

Using Spam blocker in a perimeter network or DMZ

To increase security, many organizations deploy a gateway server to relay or act as a smart host within a perimeter network, also known as Demilitarized Zone (DMZ). Since Policy Patrol requires you to open a port to retrieve the users from your Active Directory or mail server, administrators will usually choose to install Policy Patrol within the internal network rather than the DMZ or Perimeter Network. As long as you do not want to use Policy Patrol Spam blocker for checking real-time black lists, this setup is fine.

However if you wish to check real-time spam black lists, the Policy Patrol installation on the internal network will not receive email messages directly from the Internet, and therefore Policy Patrol Spam blocker will resolve the IP address of the Relay server (192.125.55.10 in Figure 1), and not the original sender of the mail. This means that if installed on the internal network, Policy Patrol is unable to check whether the sender is listed on a real-time black list. Therefore, if you wish to check for real-time black lists, Policy Patrol Spam blocker must be installed on the Relay server.

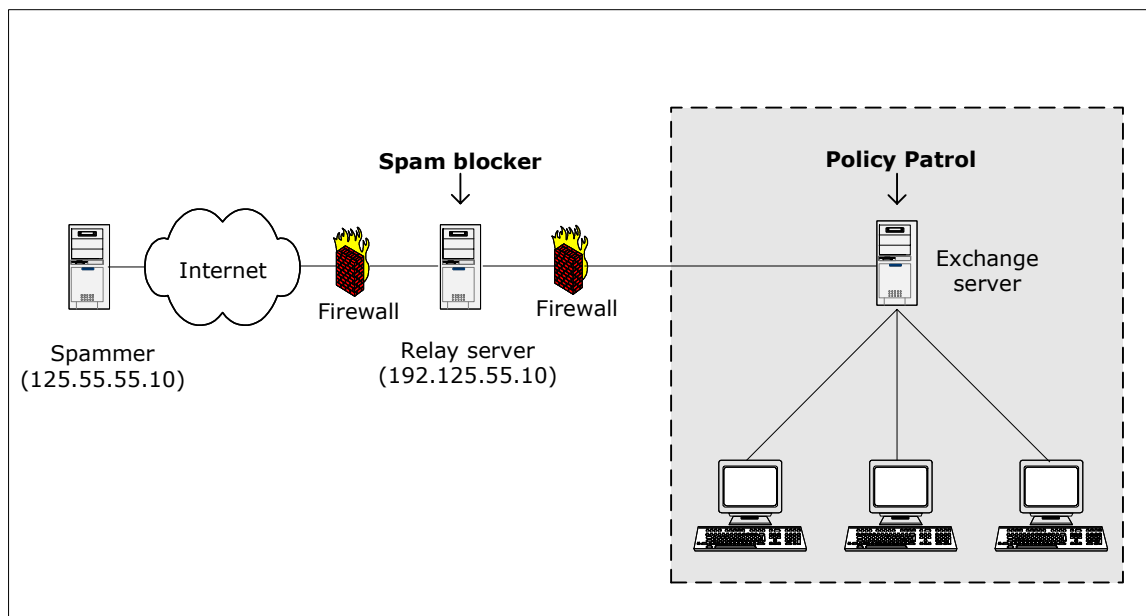


Figure 1 - Installing Spam blocker in a perimeter network or DMZ

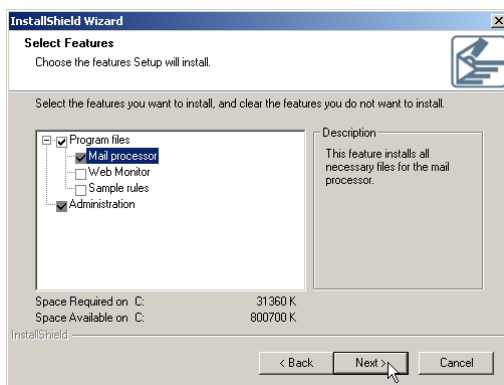
There will be no security implications since the Spam blocker installation in the DMZ will not require any users to be retrieved and hence no ports will need to be opened. This Spam blocker installation will only reject and/or add X-headers to messages that originate from real-time black lists. The full Policy Patrol version (with users) on the internal network, will process any messages that Spam blocker added an X-header

to, along with any other rules you wish to configure. For this setup you will require an additional serial number (unless you are evaluating). To request your free Spam blocker serial number, please send an email to orders@reearthsoftware.com with your current serial number. The instructions below explain the steps that need to be followed for installing and configuring Spam blocker within a DMZ or perimeter network.

