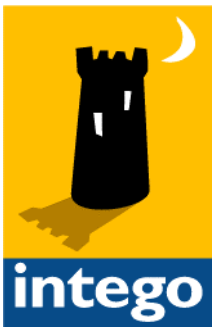
NetBarrier

User's Manual



NetBarrier for Macintosh

Intego, Inc.
www.intego.com

Contents

1- About NetBarrier

What is NetBarrier?

NetBarrier is the Internet security solution for Macintosh computers. It offers thorough protection against intrusions coming across a network, whether the Internet or a local AppleTalk network.

NetBarrier protects your computer from intrusions by constantly filtering all the activity that enters and leaves through the Internet or a network. You are protected against thieves, hackers and intruders, and warned automatically if any suspicious activity occurs.

NetBarrier's Features

NetBarrier has three lines of defense, to protect your computer and your data from intrusions and attacks.

Personal firewall

NetBarrier contains a personal firewall that filters data as it enters and leaves your computer. A full set of basic filtering rules are used by default, and its Customized protection mode allows you to create your own rules, if you need to.

Antivandal

NetBarrier's Antivandal is a powerful guardian for your computer. It watches over your computer's network activity, looking for signs of intrusion, and, if it detects anything, stops the intruder in their tracks, and sends you an alert. The Antivandal also has another powerful function, the Stop List, that records the address of any intruder who attempts to get into your computer, and ensures that they cannot come back. There are also several options that allow you to choose the type of protection you wish to have on your computer.

Alerts

NetBarrier stops all incoming data that is considered hostile. An Alert is displayed, showing why the data was stopped, and asking you to allow or deny it. There are also Alert options that can be selected, such as having NetBarrier come to the front, play a sound, or send an e-mail message to the address of your choice in the case of an Alert.

Stop List

When an intruder is detected trying to break in to your computer, NetBarrier allows you to put them on the Stop List, where their network address will be saved, and if a computer with the same address tries to enter your computer again, it will be automatically refused.

Data Filter

NetBarrier has a unique function that protects you and your information - the Data Filter ensures that any sensitive information, which you choose to protect, cannot leave your computer and go onto a network. You choose what to protect, say, your credit card number, passwords, or key words that appear in sensitive documents, and NetBarrier's Data Filter checks each outgoing packet to make sure that no documents containing this information will be sent. Not only does this protect you from sending documents containing this information, but it protects against anyone who has network access to your computer from taking copies of them.

NetBarrier's Privacy Protection

NetBarrier also helps protect your privacy. It has several features that block spam and ad banners, and lets you manage cookies, and delete them whenever you want. It also has a unique feature that hides information about your computer: its platform, which browser you are using, and the last web page you visited.

Using this user's manual

You are a:

Home user, connected to the Internet

If this is your situation, you should read chapter 2, **Introduction to Computer Security**, and then go on to chapter 3, **Installation**, and chapter 4, **Quick start**. If you feel you have learned enough, you can stop there - NetBarrier is configured to automatically protect your computer from intruders. If you want to know more, go on and read chapter 5, **The Three Lines of Defense**.

Business or Academic user, connected to a local network, and the Internet

If you are connected to a local network, you will want to read the above as well. NetBarrier's basic protection modes will probably be sufficient for you.

Advanced user, using your computer as a server, or administering a network

The entire manual concerns your situation, but you will especially want to read chapter 7, **Customized Protection**, to find out how to create your own rules.

There is a glossary at the end of the manual that defines the specific terms used.

2 - Introduction to Computer Security

Why You Need to be Protected

Whether you use your computer for work or for just surfing the Internet, whether you are on-line all day long, or just occasionally, whether you are on a local network in a home office, or part of a large corporation or educational institution, your computer contains sensitive information. This may be anything from your credit card numbers to your bank account information, contracts with customers or employees, confidential projects or e-mail messages and passwords. No matter what you have on your computer that is for your eyes only, there is somebody out there who would certainly find it interesting.

The more you use your computer for daily activities, whether personal or professional, the more information it holds that should be protected.

Think of your computer as a house. You certainly lock your doors and windows, when you go out, but do you protect your computer in the same way? As long as you are connected to a network, there is a way for wily hackers or computer criminals to get into it - unless you protect it with NetBarrier.

When your computer is connected to a network, whether it be a private, local network, or the Internet, it is like a house on a street, with doors and windows. NetBarrier works like a lock, to protect those doors and windows. You never know who is watching when you are connected to a web site. Maybe that gaming site, with the cheats you were looking for, has a cracker behind it, who wants to snoop on your computer, to see if he can find anything interesting. Or perhaps that stock market information site, where you went to get company results, has a curious hacker watching who connects, and who likes to mess up people's computers just for fun.

The worst thing is that without NetBarrier, you will never know if anyone is trying to get into your computer.

A computer is only as secure as the people who have access to it. NetBarrier protects your computer by preventing unauthorized network access to your computer, and by protecting against unauthorized export of private information.

How can a computer be totally safe?

It has been said that the only computer that is truly secure is one that is switched off and unplugged, locked in a titanium-lined safe, buried in a concrete bunker, and surrounded by nerve gas and very highly-paid armed guards. Obviously, this is not practical - if you have a computer, you want to be able to use it.

But NetBarrier provides a level of protection that goes far beyond what most users need, and its customizable rules make it a powerful tool for system and network administrators, allowing them to adapt the protection to their specific needs.

What is a firewall?

A firewall is, as its name suggests, like a wall. It protects your computer or network by separating users into two groups - those inside the wall, and those outside. It is configured to determine what access outsiders have to computers inside the wall, and what access insiders have to computers and networks on the other side of the wall.

A firewall is a kind of filter that acts between your computer, or network, and a wide area network, such as the Internet. It functions by filtering packets of data, and examining where they come from and where they are going.

NetBarrier goes even further by allowing advanced users to configure specific rules, to protect against foes that wish to infiltrate your computer.

Friend or foe?

Every wall has to have a gate, so people can get in and out. NetBarrier's Antivandal acts as a filter, or a guard standing at the gate in the wall, checking all incoming and outgoing data for signs of hackers, crackers, vandals, spies, intruders and thieves. This can be done because there are many "standard" ways to enter an unprotected computer, and NetBarrier recognizes these methods.

What You Risk

Why people break into computers

There are many different reasons why people break into computers. Sometimes, this is done just as a way to get into yet more systems; by hopping between many machines before breaking into a new one, the cracker hopes to confuse any possible pursuers and put them off the scent. There is an advantage to be gained in breaking into as many different sites as possible, in order to "launder" your connections.

Another reason is that some people simply love to play with computers and stretch them to the limits of their capabilities. This is a bit like people who write graffiti on walls - they just want to do it because it’s there.

But the more serious invaders are real criminals. These may be competitors, looking for information on your company's activities, projects or customers, criminals, looking for passwords and credit card numbers, or simply spies. While most companies have security policies, few of them think of protecting data on their employees' home computers - but these computers often have sensitive documents that employees have brought home from work.

Unfortunately, we live in a world where anything of value is a target for thieves. Since today's economy is built around information, it is obvious that information has become the latest target. Here's a simple example: last year, on Mother's Day, you sent your mother, or maybe your wife, some flowers. You ordered by fax, because you don't trust sending your credit card number over the web. But the document that you typed, containing your credit card number, is still on your hard disk. If someone found it, they would have your credit card number, and you might become a victim of fraud.

The different types of attacks and intrusions possible

There are many reasons why people attempt to obtain entry into other people's computers, and methods for doing so. Here are some of them:

- Stealing confidential documents or information.
- Executing commands on your computer that modify the system, erase your hard disk, and disable your computer.
- Hacking web sites, by replacing pages with different text and graphics.
- Launching denial-of-service attacks, that can render your computer temporarily unusable.
- Getting information about your computer, that will allow someone to break into your network, or your computer, at a later time.

Privacy Protection

One thing you don't notice when you surf the Internet is how much personal information different web sites try to get from you. You can clearly see the ones that openly ask you to register to use them; you enter a user name and a password, and sometimes your name, address, and other information as well. This information is often used to trace your behavior, to find what your interests are, and to market products and services to you.

More and more Internet users refuse to give web sites this kind of information. Sometimes you learn the hard way: you register at a web site, and end up getting spam, e-mail about things you never requested. But, at that point, it's usually too late.

But web sites have other ways of getting information about you and your behavior. Did you know that it is simple for a web site to "ask" your computer what operating system you are using, which browser you are surfing with, and even the last web page you visited?

Then there are cookies. A cookie is a file on your hard disk, which contains information sent by a web server to a web browser and then sent back by the browser each time it accesses that server. Typically, this is used to authenticate or identify a registered user of a web site without requiring them to sign in again every time they access that site. Other uses are maintaining a "shopping basket" of goods you have selected to purchase during a session at a site, site personalization (presenting different pages to different users), tracking a particular user's access to a site.

While cookies have legitimate uses, as we have seen above, unscrupulous web sites use them to collect data on your surfing habits. They then sell this data to companies that will then target you specifically for products and services that correspond to these habits, or even ensure that when you surf on certain sites, you see ad banners that correspond to these habits.

NetBarrier's approach to privacy is simple: it provides you with the means to prevent certain information from being recorded without your knowledge.

3 - Installation

System Requirements

- Any MacOS compatible computer with a PowerPC processor
- OpenTransport
- Mac OS 8.1 or higher
- 16 MB RAM
- 5 MB free hard disk space
- Internet Config 1.1 on higher
- Minimum Screen resolution 800 x 600

Installing NetBarrier

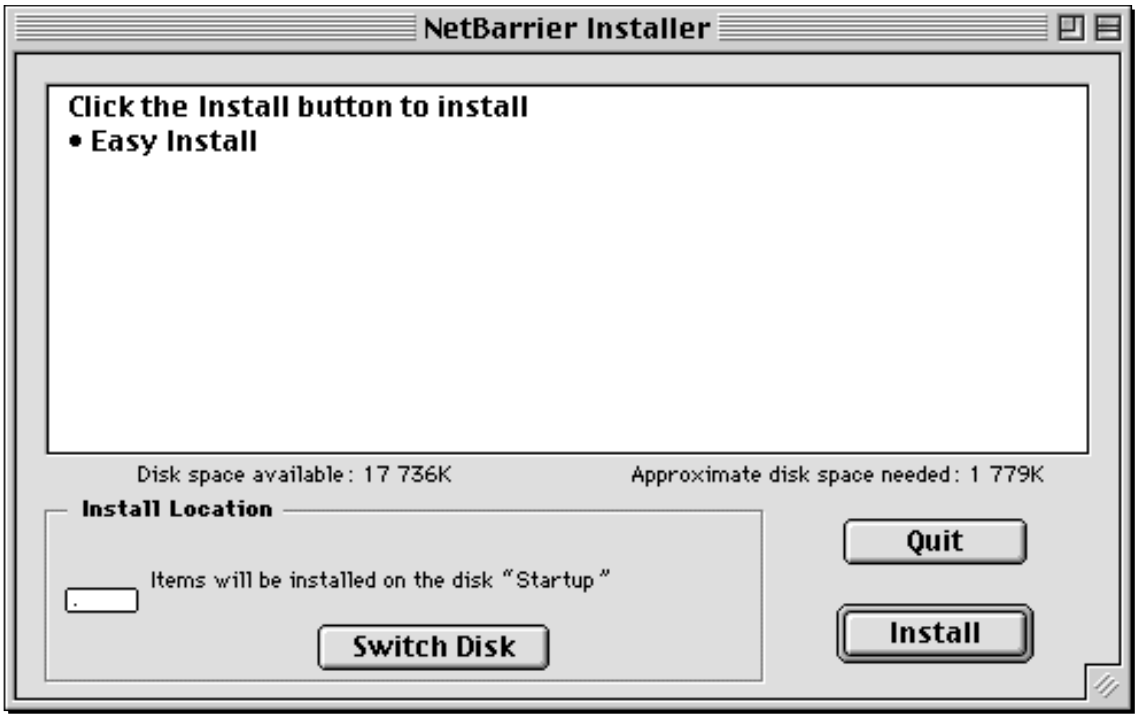
Installing NetBarrier is very simple. Insert the NetBarrier CD-ROM in your computer's CD-ROM drive. A window will open, containing the NetBarrier installer, the Read me file, the NetBarrier manual (this file), an Acrobat Reader installer, and an Internet Config installer.

First, read the Read me file, for any late-breaking changes.

Then, double-click on the NetBarrier installer.

You will see a window displayed containing the NetBarrier license. Read this license carefully, and, if you accept it, click on Accept.

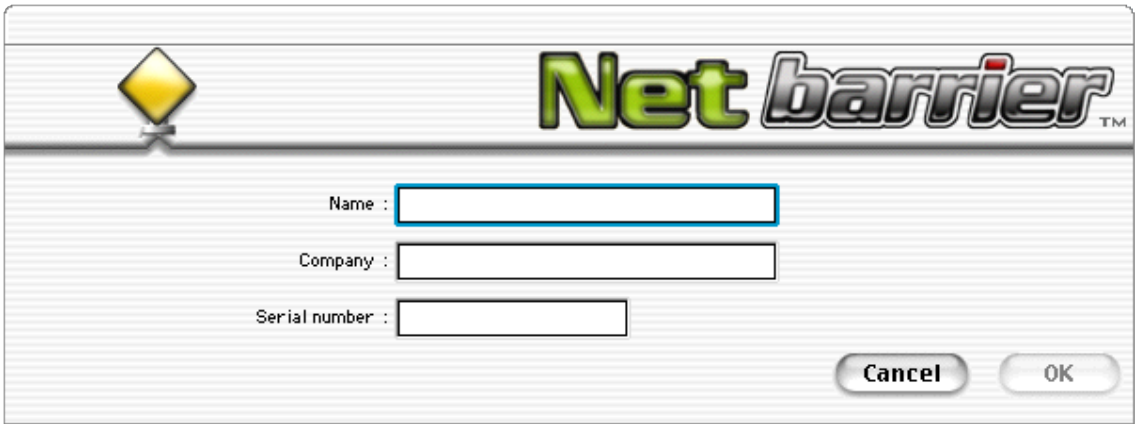
The following window will be displayed:



Click on Install to install NetBarrier. NetBarrier will be installed, and a dialog will ask if you wish to continue, and make another installation, Quit or Restart your computer. Your computer must be restarted for NetBarrier to function, so you should restart now. If not, you can restart later, but NetBarrier will not be active until you do so.

Registering NetBarrier

When you restart your computer, NetBarrier will open its Registration program, and display the following window:



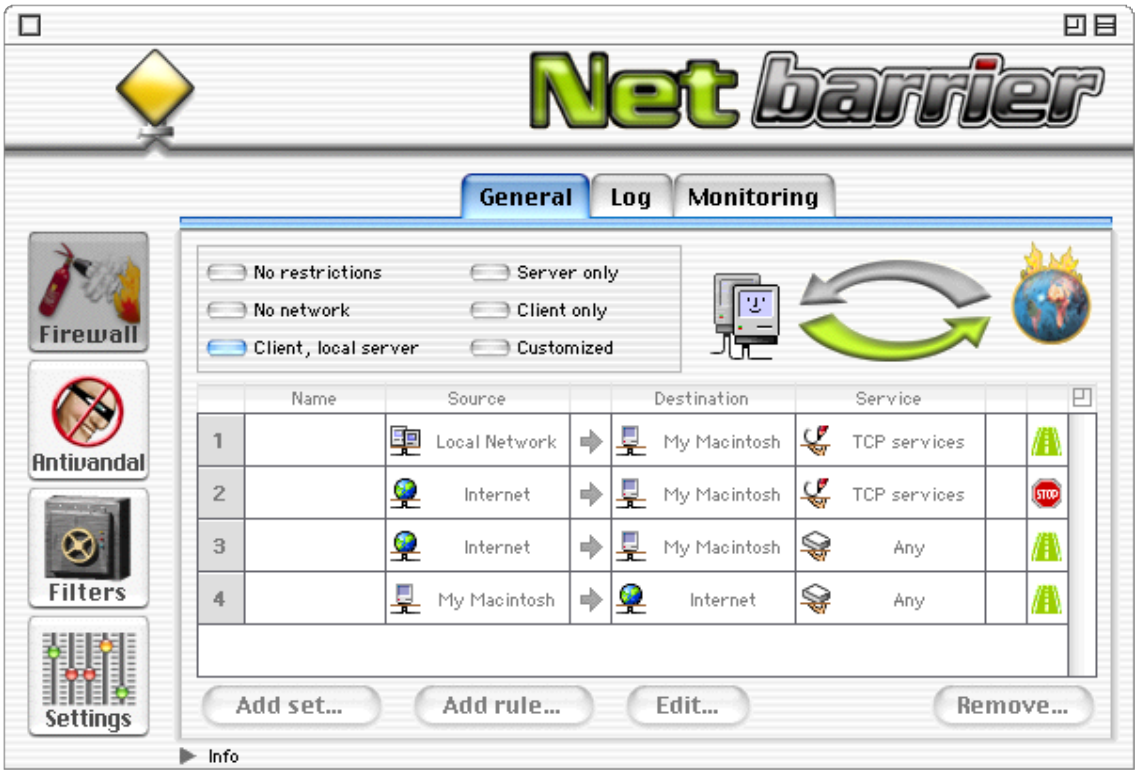
You must enter your name, company, if any, and your serial number. The serial number is found on a sticker on the NetBarrier CD, and is made up of four groups of four characters, and is not case-sensitive.

When registration is completed, NetBarrier will open its control panel, and you can configure the program.

4 - Quick Start

NetBarrier's Default Mode

When you install NetBarrier, and restart your Macintosh, it automatically begins monitoring your computer's network activity. The Antivandal is configured to protect your computer from intrusions. The Firewall, however, needs to be set to correspond to your type of network activity. See chapter 5, **The Three Lines of Defense** for information on which Firewall configuration to select.



The NetBarrier Menu

When NetBarrier is installed, it places a menu with the Intego icon in your menubar.

This menu can be used for two things: you can open the NetBarrier control panel, by selecting NetBarrier from the menu, and you can open the NetUpdate control panel, to check for update versions of NetBarrier, or to set NetUpdate preferences. See the NetUpdate User's Manual for more on NetUpdate and its preferences.

The NetBarrier Control Strip Module

NetBarrier includes a useful and practical Control Strip module. This module allows you to keep an eye on your network traffic, both incoming and outgoing. The top line, **In**, is traffic being received, and the bottom line, **Out**, is traffic being transmitted. The graphical display gives you an idea of how much data is being transmitted or received.

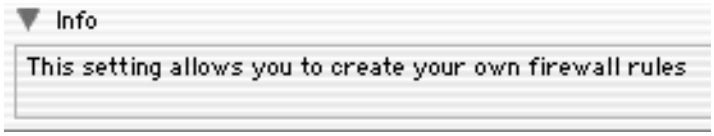
You can also open NetBarrier from this Control Strip module, by selecting Open NetBarrier from the Control Strip module, and change some of its settings on the fly. For more on the NetBarrier Control Strip module, see chapter 5, Using the NetBarrier Control Strip Module.

The control strip also gives you quick access to your different NetBarrier configurations. To change from one configuration to another, simply click on the control strip module, and select the configuration you would like to use. For more on configuration sets, see chapter 6, Configuration Sets.

Getting Help

You can get help on some of NetBarrier's functions by clicking on the info button:

This will toggle the Info field at the bottom of the NetBarrier window. If you move your cursor over different areas in NetBarrier's window, some of them will be explained in this field.



You can also get help in this manual, or by checking the Intego web site: www.intego.com.

