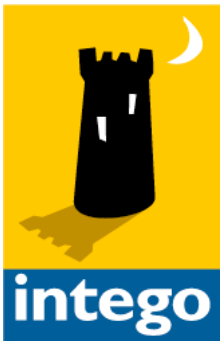
User's Manual



NetBarrier X for Macintosh

Intego, Inc.
www.intego.com

NetBarrier uses the EDCommon and EDInternet frameworks written by Erik Dörnenburg.

Contents

1- About NetBarrier X

What is NetBarrier X?

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

NetBarrier X 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 X's Features

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

Personal firewall

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

Antivandal

NetBarrier X'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 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. Several options allow you to choose the type of protection you have on your computer.

Alerts

NetBarrier X stops all incoming data that is considered hostile. An alert dialogue can be displayed, showing why the data was stopped, and asking you to allow or deny it. Other alert options can be selected, such as having NetBarrier X play a sound, putting the host automatically in the Stop List or sending an e-mail message to the address(es) of your choice in the case of an alert.

Stop List

When an intruder is detected trying to break in to your computer, NetBarrier X 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 blocked.

Trusted Group

In some cases, computers you know - friends, not foes - will be blocked by NetBarrier X. These may be computers on your local network, blocked because they are sending pings to your computer, for

example. NetBarrier X allows you to put them in the Trusted Group, where they will be considered friends for as long as you want, ensuring that computers on your network have full access to your computer.

Data Filter

NetBarrier X has a unique function that protects you and your information - the Data Filter ensures that any sensitive information you choose to protect cannot leave your computer and go onto a network. You decide what to protect, such as your credit card number, passwords, or key words that appear in sensitive documents, and NetBarrier X'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, it also protects against anyone who has network access to your computer from taking copies of them.

NetBarrier X's Privacy Protection

NetBarrier X helps protect your privacy. It can block ad banners and lets you manage cookies, deleting them whenever you want. It 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 X 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 X'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 just for 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 X.

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 X 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 enjoys messing up people's computers just for fun.

Without NetBarrier X, you may 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 X 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 X 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 X allows 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 X'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 X recognizes these methods.

What You Risk

Why people break into computers

People break into computers for many reasons. Sometimes, this is done just to get into more systems; by hopping between many computers 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; thieves, looking for passwords and credit card numbers; or simply spies. While most companies have computer 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 your browser sends information to web sites telling which 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 can 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 X'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 officially-supported Mac OS X compatible computer
- Mac OS X 10.1.1 or higher, or Mac OS X Server 10.1.1 or higher
- 10 MB free hard disk space
- Minimum screen resolution 800 x 600

Installing NetBarrier X

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

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

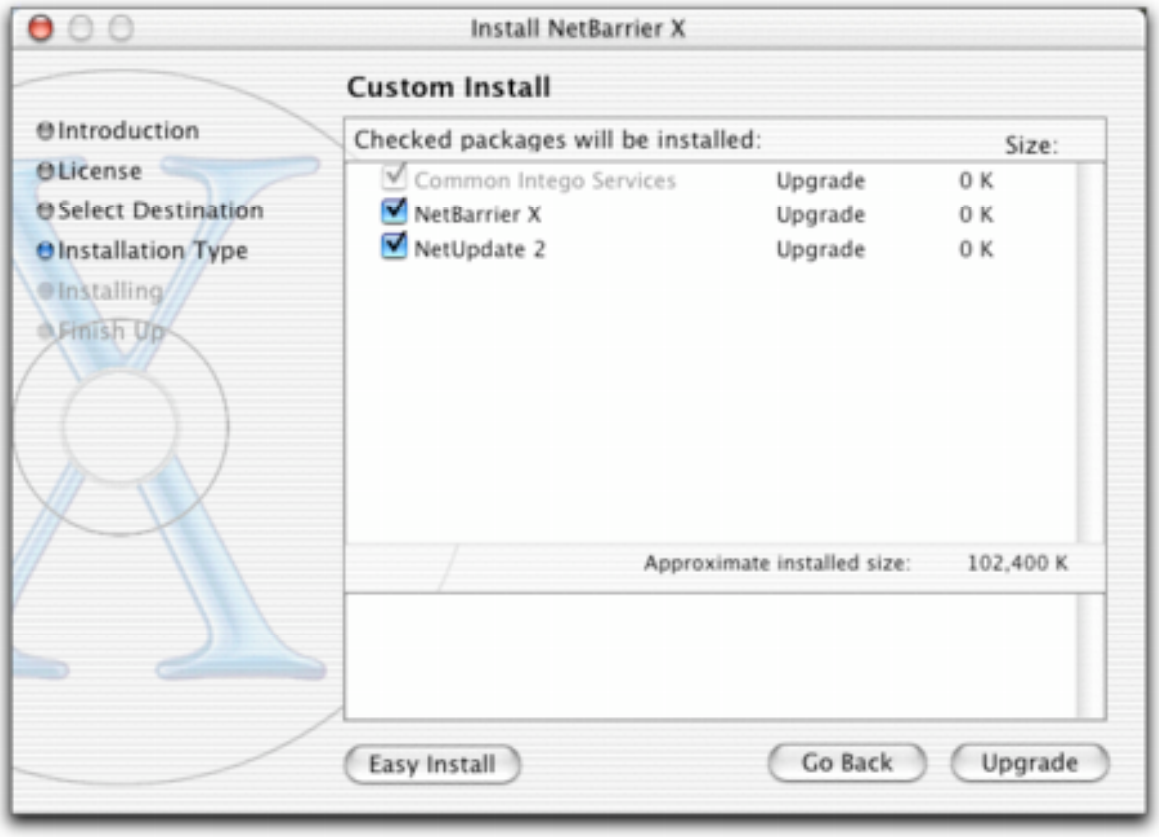
Then, double-click the NetBarrier X installer.

You will see a window displayed informing you that you must enter an administrator's password to install NetBarrier X. Click the lock to enter your password. Enter your password, then click OK. The following window will be displayed:

Click continue to proceed with installation. The Intego software license will be displayed. Click Continue, then click Agree if you accept this license; if not, click Disagree, and the installer will quit.

The next window will show all the available disks or volumes on your computer. Select the disk or volume where you want to install NetBarrier X then click Continue.

Click Install to install NetBarrier X. This will perform a basic installation. If you wish to perform a custom installation, click Customize. The following window will be displayed:



This window lets you choose which items will be installed. As you can see, the Common Intego Services check box is grayed out, because this must be installed. You have the choice of installing either NetBarrier X, NetUpdate or both.

After installation, you will have to restart your computer.

Registering NetBarrier X

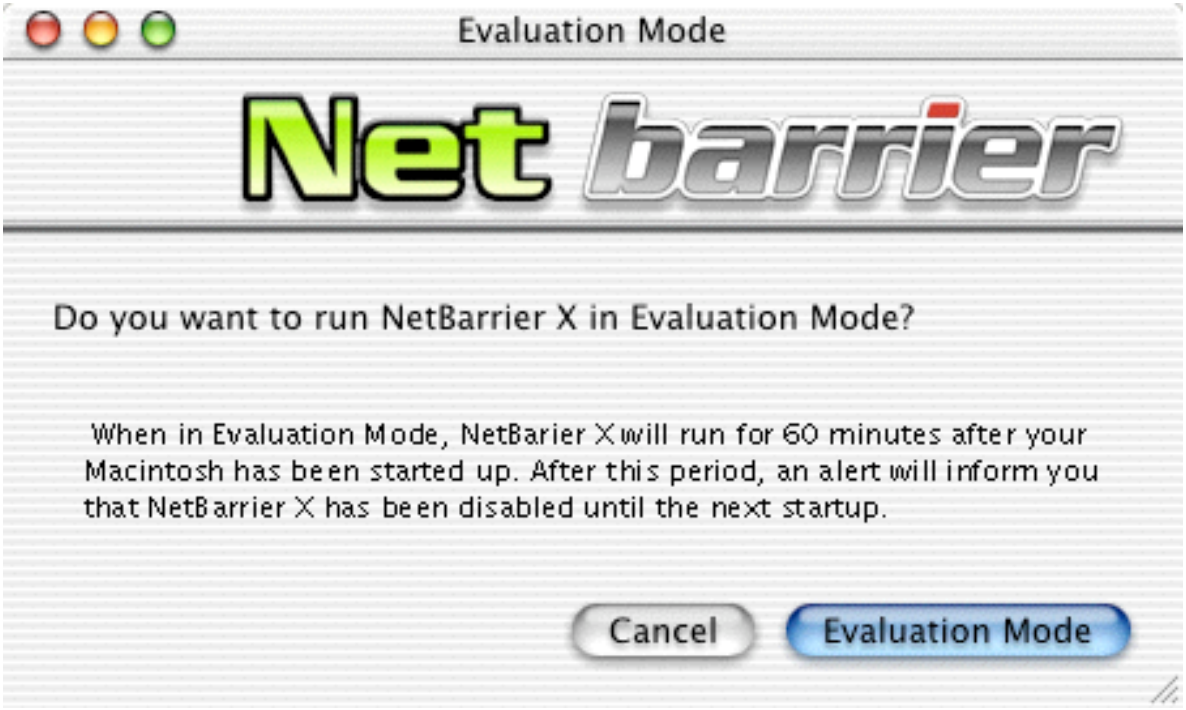
When you restart your computer, open NetBarrier X - it is found in your Applications folder. NetBarrier X will open its Registration program, and display the following window:

Since Mac OS X is a multi-user operating system, not all users have the same privileges. When starting up NetBarrier X for the first time, any user can enter the serial number, but only a user with administrator privileges can configure the program.

You must enter your name, company, if any, and your serial number. The serial number is found on a sticker on the NetBarrier X CD. When registration is completed, NetBarrier X will open, and, if you are an administrator, you can configure the program.

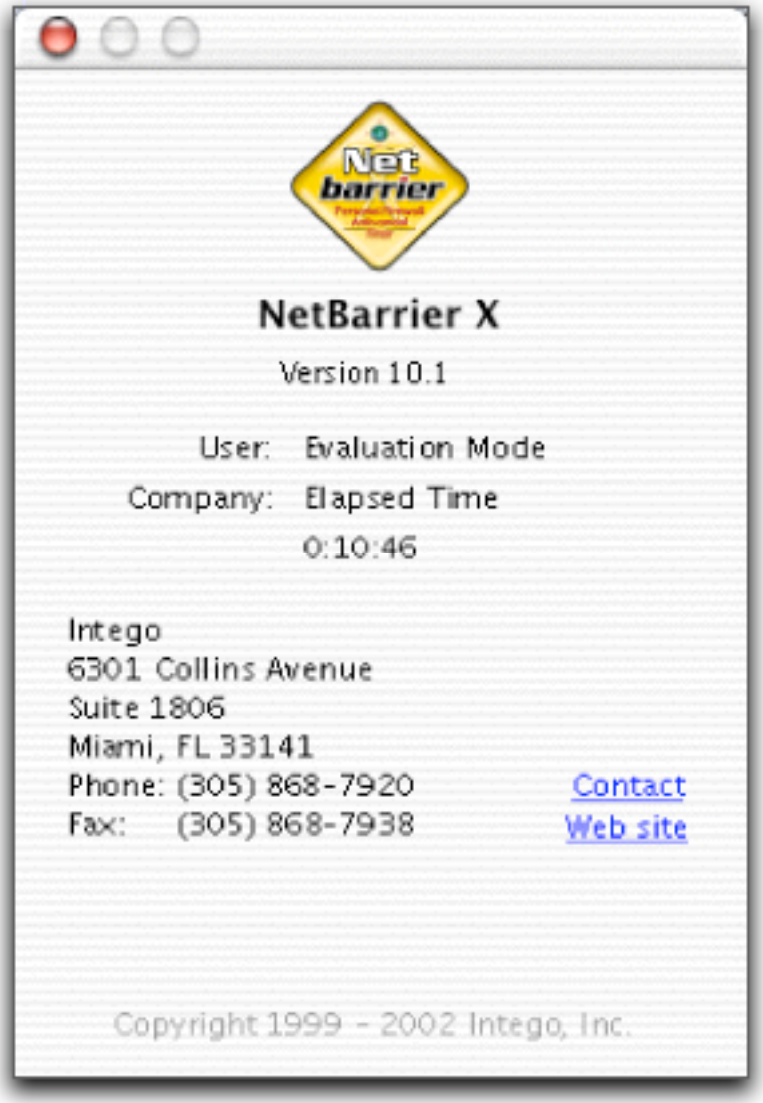
Using NetBarrier X in Evaluation Mode

NetBarrier X offers an evaluation mode, to allow you to discover how it works before purchasing the program. To use NetBarrier X in evaluation mode, click Cancel when the registration screen displays. NetBarrier X then displays a screen asking if you want to run the program in Evaluation mode. If you do, click Evaluation mode; if not, click Cancel.



When NetBarrier X runs in evaluation mode, it functions for 60 minutes after startup. It then displays an alert telling you that the program is disabled until the next startup. You will be able to enter a serial number for the program at this time, if you wish, or any time you start up your Mac and open NetBarrier X.

You can find out how much time is left in your evaluation session by choosing About NetBarrier X from the NetBarrier X menu. The About screen tells you that the program is in evaluation mode, and shows the time elapsed in the current session.

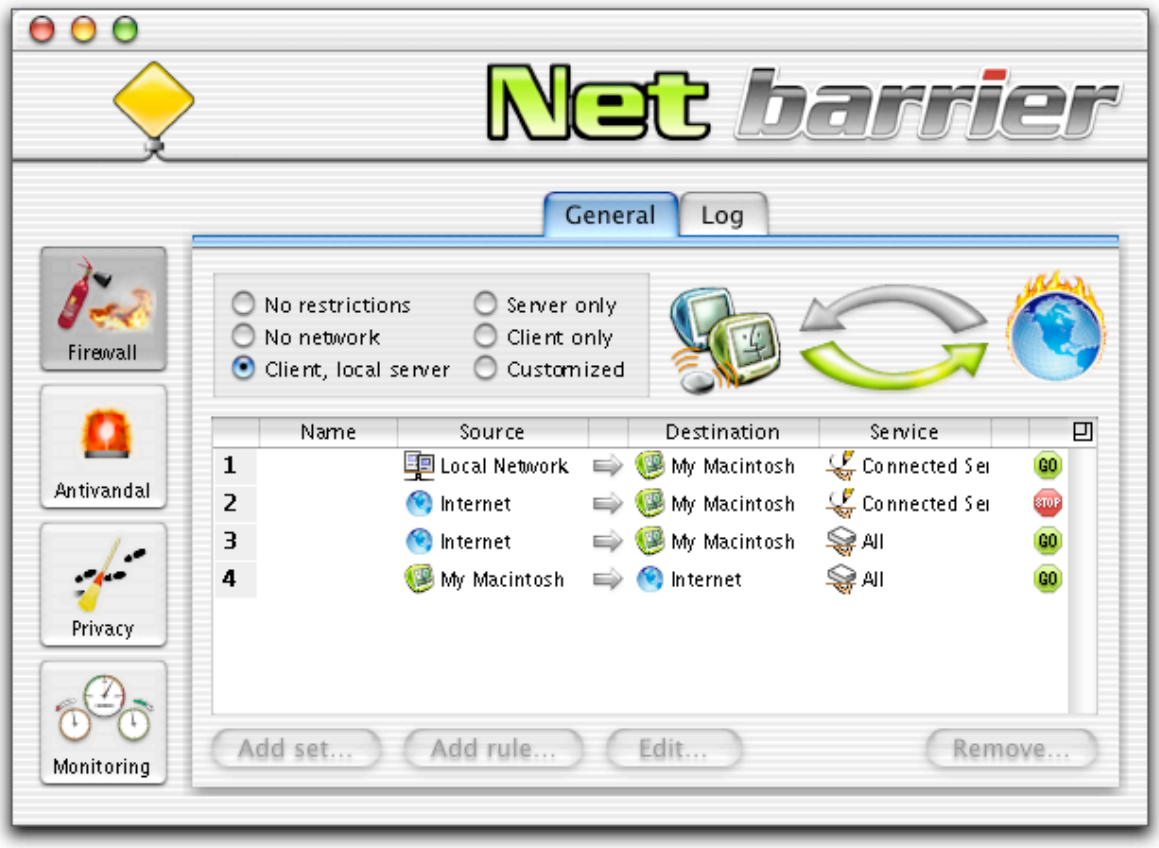


If you wish to purchase a license for NetBarrier X, click the Web Site link in the about box to go to the Intego web site.

4 - Quick Start

NetBarrier X's Default Mode

When you install NetBarrier X, 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.

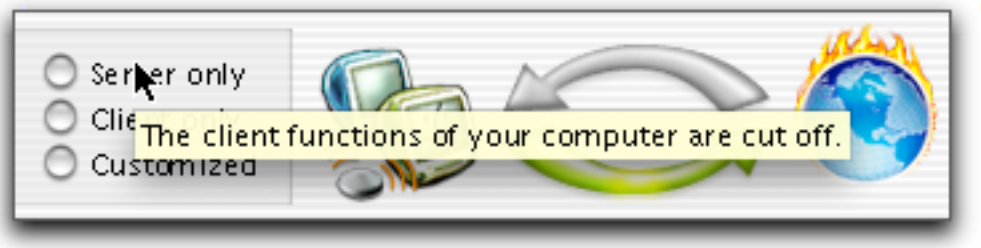


NetBarrier X Password Protection

NetBarrier X uses built-in Mac OS X password protection. In order to install and configure the program, the user must have administrator's rights, and log in with an administrator's name and password. Other users, who do not have administrator's rights, cannot change any of NetBarrier X's settings or preferences. These users can view such things as logs and traffic gauges, but this ensures that no changes to the program's operation be made by unauthorized users.

Getting Help

You can get help on some of NetBarrier X's functions by holding your cursor over certain texts and zones:



A Tool Tip will be displayed explaining the various functions and features.

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

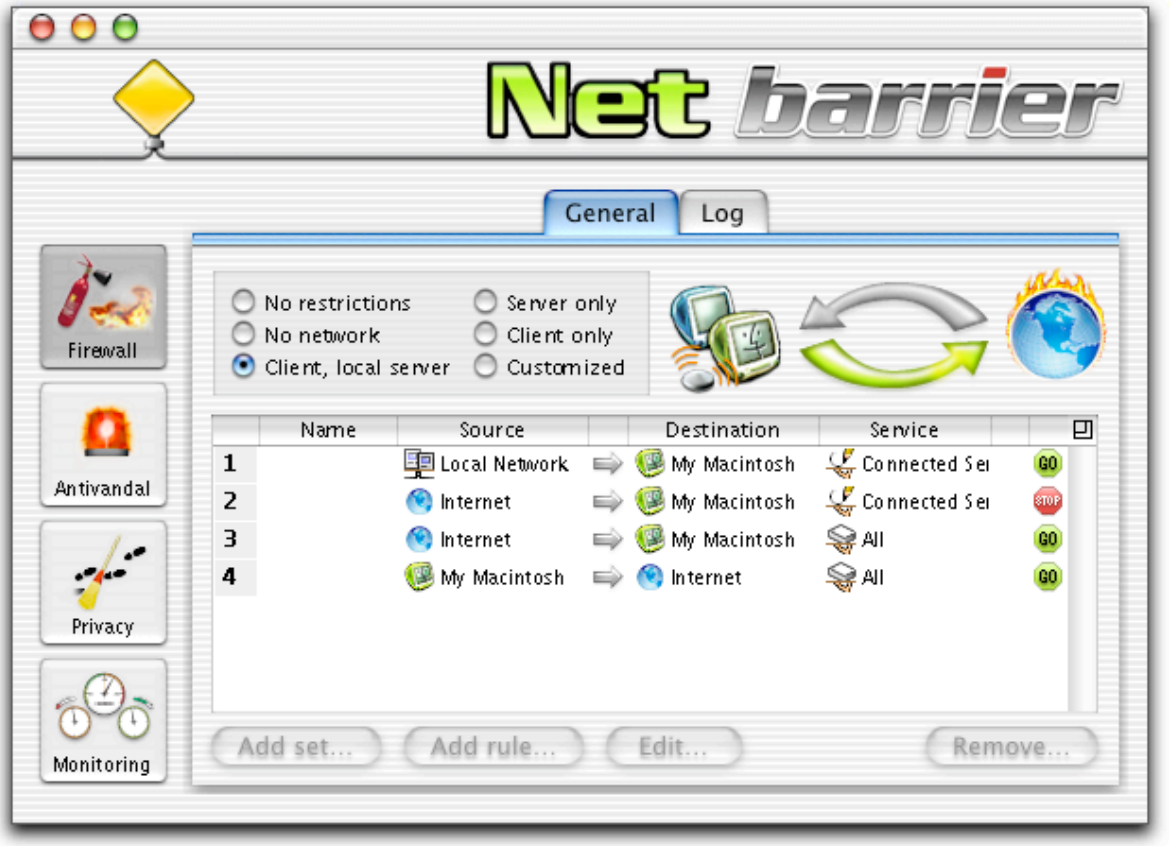
5 - The Three Lines of Defense

NetBarrier X 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

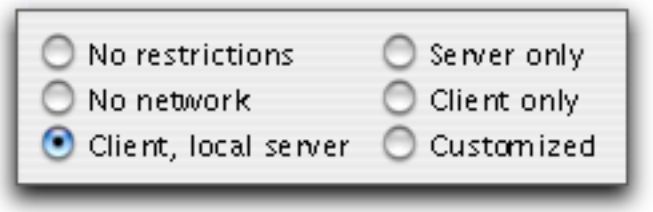
NetBarrier X contains a personal firewall. This is a powerful program that filters all the data packets that enter or leave your computer, to or from the Internet or a local TCP/IP network, to allow or prevent data going to and coming from specific sources and destinations.

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



Firewall settings

NetBarrier X's Firewall has 6 different settings that correspond to the way you use your computer. When you install NetBarrier X, 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 X'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 X's Firewall prevents all data from entering or leaving your computer to or from the Internet or a local TCP/IP network. This is useful if you are away from your computer, and wish to protect it totally.

Client, local server

In this mode, NetBarrier X'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 X'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 X'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.