Step 1. Install Spam blocker on the Relay server

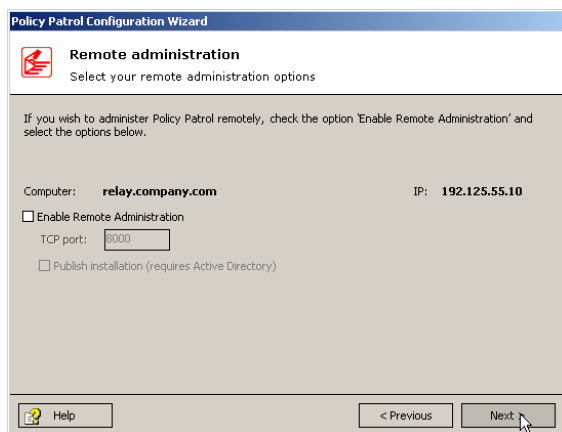
Follow the next steps to install Policy Patrol Spam blocker on the Relay server (if you are installing Policy Patrol on a different machine than Exchange 2000/2003 server, please consult the Quick Start guide for instructions on installing Policy Patrol on a separate machine):

1. Double-click on **PolicyPatrol.exe**. The Install Program will start up. If you do not have Microsoft .NET Framework 1.1 installed, the installation program will install it for you (if the Policy Patrol download included the .NET Framework), or download and then install it for you (if the Policy Patrol download did not include the .NET Framework).
2. In the welcome screen, click **Next**.
3. Read the License Agreement and click **Yes** to accept the agreement.
4. Enter your user name and company name. If you want anyone who is logged on to the computer to be able to access Policy Patrol, select **Anyone who uses this computer (all users)**. If you only wish yourself to be able to access the program, select **Only for me (user name)**. Click **Next**.
5. Select **Custom** as the setup type. Select the destination location and click **Next**. Select to install the **Mail processor** and **Administration**. Click **Next** to continue.



6. Specify a user account (The Policy Patrol installation will not actually use this account since there will be no synchronization). Click **Next**.
7. Review the installation settings. If they are correct, click **Next** to start copying files.
8. When Policy Patrol has finished copying the files, the Policy Patrol Configuration wizard will start up. In the welcome screen, click **Next** to start the wizard.

9. Check the option **Install evaluation version** or enter your serial number by unchecking **Install evaluation version** and clicking **Add**. When you are done, click **Next**.
10. Enter your local domain(s). Your local domain is the part after the @ sign of your email address, for instance `redearthsoftware.com`.
11. Select the virtual SMTP server that you wish Policy Patrol to monitor. If you only have one virtual SMTP server installed, the other options will be grayed out. Click **Next**.
12. Do not enter any email address(es) for the Policy Patrol Administrator and click **Next**.
13. Uncheck the option **Create default connector** and click **Next**.
14. Uncheck the option **Enable automatic update notifications**. Click **Next**.
15. Do not tick the check box **Enable Remote Administration** and click **Next**.