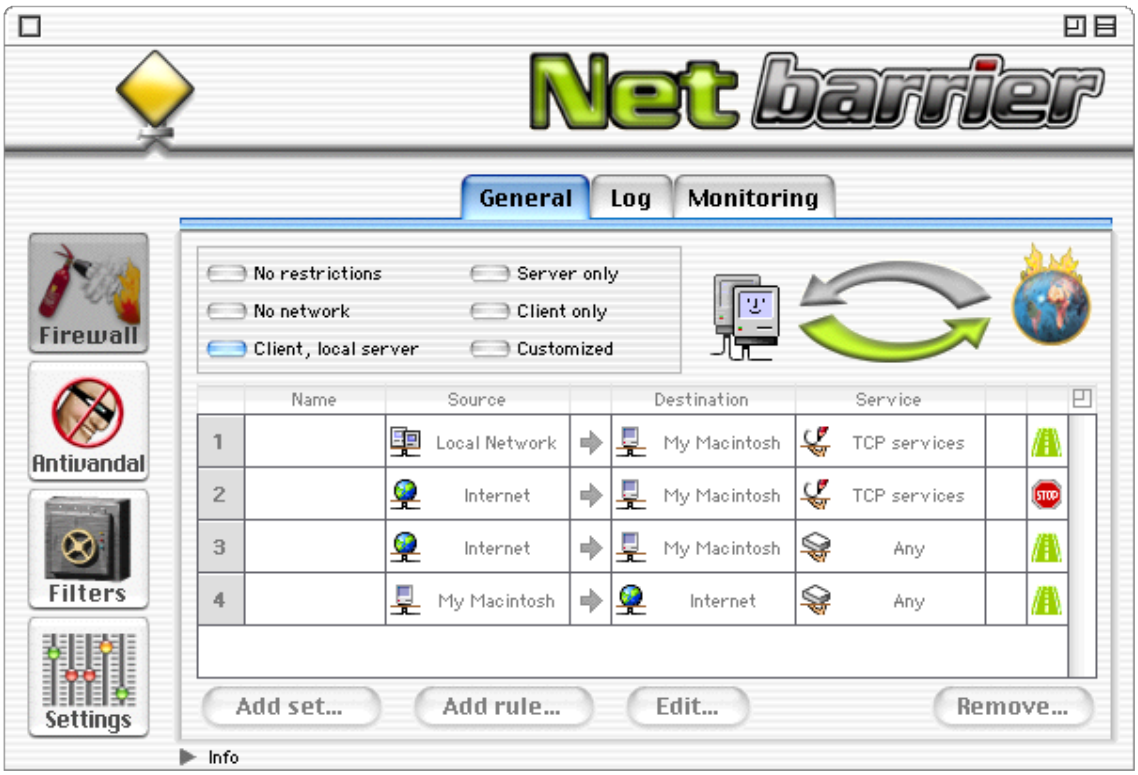
5 - The Three Lines of Defense

NetBarrier is a powerful easy-to-use program that protects your computer when connected to a network. It offers three lines of defense, to protect your computer from intrusions and attacks.

Firewall

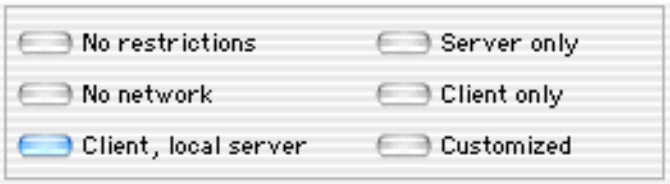
NetBarrier contains a personal firewall. This is a powerful program that filters all the data packets that enter or leave your computer, to or from the Internet, to allow or prevent data going to and coming from specific sources and destinations. Note that the Firewall does not affect local AppleTalk networks.

To view the Firewall screen, click the Firewall button on the left of the main interface. The Firewall screen will be displayed, with its three tabs: General, Log and Monitoring.



Firewall settings

NetBarrier's Firewall has 6 different settings that correspond to the way you use your computer. When you install NetBarrier, and restart your Macintosh, the program's Antivandal feature (see later in this chapter, Antivandal) starts monitoring your computer to prevent intrusions, but the Firewall must be set to correspond to your network activity. The first five settings, which are based on preprogrammed rules, cover all the situations that you will encounter in normal use. The last setting, **Customized**, allows you to design your own rules, to precisely control the levels of access to and from your computer.



No restrictions

In this mode, there are no restrictions, and NetBarrier's Firewall allows all incoming and outgoing network data to be sent and received. If you select this setting, it is as if the Firewall were turned off.

No network

In this mode, NetBarrier's Firewall prevents all data from entering or leaving your computer to or from the Internet. This is useful if you are away from your computer, and wish to protect it totally. This does not affect local AppleTalk networks.

Client, local server

In this mode, NetBarrier's Firewall protects your computer when it is functioning as a client and local network server. Activity between your computer and the Internet is available, as a client, and you can be both client and server on a local network.

Server only

In this mode, NetBarrier's Firewall protects your computer when it is functioning only as a server. The client functions of your computer are cut off.

Client only

In this mode, NetBarrier's Firewall protects your computer when it is functioning only as a client on a local network, or when you are connected to the Internet. The server functions of your computer are cut off.

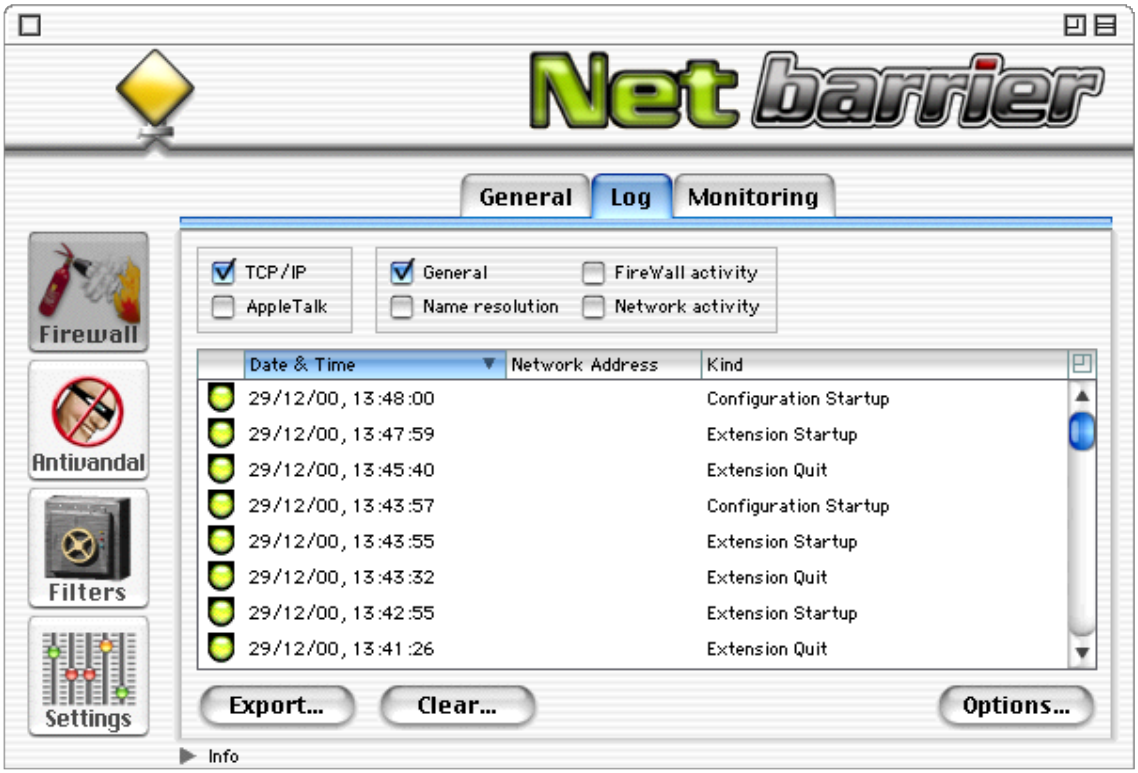
Customized

This setting gives you access to NetBarrier's most powerful features, by allowing you to create your own custom Firewall rules. But, since this setting gives access to such powerful possibilities for creating rules, it should only be used by experienced network administrators. For more on Customized mode, see chapter 7, **Customized Protection**.

The Log

How the Log works

The Log shows a record of all the activity where NetBarrier has acted. It lists each time that there has been an incident, the address of the intruder, and the type of incident recorded.



Selecting what to display in the Log

You can choose what type of information is displayed in the log. Checking any of the following check boxes will display related activity. If any of them are unchecked, their activity will not be displayed.

General

This is general NetBarrier activity, such as NetBarrier startup, and alerts.

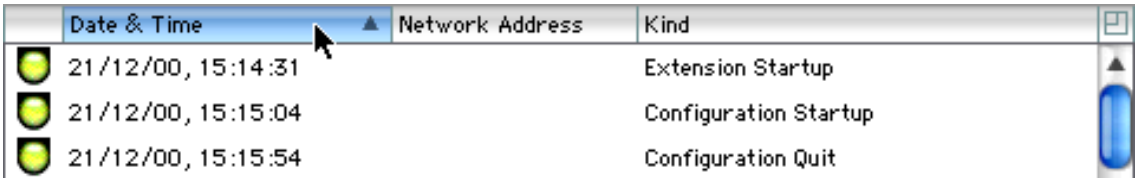
Firewall activity

NetBarrier logs all firewall activity, when rules are applied, if logging has been activated in the rules.

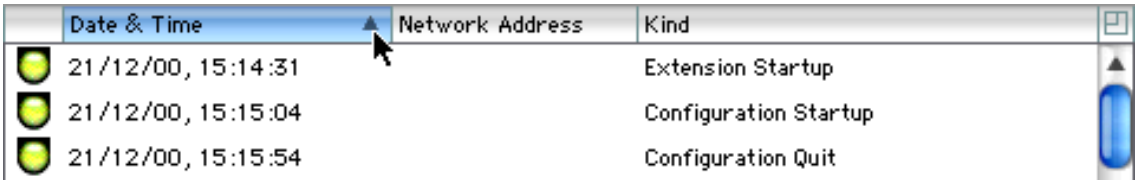
Network activity

NetBarrier logs all connections to networks or the Internet, and when IP addresses in the Stop List attempt to connect to your computer.

The log can be sorted by any of its fields by clicking on the header just above the field.



It can also be sorted in ascending or descending direction by clicking on the sort button, the small triangle in the selected sort column header.



Domain Name Resolution

NetBarrier helps you track down intruders by resolving domain names of your connections. Internet addresses exist in two forms - numbers, such as 255.255.0.0, and names, such as intego.com. The correspondence between the two is recorded in domain name servers all across the Internet.

When Name resolution is checked in the Log panel, NetBarrier will attempt to find the names for each of the Internet addresses shown in the log. If found, these names will then be displayed in their name form, rather than as numbers.

Note: In some cases, NetBarrier will not be able to resolve the names of certain Internet addresses, since not all such addresses have name equivalents.

Understanding the Log

Each Log entry contains 4 different items of information:

Icons
The Green icon indicates General information.
The Yellow icon indicates Firewall activity.
The Red icon indicates Network activity.

Date & Time
This is the date of the incident.

Network Address
This is the originating IP or AppleTalk address of the incident. If you have checked Name resolution, you will see the domain names for those addresses that NetBarrier was able to resolve.

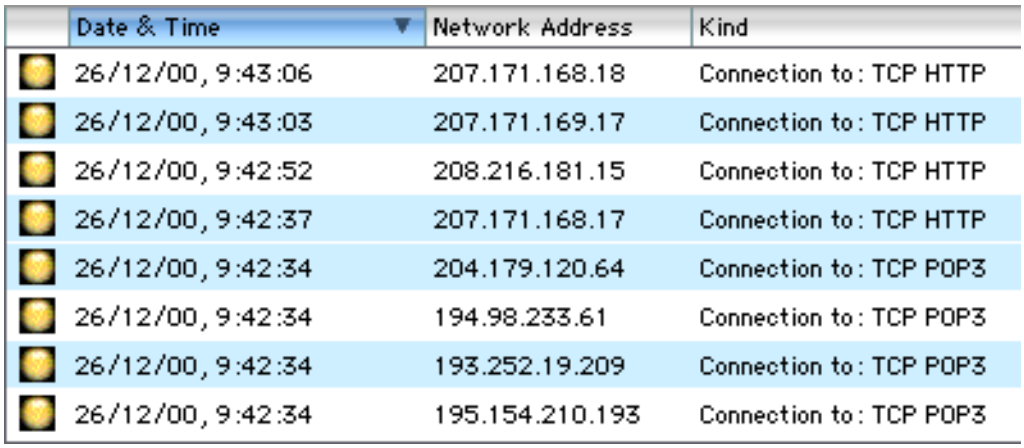
Kind
This is the kind of incident reported.

Clearing the Log

To clear the Log, and erase all information stored in the Log, click Clear..., and you will see a dialog asking if you really want to clear the Log. Click OK to clear the Log, or click Cancel to cancel the operation.

You can also selectively clear certain lines in the log, by making multiple selections in the Log window. To do this, select one item, hold down the Shift key, and select another item a few lines away. All the lines between the beginning and the end of

your selection will be highlighted, and you can delete the selected lines if you wish. To make a non-contiguous selection, hold down the Command key and select several non-contiguous lines.



Date & Time	Network Address	Kind
26/12/00, 9:43:06	207.171.168.18	Connection to: TCP HTTP
26/12/00, 9:43:03	207.171.169.17	Connection to: TCP HTTP
26/12/00, 9:42:52	208.216.181.15	Connection to: TCP HTTP
26/12/00, 9:42:37	207.171.168.17	Connection to: TCP HTTP
26/12/00, 9:42:34	204.179.120.64	Connection to: TCP POP3
26/12/00, 9:42:34	194.98.233.61	Connection to: TCP POP3
26/12/00, 9:42:34	193.252.19.209	Connection to: TCP POP3
26/12/00, 9:42:34	195.154.210.193	Connection to: TCP POP3

After you have selected log data, you can copy it, if you wish to paste it into another application, or drag and drop it into another application's window, or on the desktop.

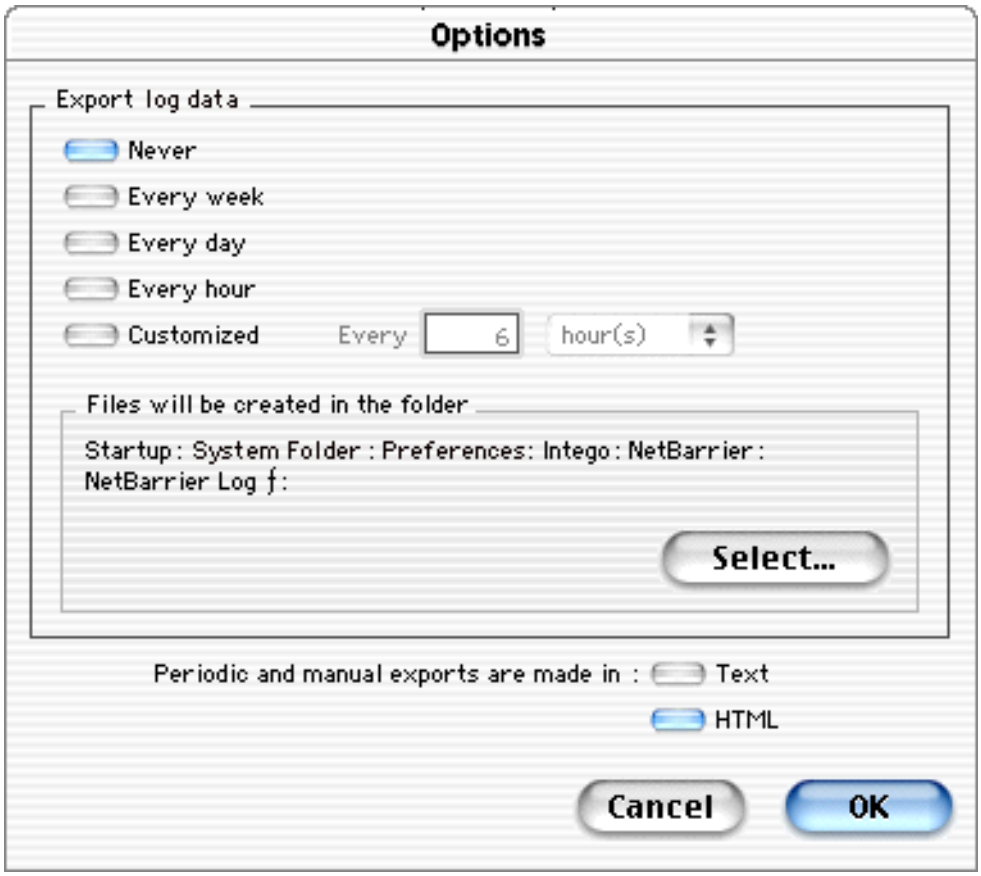
Exporting the Log

The entire log can be exported in text or HTML format. To do this, click the Export... button. A dialog will prompt you to save the file; you may change its name if you wish. Click Save. You will now have a copy of your log that you can open with any word processor (text) or web browser (HTML). See below, Log export options, for instructions on choosing the export format.

Status	Date & Time	Network Address	Kind
	21/12/00, 19:15:36	192.192.0.0	Connection to: TCP SMTP
	21/12/00, 19:21:33	192.192.0.0	Connection to: TCP POP3
	21/12/00, 19:25:13		Configuration Startup
	21/12/00, 19:25:32		Configuration Quit

Log Export Options

You can also set NetBarrier to export the log at regular intervals. To do this, click the Options... button. A window will be displayed showing the Log export options.



Export Log Data

If you wish to have your log exported at regular intervals, you can select among 5 options.

Never

The log data will never be exported.

Every week

The log data will be exported once a week, at 00h00 on Monday. If the computer is not on at this time, it will be exported at the next restart.

Every day

The log data will be exported once a day, at 00h00. If the computer is not on at this time, it will be exported at the next restart.

Every hour

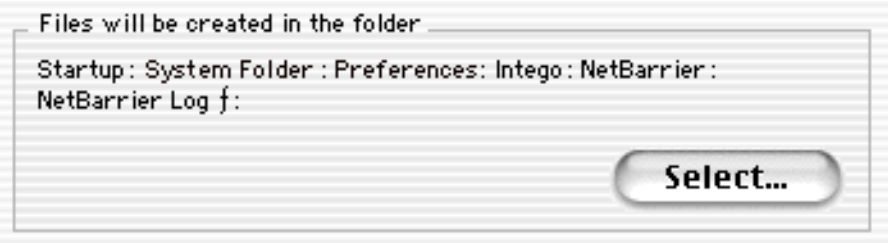
The log data will be exported once an hour, on the hour.

Customized

If you check this option, you can choose a custom interval to have your log data exported. You can enter the number of units you want, and select Months, Days, Hours or Minutes from the popup menu. The times that data will be exported will be the same as the above options.

Log Export Location

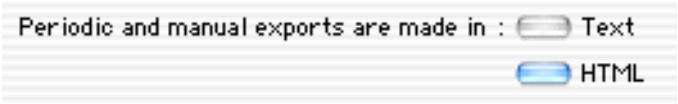
You can select the folder where log export files will be saved. By default, they will be saved in the Preferences > Intego > NetBarrier > NetBarrier Log ∫ folder of your System folder. If you wish to have these files saved in another folder, click the Select... button and navigate until you get to the folder you wish to use. Then click Select to use this folder. You can also create a new folder by clicking New Folder in the dialog box. Name this folder as you wish, and click Create.