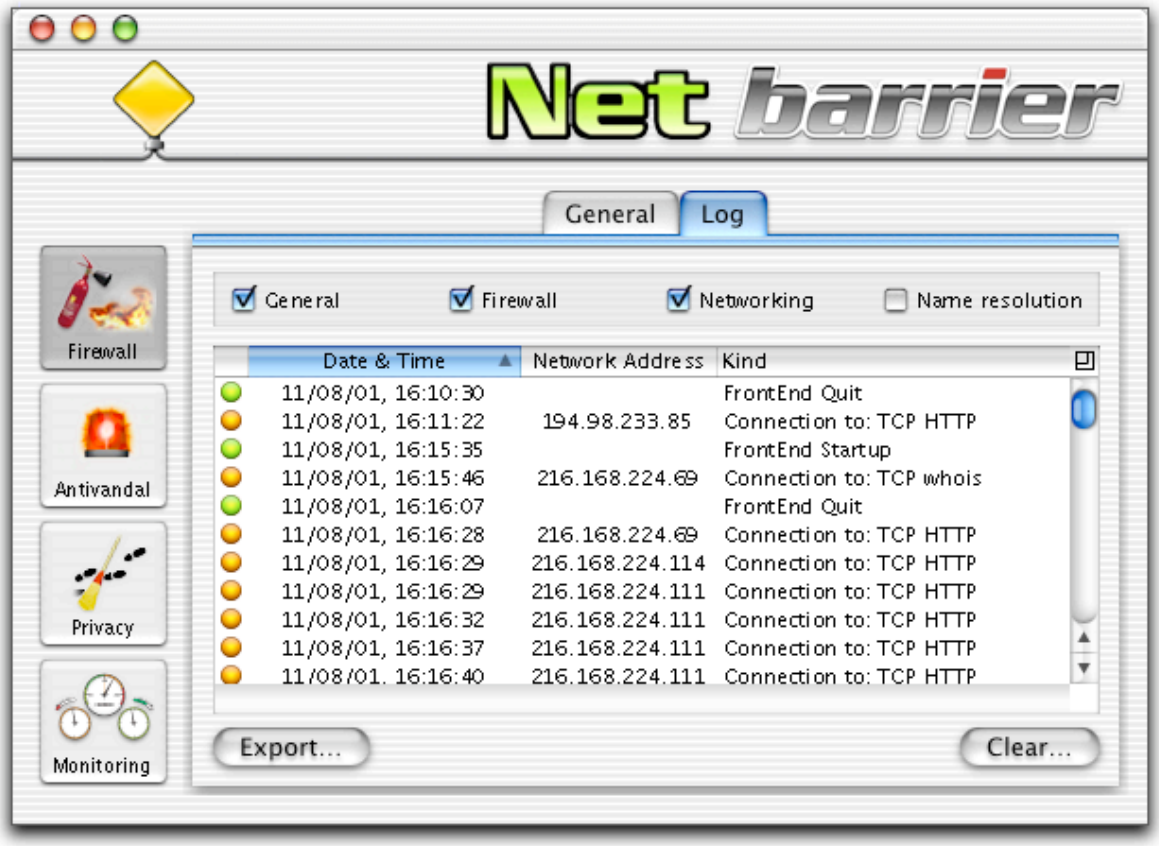
Customized

This setting gives you access to NetBarrier X'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 X 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 X activity, such as NetBarrier X startup, and alerts.

Firewall

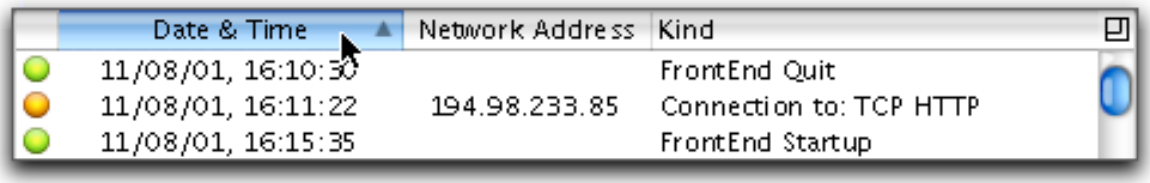
NetBarrier X logs all firewall activity, when rules are applied, if logging has been activated in the rules.

Networking

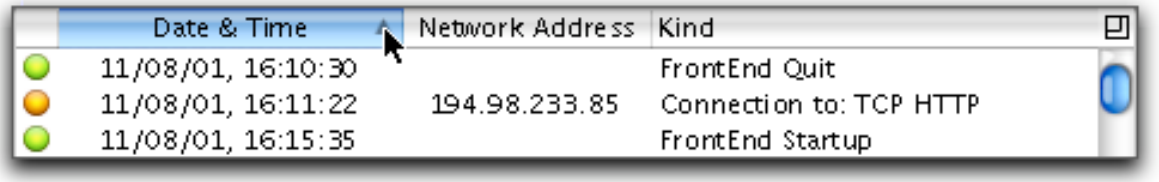
NetBarrier X logs all connections to networks or the Internet, and when IP addresses in the Stop List attempt to connect to your computer.

Changing the Log Display

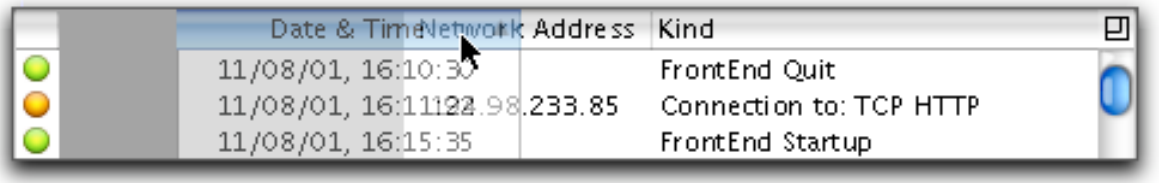
The Log can be sorted by any of its columns by clicking on the header just above the column.



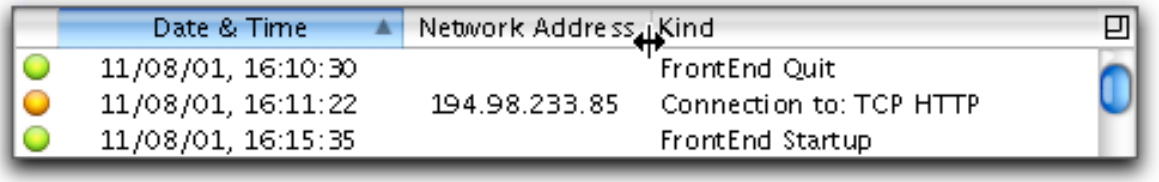
It can also be sorted in ascending or descending direction by clicking on the sort button, the small triangle in the selected sort column header.



You can drag any of the columns to change their order. To do this, click one of the column headers and drag it where you want, then release your mouse button.

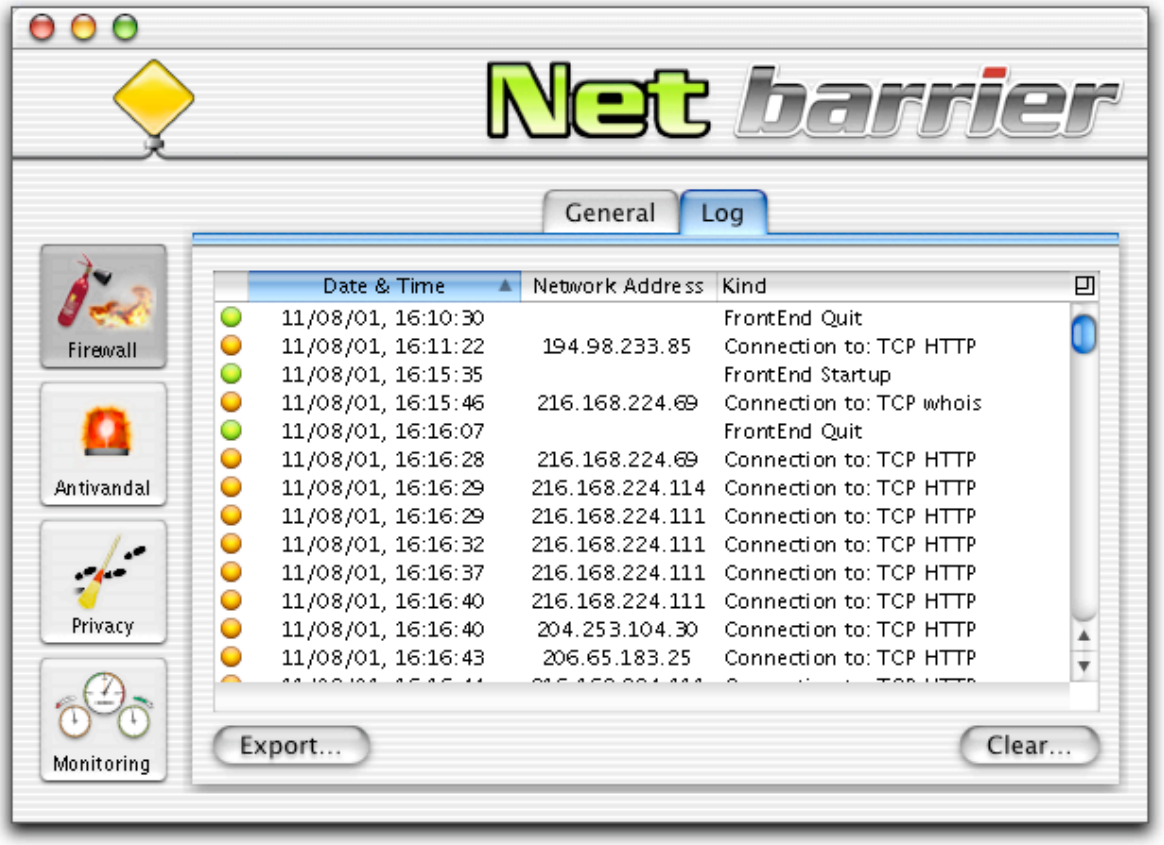


You can change the width of the Network Address and Kind columns. To do this, move the cursor to the line between two columns. The cursor will change, showing that you can move this boundary. Click the cursor and drag in either direction to make a column wider or narrower.



You can expand the list display by clicking the zoom box on the right side of the list. The list will expand, covering the area above it, giving you a display with

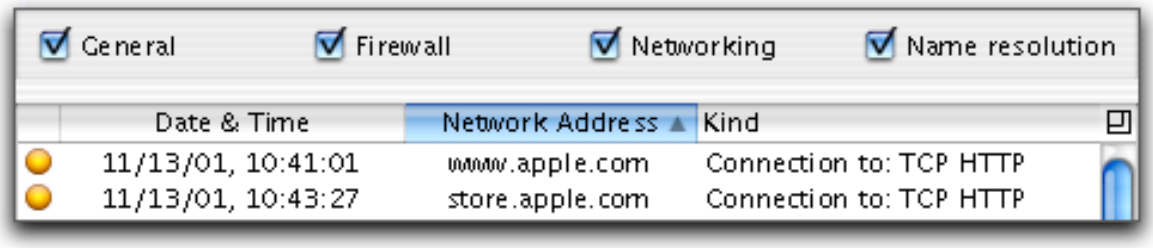
more lines. To reduce the list display, click the zoom box again. It will return to its normal size.



Domain Name Resolution

NetBarrier X 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 X will attempt to find the names for each of the Internet addresses shown in the log. If found, these domains will then be displayed in their name form, rather than as numbers.



Note: In some cases, NetBarrier X 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:

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

Date & Time
This is the date and time of the incident.

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

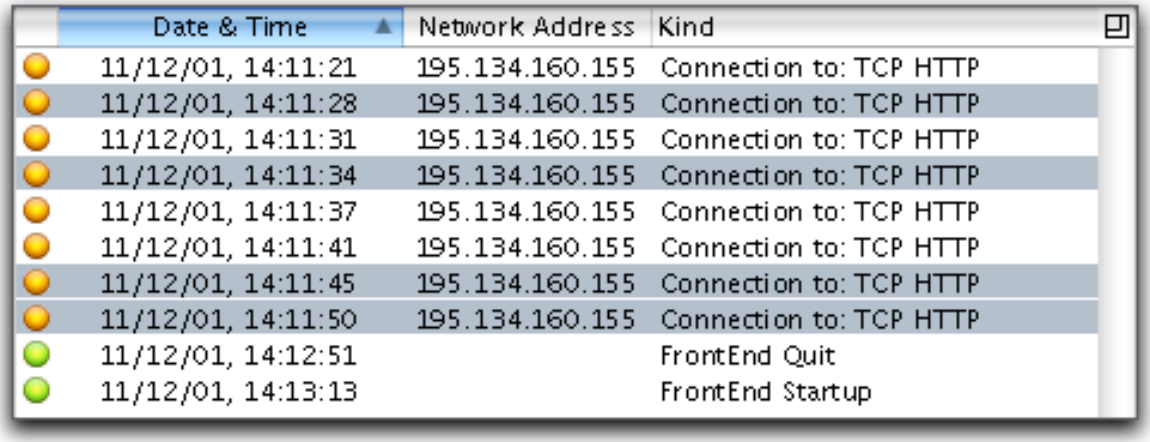
Kind
This is the kind of incident reported.

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 Clear to clear the Log, or click Cancel to cancel the operation.

Selecting Log Data

You can select log data to copy, and paste into another program or to drag into another window. You can make 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. To make a non-contiguous selection, hold down the Command key and select several non-contiguous lines.

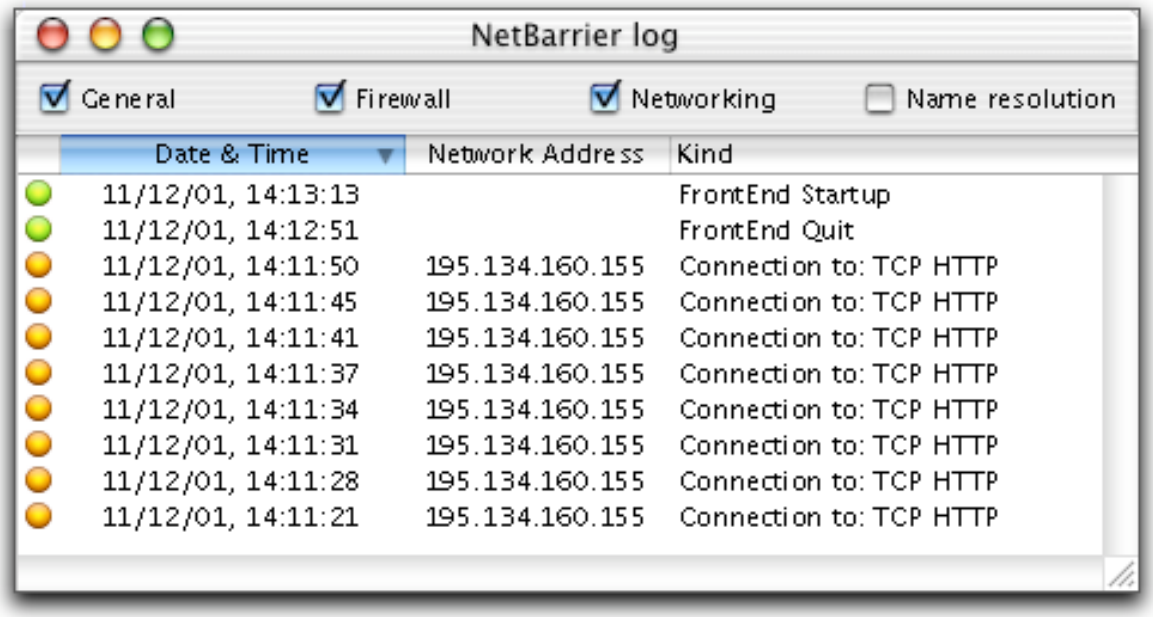


Date & Time	Network Address	Kind
11/12/01, 14:11:21	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:11:28	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:11:31	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:11:34	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:11:37	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:11:41	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:11:45	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:11:50	195.134.160.155	Connection to: TCP HTTP
11/12/01, 14:12:51		FrontEnd Quit
11/12/01, 14:13:13		FrontEnd Startup

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.

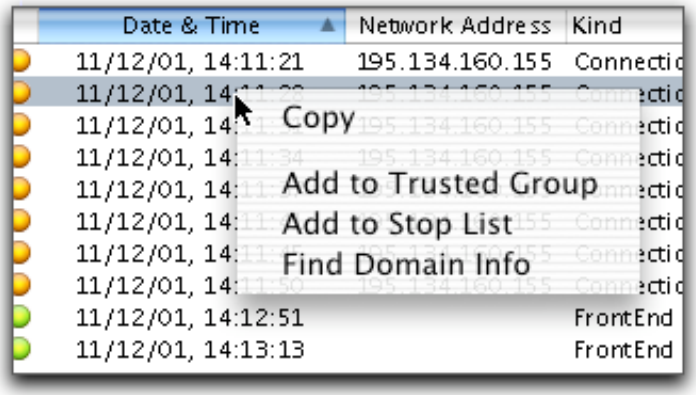
Displaying the Log Window

The Log window can be displayed alone, without the rest of NetBarrier X's interface. To do this, select Show Log Window from the Window menu. This displays the Log in a new window that you can resize, to make it easier to view long logs.



Log Window Contextual Menu

If you hold down the control key and click any Log entry a contextual menu is displayed.



This menu allows you to do the following:

Copy

If you select Copy from the contextual menu, the content of this line will be copied to the clipboard. You can then paste it into any application or document.

Add to Trusted Group

If you select this item from the contextual menu, the IP address will be added to the Trusted Group. For more on the Trusted Group, see the **Trusted Group** section later in this chapter.

Add to Stop List

If you select this item from the contextual menu, the IP address will be added to the Stop List. For more on the Stop List, see the **Stop List** section later in this chapter.

Find Domain Info

If you select this item from the contextual menu, NetBarrier X will look up the domain name or IP address using its Whois function. For more on Whois, see the **Whois** section later in this chapter.

Exporting the Log

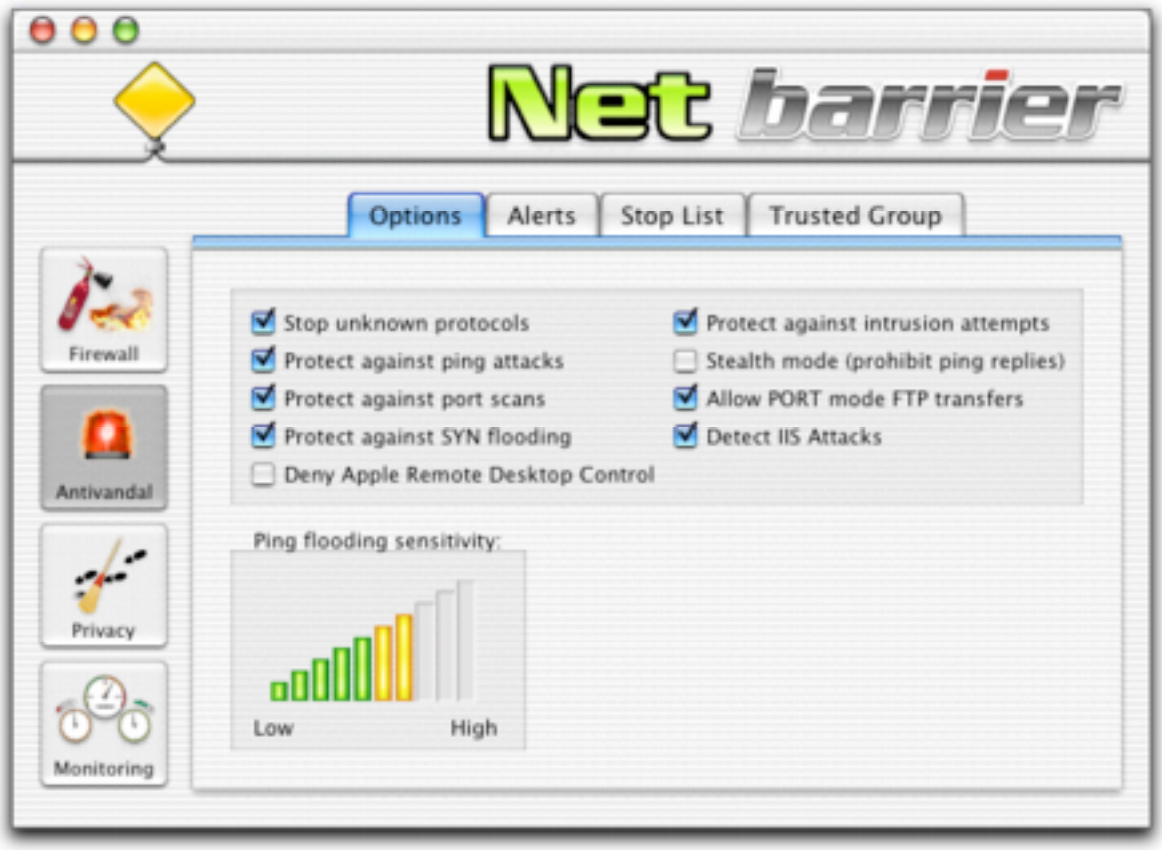
Log data can be exported in text or HTML format. When doing a manual export, only the data displayed is exported - if you have only checked, say, Firewall in the Log panel, only Firewall data will be exported. (You can have the Log data exported automatically. For more on this, see chapter 6, **Log Export Preferences**.)

To export Log data, click the Export... button. A dialog will prompt you to save the file; you may change its name if you wish. Choose where you wish to save it - by default, all export files are saved to the current user's Documents folder. The Export Format popup menu lets you choose whether you save the file in HTML or Text format (when text format is selected, the data is saved in tabulated text form, which can be easily used in a spreadsheet as well as a word processor). Click Save. You will now have a copy of your log that you can open with any word processor (text), spreadsheet (text) or web browser (HTML).

