



# Intego NetBarrier X5

## User's Manual



## **Intego NetBarrier X5 for Macintosh**

© 2007 Intego. All Rights Reserved

Intego

[www.intego.com](http://www.intego.com)

This manual was written for use with Intego NetBarrier X5 software for Macintosh. This manual and the Intego NetBarrier X5 software described in it are copyrighted, with all rights reserved. This manual and the Intego NetBarrier X5 software may not be copied, except as otherwise provided in your software license or as expressly permitted in writing by Intego.

The Software is owned by Intego and its suppliers, and its structure, organization and code are the valuable trade secrets of Intego and its suppliers. The Software is protected by United States Copyright Law and International Treaty provisions.



## Contents

<b>1- About Intego NetBarrier X5 .....</b>	<b>6</b>
<b>What is Intego NetBarrier X5? .....</b>	<b>7</b>
Personal Firewall.....	7
Antivandal.....	7
Privacy Protection.....	8
Monitoring.....	9
Erasing Your Tracks With Washing Machine.....	9
<b>Using this User's Manual .....</b>	<b>10</b>
<b>2—Introduction to Computer Security.....</b>	<b>11</b>
<b>Why You Need to be Protected .....</b>	<b>12</b>
How Can a Computer be Totally Safe?.....	13
What Is a Firewall? .....	13
Friend or Foe? .....	13
<b>What You Risk.....</b>	<b>14</b>
Why People Break into Computers.....	14
The Different Types of Attacks and Intrusions Possible.....	15
<b>Privacy Protection .....</b>	<b>15</b>
<b>3—Installation.....</b>	<b>17</b>
<b>System Requirements.....</b>	<b>18</b>
<b>Installing Intego NetBarrier X5.....</b>	<b>18</b>
<b>4—Quick Start .....</b>	<b>19</b>
Using Intego NetBarrier X5.....	20
Using the NetBarrier X5 Overview Screen.....	20
Status Indicators on the Overview Screen .....	24
Using the Setup Assistant .....	25
Using the Intego Menu.....	29
NetBarrier X5 Password Protection.....	30
Getting Help.....	30
<b>5—The Four Lines of Defense: Firewall.....</b>	<b>31</b>
<b>Firewall Rules .....</b>	<b>32</b>
Simple Mode .....	32
Advanced Mode.....	35
<b>Creating Rules with the Assistant.....</b>	<b>37</b>
Name and Behavior.....	39
Communication Direction .....	40
Service .....	42
Options.....	43
Conclusion.....	44
<b>Creating Service-Specific Rules Quickly .....</b>	<b>46</b>



<b>Creating Rules Manually .....</b>	<b>48</b>
Rule Naming, Logging, Evaluation and Schedules .....	49
Rule Sources and Destinations .....	52
Rule Services .....	55
Rule Interfaces .....	60
Rule Actions .....	61
Multi-Part Sources, Destinations, Services and Interfaces .....	61
Deleting Sources, Destinations, Services and Interfaces .....	62
<b>Working with Rules .....</b>	<b>63</b>
Rule Order .....	63
Editing and Deleting Rules .....	63
Using the Rule Contextual Menu .....	64
<b>Trojan Horse Protection .....</b>	<b>66</b>
<b>6—The Four Lines of Defense: Privacy .....</b>	<b>68</b>
<b>Data Filter .....</b>	<b>69</b>
How the Data Filter Works .....	70
What to Protect .....	71
Adding Data to the Filter .....	72
Activating, Deactivating and Deleting Data Items .....	75
Data Filter Options .....	76
<b>Surf Filters .....</b>	<b>77</b>
Banners Filter .....	78
Cookies Filter .....	82
Information Hiding .....	85
<b>7—The Four Lines of Defense: Antivandal .....</b>	<b>86</b>
<b>Antivandal .....</b>	<b>87</b>
Policy .....	88
Options .....	91
Unifying Policy Options .....	92
<b>Anti-Spyware .....</b>	<b>93</b>
Options .....	96
Applications: Adding, Removing and Changing Settings .....	97
<b>The Stop List and Trusted Group .....</b>	<b>99</b>
Stop List/Trusted Group Information .....	101
A Note About DNS Lookups .....	103
Adding Addresses .....	104
Using Wildcards .....	105
Removing Addresses .....	105
Moving Addresses Between the Stop List and Trusted Group .....	106
Editing an Address .....	107
The Contextual Menu .....	108
<b>8—The Four Lines of Defense: Monitoring .....</b>	<b>109</b>
<b>The Log .....</b>	<b>110</b>
Log View Options .....	111
Log Window Contextual Menu .....	115
Pausing the Log .....	117
Clearing the Log .....	117
Exporting the Log .....	118
Filtering Data in the Log Window .....	120



<b>Traffic.....</b>	<b>122</b>
Traffic View Modes .....	122
Selecting Activity Data Types .....	126
NetBarrier Monitor.....	127
NetBarrier Monitor Preferences.....	129
The NetBarrier Monitor Widget .....	130
The NetBarrier X5 Monitor Screen Saver.....	131
<b>Services .....</b>	<b>133</b>
<b>Network.....</b>	<b>135</b>
<b>Whois .....</b>	<b>139</b>
<b>Traceroute .....</b>	<b>140</b>
<b>NetUpdate .....</b>	<b>144</b>
<b>9—Understanding Alerts .....</b>	<b>145</b>
Alert Settings .....	146
Examples of Alerts.....	149
Attack Counter.....	152
<b>10—Preferences and Configurations.....</b>	<b>153</b>
Modem Preferences .....	154
Log Preferences .....	155
Traffic Preferences.....	157
Whois Preferences .....	159
Advanced Preferences .....	160
About NetBarrier X5.....	161
Configurations.....	162
Creating, Editing and Deleting Configurations .....	162
Exporting and Importing Settings.....	165
Locking and Unlocking the Interface .....	166
<b>11—Technical Support .....</b>	<b>167</b>
<b>12—Glossary.....</b>	<b>170</b>



# **1- About Intego NetBarrier X5**



## What is Intego NetBarrier X5?

Intego NetBarrier X5 is the Internet security solution for Macintosh computers running Mac OS X. It offers thorough protection against intrusions coming across the Internet or a local network.

NetBarrier X5 protects your computer from intrusions by constantly filtering all the activity that enters and leaves through the Internet or a network. NetBarrier X5 protects you from thieves, hackers and intruders, and warns you automatically if any suspicious activity occurs.

NetBarrier X5 has four lines of defense to protect your Mac and your data from intrusions and attacks.

### Personal Firewall

NetBarrier X5 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 X5's Antivandal is a powerful guardian for your computer. It watches over your Mac's network activity, looking for signs of intrusion. If it detects any suspicious activity, NetBarrier X5 stops the intruder in their tracks and displays an alert. The Antivandal has another powerful function, the Stop List, that records the addresses of intruders who attempt to get into your Mac, ensuring that they will always be blocked. Several options allow you to choose the type of protection you have on your computer.

#### *Policy*

NetBarrier X5 can stop incoming data that is considered hostile. It can display an alert dialogue, showing why the data was stopped, and asking you to allow or deny it. You can also select other alert options, such as having NetBarrier X5 play a sound, put the host automatically in the Stop List, or send an e-mail message to the address(es) of your choice.



### ***Stop List***

When an intruder is detected trying to break into your Mac, NetBarrier X5 allows you to put them on the Stop List, which records their network address. 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 X5. These may be computers on your local network, blocked because they are sending pings to your computer, for example. NetBarrier X5 allows you to put them in the Trusted Group, where they will be considered friends for as long as you want, ensuring that they can always access your Mac. It is important to note that the Trusted Group only applies to NetBarrier X5's Antivandal functions and data filter, and Firewall rules are still applied to computers in the Trusted Group.

### ***Anti-Spyware***

NetBarrier X5 lets you control Internet and network access by individual applications. Whenever an untrusted application tries to connect to a network, NetBarrier X5 can display an alert, informing you which application is making the connection. If you want to allow that application to access the network—if it truly is an application you know should be using the network—then you can do so. But if an application tries to connect in secret, you can block it permanently.

## **Privacy Protection**

NetBarrier X5 helps protect your privacy. It filters data to ensure that no sensitive information leaves your computer, blocks ad banners, and lets you surf anonymously. And 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.





## Monitoring

NetBarrier X5 contains powerful tools for monitoring your network activity and usage. Its activity gauges show your network traffic in real time, and its additional monitoring functions give you essential information on your computer, its network and the services and connections that are active.

NetBarrier X5 even offers a separate program, NetBarrier Monitor, that you can keep open all the time, as well as a monitoring screen saver, so you can always keep an eye on your network traffic.

## Erasing Your Tracks With Washing Machine

NetBarrier X5 includes a separate program named Washing Machine that further protects your privacy by helping you delete information about your Internet habits. It provides an easy way to remove bookmarks, cookies, caches, download histories and browsing histories for more than two dozen programs that regularly store such information, and can be set to periodically “clean” those items for effortless protection.

Washing Machine includes functions that were in previous versions of NetBarrier; you can launch the program from the Intego Menu in the NetBarrier X5 submenu. For detailed information about using Washing Machine, see the Intego Washing Machine User Manual you received with NetBarrier X5.



## Using this User's Manual

If you are a:	Read:
Home user, connected to the Internet	<ul style="list-style-type: none"><li>• Chapter 2, <b>Introduction to Computer Security</b></li><li>• Chapter 3, <b>Installation</b></li><li>• Chapter 4, <b>Quick Start</b></li><li>• Optional: chapters 5-9, <b>The Four Lines of Defense</b>.</li></ul> <p>NetBarrier X5 is configured to automatically protect your computer from intruders.</p>
Business or Academic user, connected to a local network and the Internet	<ul style="list-style-type: none"><li>• Chapter 2, <b>Introduction to Computer Security</b></li><li>• Chapter 3, <b>Installation</b></li><li>• Chapter 4, <b>Quick Start</b>.</li></ul> <p>NetBarrier X5's basic protection modes will probably be sufficient for you; however, you might also want to read chapters 5-8, <b>The Four Lines of Defense</b>.</p>
Advanced user, using your computer as a server, or administering a network	<p>The entire manual concerns your situation, but you will want to read chapters 5-8, <b>The Four Lines of Defense</b>, and especially chapter 5, which explains how to create your own rules.</p>

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



## **2—Introduction to Computer Security**



## Why You Need to be Protected

Whether you use your Mac for work or just for surfing the Internet, whether you are online 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 Mac that is for your eyes only, there is somebody out there who would certainly find it interesting.

The more you use your Mac for daily activities, whether personal or professional, the more you should protect the information it contains.

Think of your computer as a house. You certainly lock your doors and windows when you go out, but do you protect your Mac 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 X5.

When your Mac 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 X5 works like a set of locks 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 Mac and 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 enjoys messing up people's computers just for fun.

Without Intego NetBarrier X5, you may never know  
if anyone is trying to get into your Mac.

A computer is only as secure as the people who have access to it. NetBarrier X5 protects your computer by preventing unauthorized network access to your Mac, and by protecting against unauthorized export of private information.



## How Can a Computer be Totally Safe?

It has been said that the only truly secure computer 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 X5 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 X5 offers powerful firewall protection for your Mac, and its customized protection allows advanced users to configure specific rules to protect against foes who wish to infiltrate your computer.

## Friend or Foe?

Every wall has to have a gate so people can get in and out. NetBarrier X5'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 X5 knows 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, crackers hope 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” 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 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 many ways to do so. Here are some of them:

- To steal confidential documents or information.
- To execute commands on your computer that modify the system, erase your hard disk, or disable your computer.
- To hack web sites, replacing pages with different text and graphics.
- To launch denial-of-service attacks that can render your computer temporarily unusable.
- To get 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 or e-mail about things you never requested. By then, 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 that 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 of cookies are to maintain a



“shopping basket” of goods you have selected to purchase during a session at a site, site personalization (presenting different pages to different users), or to track 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 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 match these habits.

NetBarrier X5’s approach to privacy is simple: it provides you with the means to prevent certain types of information from being recorded without your knowledge.





# 3—Installation



## System Requirements

- Any officially-supported Mac OS X compatible computer
- Mac OS X 10.4 or higher, or Mac OS X Server 10.4 or higher
- 40 MB free hard disk space

## Installing Intego NetBarrier X5

For information on installing and serializing Intego NetBarrier X5, see the Intego Getting Started manual, included with your copy of the program. If you purchased the Intego NetBarrier X5 by download from the Intego web site, this manual will be in the disk image you downloaded that contains the software. If you purchased NetBarrier X5 on a CD or a DVD, you'll find this manual on the disc.



## 4—Quick Start



## Using Intego NetBarrier X5

When you first open NetBarrier X5, the Overview screen displays. If you've used an earlier version of NetBarrier, you'll notice that this screen has been simplified and streamlined. But don't worry: all the old functions are there.

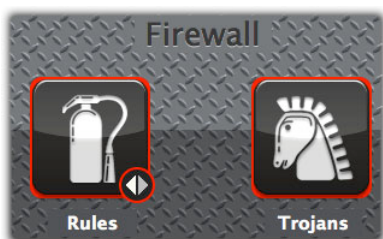


## Using the NetBarrier X5 Overview Screen

The Overview screen gives quick access to:

- NetBarrier X5's functions, settings and logs,
- Several helpful network utilities, such as Whois and Traceroute,
- Visual indicators of what sorts of protection are enabled,
- Information about the program itself, such as when it was last updated,
- A way of managing multiple configurations, so you can quickly change protection settings.

Central to the Overview screen are sections that control NetBarrier X5's four lines of defense. Controls for Firewall, Antivandal and Privacy appear as large buttons in the center of the Overview screen; controls for Monitoring are the smaller buttons in the bottom-right corner.



The Firewall section gives you access to Rules that define what programs can send and receive information to and from your Mac, and Trojan settings to protect your Mac from malicious Trojan horses.









The Privacy section gives you access to settings that prevent specific data from being sent over the Internet and local networks, and blocks certain types of information that are sent and received when you surf the internet.

The Antivandal section gives you ways to see and control your Policy of stopping certain sorts of attacks; how you're protected against programs that secretly connect to remote computers (Anti-Spyware); your Stop List, that keeps track of the bad guys; and your Trusted Group of friends who are explicitly allowed to access your Mac.

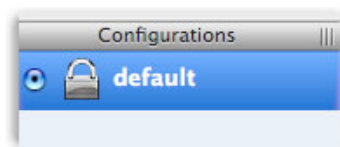


You can access Monitoring functions through buttons in the bottom-right corner of the Overview screen. They're also available through selections under the View menu, and by using keyboard shortcuts. They are:

	<b>Log</b>	Option-Command-L	Shows a record of NetBarrier's activities, and traffic to and from your Mac to the Internet or local networks
	<b>Traffic</b>	Option-Command-1	Shows network traffic entering and leaving your Mac
	<b>Services</b>	Option-Command-2	Shows a list of ways that your Mac is prepared to provide information to the outside world
	<b>Networks</b>	Option-Command-3	Shows outside networks that are currently available to your Mac
	<b>Whois</b>	Option-Command-4	Shows information about the owners and managers of Internet domains
	<b>Traceroute</b>	Option-Command-5	Shows the network path that a signal takes to get from your Mac to another computer

Each of these features is described in chapter 8, **The Four Lines of Defense: Monitoring**.

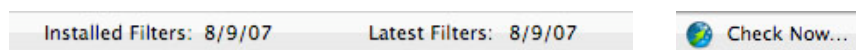
At the left of the Overview window is a list of Configurations. Each configuration is a collection of settings for NetBarrier's Firewall, Privacy and Antivandal protection. At first there is only one configuration, named "default". The radio button shows which configuration is currently active.



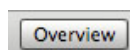
At the bottom of the Configurations list are four buttons that let you duplicate, edit, remove and hide configurations. (You can also toggle between showing and hiding the Configurations list by pressing Command-K or choosing View > Hide/Show Configurations List.) For more information, see chapter 10, **Preferences and Configurations**.



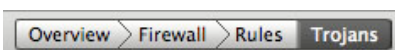
At the very top of the screen is the NetUpdate Status Bar, which shows the dates of the latest NetBarrier filters installed on your Mac, and the date of the latest filters available through Intego NetUpdate. NetUpdate periodically checks for updates, or you can have it check immediately by clicking the “Check Now...” button in the upper-left corner. To hide the NetUpdate Status Bar, choose View > Hide NetUpdate Status Bar. For more information, see the Intego Getting Started Manual.



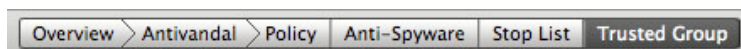
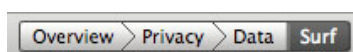
Finally, a small button near the top-left corner of the Overview screen tells you which section of the NetBarrier X5 interface you’re currently viewing. When you first launch the program, it simply says “Overview”.



But when you look at the control screen for Trojans, for example, you see a segmented button that makes clear that it’s a part of the Firewall section, along with Rules.



Clicking on Rules takes you there; clicking on Firewall or Overview takes you back to the Overview screen. The Privacy and Antivandal sections work the same way.

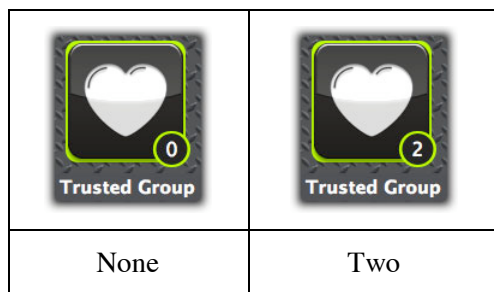


## Status Indicators on the Overview Screen

The status of various NetBarrier X5 features appears as part of the icons on the Overview Screen. When the Trojans, Data and Anti-Spyware sections are on, you'll see a small check mark in the bottom-right corner of their icons.



Similarly, the Stop List and Trusted Group icons show how many entries are in their lists.

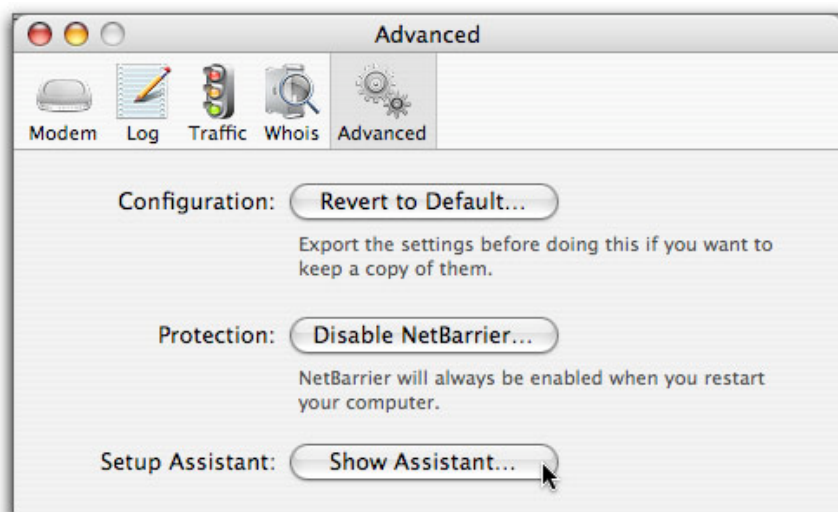




## Using the Setup Assistant

When you install NetBarrier X5 and restart your Macintosh, it automatically begins protecting your Mac. The firewall is enabled in “Client, local server” mode and activity is written to the log. In this mode, your Mac can access the Internet as a client computer, and your Mac can function as both a client and server on a local network. For more information about NetBarrier X5’s Firewall Modes, see below.

NetBarrier X5 includes a Setup Assistant to help you quickly and easily adjust NetBarrier X5’s basic settings so they are appropriate to your network usage. The first time you open NetBarrier X5, the Setup Assistant launches automatically. If you have upgraded from a previous version of NetBarrier, you will need to launch the Setup Assistant manually. To do this, choose NetBarrier X5 > Preferences and click the Advanced icon. Click Show Assistant... at the bottom of the window. You will need an administrator’s password to run the Setup Assistant.





Click the right arrow to begin configuring NetBarrier X5. You can click the left arrow at any time to return to previous screens. The NetBarrier X5 Setup Assistant briefly presents informational screens about the program's different functions:

- **Firewall (Rules and Trojans)**
- **Privacy (Data and Surf protection)**
- **Antivandal (Policy, Anti-Spyware, Stop List, and Trusted Group)**
- **Monitoring (the Log and five Monitor tools)**
- **One more thing (miscellaneous tools)**

When done, the Configuration screen allows you to choose which NetBarrier X5 configuration you want to use.



The configurations are:

Name	Best if...	Firewall setting	Other settings
<b>Default</b>	...you need to allow access to your Mac from the local network, but want to be protected from invasions from outside your local network.	“Client, local server” mode: your Mac can access the Internet as a client computer, and can function as both a client and server on a local network.	All Antivandal and Privacy filters are disabled.
<b>Normal</b>	...you do not use your computer as a network server or for local file sharing.	Client only mode: your Mac can function only as a client on a local network or the Internet. The server functions of your computer are blocked.	Antivandal filters are enabled against Buffer Overflow Attacks, Intrusion Attempts, Ping Attacks, Port Scans and SYN Flooding, but disabled against Ping Broadcasts. All Privacy filters are disabled.



<b>Strong</b>	...you want maximal protection, and can accept that this configuration might block some traffic.	Client only mode.	All Antivandal filters are enabled, as are those that protect against Trojans.
---------------	--	-------------------	--

Click the Configure button to activate the configuration you have selected.

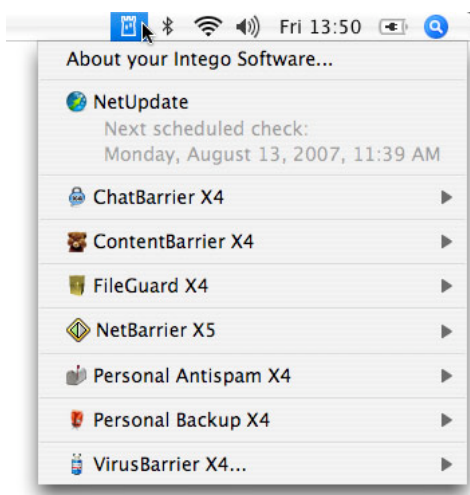


## Using the Intego Menu

NetBarrier X5, like all other Intego programs, installs a menu in the menubar, called the Intego menu. Its icon is a small tower, as in the Intego logo.



Click the Intego menu icon to display a menu that shows all your Intego software:



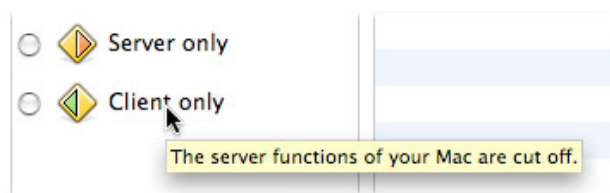
You can change many of NetBarrier X5's settings from the Intego menu. Choose the Intego Menu > NetBarrier X5. You can change configurations, and you can turn on or off settings, such as filtering or privacy settings. You can open Intego Washing Machine from the Intego menu, by choosing the Intego menu, then NetBarrier X5 > Open Washing Machine.... And you can open NetBarrier Monitor by choosing NetBarrier X5 > Open NetBarrier Monitor.

## NetBarrier X5 Password Protection

NetBarrier X5 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. Users who do not have administrator's rights cannot change any of NetBarrier X5's settings or preferences. These users can view Monitoring functions such things as logs and traffic gauges, but are not authorized to make changes to the program's operation.

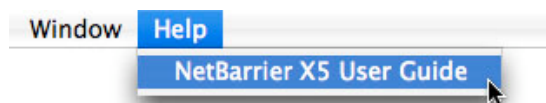
## Getting Help

You can get help on some of NetBarrier X5's functions by holding your cursor over certain texts and zones:



A Tool Tip displays explaining the various functions and features.

For complete help, this manual is available by choosing Help > NetBarrier X5 User Guide.



# **5—The Four Lines of Defense: Firewall**



NetBarrier X5 is a powerful, easy-to-use program that protects your Mac when connected to a network through four lines of defense. The first of these is a personal firewall, a powerful program that filters all data packets entering or leaving your Mac through the Internet or a local TCP/IP network. It also protects you from Trojan horses by blocking the ports they use.

The Overview screen shows the Firewall section, which contains two buttons: Rules and Trojans.

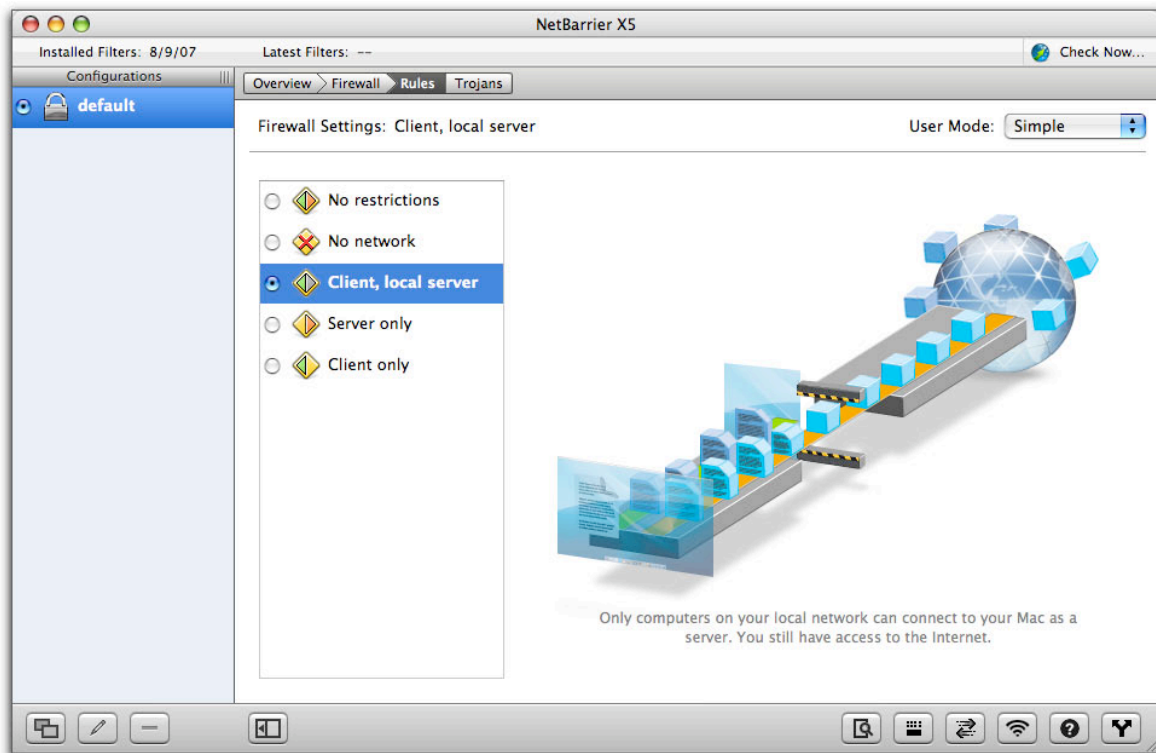


## Firewall Rules






### Simple Mode

When you click the Rules button, NetBarrier X5 presents the simple mode for controlling Firewall settings. There are five preset firewall settings that cover all the situations that you will encounter in normal use, each accompanied by an animation that graphically shows the effect of applying the setting. The screen closest to you represents your Mac; the globe represents the Internet; the screen halfway between the two represents the limit of your local network. Here the default setting, “Client, local server”, shows how your computer can receive information from beyond the local network, but that computers beyond your local network cannot access your Mac.





The following are the five firewall settings, and how they display on the Overview screen:

<b>No restrictions</b> 	NetBarrier X5's firewall allows all incoming and outgoing network data to be sent and received,.
<b>No network</b> 	NetBarrier X5'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.
<b>Client, local server</b> 	NetBarrier X5's firewall allows your Mac to function as a client and local network server. Your Mac can access the Internet as a client computer, and as both a client and server on a local network.
<b>Server only</b> 	NetBarrier X5's firewall allows your Mac to function only as a server: All client functions, including your ability to surf the Internet, are blocked.
<b>Client only</b> 	NetBarrier X5's firewall allows your Mac to function only as a client on a local network or the Internet. The server and file-sharing functions of your Mac are blocked.

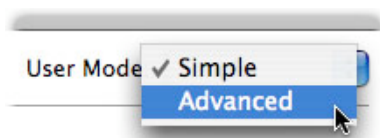
These five settings are sufficient for most people. But if you want more control over access to your computer—if, for example, you're running a gaming party and want to forbid all traffic except for communications that are part of the game—then you need to switch to NetBarrier X5's Advanced mode.