Note: If you are using Personal Web Sharing, you can export the log into a shared folder, providing access to this file from a remote computer.

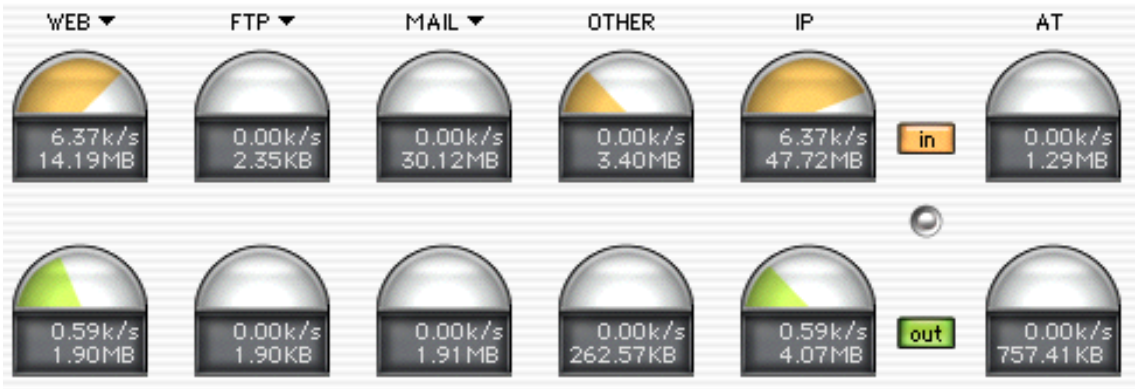
Log Export Format

Logs can be exported in two formats: text and HTML. If you select Text, they will be saved in a file that can be read by any word processor. If you select HTML, their files will be readable by any web browser, and will be presented in table form.



Monitoring

On the Monitoring tab of the Firewall panel is a set of activity gauges that inform you of the type of network activity that is coming into and going out of your computer.

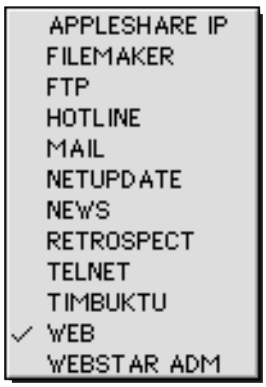


There are two rows of gauges - the In gauges show the amount of data coming into your computer, and the Out gauges show the amount of data leaving your computer. The top number is the current throughput per second, and the bottom is the total amount.

Selecting Activity Data Type

You can choose which type of data will be recorded for the first three pairs of gauges. To do this, click on the header over one of the gauges.

A popup menu will be displayed showing several choices.



The following types of data can be recorded:

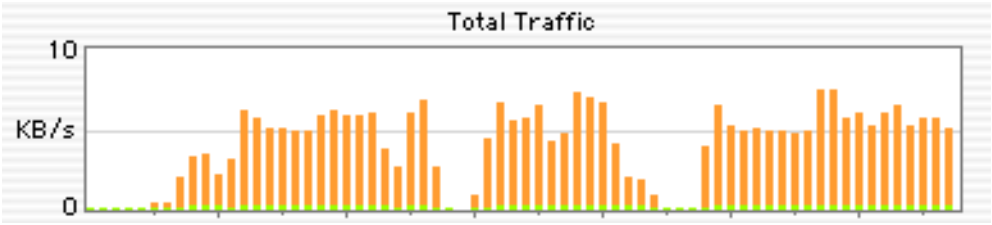
AppleShare IP:	the amount of AppleShare IP access data.
FileMaker:	FileMaker Pro data.
FTP:	ftp data.
Hotline:	Hotline server data.
Mail:	e-mail data.
NetUpdate:	data for Intego's NetUpdate program.
News:	newsgroup data.
Retrospect:	Retrospect data.
Telnet:	Telnet data.
Timbuktu:	Timbuktu data.
Web:	web access data.
WebSTAR ADM:	WebSTAR administration data.

The last three pairs of gauges are fixed, and show the following information:

Other:	the amount of data for other protocols.
IP:	the total amount of Internet Protocol data - the sum of the first four gauges.
AT:	the amount of data for AppleTalk.

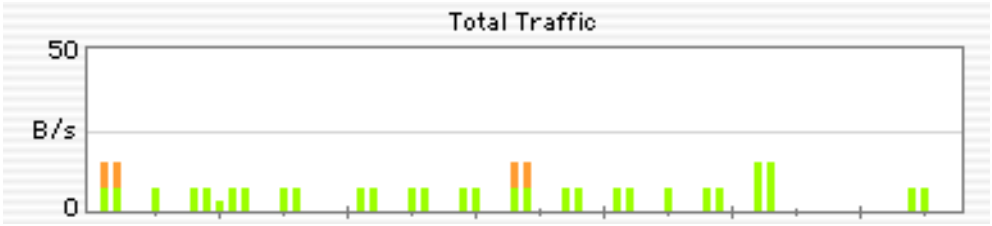
Total Traffic graph

A bar graph showing total traffic is also available in this window. When no network activity occurs, this graph will be empty, but when there is network activity, either over an AppleTalk network or the Internet, this graph will show the total activity.



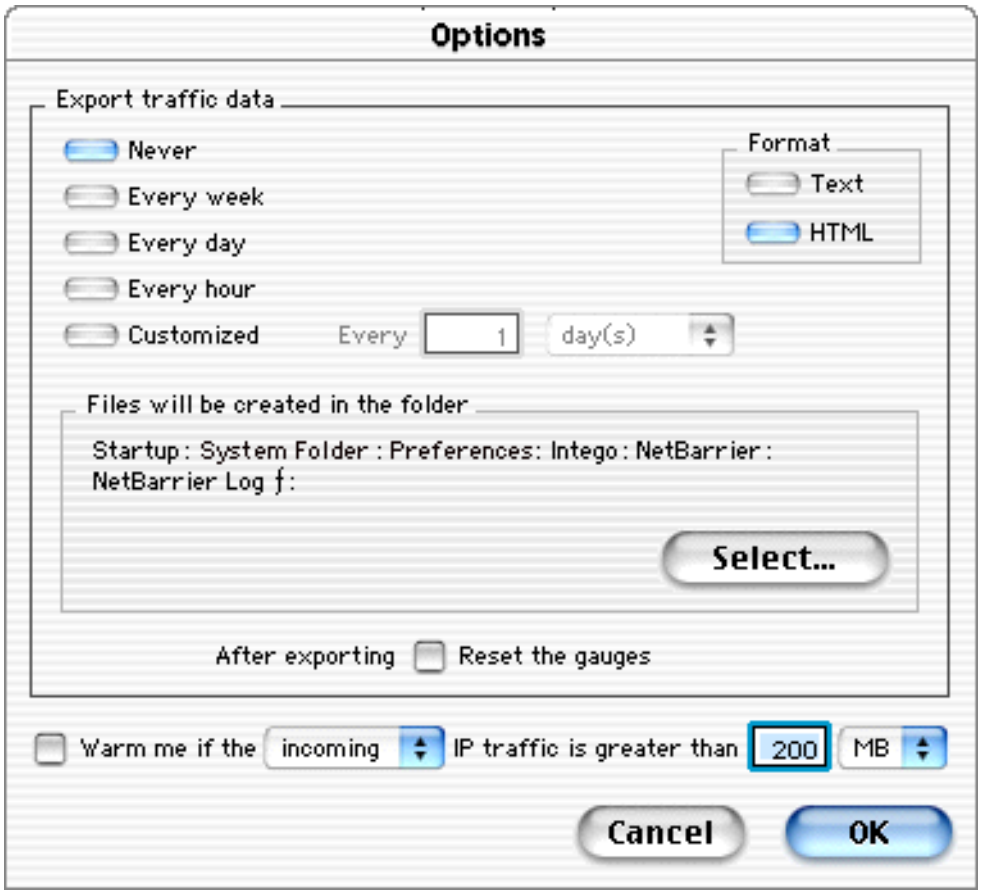
The orange parts of the bars represent incoming traffic, and the green represent outgoing traffic.

In addition, the scale of this graph is dynamic. It changes according to the amount of traffic. In the above example, a PPP connection is active, and throughput is around 5 kilobytes per second. In the second example, below, the only activity is polling over an AppleTalk network; the maximum traffic here does not exceed 25 bytes per second.



Monitoring Options

Several options are available for exporting and managing traffic data. To set these options, click the Options... button. A window will be displayed showing the traffic data export options.



Export Traffic Data

If you wish to have your traffic data exported at regular intervals, you can select among 5 options.

Never
The traffic data will never be exported.

Every week
The traffic data will be exported once a week, at 00h00 on Monday. If the computer is not on at this time, it will be exported at the next restart.

Every day
The traffic data will be exported once a day, at 00h00. If the computer is not on at this time, it will be exported at the next restart.

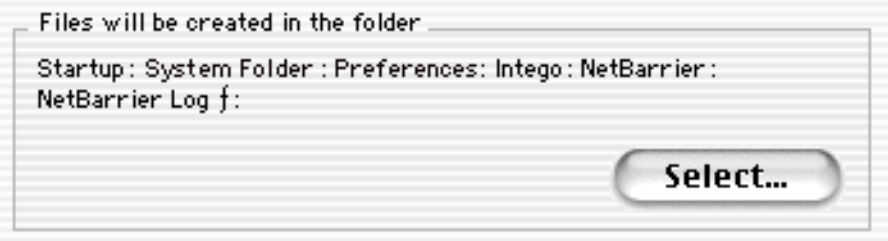
Every hour
The traffic data will be exported once an hour, on the hour.

Customized
If you check this option, you can choose a custom interval to have your traffic data exported. You can enter the number of units you want, and

select Months, Days, Hours or Minutes from the popup menu. The times that data will be exported will be the same as the above options.

Traffic Data Export Location

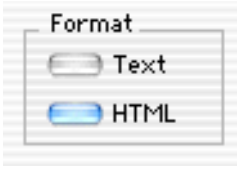
You can select the folder where traffic export files will be saved. By default, they will be saved in the Preferences > Intego > NetBarrier > NetBarrier Log ∫ folder of your System folder. If you wish to have these files saved in another folder, click the Select... button and navigate until you get to the folder you wish to use. Then click Select to use this folder. You can also create a new folder by clicking New Folder in the dialog box. Name this folder as you wish, and click Create.



Note: If you are using Personal Web Sharing, you can export the traffic data into a shared folder, providing access to this file from a remote computer.

Traffic Data Export Format

Traffic data can be exported in two formats: text and HTML. If you select Text, they will be saved in a file that can be read by any word processor. If you select HTML, their files will be readable by any web browser, and will be presented in table form.



Resetting the Gauges after Export

If you check this button, your activity gauges will be reset to zero after each export.

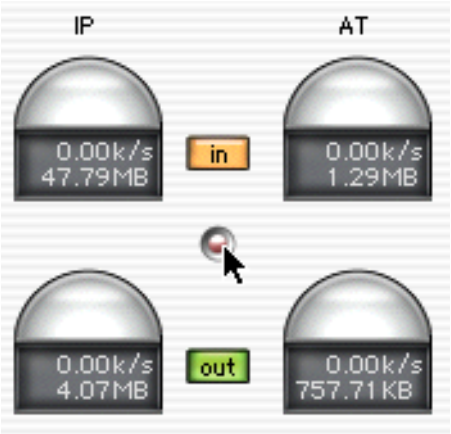
IP Traffic Threshold Warning

NetBarrier has a setting that allows you to monitor the amount of data entering or leaving your computer. This can be very useful if you have an Internet access account with uploading or downloading restrictions.

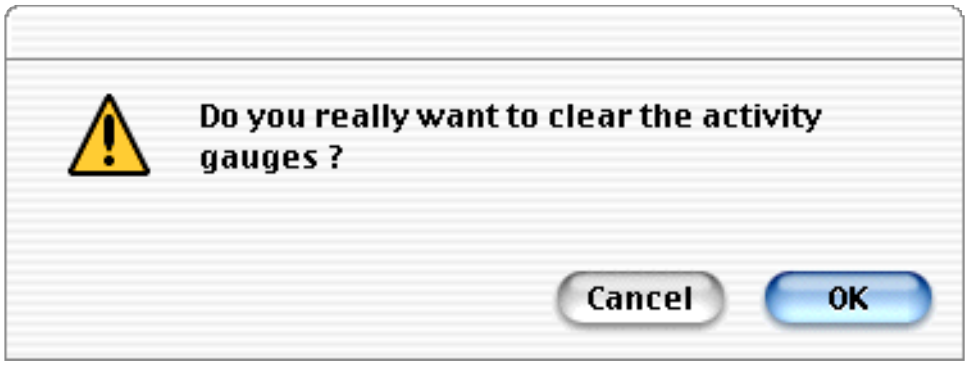
If you check this option, NetBarrier will display a warning when your traffic exceeds the amount you have selected. You can choose to have a warning for Incoming, Outgoing or Total traffic, and you can choose the amount of the threshold, in kilobytes, megabytes or gigabytes.

Resetting the Activity Gauges

If you click the Reset button, the totals beneath the gauges will all be reset to zero.

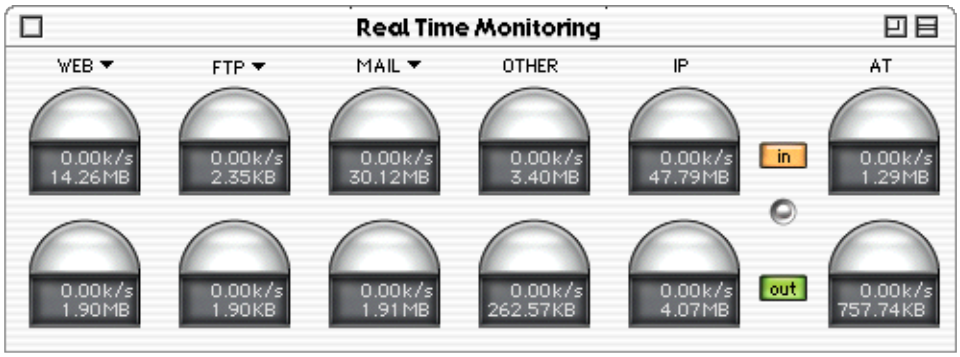


When you reset the activity gauges, an alert will be displayed asking you to confirm clearing the gauges or cancel. This ensures that you do not accidentally reset the activity gauges. If you wish to reset the activity gauges, click OK. If not, click Cancel.

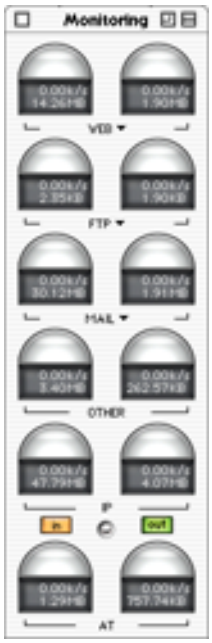


Viewing the gauges as a palette

If you click the window's resize button  the control panel will be collapsed, and the activity gauges will be displayed as a horizontal palette.

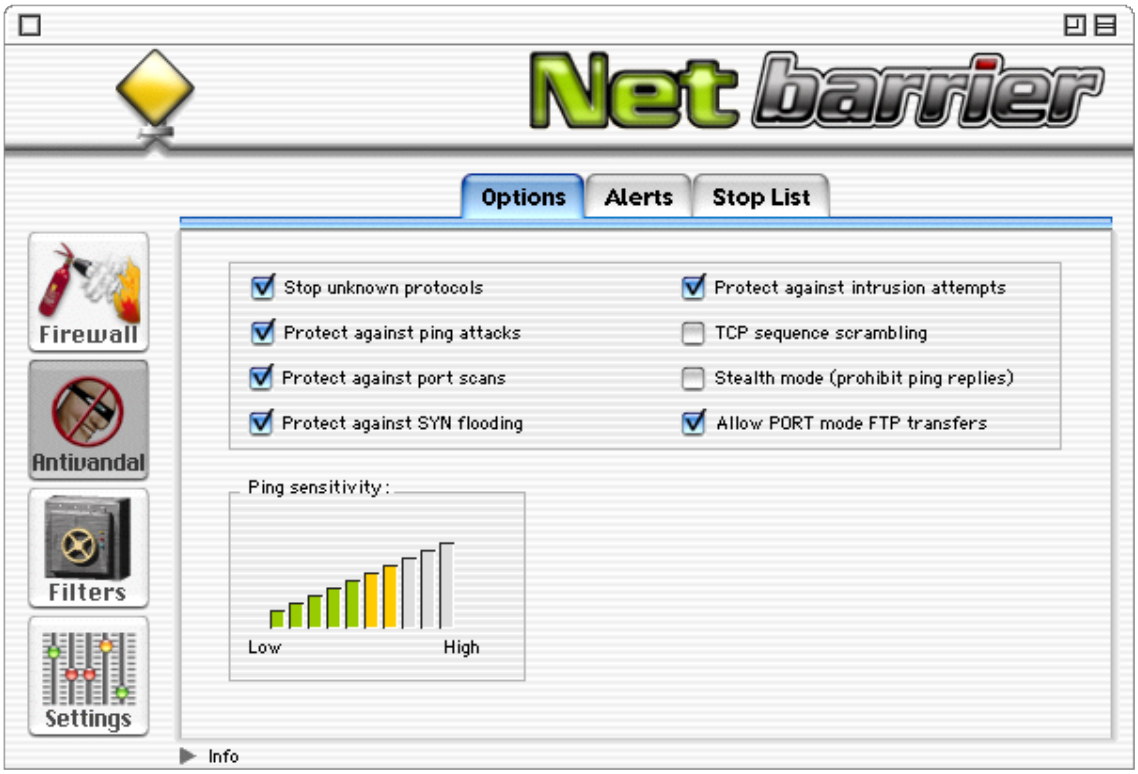


If you click the resize button while holding down the option (alt) key, the palette will be displayed vertically. This can be useful if you want to keep an eye on your network activity, and wish to leave these gauges visible. To return to the main NetBarrier window, click the resize button on the palette.



Antivandal

NetBarrier's Antivandal watches over all the data entering your computer, and filters it, looking for signs of intrusion. This filtering is transparent - the only time NetBarrier will show itself is if suspicious data is detected. If this occurs, an alert will be displayed. Otherwise, Antivandal silently monitors your computer's network activity at all times.



Options

The Antivandal panel has several options that affect NetBarrier's anti-intrusion protection.

Stop unknown protocols

If this is checked, any unknown protocols are automatically blocked.

Protect against ping attacks

If this is checked, any hostile pings are automatically blocked. Pings are accepted, but if the number or frequency of pings exceeds NetBarrier's limits, they will be blocked.

Protect against port scans

If this is checked, port scanning is automatically blocked. You may want to leave this unchecked if your computer is functioning as a server.

Protect against SYN flooding

If this is checked, the number of connections is automatically limited. This will prevent connection flood denial of service attacks.

Protect against intrusion attempts

If this is checked, NetBarrier will send you an alert if 3 incorrect password requests are sent to your machine, in an attempt to connect to it, in a given period of time. This applies to connection attempts to AppleTalk File Sharing, Personal Web Sharing, or ftp.

TCP sequence scrambling

This protects against an intruder subverting a connection. An intruder can basically take control of a computer in this manner.

Stealth mode (prohibit ping replies)

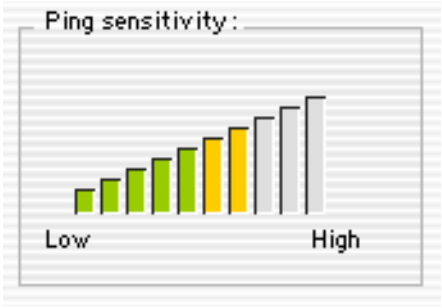
If this is checked, your computer will be invisible to other computers on the Internet or on a local network. You will not, however, be anonymous - any requests you send to other hosts will include your computer's IP address.