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

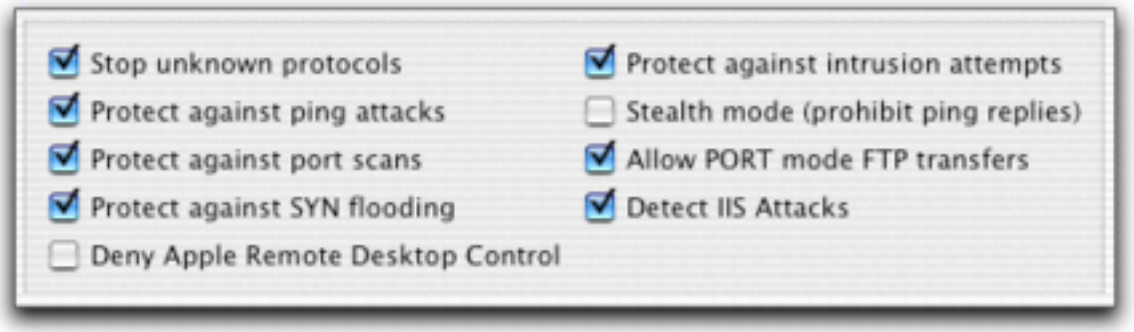
Antivandal

NetBarrier X'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 X 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 X'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 X'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 X will send you an alert if three 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 Web Sharing, File Sharing or FTP.

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.

Detect IIS Attacks

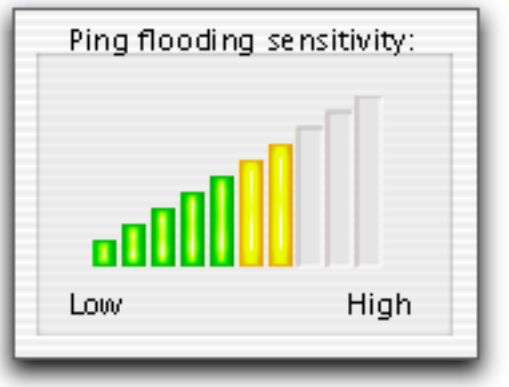
If this is checked, NetBarrier X detects CodeRed and nimda requests sent to your computer if it is configured as a web server, or if you have a server expecting calls to HTTP ports. This protects you from denial of service attacks.

Deny Apple Remote Desktop Control

If this is checked, NetBarrier will block all requests to use Apple Remote Desktop software.

Setting Ping Flooding Sensitivity

You can adjust the sensitivity of Net Barrier X's ping flooding protection. 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 flooding sensitivity, click one of the bars. The bar will be colored 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 flooding sensitivity.

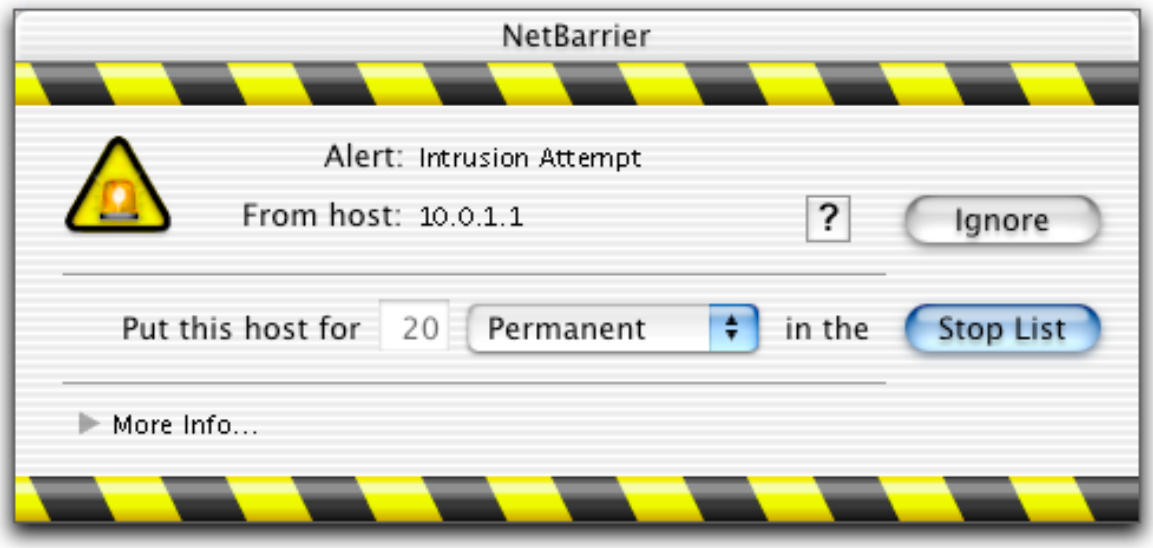
Alerts

How alerts work

NetBarrier X 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 X will display an alert, asking you whether you wish to allow the data to be sent or deny it.

Understanding alerts

The following is an example of an alert. The top line shows the reason for the alert. Here, an Intrusion Attempt was detected. The host, 10.0.1.1, shown by its IP address, tried to connect three times with a bad password. Two buttons on the right allow you to decide what action to take for this alert.



If you click the More Info… 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 blocked. 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.

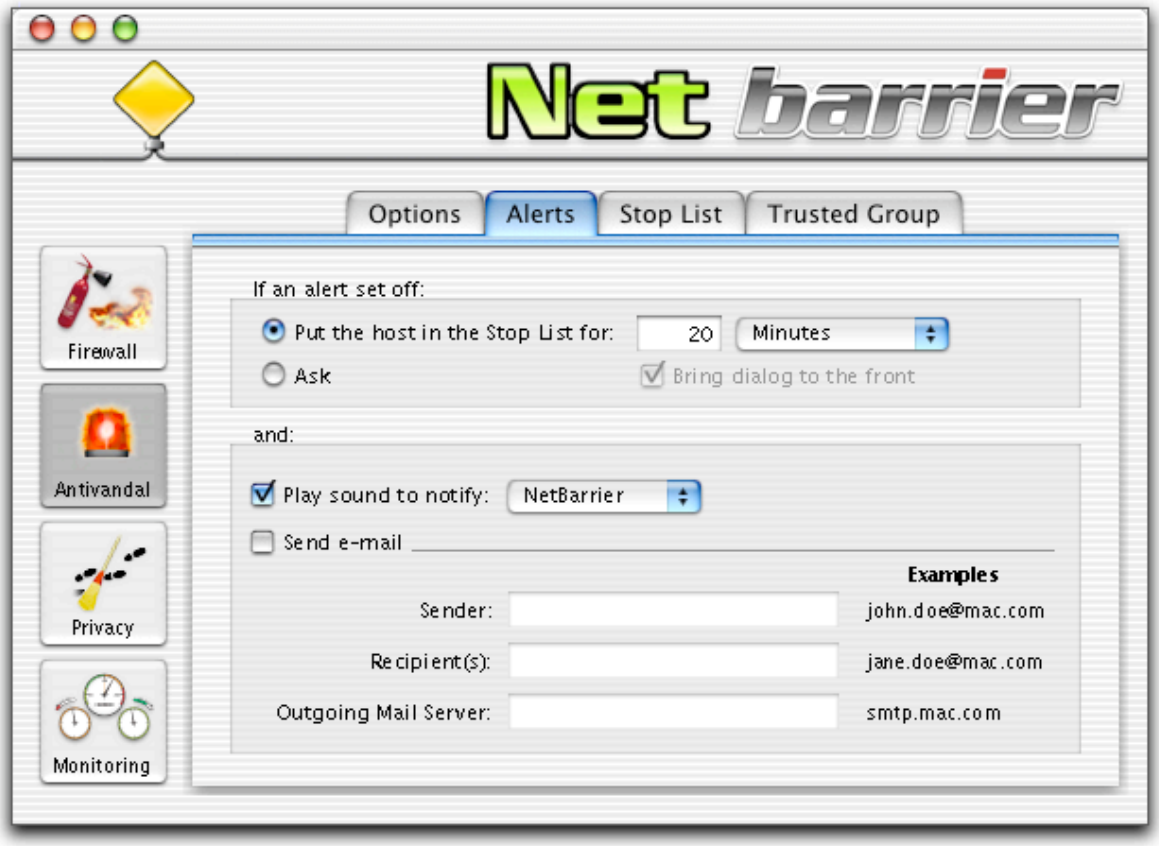
If you click Stop List, the IP address that caused this alert to be displayed will be automatically added to the Stop List, and kept there for the default time that has been set. (See **Stop List,** chapter 5.) This time can, however, be changed in the Alerts screen by entering a new time in the time field, and changing the time unit in 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 X detects another attempted intrusion. In this case, another alert will be displayed.

Alert options

The Alerts tab gives you several options as to how NetBarrier X 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 immediately placed in the Stop List. (See **Stop List,** chapter 5.) A field to the right of this button allows you to specify the default time period that the offending IP address will remain in the Stop List. You can choose any

number of seconds, minutes, hours or days, or choose to have the intruder remain on the Stop List permanently.

Ask

If this is checked, NetBarrier X 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 Stop List time period selected in the Alert options by default, but this time can be changed in the Alerts screen.

Bring dialog to the front

If this is checked, the NetBarrier X 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 X 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.

Send e-mail

If this is checked, NetBarrier X will automatically send an e-mail message to the address entered in the text field, within 30 seconds. (NetBarrier X waits to see if there are other intrusion attempts, rather than send an e-mail message each time.) The e-mail address for the sender and recipient must be entered, as well as the outgoing mail server. You can send this e-mail message to multiple recipients. To do this, enter several e-mail addresses separated by commas.

The Stop List

The Stop List is a powerful feature of NetBarrier X 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 Alerts screen (see above).

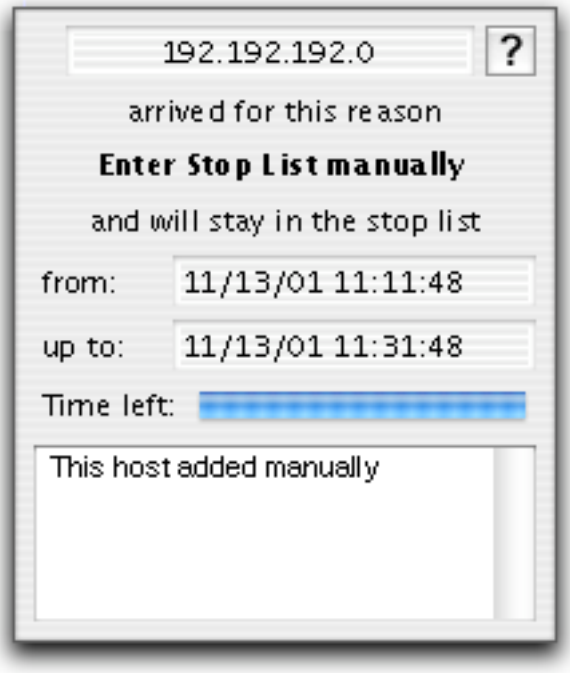
Stop List information

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.



IP address

At the top 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.

arrived for this reason … and will stay in the Stop List

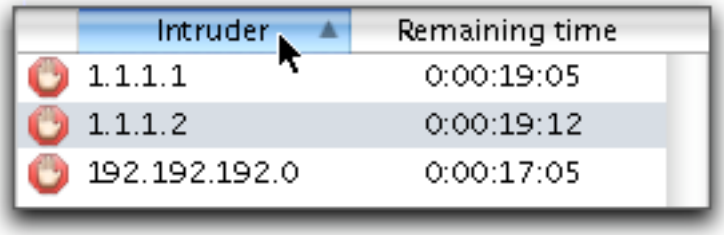
A line of text tells you how the IP address was added to the Stop List (here, it was added manually). The **from**: and **up to**: sections tell you when the address was added to the Stop List, and how long it will remain there. The progress bar shows how much of their time in the Stop List is left.

Comments

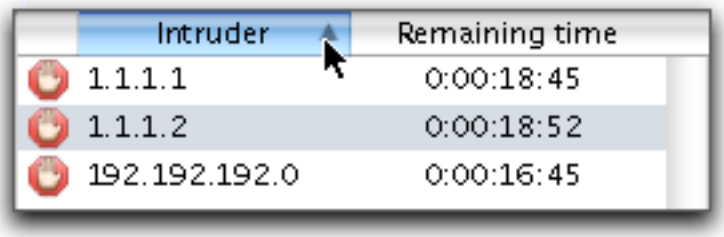
The text field below the progress bar contains any comments you have entered in the Stop List for this IP address. See below to find out how to enter or add comments to a Stop List entry.

Changing the List Display

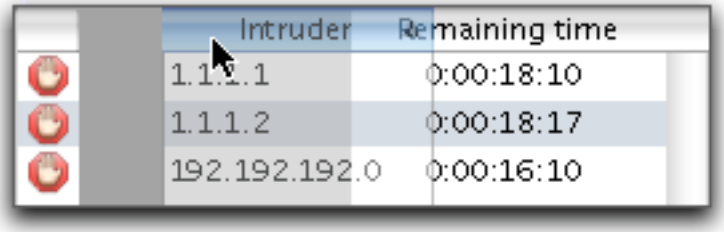
The Stop List can be sorted by any of its columns by clicking on the header just above the column.



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.



You can drag any of the columns to change their order. To do this, click one of the column headers and drag it where you want, then release your mouse button.

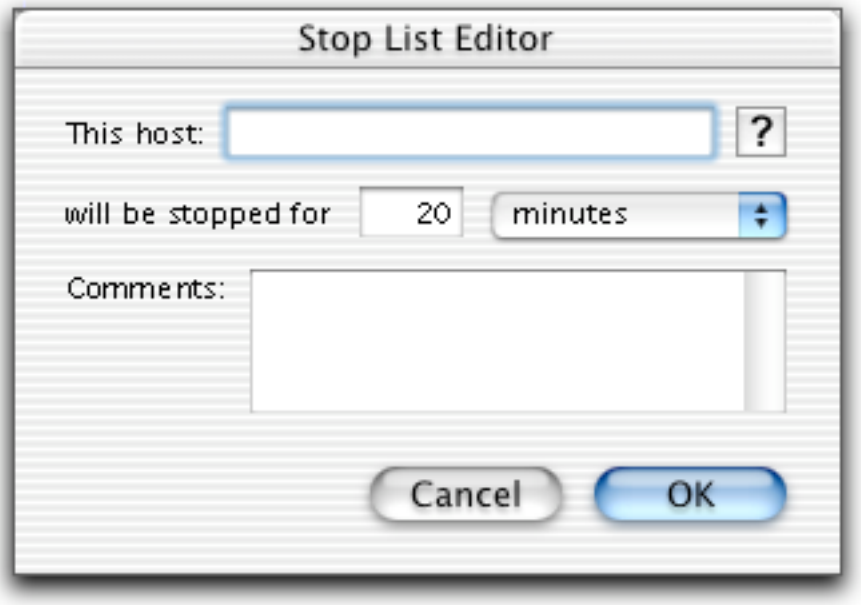


Adding addresses to the Stop List

There are three 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.

The second is by selecting an IP address in the Log window, and choosing Add to Stop List from the contextual menu. For more on this, see above, **Log Window Contextual Menu**.

You can also manually add addresses to the Stop List. To do this, click Add... The Stop List Editor will be displayed.

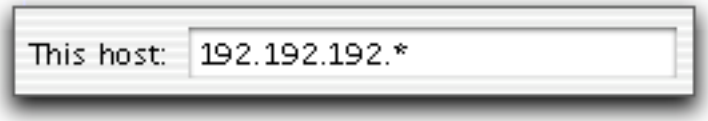


Enter a host address in the first field, and select the time this address is to remain in the Stop List by entering a number in the second field; select a time unit from the pop-up menu. If you do not know the numerical IP address of the host you wish to add, enter its name and click the **?** button. NetBarrier X 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 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

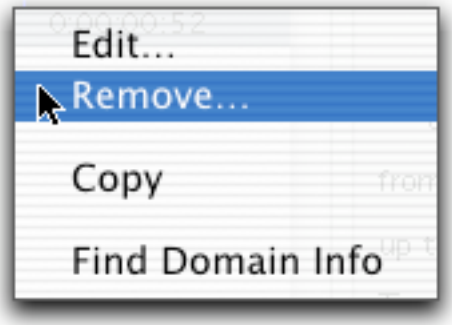
following form: 192.*.*.* or 192.192.*.* or 192.192.192.* This will block all addresses containing the numbers you have entered, whatever their endings are.



Removing addresses from the Stop List

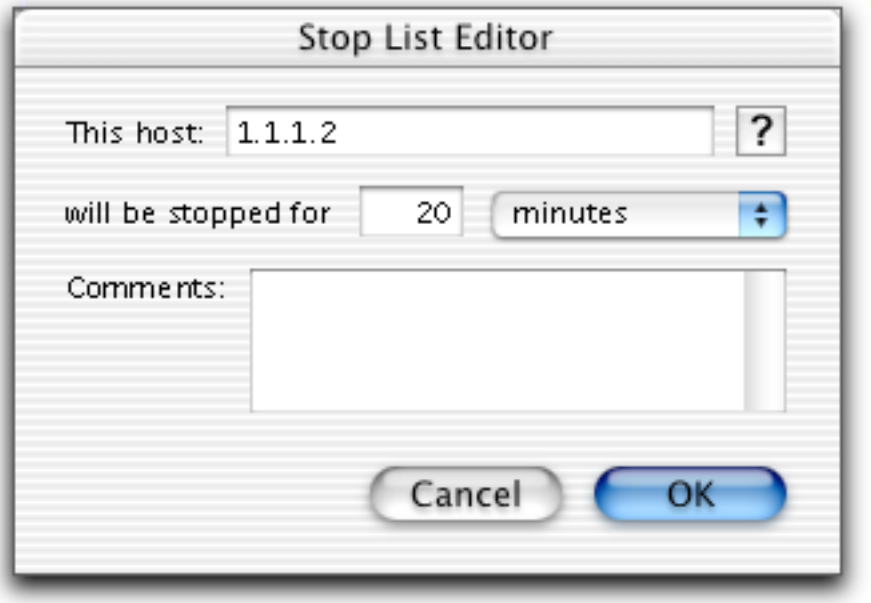
To remove an address from the Stop List, click once on the address you would like to remove, then click Remove. A dialog will ask if you really want to remove the address; click Remove. The address will be removed. If you decide you do not want to delete this address, click Cancel. You can select multiple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

You can also remove an address from the Stop List by clicking on the address while holding down the control key on your keyboard, then selecting Remove… from the contextual menu that is displayed. 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.



Editing an address in the Stop List

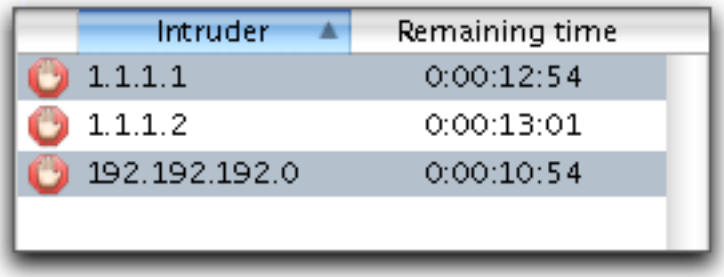
To edit an address in the Stop List, click once on the address you would like to edit, then click Edit… (You can also double-click the address, or click the address while holding down the control key on your keyboard, then select Edit…)



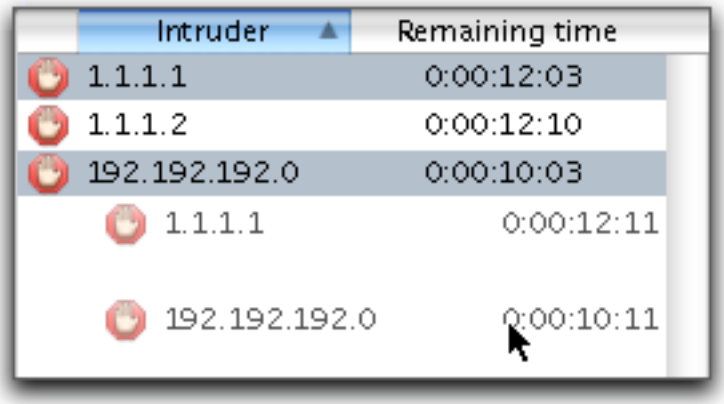
The Stop List Editor will be displayed, showing you the address, and you can change the address, add or change comments, or change the time you want it to remain on the Stop List. To confirm your changes, click OK, or to leave the address and other information as they were, click Cancel.

Copying addresses from the Stop List

You can select addresses in the Stop List and copy them, to paste them into another application. To do this, click a line of the Stop List, then copy the address. You can select multiple contiguous addresses, by shift-clicking, or non-contiguous addresses, by command-clicking, and copy them all together.

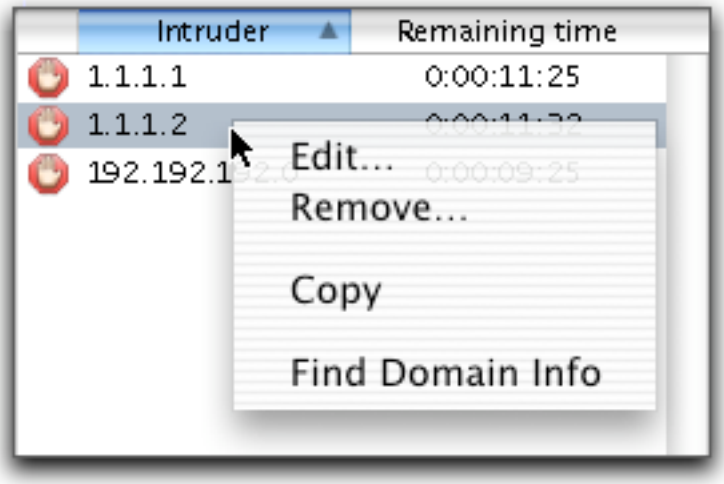


You can drag selected addresses into another application window. To do this, select one or several addresses, as above, click your cursor on one of the selected lines, and drag them into another open window.



The Stop List Contextual Menu

As you have seen above, you can click an address in the Stop List, while holding down the control key on your keyboard, and a contextual menu will be displayed. In addition to allowing you to edit and remove addresses from the Stop List, this menu contains two other functions.



