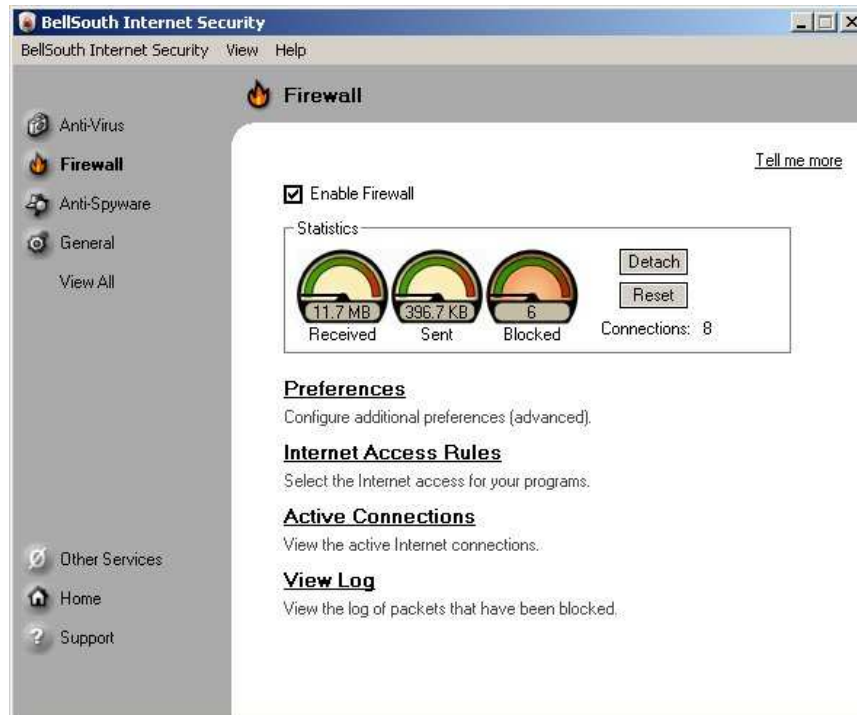


# BellSouth® Firewall

## 1 Introduction

BellSouth® Firewall monitors all traffic to and from a computer to block unauthorized access and protect personal information. It provides users with control over all outgoing connections being made from their computer as well as all incoming attempts to connect to their computer over the Internet

## 2 BellSouth® Firewall Home Page

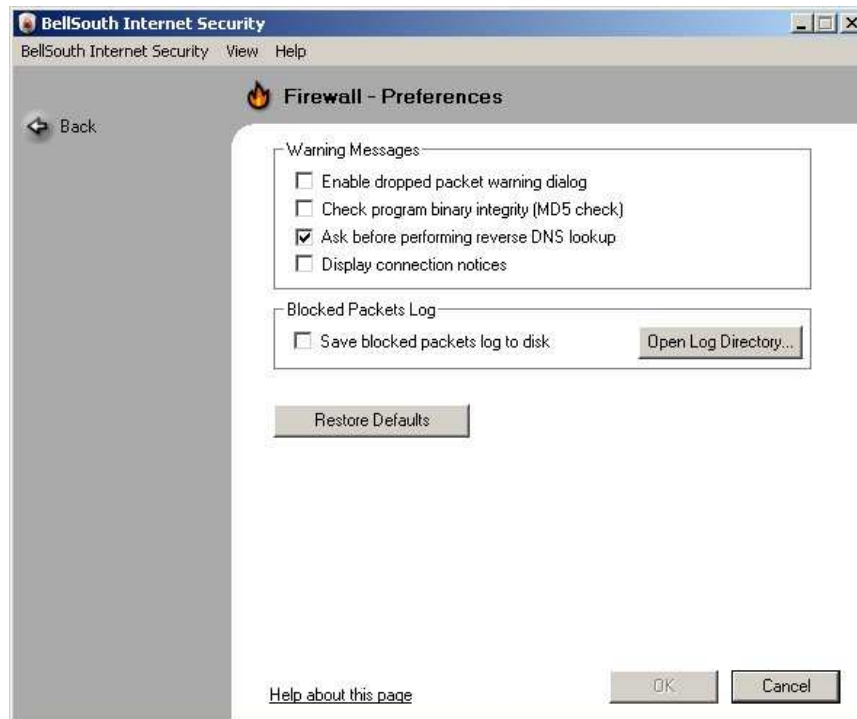


### 2.1 Statistics

The Statistics section holds information regarding the volume of packets that are sent out, and received as well as the number of packets blocked by the BellSouth® Firewall. Additionally, the user can see the number of connections that have been established. Connections counts the number of open Internet pipes thus will not directly correspond to the number of programs listed in the Active Connections section. Lastly, the reset button allows users to clear the statistics data.