Allow PORT mode FTP transfers

If this is checked, you will be able to make FTP transfers when functioning in Client only Firewall mode.

Setting Ping Sensitivity

You can adjust the sensitivity of the ping protection in Net Barrier. If your computer is on a network, it is normal that your network administrator ping your computer from time to time. However, if your computer is isolated, it is rare that you should be pinged. One exception is if you have a cable connection, your ISP might ping your computer to check if it is on-line.



To adjust the ping sensitivity, click on one of the bars. The bar will be colored, either green, yellow or red, indicating the level of protection. If you are on a network and get too many alerts, you should lower the ping sensitivity.

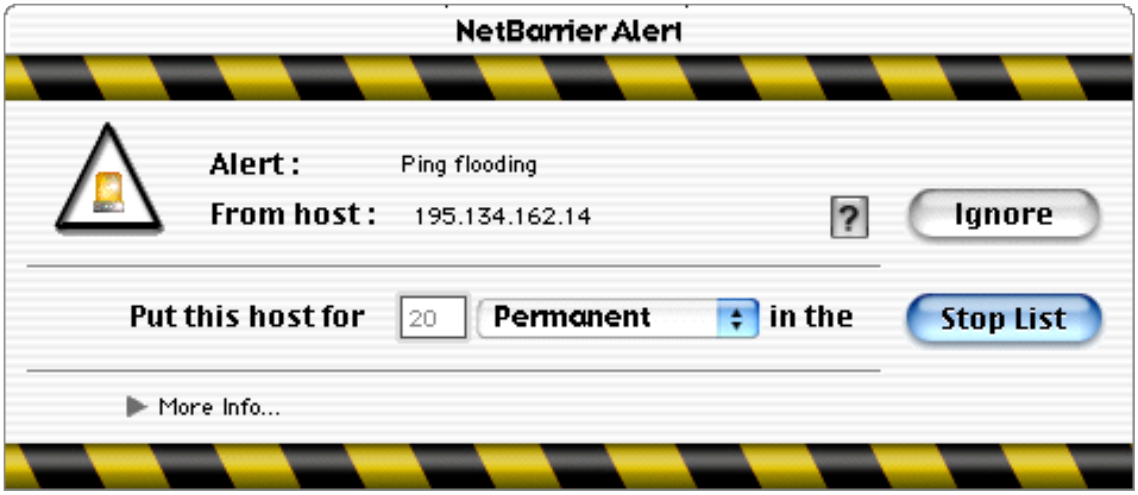
Alerts

How alerts work

NetBarrier constantly monitors all of your computer's network activity, whether it is to the Internet or a local network. It is pre-configured to look out for specific types of data that indicate an intrusion or attack. If any suspicious data is found, NetBarrier will display an alert, asking you whether you wish to allow the data to continue, or deny it.

Understanding alerts

The following is an example of an alert. The top line shows the reason for the alert. Here, a Ping flood was detected. The host, 195.134.162.14, is shown by its IP address. Two buttons at the right allow you to decide what action to take for this alert.



If you click on the small arrow at the bottom left, an information field is displayed, showing the cause of the alert.

Responding to alerts

Stop List

The default response to all alerts is Stop List. If you click this button, or press the Enter or Return key, the data being received will be refused, and the intrusion will be prevented. When this happens, the packet is dropped, and it is as if the data was never received. If the suspicious packet is part of a file, this means that the file will not reach its destination. If it is a command, the command will not have a chance to be carried out, since it will not reach its target.

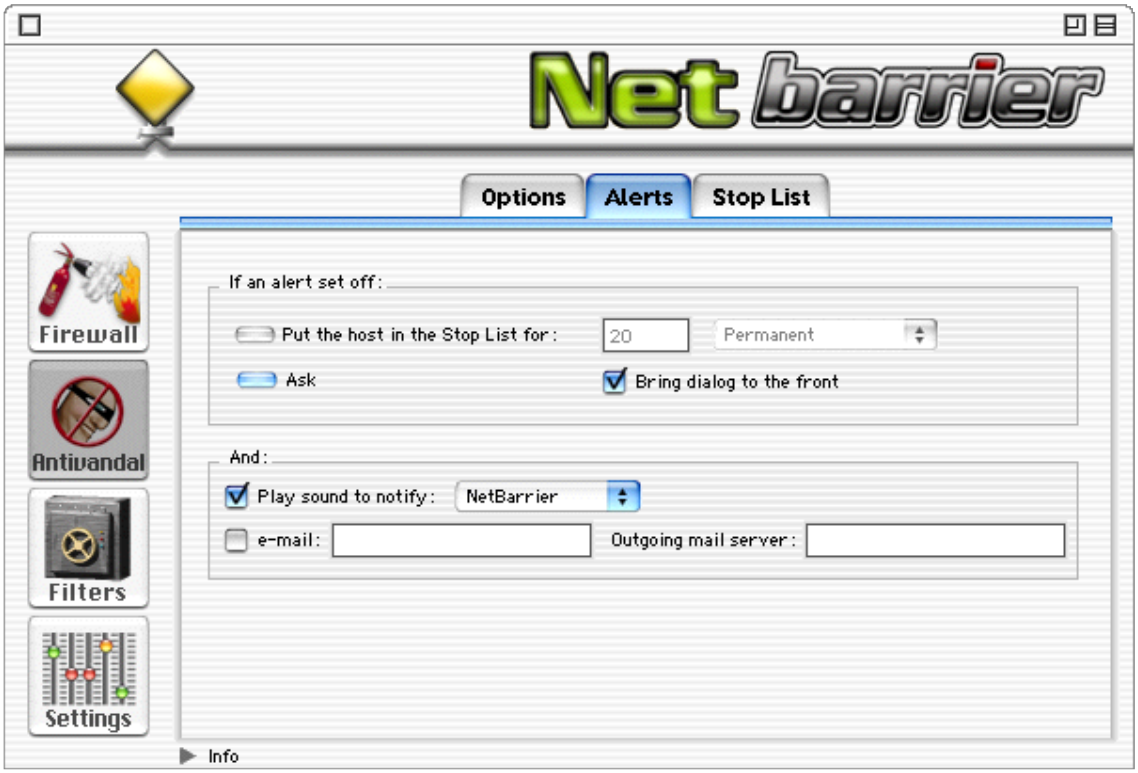
If you click Stop List, the IP address that caused this alert to be displayed will be automatically added to the Stop List, and kept there for the default time that has been set. (See **Stop List,** chapter 5.) This time can, however, be changed in the Alert dialogue by entering a new time in the time field, and changing the time unit, from the popup menu.

Ignore

If you click this button, you will allow the data to be received. Data transmission will continue as usual, unless NetBarrier detects another attempted intrusion. In this case, another alert will be displayed.

Alert options

The Alert tab gives you several options as to how NetBarrier will act when presenting an Alert.



Put the host in the Stop List for:

If this is checked, the connection will automatically be dropped when there is an alert, and the offending IP address will be automatically placed in the Stop List. (See **Stop List,** chapter 5.) A field to the right of this button allows you to specify the default length of time that the offending IP address will remain in the Stop List. You can choose any amount of seconds, minutes, hours or days, or choose to have the intruder remain on the Stop List permanently.

Ask

If this is checked, NetBarrier will present an Alert dialog asking what to do. It is up to you to decide how the Alert is then to be handled. This Alert dialog will show the time that is selected in the Alert options by default, but this time can be changed in the Alert dialog.

Bring dialog to front

If this is checked, the NetBarrier alert will come to the front automatically whenever there is an alert. If not, it will remain in the background. If no action is taken for 90 seconds, the alert will automatically close, and the connection will be denied.

Play sound to notify

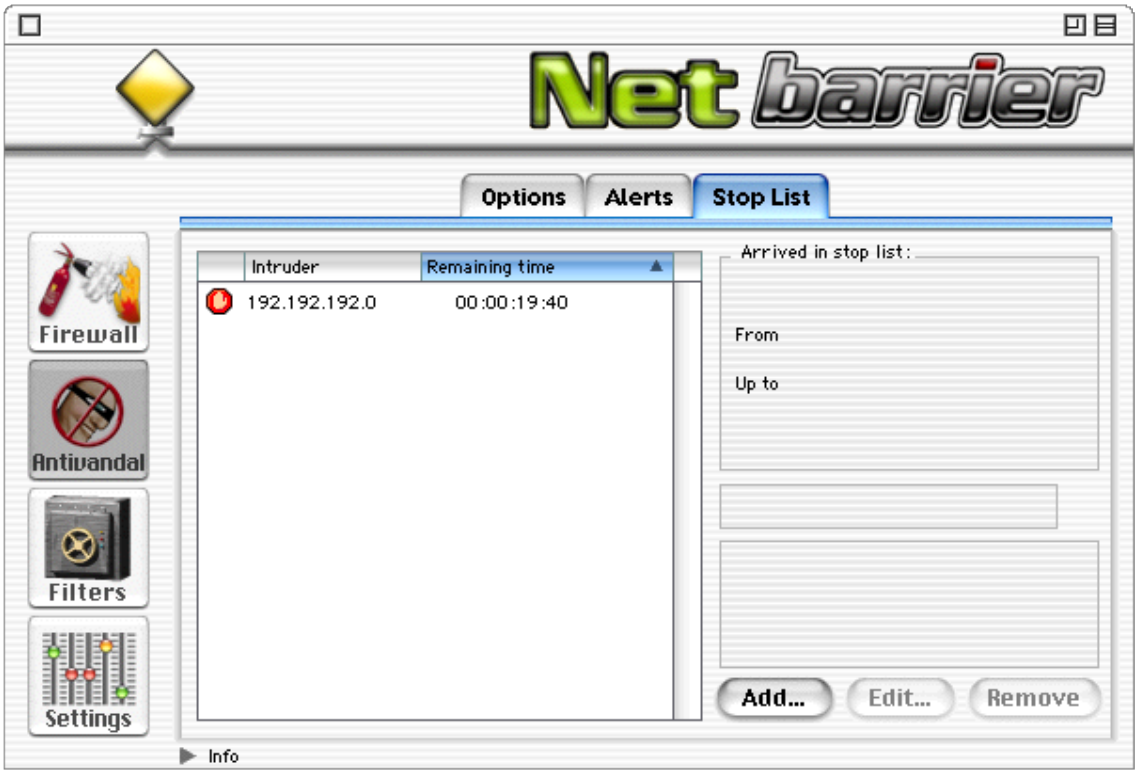
If this is checked, NetBarrier will play the sound of your choice whenever there is an Alert. You can select the sound you wish to have played from the pop-up menu to the right of the button.

E-mail

If this is checked, NetBarrier will automatically send an e-mail message to the address entered in the text field, within 5 minutes. NetBarrier waits to see if there are other intrusion attempts, rather than send an e-mail message each time. The e-mail address and mail server are those entered in the Internet Config preferences, or the MacOS Internet preferences.

The Stop List

The Stop List is a powerful feature of NetBarrier that ensures that once an attempted attack or intrusion has been foiled, the originating machine will not be allowed to send any data to your computer, and your computer will not be allowed to connect to them either. The offender can be put on the Stop List for a limited time, or indefinitely. The default time that the offender will remain on the Stop List can be set in the Options panel. (See **Alert Options,** chapter 5)



Stop List information

The Stop List panel shows you information on the various IP addresses that are currently in the Stop List, if any.

Intruder

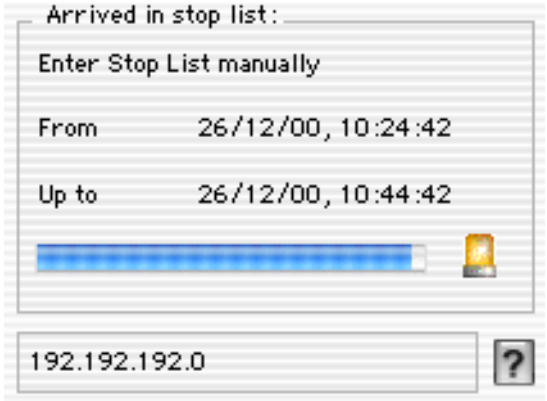
This is the IP address of the offender.

Remaining time

This is the time that the offending IP address is scheduled to remain in the Stop List.

Other Stop List information

If you click once on an address in the Stop List, you will see some additional information on the right side of the panel.



Arrived in Stop List

This is the date and time that the offending IP address was added to the Stop List. A line of text tells you how the IP address was added to

the Stop List (here, it was added manually). The **From**: and **Up to**: sections tell you when the address was added to the Stop List, and how long it will remain there. The progress bar shows how much of their time in the Stop List has passed.

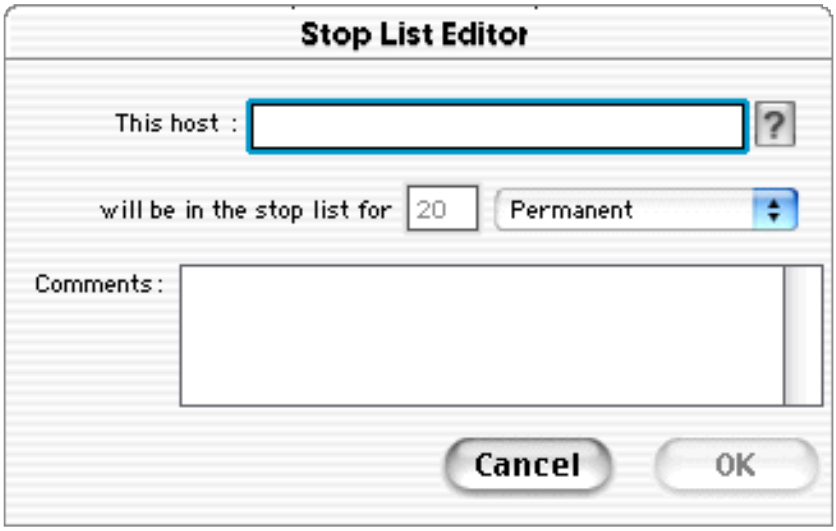
IP address

At the bottom of this section, is the IP address of the offender. By clicking on the DNS lookup button (the **?**), you can toggle from the numerical IP address to the actual domain name of the offender, if there is one.

Adding addresses to the Stop List

There are two ways to add addresses to the Stop List. The first is by responding to an Alert. (See above, **Alerts**.) If an Alert is displayed, and you reply Stop List, the offending IP address will be automatically added to the Stop List.

You can also manually add addresses to the Stop List. To do so, click Add...



A dialog box will be displayed. Enter the address in the first field, and select the time this address is to remain in the Stop List by entering a number in the second field, and selecting the time unit from the pop-up menu. If you do not know the numerical IP address of the host you wish to add, click on the **?** button. NetBarrier will query your Internet provider's DNS server, and enter the correct number in the field. You can also add comments, such as the reason for adding the address to the Stop List, in the Comments field. If you decide you do not wish to add this address to the Stop List, click Cancel.

Using Wild Cards in the Stop List

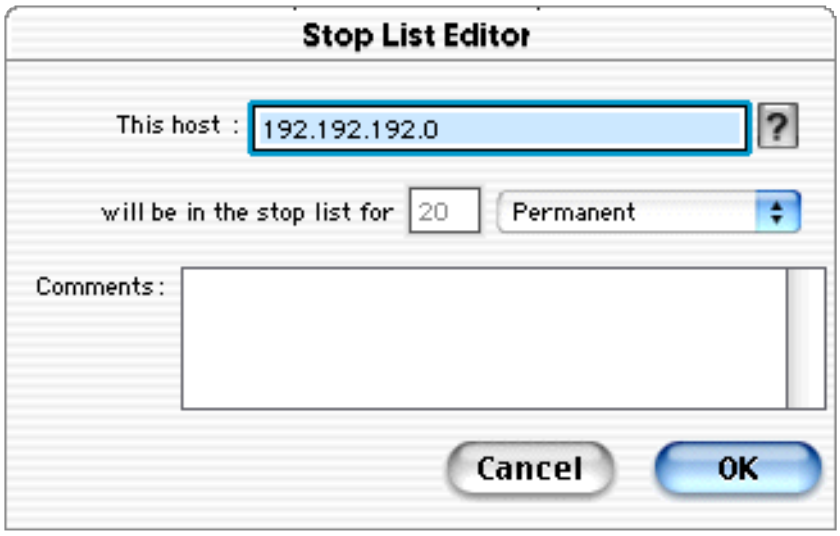
You can also use wild cards to block ranges of IP addresses in the Stop List. To do this, enter the first part of the IP address you wish to block, followed by asterisks, in the following form: 192.*.*.* or 192.192.*.* or 192.192.192.* This will block all addresses containing the numbers you have entered, whatever their endings are.

Removing addresses from the Stop List

To remove an address from the Stop List, click once on the address you would like to remove, then click Remove. A dialog will ask if you really want to remove the address; click OK. The address will be removed. If you decide you do not want to delete this address, click Cancel. You can select multiple contiguous addresses, by shift-clicking, or non-contiguous addresses, by command-clicking, and delete them all together.

Editing an address in the Stop List

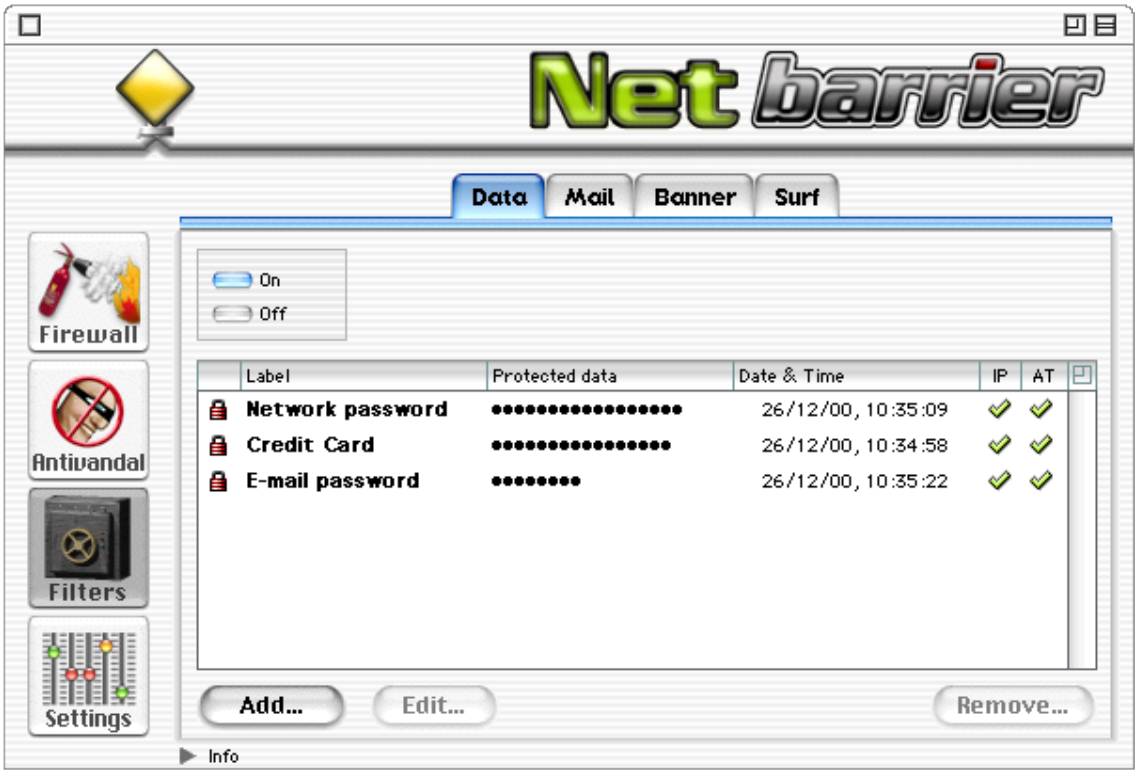
To edit an address in the Stop List, click once on the address you would like to edit, then click Edit... (You can also double-click on the address.)



