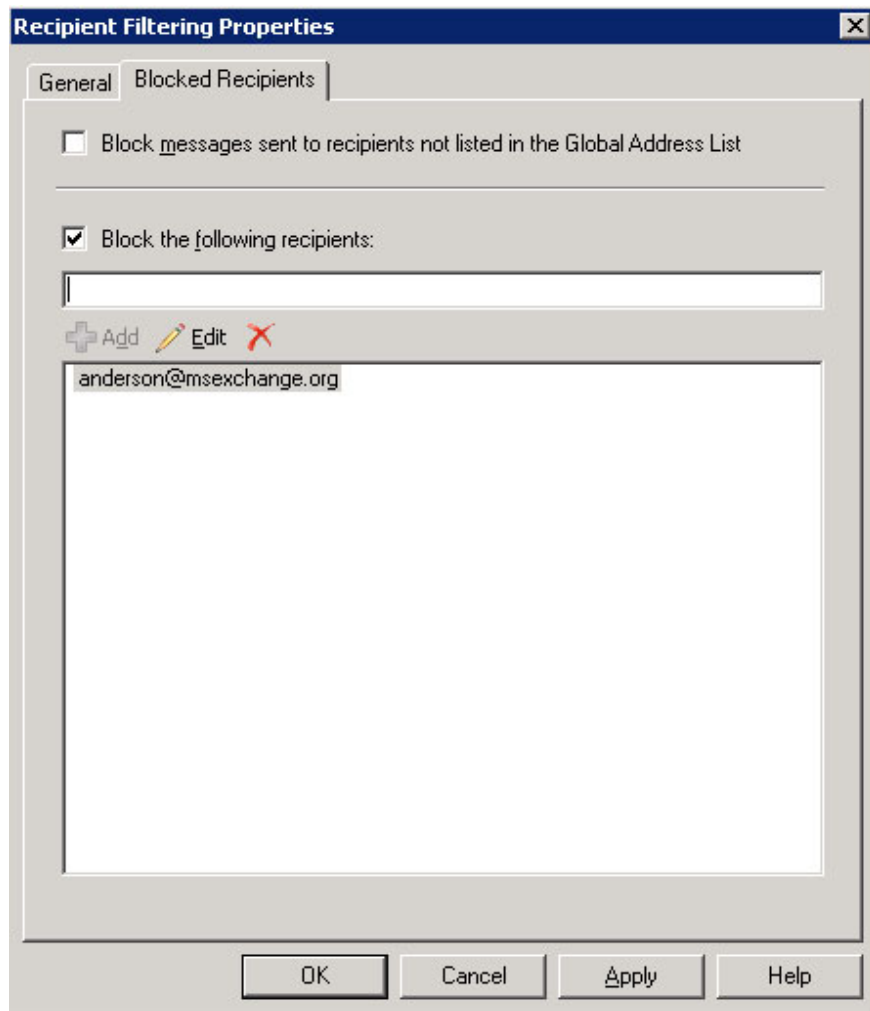


Figure 2: Installation prevents users from receiving mail from the Internet.

Then all mail sent from the Internet to anderson@msexchange.org will receive an NDR indicating that the user does not exist on the system.

However, sometimes you want to apply a higher number of users than just blocking mail traffic sent to a user, for example, allowing only one user to receive mail from the upper level and not receive mail from a mail client. Any other.

Note: You can also do this with the Transport Rule, but the purpose of this article is to introduce many different methods so we will perform the configuration in the mailbox.

The configuration process is done as follows:

1. Open the **Exchange Management Console** .

2. Expand **Recipient Configuration** .
3. Select **Mailbox** .
4. Double click on the mailbox you want to limit.
5. Click the **Mail Flow Settings** tab.
6. Right-click on **Message Delivery Restriction** and select **Properties** .
7. On the dialog box that appears we can limit users to accept or refuse to receive mail from specific users. This user can only receive mail from authenticated users (Figure 3).