Copy

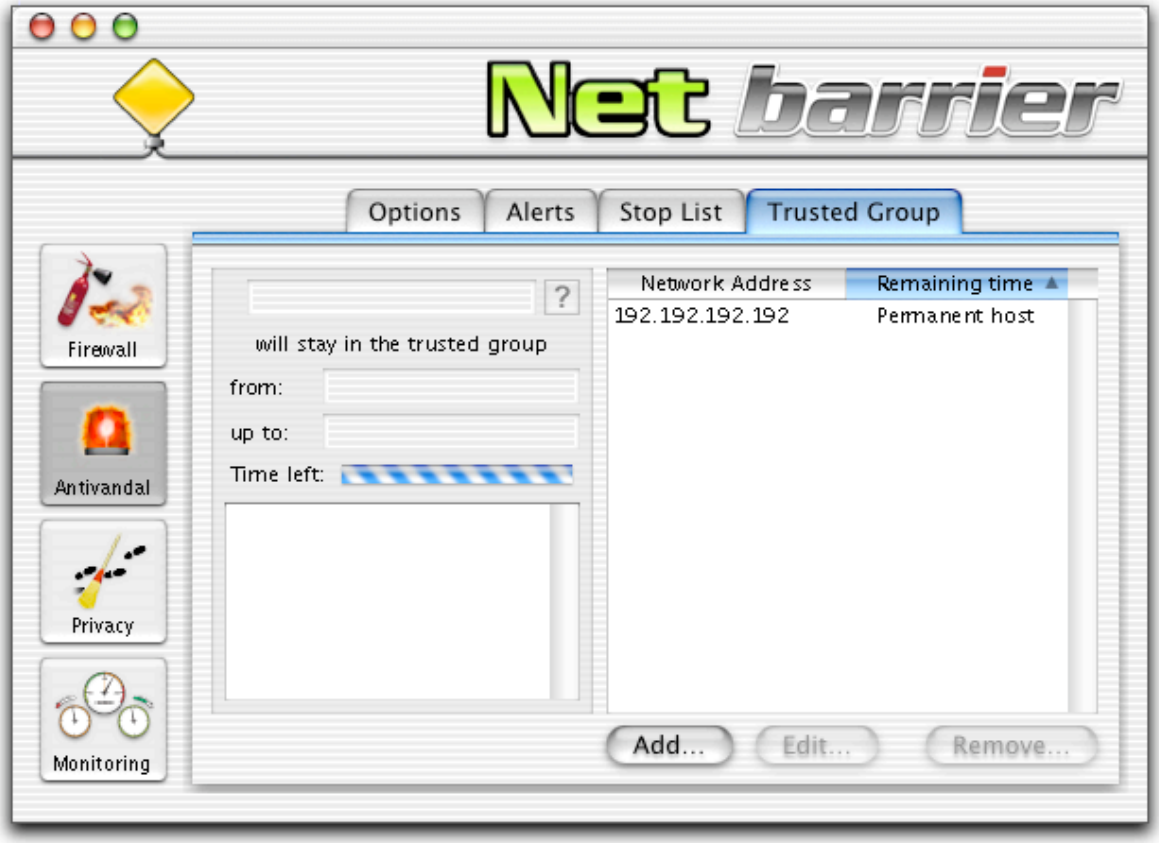
If you select Copy from the contextual menu, the address will be copied to the clipboard. You can then paste it into any application or document.

Find Domain Info

If you select Find Domain Info from the contextual menu, NetBarrier X's Whois panel will open and look up the domain name, giving you information on that domain. For more about Whois, see the **Whois** section below.

The Trusted Group

The Trusted Group feature allows you to select "friendly" computers that will not be treated as intruders if they perform certain actions, such as sending pings or other requests. It is a kind of friendly Stop List. While the Stop List protects you from foes, the Trusted Group contains your friends. You can add computers on your local network or other hosts on the Internet that you are certain to be friends. This ensures that NetBarrier X's Antivandal will not block their access nor set off alerts for any actions they carry out. They will, however, be affected by all of the active Firewall rules.



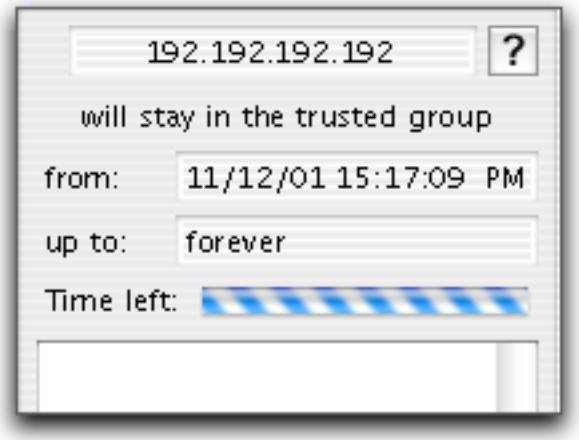
Trusted Group Information

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

Network Address
This is the IP address of the friendly computer.

Remaining time
This is the time that the friendly computer is scheduled to remain in the Trusted Group.

Other Trusted Group information
If you click once on an address in the Trusted Group, you will see some additional information on the left side of the panel.



IP address
At the top of this section is the IP address of the friendly computer. By clicking on the DNS lookup button (the **?**), you can toggle from the

numerical IP address to the actual domain name of the friendly computer, if there is one.

will stay in the trusted group

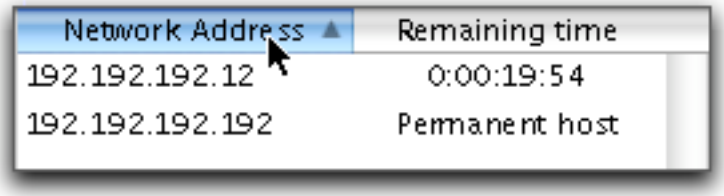
The **from**: and **up to**: sections tell you when the address was added to the Trusted Group, and how long it will remain there. The progress bar shows how much of their time in the Trusted Group is left.

Comments

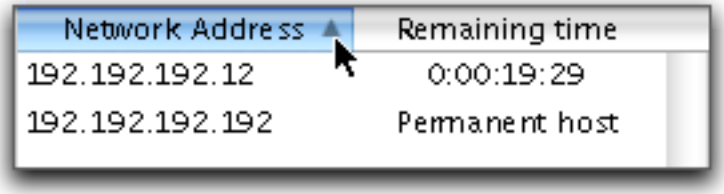
The text field below the progress bar contains any comments you have entered in the Trusted Group for this IP address. See below to find out how to enter or add comments to a Trusted Group entry.

Changing the List Display

The Trusted Group list can be sorted by any of its columns by clicking on the header just above the column.



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.

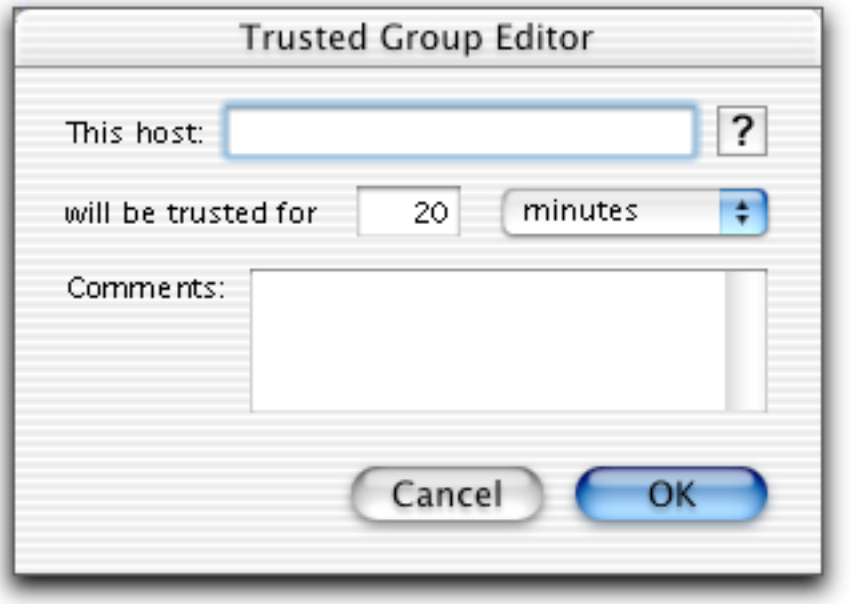


You can drag any of the columns to change their order. To do this, click one of the column headers and drag it where you want, then release your mouse button.

Adding addresses to the Trusted Group

There are two ways to add addresses to the Trusted Group. The first is by selecting an IP address in the Log window, and choosing Add to Trusted Group from the contextual menu. For more on this, see above, **Log Window Contextual Menu**.

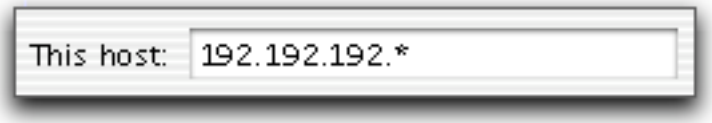
You can also manually add addresses to the Trusted Group. To do this, click Add...



The Trusted Group Editor will be displayed. Enter a host address in the first field, and select the time this address is to remain in the Trusted Group by entering a number in the second field; select a time unit from the pop-up menu. If you do not know the numerical IP address of the host you wish to add, enter its name and click the **?** button. NetBarrier X 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 Trusted Group, in the Comments field. If you decide you do not wish to add this address to the Trusted Group, click Cancel.

Using wild cards in the Trusted Group

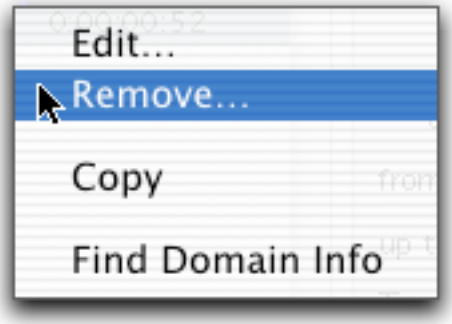
You can use wild cards to allow ranges of IP addresses in the Trusted Group. To do this, enter the first part of the IP address you wish to add to the Trusted Group, followed by asterisks, in the following form: 192.*.*.* or 192.192.*.* or 192.192.192.* This will add to the Trusted Group all addresses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



Removing addresses from the Trusted Group

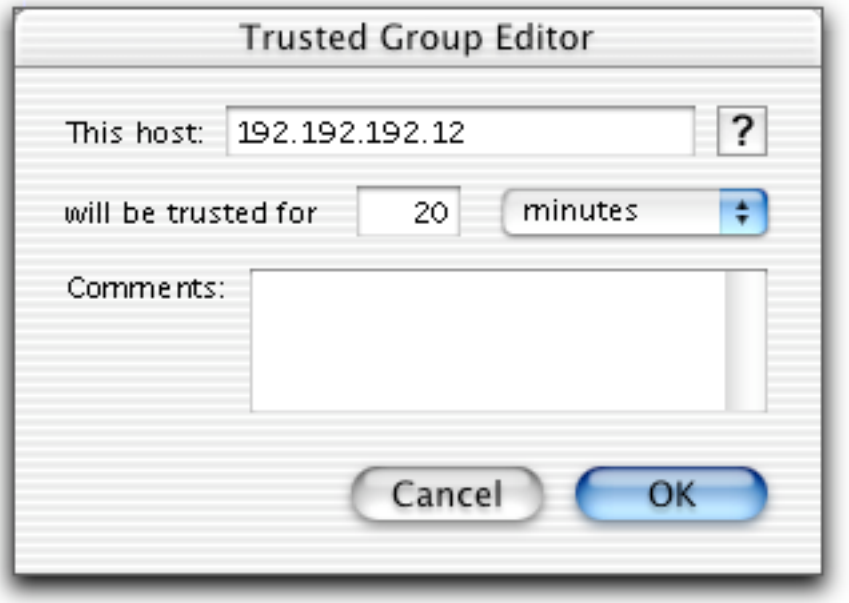
To remove an address from the Trusted Group, click once on the address you would like to remove, then click Remove. A dialog will ask if you really want to remove the address; click Remove. The address will be removed. If you decide you do not want to delete this address, click Cancel. You can select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

You can also remove an address from the Trusted Group by clicking on the address while holding down the control key on your keyboard, then selecting Remove… from the contextual menu that is displayed. A dialog will ask if you really want to remove the address; click Remove. The address will be removed. If you decide you do not want to delete this address, click Cancel.



Editing an address in the Trusted Group

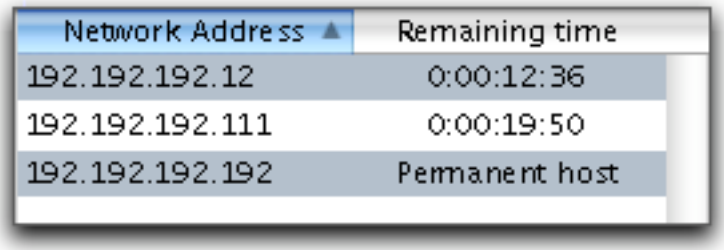
To edit an address in the Trusted Group, click once on the address you would like to edit, then click Edit… (You can also double-click the address, or click the address while holding down the control key on your keyboard, then select Edit…)



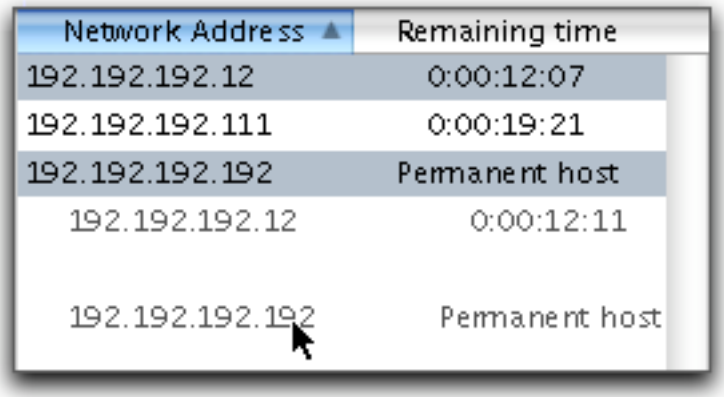
The Trusted Group Editor will be displayed, showing you the address, and you can change the address, add or change comments, or change the time you want it to remain on the Trusted Group. To confirm your changes, click OK, or to leave the address and other information as they were, click Cancel.

Copying addresses from the Trusted Group

You can select addresses in the Trusted Group and copy them, to paste them into another application. To do this, click a line of the Trusted Group, then copy the address. You can select multiple contiguous addresses, by shift-clicking, or non-contiguous addresses, by command-clicking, and copy them all together.

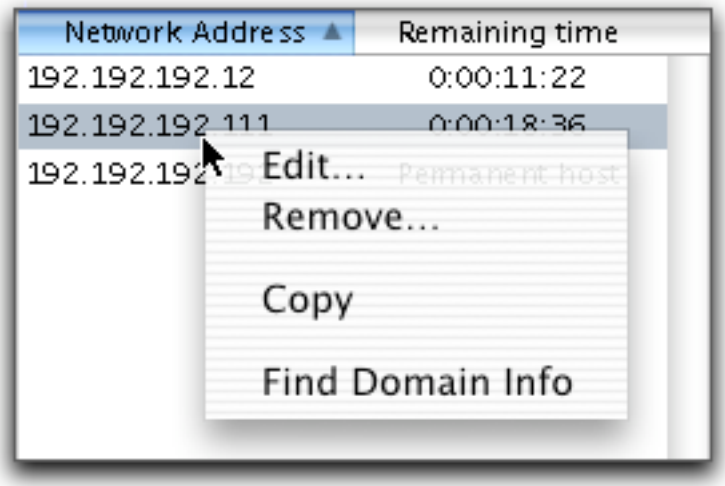


You can drag selected addresses into another application window. To do this, select one or several addresses, as above, click your cursor on one of the selected lines, and drag them into another open window.



The Trusted Group Contextual Menu

As you have seen above, you can click an address in the Trusted Group, while holding down the control key on your keyboard, and a contextual menu will be displayed. In addition to allowing you to edit and remove addresses from the Trusted Group, this menu contains two other functions.



Copy

If you select Copy from the contextual menu, the address will be copied to the clipboard. You can then paste it into any application or document.

Find Domain Info

If you select Find Domain Info from the contextual menu, NetBarrier X's Whois panel will open and look up the domain name, giving you information on that domain. For more about Whois, see the **Whois** section below.

Privacy Filters

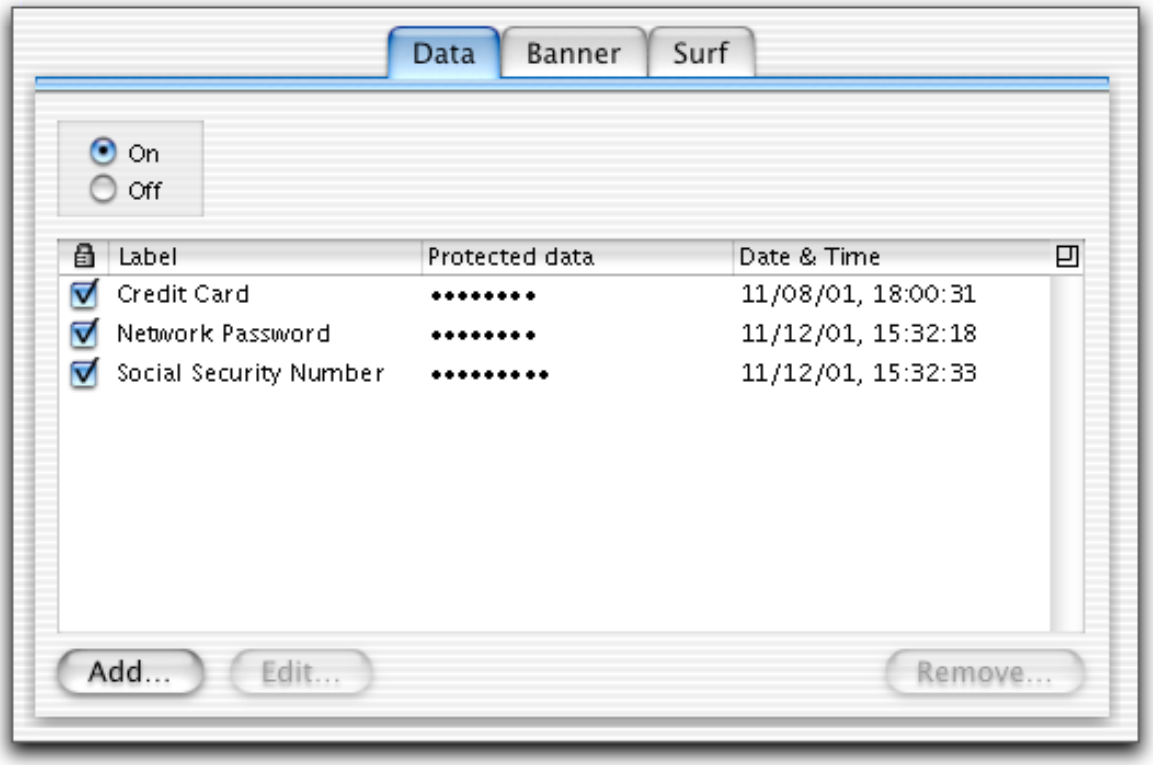
NetBarrier X's privacy filters examine both incoming and outgoing data, looking for specific types of data. There are several different filters, each of which is designed to protect your data or privacy, or help you surf the web faster.

Data Filter

The Data Filter ensures that any sensitive information you choose to protect cannot leave your computer and go onto a network. You decide what to protect - your credit card number, passwords, or key words that appear in sensitive documents - and NetBarrier X's Filter checks each outgoing packet to make sure that no

documents containing this information are 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.

Remember that, 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.



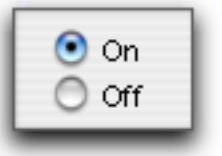
How the Filter works

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 network or the Internet, they are all examined. If any of the Filter's protected data is found, the packet is blocked.

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 X 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.

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 check box. 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 check box.



What to protect

The Filter is designed to protect sensitive information. You may want to protect different types of information, depending on your needs and the type of data on your computer. 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

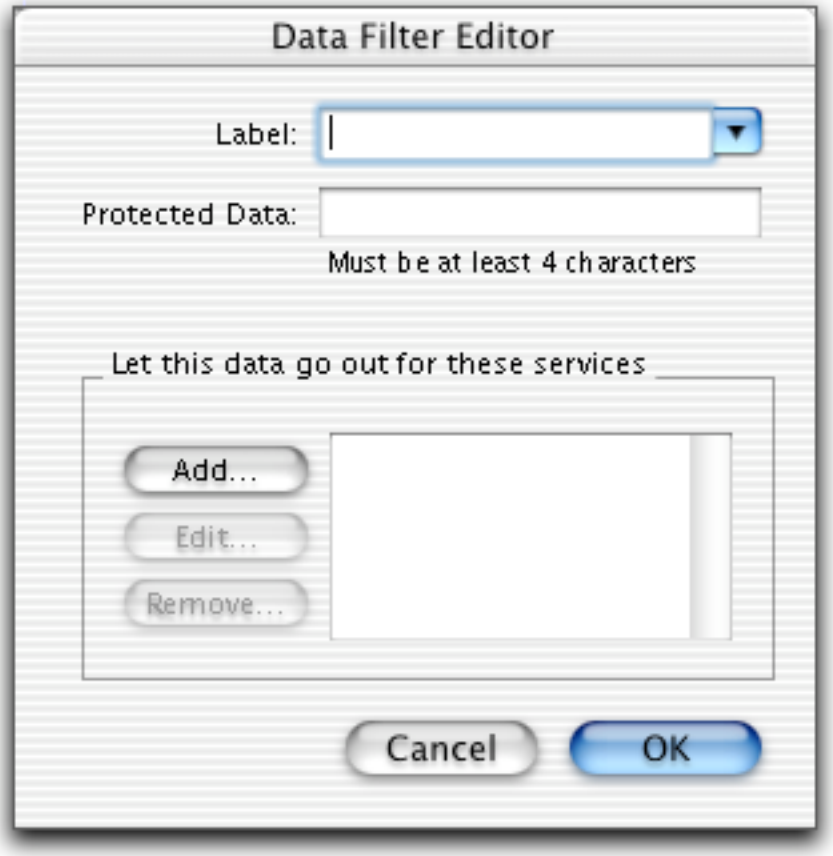
If you use the Internet or any other network, you probably have some passwords. The more sites you use, the more passwords you have. Some users even have files on their computers containing lists of their passwords. Add your passwords to the Filter, and none of them will be able to leave your computer and go onto a network. Note: if you store your passwords in the Mac OS X Keychain, they are encrypted, and you will not need to protect them in the Filter.

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.