A dialog box will show you the address, and you can change the address, add or change comments, or change the time you want it to remain on the Stop List. To confirm your changes click OK, or to leave the address and time as they were, click Cancel.

Filters

NetBarrier's filters examine both incoming and outgoing data, looking for specific types of data. There are several different filters, each of which is designed to protect your data or privacy, or help you surf the web faster.

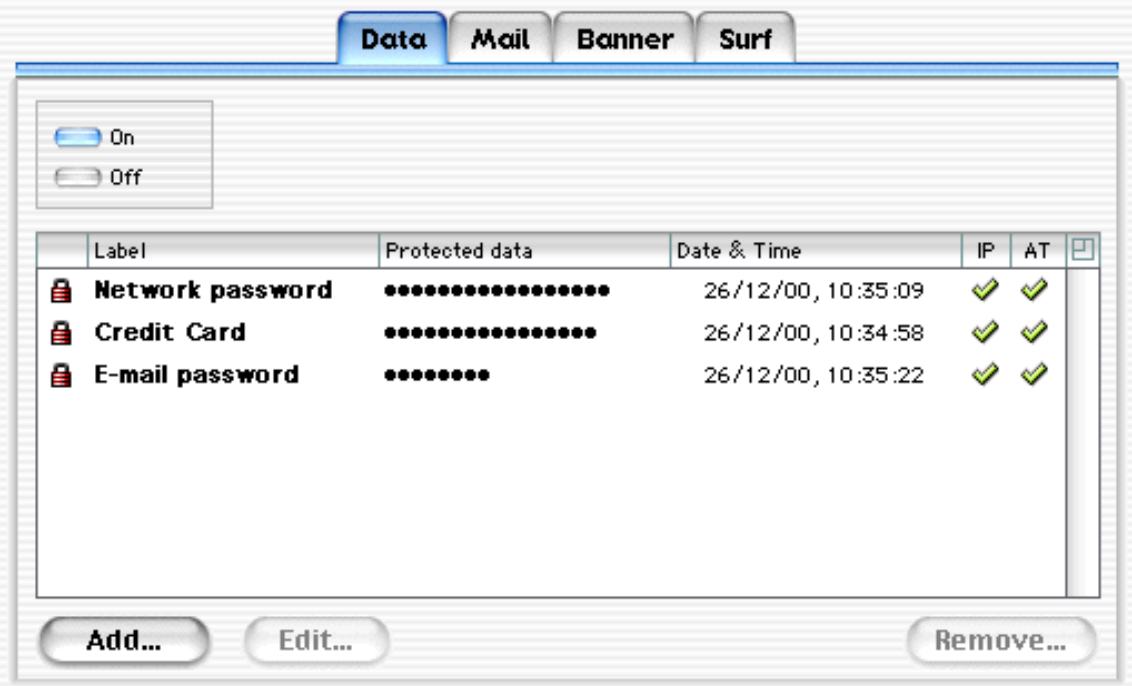


Data Filter

The Data Filter ensures that any sensitive information, that you choose to protect, cannot leave your computer and go onto a network. You choose what to protect, say, your credit card number, passwords, or key words that appear in sensitive documents, and NetBarrier's Filter checks each outgoing packet to make sure that no documents containing this information will be sent. Not only does this protect

you from sending documents containing this information, but it protects against anyone who has network access to your computer from taking copies of them.

If your computer is accessible across a network, and file sharing privileges are given to other users, it is possible for anyone with access to your computer to copy your files.



How the Filter works

The Filter works in a very simple manner. Each unit of data you protect is called Protected data. When data packets are sent from your computer to a network, whether it be a local AppleTalk network or the Internet, they are all examined. If any of the Filter's Protected data is found, the packet is stopped.

Note: the Filter only works on data that corresponds exactly to the Protected data that you set. For example, if you set Protected data for your credit card number

(see below), NetBarrier will prevent its being sent out from your computer. But if you enter the same number in a secure web page, this number is encrypted by your browser, and the data no longer corresponds to the Protected data, and will therefore be sent. The same is true for data that is encoded or compressed.

What to protect

The Filter is designed to protect sensitive information. There may be different types of information that you wish to protect, depending on your needs. Here are some examples:

Credit card numbers

Even if you don't want to send your credit card number across the Internet, via web servers or e-mail, you may have already sent faxes containing this number. If so, the files you sent as faxes contain this number, and anyone could open the files and copy it. Add your credit card numbers to the Filter list, and they will not be able to leave your computer and go onto a network.

Passwords

If you use the Internet or any other network, you probably have some passwords. The more sites you use, the more passwords you probably have. Some users even have files on their computers containing lists of their passwords. Add your passwords to the Filter, and none of them will be able to leave your computer and go onto a network.

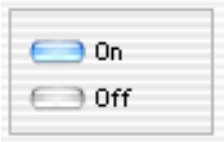
Other sensitive information

You may have confidential files concerning projects or customers, contracts, specifications or other sensitive information. You can easily choose to protect the name of a project or customer, or add a key word

to any of these files to make sure that they cannot be copied across a network.

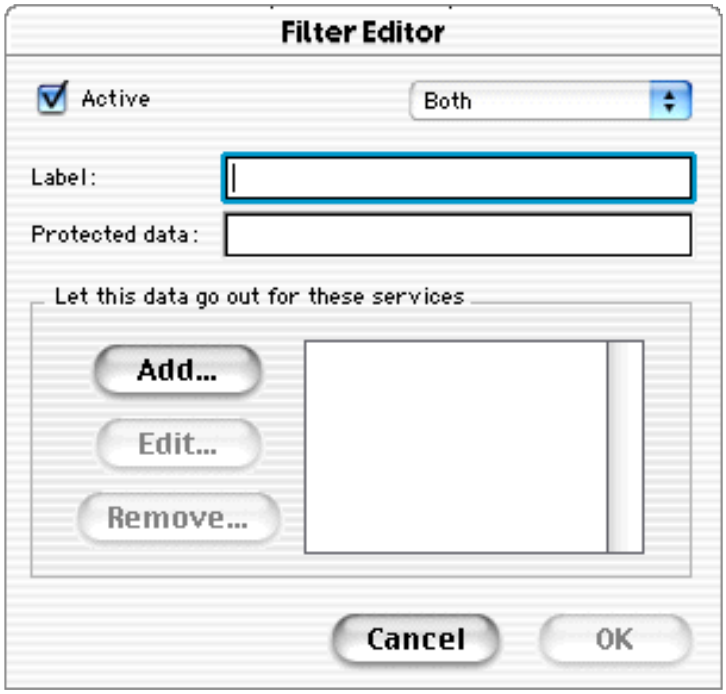
Turning the Filter on

First, for the Filter to check for protected data, you need to turn it on. To do this, click the On checkbox. You can turn it off at any time, if you temporarily want to allow any of your protected data to be sent, by clicking the Off checkbox.



Adding Protected data to the Filter

To add Protected data to the Filter, click Add... The Filter Editor window will be displayed.



Enter a name for your Protected data, in the first text field, then the actual text you wish to protect in the second text field. This text will appear hidden by bullets.

Note: You must enter your text exactly as it will be found in your documents for the Filter to protect it. For example, a credit card number may be found as ####-####-####-#### or as #### #### #### ####. If you protect only the first example, the Filter will not look for the second one.

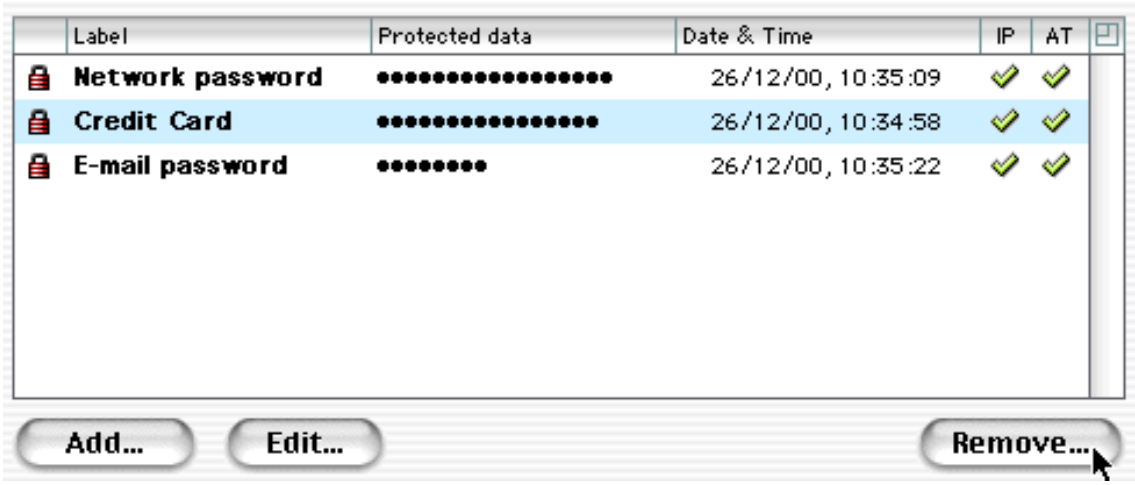
A pop-up menu lets you choose whether you want this Protected data to be protected on TCP/IP networks, AppleTalk networks or both. A check box in the upper left corner lets you choose whether this Protected data is active. If you uncheck this box, the filter will not stop this Protected data.

The section labeled **Let this data go out for these services** allows you to choose to block data for all but the selected services. To do this, click the Add... button. Then, either enter the port number of the service, or choose its name from the popup menu. This data will not be blocked for this service, and this service only. To add another service, repeat the above operation. You can add as many services as you wish.

When you have finished entering this information, click OK, and your Protected data will now be displayed in the Filter window. If you decide that you do not wish to keep this Protected data, click Cancel.

Deleting Protected data from the Filter

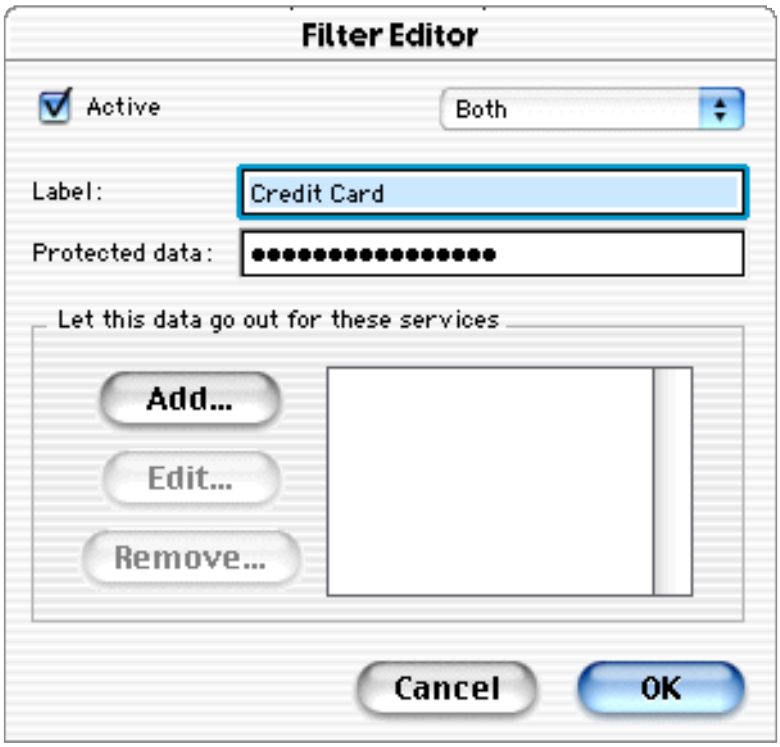
To delete Protected data from the filter, click once on the Protected data you wish to delete, and click Remove... A dialog will ask if you really want to remove the Protected data; click OK. The Protected data will be removed. If you decide you do not want to delete this Protected data, click Cancel.



Editing Protected data in the Filter

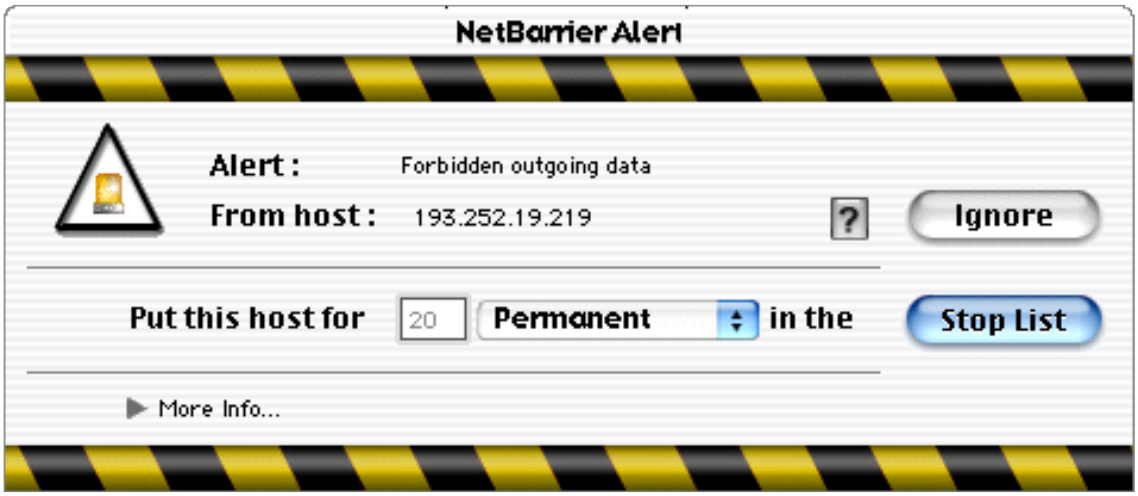
You can edit Protected data in the Filter, either to make changes, or to make active Protected data inactive, or change the protocols that it is active under.

To edit Protected data in the Filter, click once on the Protected data you would like to edit, then click Edit... (You can also double-click on the Protected data.) The Filter Editor window will show you the Protected data, and you can make any changes you want. To confirm your changes click OK, or to leave the Protected data as it was, click Cancel.



Filter Alerts

If the Filter detects that Protected data is leaving your computer, an alert will be displayed.



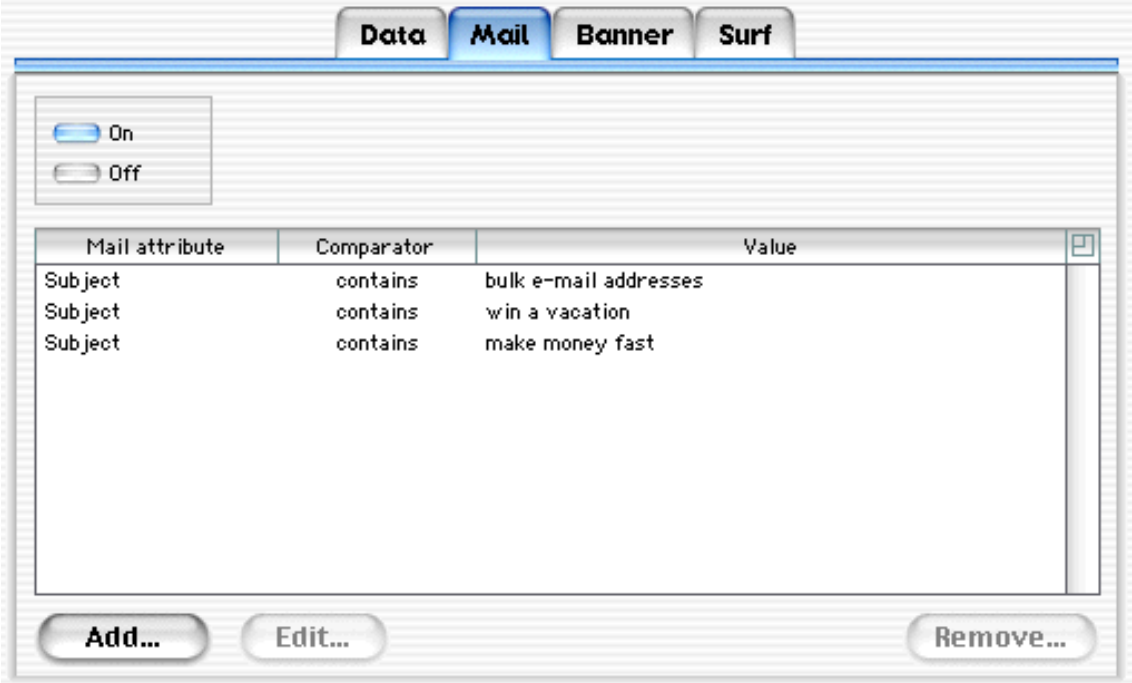
This alert is similar to other NetBarrier alerts. You have the possibility of ignoring the alert, or putting the host on the Stop List. If you click Ignore, NetBarrier will allow the data to be sent for 10 seconds, which is long enough for the file in question to be sent. If you click Stop List, the host will be added to the Stop List.

Privacy Filters

In addition to protecting your computer and your data, NetBarrier has several features to protect your privacy and make netsurfing faster and easier.

Mail Filter

The Mail Filter makes your Internet use faster and easier by blocking spam before you download it. You can create specific anti-spam rules, and NetBarrier will check your mail server and delete any messages that correspond to your rules. Be careful, though, to make sure your rules only filter spam.



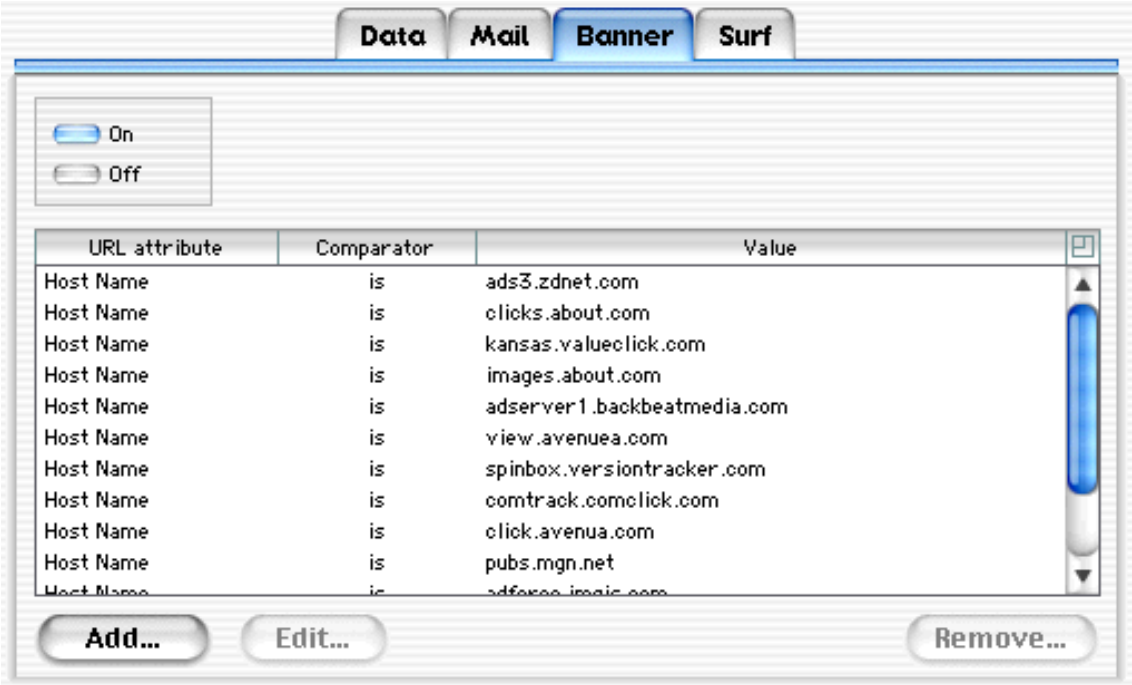
To create a new anti-spam rule, click the Add... button.