## Advanced Mode

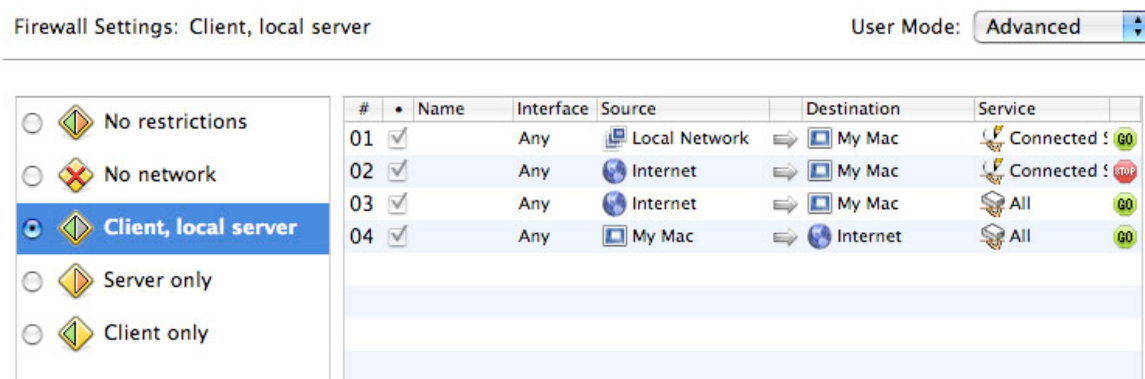
Each of the five settings described above is actually a collection of rules, each of which in turn is defined by naming permitted or forbidden sources, destinations, services and interfaces. Simple mode doesn't permit you to change the rules or any of their parts. To do that, you need to enter the Firewall screen's advanced mode.

To access NetBarrier X5's complete set of firewall rules, change the User Mode popup menu in the upper-right corner from Simple to Advanced.



**WARNING:** Changing these settings could dramatically affect your computer's ability to access local networks and the Internet. You should only use advanced mode if you fully understand its effects and how it functions.

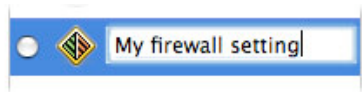
In simple mode, clicking any of the five preset firewall settings displays an animation; in advanced mode, you see the details of each setting's rules.



In this example, the “Client, local server” setting shown has four rules. The first allows the local network to access your Mac through all Connected Services—that is, TCP connections that involve back-and-forth communications, such as serving files from your Mac. The second rule, however, forbids such connections from the Internet at large, preventing your Mac from acting as a server to an unknown computer outside your local network. The third rule allows all other communications from the Internet to your Mac, while the fourth allows all communications from your Mac *to* the Internet.

The five preset firewall settings are “frozen” for convenience and stability: you can’t change their rules, or the order in which they appear. But NetBarrier X5 gives you two ways to create additional, customized settings: through the Assistant, and manually.

In either case, the first step is to click the + button below the list of settings. You’ll see a new setting appear, named “untitled setting”. Click it and type any name you prefer, then press Enter or Return to make the change permanent.



Note that you have only created this setting, but have **not** enabled it yet. It’s a good idea to not enable firewall settings until you have finished adding all your rules. To make it the active setting, click the radio button to its left.

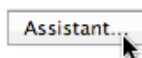
## Creating Rules with the Assistant

NetBarrier X5 contains an assistant to help you create your own custom firewall rules. With this assistant, you can create your own rules with just a few mouse clicks. While not all of NetBarrier X5's rule features are available when you create rules with the assistant, it can cover most of your needs for firewall rules. If you need more customization, you can create rules using the assistant then edit them manually.

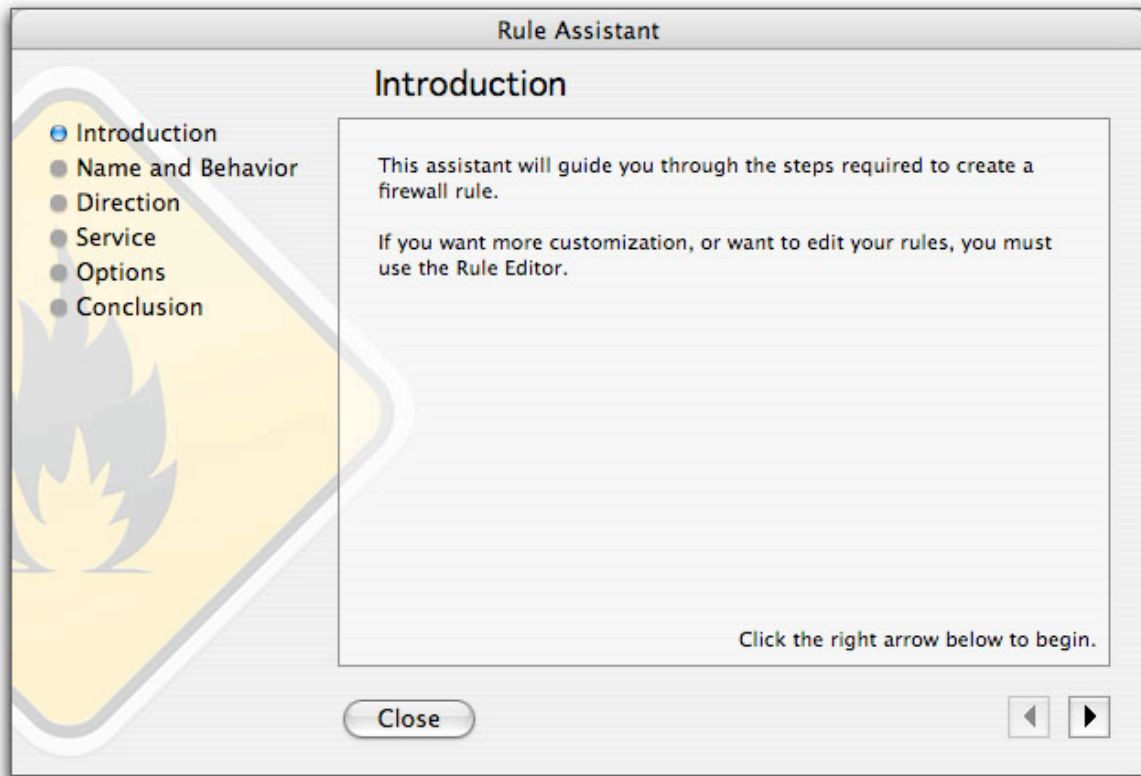
The NetBarrier X5 Assistant walks you through a series of steps to create your rule:

- **Name and Behavior**
- **Direction**
- **Service**
- **Options**
- **Conclusion**

To create a new rule using the assistant, click the Assistant button.



The first assistant screen displays.

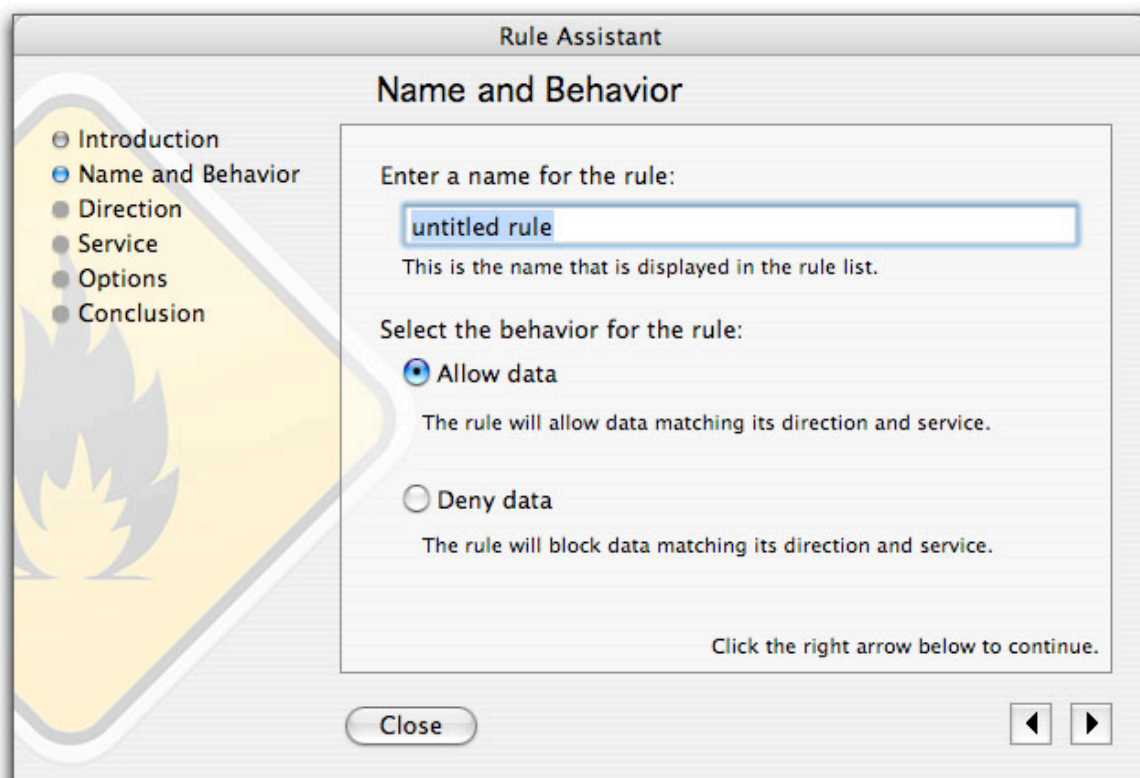


Click the right arrow to begin creating a new rule. You can click the left arrow at any time to return to previous screens.

Or click Close to exit the Assistant.

## Name and Behavior

This screen lets you choose a name for your rule and its behavior.



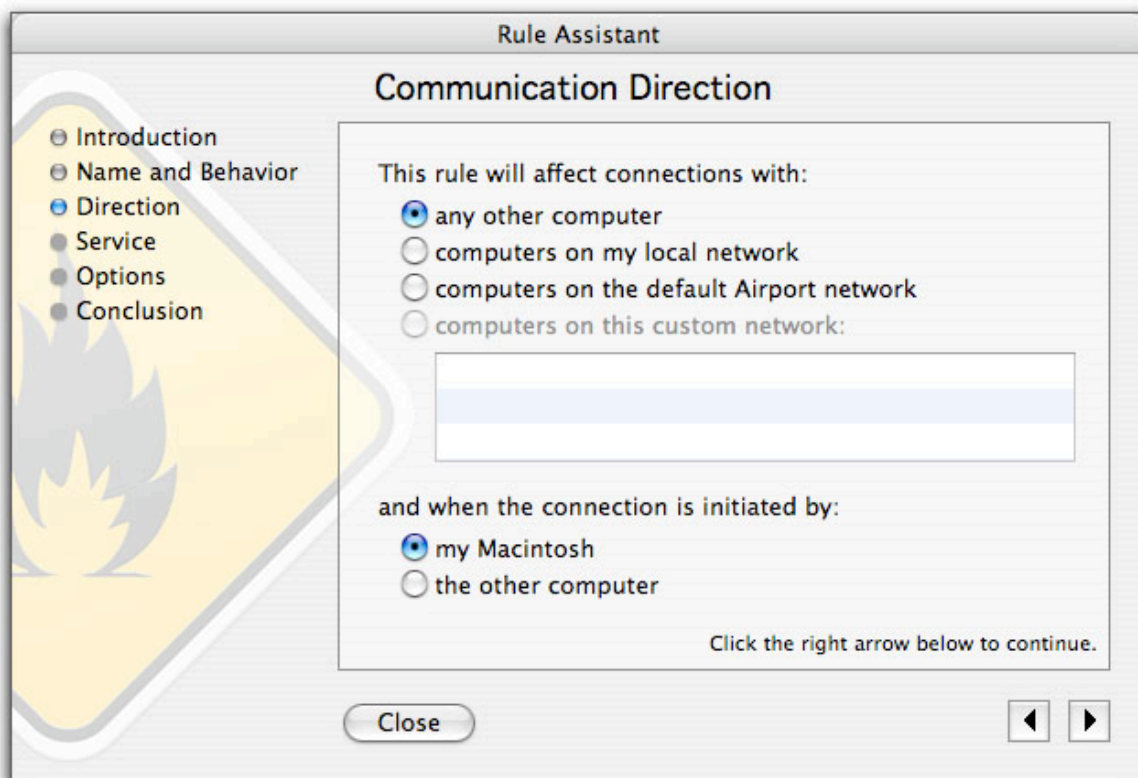
The screenshot shows a window titled "Rule Assistant" with a sub-header "Name and Behavior". On the left is a sidebar with a list of steps: Introduction, Name and Behavior (selected), Direction, Service, Options, and Conclusion. The main area contains a text input field with "untitled rule" and a description: "This is the name that is displayed in the rule list." Below this, there are two radio button options: "Allow data" (selected) and "Deny data". Each option has a description: "The rule will allow data matching its direction and service." and "The rule will block data matching its direction and service." respectively. At the bottom right, it says "Click the right arrow below to continue." At the bottom left is a "Close" button, and at the bottom right are left and right navigation arrows.

Enter a name for your rule in the name field, then select the behavior for the rule: Allow data or Deny data. If you select Allow data, the rule will allow data matching its direction and service to pass. If you select Deny data, the rule will block data matching its direction and service.

Click the right arrow to go to the next screen.

## Communication Direction

This screen lets you choose the communication direction and which host initiates the communication.



First, in the **This rule will affect connections with:** section, select a remote host. You have four choices for the remote host:

<b>Any other computer</b>	Any computer other than your Macintosh.
<b>Computers on my local network</b>	Any computer on the same local network as your Macintosh.
<b>Computers on the default AirPort network</b>	Any computer on your default AirPort network, if you have one.
<b>Computers on this custom network</b>	If you have created any custom networks using the standard rule editor, you can select one of them here.





Next, select the computer that initiates the connection:

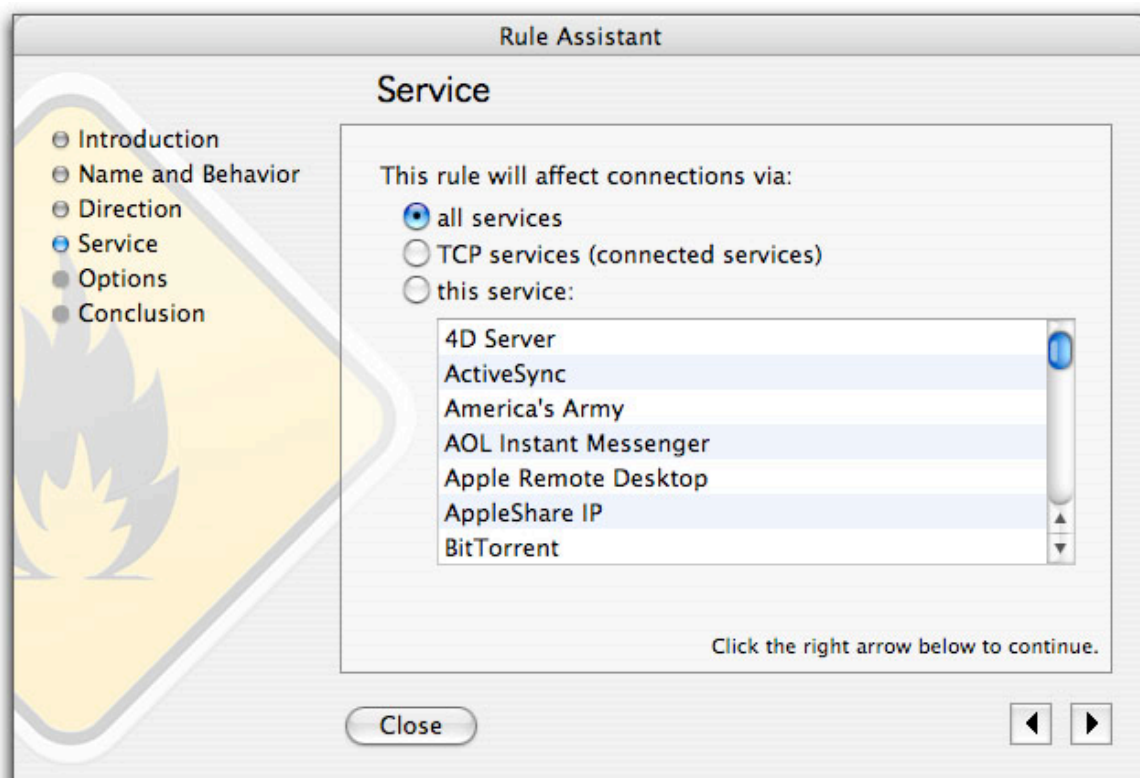
<b>My Macintosh</b>	Your Macintosh, the computer using this rule.
<b>The other computer</b>	The remote host, as was defined in the first part of this screen.

When you have finished, click the right arrow to go to the next screen.



## Service

This screen lets you choose the service that the rule affects.



You can choose from three types of services:

<b>All services</b>	All network services.
<b>TCP services (connected services)</b>	Services that require that a connection be open and maintained between two computers, such as HTTP, FTP, TELNET, SSH, POP3, AppleShare, etc. This covers all TCP connections.
<b>This service</b>	You can choose from a list of services that correspond to popular applications and protocols. Select the service you want to use by clicking its name in the list.

When you have finished, click the right arrow to go to the next screen.

## Options

This screen lets you choose additional options for your rule.



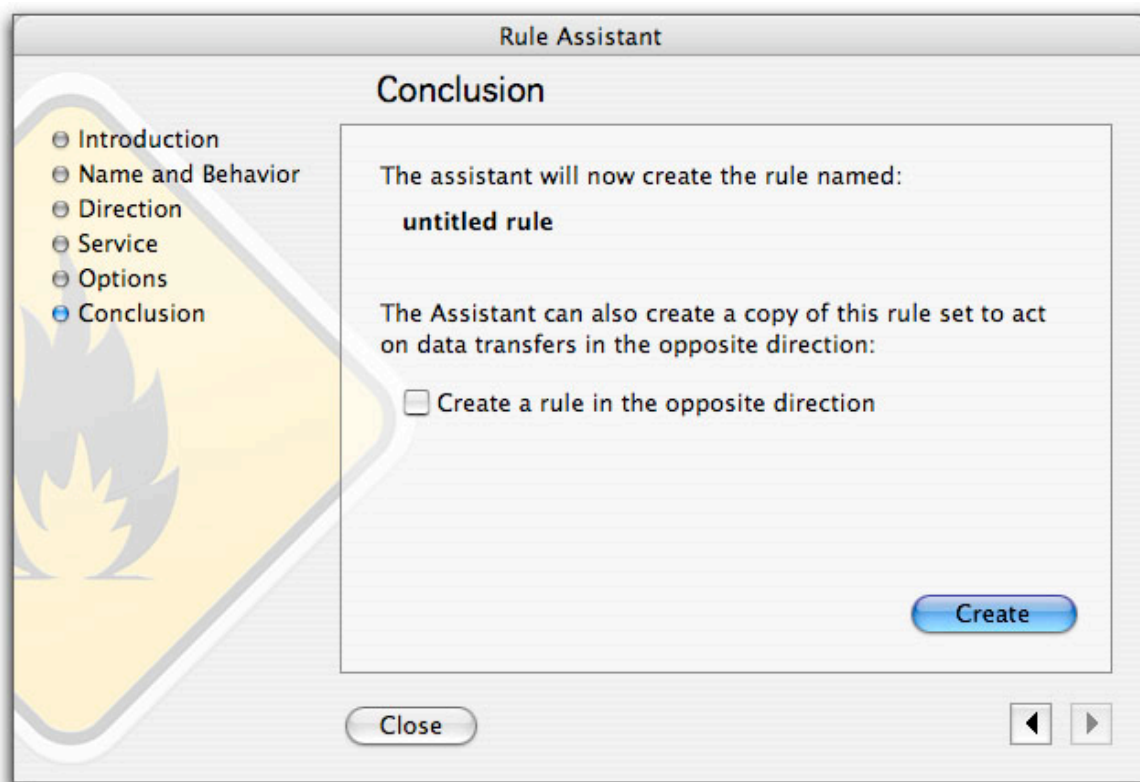
Two options are available on this screen:

<b>Log rule usage</b>	The firewall records each time this rule is used in its log.
<b>Disable the rule</b>	NetBarrier X5 creates the rule but disables it. You can enable it manually later.

When you have finished, click the right arrow to go to the next screen.

## Conclusion

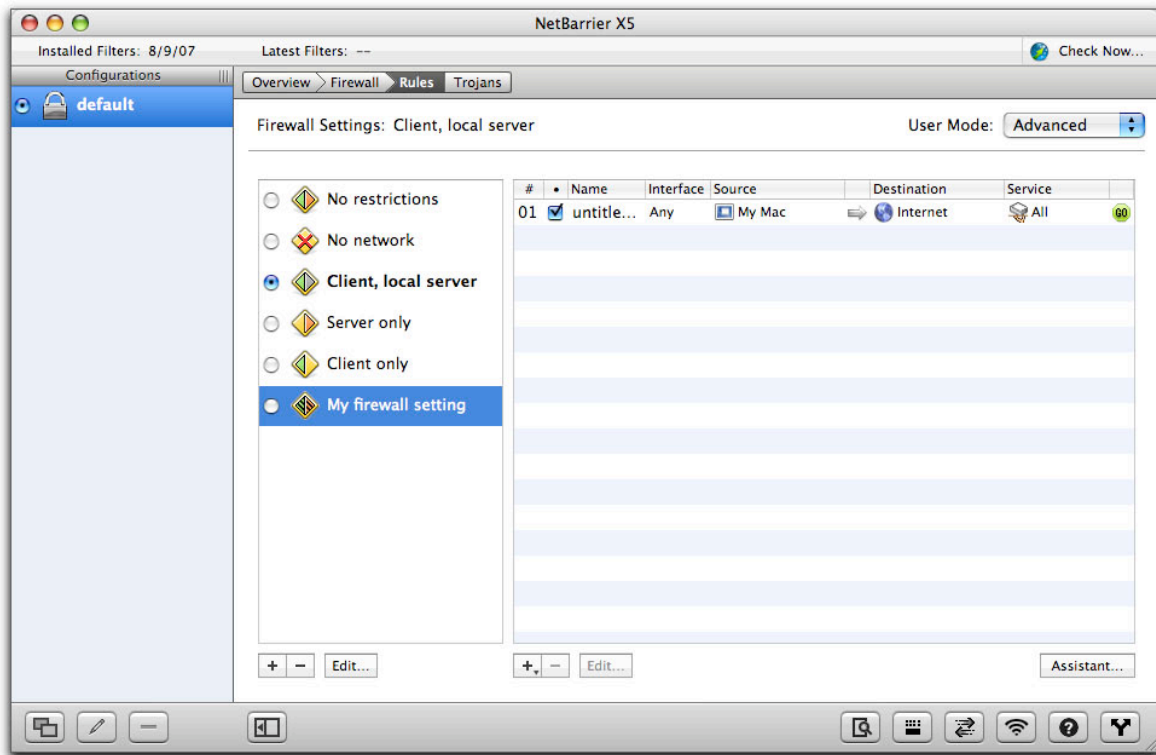
This screen creates the rule according to the settings you have selected in the assistant.



This screen offers one final option: if you check **Create a rule in the opposite direction**, the assistant creates a matching rule with the source and destination switched.

Click Create to create your rule and exit the assistant.

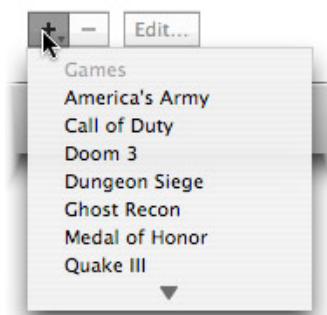
When you have finished, you will see that your rule (or rules, if you checked **Create a rule in the opposite direction**) displays in the NetBarrier X5 list of firewall rules.



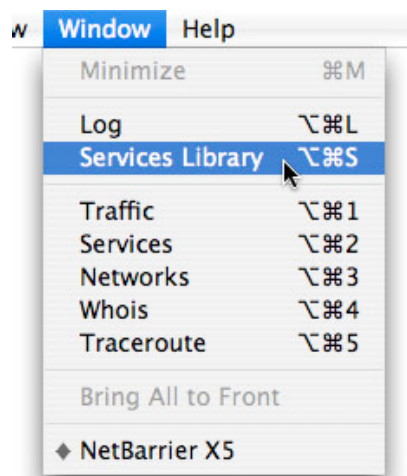
If you wish to further customize the rule, or edit it, see below, Editing Rules.

## Creating Service-Specific Rules Quickly

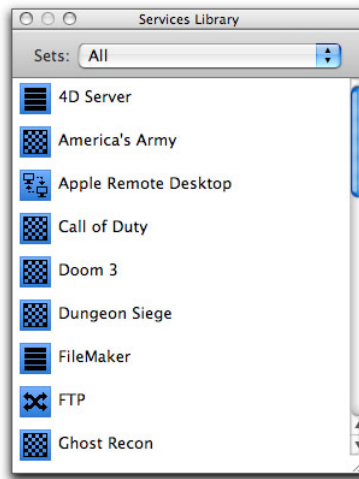
There are two ways to quickly create rules to control information to and from common services and programs. The first is by clicking the + button at the bottom of the Rule list and holding your mouse button down for a second. You'll be able to choose from a popup list of the most common services. A rule governing your selection then appears in the Rules list.



The second way to quickly create service-specific Rules is through the Services Library. To display the Services Library, choose Window > Services Library, or press Option-Command-S.



The Services Library window opens and displays a list of the most common services.

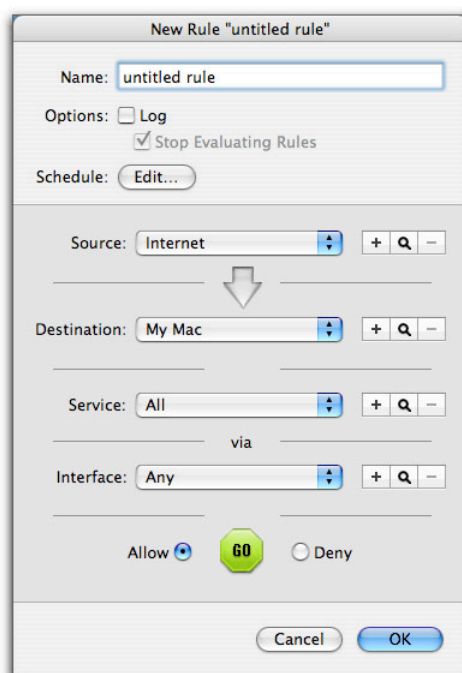


To create a new rule, select the desired service and drag it to the rule list. By default, rules added in this way allow all traffic from your Mac to the Internet, on all interfaces. In other words, the rule doesn't prohibit any activity until you edit its settings, as is described below.



## Creating Rules Manually

You can also create individual rules using the Rule Editor. Click the + button at the bottom of the list of rules and the Rule Editor displays.



NetBarrier X5'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 in seconds. To create a rule, you need to specify details in six areas:

- **Rule Name, Logging and Schedule**
- **Rule Source**
- **Rule Destination**
- **Rule Service**
- **Rule Interface**
- **Rule Action**



## Rule Naming, Logging, Evaluation and Schedules

At the top of the Rule Editor is a field where you can name this rule. Just below it is the Log checkbox. If you check the Log box, an entry is added to the NetBarrier X5 log any time this rule acts; a small red dot to the right of the rule's name in the Rules list indicates that the rule is logged. If it is not checked, this rule is not logged.

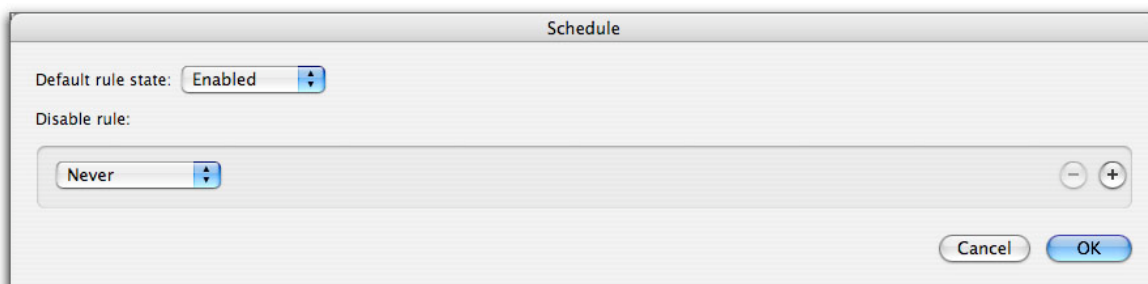


The screenshot shows a rule configuration window. At the top, there is a text field labeled "Name:" containing the text "untitled rule". Below this, under the "Options:" section, there are two checkboxes: "Log" which is unchecked, and "Stop Evaluating Rules" which is checked. At the bottom, under the "Schedule:" section, there is a button labeled "Edit...".

If the Log checkbox is checked, the Stop Evaluating Rules checkbox will be available, and is checked by default. These two settings, in tandem, are a powerful way to troubleshoot a network without hampering its traffic.

**WARNING:** If you can't figure out why some of your rules aren't taking effect, look at the rules above it and ensure that the "Stop Evaluating Rules" checkbox is off for each of them.

To edit the Schedule, click the Edit... button. The Schedule window displays.

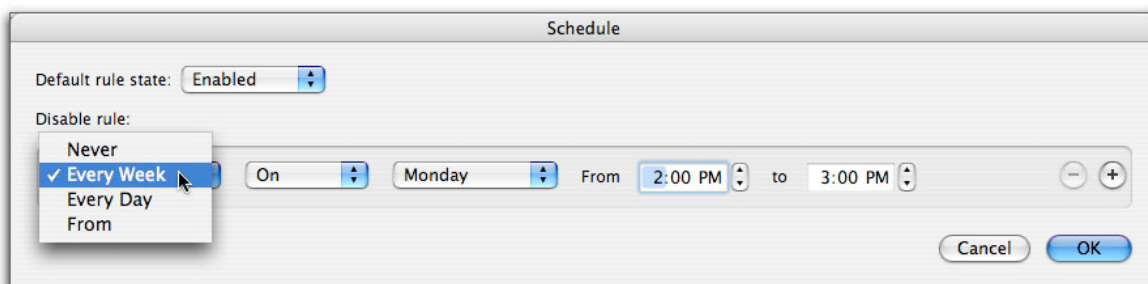


The screenshot shows a window titled "Schedule". It has two main sections. The first section is labeled "Default rule state:" and has a dropdown menu set to "Enabled". The second section is labeled "Disable rule:" and has a dropdown menu set to "Never". To the right of the "Disable rule:" dropdown are two small circular buttons with minus and plus signs. At the bottom right of the window are two buttons: "Cancel" and "OK".