Adding Protected data to the Filter

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

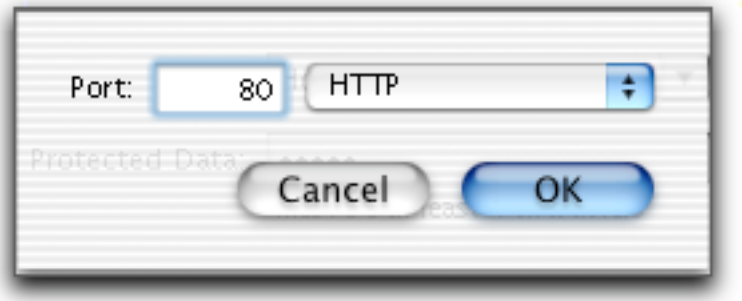


Enter a name for your Protected data in the Label field. You can select some of the most common names from the popup menu next to this field. Then enter the actual text you wish to protect in the second text field. This text will appear hidden by bullets.

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. Also, this data is case sensitive. If you need to protect a key word, such as a project name, you must enter it in all possible cases: i.e., Marketing Study, marketing study, MARKETING STUDY.

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.

Activating or Deactivating Protected Data Items

Each item of protected data appears on a line in the Data window. A check box at the left of each line allows you to activate or deactivate the filter for each data item. When you add a new data item, the box is checked, indicating that the filter is active for this item. If you wish to send any protected data over the Internet or a local network, you must uncheck the check box for the item in question.

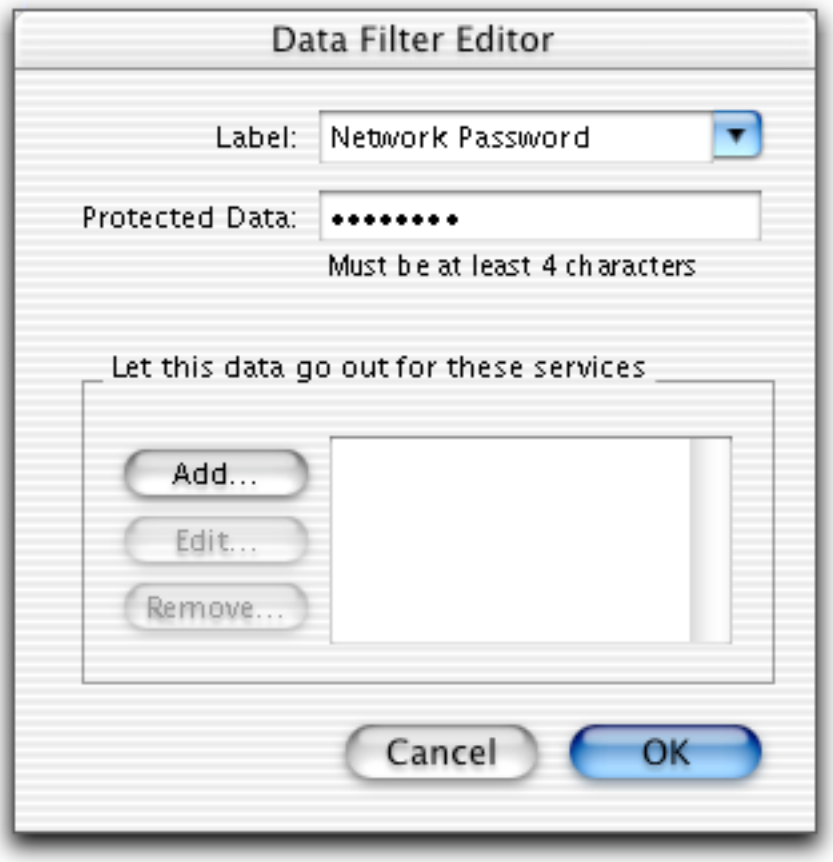
Deleting Protected data from the Filter

To delete Protected data from the filter, click once on the Protected data item 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

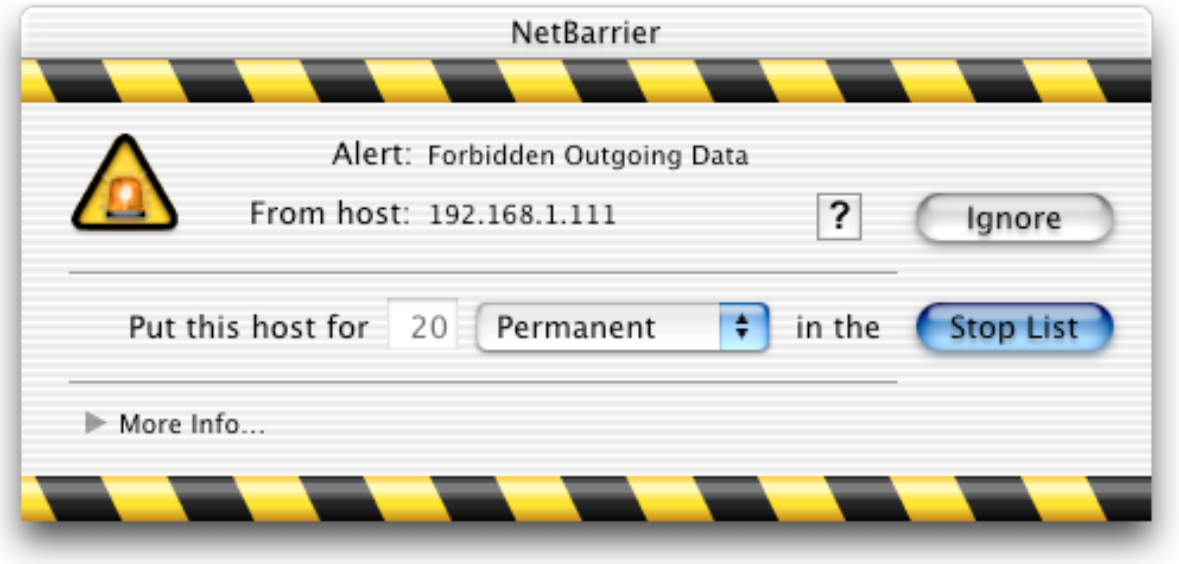
You can edit Protected data in the Filter, either to make changes, or to change the services it is active under.

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 the Protected data.) The Data Filter Editor 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

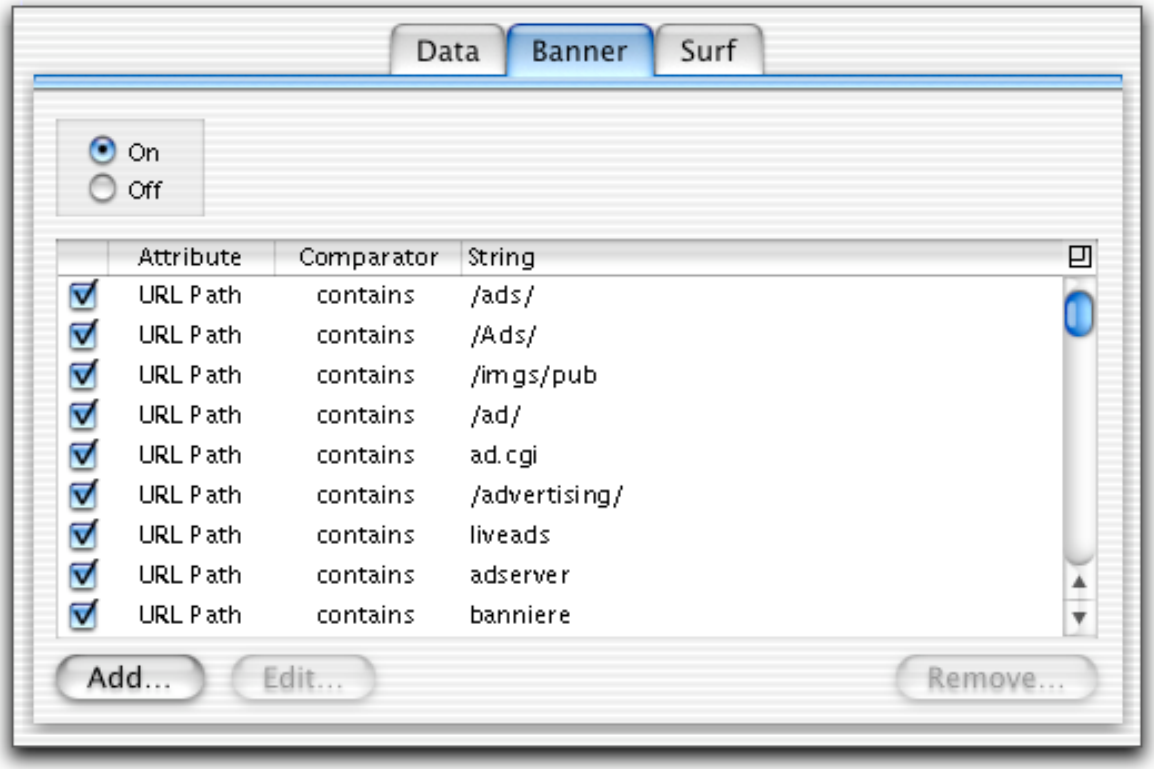
If the Filter detects that Protected data is leaving your computer, an alert will be displayed.



This alert is similar to other NetBarrier X alerts. You have the possibility of ignoring the alert, or putting the host on the Stop List. If you click Ignore, NetBarrier X 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.

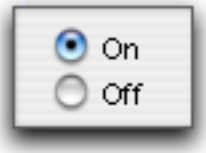
Banner Filter

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



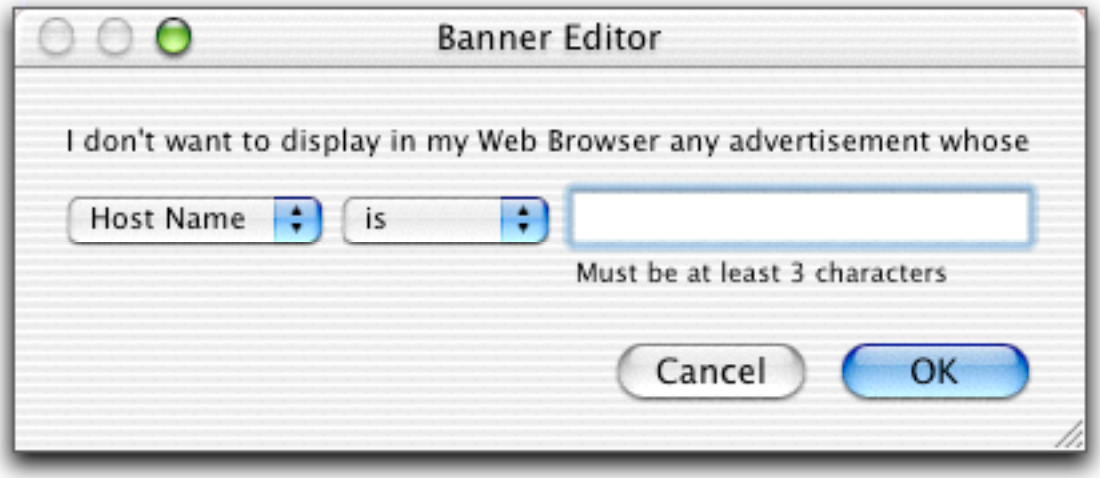
Turning the Filter on

First, for the Filter to block ad banners, you need to turn it on. To do this, click the On check box. You can turn it off at any time, if you temporarily want to allow all hosts to be accepted by your computer, by clicking the Off check box.



Adding Rules to the Banner Filter

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

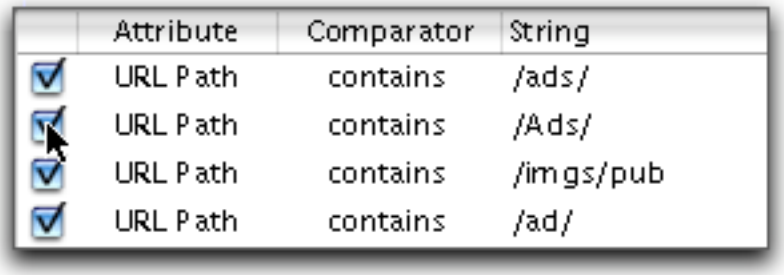
select from the second popup menu **is** or **contains**. For example, if you want to block ad banners from the host doubleclick.net, select **Host Name contains**, and enter **doubleclick.net** in the text field. If you wish to validate this ad banner filter rule, click OK; if not, click Cancel.

You can easily add new hosts to NetBarrier X's list of banner filters by dragging a graphic from a web page into the Banner filter window. NetBarrier X will automatically add the exact file path of the graphic - you should edit it, retaining merely the beginning section of the text, since the end is often specific to the individual ad.

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

Activating or Deactivating Banner Rules

Each banner rule appears on a line in the Banner window. A check box at the left of each line allows you to activate or deactivate the filter for each banner rule. When you add a new banner rule, the box is checked, indicating that the filter is active for this rule. If you wish to stop blocking certain banners, you must uncheck the check boxes for the banners in question.



Note: when using the banner filter, you may find that you cannot access some web pages correctly. If this is the case, try turning off the Banner filter; their URLs may contain texts that are in one of the banner rules.

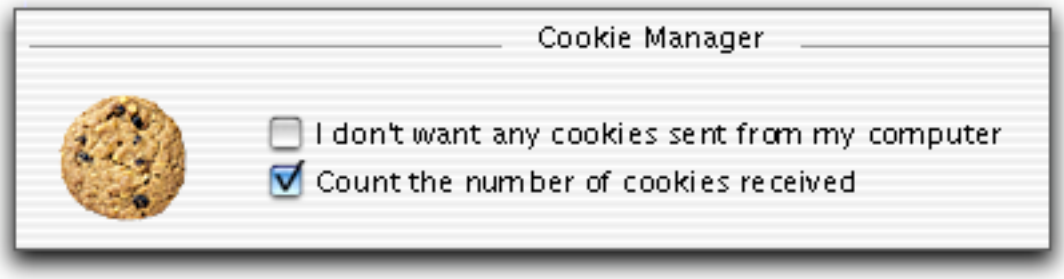
Surf Filter

NetBarrier X 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 Manager

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 X 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** check box. If web sites send cookies, 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 X can also count the number of cookies sent to your computer, if you check the **Count the number of cookies received** check box.

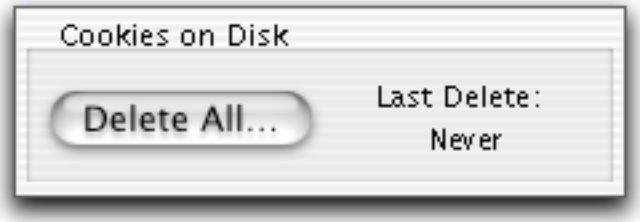
Cookie Counter

The Cookie Counter section records the number of cookies received by all users 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. This will reset the cookie counter for *all* users on your computer.

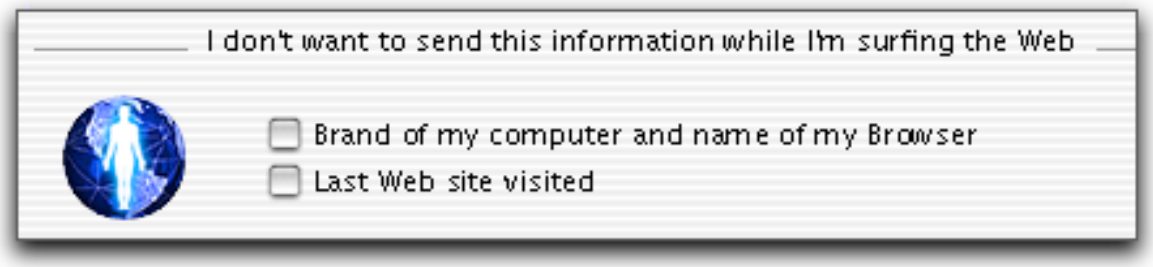
Cookies on Disk

You can also erase all cookies for the *current user* 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 X can "spoof" some information concerning your computer, that is, send false information.



NetBarrier X 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 X to do this, check the **Brand of my computer and name of my Browser** check box.

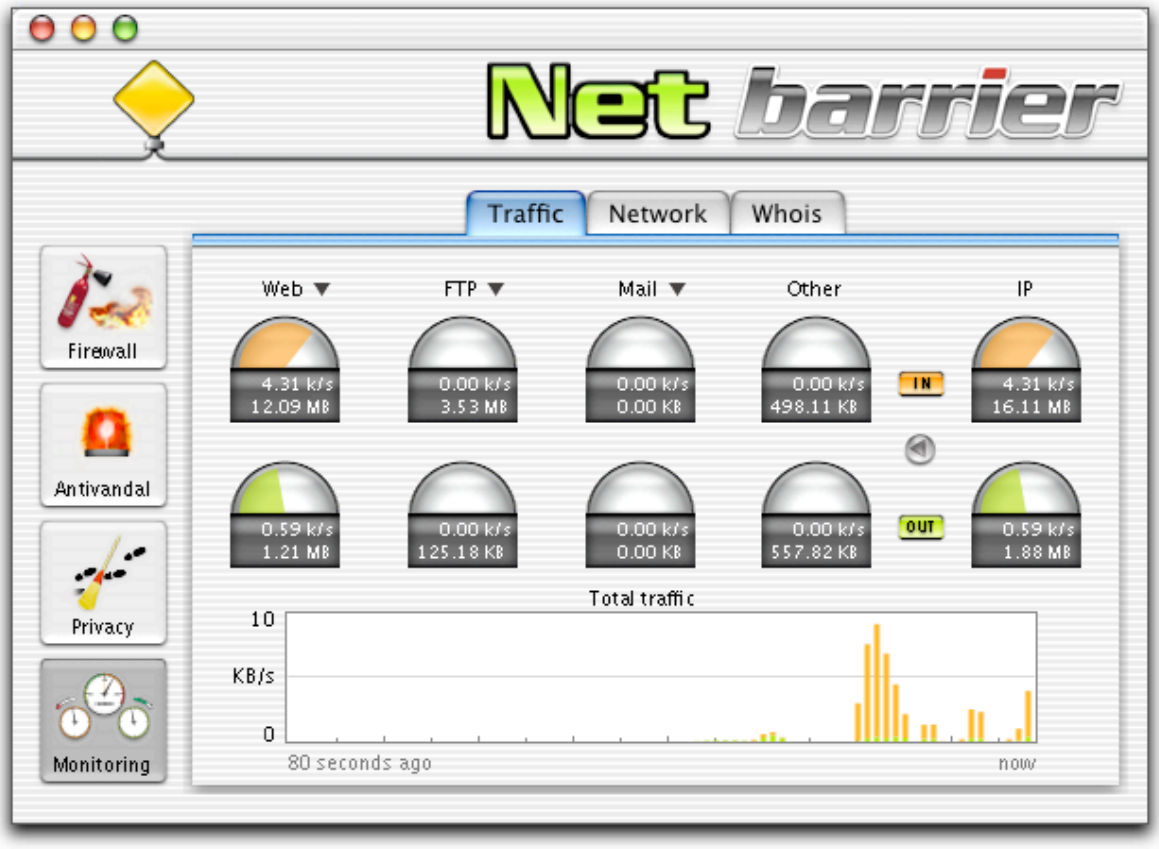
Some sites also request the last site you visited. Again, this can be useful (some sites want to know where their users have come from), but unscrupulous sites might use this to follow your browsing habits. By checking the **Last Web site visited** check box, NetBarrier X will prevent a reply from being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

Monitoring

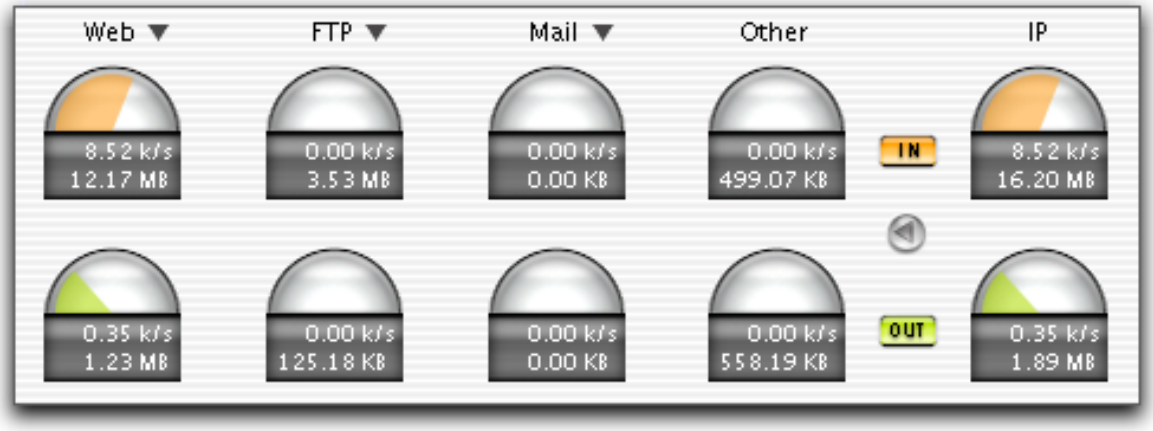
NetBarrier X's Monitoring panel gives you information on your computer's network activity.

Traffic

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



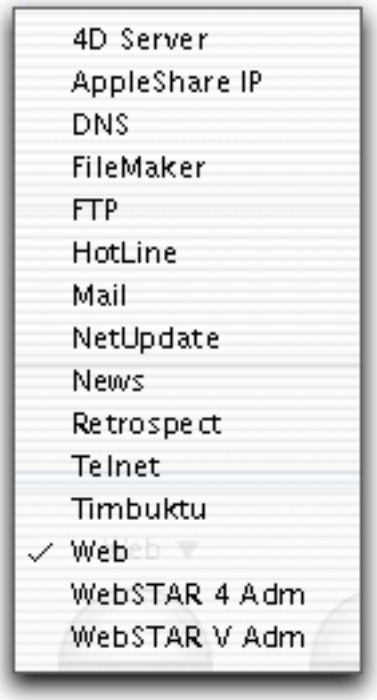
There are two rows of gauges - the IN gauges show the amount of data coming into your computer, and the OUT gauges show the amount of data leaving your computer. The top number is the current throughput per second, and the bottom is the total amount.



Selecting Activity Data Types

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

A popup menu will be displayed showing several choices.



The following types of data can be recorded:

4D Server:	the amount of 4D Server data.
AppleShare IP:	the amount of AppleShare IP data.
DNS:	the amount of DNS 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.