The Spam Editor dialog box will be displayed. This contains three sections: two popup menus and a text field. To create an anti-spam rule, select from the first popup menu **Subject**, **Author** or **Sender**, then, select from the second popup menu **is** or **contains**. For example, if you want to block spam with a subject of "Make money fast", select **Subject contains**, and enter **Make money fast** in the text field. If you wish to validate this anti-spam rule, click OK; if not, click Cancel.

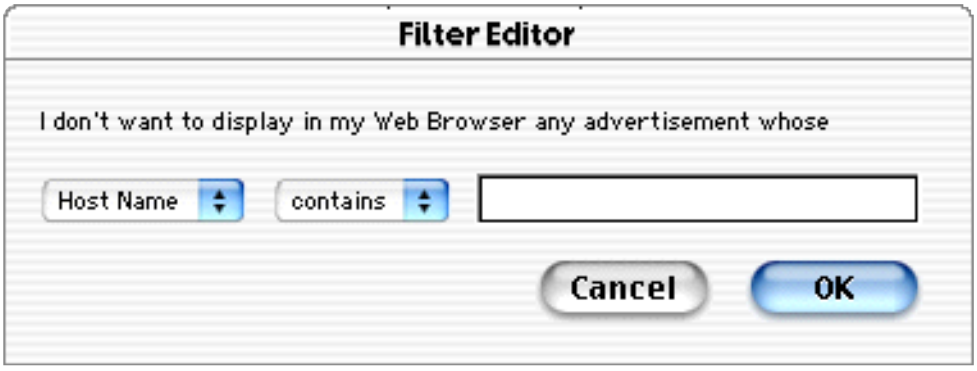
If you receive an e-mail message with this subject, NetBarrier will erase it on your mail server, so you never have to download it. NOTE: this may slow down your reception of e-mail slightly, as it can take a few seconds to delete a message on your mail server.

Ad Banner Filter

If you click the Banner tab, you will see the Ad Banner screen. This is a list of rules that NetBarrier uses to filter ad banners, helping you surf much faster. Ad banners are small graphic ads that are usually displayed at the tops of web pages. By filtering them, you will see web pages load much faster, and you will be spared from seeing annoying advertisements.



The filter already contains a set of rules, but you can easily add your own. To do this, click the **Add...** button.

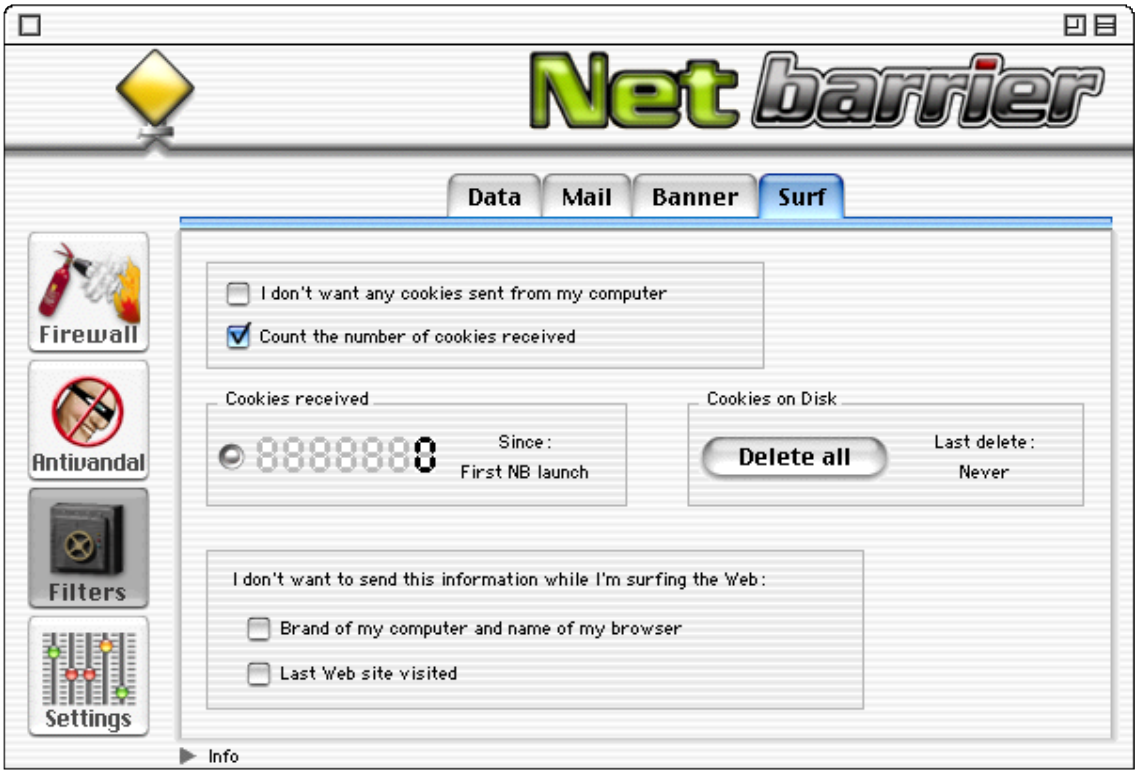


The Filter Editor dialog box will be displayed. This contains three sections: two popup menus and a text field. To create an ad banner filter rule, select from the first popup menu **Host Name** or **URL Path**, then, select from the second popup menu **is** or **contains**. For example, if you want to block ad banners from the host doubleclick.net, select **Host Name contains**, and enter **doubleclick.net** in the text field. If you wish to validate this ad banner filter rule, click OK; if not, click Cancel.

NetBarrier will block all ads coming from the servers or URL paths listed in this panel, helping you surf much faster.

Surf Filter

NetBarrier has several additional features to help maintain your privacy when surfing the Internet. The Surf tab displays a screen where you can choose specific options concerning cookies and information about your computer.

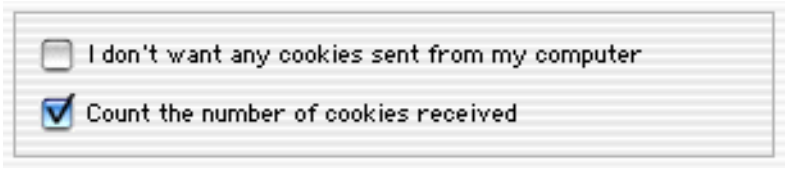


Cookie Control

A cookie is a small file on your computer used by some web sites to record information on you. Cookies can contain your user name and password for some sites, information identifying you for e-commerce sites, as well as other information on your surfing habits that you don't even know about. While cookies

are not always bad (you cannot make purchases from most web sites without them), some sites use them to track your behavior.

NetBarrier provides the means to block cookies from being sent from your computer. To do this, check the **I don't want any cookies sent from my computer** checkbox. This will allow web sites to send cookies, but your computer will not send back any information. Note: if this is checked, you may have trouble accessing some sites that require user identification, or most e-commerce sites.



NetBarrier can also count the number of cookies sent to your computer, if you check the **Count the number of cookies received** checkbox.

Cookie Counter

The Cookie Counter section records the number of cookies received on your computer, if you have checked **Count the number of cookies received**, as above.

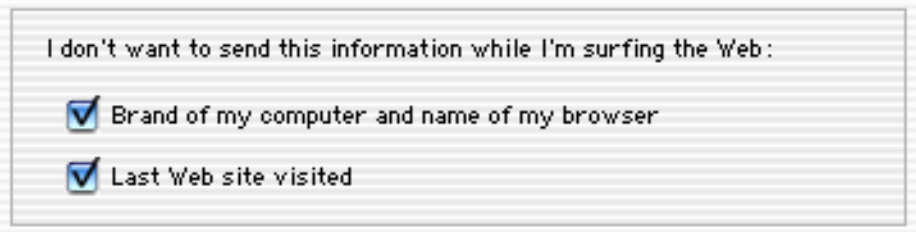
You can reset this counter by clicking the reset button to the left of the number of cookies.

Cookies on Disk

You can also erase all cookies on your computer by clicking the **Delete all** button. This section tells you the last time you deleted your computer's cookies.

Information on your Computer

All web browsers are set to reply to requests from web sites, telling which platform you are using (Mac, Windows, Linux, etc.) and which type and version browser you are using. Again, this can be useful (such as for sites with different versions for different browsers), but you may find some sites that will not let you access them if you are on a Mac. NetBarrier can "spoof" some information concerning your computer, that is, send false information.



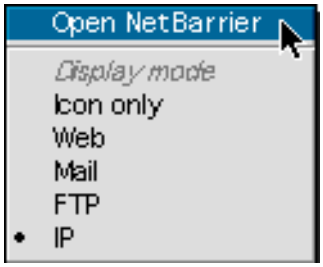
NetBarrier can reply to these requests, and send only generic information—it will reply that you are using Netscape, but with no version number nor platform. If you wish NetBarrier to do this, check the **Brand of my computer and name of my browser** checkbox.

Some sites also request the last site you visited. Again, this can be useful (some sites want to know where their users have come from) but unscrupulous sites might use this to follow your browsing habits. By checking the **Last web site visited** checkbox, NetBarrier will prevent a reply from being sent to this type of request.

Using the NetBarrier Control Strip Module

NetBarrier includes a useful and practical Control Strip Module. This module allows you to keep an eye on your network traffic, both incoming and outgoing. The top line, **In**, is traffic being received, and the bottom line, **Out**, is traffic being transmitted. The graphical display gives you an idea of how much data is being transmitted or received.

Opening NetBarrier



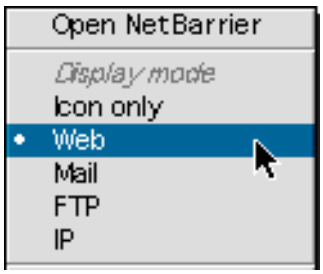
You can easily open the NetBarrier Control Panel by selecting Open NetBarrier from the Control Strip module.

Selecting the Control Strip Module Display Mode

Several options are available for displaying the Control Strip module. You can have it display incoming and outgoing traffic, in a series of small lights with an icon showing which firewall mode is selected. This is the default mode.

To change this display mode, click on the Control Strip module, and a menu will be displayed. Select Icon Only from the Display mode section, and the Control Strip module will display only the NetBarrier icon and an icon showing which firewall mode is selected.

You can also choose which type of traffic data is shown in the lights on the Control Strip module. You can choose among Web, Mail, Ftp or IP. If you choose Web, only web page traffic will be shown. If you choose Mail, only e-mail traffic will be shown. If you choose FTP, only FTP, or file transfer protocol traffic will be shown. If you choose IP, all IP traffic will be shown, from all sources.



To select the type of traffic data shown, click on the Control Strip module, and a menu will be displayed. Select the appropriate choice from the Display Mode section of the Control Strip module. This change will be made immediately.

Changing the Firewall Mode

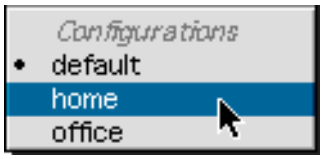
You can quickly and easily change NetBarrier's Firewall mode from the control strip. To do this, click on the Control Strip module, and a menu will be displayed. Select the appropriate choice from the Firewall Mode section. This change will be made immediately.

Activating and Deactivating Filters

All of NetBarrier's filters can be activated and deactivated on the fly from the Control Strip module. To do this, click on the Control Strip module, and a menu will be displayed. Select the filter you wish to change. If a diamond is displayed next to one of the filters, this means it is active. If not, it is inactive.

Changing Configurations

You can change NetBarrier's configuration on the fly from the Control Strip module. To do this, click on the Control Strip module, and a menu will be displayed. Select the appropriate configuration from the Configurations section. This change will be made immediately.

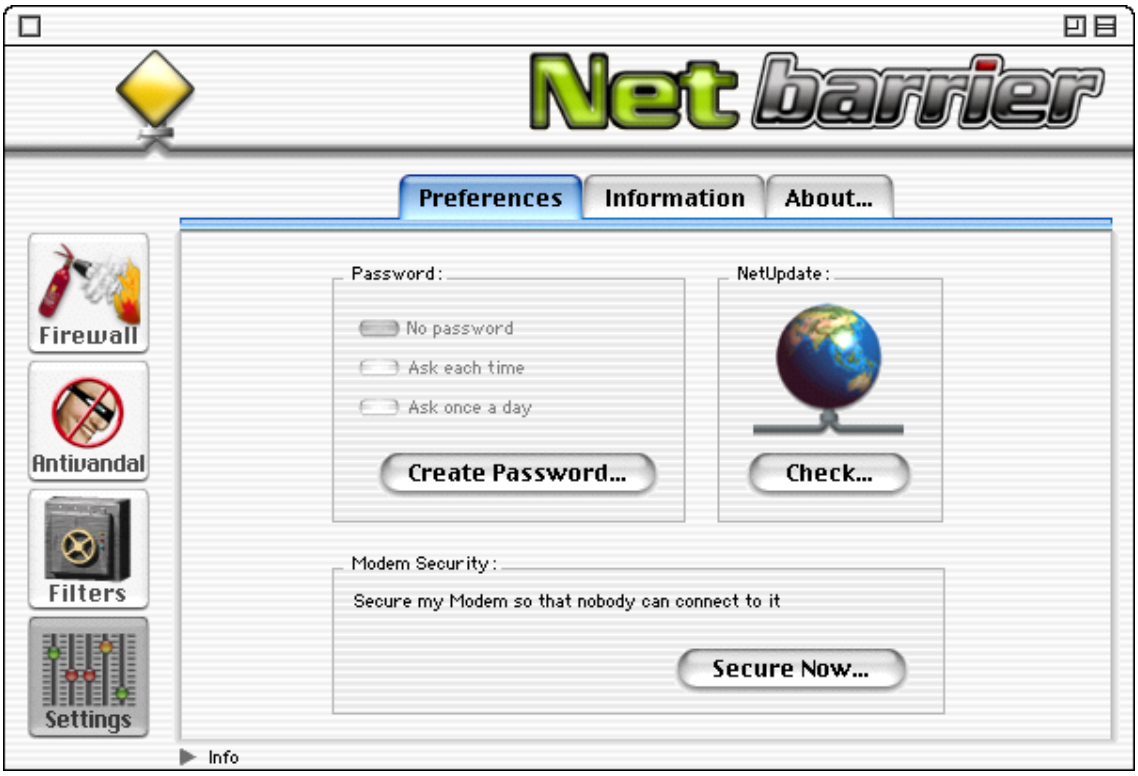


6 - Settings and Configurations

The Settings Panel

Preferences

Several preferences can be adjusted from this panel.

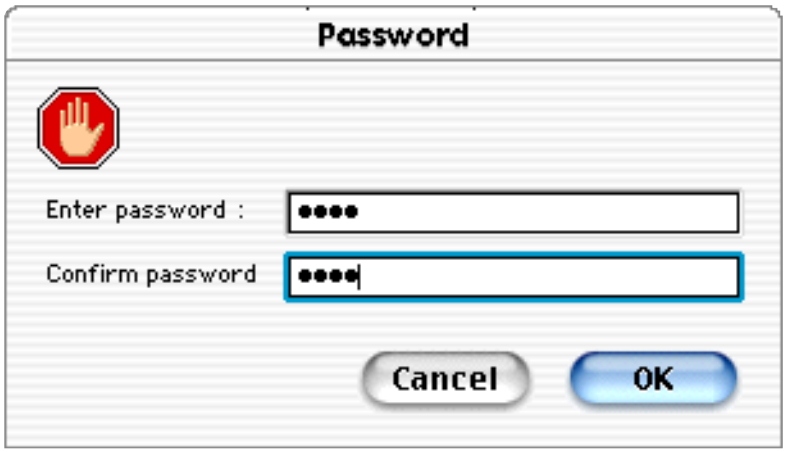


Using a Password with NetBarrier

NetBarrier has an additional level of protection, to prevent other users from making changes to your configurations, or allowing network traffic that you have set NetBarrier to deny. You can set a password in NetBarrier, and several options allow you to choose how NetBarrier will work with this password.

Creating a password

To create a password, click on Create Password... A dialog box will be displayed, asking you to enter a password. Type your password in the first field, then type it again in the second field for confirmation. The password will be hidden.



If you wish to validate this password, click OK; if not, click Cancel.

Note: your password must be a minimum of 4 characters and is case-sensitive.

Password options

There are three options as to how NetBarrier will request that you enter your password.

No password

If you check this option, after setting a password, NetBarrier will not ask you to enter your password. This is useful if you have set a password, but want to deactivate the password protection temporarily. Your password will still be saved, but you will only be asked to enter it if you check one of the other two options.

Ask each time

If you check this option, NetBarrier will ask you to enter your password each time it is opened, or each time an alert is displayed. This offers total protection, but will require you to enter your password more often.

Ask once a day

If you check this option, NetBarrier will ask you to enter your password once each day. You will be asked the first time NetBarrier is opened, or when an alert is displayed, and then you will not be asked again until the following day.

Changing your password

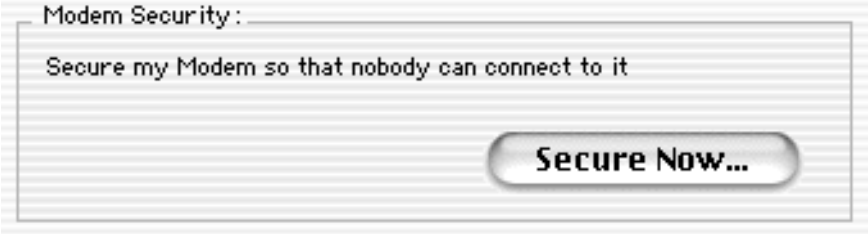
If you have entered a password in NetBarrier, there will now be a Change Password... button on this panel. To change your password, click this button, and simply enter and confirm your new password. If you wish to validate this new password, click OK; if not, click Cancel.

Erasing your password

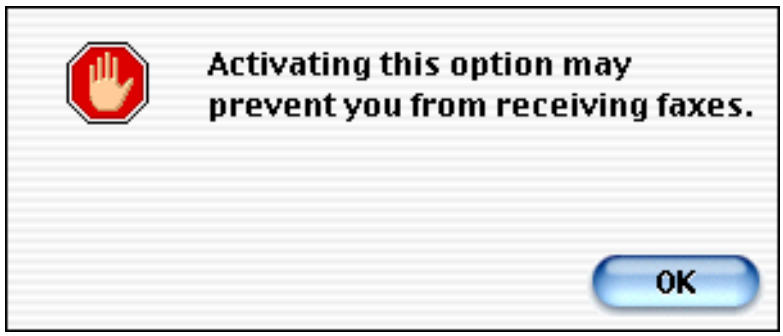
To erase your password, erase both password fields. If you wish to validate this change, click OK; if not, click Cancel.

Modem Security

You can provide total security for your modem with this option. It may prevent your modem from answering any calls. To apply modem security, click the Secure Now... button.