### 3. Preferences

For advanced users, five additional Preferences are available.



#### 3.1 Warning Messages

There are four warning messages that can be displayed when the firewall is active. Users may choose which warning message(s) they would like displayed.

##### 3.1.2 Dropped Packet Warning



A Dropped Packet Warning will appear if an Internet communication was blocked either to or from your computer. The warning will contain information about the source and the destination of the blocked packet.

### 3.1.3 Binary Integrity Check



The Check program binary integrity (MD5 check) option is a tool that validates programs with networking activity for changes that may have occurred with or without your knowledge. An example of this type of program is Internet Explorer and Microsoft Outlook.

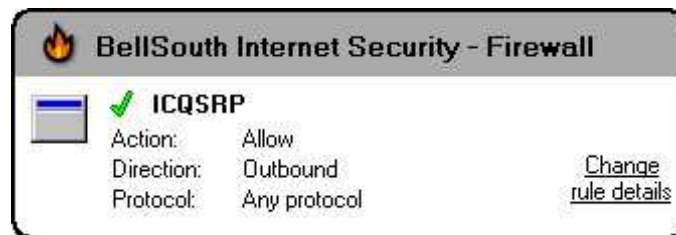
BellSouth® Firewall reads the program on your computer and creates an identification that is very difficult to duplicate. If a program has not changed, the same identification should be generated each time. Thus if a program is going to connect and the identification generated differs in comparison with an older I.D, it would imply that the file has been changed.

### 3.1.4 Reverse DNS Look up



The Ask before performing reverse DNS lookup option provides the user with the name of the source or destination host instead of just an IP address. When this feature is enabled, you have the option to select the name of the source or destination host to display. This option appears during a blocked packet alert. The source and destination hosts appear as hyperlinks. When the hyperlink is selected, a prompt appears warning the user that they may be risking their privacy. When performing a reverse lookup, your IP address can be viewed by external sources. If the user chooses to 'Continue', the name of the source and destination hosts replaces the IP address.

### 3.1.5 Connection Notices



The Display Connection notices provide the user with the current Internet Access Rule information for a program trying to perform a connection.

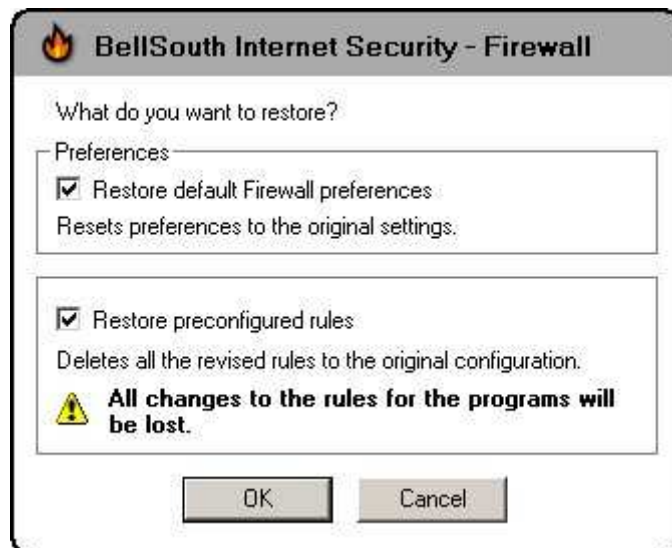
### 3.2 Blocked Packets Log

Users have the option to save the dropped packets warnings in a log to view as a report. This may be a preferred alternative to enabling the Dropped Packet warning message and having messages pop up.

This Log as well as all other logs generated by BellSouth® Firewall and stored on the users computer maybe accessed using the Open Log Directory button.