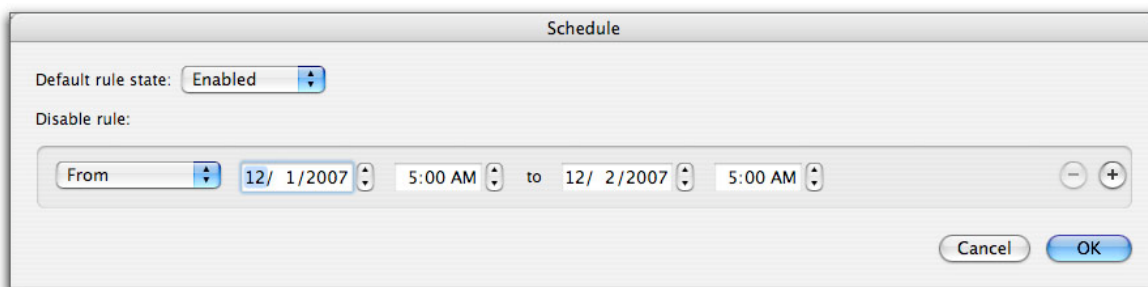
The Default rule state is set to Enabled, which means that your rule is activated. If you set it to Disabled, NetBarrier X5 does not use this rule. You may want to have certain rules active in one configuration, and not another. For more on using configuration sets, see chapter 10, **Preferences and Configurations**.

If your default rule state is enabled, you can set specific times for the rule to be disabled. If your default rule state is disabled, you can set specific times for the rule to be enabled.

When you first create a rule, the Default rule state is set to Enabled and the Disable rule menu is set to Never. In other words, if you make no other changes, the rule will always be active. If you wish to have the rule enabled or disabled at certain times, click the popup menu for either Enable rule or Disable rule, depending on which Default rule state you have chosen, and select one of the time intervals in the list.

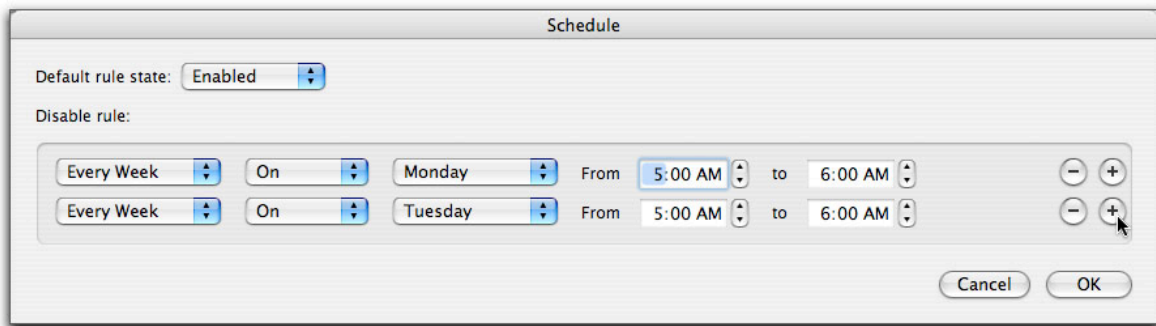


Three options are available in addition to Never. Every Week and Every Day allow you to disable or enable the rule on a recurring basis at fixed times every week or every day, or on specific days of the week. The third option, From, allows you to disable or enable the rule for a specific period of time. In this case you must set the date and time at which you want the rule to start being active in the From field. Set the date and time that you want the rule to expire in the to field.



You can schedule additional times for rules to be enabled or disabled using the + button. For example, if you need a rule to be disabled only on Mondays and Tuesdays, you can set these two days in the Schedule window. To remove a scheduled time from the list, click the – button next to the time line.



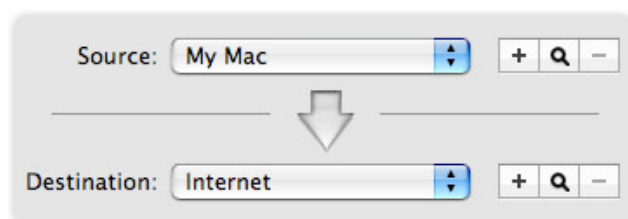


Scheduled rules are displayed with a calendar icon in the rule list. This particular rule also has logging turned on, as is indicated by the small red dot next to its name.

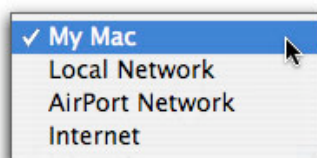


## Rule Sources and Destinations

When defining rules, the Source is the entity that sends data; the Destination is where the data goes. You can choose from a list of four sources and destinations for any rule. However, NetBarrier X5 will not allow you to choose the same source and destination for a given rule.



These four Sources and Destinations are available by default:

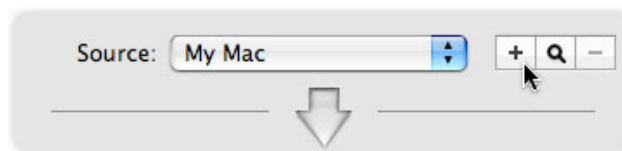


<b>My Mac</b>	Your computer.
<b>Local Network</b>	A local network that your computer is connected to.
<b>AirPort Network</b>	A wireless AirPort network that your computer is connected to.
<b>Internet</b>	The Internet, in addition to any local network you may be connected to; effectively, all networks.

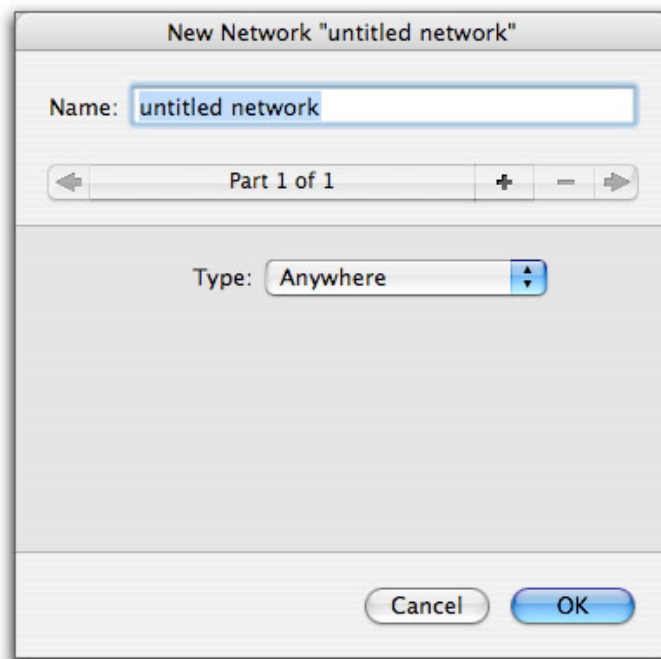
## Creating New Sources and Destinations

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

To create a new source, click the + button to the right of the Source or Destination popup menu. In our example, we'll create a new Source; however, once it's created, it will also show up in the list of possible Destinations.

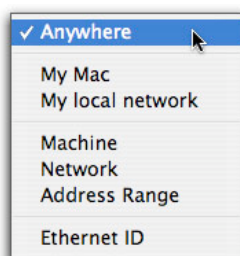


The New Network editor displays.



Enter a name that will help you remember the network. If, for example, you're blocking IP addresses whose last octet is in the range of 100-155, you might name the Source/Destination "IPs from 100-155".

The pop-up menu offers a selection from seven types of network.

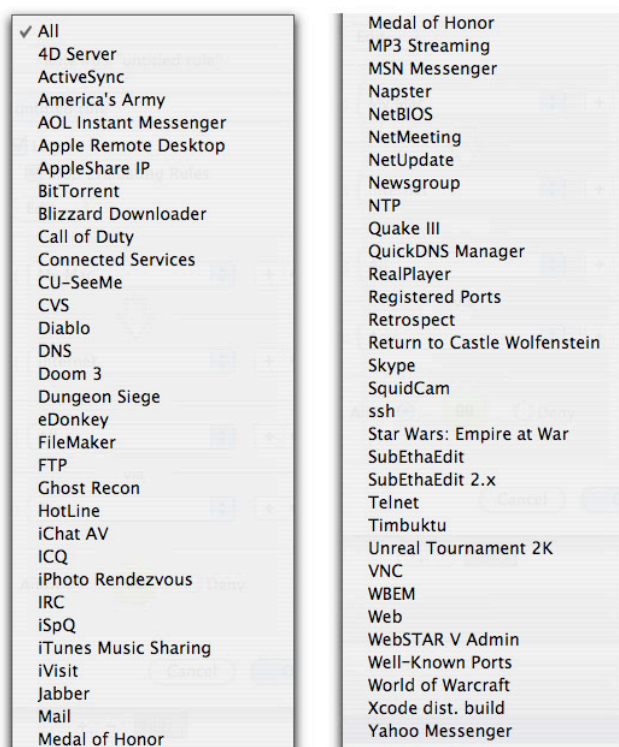


Name	Definition	Address Type
<b>Anywhere</b>	Any network.	None, as this source covers all networks.
<b>My Mac</b>	Your computer.	The IP address(es) of your Mac displays in the Address field, and cannot be changed.
<b>My local network</b>	The local network your computer is connected to.	The IP address(es) of your Mac and subnet mask of your local network display in the Address field, and cannot be changed.
<b>Machine</b>	A specific IP address.	Any IP address. If you enter a domain name, NetBarrier X5 will resolve it to a single IP address.
<b>Network</b>	A specific network.	Any Subnet IP address and Subnet mask. As above, NetBarrier X5 will resolve domain names to a single IP address.
<b>Address Range</b>	A group of IP addresses.	Beginning and ending addresses. NetBarrier X5 will resolve domain names to a single IP address.
<b>Ethernet ID</b>	A single device connected to the network by Ethernet.	An Ethernet ID, as six two-character hexadecimal numbers.

## Rule Services

“Service” refers to a combination of protocol type, port (or ports) used, and protocol-specific criteria. These items, taken together, typically describe a program or class of program that sends and receives information. For example, information sent by the TCP protocol over port 80 using HTTP would be a Web service.

NetBarrier X5 comes with over 50 common services preprogrammed so you can easily stop (or allow) traffic that appears to be of a specific type.



While most preprogrammed Services clearly map to a specific program, some selections in this list, such as “Web” pertain to a class of communications instead. Here are some of those non-specific Services:

<b>Name</b>	<b>Description</b>	<b>Settings</b>
<b>All</b>	All communications, regardless of protocol or port.	All protocols, on all ports.
<b>Apple Remote Desktop</b>	A program that allows an administrator Mac to control another Mac over a network connection.	Port 3283 over UDP.
<b>Connected Services</b>	All TCP communications. A TCP session maintains a connection between computers, so it's always clear that it was initiated by the Mac and can therefore be trusted. By comparison, a UDP session is a series of communications without a "memory" of who initiated it.	All TCP communications, on any port.
<b>FTP</b>	File Transfer Protocol.	TCP, ports 20 or 21.
<b>iChat AV</b>	An instant messaging program with video and sound.	Port 5060 over UDP.
<b>IRC</b>	Internet Relay Chat.	TCP on port 194 for IRC, and all TCP traffic between ports 6665 and 6669, inclusive.
<b>iTunes Music Sharing</b>	A way to share your iTunes music library over your local network.	Port 3689 over TCP.
<b>Mail</b>	E-mail communications.	TCP port 25 for SMTP, port 110 for POP3, port 143 for IMAP4, port 220 for IMAP3 port 389 for LDAP, and port 587 for message submission.
<b>NTP</b>	Network Time Protocol.	UDP on port 123.
<b>SSH</b>	Secure Shell.	TCP on port 22 using SSH.
<b>Telnet</b>	Remote login.	TCP on port 23 using telnet.
<b>VNC</b>	Virtual Network Computing, a graphical	TCP on ports 5900-5999.





	remote-control system.	
<b>Web</b>	Web browsing, for example through a browser such as Firefox.	TCP on ports 80 and 8080 through HTTP, and on port 443 on HTTPS.
<b>Well-Known Ports</b>	A large range of ports with long usage traditions in network communications.	TCP and UDP on all ports from 0 to 1023.

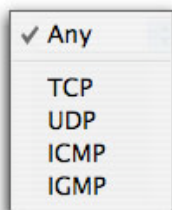
The remaining services are for specific programs or protocols.

Be careful 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.

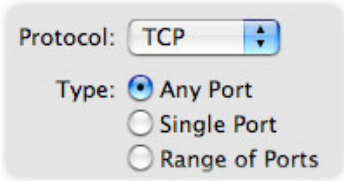

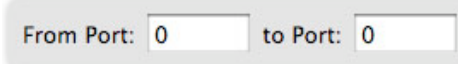
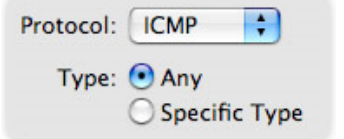
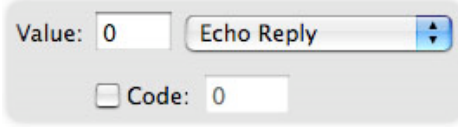


## Creating New Services

Four different protocol suites are available 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, additional options display in the bottom section of the panel, with a list of services that you can select from. The options depend on the protocol you have selected. For more information on these protocols and services, see chapter 12, **Glossary**.

Protocol	Port selections	Options
<b>TCP or UDP</b>  	Any Port	No additional options
	Single Port	 (Popup menu has over 100 options.)
	Range of Ports	
<b>ICMP or IGMP</b>  	Any	No additional options
	Specific Type	 (Popup menu has over 20 options.)

For each of these, an option is available to Allow Broadcast Packets. If checked, packets sent to all computers on a local network are included in this service.



Options: ☒ Allow Broadcast Packets  
☒ Destination Port

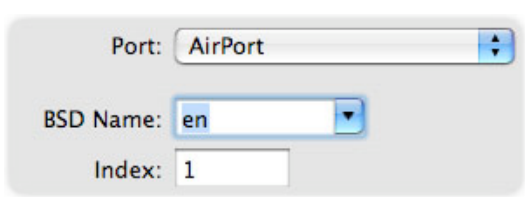
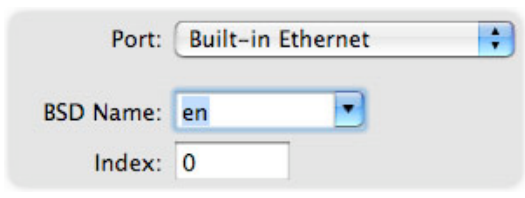
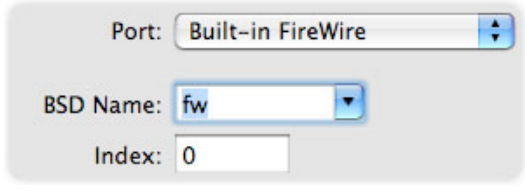
Destination Port is a final option, available only for services utilizing the UDP protocol. If it is checked, packets are filtered according to the function of the Destination Port. If left unchecked, packets are filtered according to the function of the source Port.



## Rule Interfaces

The Interface is the network adapter that the data passes through. This can be an Ethernet card, a wireless AirPort card, a PPP connection or any other type of network interface. You can choose from a list of preprogrammed interfaces that exist on your computer, or you can create your own interfaces.

The Type pop-up menu has two options. The first, Any, uses all available network interfaces. The second, Specific, lists those interfaces that are available to you, depending on your computer's hardware and software. Typical interfaces are:

<b>Airport</b> Wireless networking	
<b>Built-in Ethernet</b> Wired interface commonly used for networking	
<b>Built-in FireWire</b> Wired interface commonly used for peripherals	

The BSD Name and Index number are the identifiers used by the Unix layer of Mac OS X. You can set these manually, if you need to. If other interfaces are present in your Mac, an Other option will also be available.

## Rule 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.

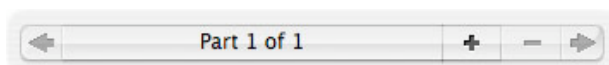


Finally, click OK to add this rule to your NetBarrier X5 firewall rules.

## Multi-Part Sources, Destinations, Services and Interfaces

Rule sources, destinations, services and interfaces can have several parts. You can, for example, dictate that traffic from several specific IP addresses be banned, listing each one separately in a given Source.

When you create or edit a source, destination, service or interface, you see a bar at the top of the window that looks like this:

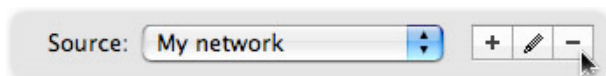


<b>Create a new part</b>	Click the + button.
<b>Move among parts</b>	Click the arrow icons. Note that the text in the middle will tell you where you are, and how many parts exist in total. When you reach the last part, clicking the right arrow takes you back to the first one.
<b>Delete a part</b>	To delete a part, it must be visible. Click one of the arrow icons until the part you wish to delete is displayed. Click the – button, then confirm the deletion in the dialog box that follows.



## Deleting Sources, Destinations, Services and Interfaces

You can delete any sources that you have created. To do so, select the source, and then click the – button.



A dialog box displays, asking if you really want to remove that network. Click Remove to delete the source network, or Cancel if not.

## Working with Rules

### Rule Order

Rules you add to NetBarrier X5's firewall are enacted from first to last, so you need to make sure that your rules are in the correct order to function properly.

#	Name	Interface	Source	Destination	Service	
01	<input checked="" type="checkbox"/> Input	Any	Internet	⇒ My Mac	All	
02	<input checked="" type="checkbox"/> Output	Any	My Mac	⇒ Internet	All	
03	<input checked="" type="checkbox"/> Network	Any	Local Network	⇒ My Mac	All	

In this example, the first rule blocks data coming from the Internet (which includes all networks, even a local network). Rule 3, however, allows traffic from a local network, but since it is in 3rd position, it is not applied; the 1st rule takes 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 drag it to the appropriate position.

#	Name	Interface	Source	Destination	Service	
03	<input checked="" type="checkbox"/> Network	Any	Local Network	⇒ My Mac	All	
01	<input checked="" type="checkbox"/> Input	Any	Internet	⇒ My Mac	All	
02	<input checked="" type="checkbox"/> Output	Any	My Mac	⇒ Internet	All	
03	<input checked="" type="checkbox"/> Network	Any	Local Network	⇒ My Mac	All	

### Editing and Deleting Rules

To edit a rule, select the rule by clicking it, then click the button with the pencil icon at the bottom of the list. The Rule Editor will open, and you can make any changes you want 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.

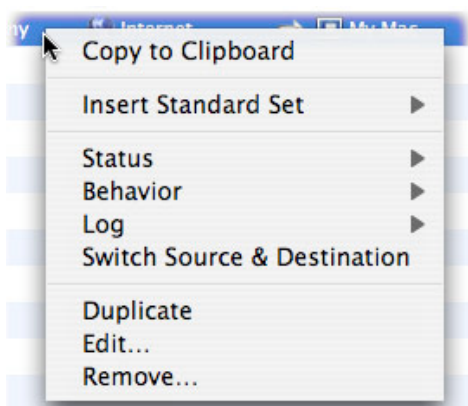
To delete a rule, click the rule in the list of rules, then click the – button at the bottom of the list.



## Using the Rule Contextual Menu

NetBarrier X5 lets you make changes to Firewall Rules quickly through a contextual menu. 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, you can just click the right button of your mouse.)



The menu offers the following options:

<b>Copy to Clipboard</b>	Copies the contents of a Rule to the Mac's Clipboard in plain-text format. You can then paste the rule into a document, where it will look something like this: "#02/ON/Input/Any/Internet -> My Mac/All/Deny" (where slashes are tabs).
<b>Insert Standard Set / Add Standard Set</b>	Insert or add a standard set of rules, from the same selection as is found in simple mode: No restrictions, No network, Client, Local Server, Server only, or Client only.
<b>Status</b>	You can toggle the state of a rule, turning it On or Off. If the rule is scheduled to run at certain times, a check mark is displayed next to Scheduled in the submenu.
<b>Behavior</b>	Toggle the behavior of a rule between Allow or Deny traffic.
<b>Log</b>	Toggle whether the rule records traffic information in the log.



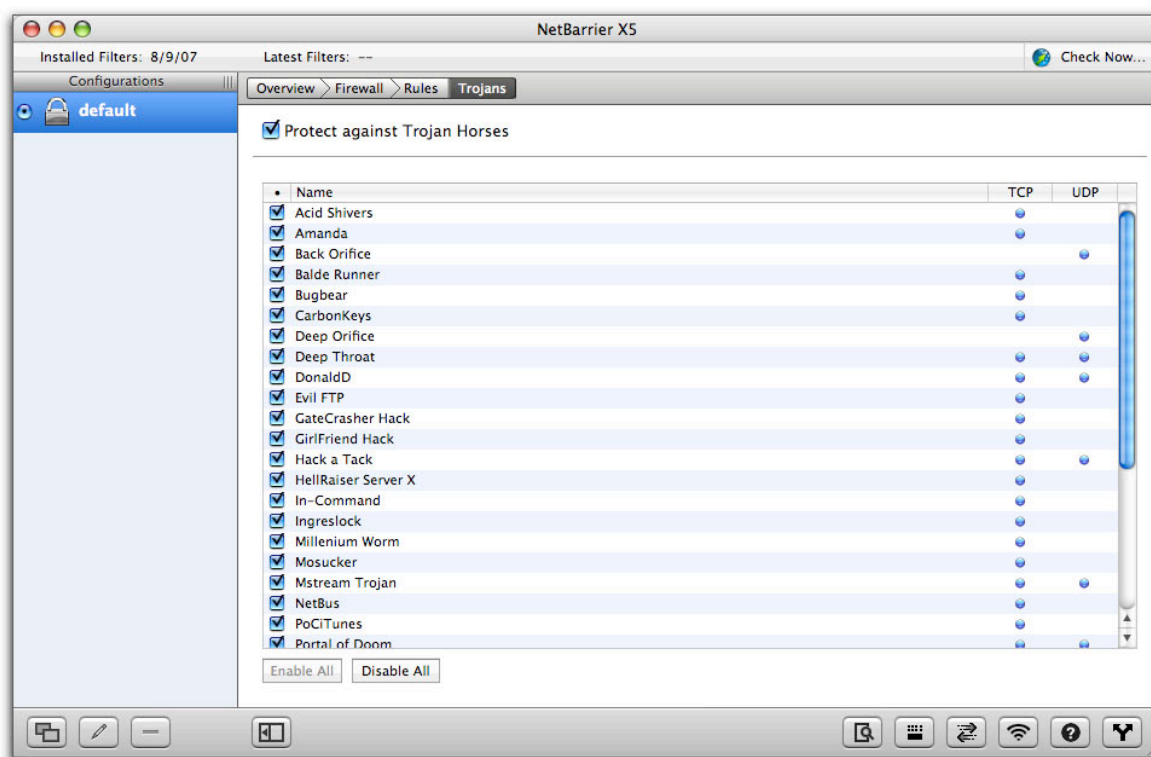


<b>Switch Source &amp; Destination</b>	“Reverses” a Rule, exchanging the source and destination.
<b>Duplicate</b>	Makes a new copy of the Rule.
<b>Edit...</b>	Opens the Rule Editor for the indicated Rule.
<b>Remove...</b>	Deletes the Rule.



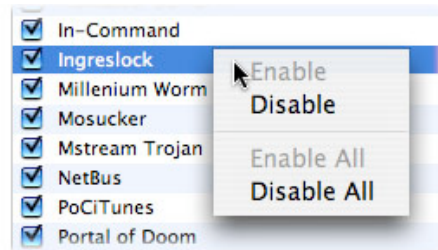
## Trojan Horse Protection

Trojan horses are applications that are surreptitiously installed on your computer, either by virus-laden attachments you receive with e-mail messages, or by programs you download or buy on disc. In some cases, programs install a specific type of Trojan horse, known as spyware, which sends personal information to a server. Since the connection is made *from* your computer, it is generally trusted. But NetBarrier X5 knows how to spot the actions of the most common Trojan horses and stop them in their tracks. There have been cases where such programs have sent information about users' browsing habits to a central server; other Trojan horses open "back doors" in your computer that allow hackers to take control of it or delete files.



To turn on Trojan horse protection, click the Protect against Trojan Horses checkbox, then click the checkboxes of individual Trojans to select them. The Enable All and Disable All buttons at the bottom are handy shortcuts that select or deselect all checkboxes at once.

You can also enable Trojan blocking for an individual Trojan horse, or for all Trojan horses, by holding down the Control key on your keyboard and clicking on the name of a Trojan. A contextual menu displays.



## **6—The Four Lines of Defense: Privacy**



NetBarrier X5's privacy filters examine both incoming and outgoing packets, looking for specific types of data. There are several filters, separated into two sections: Data, and Surf.

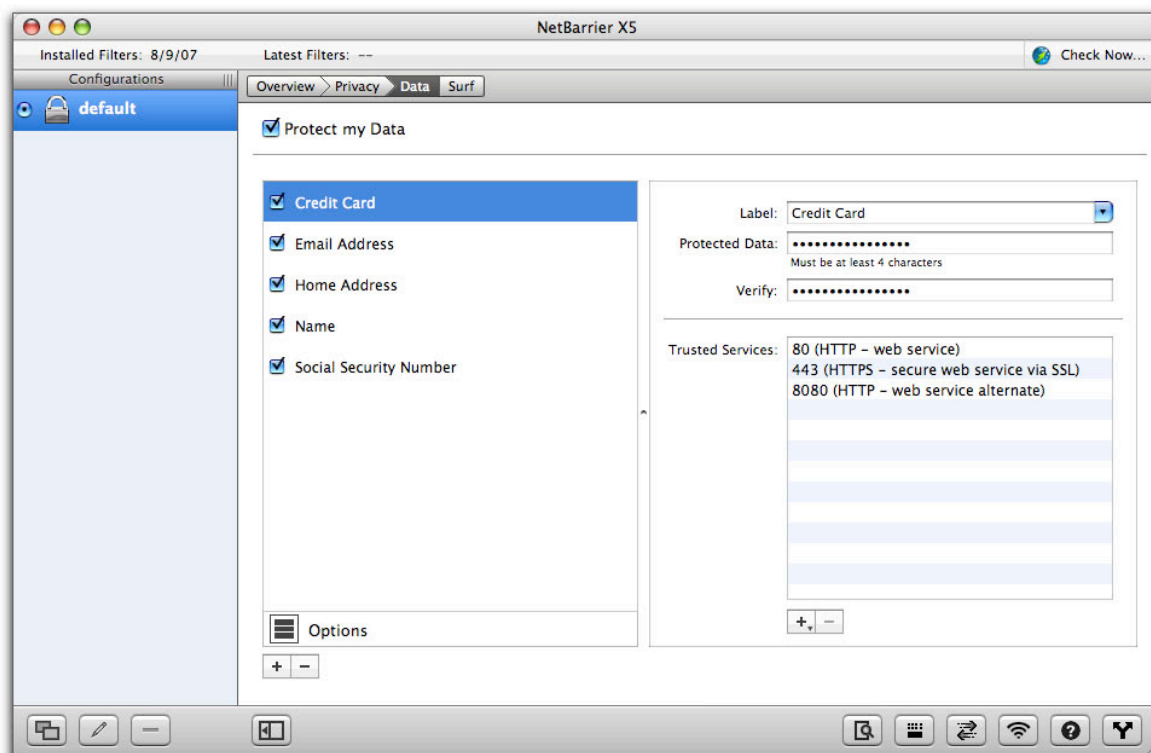


## Data Filter

The data filter ensures that any sensitive information you choose to protect cannot leave your Mac 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 X5's data filter checks each outgoing packet to make sure that no documents containing this information are sent. Not only does this protect you from accidentally sending documents containing this information, but it also protects against anyone who has network access to your Mac from taking copies of them.

Remember that, if your computer is accessible across a network and other users have file-sharing privileges, they may be able to copy your files.

Here is the data filter window with some sample data in place:



## How the Data Filter Works

NetBarrier X5 examines all data packets that are sent from your computer to the Internet or a local network. If any of the data you indicated in the filter is found, the packet is blocked.

The data filter only blocks data that corresponds *exactly* to the text you indicated, including punctuation and case. For example, if you entered your credit card number as protected data, NetBarrier X5 prevents it from leaving your computer and can warn you in several ways if you choose. But if you enter the same number in a secure web page, your browser encrypts this number. The data therefore no longer corresponds to the protected data, and is sent. The same is true for data that is encoded in other manners, or compressed.

In extremely rare instances, the data filter stops data that matches your criteria but not your intention. For example, graphic files (such as images on web sites) are essentially just strings of data thousands of characters long. It's possible that a graphic file could coincidentally contain a



piece of data you want protected, and would therefore be blocked by the data filter. (If you decided to block the name “Jodie”, for example, a graphic file containing the string “Cg34gb\$sEbOJodie8%” would be stopped.) If you find yourself unable to send or receive a specific piece of information, try turning off the data filter momentarily, then turn it on after the information has been transferred.