Note: *Any mail sent from the Internet is not authenticated.*

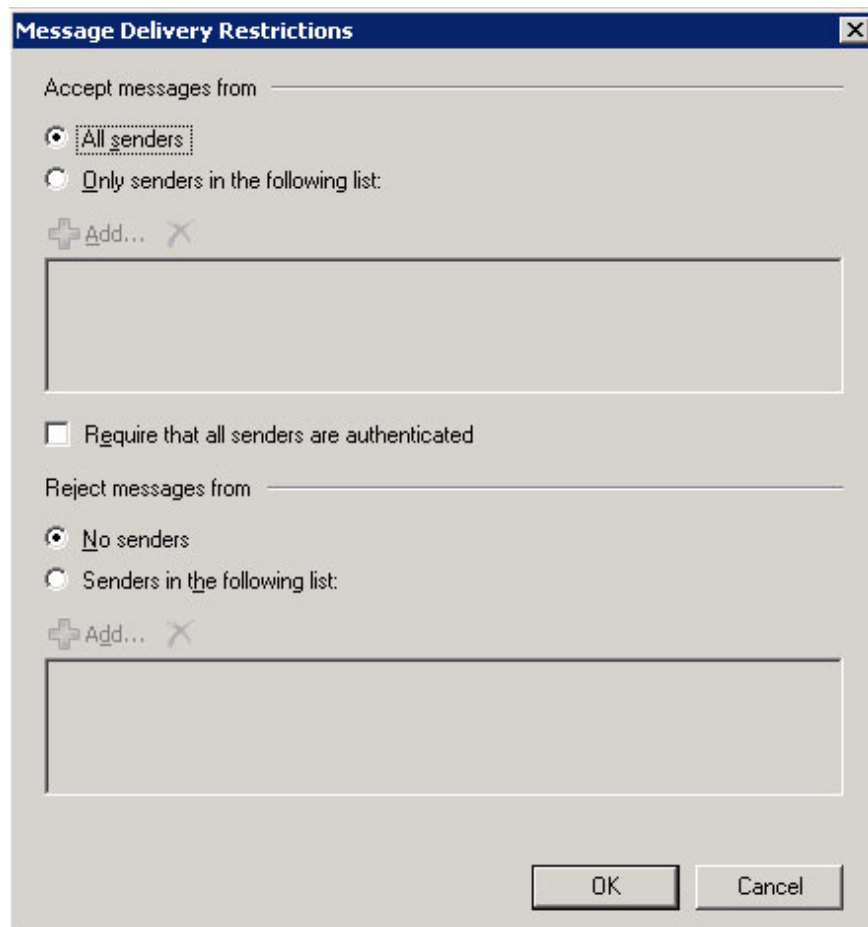


Figure 3: *Configuring mail blocking in the Message Delivery Restriction Properties dialog box.*

Manage outgoing mail traffic

We have explored some methods of blocking incoming mail traffic that apply to specific users in the system, followed by limiting our ability to send internal mail as well as sending mail out of the system. When implementing the limitation, we have applied the method of using Hub Transport structure with Transport Rule that when combined will have great management efficiency. Therefore, a simple way to manage outgoing mail is to use Transport Rules.

1. Open the **Exchange Management Console** .

2. Expand **Organization Configuration** .
3. Click on **Hub Transport** .
4. Select the **Transport Rules** tab.
5. In **Toolbox Actions** , click **New Transport Rule** .
6. On the **Introduction** page, enter a name for the Rule and then click **Next** .
7. On the **Conditions** page, select the **From users inside or outside the organization** section and the **Sent to people** section . In the Step 2 box you can specify the value of the previously selected items. However, in order to do this, you must make sure that the first from the link you have selected all users that are not allowed to send mail, and the **Outside** value is selected for the second link.
8. On the **Actions** page, select the option **Send bounce message to sender with enhanced status code** , then change the content of the mail and status code. In this case we will change the text to *You are not allowed to send external messages* (Figure 4).