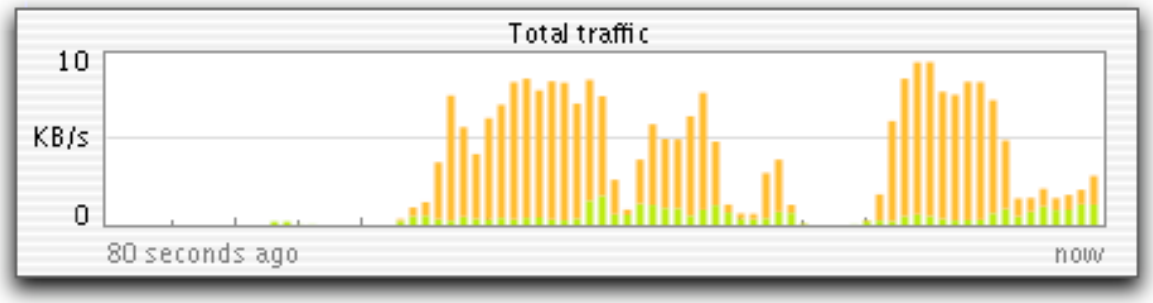
WebSTAR 4 Adm: WebSTAR administration data.
WebSTAR V Adm: WebSTAR administration data.

The last two 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 three gauges.

Total Traffic graph

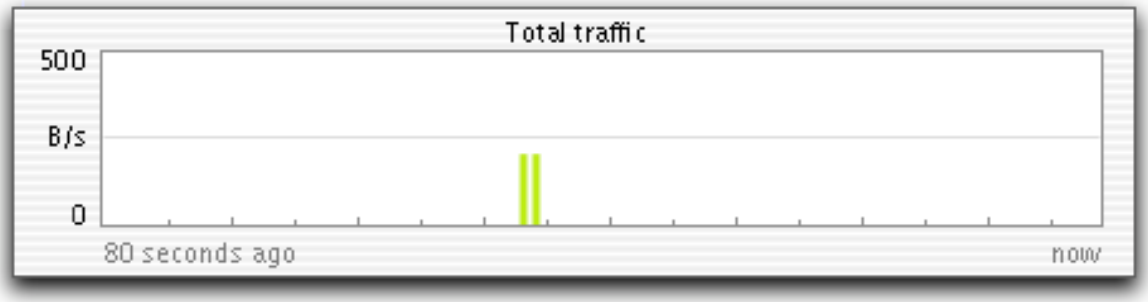
A bar graph showing total traffic is available in this window. When no network activity occurs, this graph will be empty, but when there is network activity, either over a local network or the Internet, this graph will show the total activity.



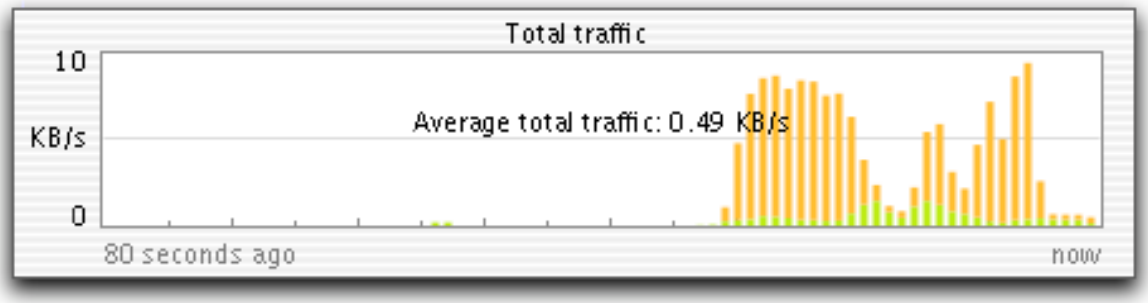
The orange parts of the bars represent incoming traffic, and the green represent outgoing traffic.

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 a local network; the maximum traffic here does not exceed 250 bytes per second.

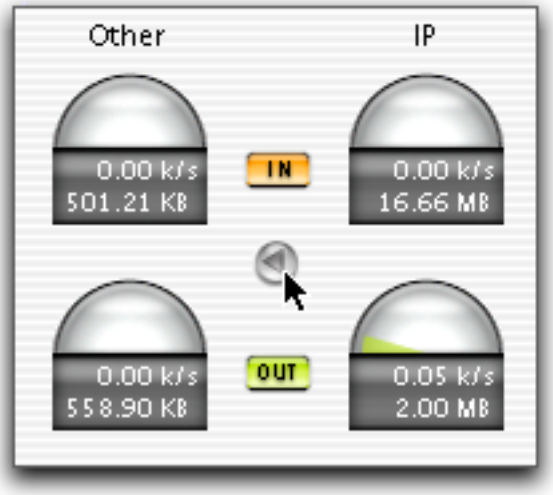


If you place your cursor over this graph, a text will be displayed showing the actual data throughput, which is updated every second.

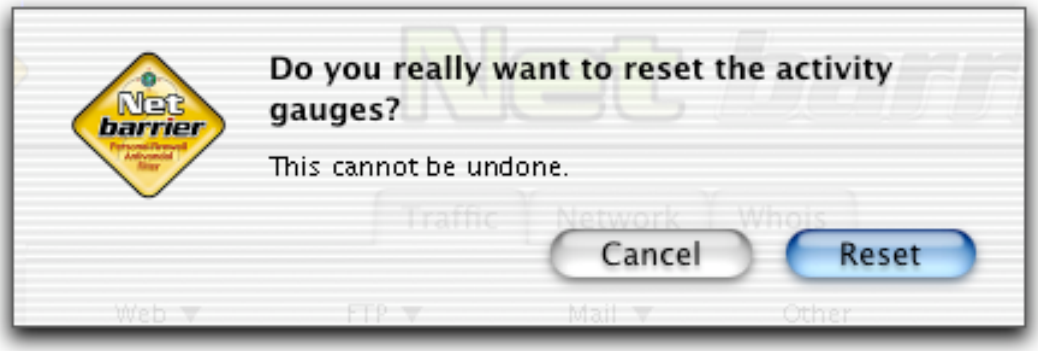


Resetting the Activity Gauges

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



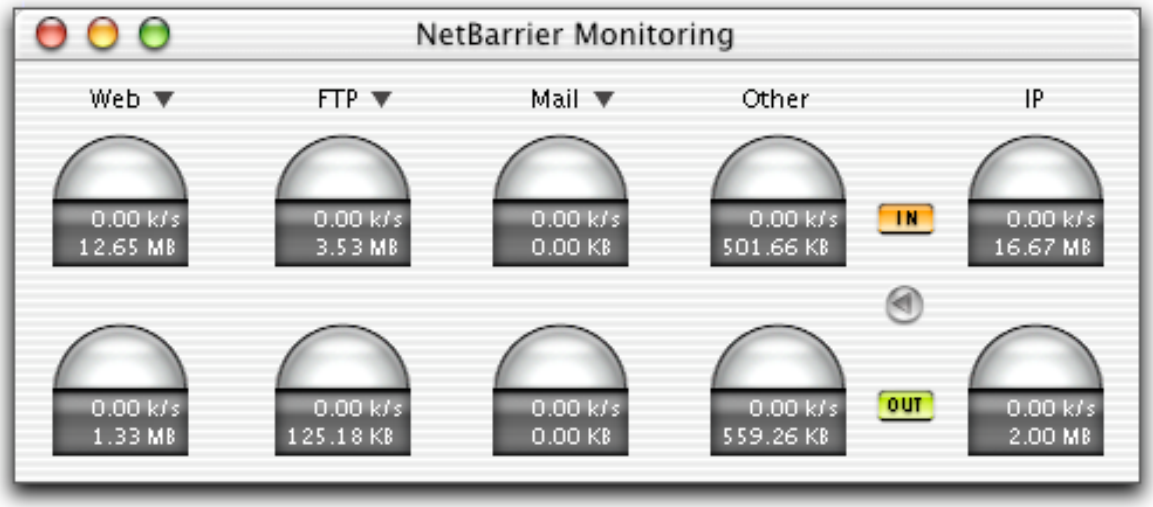
When you reset the activity gauges, an alert will be displayed asking you to confirm clearing the gauges. This ensures that you do not accidentally reset the activity gauges. If you wish to reset the activity gauges, click Reset. If not, click Cancel.



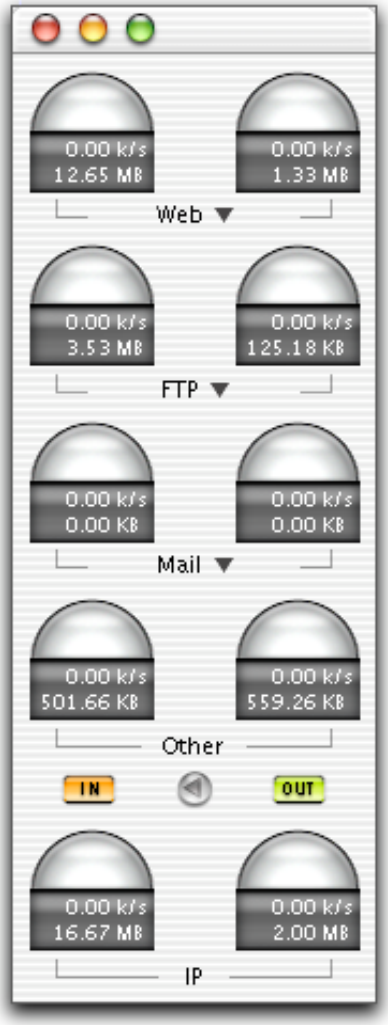
Viewing the gauges as a palette

If you click the window's resize button

the NetBarrier X window will collapse and the activity gauges will be displayed as a horizontal palette.

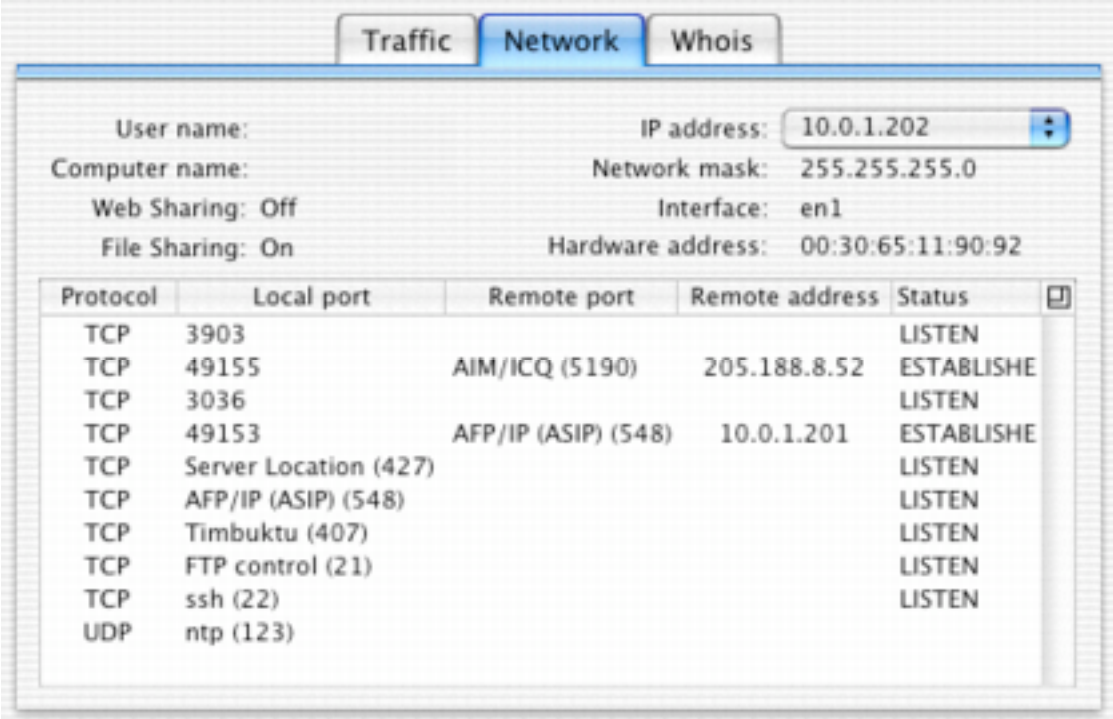


If you click the resize button while holding down the shift key, the palette will be displayed vertically. This can be useful if you want to keep an eye on your network activity, and wish to leave these gauges visible. To return to the main NetBarrier X window, click the resize button on the palette.



Network

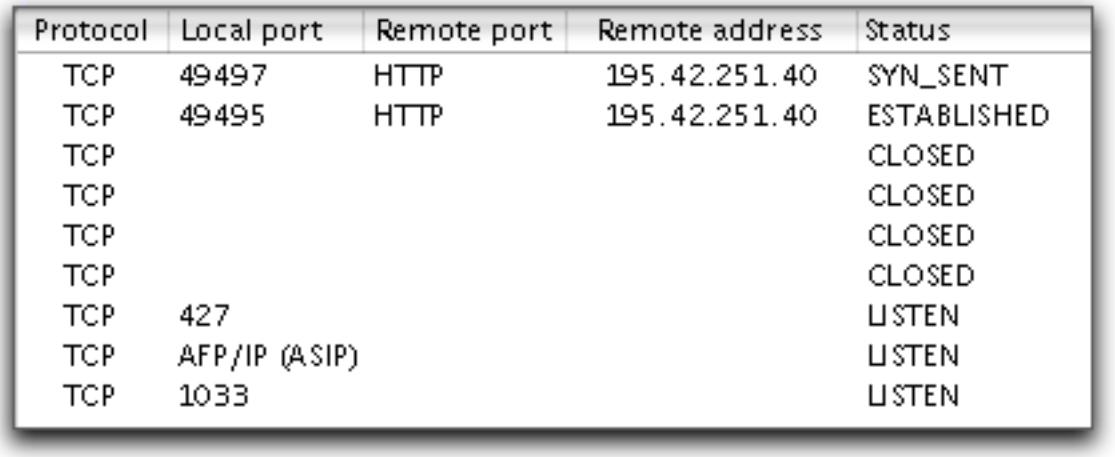
This panel gives some useful information about your computer.



It shows the user name, the name of the computer, its IP address and other network information. A popup menu shows you all of the IP addresses that are active on your computer - if you have, say, several network adapters with different addresses, or are running several servers. It also tells if Web Sharing and File Sharing are running. In addition, it gives you real-time information on your network activity.

Services

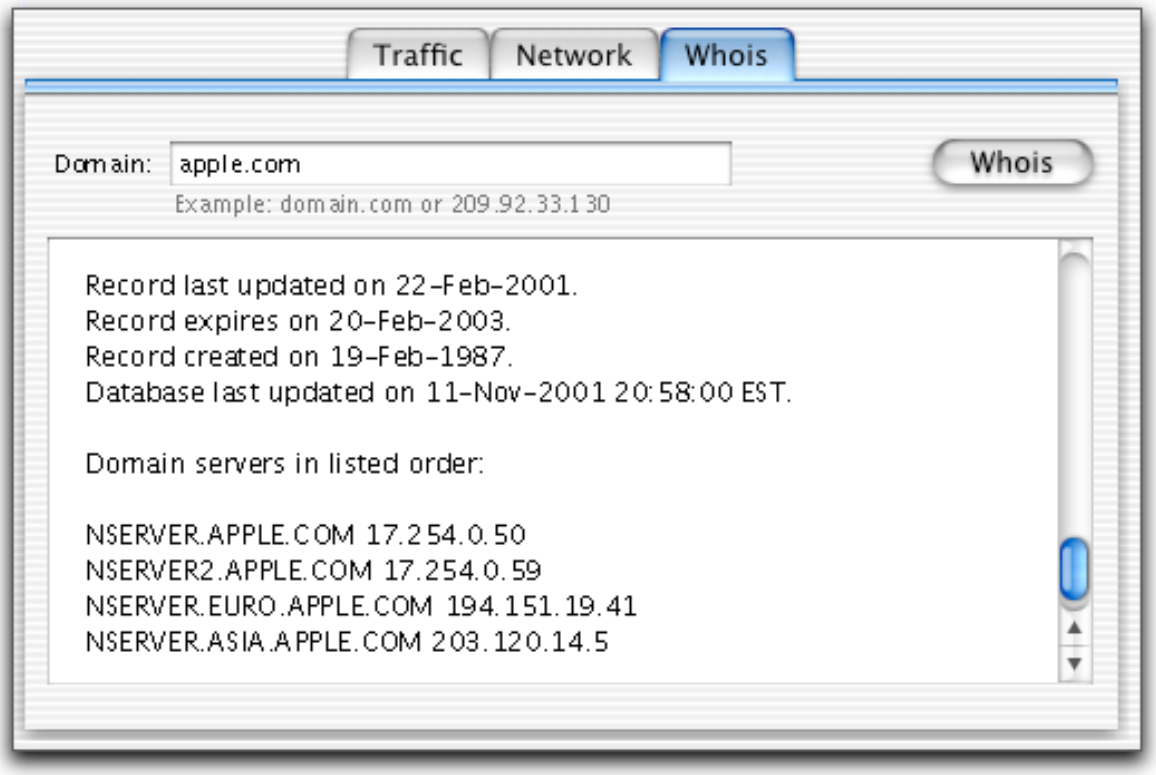
This section lists any services currently running on your computer that are accessible to other users via the Internet Protocol, such as a web server, mail server, etc. For each port being used, the following information is shown: the protocol (TCP or UDP), the local port number, the remote port, according 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	Status
TCP	49497	HTTP	195.42.251.40	SYN_SENT
TCP	49495	HTTP	195.42.251.40	ESTABLISHED
TCP				CLOSED
TCP				CLOSED
TCP				CLOSED
TCP				CLOSED
TCP	427			LISTEN
TCP	AFP/IP (ASIP)			LISTEN
TCP	1033			LISTEN

Whois

NetBarrier X allows you to look up domain names and Internet IP addresses using its built-in Whois tool. To do this, enter a domain name or IP address in the Domain field, then click the Whois button. The text field below will give you information about the domain.



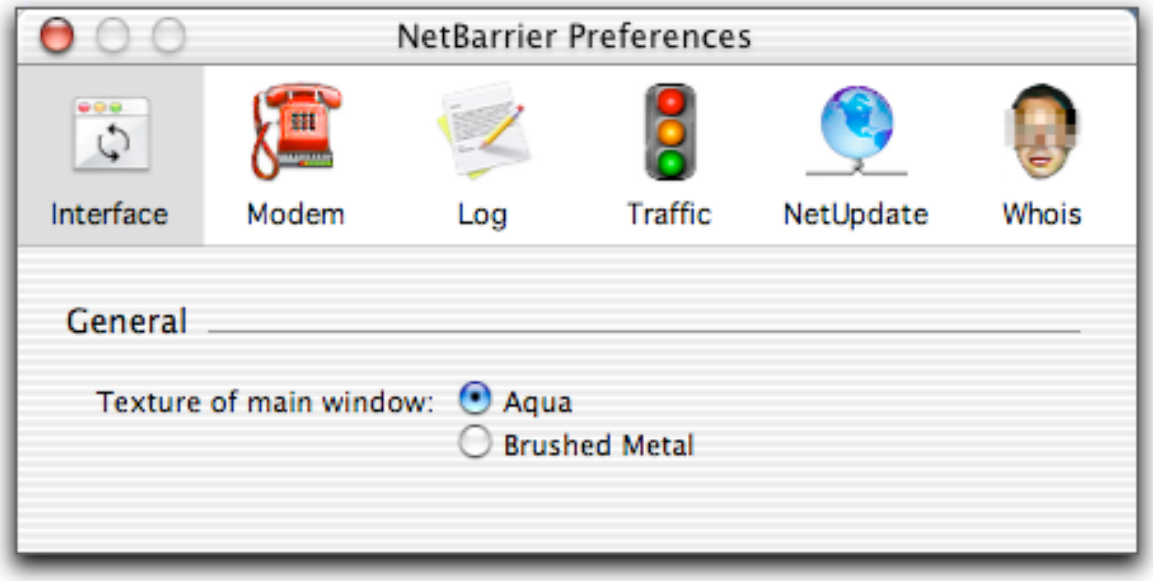
NetBarrier X has four default Whois servers, but you can add others. To find out how to add Whois servers, see chapter 6, **Preferences and Configurations**.

6 - Preferences and Configurations

NetBarrier X Preferences

Preferences

Preferences for several of NetBarrier X's functions are available from the NetBarrier Preferences screen. To view this screen, select Preferences from the NetBarrier X menu.



Interface

NetBarrier X lets you choose from two interfaces: the standard Aqua interface, or a Brushed Metal Interface. By default, the Aqua interface is used. If you wish to use the Brushed Metal interface, check the Brushed Metal radio button.