Click the “Protect my Data” checkbox in the upper-left corner to enable the data filter. You can turn it off at any time, for example to temporarily allow your protected data to be sent.

## **What to Protect**

The data filter includes labels for the five most common types of sensitive information:

- **Credit Cards**
- **E-mail Addresses**
- **Home Addresses**
- **Name**
- **Social Security Number**

However, these labels are merely for convenience. NetBarrier itself doesn’t treat these types differently from one another, or differently from any additional types you might decide to enter later—for example, “Phone Number”, “Children’s Names” or “Passwords”.



## Adding Data to the Filter

To add data to the filter, click the + button below the Options icon. A new entry named “untitled data” appears in the filter list.

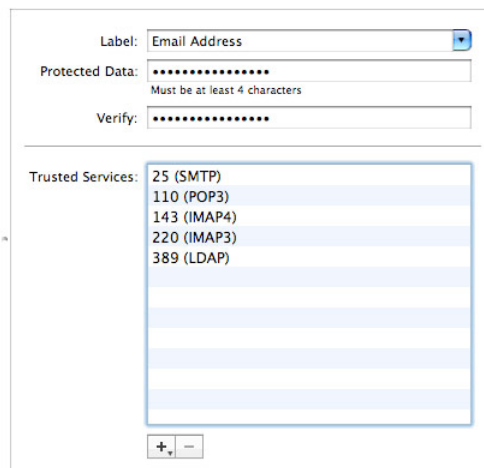
The screenshot shows the Intego NetBarrier X5 interface. On the left, a list titled 'untitled data' is visible. Below the list is an 'Options' icon (three horizontal lines) and a '+ -' button. On the right, the configuration panel for the selected entry is shown. It includes a 'Label' field with a dropdown menu currently set to 'untitled data'. Below this are 'Protected Data' and 'Verify' text input fields. A note under the 'Protected Data' field states 'Must be at least 4 characters'. At the bottom of the configuration panel is a 'Trusted Services' section with a list of services and a '+ -' button.

Enter a description for your protected data in the Label field, or choose it from the popup menu: you'll notice that it is echoed in the filter list. Then enter the actual data you wish to protect in the Protected Data field. This text is hidden so nobody watching over your shoulder or with later access to your Mac can see it. You must enter the data a second time in the Verify field. If the Protected Data and Verify fields do not match, a window displays, giving you the choice of either resetting the protected data, in which case you will have to retype both data fields, or clicking OK. If you click OK, you will have to retype the verified protected data.

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 does 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 Trusted Services section allows you to choose to block data for all but the selected services. To do this, click the + button. Then, type the port number of the service. Alternately, click the + sign and hold the mouse button down for a few seconds: you'll be able to choose from a popup list of common services. (Some of them, such as Mail in the example below, add several ports in one go.) You can add a single port number, or a range of port numbers, for example 110-123. Data to this port (or these ports) will not be blocked. To add another service, repeat the above operation. You can add as many services as you wish.

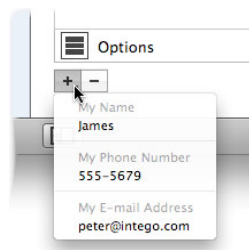


The screenshot shows a configuration window with the following fields and sections:

- Label:** A dropdown menu currently set to "Email Address".
- Protected Data:** A text field containing a series of asterisks. Below it, a note says "Must be at least 4 characters".
- Verify:** A text field containing a series of asterisks.
- Trusted Services:** A list box containing the following entries:
  - 25 (SMTP)
  - 110 (POP3)
  - 143 (IMAP4)
  - 220 (IMAP3)
  - 389 (LDAP)
- At the bottom of the list box are two buttons: a "+" button and a "-" button.

You can also drag and drop services from the Services Library. This is particularly helpful if you do not know the specific port numbers you wish to add to the list. To display the Services Library, choose Window > Services Library, or press Option-Command-S. Select the desired service, then drag it onto the Trusted Services list.

You can also add certain personal information from your card in Apple's Address Book, if you have filled one out. To do this, click and hold the + button, and you'll see three items: My Name, My Phone Number and My E-mail Address. Select one of these to add it as protected data.

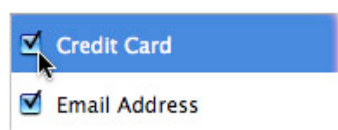


Once you have finished entering this information, your data is protected. You can go back at any time to edit the data item by clicking on it in the Data Filter list and changing information in its pane to the right.

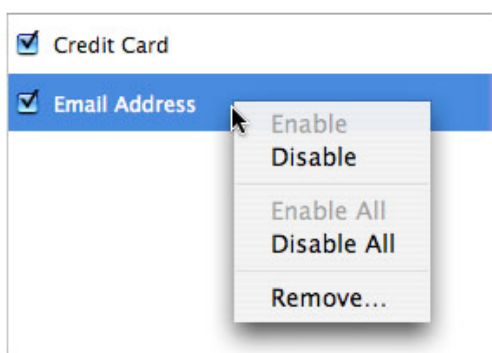


## Activating, Deactivating and Deleting Data Items

Each item of protected data appears on a line in the data filter window. A checkbox 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 that data over the Internet or a local network, you must uncheck the checkbox for the item in question, or deactivate all the data filters by unchecking “Protect my Data” as was mentioned earlier.



You can also activate or deactivate Data Filters for individual protected data items, or for all protected data items, by holding down the Control key on your keyboard and clicking the name of a data item, or by clicking with your right mouse button. A contextual menu displays.

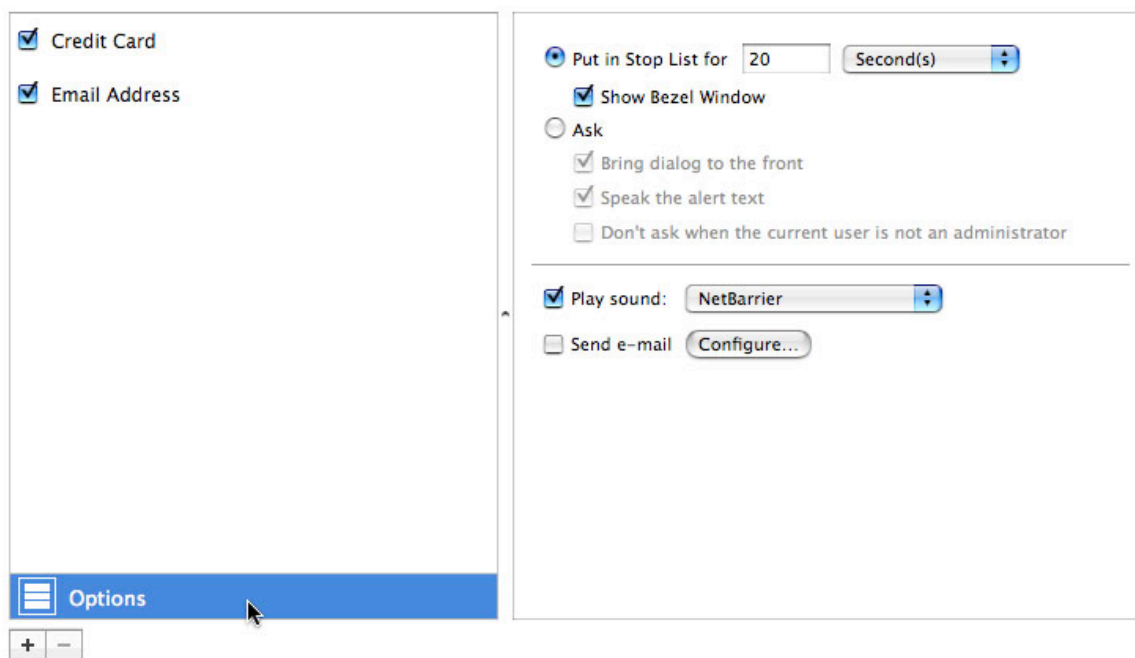


Select Disable to disable protection for the selected data item, or select Disable All to disable protection for all data items. (If the selected item in the above example had been disabled already, the choices for Enable and Enable All would be available.)

If you'd like to permanently remove the item from the Data Filter list, either Control-click as described above and choose Remove..., or select the data item and click the – button. In either case, a dialog box asks you to confirm that you really want to remove the data item.

## Data Filter Options

When protected data attempts to enter or leave your Mac, you have several options on how you're notified, and what to do about future attempts. To see these options, click the Options button in the lower-left of the data screen. Changes to data filter options affect all data filters.



To understand these options, see chapter 9, **Understanding Alerts**.

## Surf Filters

NetBarrier X5 includes three kinds of filters that help you control the information your Mac sends and receives while surfing the Internet:

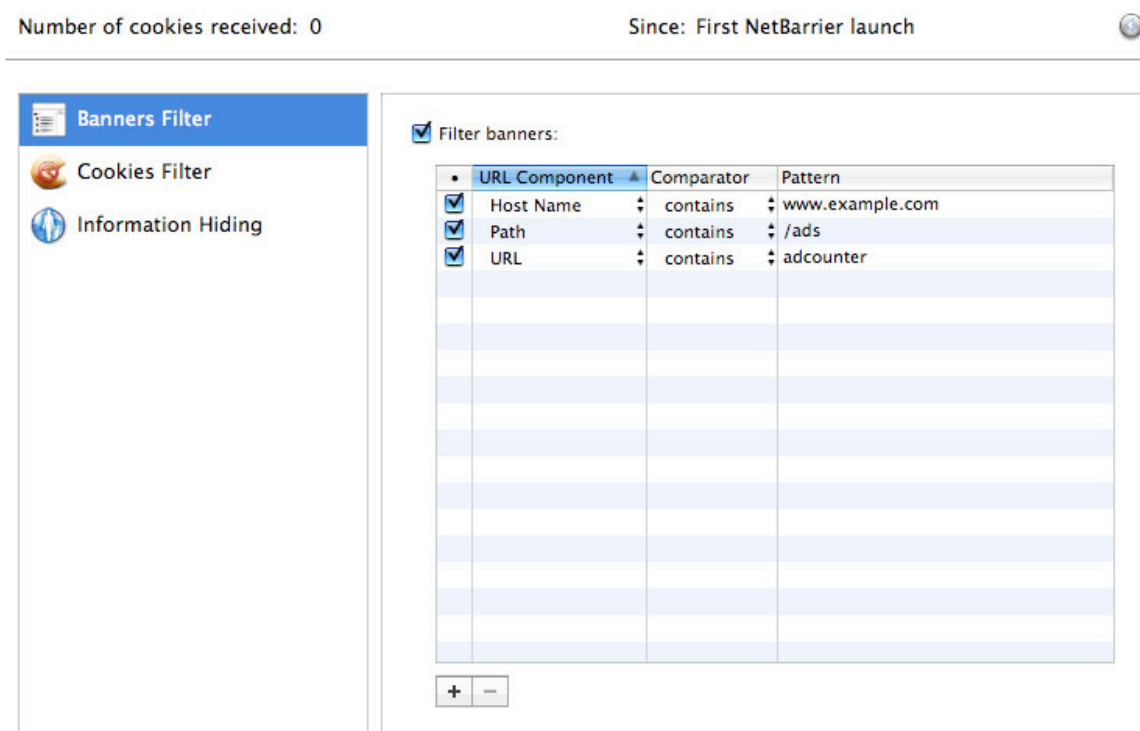
- The **Banners Filter** hides ad banners on web sites that you visit;
- The **Cookies Filter** prevents your Mac from sending certain information to web sites that tracks your movements;
- The **Information Hiding** filter cloaks certain facts about your Mac, web browser, last web site visited and iTunes account.

Surf filters affect all computer programs that communicate using HTTP (see chapter 12, **Glossary**). Web browsers are the most common programs using HTTP, but it's also part of iTunes, RSS newsreaders, and a lot of other software that has Internet browsing capabilities. If you have unexpected difficulties with such programs—downloading music through iTunes, for example—try disabling the surf filters temporarily.



## Banners Filter

The Banners Filter is a list of rules that NetBarrier X5 uses to filter unwanted web material such as graphic ads known as “ad banners”, helping you surf much faster and with less distraction. NetBarrier X5 blocks these ads, and replaces them with tiny, transparent graphics. NetBarrier X5 contains an internal list of ad banner strings to filter, but you can also add custom strings to filter more ads you encounter when surfing. Here is the banners filter window, populated with sample data:



To enable the banners filter, click the “Filter banners:” checkbox.

## Adding Rules to the Banners Filter

The Banners filter already contains a set of rules, which is kept up-to-date when you update your NetBarrier X5 Filters using NetUpdate X5, but you can easily add your own. To add rules to the banners filter, click the **+** button. A new line is added to the banner list for you to edit.

☒ Filter banners:

<input type="checkbox"/> URL Component	Comparator	Pattern
<input checked="" type="checkbox"/> Host Name	contains	www.example.com

The list contains four columns: a checkbox, URL Component, Comparator and Pattern. The pattern, obviously, is how you define what you want blocked.

The URL Component popup menu has three options. NetBarrier X5 searches each banner filter in the selected element:

<b>Host Name</b>	The Internet domain—that is, anything in a Web address between the http:// and the first “/”. The default value is www.example.com. Note that such an entry wouldn’t block (for example) http://forums.example.com; to block both, you should simply enter example.com.
<b>Path</b>	Any part of the URL following the host name, such as /ads/ in http://www.example.com/home/graphics/ads/6542.html.
<b>URL</b>	The entire URL, such as http://www.example.com/home/graphics/ads/6542.html.

The **Comparator** popup menu lets you choose whether content should be blocked based on an exact match (“is”) or when your text matches at least a portion of the URL (“contains”).

## ***Activating or Deactivating Banner Rules***

Each banner rule appears on a line in the banner window. A checkbox 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. To stop blocking certain banners, uncheck the checkboxes for the banners in question.

<input checked="" type="checkbox"/>	URL Component	Comparator	Pattern
<input checked="" type="checkbox"/>	Host Name	contains	www.example.com
<input checked="" type="checkbox"/>	Path	contains	/advertising/
<input checked="" type="checkbox"/>	Path	contains	Ads

You can also enable ad banner blocking for an individual ad banner rule, or for all ad banner rules, by holding down the Control key on your keyboard and clicking on the name of an ad banner rule. A contextual menu displays.

<input checked="" type="checkbox"/>	URL Component	Comparator	Pattern
<input checked="" type="checkbox"/>	Host Name	contains	www.example.com
<input checked="" type="checkbox"/>	Path	contains	/advertising/
<input checked="" type="checkbox"/>	Path	contains	Ads

Enable

Disable

Enable All

Disable All

Remove...

Select **Disable** to disable protection for the selected ad banner rule, or select **Disable All** to disable protection for all ad banner rules. (If the Rule was already disabled, the “Enable” and “Enable All” choices would be available.)

To remove banner rules, either choose the **Remove** option in the contextual menu or click the – button below the list of banner rules.



Note that the banners filter doesn't know what content it's filtering, only that the URL matches the criteria you specified. Therefore, you might occasionally have difficulty seeing information on Web pages that coincidentally matches your criteria, but isn't actually an ad banner. If this is the case, try turning off the banners filter temporarily. You can do this from the NetBarrier X5 application, or from the Intego menu in your menubar.

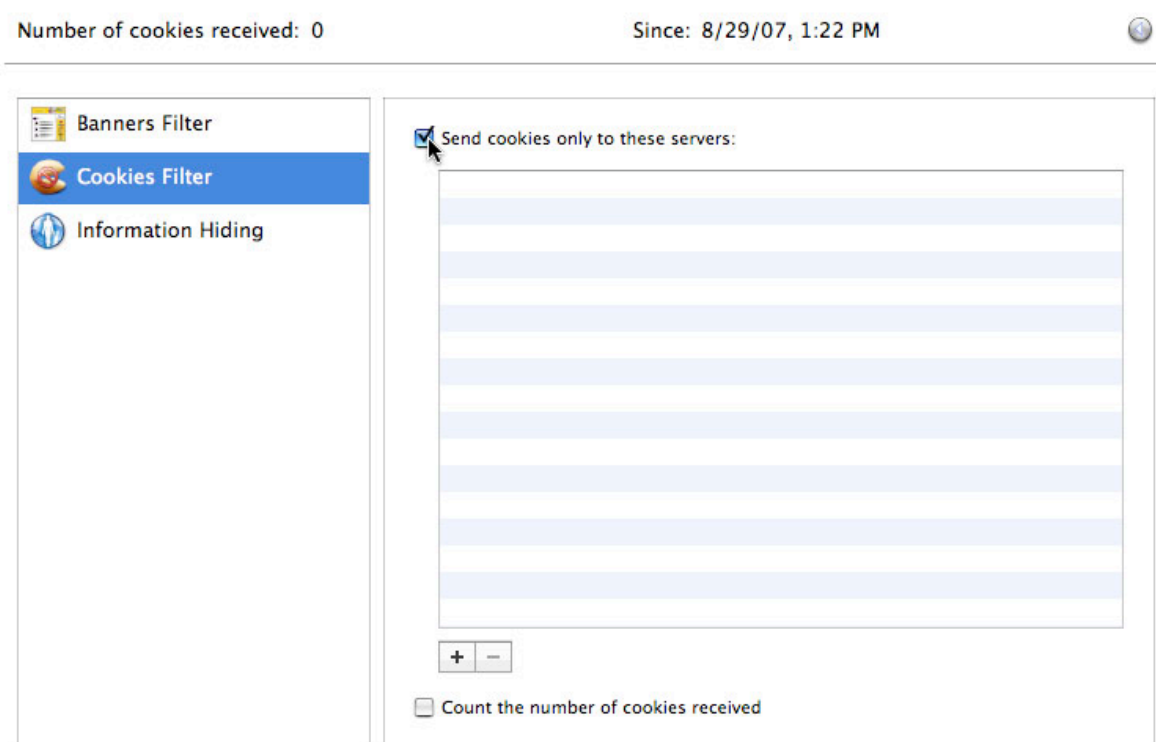


## Cookies Filter

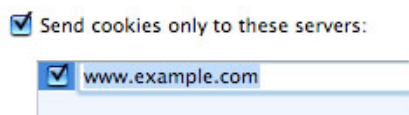
NetBarrier X5 includes a cookies filter, which prevents your Mac from sending tracking information, called “cookies”, to all Internet sites except for those you specify.

The cookies filter is useful when you want to surf in extreme privacy, only telling a few, trusted sites about your actions. However, many Web sites—particularly those that require a password—won’t work correctly unless you specifically include them in the list of trusted sites.

To turn on the cookies filter, click the “Send cookies only to these servers:” checkbox.



To add a server to the Cookies Filter list, click the + button at the bottom of the list. A dummy server address (www.example.com) displays: change it to the site of your choice.



Erase the dummy server address and enter the name of the server you want to allow cookies to be sent to. You can also drag a URL from a browser, or even a URL in text format, to this field to add it to the list.

As with the banners filter, you can enable or disable individual cookies filters by clicking the checkboxes next to them, or by holding down the Control key while clicking on them and using the contextual menu, or clicking with your right mouse button.

To remove cookies that are already on your Mac, see the separate manual for Intego Washing Machine that accompanies NetBarrier X5.



## Cookie Counter

NetBarrier X5 can also count the number of cookies for all users on your Mac, if you check the **Count the number of cookies received** checkbox at the bottom of the cookies filter screen.

☒ Count the number of cookies received

A display at the top of the screen tells you how many cookies your Mac has accepted since you turned on, or last reset, the counter. At any time you can reset the counter to zero by clicking the small arrow in the upper-right corner.

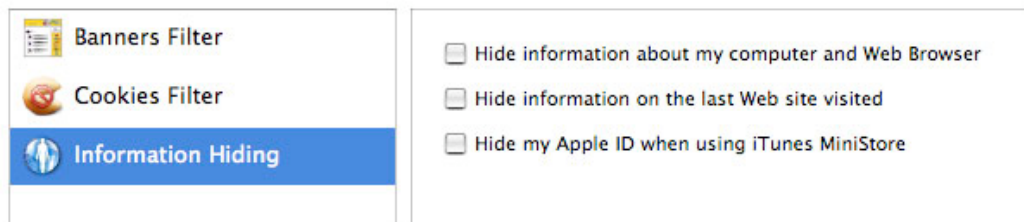
Number of cookies received: 21

Since: 8/29/07, 1:22 PM



## Information Hiding

All Web browsers are set to reply to requests from Web sites, telling which platform you are using (Mac, Windows, Linux, etc.) and which browser and version you are using. This information can help the site deliver information in the best way, for example by turning on features that only work for the Web browser that you're using. On the other hand, some sites limit access by platform and browser, in some cases forbidding access to everybody using a Mac. NetBarrier X5 can hide some information concerning your computer, possibly permitting access where it would otherwise be denied.



NetBarrier X5 can reply to these requests, and send only generic information. For example, your computer will reply to the Web site that you're using a Netscape or Mozilla browser, but with no version number or platform. To do this, check the **Hide information about my computer and Web Browser** checkbox.

Some sites also keep track of the last site you visited. Again, this can improve your Web experience if, for example, a shopping site offers you discounts if you come from a specific Web site. But unscrupulous sites might use this feature to follow your browsing habits in ways you don't want. By checking the **Hide information on the last Web site visited** checkbox, NetBarrier X5 prevents your Mac from replying to this type of request.

Finally, if you use iTunes and display the iTunes MiniStore, iTunes sends your Apple ID to Apple's servers each time you click on a song. To block this, check **Hide my Apple ID when using iTunes MiniStore**. This will not prevent you from purchasing songs from the iTunes Store, but will prevent iTunes from sending information that links your browsing to your iTunes Store account.

## **7—The Four Lines of Defense: Antivandal**



## Antivandal

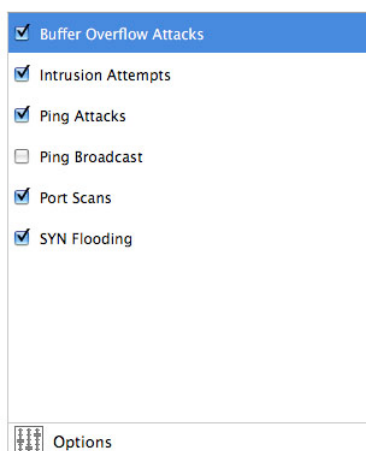
NetBarrier X5's Antivandal watches over data entering your Mac and filters it, looking for signs of intrusion. This filtering is transparent—the only time NetBarrier X5 will show itself is if it detects suspicious data. If this occurs, an alert displays. Otherwise, Antivandal silently monitors your computer's network activity at all times.

The Antivandal section has two parts that control how data enters your computer: Policy and Anti-Spyware. The Stop List and Trusted Group store specific hosts, or IP addresses, that you deem trustworthy or not.



## Policy

The Antivandal panel provides policy tools to prevent six types of intrusions.



<b>Buffer Overflow Attacks</b>	Attacks that may occur when certain software has flaws in the way it handles memory.
<b>Intrusion Attempts</b>	Attempts to access your Mac through a preset number of incorrect password requests within a given period of time. Different settings are available for AppleShare IP (ASIP), FTP, HTTP, IMAP, POP and SMTP.
<b>Ping Attacks</b>	Your Mac receives a number or frequency of ping requests so great that responding would cause a strain on your Mac.
<b>Ping Broadcasts</b>	Ping requests to broadcast addresses, where a single ping is multiplied throughout your local network.
<b>Port Scans</b>	Attempts by remote computers to search your Mac's ports for vulnerabilities. You may want to leave this unchecked if your computer is functioning as a server.
<b>SYN Flooding</b>	Multiple TCP requests sent by an attacker who then doesn't complete the final stage of the exchange, causing the target computer to consume resources.



Clicking the checkbox next to each of these enables or disables protection for that intrusion type. Clicking on the name of the intrusion type shows the notification and action policies for that intrusion type. Here, for example, we see the policy for Buffer Overflow Attacks.

The screenshot displays the configuration window for NetBarrier X5, specifically the 'Policy' tab for 'Buffer Overflow Attacks'. On the left, a list of intrusion types is shown with checkboxes: 'Buffer Overflow Attacks' (checked), 'Intrusion Attempts' (checked), 'Ping Attacks' (checked), 'Ping Broadcast' (unchecked), 'Port Scans' (checked), and 'SYN Flooding' (checked). The right pane is titled 'Policy' and contains several settings: 'Put in Stop List for' is set to '∞' with a 'Permanent' dropdown; 'Show Bezel Window' is unchecked; 'Ask' is selected with a radio button, and its sub-options are 'Bring dialog to the front' (checked), 'Speak the alert text' (unchecked), and 'Don't ask when the current user is not an administrator' (unchecked); 'Play sound:' is checked with a dropdown set to 'NetBarrier'; and 'Send e-mail' is unchecked.

These options are described in full in chapter 9, **Understanding Alerts**.

While an intrusion type is selected, clicking on the Advanced tab in the right-side pane brings up additional options that are specific to that intrusion type. These are:

<b>Buffer Overflow Attacks</b>	No advanced settings.
<b>Intrusion Attempts</b>	You can separately set the number of incorrect password attempts permitted for AppleShare IP (ASIP), FTP, HTTP, IMAP, POP and SMTP.
<b>Ping Attacks</b>	Ping flood sensitivity, measured in milliseconds (ms) permitted between ping attempts. If your computer is on a network, it is normal that your network administrator ping your computer from time to time. But if your computer is isolated pings are rarer. One exception is if you have a DSL or cable connection; your ISP might ping your computer to check if it is on-line.
<b>Ping Broadcasts</b>	No advanced settings.
<b>Port Scans</b>	Sensitivity is adjustable as a slider from low to high in increments according to an internal calculation.
<b>SYN Flooding</b>	Sensitivity, measured in number of attempted connections allowed per second.



## Options

Additional filtering options are available within the Options panel of the Policy tab. Click Options to adjust these settings.

Filtering \_\_\_\_\_

- ☐ Stealth Mode (prohibit ping replies)
- ☐ Stop unknown protocols
- ☐ Deny Apple Remote Desktop Control
- ☐ Allow PORT mode FTP transfers

E-mail \_\_\_\_\_

Settings: [Configure...](#)

Policy \_\_\_\_\_

- ☐ Use same policy for all types of protection

<b>Stealth mode (prohibit ping replies)</b>	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.
<b>Stop unknown protocols</b>	If this is checked, NetBarrier X5 automatically blocks any unknown protocols.
<b>Deny Apple Remote Desktop Control</b>	If this is checked, NetBarrier X5 blocks all access to your Mac by Apple Remote Desktop software.
<b>Allow PORT mode FTP transfers</b>	If this is checked, you will be able to make FTP transfers when functioning in Client Only firewall mode.

The second part of this screen allows you to be notified by e-mail when an attack is detected. See chapter 9, **Understanding Alerts** for more information.



## Unifying Policy Options

Each type of intrusion has settings that determine how you're alerted and what actions are taken when that type of intrusion is detected. These settings are fully explored in chapter 9, **Understanding Alerts**.

The “Use same policy for all types of protection” checkbox unifies all notifications and actions. With this box unchecked, you could (for example) choose to receive an e-mail when a buffer overflow attack is detected, but only see an alert box when an intrusion attempt occurs. Checking the box tells NetBarrier X5 that you want to get the same sort of response no matter what sort of intrusion occurs.

When you turn on this option, you'll see a dialog box that asks which settings should become the model that other intrusion types will follow.



## Anti-Spyware

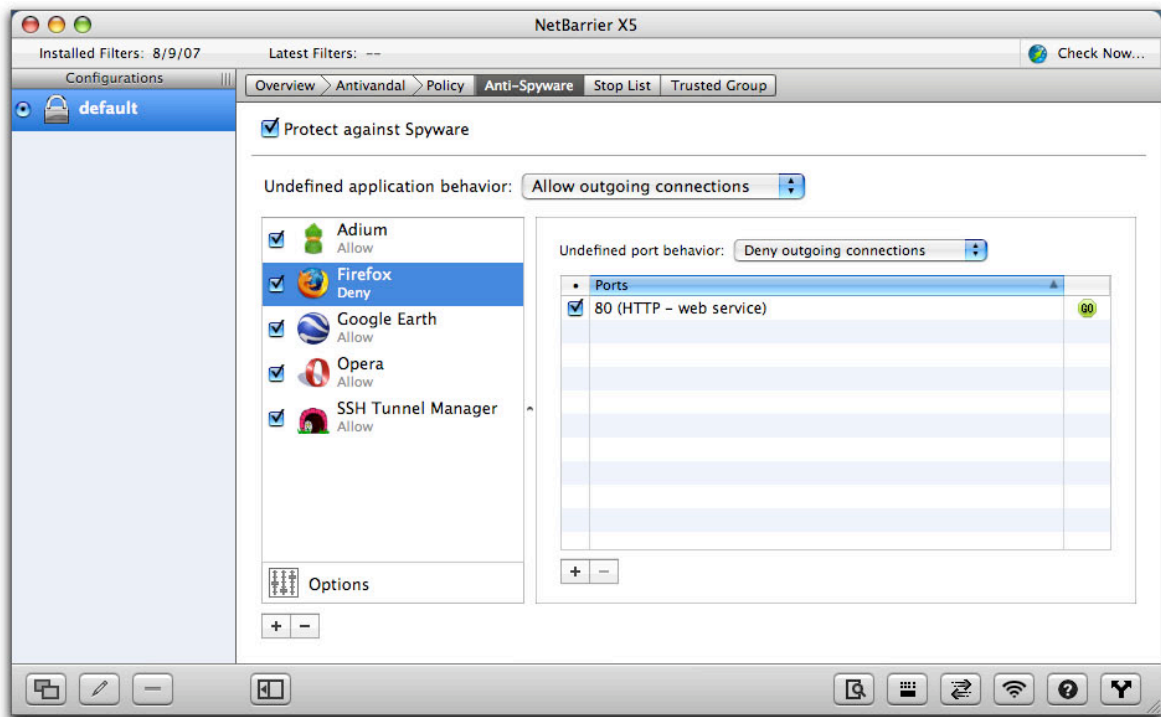
NetBarrier X5 lets you control access from your Mac to the Internet and local networks by individual applications. While your firewall settings may allow general network access, the Anti-Spyware tab lets you choose how NetBarrier X5 reacts when specific applications try to access the network. This helps you in two ways:

- If you wish to prevent users from accessing the network with specific applications, you can block them in the Applications tab.
- If an application attempts to connect to the network behind your back, NetBarrier X5 stops it in its tracks, alerts you, and waits for you to decide whether to allow it to do so or to block it.