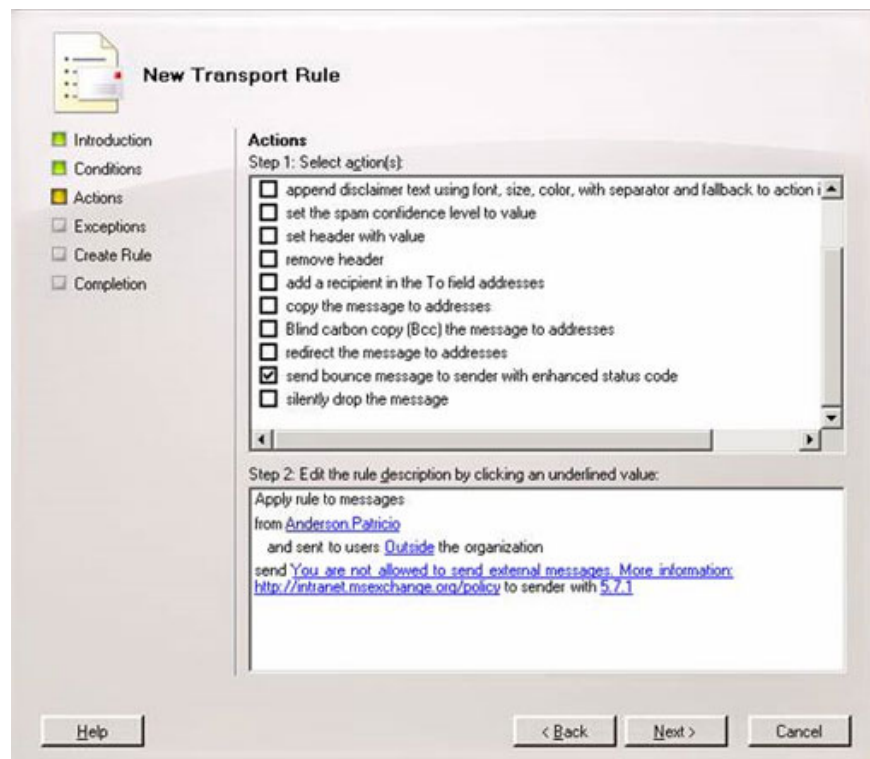


Figure 4: Configuring Actions for Transport Rules.

Then all mail sent by user Anderson Patricio will create an NDR in the mailbox and the user will be able to check the information about the installation information in the internal system we just added in the Transport Rule.

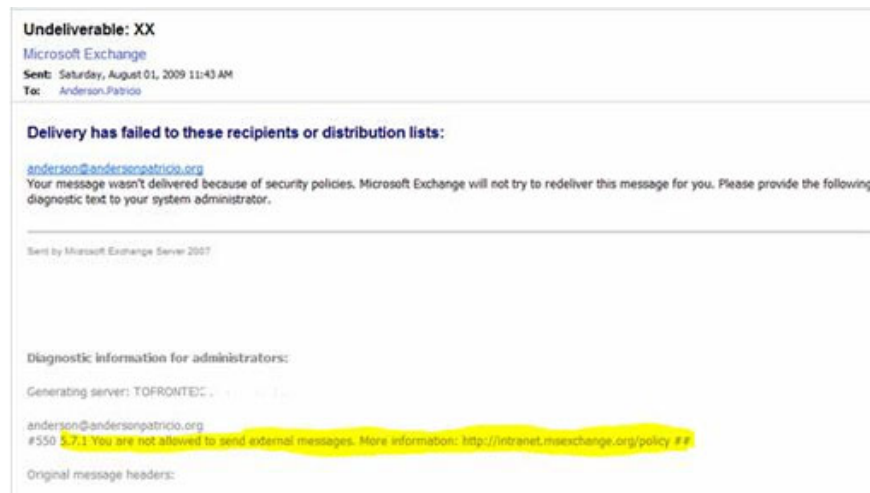


Figure 5: Notice received after sending mail.

Create exceptions

Applying rules on the system is really necessary, but we need to know that there are always some exceptions on the system. Setting these exceptions is quite easy because you can perform it during the process of initializing the Rule.

However, in the Transport Rules we just created, there is no rule that allows an internal user to send mail to an external domain. You can create a new address and specify an exception for this address, but this will not be possible for the entire domain, because in the case the user has a lot of addresses to contact on the domain. then the process of creating a new address will be very difficult and you will be difficult to manage these addresses.

Next we will go back to editing the Transport Rule we created to block mail sent from outside the system, and we select the **except** item **when the pattern text appears in a message header** on the **Exceptions** page. Click on the **message header** link to enter **TO** , and click on the **Text Patterns** link and enter **@ domain.com \$** (where **@ domain.com** is the external domain name to allow users to send mail to).

We will use a RegEx formula to select the domain (s) that we want to accept the current Transport Rule. When using the string '**@ domain.com \$**', all disks containing only that string will match, for example, **user1@domain.com** , **userXX@domain.com** .

The exception we have added to the Transport Rule to allow internal users to send mail to an external domain is shown in Figure 6. At that time, Anderson Patricio users can send mail to an external domain **@ andersonpatricio.org \$** (shown in the TO link).