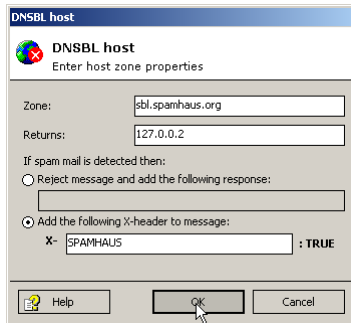


16. Click **Finish** to exit the configuration wizard.

Step 2. Configure Spam blocker on the Relay server

Follow the next instructions to enable the Spam blocker:

1. Go to Start > Programs > Policy Patrol > Administration. Select **<server name>** and choose **Connect**.
2. Go to **Spam blocker**. Tick **Enable real time spam blocker**. Click **Add** to configure a spam black list. Enter the Zone and Return values for the list. For instance for the Spamhaus Block List (SBL), enter `sbl.spamhaus.org` for the zone and `127.0.0.2` for the Returns. If you select **Reject message and add the following response** the message will not be accepted and will therefore not use up any bandwidth. The response you enter will be sent to the sending mail server. If you want to quarantine or delete the message (with the option to undelete), or add a tag, select **Add the following X-header to message** and enter the header to be added. For instance for the Spamhaus Block List, enter `SPAMHAUS`. When you are done, click **OK**.

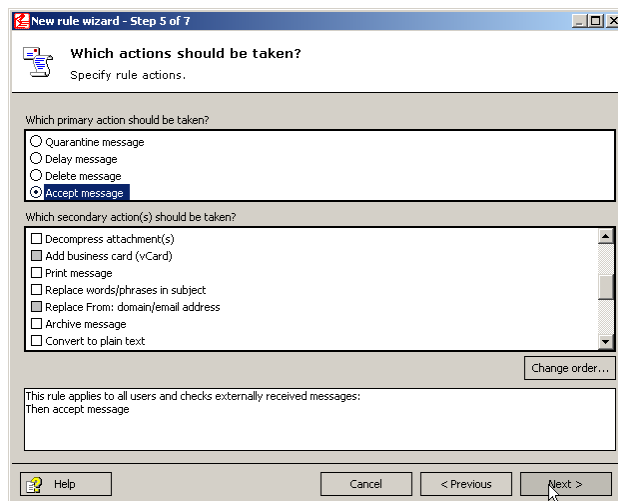


You can add as many spam black lists as you wish. For a list of possible spam lists, go to: <http://www.email-policy.com/spam-black-lists.htm>. If you configure Spam blocker to add an X-header, you must create the rule that processes messages with this X-header on the Policy Patrol installation within the internal network. When you are ready configuring the real time spam black lists, click **Commit**.

If you configured Spam blocker to add a header for a real time black list:

If you want Spam blocker to add a header to messages that originate from a real time black list, you must create a rule that accepts all externally received messages (this is needed for the header to be saved in the message):

1. Go to **Policy rules > New**.
2. Select **All users** and click **Next**.
3. Select **Only the following messages** and tick **Externally received**. Click **Next**.
4. Select **No conditions**, click **Next**.
5. Select **No exceptions**, click **Next**.
6. Select **Accept** as the primary action and do not select any secondary actions. Click **Next**.