Your Mac has many applications that access the Internet or other networks, including web browsers, e-mail programs, FTP (file transfer) programs and instant messaging applications. But there may also be programs that connect to the network without telling you, in order to verify the serial numbers of software installed on your computer, collect and send personal information without your awareness, or open a backdoor on your Mac to provide access to hackers or vandals. NetBarrier X5 notifies you of such attempts and allows you to decide whether to allow them.

To turn on Application Blocking, check the Protect against Spyware checkbox in the upper-left corner of the Anti-Spyware window.



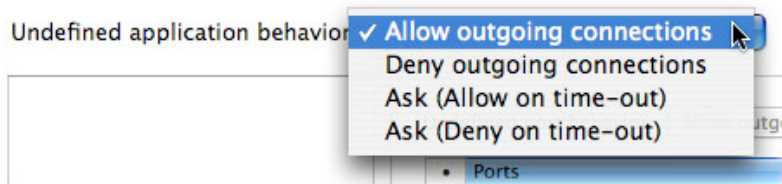


Anti-Spyware works by first asking you to make a list of applications for which you want to apply settings. These are known as “defined” applications, while all those that aren’t on the list are “undefined”. In the example above, Google Earth is defined, while Internet Explorer (which isn’t on the list) is undefined.

Once you’ve built this list, you can finely control communications from defined applications and set a general policy for communications from undefined applications. Two typical configurations would be:

- You run a computer lab and want people to be able to send e-mail using Apple’s Mail program, but not browse the Web or play network games. You would define Mail as Allowed, but deny all outgoing connections from other programs.
- You suspect that an application you downloaded to your Mac is sending unauthorized communications, perhaps from hidden spyware built into the program. You define that program and deny all communications from it, but allow all communications from undefined applications.

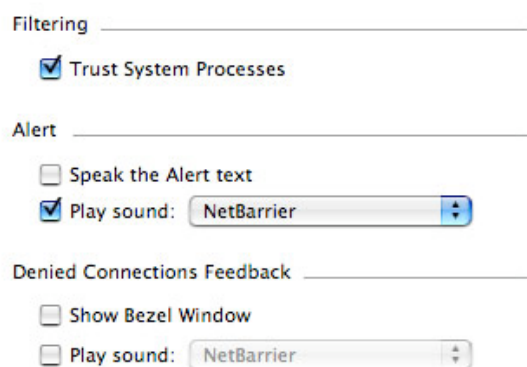
Four behavior options are available for undefined applications:



<b>Allow outgoing connections</b>	NetBarrier X5 allows all applications to access the Internet or any other network. However, any firewall rules you may have defined concerning access to and from specific ports still function. For example, if an FTP program attempts to connect to a Web page, NetBarrier X5 does not block the application, but if you have set up a firewall rule blocking port 20, the standard FTP port, the data does not go through. If the FTP program attempts to make a connection to a different port, it is not blocked.
<b>Deny outgoing connections</b>	NetBarrier X5 blocks all access to the Internet or other network. This supercedes all firewall rules you have defined.
<b>Ask (Allow on time-out)</b>	NetBarrier X5 asks you for each application that attempts to connect to the Internet or other network. If you do not respond within 90 seconds, the application will be allowed to access the Internet, but only this time.
<b>Ask (Deny on time-out)</b>	NetBarrier X5 asks you for each application that attempts to connect to the Internet or other network. If you do not respond within 90 seconds, the application will be denied access, but only this time.

## Options

The Options button in the lower-left corner of the Anti-Spyware pane allows you to configure some general Anti-Spyware settings.



The one option that's special to Anti-Spyware is Trust System Processes, which allows communications from the many parts of Mac OS X itself that request Internet or network access. Such requests might relate to printing services, domain name resolution, checks for software updates or clock synchronization. These are requests that come from parts of Mac OS X, not separate applications. To trust these processes, and not be asked when they attempt to connect to the Internet or network, check the Trust System Processes checkbox.

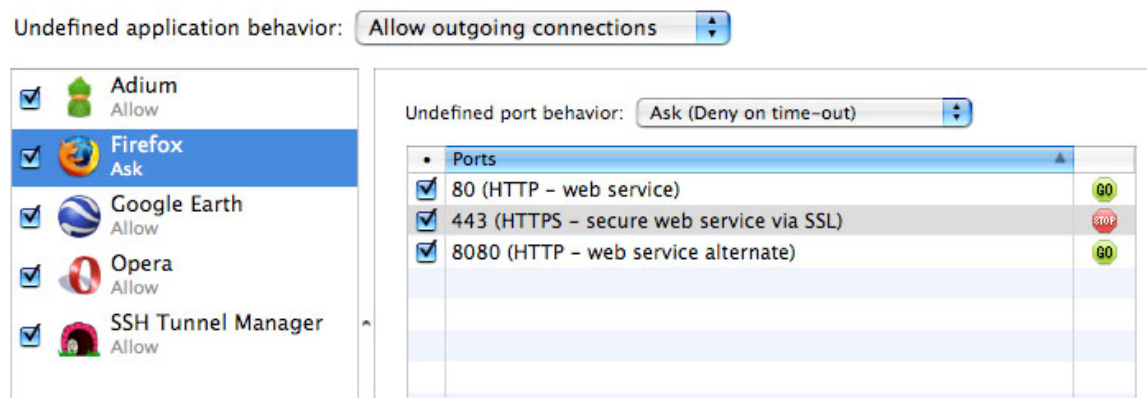
For details on other Anti-Spyware options, see chapter 9, **Understanding Alerts** for more information.



## Applications: Adding, Removing and Changing Settings

After you have chosen to allow or deny network access to undefined applications, define an application by clicking the + button, then navigating through the Mac OS X dialog box to the application itself to add it. Repeat the process for all the applications you wish to add. (To remove an application from the list, click it and then click the – button at the bottom of the application list.)

You can then change the settings for each application to allow or block communications from the application as a whole, or over specific ports. Similar to the process above, where you specify what should happen when undefined applications attempt outgoing communications, here you define what you'd like to happen when a specific application attempts communication from an undefined port. Then you define a list of ports for that specific application that are exceptions to the general rule.



In the above example:

- Five applications (listed on the left) have specific rules governing them; outgoing connections are allowed from all other applications.
- Firefox is permitted to send two kinds of communications, via ports 80 and 8080.
- Communications by Firefox via port 443 are forbidden.
- Communications by Firefox via any other port raise an alert on your Mac's screen; if you don't respond to allow the communication within 90 seconds, it is denied.

This list of ports contains three columns:

- The first column, containing checkboxes, indicates the port behavior that is currently activated for the application. If the box next to a port is checked, the behavior you have specified is active. If you want to deactivate this behavior, then uncheck the box. You can reactivate it later by checking the box.
- The second column, Ports, provides information on the ports that the application uses to access the network. It tells you the port number, and, in some cases, the protocol used and a brief description. (This description appears automatically when you enter a port number that NetBarrier X5 recognizes.) You can add a port number, or a range of port numbers, for example 110-123.
- The third column contains one of two icons: a green, GO icon, indicates that network access is allowed; a red, STOP icon, indicates that network access is denied.



- If you want to change an Allow setting to Deny, you can just click the green GO icon, and it will change to the red STOP icon. You can also toggle from STOP to GO in the same manner.

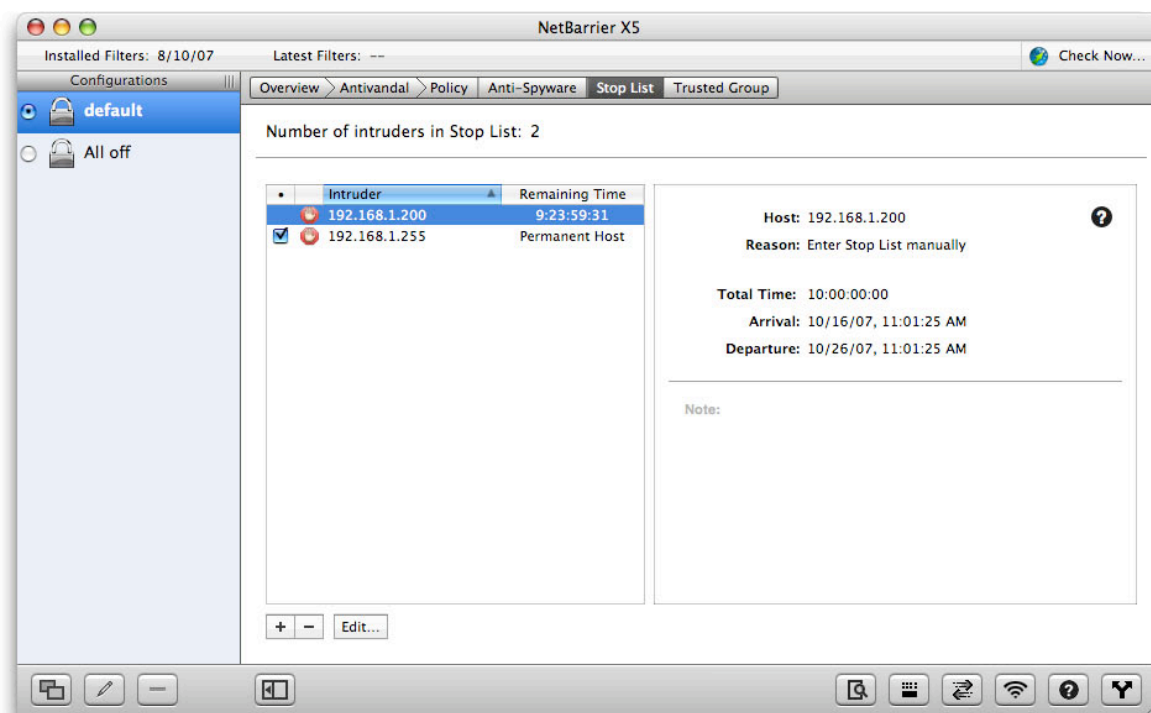
To view an application on the Applications list in the Finder, hold down the Control key on your keyboard and click on the name of an application. A contextual menu appears. Select Show in Finder, and a Finder window opens revealing the location of the application.

## The Stop List and Trusted Group

The Stop List ensures that once an attempted attack or intrusion has been foiled, communication between the attacking machine and your Mac won't occur for a period of time that you define.

The Trusted Group is the opposite of the Stop List: it lists “friendly” computers that *are* allowed to connect to your Mac. While the Stop List protects you from foes, the Trusted Group opens the door to your friends. NetBarrier X5's Antivandal will not block access to computers listed in the Trusted Group, nor will it set off alerts for any actions they carry out. However, computers in the Trusted Group will still be affected by all active Firewall rules.

The interface for the Trusted Group window is essentially the same as for the Stop List window, so we'll examine them both at the same time, pointing out differences as necessary. Here's the Stop List window with some sample data.



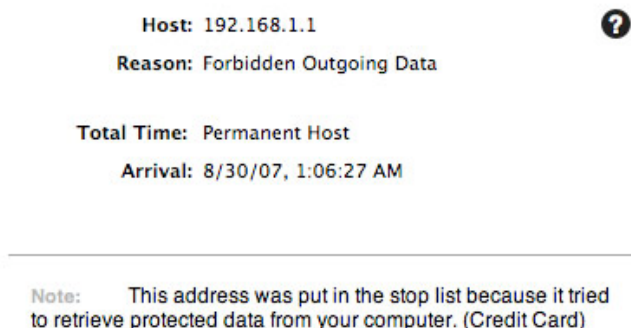
The panel on the left displays information on the various IP addresses that are currently in the Stop List or Trusted Group, if any.

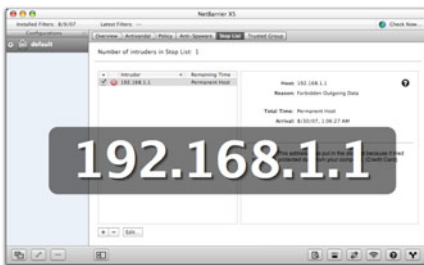
<b>Checkbox</b>	You can temporarily disable a Stop List/Trusted Group item by unchecking this box, which is checked by default when you add a host to either list. When disabled, clicking it enables the item again. (This checkbox only appears if the IP address is set to be blocked permanently.)
<b>Intruder/Host</b>	The second column shows the intruding IP address (in the Stop List) or permitted IP address (in the Trusted Group).
<b>Remaining Time</b>	If you've set this IP address to be forbidden/permitted for a specific period of time, this column shows how much time is remaining, updated every second. Otherwise, this column says "Permanent Host" to indicate that the IP address will be there until you remove it manually.



## Stop List/Trusted Group Information

Clicking an item in the Stop List/Trusted Group shows some additional information on the right side of the panel.



<b>Host</b>	<p>The host's IP address. By clicking 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. (see <b>A Note About DNS Lookups.</b>) You can display this address in large type by moving your cursor over the word "Host", clicking, and selecting Large Type from the contextual menu that appears. The result looks like this:</p> 
<b>Reason</b>	<p>Why the IP address was added to the Stop List. This text doesn't appear in the Trusted Group screen, as all items there are added manually.</p>
<b>Total Time</b>	<p>The amount of time the host is to remain in the Stop List/Trusted Group. Clicking the words "Total Time" changes the display to show Remaining Time; clicking again shows Elapsed Time, indicating how long the offender has been in the Stop List. Clicking Elapsed Time will display the Total Time once again.</p>
<b>Arrival</b>	<p>When the address was added to the Stop List/Trusted Group.</p>

<b>Departure</b>	If you specified an amount of time for an IP address to remain in the Stop List/Trusted Group, the time it will be released is given here.
<b>Notes</b>	Any comments you have entered for this IP address. NetBarrier X5 will also automatically add comments to this field when it puts an item in the Stop List, as in the example above.



## A Note About DNS Lookups

In various places throughout NetBarrier X5 you'll see a question mark in a dark circle. Clicking it toggles nearby information from a numerical IP address to its associated domain name and back again.



Be aware that IP addresses do not have a one-to-one relationship to domain names. For example, a large domain might have `www.example.com` hosted on one IP address, `forums.example.com` hosted on another, and `blog.example.com` hosted on another.

Meanwhile, small domains often share one IP address with others, all hosted as “virtual domains” on a single computer. In such cases a domain lookup gives an IP address that actually leads to the larger, unexpected machine name, for example `apache2-vat.marketstreet.example.com`.

As a result, entering an IP address could block (or allow) traffic from unintended domains, while entering a domain might not block (or allow) all desired traffic. This is the nature of the Internet domain structure, and isn't an error of NetBarrier X5. If you have problems with unexpectedly blocked or permitted traffic, try using a domain name instead of an IP address, or vice-versa.

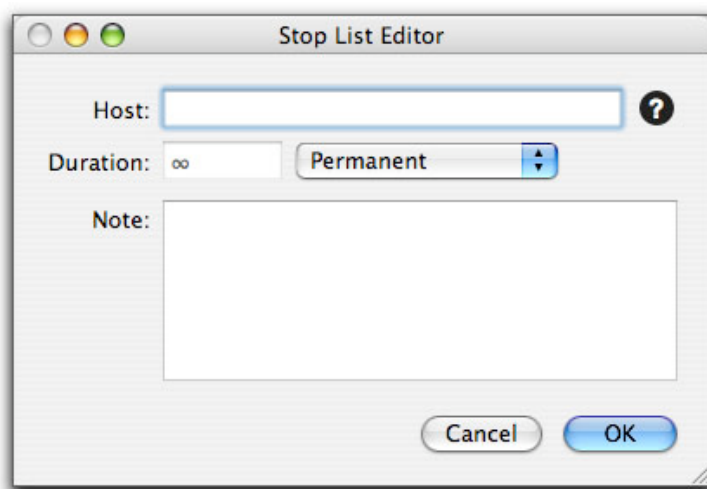


## Adding Addresses

There are two ways to manually add addresses to the Stop List or Trusted Group. (NetBarrier X5 can also add addresses automatically to the Stop List in response to Alerts. For more details, see chapter 9, **Understanding Alerts**.)

The first way to add an address to the Stop List or Trusted Group 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 chapter 8, **The Four Lines of Defense: Monitoring**.

You can also manually add addresses to the Stop List/Trusted Group. To do this, click the + button at the bottom of the list. A window appears.

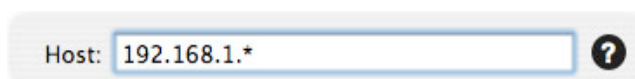


Enter a host address in the Host field, and select the time this address is to remain in the Stop List or Trusted Group by entering a number in the Duration field. Then, select a time unit from the popup menu. If you do not know the numerical IP address of the host you wish to add, enter its name and click the ? button. NetBarrier X5 queries your Internet provider's DNS server and enters the correct number in the field. (See **A Note About DNS Lookups**.) You can also add comments, such as the reason for adding the address, in the Comments field. If you decide you do not wish to add this address to the Stop List or Trusted Group, click Cancel.



## Using Wildcards

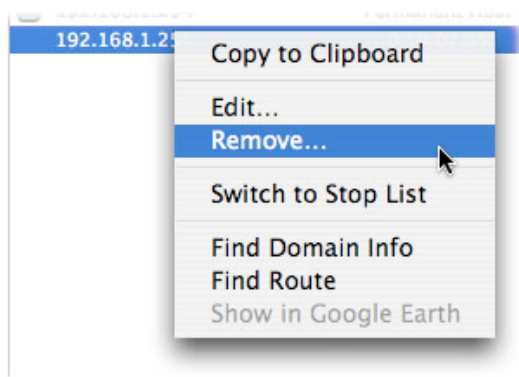
You can use wildcards to indicate ranges of IP addresses in the Stop List or Trusted Group. To do so, enter the first part of the IP address you wish to block, followed by asterisks. For example, 192.168.1.\* will block all IP addresses from 192.168.1.0 to 192.168.1.255 inclusive; 192.168.\*.\* will block IP addresses from 192.168.[0-255].[0-255]; and so on.



## Removing Addresses

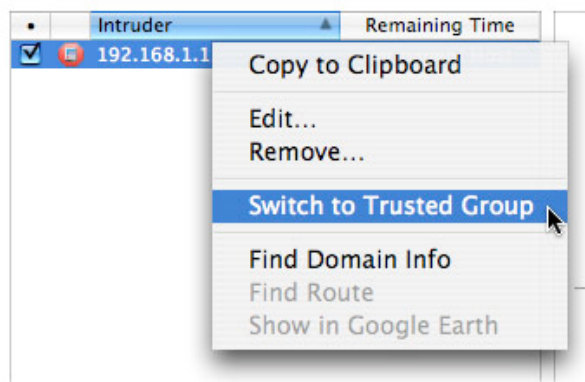
To remove an address from the Stop List or Trusted Group, click the address you want to remove, then click the – button. A dialog asks if you really want to remove the address.

You can also remove an address by clicking the address while holding down the control key on your keyboard, then selecting Remove... from the contextual menu that is displayed. A dialog asks if you really want to remove the address.



## Moving Addresses Between the Stop List and Trusted Group

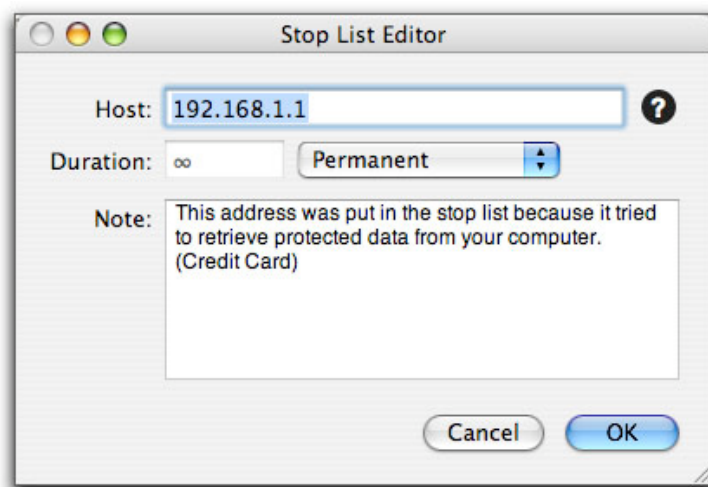
You may decide that you want to move an address from the Stop List to the Trusted Group, or vice-versa. To do this, hold down the control key on your keyboard, then select Switch to Trusted Group or Switch to Stop List from the contextual menu that is displayed.



## Editing an Address

There are three ways to edit an address in the Stop List or Trusted Group:

- Click the address you would like to edit, then click the Edit... button at the bottom left side of the pane;
- Double-click the address; or
- Click the address while pressing the Control key on your keyboard, then select Edit... from the contextual menu.



The Stop List/Trusted Group Editor appears. You can change the address, add or change comments, or change the time you want the item to remain on the Stop List/Trusted Group.

## The Contextual Menu

As you have seen above, you can click an item in the Stop List/Trusted Group while pressing the Control key on your keyboard to raise a contextual menu. There are four functions on this list not yet discussed: Copy to Clipboard, Find Domain Info, Find Route, and Show in Google Earth.

<b>Copy to Clipboard</b>	Puts the IP address on the Mac OS X Clipboard, where it can be pasted into other programs (such as a text editor).
<b>Find Domain Info</b>	Opens NetBarrier X5's Whois window and performs a search on the selected IP address. See chapter 8, <b>The Four Lines of Defense: Monitoring</b> for more information.
<b>Find Route</b>	Opens NetBarrier X5's Traceroute window and performs a search on the selected IP address. See chapter 8, <b>The Four Lines of Defense: Monitoring</b> for more information.
<b>Show in Google Earth</b>	Launches the Google Earth program and attempts to find the geographic location of the selected IP address.



## **8—The Four Lines of Defense: Monitoring**

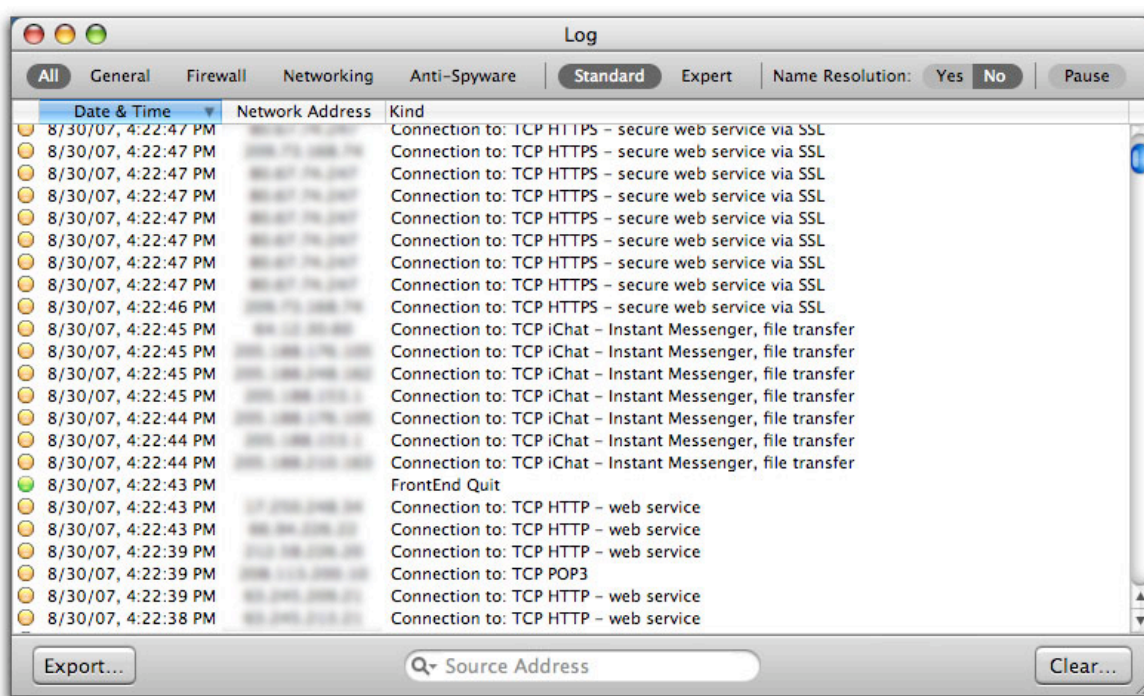


## The Log

The log shows a record of all the activity where NetBarrier X5 has acted. It lists each time there has been an incident, the address of the intruder, and the kind of incident recorded. To access the log, click the small “magnifying glass” icon at the bottom of the screen, choose Window > Log, or press Command-Option-L.



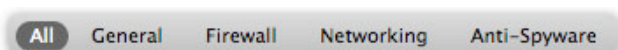
You'll see the main log window. Of course your entries won't be the same as those shown here, but rather will reflect activity on your Mac since you installed NetBarrier X5 (or last cleared the log).



## Log View Options

The top of the log window contains three sets of options that affect how the log appears. The first group shows subsets of log activity to help you see potential issues more clearly; the second group toggles between the default Standard view and an extended Expert view; the third group lets you choose whether to view raw IP addresses or domain names according to DNS lookup. We'll examine each of these sets of options separately.

Activities fall into three groups: General, Firewall and Networking. You can choose to see activities relating to all the groups at once, or only activities relating to a specific one. Click one of the button bar buttons to change the log view.



<b>All</b>	All activity that NetBarrier X5 tracks. This is the default setting.
<b>General</b>	Activity related to the operation of NetBarrier X5 itself, such as instances when you launched and terminated the program, added applications to Anti-Spyware, entered items into the Stop List and Trusted Group, and so forth.
<b>Firewall</b>	Incidents when network activity called a Firewall Rule into play, if logging was turned on for that Rule. Records of any Trojan horse attacks also appear in the Log, if you've turned on Trojan protection.
<b>Networking</b>	All connections to networks or the Internet, and when IP addresses in the Stop List attempt to connect to your computer.
<b>Anti-Spyware</b>	A subset of the General group, showing only when applications were added to or removed from the Anti-Spyware list, or when Anti-Spyware rules were called into play.



## Standard and Expert Log Views

Standard Expert

**Standard:** The default view for the Log screen. This displays only four pieces of information for each Log entry

	Date & Time ▼	Network Address	Kind
●	8/30/07, 4:35:59 PM		FrontEnd Startup
●	8/30/07, 4:35:35 PM		Connection to: TCP HTTP – web service
●	8/30/07, 4:34:59 PM		Connection to: TCP HTTP – web service

- Type of activity, indicated by dot color:
  - Green = General
  - Yellow = Firewall
  - Red = Network
- Date & Time of activity, according to your Mac's clock setting.
- Network address, given by default as an IP address. If you have checked Name Resolution (see below), you will see the domain names for those addresses that NetBarrier X5 was able to resolve.
- Kind, a short description of the activity.

**Expert:** An extended view, showing the following fields where applicable.

	Date & Time ▼	Source	Destination	Protocol	Src Port	Dest Port	Flags	Interface	Kind
●	8/30/07, 4:35:59 PM								FrontEnd Startup
●	8/30/07, 4:35:35 PM			TCP	53181	80	S	en1	Outgoing connection
●	8/30/07, 4:34:59 PM			TCP	53180	80	S	en1	Outgoing connection

- Type of activity, as described above.
- Date & Time of activity.
- Source address, which is the originating IP address (or domain) of the incident. For most activities, the source will be your Mac's IP address, although for attacks it will be that of the attacking computer. If you have checked Name Resolution, you will see the domain names for those addresses that NetBarrier X5 was able to resolve.
- Destination address, given by default as an IP address.





- Protocol, which describes how the connection was attempted, i.e. TCP, UDP, ICMP or IGMP.
- Source Port: The port from which data was sent.
- Destination Port: The intended port for the data.
- Flags, which displays TCP flags: A (acknowledge), S (synchronize), F (end of data), or R (reset).
- Interface, the network interface used to send the data, such as Ethernet or AirPort, given by BSD Name.
- Kind, a short description of the activity.

General activities, such as starting or quitting NetBarrier X5 itself, don't involve any computers other than your own Mac, and will therefore lack all fields related to network activity.



## Domain Name Resolution

Name Resolution: ☒ Yes ☐ No

NetBarrier X5 helps you track down intruders by resolving the domain names of your connections. Internet addresses exist in two forms: IP numbers, such as 192.168.1.1, and names, such as example.com. The correspondence between the two is recorded in domain name servers all across the Internet.