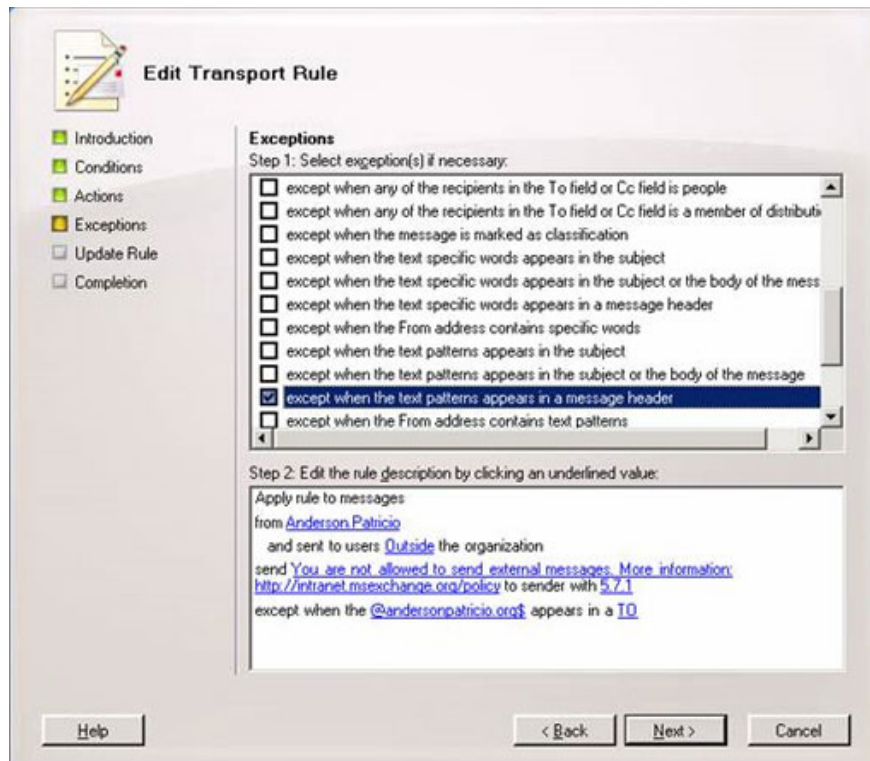


Figure 6: Configuration allows users to send mail to an external domain.

We can use the above method to allow users to receive mail from the Internet by editing the Transport Rule configuration and selecting **except when the text patterns appear in a message header** on the Exceptions page. You then need to add the word **FROM** to the **message header** link, and in the list of approved domains use the same template we used earlier (@ domain.com \$). After configuration allows users to receive mail from the Internet, the Exceptions configuration information of the Transport Rule is shown in Figure 7.

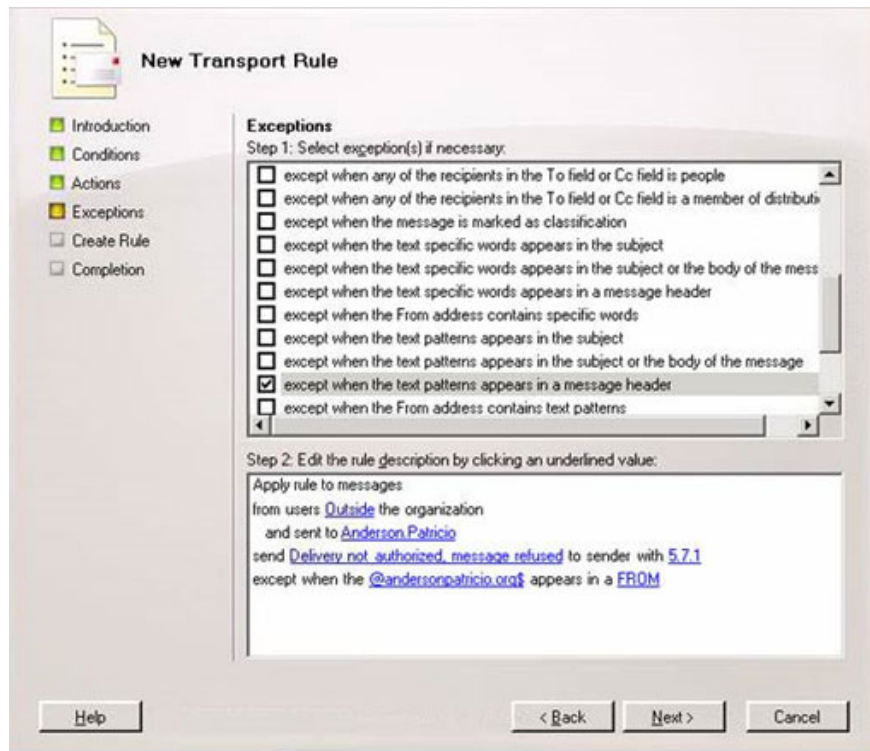


Figure 7: Configuration allows users to receive mail from the external domain.

Then user Anderson Patricio can receive mail sent from the domain outside @ andersonpatricio.org \$ (shown in the FROM link).

Conclude

In this article we learned how to limit internal and inbound mail traffic, the amount of mail received from the Internet, the amount of mail sent out of the system, and a number of rules for the most users. determined. These are common operations that the Mail Server system administrator must always perform.

You finished reading the article "**Limit sending and receiving mail in Exchange 2007**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.