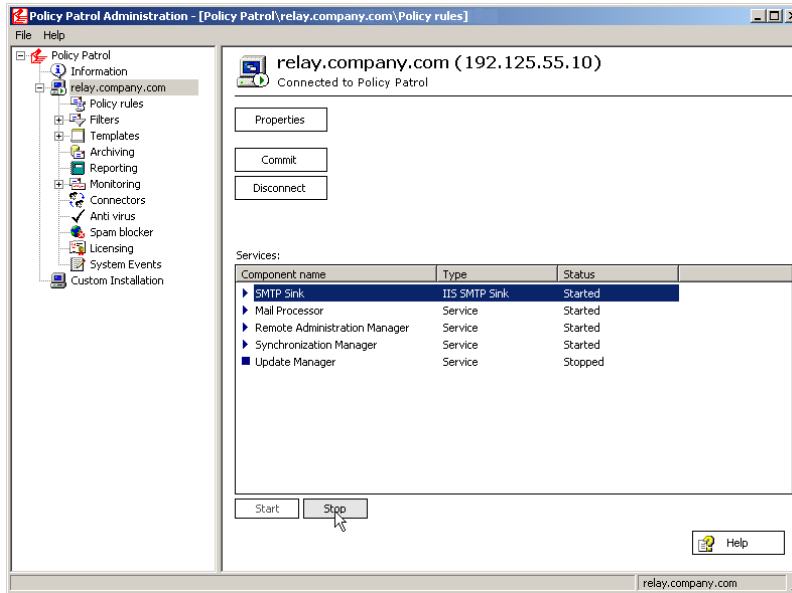


7. Do not configure any scheduling and click **Next**.

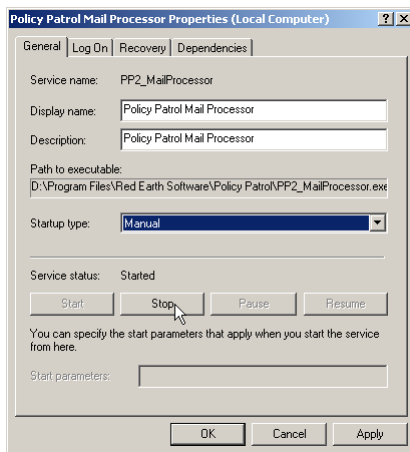
8. Enter 'Accept all messages' as the rule name and click **Finish**.
9. Select **<server name>** and press **Commit** to save the changes.

Only if you did not select to add a header for any real time black list:

1. Stop the Policy Patrol SMTP Sink by clicking on **<server name>**, selecting **SMTP Sink** and clicking **Stop**.



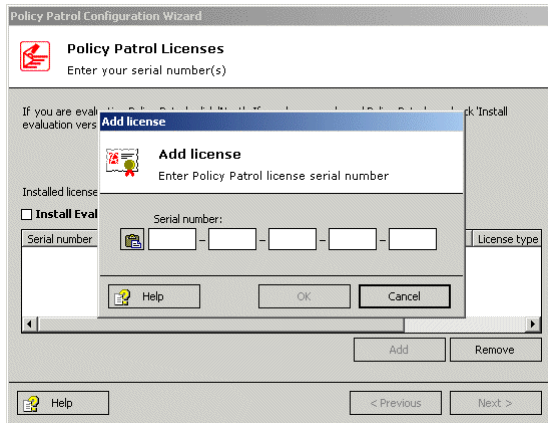
2. Stop all Policy Patrol services by going to Start > Settings > Control Panel > Administrative tools > Services. Double-click on the **Policy Patrol Mail Processor** service. In Startup type select **Manual**, and press **Stop**. Follow the same procedure for each of the remaining Policy Patrol services: Policy Patrol Remote Manager, Policy Patrol Synchronization Manager and Policy Patrol Update Manager (this service will already be stopped and set to manual if you did not check 'Enable automatic update notifications' during installation).



Step 3. Install Policy Patrol within the internal network

Now you must install Policy Patrol on the machine within the internal network as per the usual instructions (if you are installing Policy Patrol on a different machine than Exchange 2000/2003 server, please consult the Quick Start guide for instructions on installing Policy Patrol on a separate machine):

1. Double-click on **PolicyPatrol.exe**. The Install Program will start up. If you do not have Microsoft .NET Framework 1.1 installed, the installation program will install it for you (if the Policy Patrol download included the .NET Framework), or download and then install it for you (if the Policy Patrol download did not include the .NET Framework).
2. In the welcome screen, click **Next**.
3. Read the License Agreement and click **Yes** to accept the agreement.
4. Enter your user name and company name. If you want anyone who is logged on to the computer to be able to access Policy Patrol, select **Anyone who uses this computer (all users)**. If you only wish yourself to be able to access the program, select **Only for me (user name)**. Click **Next**.
5. Select the setup type. If you select **Complete**, the complete program will be installed in the default folder C:\Program Files\Red Earth Software\Policy Patrol. If you select **Custom**, you will be able to change the location of the Policy Patrol folder and specify whether you wish to install the Mail processor, Administration console, Web monitor and/or sample rules. Click **Next** to continue.
6. Specify the user account that must be used for synchronization. Make sure that this account has access rights to the Active Directory. Click **Next**.
7. Review the installation settings. If they are correct, click **Next** to start copying files.
8. When Policy Patrol has finished copying the files, the Policy Patrol Configuration wizard will start up. In the welcome screen, click **Next** to start the wizard.
9. If you are evaluating Policy Patrol, click **Next**. If you have purchased Policy Patrol, uncheck **Install evaluation version** and click **Add**. Enter your serial number and click **OK**. If you received your serial number via email, you can copy the serial number from your email and click on the 'Paste' button. Click **Next** to continue.