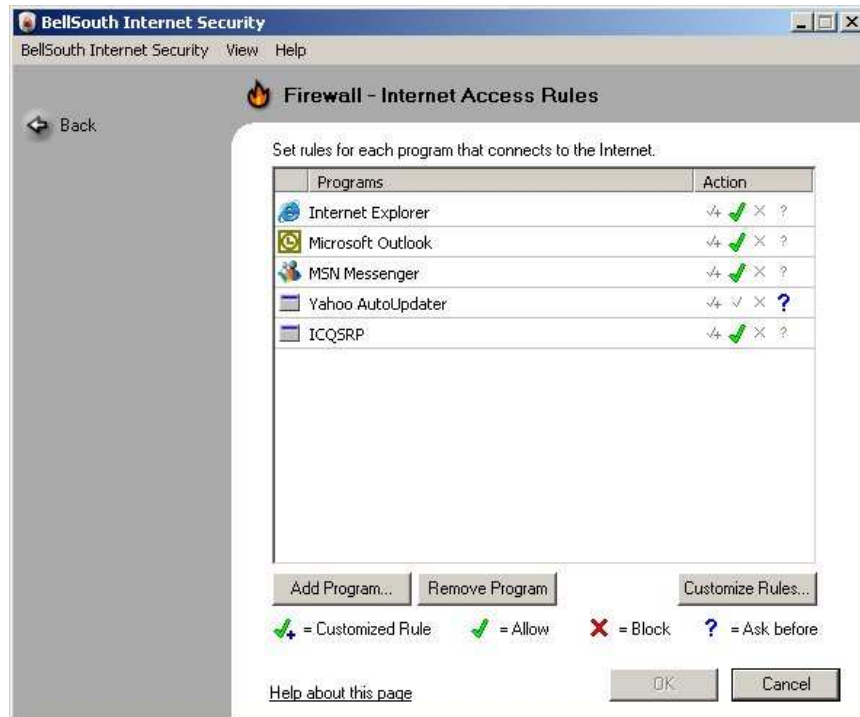
### 3.3 Restore Defaults

Users may revert to the default BellSouth® Firewall settings through the Restore Defaults option. Default settings can be restored for the BellSouth® Firewall Preferences, the Internet Access Rules or both by checking the desired boxes.



#### 4. Internet Access Rules

Internet access rules provide a set of criteria on how programs perform a network activity. The BellSouth® Firewall works interactively with the user to create a set of rules for programs that connect to the Internet.



The first time a program requests permission to send or receive a communication a pop-up appears requesting permission to perform this activity. The user may then choose to Allow or Block this connection.



Checking the 'Remember for this program' box and choosing to 'Allow' will result in a green check mark in the Internet Access Rules. Choosing the remember option and Block will enter a red cross. Every subsequent attempt will then be handled according to this rule specified by the user. Alternatively, by not checking the remember option, a blue question mark will be entered in the Internet Access Rules and the user will be prompted each time the program tries to establish a connection. These rules can be modified for each program at any time. The 'Show Details' link will expand the dialog box to show the full program path and IP address the program is attempting to contact.

#### 4.1 Add Program

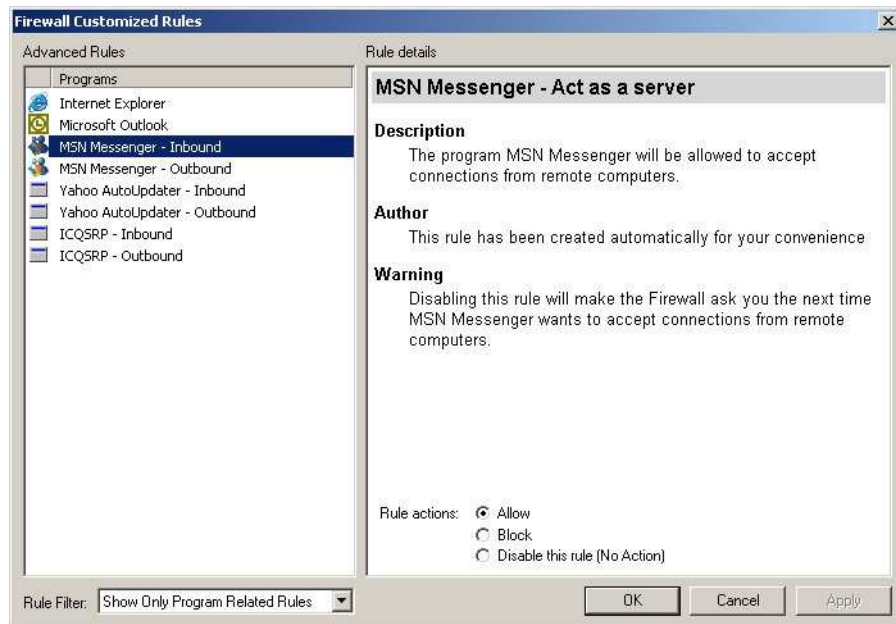
The Add Program button allows users to add a program to the Internet Access Rules list. Clicking on it will display a windows dialogue box from which one can navigate and find the program that they wish to add. Once added, the default rule will be set to 'Allow'