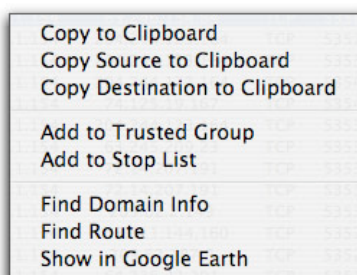
When Name Resolution is checked in the Log panel, NetBarrier X5 will attempt to find the names for each of the Internet addresses shown in the log. If NetBarrier X5 can find this information, it then displays it in name form rather than as numbers.

Date & Time	Network Address	Kind
8/30/07, 5:43:37 PM	www.intego.com	Connection to: TCP HTTPS – secure web service via SSL
8/30/07, 5:43:35 PM	www.intego.com	Connection to: TCP HTTPS – secure web service via SSL
8/30/07, 5:42:08 PM	74.125.19.99	Connection to: TCP HTTP – web service

NetBarrier X5 is not able to resolve the names of all Internet addresses, since some addresses have no name equivalents. For more information, see **A Note About DNS Lookups**.

## Log Window Contextual Menu

If you hold down the Control key and click any log entry, a contextual menu displays.



Its options are:

<b>Copy to Clipboard</b>	Copies visible columns of this log entry to the Mac OS X clipboard, in tab-delimited text format. You can then paste it into any application or document.
<b>Copy Source to Clipboard</b>	Copies only the Source field of this log entry to the Mac OS X clipboard: only available when viewing the log in Expert mode.
<b>Copy Destination to Clipboard</b>	Copies only the Destination field of this log entry to the Mac OS X clipboard: only available when viewing the log in Expert mode.
<b>Add to Trusted Group</b>	Permanently adds this IP address to the Trusted Group, thereby allowing future communications from it regardless of Antivandal settings. However, NetBarrier X5's Firewall will still affect communications from this IP address.
<b>Add to Stop List</b>	Permanently adds this IP address to the Stop List, thereby blocking future communications from it regardless of Antivandal settings. However, NetBarrier X5's Firewall will still affect communications from this IP address.
<b>Find Domain Info</b>	Launches NetBarrier X5's Whois window and performs a search on the selected IP address. See <b>Whois</b> for more information.
<b>Find Route</b>	Launches NetBarrier X5's Traceroute window and performs a search on the selected IP address. See <b>Traceroute</b> for more information.



<b>Show in Google Earth</b>	Launches the Google Earth program, if you have it installed, and attempts to find the geographic location of the selected IP address. See <b>Viewing IP Addresses in Google Earth</b> for more information.
-----------------------------	---



## Pausing the Log

A rectangular button with a light gray background and a thin border. The word "Pause" is centered on the button in a small, dark gray font.

If you have many connections entering and leaving your computer, you may find it difficult to follow the log as it displays. To view the log more easily, click the Pause button in the log screen's upper-right corner. The log display stops so you can read the data, but keeps recording and will display new data when the log is no longer paused. Click the Pause button again to resume real-time display.

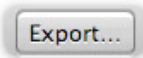
## Clearing the Log

A rectangular button with a light gray background and a thin border. The text "Clear..." is centered on the button in a small, dark gray font.

To clear the log, and erase all information it contains, click the Clear... button in the lower-right corner. A dialog appears, asking you to confirm your request.

The log will also be cleared automatically if you've checked the "Clear log after exporting" checkbox in the Log Preferences and have set NetBarrier X5 to export a log periodically. See chapter 10, **Preferences and Configurations**.

## Exporting the Log

A rectangular button with a light gray gradient and a thin border, containing the text "Export..." in a small, dark font.

You can export log data in several formats. 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 also have the Log data exported automatically: see chapter 10, **Preferences and Configurations**.)

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 your ~/Library/Logs/Net Barrier folder.

**WARNING:** Log exports could take several minutes if the Domain Resolution feature is turned on.

Logs can be exported in six formats. Click the Format popup menu to select the export format.



The available formats are:

<b>Expert HTML</b>	HTML format, showing all columns visible in Expert mode. In this format you can partially retrace past browsing history, as NetBarrier X5 provides clickable links to all attempts to reach non-secure Web pages. (That is, Destination Ports, connected by TCP, targeting ports 80 or 8080.)
<b>Expert Text</b>	Tab-delimited, plain text format with additional columns to show all columns visible in Expert mode. This is the best mode to use for import into a spreadsheet or database program.

<b>HTML</b>	HTML format, showing all columns visible in Standard mode. As with Expert HTML exports, this file format helps you retrace past browsing history.
<b>Analytic</b>	A text format similar to Expert Text, without tab separators, but with labels in front of some fields.
<b>Text</b>	Tab-delimited, plain text format with all columns visible in Standard mode.
<b>Who's there?</b>	The log as a text file, with the following columns: Date, Time, Result, Hostname, Server Port, and Method: useful in some log analysis programs.

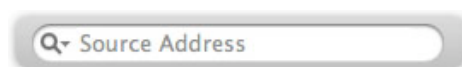


## Filtering Data in the Log Window

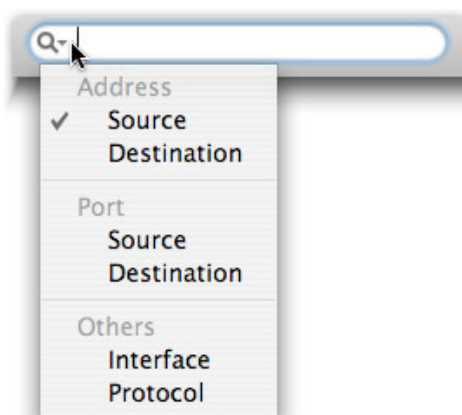
At the bottom of the log window toolbar is a search field that lets you filter data according to several criteria, displaying only those entries that contain the selected criteria in the following categories:

- **Source address**
- **Destination address**
- **Source port**
- **Destination port**
- **Interface**
- **Protocol**

Source Address is the default criterion, as the search field shows.



To search for log data containing any of these criteria, click the disclosure triangle next to the Search icon.

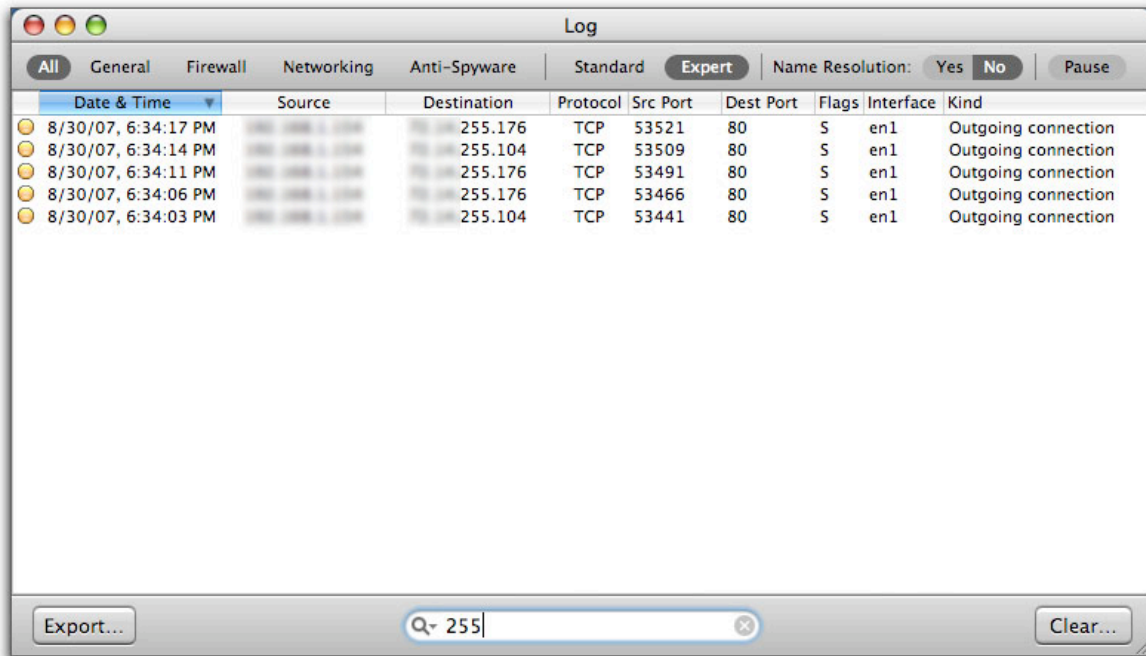


Select the criterion you want to search for, then enter a string in the search field. You don't need to enter the entire string; the display is dynamic, and automatically narrows down log data as you enter characters in the search field.





In the example below, we're searching for "255" in the Destination Address. The search text can occur anywhere in the field, not just at the beginning. Also, the search works even if you're viewing the log in Standard mode, where the search field (the Destination, in this case) is hidden.



To clear the search field and begin a new search, click the small "X" button in the search field.

## Traffic

The Traffic window contains a set of activity gauges that tell you the type and quantity of network activity that is coming into and going out of your Mac from both the Internet and local networks. To access the Traffic window, click the small icon shown below, choose Window > Traffic, or press Command-Option-1.

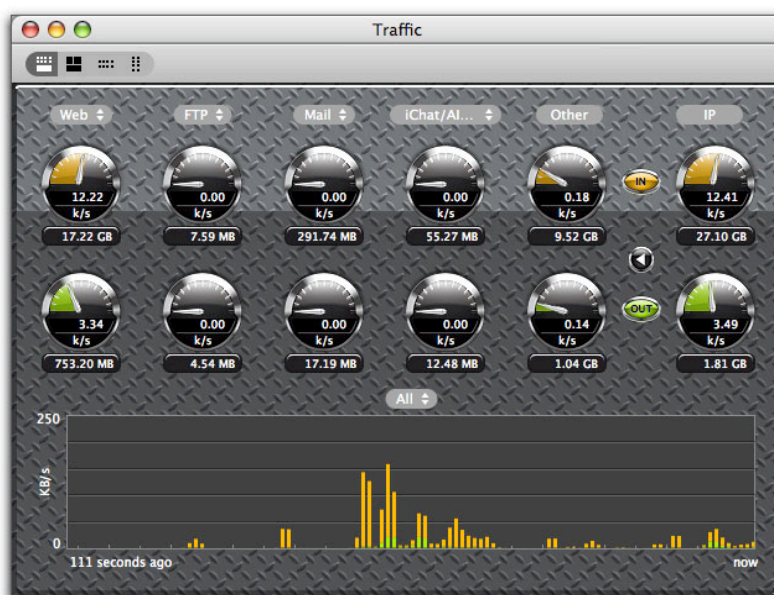


## Traffic View Modes

The Traffic screen has four viewing modes, switchable by clicking the small buttons at the top of the screen.



The first button is the default view and shows traffic as two rows of gauges and a timeline.

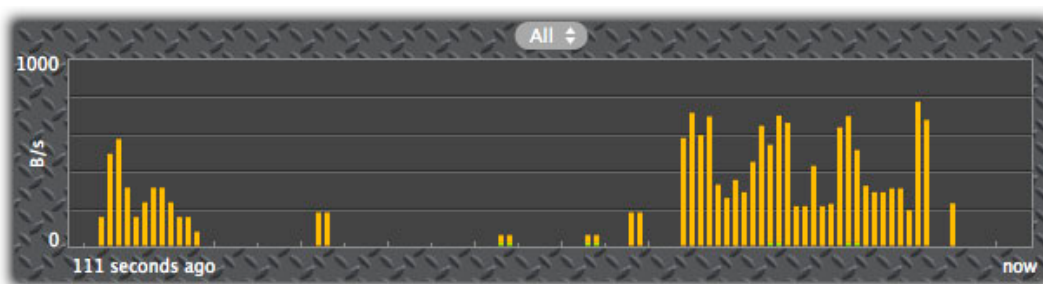


The IN gauges on top, with values shown in orange by default, display the amount of data coming into your Mac. The OUT gauges in the second row, with values shown in green by default, display the amount of data leaving your computer. The number inside the gauge is the current throughput in kilobytes per second (k/s), and the bottom is the total amount, usually in megabytes (MB) or gigabytes (GB).

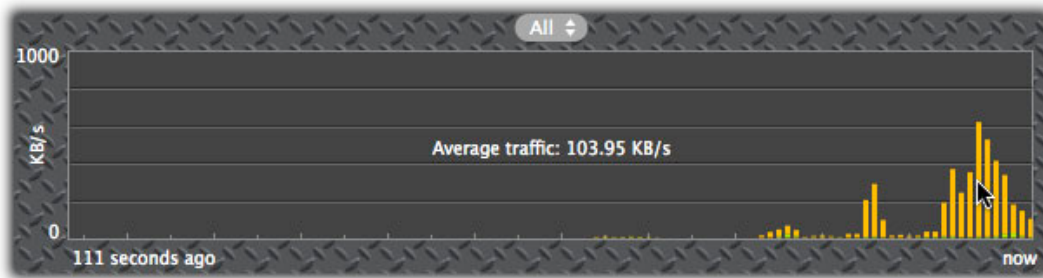
The timeline at the bottom shows traffic over time, where the bars the furthest to the right represent the present time, and those to the left represent the past. As above, orange values show incoming traffic while green values show outgoing traffic.

The scale of the timeline is dynamic; it changes according to the amount of traffic. In the above example, throughput ranges from 0 to about 150 kilobytes per second, so the graph tops out at 250 kilobytes per second, as is seen in the legend to the left of the graph. But in this second example, there's very little traffic, going only as high as 800 *bytes* per second—that is, less than one kilobyte. So the unit of measurement changes to bytes, and the graph tops out at 1,000.

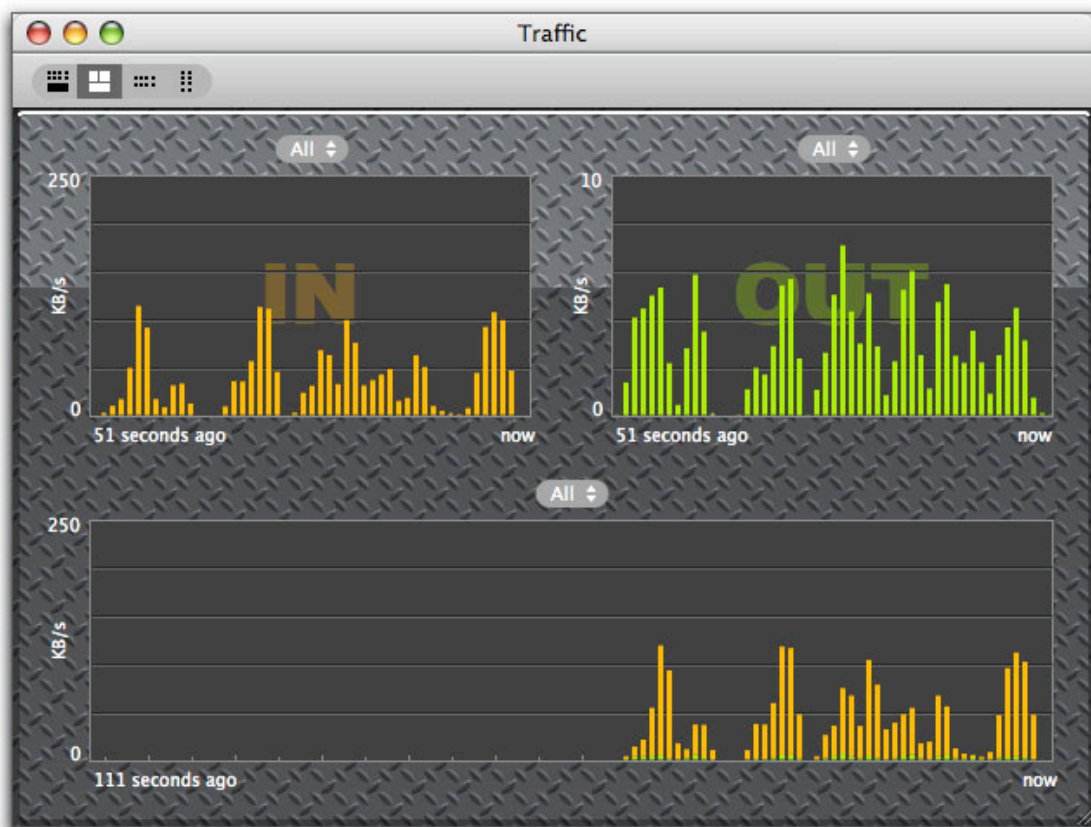
By default, the timeline records activity going back 111 seconds in time. You can increase this time period by making the window larger, either by clicking the green Mac OS X “grow” button in the upper-left corner, or by clicking and dragging the window’s bottom-right corner. The maximum time is determined by the size of your screen or your willingness to see only a section of the timeline at one time.



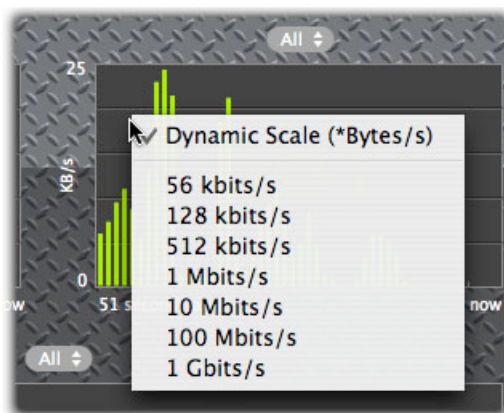
If you place your cursor over a timeline, text appears showing the current average data throughput, which is updated every second.



The second view button shows traffic as three timelines, respectively showing traffic in, out, and in total.

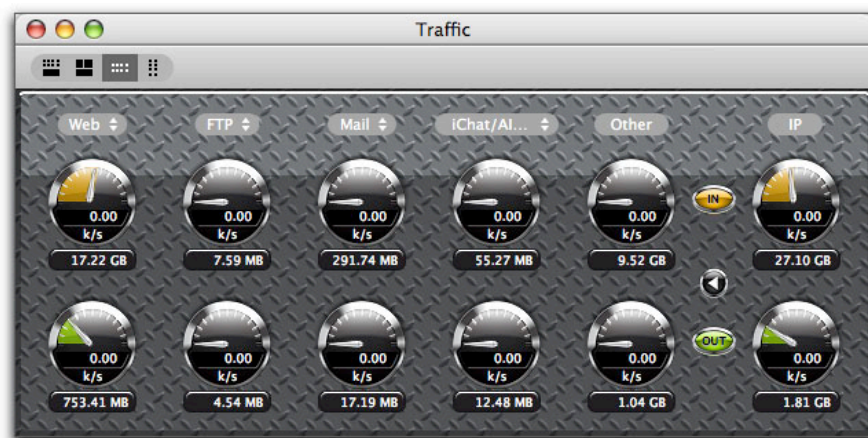


This view mode has a special feature that lets you choose the scale for the In and Out graphs by moving the mouse over one of them, holding down the Control key, and clicking. a popup menu offers several options.



This lets you choose your maximal throughput and displays graphs that are correctly scaled for that throughput. Choose Dynamic Scale if you want the graph to change its scale according to the data throughput as was described earlier.

The third view mode button shows traffic as a series of gauges in horizontal orientation, with no timeline. The fourth button shows the same gauges, but in a vertical orientation (not shown here).



The three views that contain round gauges also have Reset buttons. Clicking this button sets the totalizing, bottom row of gauges back to zero.



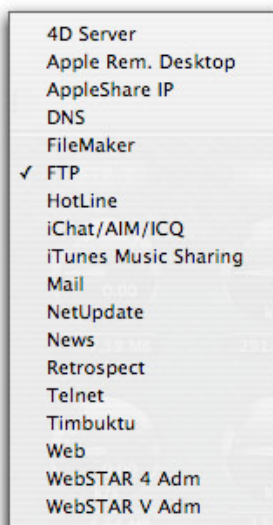
## Selecting Activity Data Types

In each view mode, you have a choice of what type of traffic to view: by default, the activity data types monitored are Web, FTP, Mail, iChat/AIM. The fifth gauge shows all other traffic, while the sixth shows total traffic.

But you can choose which type of data will be shown for the first four pairs of gauges by clicking the indicator over one of the gauges.



A popup menu displays showing several choices.

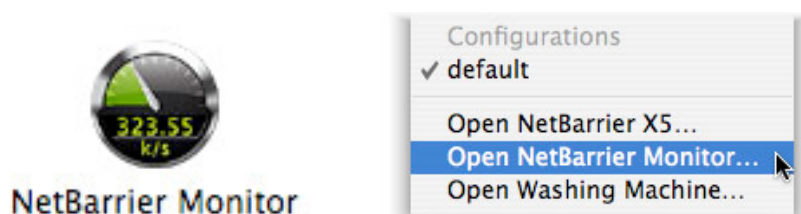


You can add or remove services from this list through the Traffic Preferences pane: see **Traffic Preferences** for details.



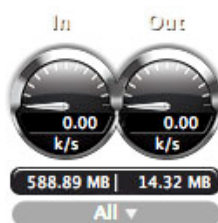
## NetBarrier Monitor

Installing NetBarrier X5 also places an application called NetBarrier Monitor in your Applications folder. You can launch this program by double-clicking its icon, or through the Intego Menu (see **The Intego Menu**).



The NetBarrier Monitor application provides a small, floating window that lets you keep an eye on network activity at all times, without needing to display the entire NetBarrier X5 activity gauge palette.

When you open NetBarrier Monitor, it displays its activity gauge window in the bottom-right corner of your screen. You can move NetBarrier Monitor's location by clicking it and dragging to a new place on your screen.

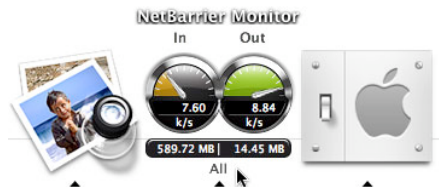


By default, NetBarrier Monitor displays the total network traffic for all services. As in the Traffic section of the main NetBarrier X5 program, you can change what kind of traffic is displayed by clicking All at the bottom of the NetBarrier Monitor window, and selecting a service from the popup menu.

If you hold down the Control key on your keyboard and click anywhere in the NetBarrier Monitor window, a popup menu offers two options.



Show in Dock closes NetBarrier Monitor's window, and the program's Dock icon changes to show its activity gauges, updated in real time.

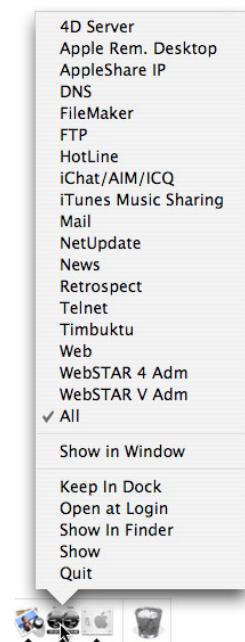


Network activity also appears in the NetBarrier Monitor icon that appears when you switch among applications by hitting Command-Tab.

To return NetBarrier Monitor to its window, hold down the Control key, click on the NetBarrier Monitor Dock icon, and select Show in Window.

When NetBarrier Monitor displays in the Dock, you can change its display by holding down the Control key, clicking on its Dock icon, and selecting a different service from its Dock menu.

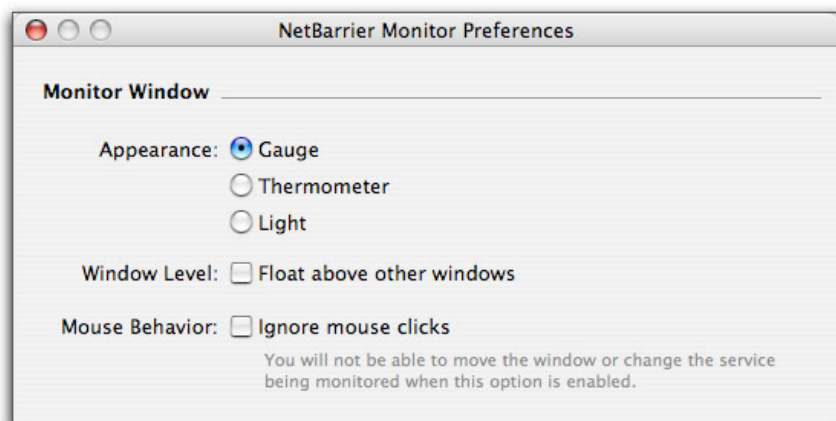
The Keep in Dock selection makes the NetBarrier Monitor icon a permanent fixture in the Dock, even when the program is not running, so you can open it just by clicking its Dock icon. The Open at Login selection starts the program each time you start a user's session on your Mac.

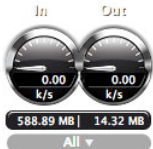

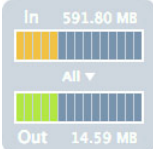




## NetBarrier Monitor Preferences

Several preference settings affect the behavior of NetBarrier Monitor. To set them, go to NetBarrier Monitor > Preferences or press Command-comma while NetBarrier Monitor is running.

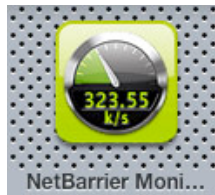


<b>Appearance</b>	<div>    </div>
<b>Window Level</b>	“Float above other windows” makes NetBarrier Monitor always appear in the foreground, above all other applications.
<b>Mouse Behavior</b>	“Ignore mouse clicks” prevents you from moving NetBarrier Monitor’s window or changing the service it monitors.

## The NetBarrier Monitor Widget

NetBarrier X5 installs the NetBarrier Monitor widget that loads into Mac OS X's Dashboard (Mac OS X 10.4 Tiger and higher only) to show you network activity at all times.

To display the NetBarrier Monitor widget, activate Dashboard. Click the + button to display all the widgets available on your computer. Select NetBarrier Monitor from the list. Its icon looks like this:

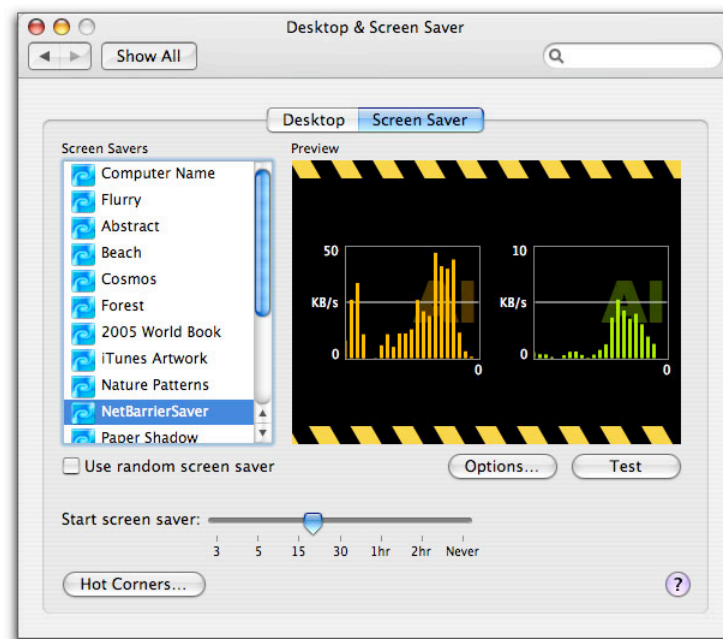


By your selection it is added to the active widgets, you will see NetBarrier Monitor whenever you switch to Dashboard. As with the NetBarrier Monitor application, you can move the window or change the type of activity displayed.

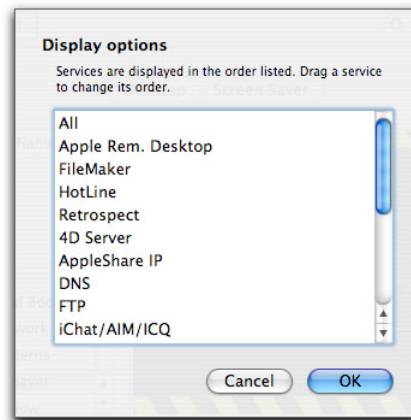
## The NetBarrier X5 Monitor Screen Saver

NetBarrier X5 installs a screen saver that gives you an overview of network activity when your computer is otherwise idle. In addition, if your Macintosh is running as a server, you can use this screen saver to keep an eye on its network activity.

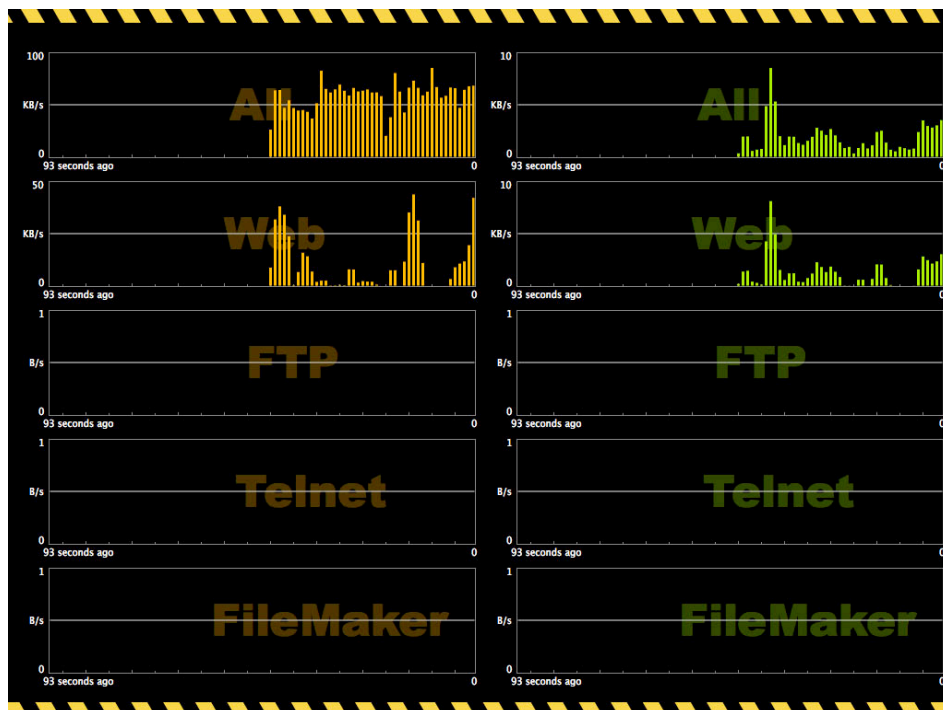
To use the NetBarrier X5 screen saver, open the System Preferences from the Apple menu, click on Desktop & Screen Saver, and click the Screen Saver Tab. Select NetBarrierSaver in the screen saver list.