A dialog will be displayed. NOTE: this option is irreversible. If it is activated, at cannot be deactivated. If you activate this option, your modem may no longer be able to answer calls, such as for receiving faxes.



Click OK. Another window will be displayed, showing any modems you have installed. Select your modem and click OK, or click Cancel to cancel this operation.

Using NetUpdate

NetUpdate is an application that Intego's programs can use to check if the program has been updated. This application, in the form of a control panel, is installed at the same time as Intego's NetBarrier, VirusBarrier or ContentBarrier. It checks updates for all of these programs at the same time, and downloads and installs those for the programs installed on your computer.

For more on using NetUpdate, see the NetUpdate User's Manual.

Information

This panel gives some useful information about your computer. It shows the user name, the name of the computer, its IP address and other network information. It also tells if AppleShare and Personal Web Sharing are running, and whether an Airport card is present or not. In addition, it gives you real-time information on your network activity.

Services

This section lists any services currently running on your computer that are accessible to other users via the Internet Protocol, such as a web server, mail server, etc. For each port being used, the following information is shown: the protocol (TCP or UDP), the local port number, the remote port, according to the protocol it represents, if it is a standard protocol (for example, port 80 is HTTP), the remote address, that is the IP address of the connection, and the status of the connection.

Protocol	Local Port	Remote Port	Remote Address	State
TCP	1678	HTTP	195.158.253.31	ESTABLISHED
TCP	1679	HTTP	195.158.253.31	ESTABLISHED
TCP	1680	HTTP	195.158.253.31	ESTABLISHED
TCP	1681	HTTP	195.158.253.31	ESTABLISHED

About...

This panel gives information about NetBarrier, such as the version number, your support number (a number you will need for technical support), clickable links to Intego's web site and e-mail address, and Intego's address and telephone number.

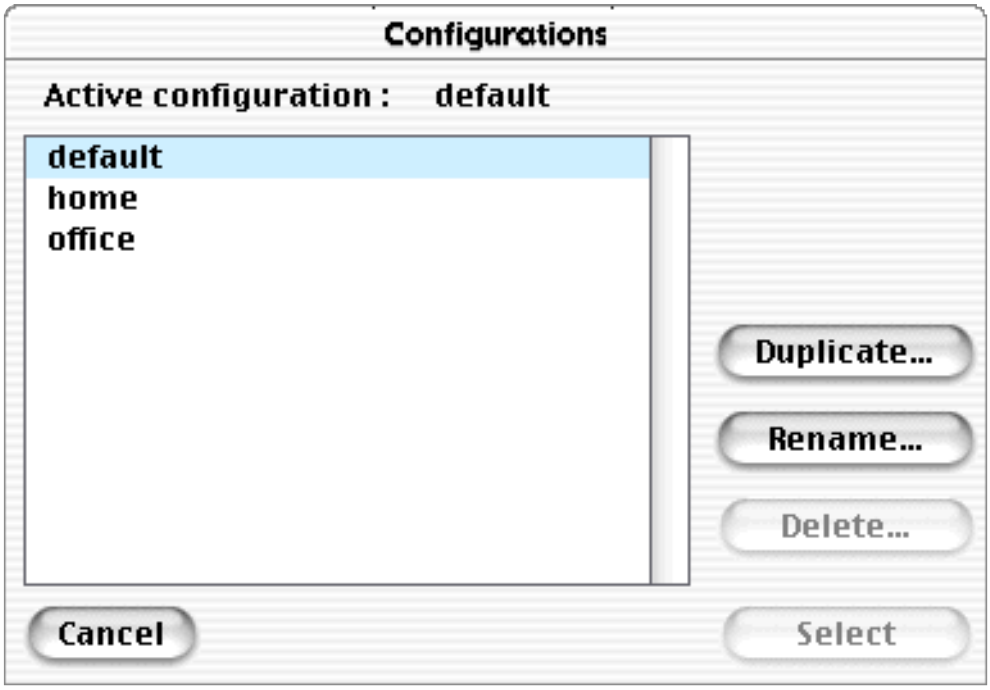
If you haven't yet registered online, you can do so quickly and easily by clicking the Register online... button. This will take you to the registration page on the Intego web site.

Configuration Sets

NetBarrier gives you the possibility of saving as many configuration sets as you want. You may want to have one set that includes additional protection for the times your computer is used as a server, and another for when it is a client. You may also want a specific set for less protection when you are connected to a local network, and additional protection when you are surfing the web. You may want to have a set that sends you e-mail messages when any intrusions occur, for when you are not at your computer.

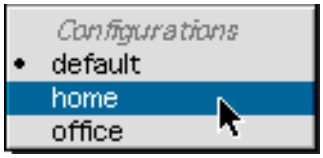
Selecting the active configuration set

To select a configuration set, select Configurations... from the File menu. A dialog box will open.



Select the set you wish to activate, and click Select. If you decide you do not want to activate this set, click Cancel, or select a different set.

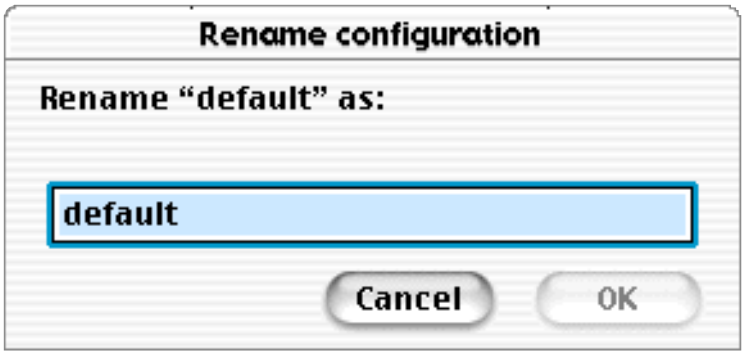
You can change NetBarrier's configuration on the fly from the Control Strip module. To do this, click on the Control Strip module, and a menu will be displayed. Select the appropriate configuration from the Configurations section. This change will be made immediately.



Adding configuration sets

To add a configuration set, select Configurations... from the File menu. A dialog box will open.

To create a new configuration set, you first need to copy an existing set, and rename it. To do this, click on one of the sets in the list, and then click Rename. You will see the following dialog box:



Enter the name for your new set, and click OK. If you decide you do not want to rename this set, click Cancel.

Now that you have a new configuration set, activate it by clicking Select.

You can now make any changes to the configuration that you want, and they will be saved under the current set. To return to another set, select it from the list of configuration sets.

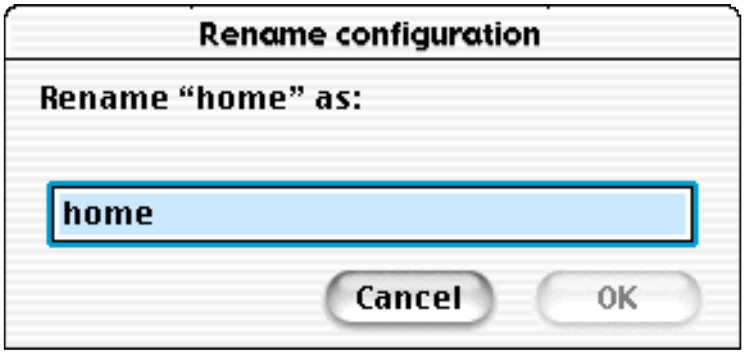
Deleting configuration sets

To delete a configuration set, select Configurations... from the File menu. A dialog box will open. Select a set by clicking on one of the sets in the list, and then click Delete.

A dialog box will ask if you really want to delete this set. Click OK. If you decide you do not want to delete this set, click Cancel.

Renaming configuration sets

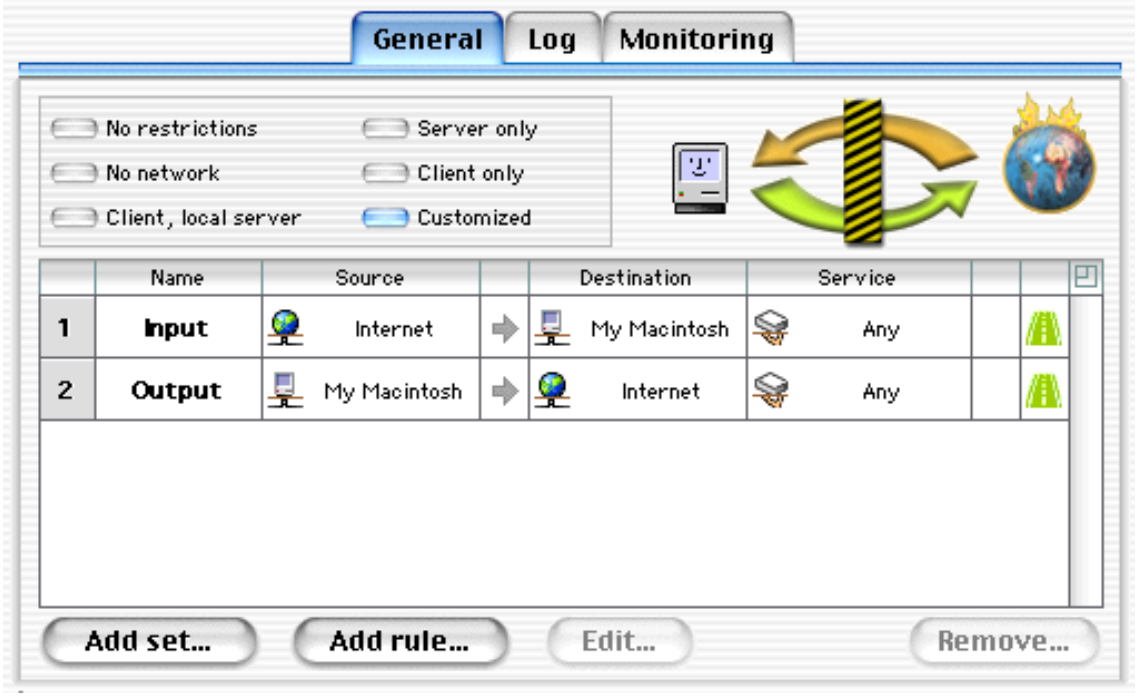
To rename a configuration set, select Configurations... from the File menu. A dialog box will open. Select a set by clicking on one of the sets in the list, and then click Rename.



Enter the name for your new set, and click OK. If you decide you do not want to rename this set, click Cancel.

7 - Customized Protection

Additional options concerning NetBarrier's Firewall feature are available in **Customized** mode. All the other features function in the same manner as presented above.



Customized protection gives access to NetBarrier's most powerful functions, by allowing you to configure its Firewall rules as precisely as you wish.

Important: NetBarrier's Customized protection should only be used by experienced network administrators. Incorrectly setting its options may disrupt your network activity.

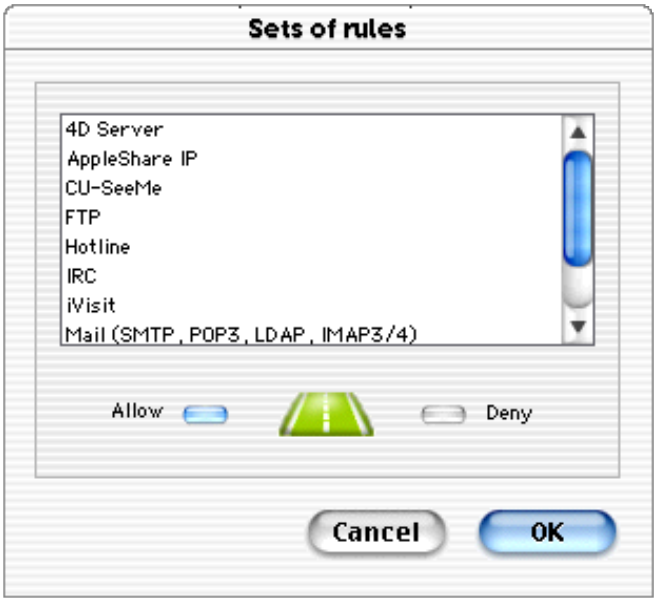
User-configurable Firewall Options

NetBarrier's Firewall allows you to create rules that examine incoming and outgoing data for specific sources, destinations and services, and act according to your choices. Your rules can be wide, such as preventing any incoming traffic from connecting to your computer, or precise, such as preventing incoming traffic from a specific host from connecting to a specific service on your computer.

Using Predefined Rule Sets

NetBarrier includes many predefined rule sets, corresponding to the most common Internet applications, so you can add specific rules for the applications and protocols you use. These rules make it easy to either allow or deny traffic for any of these applications or protocols.

To add a rule set, click the Add Set... button. The Rule Set window will be displayed.



To select one of the Rule Sets, just click on one of the applications or protocols in the list, click either Allow or Deny, and click OK. You will see that the rules for this application or protocol have been added to the rule list.

	Name	Source		Destination	Service		
1	Input	Internet	→	My Macintosh	Any		
2	Output	My Macintosh	→	Internet	Any		
3	AppleShar...	Internet	→	My Macintosh	AppleShare IP		
4	AppleShar...	My Macintosh	→	Internet	AppleShare IP		

All you need to do now is make sure the rule order corresponds to the way your rules should be applied. For more on this, see the Rule Order section later in this chapter.

Creating rules

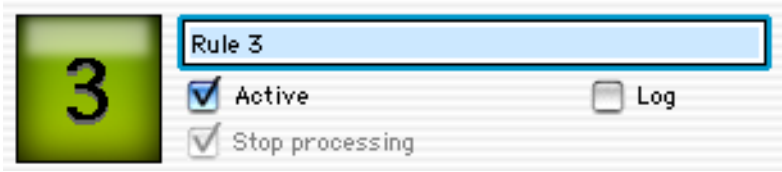
Creating a new rule is easy - just click on the Add rule... button and the Rule Editor will open.

NetBarrier's Rule Editor allows network administrators to quickly and easily define and implement a comprehensive security policy. It is extremely flexible, and allows you to define an unlimited number of rules.

The Rule Editor is a simple interface for creating rules. You can create a new rule in seconds.

To create a rule, you need to specify four things:

1. The Action
2. The Source
3. The Destination
4. The Service



At the top of the Rule Editor box is a field where you can name this rule. Just below it, are two check boxes. You must check the first one, Active rule, if you wish your rule to be activated. If it is not checked, NetBarrier will not use this rule. You may want to have rules that are not active at all times, so, in some cases you will not want to check this box. Or you may want to have certain rules active in one configuration, and not another. For more on using configurations, see chapter 6, **Settings and Configurations**.

Next to this check box is the Log check box. If this is checked, any time this rule acts, an entry will be added to the log. If it is not checked, this rule will not be logged.

Also, if the Log check box is checked, the Stop processing check box will be active. If you check this box, and the rule is activated, the rules following this one will not be checked. See below Rule Order for more on using the Stop processing function.

Actions

Two actions are possible for any rule: Allow or Deny. Select the action you wish to use for your rule by checking the appropriate radio button, at the bottom of the Rule Editor window.

Sources

The Source, for a rule, is the entity that is sending data. You can choose from three sources for any rule. You may notice that NetBarrier will not allow you to choose the same source and destination in a rule.

There are three sources available by default:

My Macintosh
This is your computer.

Local Network
This is a local network that your computer is connected to.

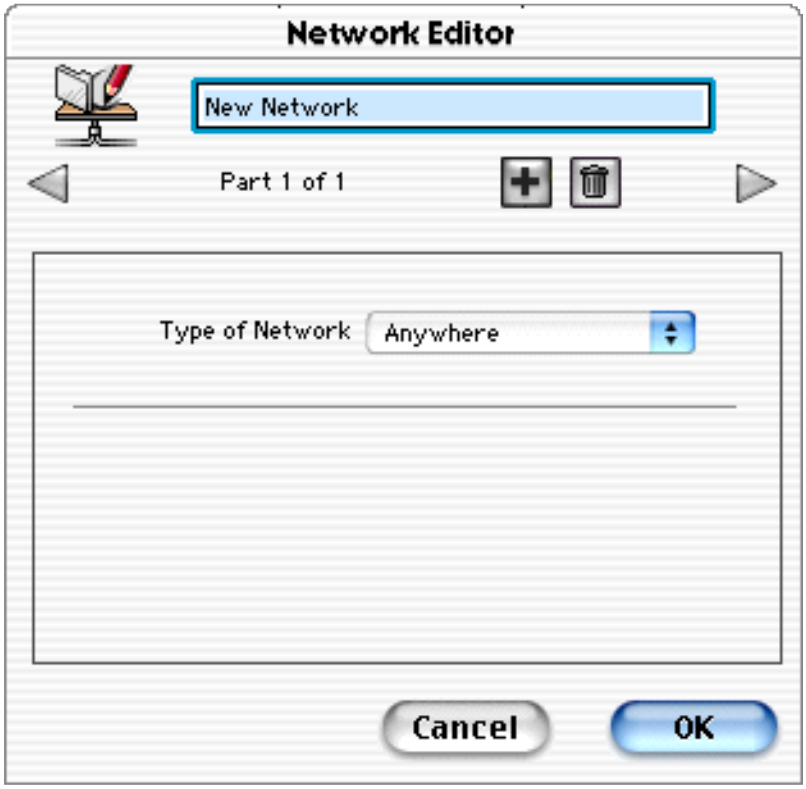
Internet
This is the Internet, in addition to any local network you may be connected to. Selecting Internet actually means all networks.

Creating new sources

You can create new sources to use in your rules. This allows you to specify exactly which computers you wish to have your computer communicate with.

To create a new source, select **Add new network**... from the source pop-up menu of the Rule Editor.

The Network Editor will open.



Source name

You may give the source any name you wish, by entering a name in the text field.

Source part

Sources can have several parts. You can, for example, select several specific IP addresses and include them in a given source. See below, Address for more on addresses.

Adding parts

To add a part, click on the plus icon in the part section of the Network Editor.

Moving from one part to another

You can move from one part to another by clicking either of the arrow icons, to move either forward or backward.

Deleting parts

To delete a part, it must be the part that is displayed. Click on one of the arrow icons until the part you wish to delete is displayed. Click on the trash can icon. A dialog box will be displayed, asking if you really want to delete this part. Click on OK to delete the part, if not, click Cancel.

Type of network

A pop-up menu lets you select from six types of network.

Anywhere

This is any network.

My Macintosh

This is your computer.

My local network

This is the local network your computer is connected to.

Machine

This is a specific IP address.

Network

This is a specific network, identified by its IP address and Subnet mask.

Interval

This is a group of IP addresses, delimited by a beginning and ending address.

Address

Depending on the type of network you select, the address section of the Network Editor will be different.

Anywhere

If you have selected this type of network, there will be nothing to enter in the Address section, since this source covers all networks.

My Macintosh

If you have selected this type of network, the IP address of your computer will be displayed in the Address field.

My local network

If you have selected this type of network, the beginning and ending addresses of your local network will be displayed in the Address field.

Machine

If you have selected this type of network, you must enter the IP address of a specific computer in this field.

Network

If you have selected this type of network, you must enter the IP address and Subnet mask of the network you wish to use.

Interval

If you have selected this type of network, you must enter the beginning and ending IP addresses of the networks you wish to use.

Deleting Sources

You can delete any sources that you have created. To do so, select the source, and then click on the trash can icon. A dialog box will be displayed, asking if you really want to delete that source. Click on OK to delete the source, if not, click Cancel.

Destinations

The destination, for a rule, is the entity that data is being sent to.
You can choose among three destinations for any rule. You may notice that NetBarrier will not allow you to choose the same source and destination in a rule.

There are three destinations available by default:

My Macintosh
This is your computer.

Local Network
This is a local network that your computer is connected to.