10. Enter your local domain(s). Your local domain is the part after the @ sign of your email address, for instance `redearthsoftware.com`. If you have installed Policy Patrol on the same machine as your mail server (only possible for Exchange 2000 or 2003), Policy Patrol will retrieve your local domains for you. To add a local domain, click on **Add**. Enter the domain, for instance `redearthsoftware.com`, and click **OK**. To remove a local domain, click **Remove**.

If you do not wish Policy Patrol to process emails from certain mail servers, enter the IP addresses in **Exclude IP addresses**. Click on **Add**, enter the IP address and click **OK**. When you are ready, click **Next**.

11. Select the virtual SMTP server that you wish Policy Patrol to monitor. If you only have one virtual SMTP server, the other options will be grayed out. Click **Next**.
12. Enter the email address(es) for the Policy Patrol Administrator. These addresses will be used for Policy Patrol system notifications and Administrator notifications configured in rules. You can enter a To:, Cc: and Bcc: email address. Remember that the From: field must include an existing, internal email address. Click **Next**.
13. You must configure at least one connector so that Policy Patrol can retrieve your users. Select the type of connector you wish to create; **Active Directory/Exchange 2000, Exchange 5.5** or **Lotus Domino** connector. If you selected Active Directory, you can use the default Active Directory domain controller, or you can enter the name or IP address of another server. If you selected Exchange 5.5 or Lotus Domino you must enter the name or IP address of the mail server (if your LDAP service is listening on a different port than 389, you must also enter the LDAP port as follows: `<IP address>:<LDAP port>`, e.g. `10.0.0.15:390`).

Policy Patrol will synchronize all users from the connector. If you wish to create a more specific connector, or if you wish to pick up users from a text file, uncheck **Create default connector**. You will then be able to configure your connector after installation in 'Connectors'. For instance, if you have a lot of users in your Active Directory and you only want to use Policy Patrol for selected users, it is better to create a more specific connector, rather than synchronizing all the users in your Active Directory. If you wish to use multiple connectors, for instance one Exchange 2000 connector and one Lotus Domino connector, you can create the default connector during installation, and add more connectors in the Administration console after installation. When you are ready, click **Next**.

Note: The Default connector is not **scheduled**. If you want Policy Patrol to automatically retrieve new users and updated user properties, you must configure scheduling of the Default connector after installation from **Connectors > Default connector > Properties > Schedule** tab.

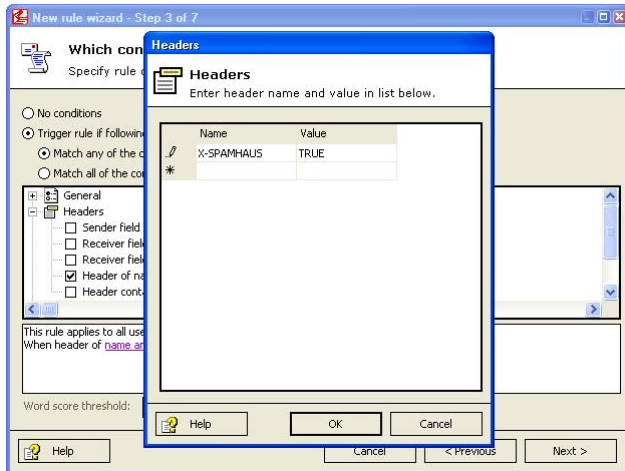
14. Policy Patrol will now display all the users from the default connector. All users will automatically be licensed. If you have more users than licenses, you must remove some licensed users after installation in 'Licensing', since otherwise Policy Patrol will select the licensed users randomly. Click **Next**.
15. If you wish the Administrator to receive an email notification when a new Policy Patrol update is available, check the option **Enable automatic update notifications**. In addition to an email notification, the Policy Patrol Update Wizard icon will appear in the system tray. Note that this option requires an Internet connection on the Policy Patrol machine. Click **Next**.
16. If you wish to be able to administer Policy Patrol remotely, you must tick the check box **Enable Remote Administration**. Enter the TCP port to use. By default 8000 is used. If you have multiple Policy Patrol installations that you wish to access remotely, each installation must use a different port. Select **Publish installation** to display the computer in a list that can be connected to from the remote machine. Note that this option is only possible if you have Active Directory.
17. Click **Finish** to exit the configuration wizard.