The preview screen only shows All traffic; however, it will show traffic broken down by service when actually running. Click Options to choose the order in which services are displayed.



Drag them into the order you want. The number of services displayed depends on your screen resolution and the number of screens you have: therefore, the ones most important to you should be listed first.



For more on screen saver settings, see the Mac OS X help.

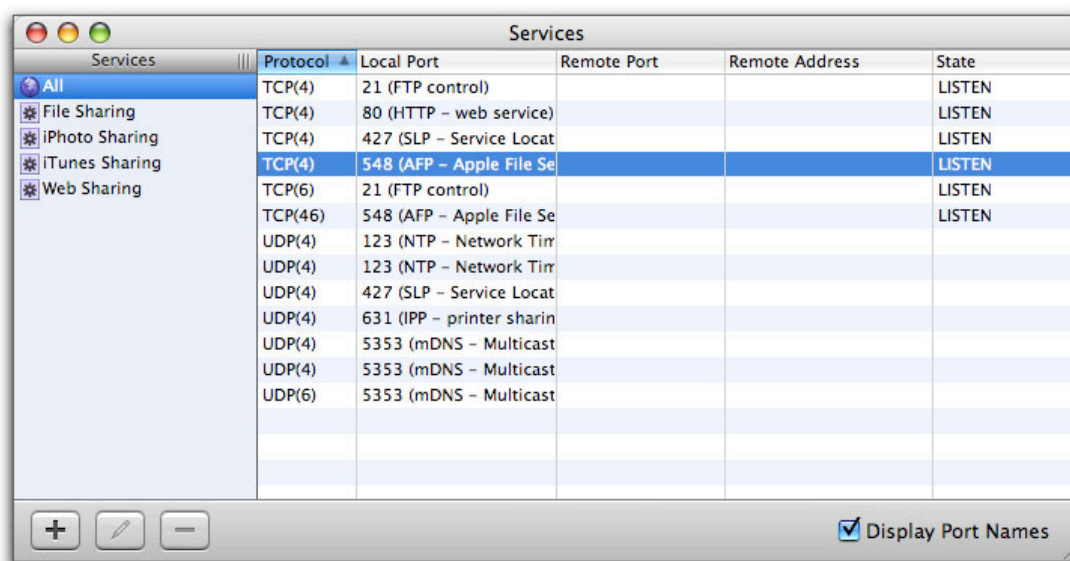
## Services

The Services window lists all active network services on your computer that are accessible to other users via Internet Protocol, such as a web server, mail server, etc.

To show the Services window, click the double-arrow icon in the bottom-right corner of NetBarrier X5's main window.

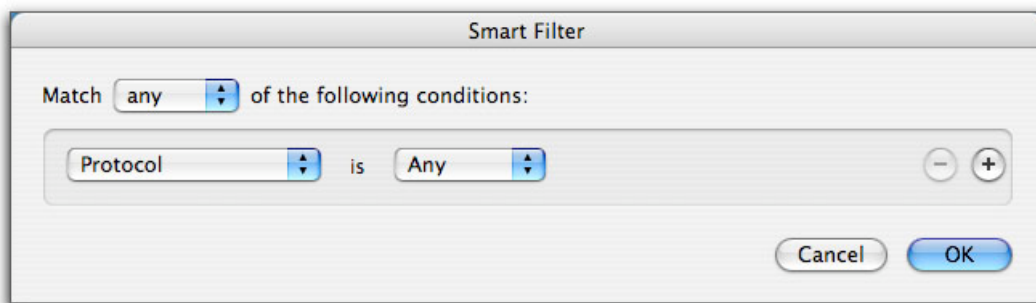


For each port used, the following information is shown: the protocol (TCP or UDP), the local port number (depending on the protocol it represents, if it is a standard protocol, such as port 21 for FTP), the remote port number, the remote address (the IP address of the remote connection), and the state of the connection—for example, whether the connection is active or if it's just listening for traffic. To obtain the names of the ports in addition to their numbers, click the Display Port Names checkbox in the lower-right corner, as is shown here.



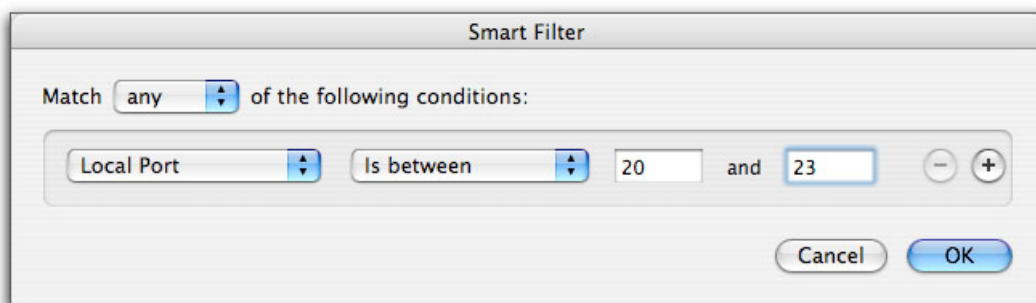
Since the list of ports used by all services can be long, NetBarrier X5 provides filters to allow you to view ports used by specific services. You can choose from File Sharing, iPhoto Sharing, iTunes Sharing and Web Sharing, or you can create your own filters.

To create a filter, click the + button in the lower-left corner of the panel. The Smart Filter window displays.



The first popup menu lets you specify whether you want the filter to match Any of the conditions you give, or All of them.

The second popup menu specifies the type of information that you want the filter to find. The choices are the same as the Services window's columns: Protocol, Local Port, Remote Port, Remote Address and State. After choosing one of these, you'll have the opportunity to specify filter details. In this example, we're only going to list those services where the local port is in a given range.



Clicking the + button at the right of the window adds additional conditions, while clicking the – button next to a condition removes it from the list. You can also modify filter conditions by simply changing their popup menu options or typing new data into the data fields.

When you finish creating your filter, click OK to save it, then enter a name for the filter in the Services list. Click the filter at any time in the list to view the network services that correspond to your conditions.

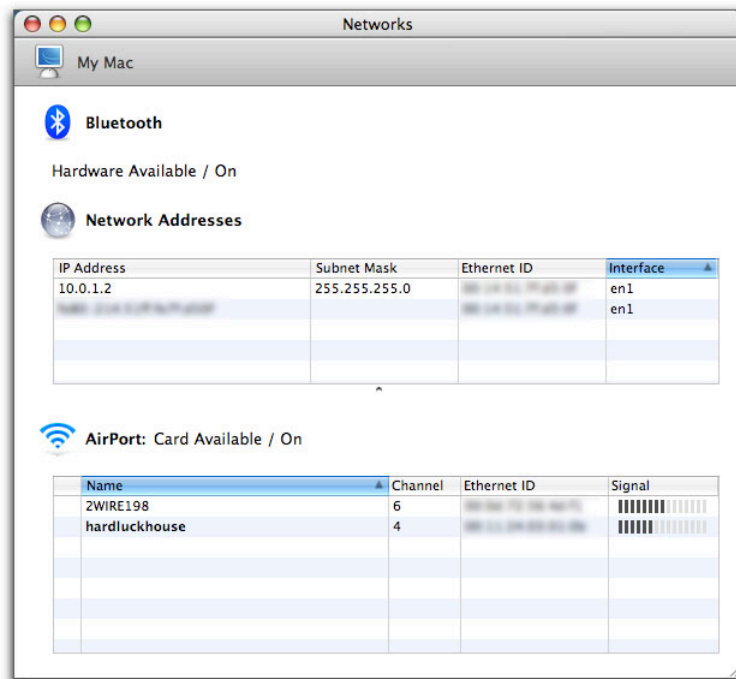
## Network

The Network window provides useful information about your Mac, its network configuration, and local networks available to it. To show the Network window, click the radio icon in the bottom-right corner of NetBarrier X5's main window.

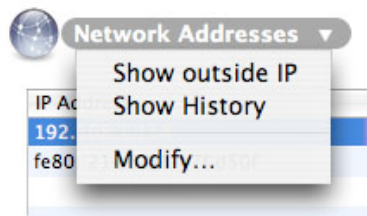


The Network window shows:

<b>Your Mac's name</b>	Shown in the gray bar at top: in the example below, it's "My Mac". This is the name that your computer shows to anyone browsing for it on a network. You can change this name in the Sharing pane of the System Preferences.
<b>Bluetooth</b>	Whether Bluetooth hardware is available and active.
<b>Network Addresses</b>	All the IP addresses that are active on your Mac. If you have several network adapters with different addresses, or are running several servers, more than one address will be shown. It also tells you about any related Subnet Masks, Ethernet IDs and Interfaces (in BSD name format).
<b>AirPort</b>	Availability and status of a wireless networking card. If your AirPort card is available and on, the table shows available wireless networks, their Channels, Ethernet IDs, and signal strengths in relation to your current position. (The more dark bars, the stronger the signal.) Wireless networks that require a password or other key to join display a small icon of a lock. Those with no lock have no networking password: however, they may be protected in other ways, such as Web authentication. If you're connected to a wireless network, its name will appear in bold type.



Several functions and options are available for the Networks screen by clicking on the words, “Network Addresses”.



These options are:

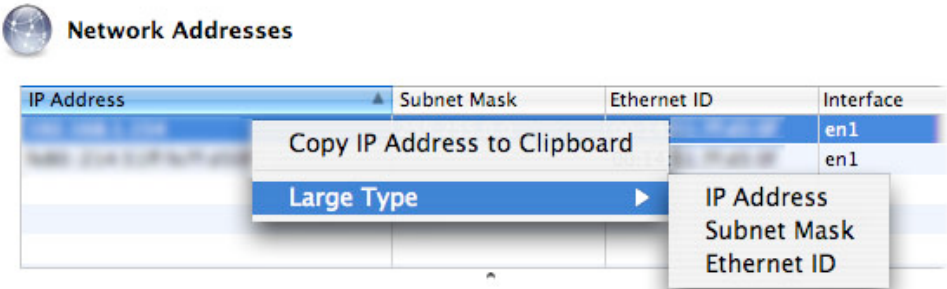
<b>Show outside IP</b>	Shows in large type the IP address that your computer uses when it connects to the Internet or other networks. This address is different from what NetBarrier X5 displays on this pane if you have a router, a cable or a DSL modem. Click anywhere on the screen to dismiss the information.
<b>Show History</b>	Displays a list showing the different IP addresses attributed to your Mac by your ISP, if you have dynamic IP addressing. However, if you have a router, or a cable modem, this only shows the IP address your computer uses internally.



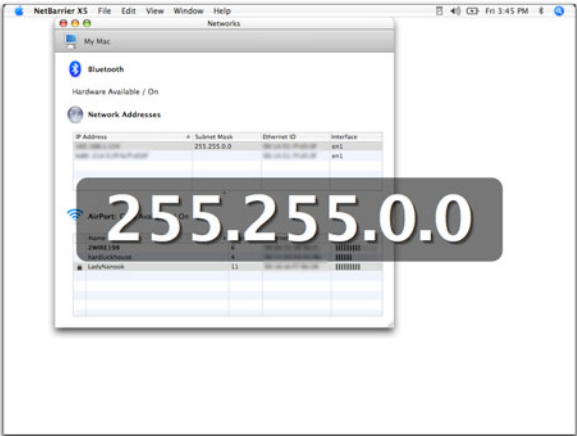


<b>Modify...</b>	Opens the Network pane of Mac OS X's System Preferences. You can change your computer's name or network addresses in this pane. For more on Network settings, see the Mac OS X help.
------------------	--

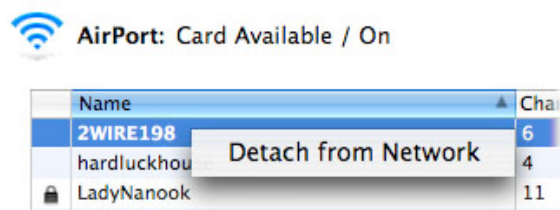
Additional options are available for individual entries in the Network Addresses area as well. To reveal them, press the Control key while clicking on the entry you mean to affect. A contextual menu appears.



<b>Copy IP Address to Clipboard</b>	Puts the information in plain text form on the Mac OS X clipboard, where you can paste it in other applications.
<b>Large Type</b>	Offers to show a full-screen display of any of three kinds of information related to the entry: its IP address, Subnet Mask or Ethernet ID. Clicking anywhere on the screen dismisses the large-type display. An example is shown below.



Finally, Control-clicking on entries in the AirPort section brings up a contextual menu where you can detach your Mac from a network to which you're currently attached.

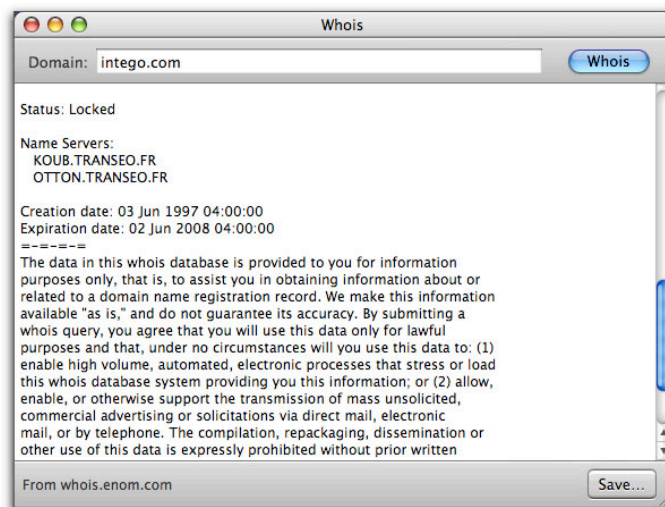


## Whois

NetBarrier X5 allows you to look up domain names and Internet IP addresses using its built-in Whois tool, which you launch by clicking the “?” button in the bottom-right corner of the screen.



Then, enter a domain name or IP address in the Domain field, and click the Whois button or press the Enter key. The large text field below gives you information about the domain, fetched from publicly accessible information servers. You can save this information to a text file by pressing the Save... button.



After you receive your information, text in the gray bar at the bottom of the window tells you the name of the server where that information originated. NetBarrier X5 includes four default Whois servers, but you can change these or add others. To find out how to add Whois servers, see chapter 10, **Preferences and Configurations**.

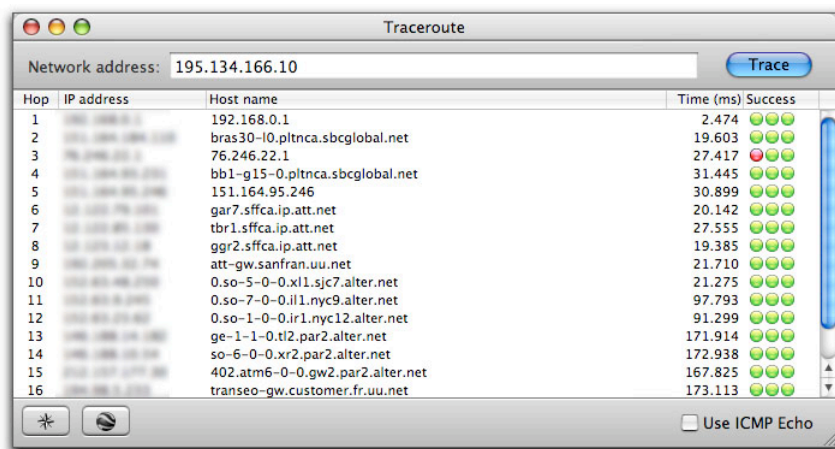
## Traceroute

When you send or receive data over the Internet or other networks, it travels in packets from host to host until it reaches its destination, possibly making dozens of hops along the way. NetBarrier X5's Traceroute function can help you see exactly how your data gets to its destination; this is especially useful when you are having problems accessing a specific host, and want to see where the data is blocked. When this happens, it usually means a key host or router is not functioning.

Launch NetBarrier's Traceroute tool by clicking the "Y-arrow" button in the bottom-right corner of the screen.



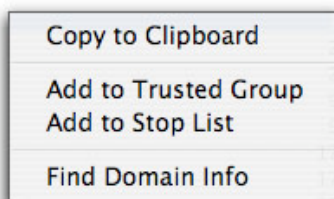
To run a traceroute, enter an IP address or a domain name in the Network address field, then click Trace or press the Return key. If you enter a domain name, NetBarrier X5 resolves it and displays the actual IP address. If you check Use ICMP Echo, the traceroute sends ICMP requests instead of UDP requests; in some cases, this may be more effective.



The Traceroute window then shows all the hops between your computer and the final host. For each hop, NetBarrier X5 displays the hop number, the IP address, the host name, the response time in milliseconds, and the number of pings that succeed (green circles) or fail (red circles). NetBarrier X5 sends three pings for each hop, or each step along the route. Note that if you have a router on

your network, it may not respond to the Traceroute request, and may display as failed requests. This won't prevent the rest of the Traceroute from being executed.

After your Traceroute has completed, you can Control-click on an entry to view a contextual menu.

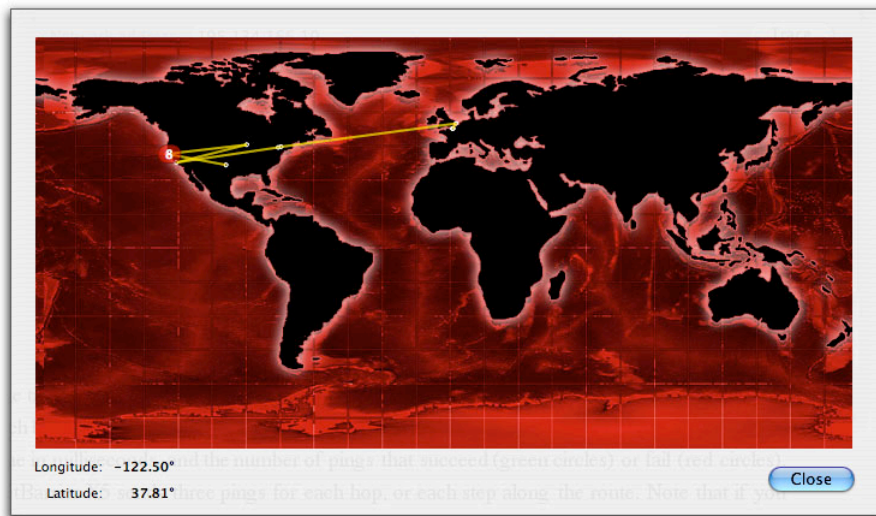


<b>Copy to Clipboard</b>	Puts the information in plain text form on the Mac OS X Clipboard, where you can paste it in other applications.
<b>Add to Trusted Group</b>	Permanently adds this IP address to the Trusted Group, thereby allowing future communications from it regardless of Antivandal settings. However, NetBarrier X5's Firewall will still affect communications from this IP address.
<b>Add to Stop List</b>	Permanently adds this IP address to the Stop List, thereby blocking future communications from it regardless of Antivandal settings. However, NetBarrier X5's Firewall will still affect communications from this IP address.
<b>Find Domain Info</b>	Launches NetBarrier X5's Whois window and performs a search on the selected IP address. See <b>Whois</b> for more information.

You can see a visual display of the route your data takes by clicking the map rosette button in the bottom-left corner.



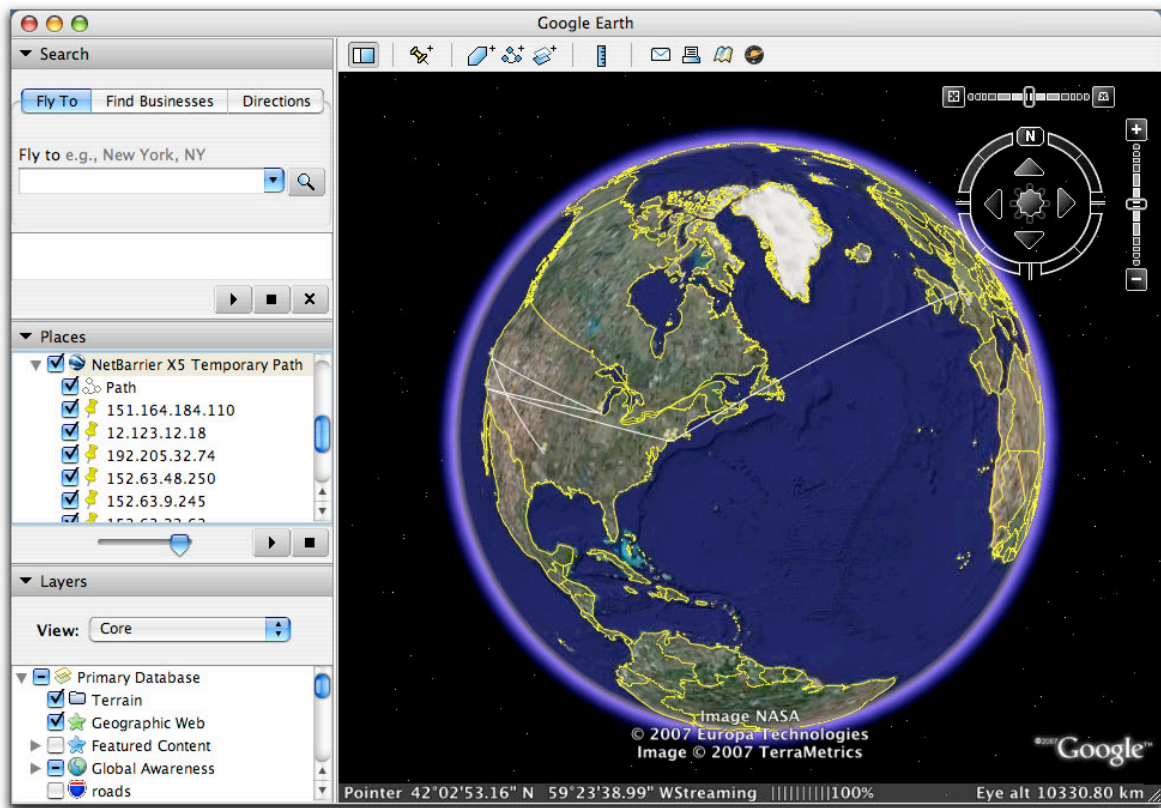
This shows a world map with lines connecting each hop, and numbers showing their position on the path.



If you click the Google Earth button in the bottom-left corner, and you have Google Earth software on your Mac, NetBarrier X5 will open Google Earth and zoom to the precise geographical location of the IP address. Note that this will not work with addresses on your local network, and it will not work with all IP addresses.



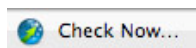
The path and its hops appear in “NetBarrier X5 Temporary Path” under the Places section of Google Earth, and are automatically displayed. For more information about the freely downloadable Google Earth, visit <http://earth.google.com>.



## 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 X5 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.

NetUpdate periodically checks for updates, or you can force it to check immediately by clicking the "Check Now..." button in the upper-left corner of NetBarrier X5's main Overview screen.



For more on using NetUpdate, see the Intego Getting Started Manual.





# 9—Understanding Alerts



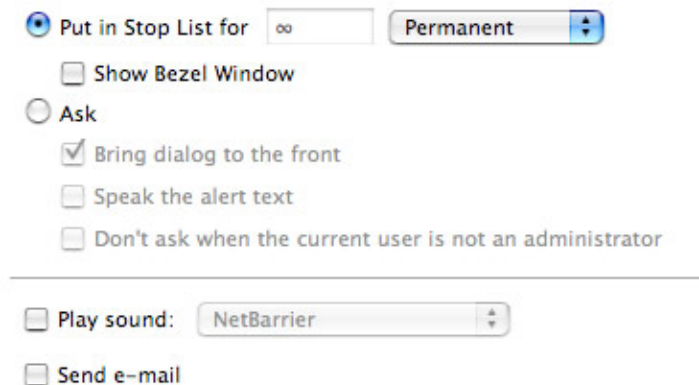
NetBarrier X5 constantly monitors your computer's network activity to both the Internet and local networks, and will look out for specific types of data that indicate an intrusion or attack. If any suspicious data is found, NetBarrier X5 displays an alert, asking you whether you wish to allow the data to be sent or deny it.

## Alert Settings

Alerts appear in reaction to settings in the following areas:

- Trojans
- Data
- Surf
- Policy
- Anti-Spyware

Settings for these alerts appear in several places throughout NetBarrier X5, as is described in relevant sections of this manual. To understand these settings better, we'll look at them as they appear in the Policy section.

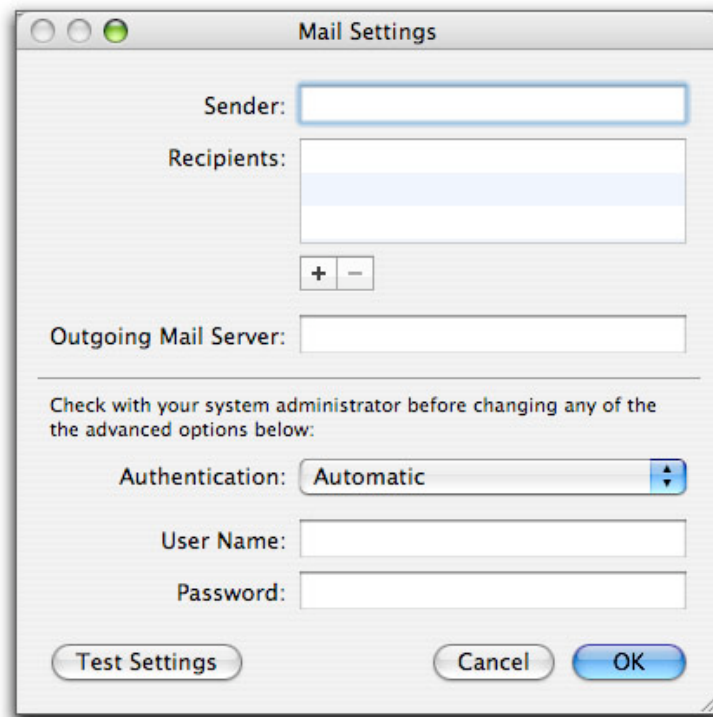


The screenshot shows a settings window for alerts. At the top, there is a radio button selected for "Put in Stop List for" with a text field containing "∞" and a dropdown menu set to "Permanent". Below this is a checkbox for "Show Bezel Window". Underneath is a radio button for "Ask", which is currently selected. Below the "Ask" radio button are three checkboxes: "Bring dialog to the front" (checked), "Speak the alert text", and "Don't ask when the current user is not an administrator". A horizontal line separates this section from the bottom section, which contains a checkbox for "Play sound:" with a dropdown menu set to "NetBarrier", and a checkbox for "Send e-mail".

<b>Put in Stop List</b>	<p>If this radio button is on, the connection is automatically dropped when there is an alert, and the offending IP address is immediately placed in the Stop List (See <b>The Stop List and Trusted Group.</b>) 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 put the intruder in the Stop List permanently.</p>
<b>Ask</b>	<p>If this radio button is on, NetBarrier X5 presents an Alert dialog asking what to do. When an alert appears, it shows the Stop List time period selected by default, but this time can be changed in Policy tab for each type of attack. In addition, you have three options:</p> <ul style="list-style-type: none"> <li>• <b>Bring dialog to the front:</b> The alert comes to the front automatically whenever there is an alert. If not, it remains in the background. If you take no action within 90 seconds, the alert automatically closes, and the connection is denied.</li> <li>• <b>Speak the Alert Text:</b> NetBarrier X5 uses Mac OS X's Text-to-Speech feature to speak the text of the alert.</li> <li>• <b>Don't ask when the current user is not an administrator:</b> NetBarrier X5 only gives the above options if the Mac OS X user has administrator's privileges. Otherwise, it automatically puts the offending host in the Stop List.</li> </ul>
<b>Play sound</b>	<p>NetBarrier X5 plays the sound of your choice whenever there is an alert. You can select the sound you want from the pop-up menu to the right of the button.</p>
<b>Send e-mail</b>	<p>NetBarrier X5 automatically sends an e-mail message to the address configured in the Options panel (see above), within 30 seconds. (NetBarrier X5 waits to see if there are other intrusion attempts, rather than sending an e-mail message each time.)</p>



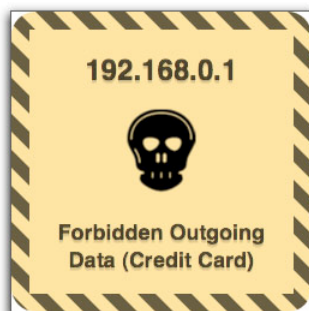
If you've requested e-mail notification, you must configure your e-mail settings to receive any alert notifications by e-mail. In the Policy section, you do that by clicking Options, then clicking the Configure... button.