The Brushed Metal interface looks like this:

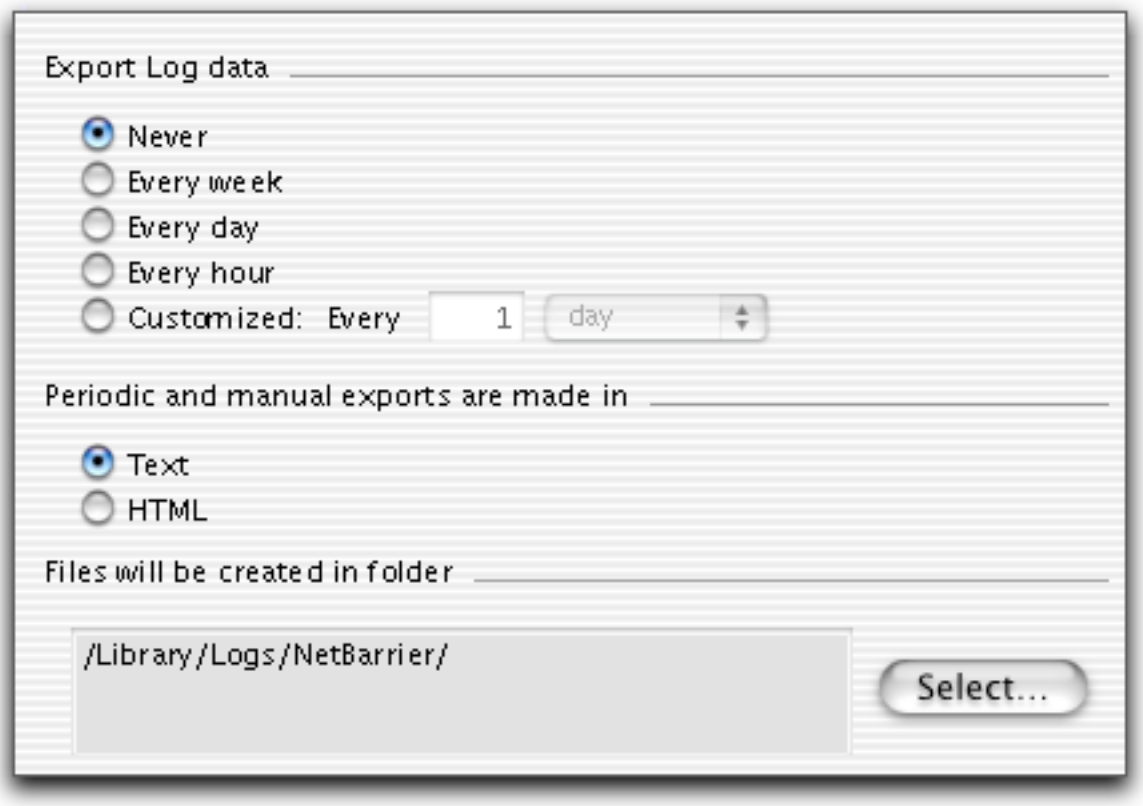
Modem

You can provide total security for your modem with this option. To do this, click the Modem button on the Preferences screen. It may prevent your modem from answering any calls. To secure your modem, click the Secure now button. To reset your modem, if you have secured it, click the Reset button.

NetBarrier X will secure your modem, blocking incoming calls, so it will be fully protected.

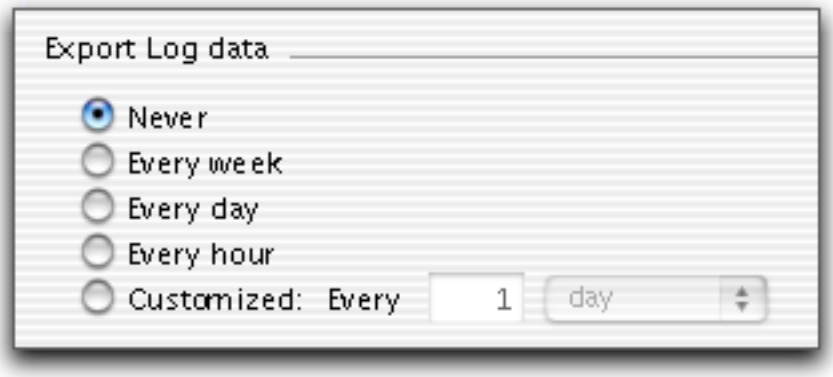
Log Export Preferences

You can set NetBarrier X to export the Log at regular intervals. To do this, click the Log button on the Preferences screen.



Export Log Data

If you wish to have your log exported at regular intervals, you can select among 5 options. By default, this is set to Never.



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.

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.

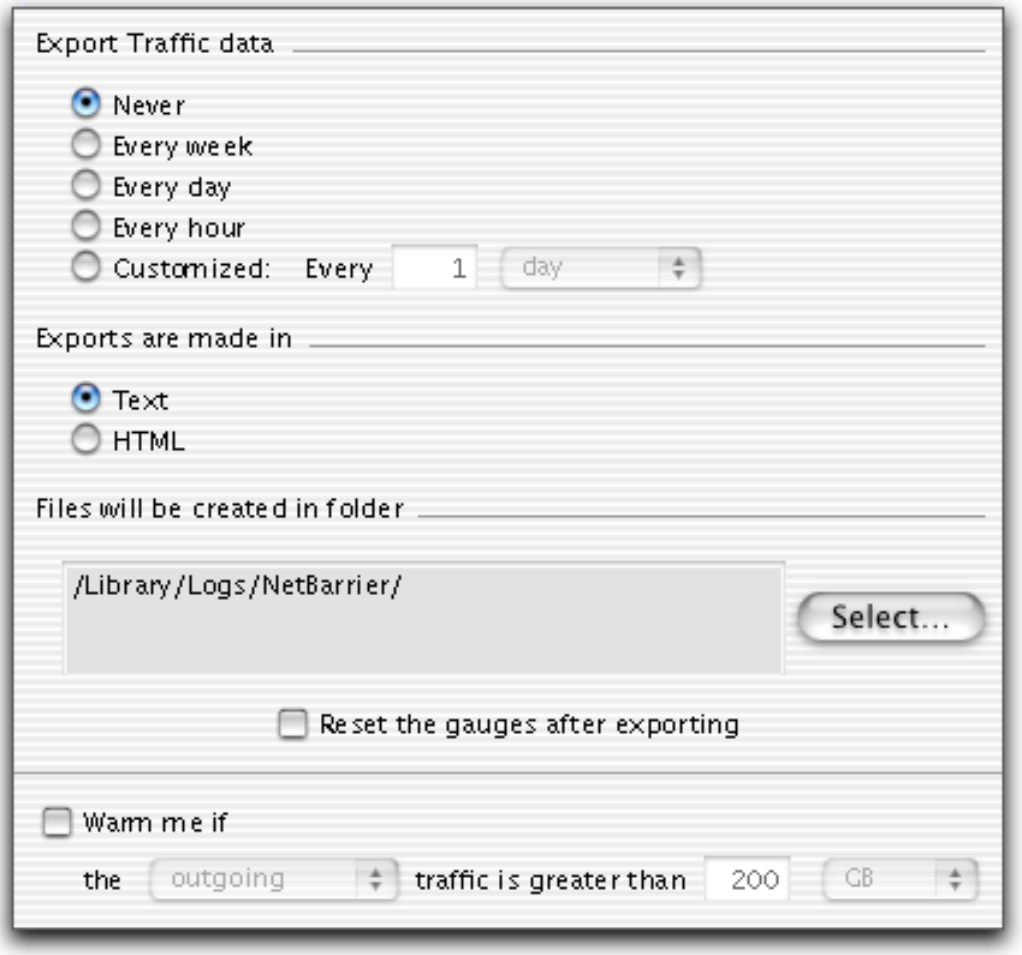
Log Export Location

You can select the folder where log export files will be saved. By default, they will be saved in the /Library/Logs/NetBarrier 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 Web Sharing, you can export the log into a shared folder, providing access to this file from a remote computer.

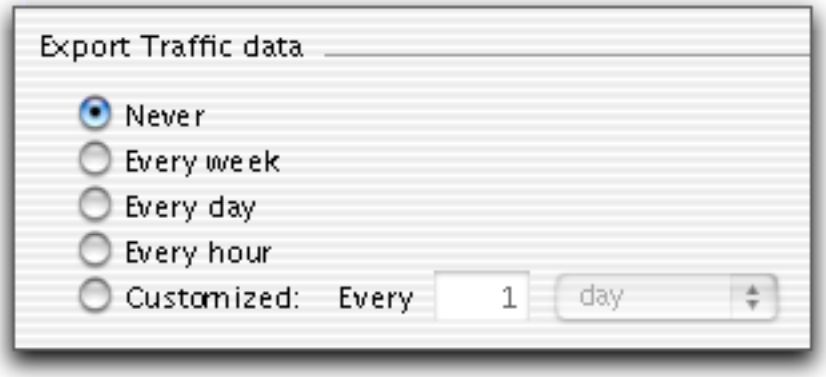
Traffic Export Preferences

You can set NetBarrier X to export traffic data at regular intervals. To do this, click the Traffic button on the Preferences screen. This screen also gives you several options for managing traffic data.



Export Traffic Data

If you wish to have your traffic data exported at regular intervals, you can select among 5 options. By default, this is set to Never.



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.

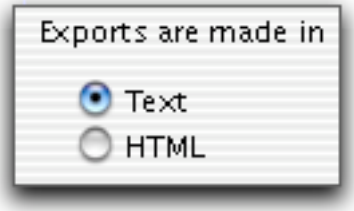
Every day
The traffic data will be exported once a day, at 00h00. If the computer is not on at this time, it will be exported at the next restart.

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.

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.



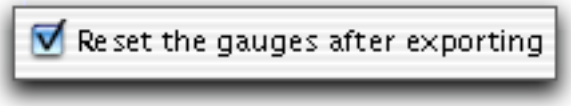
Traffic Data Export Location

You can select the folder where traffic export files will be saved. By default, they will be saved in the /Library/Logs/NetBarrier 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 Web Sharing, you can export the traffic data into a shared folder, providing access to this file from a remote computer.

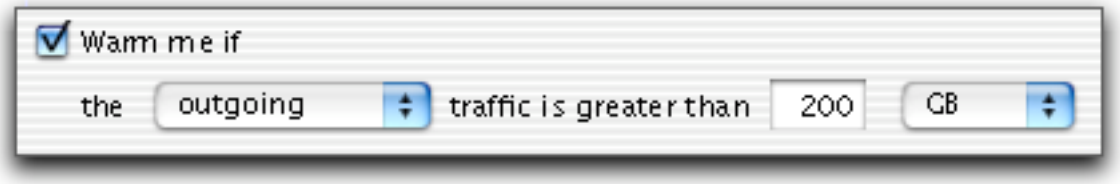
Resetting the Gauges after Export

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



IP Traffic Threshold Warning

NetBarrier X 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 X 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.

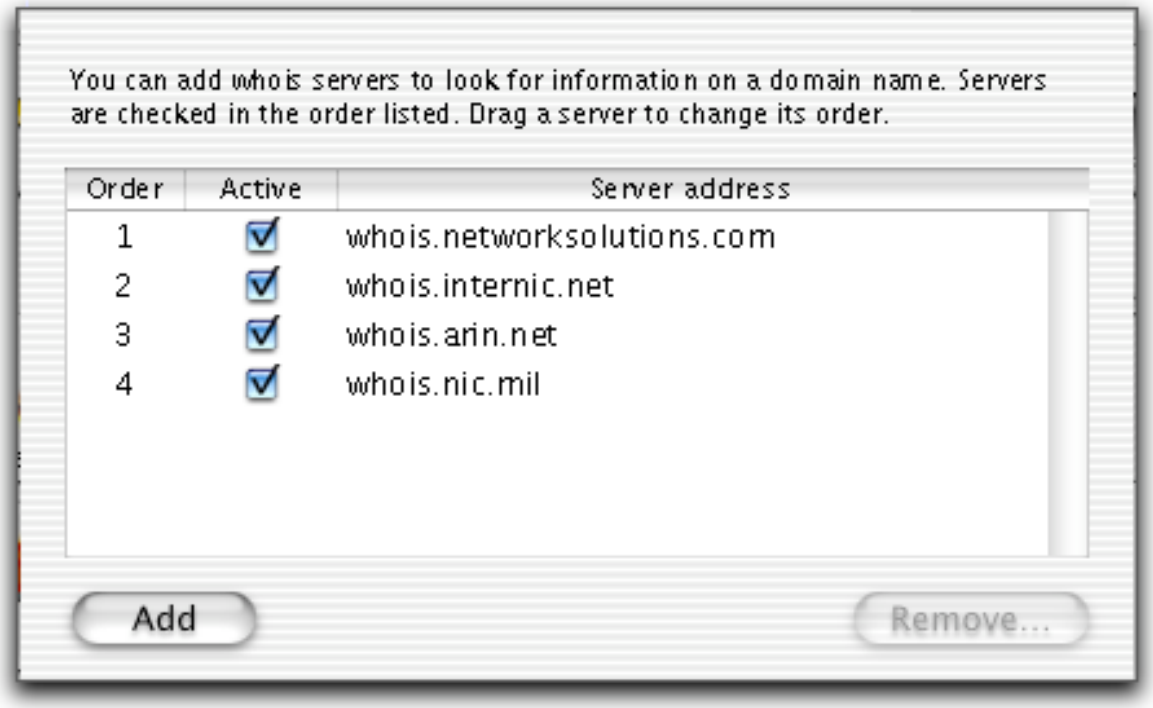
NetUpdate

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

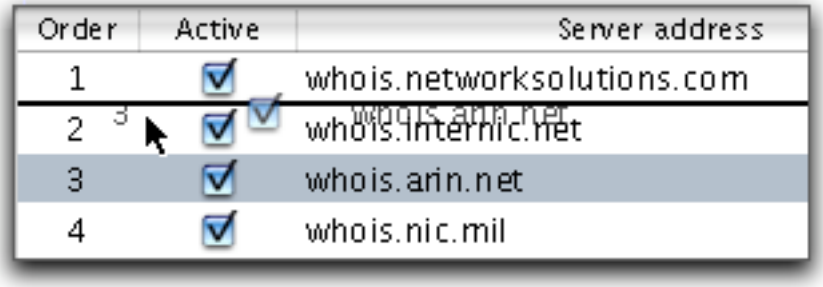
For more on using NetUpdate, see the NetUpdate User's Manual.

Whois

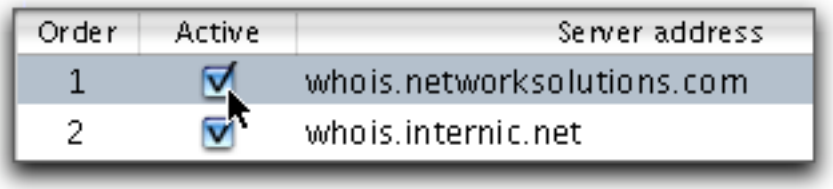
NetBarrier X's Whois function allows you to search for information on domain names and IP addresses. Four Whois servers are preset in this pane, and they are queried in the order shown in this panel.



If you wish to change their order, you can do so by selecting one of the servers and dragging it to a new location.



You can activate or deactivate the Whois servers in this panel. To deactivate a server, uncheck its check box. To activate a deactivated server, check its check box.

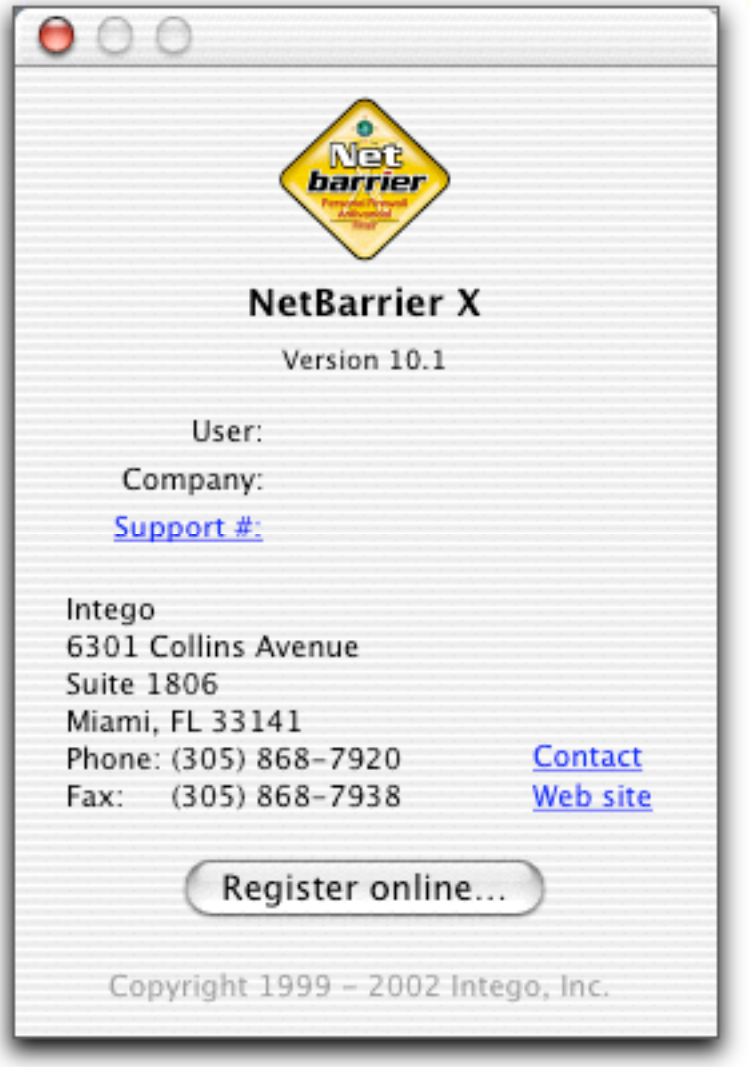


You can also add new Whois servers. To do this, click Add. A new line will be added to the list, with the server address highlighted. Type in the name of the new Whois server you wish to add.

To remove a Whois server, select it by clicking it, and click Remove… A dialogue box will ask you to confirm this removal or cancel it.

About NetBarrier X

If you select About NetBarrier… from the NetBarrier menu, a window will be displayed showing some information about NetBarrier X, 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.



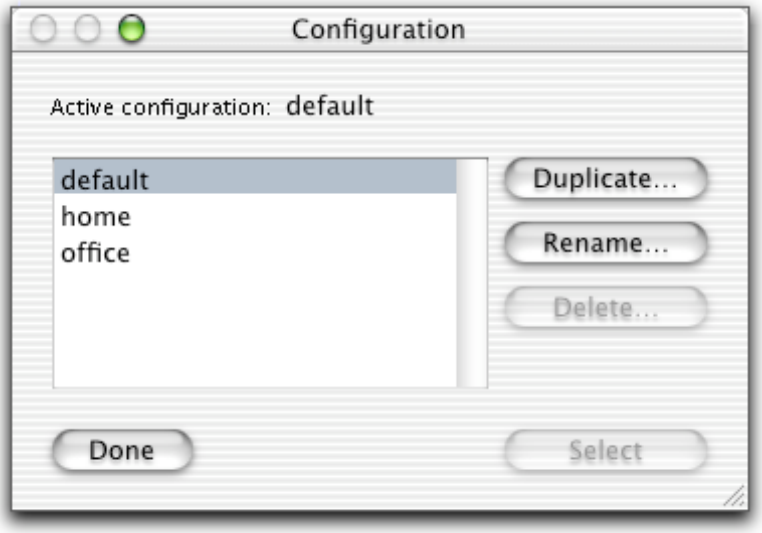
If you haven't yet registered online, you can do so quickly and easily by clicking the Register online... button. This will take you to the registration page on the Intego web site.

Configuration Sets

NetBarrier X gives you the possibility of saving as many configuration sets as you want. Each configuration set contains all of the settings and preferences you have applied to NetBarrier X. You can make sets for different locations, if you have a PowerBook or iBook - one set for office use, another for home use. 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.

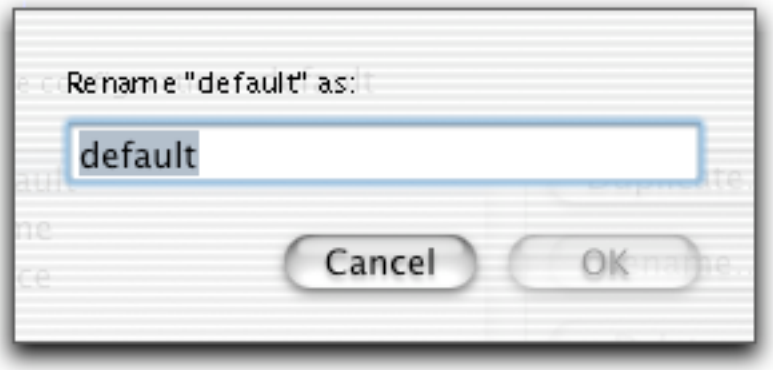


Select the set you wish to activate, and click Select. If you decide you do not want to activate this set, click Done, or select a different set.

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 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.

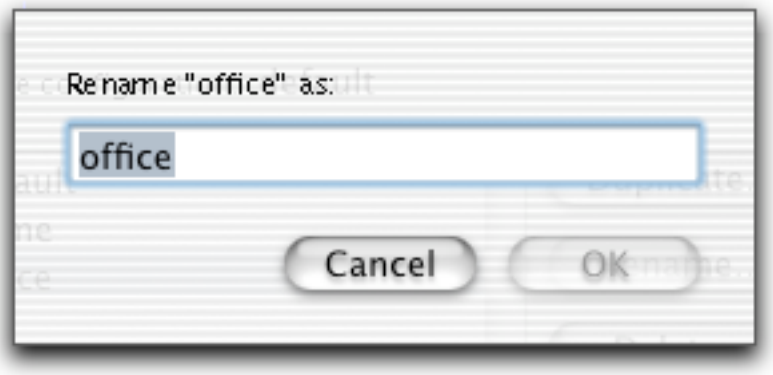
Deleting configuration sets

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 Delete. 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.

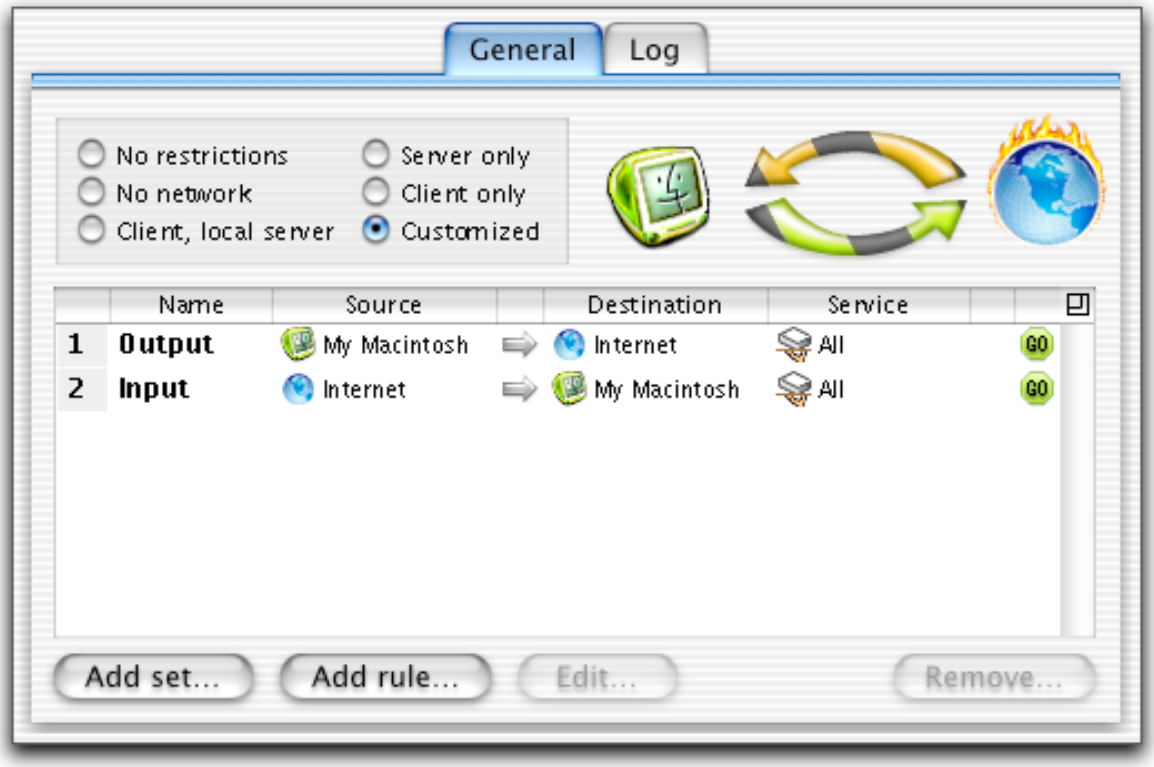


Enter the name for your new set, and click OK. If you decide you do not want to rename this set, click Cancel.