Step 4. Configure a rule to process emails identified by Spam blocker

If in step 2 you configured Spam blocker to reject messages, these messages will not be accepted and therefore will never reach the Policy Patrol installation within the internal network. However, if you configured Spam blocker on the Relay server to add a header to messages that originate from real-time spam black lists, these messages will arrive at the second Policy Patrol installation, with the header added.

To further process these messages, you must create a rule on the Policy Patrol installation within the internal network that specifies what actions Policy Patrol should take:

1. Go to Policy rules and click **New**.
2. Select the users for the rule. Click **Next**.
3. Select **Only the following messages** and tick **Externally received**. Click **Next**.
4. Select **Trigger rule if following conditions are met**. Go to 'Headers' and select the option **Header of name and value exists**. Click on the link in the description and enter the X-header that Policy Patrol should search for, for instance `X-SPAMHAUS` as the name and `TRUE` as the value. Click **OK** and **Next**.



5. If you want to set exceptions, select **Do not trigger rule if following exceptions are met**. For instance you can exclude allowed newsletters and existing contacts by going to 'Headers' and selecting the option **Sender field contains domain or email address**. Then click on the link and select the sample 'Automatic white list' and 'Newsletters' filters (remember to enter your newsletter email addresses in the Newsletters filter). Click **OK** and **Next**.
6. Now specify what actions you wish to take. You can quarantine, delay, delete or accept the message. Furthermore, you can select secondary actions, such as sending an email notification, adding a tag, or adding the sender to a filter. When you are ready, click **Next**.
7. Leave the rule unscheduled and click **Next**.
8. Enter a name for the rule and any comments and click **Finish**.
9. Click on **<server name>** and press **Commit** to save the changes.

More information

- ⇒ For more information on how to configure Policy Patrol to stop junk mail, please download the document 'How to filter spam with Policy Patrol' from: <http://www.policypatrol.com/docs/How-to-filter-spam-with-Policy-Patrol.pdf>.
- ⇒ For more information on how to configure Policy Patrol, please consult the program help or download the product manual from: <http://www.policypatrol.com/docs/policypatrol2manual.pdf>.
- ⇒ For more information on relaying your mail through the Windows SMTP service, consult the following Microsoft Knowledge Base article 'XCON: How to set up Windows 2000 as an SMTP Relay Server or Smart Host' at: <http://support.microsoft.com/default.aspx?scid=kb;en-us;293800>.
- ⇒ For a list of available real-time black lists, go to: <http://www.email-policy.com/spam-black-lists.htm>.
- ⇒ If you still have questions after reading this document, please consult our online knowledge base at <http://www.redearthsoftware.com/kb.asp>, or send an email to support@redearthsoftware.com.

Contacting Red Earth Software

Red Earth Software LLC
200 Marcy Street
Portsmouth, NH 03801
United States
Phone: (603) 436-1319
Fax: (603) 457-8455
Sales: sales@reearthsoftware.com
Support: support@reearthsoftware.com

Red Earth Software (UK) Ltd
20 Market Place
Kingston-upon-Thames
Surrey KT1 1JP
United Kingdom
Tel: +44-(0)20-8605 9074
Fax: +44-(0)20-8605 9075
Sales: sales@reearthsoftware.co.uk
Support: support@reearthsoftware.co.uk

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2003 by Red Earth Software.