A screenshot of a 'Mail Settings' dialog box. The dialog has a title bar with three window control buttons (red, yellow, green) on the left. The main area contains several fields: 'Sender:' with a text input field; 'Recipients:' with a list box containing one empty row and a '+' button below it; 'Outgoing Mail Server:' with a text input field. Below these is a section header 'Check with your system administrator before changing any of the the advanced options below:'. This section contains 'Authentication:' with a dropdown menu showing 'Automatic'; 'User Name:' with a text input field; and 'Password:' with a text input field. At the bottom are three buttons: 'Test Settings', 'Cancel', and 'OK'.

You must enter e-mail addresses for the Sender and Recipient(s), as well as the Outgoing Mail Server. Further, you'll need to enter a username and password that your mail server will accept. E-mail messages can be sent to multiple recipients. To add a recipient, click the + button. To remove a recipient, click the – button.

## Examples of Alerts

The following is an example of an alert when the Put in Stop List radio button is on and the Show Bezel Window checkbox is enabled.



As you can see, you're given no options, only a notification. If the Show Bezel Window checkbox had been disabled, you'd have seen nothing, and NetBarrier X5 would have silently added the IP address to the Stop List.

Here's an example of an alert when the Ask radio button is on, and the "Bring dialog to the front" checkbox is enabled.

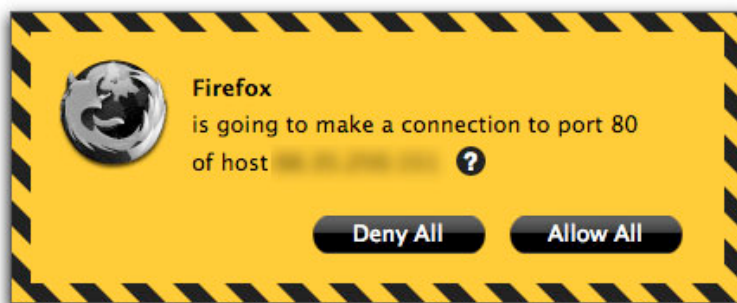


The top line shows the reason for the alert. The host (shown here blurred) is given as an IP address, but you could find out its associated domain name (if any) by clicking the “?” icon. We’ve already clicked the disclosure triangle to show More Info, which gives further details and instructions.

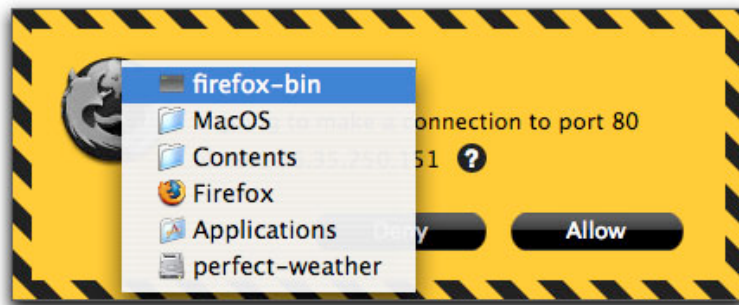
Two buttons on the lower right allow you to decide what action to take for this alert.

<b>Stop List</b>	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. In addition, the IP address that caused this alert will be automatically added to the Stop List, and kept there for the default time that has been set. You can make changes this time in the pop-up menu.
<b>Ignore</b>	If you click this button, you will allow the data to be sent. Data transmission will continue as usual, unless NetBarrier X5 detects another attempted intrusion, in which case another alert will appear.

Finally, here’s an example of an alert that occurred when an application attempted to reach the Internet in violation of Anti-Spyware rules.



Anti-Spyware alerts have a special feature that lets you see where in the Finder the offending program is. Click on the name of the program (“Firefox”, in this example) and you’ll be able to see and navigate the path to it.



## Attack Counter

NetBarrier X5 records the number of attacks it has protected you from and displays this number in a counter at the top of the Policy section of the Antivandal tab. It also shows the type of attack it blocked last, and the date and time of the last attack. First, the number of attacks displays:

Number of detected attacks: 124

Since: First NetBarrier launch

After a few seconds, NetBarrier X5 shows information about the most-recent attack:

Last Detected Attack: Ping Flooding

at: 8/24/07, 1:22 AM

To reset this counter, click the Reset button next to the counter.

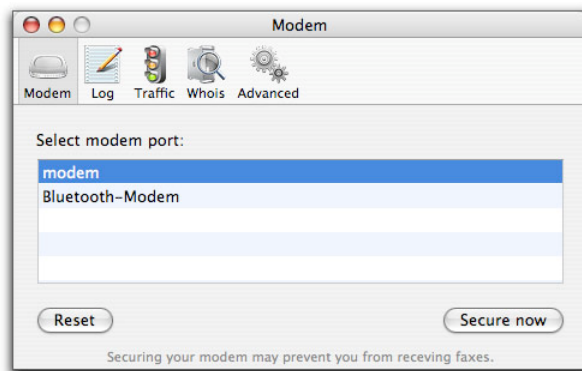




# 10—Preferences and Configurations



Preferences for several of NetBarrier X5's functions are available from the NetBarrier Preferences screen. To view this screen, choose NetBarrier X5 > Preferences..., or press Command-comma. A window appears with the Modem icon selected, the first of five.

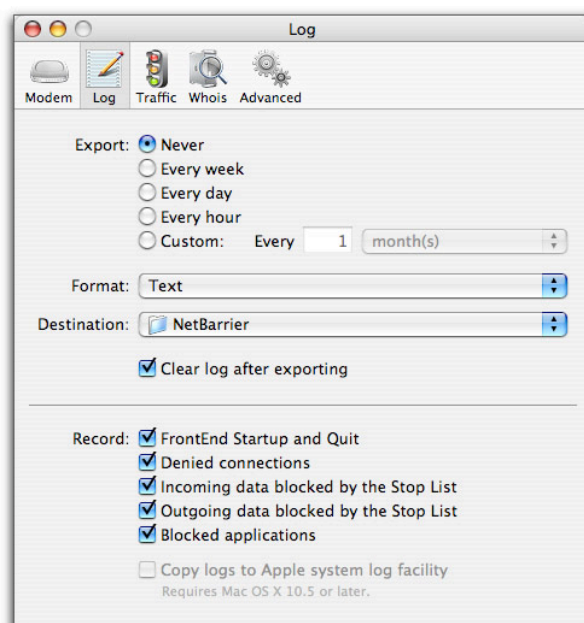


## Modem Preferences

You can provide total security for your modem with this option. To do this, click the Modem button on the Preferences screen. Securing your modem may prevent it from answering any calls. By clicking the Secure now button, you're telling NetBarrier X5 not to accept any incoming calls: however, you'll still be able to make outgoing calls. To return your modem to its normal, unsecured state, click the Reset button.

## Log Preferences

You can set NetBarrier X5 to export its log at regular intervals. To do this, click the Log button on the Preferences screen.



Your first choice is how often you'd like the log export to occur. If the "Every week" radio button is on, exports occur every midnight between Sunday and Monday; for "Every day", they occur at midnight; for "Every hour", they occur at the top of the hour. The Customized selection allows you to name a multiple of these times, for example once every two weeks. (The Customized selection also allows you to do the export once a month, at midnight on the first day.)

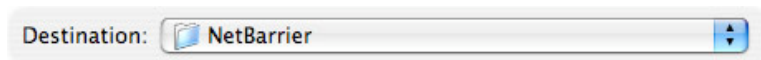
If the computer is off when an export is scheduled, it will occur when it is next turned on.

Logs can be exported in any of six formats. Click the Format popup menu to select the export format.



For a description of Log export formats, see **Exporting the Log**.

You can select the folder where log export files are saved. By default, they are saved in the /Library/Logs/NetBarrier folder. If you wish to have these files saved in another folder, select Other... from the popup menu and navigate until you get to the folder you wish to use. Then click Select to use this folder.



NetBarrier X5 uses two logs. There is a rotating log, which contains a maximum of 4096 entries, which you see in NetBarrier X5's Log panel. If automatic exports are enabled, a second log stores all entries. If you wish to retain full logs of all activity, you should therefore activate periodic exports. These logs are not limited by size (other than the available space on your hard disk). If you check "Clear log after exporting", this will delete the log entries after each export so each new export contains only those entries recorded after the previous export. This setting only affects automated exports, and doesn't affect log exports done manually from the Log window.

You have a choice of which elements are recorded in your logs, as indicated by the checkboxes at the bottom of the Log preferences pane. The options are:

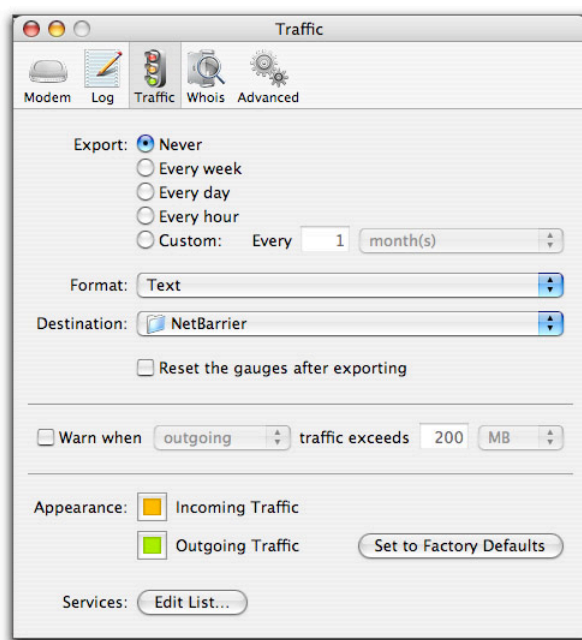
<b>FrontEnd Startup and Quit</b>	General NetBarrier X5 activity, such as when NetBarrier X5 launches.
<b>Denied connections</b>	Attempts to reach your Mac that were blocked because they violated rules you set up in NetBarrier X5.
<b>Incoming data blocked by the Stop List</b>	Attempts to send data to your Mac from hosts that are in the Stop List.
<b>Outgoing data blocked by the Stop List</b>	Attempts to send data from your Mac to hosts that are in the Stop List.
<b>Blocked applications</b>	Instances where NetBarrier X5's Anti-Spyware prevented an application from communicating with the network.

The last checkbox is "Copy logs to Apple system log facility". When checked, the Log data will be registered in the unified log system found in Mac OS X 10.5 and later.



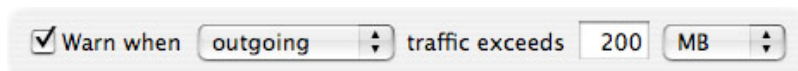
## Traffic Preferences

Like the Log preferences, the Traffic preferences screen gives you options to export traffic data at regular intervals. This screen also gives you several options for managing traffic data. To change these settings, click the Traffic button on the Preferences screen.



In the top section of this screen you control automated, periodic exports of traffic data. It works exactly the same as the log preferences: see above for details. The one setting that's different is the checkbox, “Reset the gauges after exporting”, which in essence is the same as the log's “Clear log after exporting” checkbox. Checking it is the equivalent of clicking the Reset button next to the gauges to change total traffic to zero after automated exports. For more information about Traffic gauges, see **Traffic**.

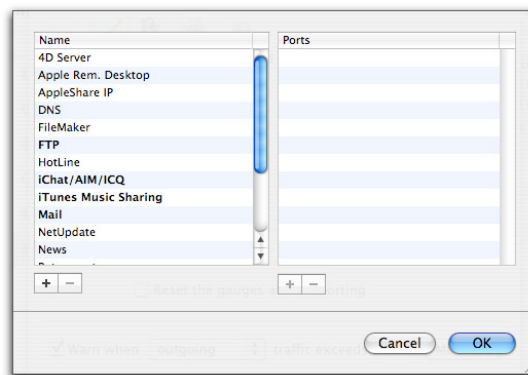
NetBarrier X5's Traffic preferences include a setting that allows you to monitor the amount of data entering or leaving your computer. This can be very useful if you have an Internet access account with uploading or downloading restrictions.



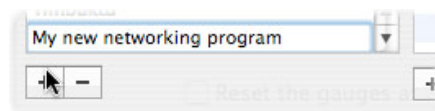
If you check this option, NetBarrier X5 displays a warning when your traffic exceeds the amount you have selected. You can choose to have a warning for Incoming, Outgoing or Global (total) traffic, and you can choose the amount of the threshold in kilobytes, megabytes or gigabytes.

Below that is an Appearance section where you can change the color of incoming and outgoing traffic in all Traffic gauges and timelines. Clicking either colored box brings up a standard Mac OS X color picker: select your preferred color, then close the window by clicking the red Close button in the upper-left corner. The Set to Factory Defaults button returns the colors to orange for incoming traffic and green for outgoing traffic.

Finally, the Services button at the bottom lets you add, remove and change the kinds of traffic displayed in the Traffic gauges, which is very helpful if you're testing a new networking program. Clicking the Edit List... button opens a window that lists existing services



To add a service, click the + button in the lower-left corner, then enter the name of the service.

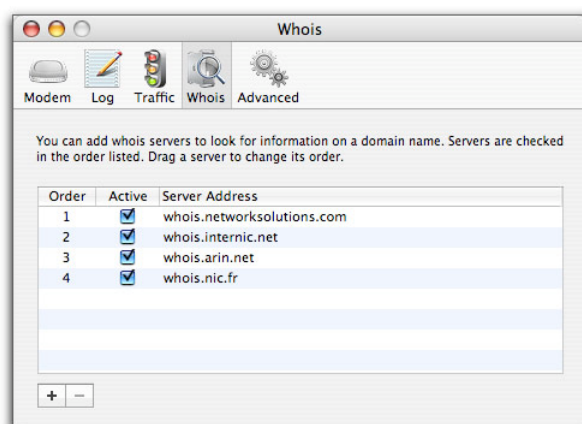


With that service highlighted, you then click the other + button, below the right column, to add ports that are associated with that program.

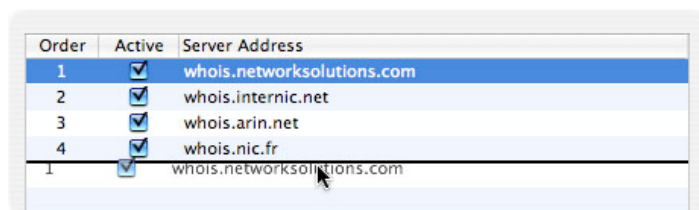
Similarly, you can edit or delete any services in the list that aren't listed in bold. Bold services such as Chat, Mail and Web are core to networking, and are therefore locked in place as a safety measure.

## Whois Preferences

NetBarrier X5'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.



Adding new Whois servers to NetBarrier X5 is easy: just click the + button and type in the name of the Whois server you wish to add.

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

To remove a Whois server, select it by clicking it, and click the – button. A dialog box asks you for confirmation.

## Advanced Preferences

Three options are available in the Advanced panel of NetBarrier X5 Preferences.

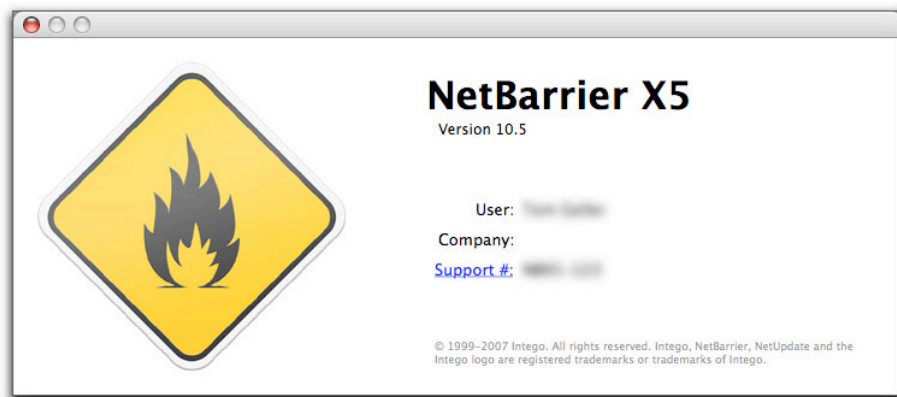


<b>Configuration</b>	Clicking the Revert to Default... button allows you to reset NetBarrier X5 to its default configuration: “Client, local server” mode for the Firewall, with Antivandal and Privacy functions disabled. You will need an administrator’s password to activate this configuration. Doing so also clears all Firewall Modes and other settings you created, along with your Stop List and Trusted Group. It is recommended to export your current NetBarrier X5 settings (File > Export settings...) before reverting to Default settings in case you want to recover your settings at a later date.
<b>Protection</b>	Clicking the Disable NetBarrier... button will completely turn off NetBarrier X5, including the Log feature. You will need an administrator’s password to do this. Once NetBarrier X5 is disabled, the button changes to Enable NetBarrier... Click it and enter an administrator’s password to Enable NetBarrier once again. Regardless of the setting, NetBarrier X5 will automatically be re-enabled when you restart your Mac.
<b>Setup Assistant</b>	Clicking the Show Assistant... button will launch NetBarrier X5’s Setup Assistant. See chapter 4, <b>Quick Start</b> for more information.



## About NetBarrier X5

If you choose About NetBarrier X5... from the NetBarrier menu, a window displays showing information about NetBarrier X5 such as the version number and your support number (which you'll need for technical support).



Clicking the Support # link launches your e-mail program with a message addressed to Intego Technical Support, with information in the Subject line that will help Intego's support staff respond to your problem.



## Configurations

NetBarrier X5 lets you save multiple configuration sets. Each configuration set contains all the settings and preferences you have applied to NetBarrier X5. You can make sets for different locations, for example—one set when you’re using your laptop at the office, and another for home use. You may want to have one set that includes additional protection for the times your Mac works 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.

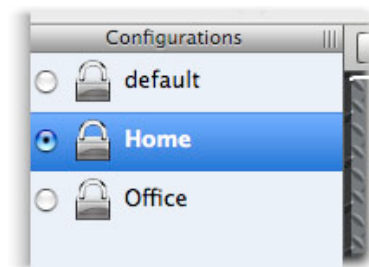
Configurations appear in a list on the left of the Overview screen. (For more about the Overview screen, see chapter 4, **Quick Start**.) Four buttons below the list let you duplicate, edit, remove and hide configurations. If you don’t see the Configuration list, it might be hidden: display it by pressing Command-K, choosing View > Hide/Show Configurations List, or clicking the rightmost button of the four.



### Creating, Editing and Deleting Configurations

The first time you use NetBarrier X5 you’ll see one Configuration in the list, named “default”. To create a new Configuration, you duplicate an existing set by highlighting it and clicking the leftmost button, which looks like two windows. Or, you can press the Control key and click on the existing Configuration, then choose Duplicate from the contextual menu. Then rename the new Configuration by double-clicking on it and typing a new name.

Now that you have a new configuration, activate it by clicking its radio button. Here, we’ve created two new configurations by duplicating “default” twice, renamed them, and selected the one named Home.

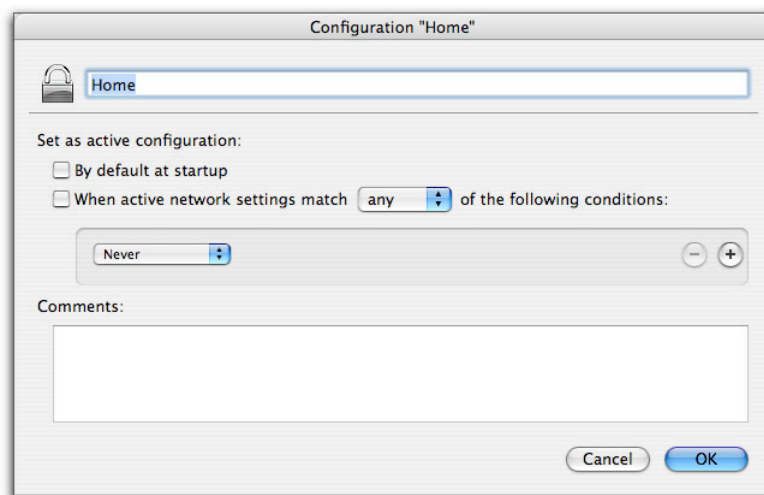


You can now make any changes to the NetBarrier X5 configuration that you want, and they are saved under the current set. To make another set active, simply click its radio button. You can also select another configuration set from the Configurations list in the Intego Menu.

Once you've created a configuration, there are three ways to edit it. First, click on the configuration, then either:

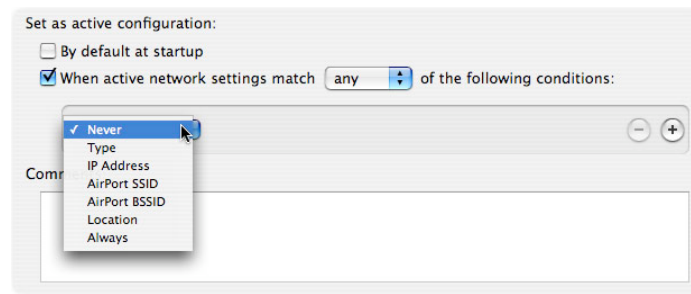
- Click the pencil icon at the bottom of the Configurations list,
- Press the Control key while clicking on the configuration, then select Edit... from the contextual menu, or
- Choose File > Edit Configuration....

You'll see a window like this:



This Configuration will become active when you turn on or restart your Mac if you check the “By default at startup” checkbox.

In addition, by checking the “When active network settings match...” checkbox it will automatically become active when any or all conditions you specify regarding the following networking criteria are true.



<b>Never</b>	This condition will never be true, so the configuration will never turn on automatically.
<b>Type</b>	Choices are Ethernet, AirPort, FireWire, PPP or Bluetooth.
<b>IP Address</b>	You can choose a specific IP address, or a range. A Current button identifies the IP address your Mac has at the moment.
<b>AirPort SSID</b>	The common name for a wireless network, such as “My AirPort”. You can choose for this condition to be true when the SSID is, is not, or contains a text string you specify.
<b>AirPort BSSID</b>	The MAC address of a wireless network connection point, expressed as a string of hexadecimal numbers.
<b>Location</b>	The Location defined in your Mac’s Network preferences.
<b>Always</b>	The condition is always true.

The Comments field is a place for any freeform description or notes you’d care to add: they don’t affect operation of the configuration in any way.

There are two ways to delete a configuration: by clicking on the – button below the configuration list, or by pressing Control while clicking the configuration and choosing Remove... from the contextual menu. In either case, a dialog box then asks you to confirm the deletion. You can’t remove the active configuration: instead, you must switch to another before removing it.



## Exporting and Importing Settings

You can save all your NetBarrier X5 settings in a special file that you can then use to import these settings into another copy of NetBarrier X5. This is especially useful if you manage many computers and want to use the same settings for all of them.

To export your settings, select File > Export Settings... A dialog box asks you to name the settings file and choose a location to save it. Click Export when you have finished. The result is an XML file that can be imported into any copy of NetBarrier X5, including the one that created it.

To import settings, select File > Import Settings... A file dialog asks you to locate the settings file. Once you have located the file, click Import and these settings are immediately applied to NetBarrier X5. You can also double-click a NetBarrier X5 settings file to import it.



## Locking and Unlocking the Interface

NetBarrier X5's controls are effective because of their extreme power and flexibility: it will notice any sort of network activity it encounters, and react in a wide variety of ways according to your preferences. However, this power is a double-edged sword, as it could cause tremendous difficulty if the wrong people gain access. Therefore, NetBarrier X5 gives you a way to lock the program's interface so that even those who have physical access to your Mac won't be able to overcome its protections.

To lock NetBarrier X5, either press Command-L, or choose File > Lock Interface. Its basic settings will still be visible, but the details will be untouchable, and nobody will be able to change them without unlocking the interface.

To unlock NetBarrier X5, press Command-L or choose File > Unlock Interface, then enter your administrator's password to complete the process.



# 11—Technical Support



Technical support is available for registered purchasers of Intego NetBarrier X5.

### **By e-mail**

support@intego.com: North and South America

eurosupport@intego.com: Europe, Middle East, Africa

supportfr@intego.com: France

supportjp@intego.com: Japan

### **From the Intego web site**

[www.intego.com](http://www.intego.com)





## Acknowledgements

Portions of this Intego Software may utilize the following copyrighted material, the use of which is hereby acknowledged.

EDCommon and EDInternet frameworks written by Erik Dörnenburg.

Omni Development (OAGradientTableView)

Copyright 2003-2004 Omni Development, Inc. All rights reserved.



# 12—Glossary



<b>Address mask</b>	A bit mask used to identify which bits in an IP address correspond to the network address and subnet portions of the address.
<b>Address mask reply</b>	A reply sent to an address mask request.
<b>Address mask request</b>	A command that requests an address mask.
<b>ASIP</b>	AppleShare IP; a protocol specific to Apple networking.
<b>Bootp</b>	The Bootstrap Protocol. A protocol used for booting diskless workstations.
<b>Bootp client</b>	A computer operating as a Bootp client.
<b>Bootp server</b>	A computer operating as a Bootp server.
<b>Broadcast packet</b>	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.
<b>Chat</b>	A system that allows two or more logged-in users to set up a typed, real-time, on-line conversation across a network.
<b>Client</b>	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.
<b>Connected service</b>	Service that requires a connection open and maintained between two computers, such as HTTP, FTP, TELNET, SSH, POP3, AppleShare, etc. This covers all TCP connections.
<b>Connection flood</b>	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.
<b>Cookie</b>	A file on your hard disk that 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.
<b>Datagram</b>	A self-contained package of data that carries enough information to be routed from source to destination independently of any previous and subsequent exchanges.
<b>DNS</b>	Domain Name System. Used by routers on the Internet to translate addresses from their named forms, such as <a href="http://www.intego.com">www.intego.com</a> , to their IP numbers.
<b>Echo</b>	The request sent during a ping.
<b>Echo reply</b>	The reply sent to an echo request.
<b>Finger</b>	A program that displays information about a particular user on the Internet, or on a network.
<b>FTP</b>	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.
<b>Gopher</b>	A distributed document retrieval system, which was a precursor to the World Wide Web.
<b>Host</b>	A computer connected to a network.
<b>HTTP</b>	HyperText Transfer Protocol, the protocol used to send and receive information across the World Wide Web.
<b>ICMP</b>	Internet Control Message Protocol. This protocol handles error and control messages sent between computers during the transfer process.
<b>IGMP</b>	Internet Group Management Protocol.
<b>IMAP</b>	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.
<b>Intranet routing</b>	The process, performed by a router, of selecting the correct interface and next hop for a packet being forwarded on an Intranet.
<b>IP</b>	The network layer for the TCP/IP protocol suite widely used on Ethernet



	networks and on the Internet.
<b>IP address</b>	An address for a computer using the Internet Protocol.
<b>IRC</b>	Internet Relay Chat. A medium for worldwide “party line” networks that allowing one to converse with others in real time.
<b>Local network</b>	A network of computers linked together in a local area. This may be a single building, site or campus.
<b>NETBIOS</b>	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.
<b>Network</b>	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.
<b>NNTP</b>	Network News Transfer Protocol. A protocol for the distribution, inquiry, retrieval and posting of Usenet news articles over the Internet.
<b>NTP</b>	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.
<b>Packet</b>	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.
<b>Ping</b>	A program used to test reachability of computers on a network by sending them an echo request and waiting for a reply.
<b>Ping broadcast</b>	An attack similar to a ping flood. See below.
<b>Ping flood</b>	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.
<b>Ping of death</b>	An especially dangerous ping attack that can cause your computer to crash.
<b>POP3</b>	Post Office Protocol, version 3. POP3 allows a client computer to retrieve



	electronic mail from a POP3 server.
<b>Port scan</b>	A procedure where an intruder scans the ports of a remote computer to find which services are available for access.
<b>Protocol</b>	The set of rules that govern exchanges between computers over a network. There are many protocols, such as IP, HTTP, FTP, NNTP, etc.
<b>Router</b>	A device that forwards packets between networks, reading the addressing information included in the packets.
<b>Server</b>	A computer connected to a network that is serving, or providing data or files to other computers called clients.
<b>Service</b>	A network function available on a server, i.e. http, ftp, e-mail etc.
<b>SMTP</b>	Simple Mail Transfer Protocol A protocol used to transfer electronic mail between computers.
<b>Spam</b>	Unwanted e-mail messages, usually sent to thousands, even millions of people at a time, with a goal of selling products or services.
<b>Spyware</b>	Software that secretly collects information from your computer and sends it to a remote recipient.
<b>TCP</b>	Transmission Control Protocol. The most common data transfer protocol used on Ethernet and the Internet
<b>TCP/IP</b>	The Internet version of TCP -TCP over IP.
<b>Telnet</b>	The standard Internet protocol used for logging into remote computers.
<b>TFTP</b>	Trivial File Transfer Protocol. A simple file transfer protocol used for downloading boot code to diskless workstations.
<b>Traceroute</b>	A utility used to determine the route packets are taking to a particular host.
<b>Trojan horse</b>	A malicious program that hides inside an innocent-seeming one.
<b>UDP</b>	User Datagram Protocol. An Internet protocol that provides simple but unreliable datagram services.
<b>Whois</b>	An Internet directory service for looking up information on domain names and IP addresses.