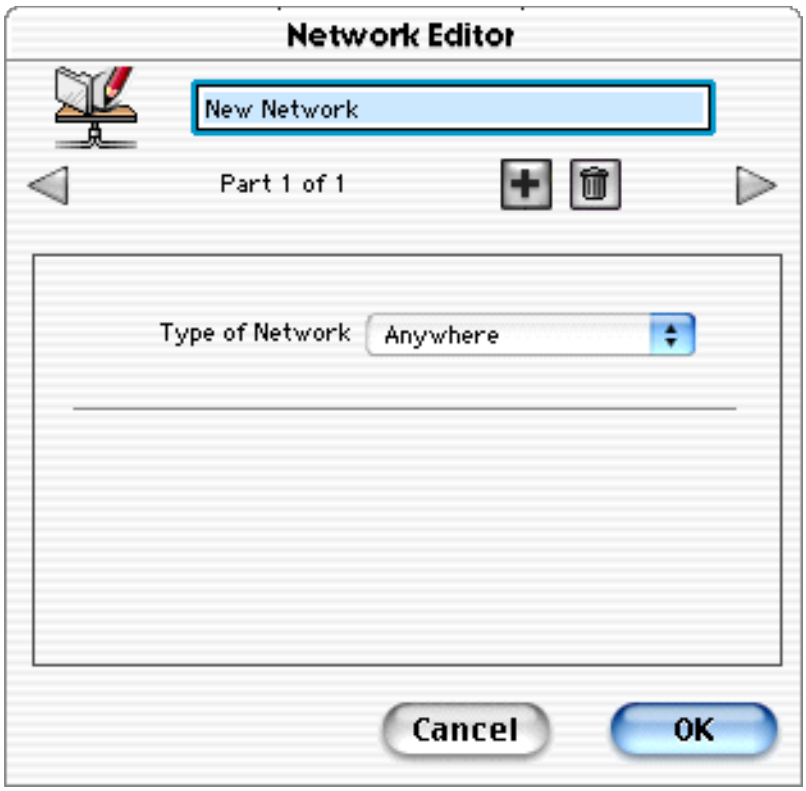
Internet
This is the Internet, in addition to any local network you may be connected to. Selecting Internet actually means all networks.

Creating new destinations

You can also create new destinations to use for your rules. This allows you to specify exactly which computers you wish to have your computer communicate with. This is done in the same manner as creating sources.

To create a new destination, select **Add new network**… from the destination pop-up menu of the Rule Editor.

The Network Editor will open.



Destination name

You may give the destination any name you wish, by entering a name in the text field.

Destination part

Destinations can have several parts. You can, for example, select several specific IP addresses and include them in a given destination. See below, Address for more on addresses.

Adding parts

To add a part, click on the plus icon in the part section of the Network Editor.

Moving from one part to another

You can move from one part to another by clicking either of the arrow icons, to move either forward or backward.

Deleting parts

To delete a part, it must be the part that is displayed. Click on one of the arrow icons until the part you wish to delete is displayed. Click on the trash can icon. A dialog box will be displayed, asking if you really want to delete this part. Click on OK to delete the part, if not, click Cancel.

Type of network

A pop-up menu lets you select from six types of network.

Anywhere

This is any network.

My Macintosh

This is your computer.

My local network

This is the local network your computer is connected to.

Machine

This is a specific IP address.

Network

This is a specific network, identified by its IP address and Subnet mask.

Interval

This is a group of IP addresses, delimited by a beginning and ending address.

Address

Depending on the type of network you select, the address section of the Network Editor will be different.

Anywhere

If you have selected this type of network, there will be nothing to enter in the Address section, since this destination covers all networks.

My Macintosh

If you have selected this type of network, the IP address of your computer will be displayed in the Address field.

My local network

If you have selected this type of network, the beginning and ending addresses of your local network will be displayed in the Address field.

Machine

If you have selected this type of network, you must enter the IP address of a specific computer in this field.

Network

If you have selected this type of network, you must enter the IP address and Subnet mask of the network you wish to use.

Interval

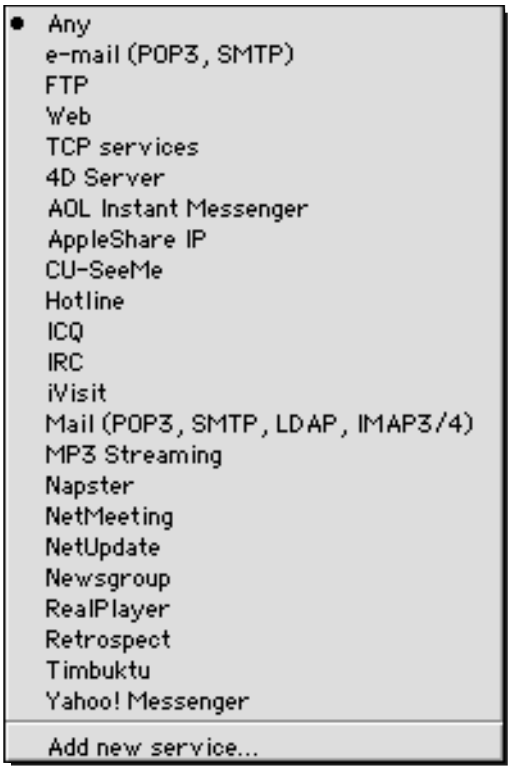
If you have selected this type of network, you must enter the beginning and ending IP addresses of the networks you wish to use.

Deleting Destinations

You can delete any destinations that you have created. To do so, select the destination, and then click on the trash can icon. A dialog box will be displayed, asking if you really want to delete that destination. Click on OK to delete the destination, if not, click Cancel.

Services

There are several services available by default:



Any

If this is selected, the rule will be active for all types of service.

E-mail

If this is selected, the rule will be active for e-mail only.

FTP

If this is selected, the rule will be active for ftp only.

Web

If this is selected, the rule will be active for HTTP, or web access, only.

TCP services

If this is selected, the rule will be active for TCP services only.

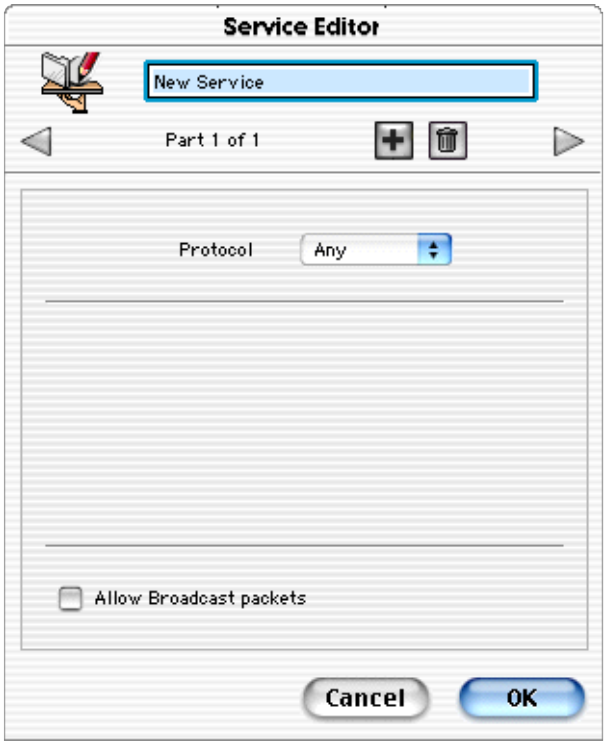
The remaining services are for specific programs

Creating new Services

You can also create new services to use for your rules. This allows you to specify exactly which services you wish to have your computer accept or use. This is done in the same manner as creating sources.

To create a new service, select **Add new service**… from the service pop-up menu of the Rule Editor.

The Service Editor will open.



Service name

You may give the Service any name you wish, by entering a name in the text field.

Service part

Services can have several parts. You can, for example, select several specific services and include them in a given rule.

Adding parts

To add a part, click on the plus icon in the part section of the Service Editor.

Moving from one part to another

You can move from one part to another by clicking either of the arrow icons, to move either forward or backward.

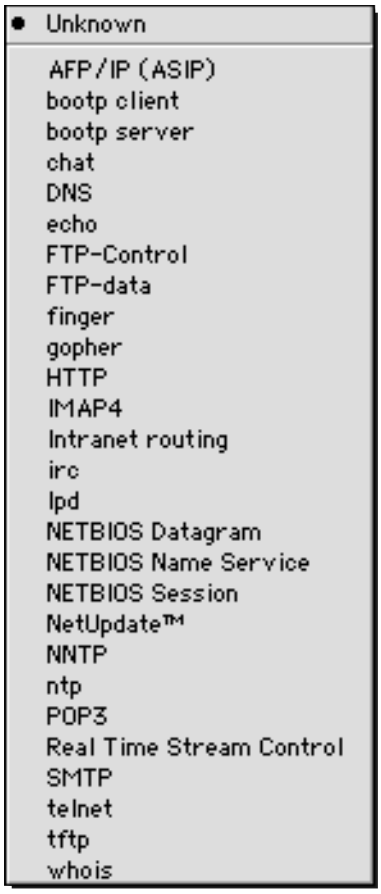
Deleting parts

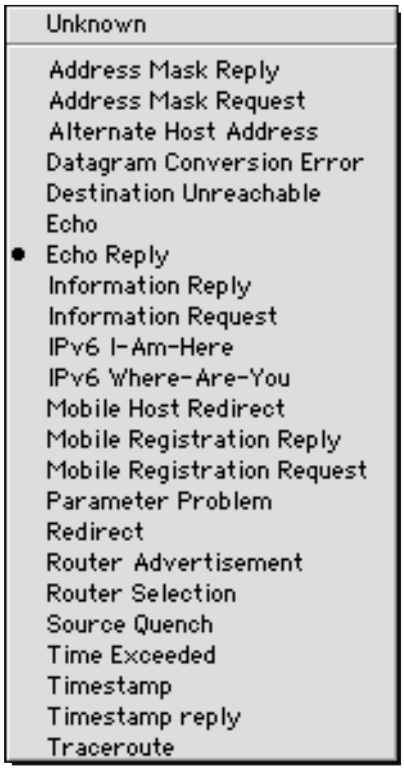
To delete a part, it must be the part that is displayed. Click on one of the arrow icons until the part you wish to delete is displayed. Click on the trash can icon. A dialog box will be displayed, asking if you really want to delete this part. Click on OK to delete the part, if not, click Cancel.

Protocol

There are four different protocol suites that can be selected from the pop-up menu: TCP, UDP, ICMP and IGMP. You can also select Any, which covers all protocols.

When you select one of these protocol suites, another pop-up menu will be displayed in the bottom section of the panel, with a list of protocols that you can select from. This menu depends on the protocol you have selected. For more information on these protocols, see chapter 9, **Glossary**.





Port or **Type**

There are two possibilities when selecting the Port, for TCP or UDP services, or Type, for ICMP or IGMP services.

Any port or **Any type**

If this is selected, the rule will be active for all ports, or types.

Specified port or **Specified type**

You can also specify the port number, or type. Selecting different services will automatically insert their standard port numbers in this field. If you need to use a different port number, you can enter it manually.

Intervals

For TCP and UDP services, you can also enter a range of ports. If you select Interval, you must enter the lowest and highest port numbers you wish to use in the **From** and **To** interval fields.

Allow Broadcast packets

If this is checked, broadcast packets, which are packets sent to all computers on a local network, will be included in this service.

Deleting services

You can delete any services that you have created. To do so, select the service, and then click on the trash can icon. A dialog box will be displayed, asking if you really want to delete that service. If so, click OK. If not, click Cancel.

Deleting rules

If you wish to delete a rule, select the rule by clicking on it once, then click Remove... A dialog box will open, asking if you really want to delete this rule. Click OK. If you decide you do not want to delete this rule, click Cancel.

Editing Rules

If you wish to edit a rule, select the rule by clicking on it once, then click Edit... The Rule Editor will open, and you can make any changes you wish to this rule. When you have finished making changes, click OK to save your changes. If you decide you do not want to save the changes, click Cancel.

Rule order

Rules added to the Firewall function from the first to the last. This means that you need to make sure that your rules are in the correct order to function correctly. Look at the following example:

	Name	Source		Destination	Service		
1	**Input**	Internet	→	My Macintosh	Any		STOP
2	**Output**	My Macintosh	→	Internet	Any		
3	**Rule 3**	Local Network	→	My Macintosh	Any		

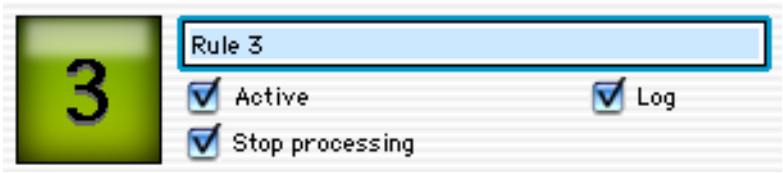
In this example, the first rule is blocking data coming from the Internet (which includes all networks, even a local network). Rule 3, however, is allowing traffic from a local network, but since it is in 3rd position, it will not be applied. The 1st rule will take precedence.

For rule 3 to be applied, it needs to be moved to the top of the rule list. To do this, select the rule, and slide it above the rule you want to place it in front of.

	Name	Source		Destination	Service		
1	**Rule 3**	Local Network	→	My Macintosh	Any		
2	**Input**	Internet	→	My Macintosh	Any		STOP
3	**Output**	My Macintosh	→	Internet	Any		

Using the Stop Processing Function

When you create a rule, and check the Log check box, the Stop processing check box will also be activated. It is checked by default. If you leave it checked, the rules following the current rule will not be verified.



However, if you uncheck this check box, you can create a rule that logs incoming or outgoing traffic, but does not take any other action on the traffic. If the traffic's IP address or service corresponds to that selected in the rule, and the Stop processing check box is not checked, the traffic will be logged, but nothing else will be done to it.

Note: care should be taken when creating rules for specific services. When you select a service for a specific program, it is possible that this program uses the same port as another program or service. Blocking or authorizing a specific service may conflict with other, more general rules. For example, if you wish to block ICQ traffic, selecting ICQ as a service will also block AOL Instant Messenger traffic since the two programs use the same port. Other programs may also use the same ports. If you find that you cannot connect to a given service, or send or receive traffic, try deactivating your rules one by one to see if there is a conflict.

8 - Technical support

Technical support is available for registered purchasers of NetBarrier.

By e-mail

support@intego.com

From the Intego web site

www.intego.com

9 - Glossary

Address mask: A bit mask used to identify which bits in an IP address correspond to the network address and subnet portions of the address.
Address mask reply: A reply sent to an address mask request.
Address mask request: A command that requests an address mask.
AppleTalk: A local area network protocol developed by Apple Computer, for use in local Macintosh networks.
Bootp: The Bootstrap Protocol. A protocol used for booting diskless workstations.
Bootp client: A computer operating as a Bootp client.
Bootp server: A computer operating as a Bootp server.
Broadcast packet: On an Ethernet network, a broadcast packet is a special type of multicast packet which all nodes on the network are always willing to receive.
Chat: A system that allows two or more logged-in users to set up a typed, real-time, on-line conversation across a network.
Client: A computer system or process that requests a service of another computer system or process (a "server"). For example, a workstation requesting the contents of a file from a file server is a client of the file server.
Connection flood: An attack on a computer, where the sending system sprays a massive flood of packets at a receiving system, in an attempt to connect to it, more than it can handle, disabling the receiving computer.
Cookie: file on your hard disk, which contains information sent by a web server to a web browser and then sent back by the browser each time it accesses that server. Typically, this is used to authenticate or identify a registered user of a web site without requiring them to sign in again every time they access that site. Other uses are, e.g. maintaining a "shopping basket" of goods you have selected to purchase during a session at a site, site personalization (presenting different pages to different users), tracking a particular user's access to a site.
Datagram: A self-contained package of data that carries enough information to be routed from source to destination independently of any previous and subsequent exchanges.

Datagram conversion error: An error in datagram conversion.

DNS: Domain Name System. Used by routers on the Internet to translate addresses from their named forms, such as www.intego.com, to their IP numbers.

Echo: The request sent during a ping.

Echo reply: The reply sent to an echo request.

Finger: A program that displays information about a particular user on the Internet, or on a network.

FTP: File Transfer Protocol. A protocol used for transferring files from one server to another. Files are transferred using a special program designed for this protocol, or a web browser.

Gopher: A distributed document retrieval system, which was a precursor to the World Wide Web.

Host: A computer connected to a network.

HTTP: HyperText Transfer Protocol, the protocol used to send and receive information across the World Wide Web.

ICMP: Internet Control Message Protocol. This protocol handles error and control messages sent between computers during the transfer process.

IGMP: Internet Group Management Protocol.

IMAP4: Internet Message Access Protocol. A protocol allowing a client to access and manipulate electronic mail messages on a server. It permits manipulation of remote message folders (mailboxes), in a way that is functionally equivalent to local mailboxes.

Intranet routing: The process, performed by a router, of selecting the correct interface and next hop for a packet being forwarded on an Intranet.

IP: The network layer for the TCP/IP protocol suite widely used on Ethernet networks and on the Internet.

IP address: An address for a computer using the Internet Protocol.

Irc: Internet Relay Chat. A medium for worldwide "party line" networks that allowing one to converse with others in real time.

Local network: A network of computers linked together in a local area. This may be a single building, site or campus.

NETBIOS: Network Basic Input/Output System. A layer of software originally developed to link a network operating system with specific hardware. It can also open communications between workstations on a network at the transport layer.

Network: A group of interconnected computers that can all access each other, or certain computers. This may be a local network, or a very large network, such as the Internet.

NNTP: Network News Transfer Protocol. A protocol for the distribution, inquiry, retrieval and posting of Usenet news articles over the Internet.

Ntp: Network Time Protocol. A protocol that assures accurate local timekeeping with reference to radio, atomic or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

Packet: The basic unit of data sent by one computer to another across most networks. A packet contains the sender's address, the receiver's address, the data being sent, and other information.

Ping: A program used to test reachability of computers on a network by sending them an echo request and waiting for a reply.

Ping broadcast: An attack similar to a ping flood. See below.

Ping flood: A ping attack on a computer, where the sending system sends a massive flood of pings at a receiving system, more than it can handle, disabling the receiving computer.

Ping of death: An especially dangerous ping attack, that can cause your computer to crash.

POP3: Post Office Protocol, version 3. POP3 allows a client computer to retrieve electronic mail from a POP3 server.

Port scan: A procedure where an intruder scans the ports of a remote computer to find which services are available for access.

Protocol: The set of rules that govern exchanges between computers over a network. There are many protocols, such as IP, HTTP, FTP, NNTP, etc.

Router: A device that forwards packets between networks, reading the addressing information included in the packets.

Server: A computer connected to a network that is serving, or providing data or files to other computers called clients.

Service: A network function available on a server, i.e. http, ftp, e-mail etc.

SMTP: Simple Mail Transfer Protocol A protocol used to transfer electronic mail between computers.

Spam: Unwanted e-mail messages, usually sent to thousands, even millions of people at a time, with a goal of selling products or services.

TCP: Transmission Control Protocol. The most common data transfer protocol used on Ethernet and the Internet

TCP/IP: The Internet version of TCP -TCP over IP.

Telnet: The standard Internet protocol used for logging into remote computers.

Tftp: Trivial File Transfer Protocol. A simple file transfer protocol used for downloading boot code to diskless workstations.

Traceroute: A utility used to determine the route packets are taking to a particular host.

UDP: User Datagram Protocol. Internet protocol which provides simple but unreliable datagram services.

Whois: An Internet directory service for looking up names of people on a remote server.