7 - Customized Protection

Using NetBarrier X's Customized Mode

Additional options concerning NetBarrier X'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 X's most powerful functions, by allowing you to configure its Firewall rules as precisely as you wish.

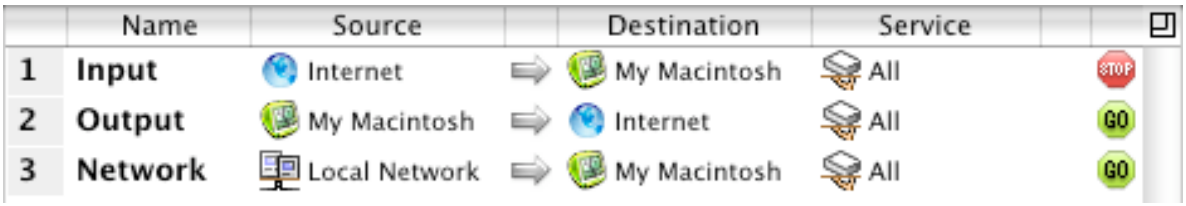
Important: NetBarrier X's Customized protection should only be used by experienced network administrators. Incorrectly setting its options may disrupt your network activity.

User-configurable Firewall Options

NetBarrier X'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.

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.

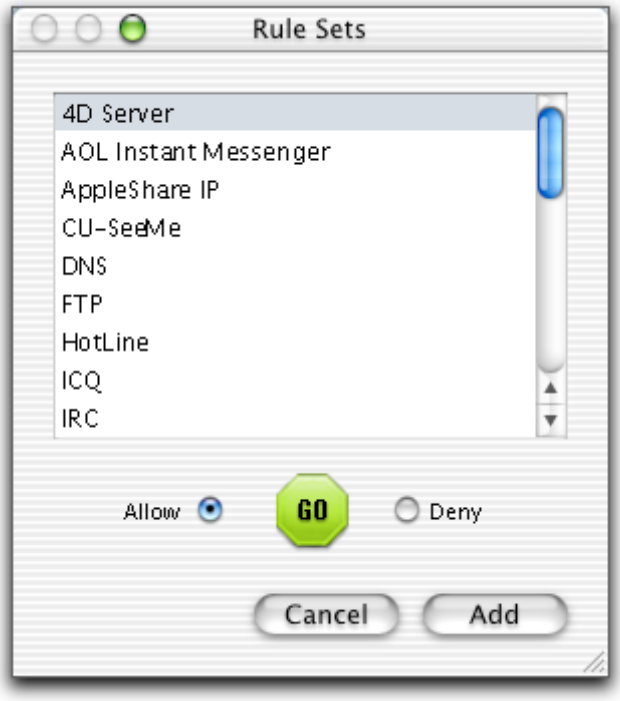


In this example, the first rule is blocking data coming from the Internet (which includes all networks, even a local network). Rule 3, however, is allowing traffic from a local network, but since it is in 3rd position, it will not be applied. The 1st rule will take precedence. For rule 3 to be applied,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

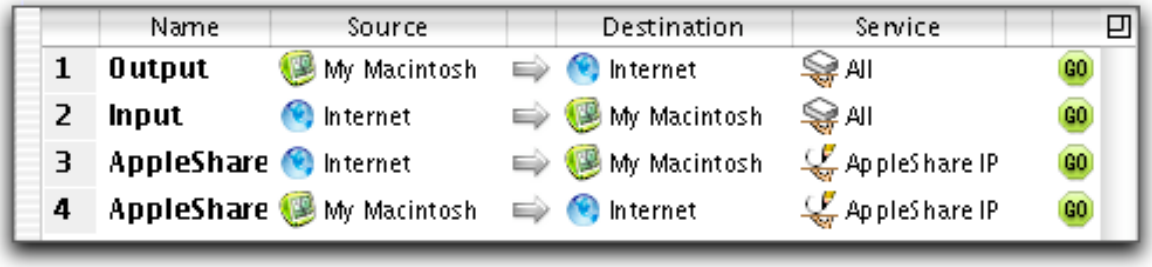
Using Predefined Rule Sets

NetBarrier X includes many predefined rule sets, corresponding to the most common Internet and network 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 Sets window will be displayed.



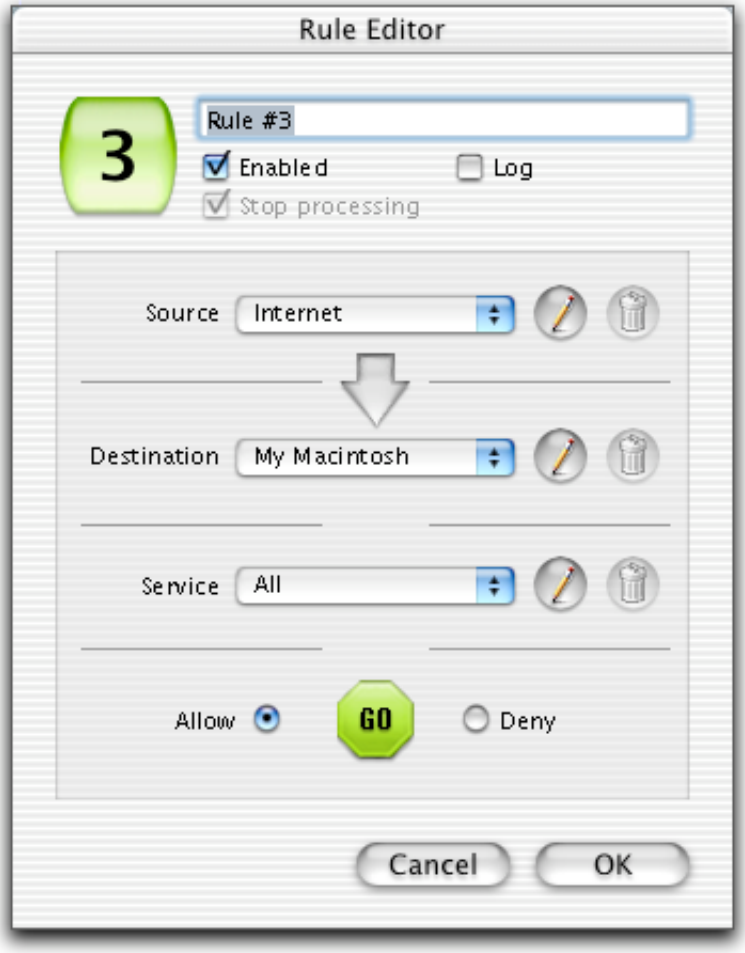
To select one of the Rule Sets, just click one of the applications or protocols in the list, click either Allow or Deny, and click Add. You will see that the rules for this application or protocol have been added to the rule list.



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 above.

Creating rules

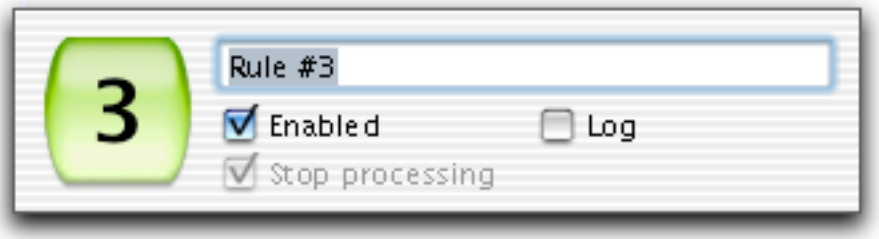
Creating a new rule is easy - just click the Add rule... button and the Rule Editor will open.



NetBarrier X'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 Source
2. The Destination
3. The Service
4. The Action



At the top of the Rule Editor box is a field where you can name this rule. Just below it, are three check boxes. You must check the first one, Enabled, if you wish your rule to be activated. If it is not checked, NetBarrier X 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 configuration sets, see chapter 6, **Preferences and Configurations**.

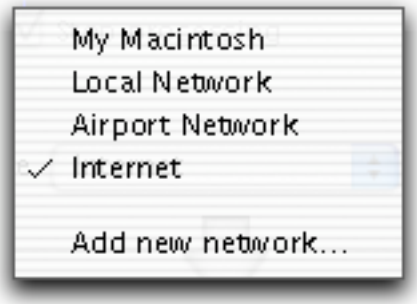
Next to this check box is the Log check box. If this is checked, any time this rule acts, an entry will be added to the log. If it is not checked, this rule will not be logged.

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, **Using the Stop Processing Function**, for more on this function.

Sources

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



There are four sources available by default:

My Macintosh
This is your computer.

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

Airport Network
This is a wireless Airport 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 the plus icon in the part section of the Network Editor.

Moving from one part to another

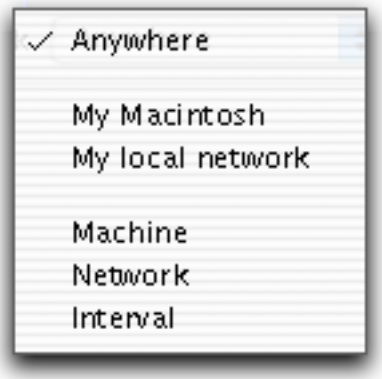
You can move from one part to another by clicking either of the arrow icons, to move either forward or backward.

Deleting parts

To delete a part, it must be displayed. Click one of the arrow icons until the part you wish to delete is displayed. Click the trash can icon. A dialog box will be displayed, asking if you really want to delete this part. Click Delete 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 beginning and ending addresses.

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.

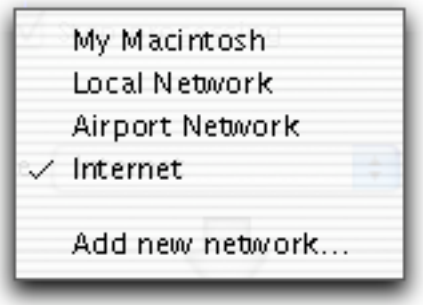
Deleting Sources

You can delete any sources that you have created. To do so, select the source, and then click the trash can icon. A dialog box will be displayed, asking if you really want to delete that source. Click Delete 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 four destinations for any rule. You may notice that NetBarrier X will not allow you to choose the same source and destination in a rule.

There are four destinations available by default:



My Macintosh
This is your computer.

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

Airport Network
This is a wireless Airport network that your computer is connected to.

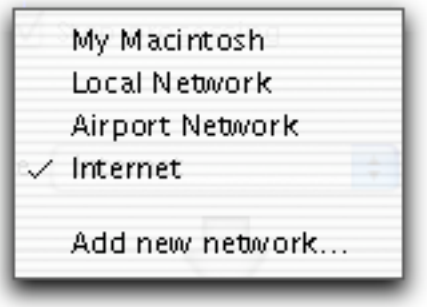
Internet

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

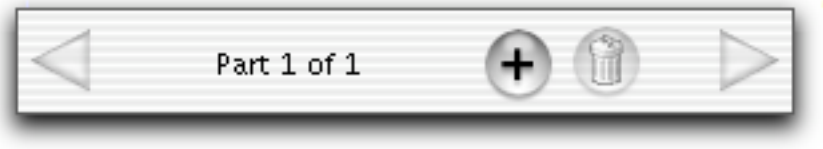
You may give the destination any name you wish, by entering a name in the text field.

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 the plus icon in the part section of the Network Editor.



Moving from one part to another

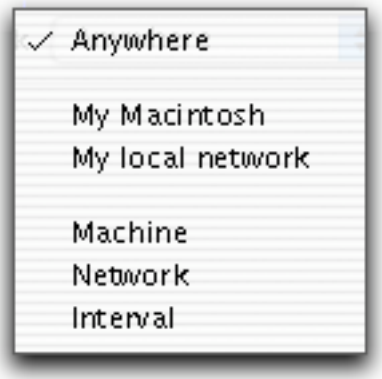
You can move from one part to another by clicking either of the arrow icons, to move either forward or backward.

Deleting parts

To delete a part, it must be displayed. Click one of the arrow icons until the part you wish to delete is displayed. Click the trash can icon. A dialog box will be displayed, asking if you really want to delete this part. Click Delete 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 beginning and ending addresses.

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

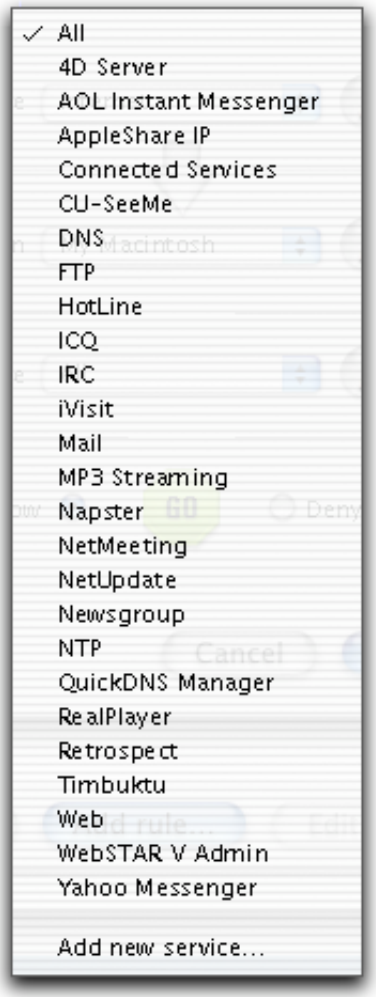
If you have selected this type of network, you must enter the beginning and ending IP addresses of the networks you wish to use.

Deleting Destinations

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

Services

There are several services available by default:



All

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

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.

Connected services

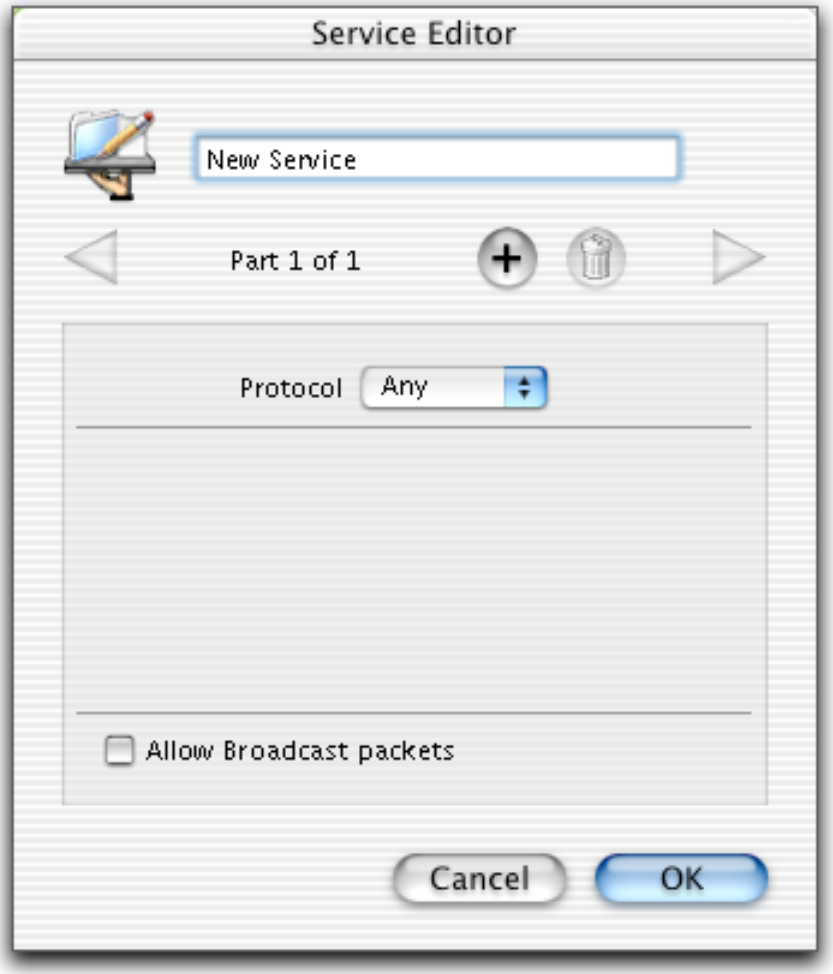
If this is selected, the rule will be active for TCP services only.

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 the plus icon in the part section of the Service Editor.

Moving from one part to another

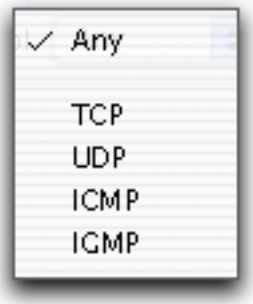
You can move from one part to another by clicking either of the arrow icons, to move either forward or backward.

Deleting parts

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

Protocol

Four different protocol suites 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 services that you can select from. This menu depends on the protocol you have selected. For more information on these protocols and services, 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 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.

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.

Deleting rules

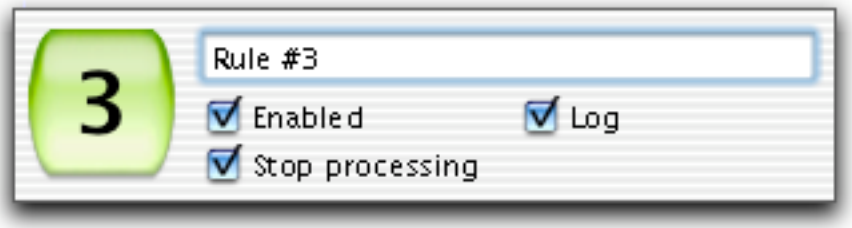
If you wish to delete a rule, select the rule by clicking on it once, then click Remove... A dialog box will open, asking if you really want to delete this rule. Click OK. If you decide you do not want to delete this rule, click Cancel.

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.

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.

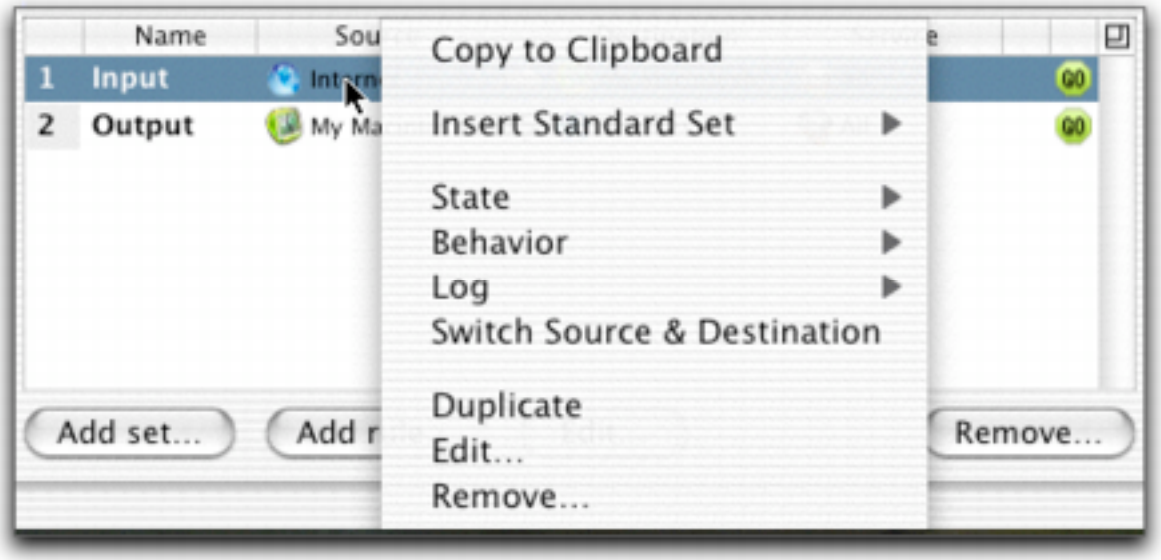
Note: care should be taken when creating rules for specific services. When you select a service for a specific program, it is possible that this program uses the same port as another program or service. Blocking or authorizing a specific service may

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 both 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.

Using the Rule Contextual Menu

NetBarrier X offers a contextual menu to work with firewall rules, which gives you quick access to many rule functions, and lets you make changes to rules with just a click. You can use this contextual menu to add new rules, to edit existing rules, or to change rule characteristics on the fly.

To see this contextual menu, hold down the Control key and click on a rule. (If you have a two button mouse, and have mapped the right mouse button to the Control key, you can just click the right button of your mouse.)



This contextual menu offers several options:

Copy to Clipboard
This lets you copy the contents of a rule to the clipboard.

Insert Standard Set / Add Standard Set
This lets you insert or add a standard set of rules. You can choose from five sets, in the Insert Standard Set submenu: No restrictions, No network, Client, local server, Server only, or Client only.

State
You can toggle the state of a rule, turning it On or Off.

Behavior
You can toggle the behavior of a rule, setting it to Allow or Deny traffic.

Log
You can toggle whether or not the rule records traffic information in the log.

Switch Source & Destination
This switches the source and destination of the rule.

Duplicate
This makes a copy of the rule.

Edit…
This lets you edit the rule using the Rule Editor window.

Remove…
This lets you delete the rule.

8 - Technical Support

Technical support is available for registered purchasers of NetBarrier X.

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.
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 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. An Internet protocol that provides simple but unreliable datagram services.
Whois: An Internet directory service for looking up information on domain names and IP addresses.