#### 4.2 Remove Program

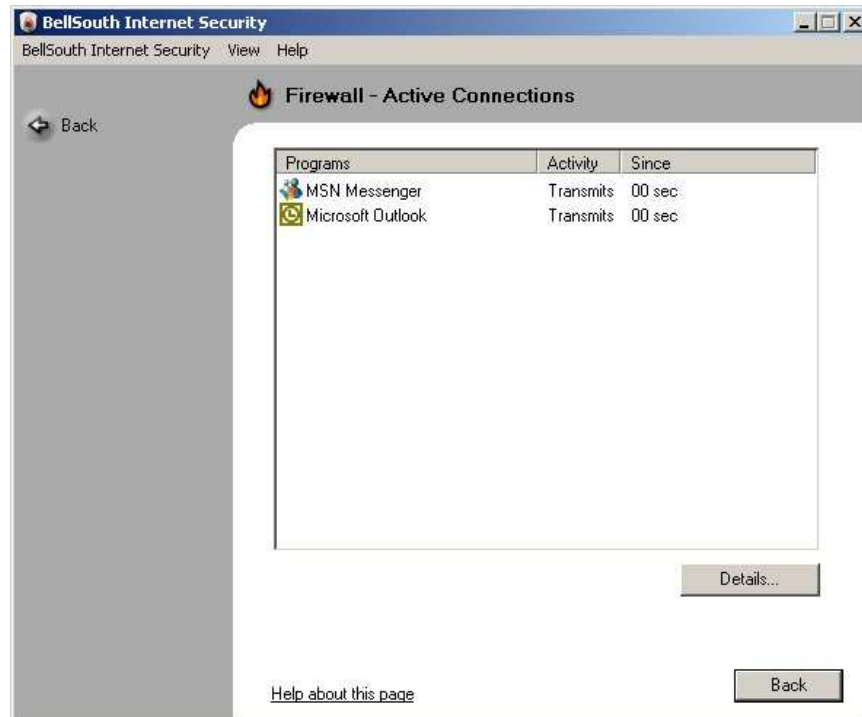
Choosing a program in Internet Access Rules and pressing the Remove Program button will delete program from the list and its corresponding rule. The next time this program tries to establish a connection a pop up will appear requesting permission.

#### 4.3 Customize Rules

Customized rules will allow users to configure each rule for inbound and outbound connections. It will also allow users to configure the firewall to block some of the default allowed system applications. This is only recommended for advanced users.



## 5 Active Connections



The Active Connections displays a real-time list of programs that currently have connections open with the Internet. The list includes the program name, its respective icon, and the time elapsed since the initial connection. The connection is tracked for the duration the program is connected to the Internet and the most recent program to connect appears at the bottom of the list.

### 5.1 Details

Advanced users can click on Details to obtain additional connectivity information for a particular program. Specific information regarding protocols, the ports and IP addresses used by the local and remote computer are included on the detailed report.

Program	Protocol	Local IP	Port	Remote IP	Port	State
System	TCP	0.0.0.0	1183	127.0.0.1	445	Connected
C:\Program Files\MSN Messenger\msnmsgr.exe	TCP	0.0.0.0	1173	67.30.136.62	80	Connected
C:\Program Files\MSN Messenger\msnmsgr.exe	TCP	0.0.0.0	1170	65.54.194.118	80	Connected
C:\Program Files\MSN Messenger\msnmsgr.exe	TCP	0.0.0.0	1165	67.30.136.62	80	Connected
C:\Program Files\MSN Messenger\msnmsgr.exe	TCP	0.0.0.0	1163	67.30.136.62	80	Connected
C:\Program Files\MSN Messenger\msnmsgr.exe	TCP	0.0.0.0	1149	69.44.123.183	80	Connected
C:\Program Files\MSN Messenger\msnmsgr.exe	UDP	192.168.0.101	41029	0.0.0.0	0	
C:\Program Files\MSN Messenger\msnmsgr.exe	UDP	0.0.0.0	1144	0.0.0.0	0	
C:\Program Files\MSN Messenger\msnmsgr.exe	UDP	192.168.0.101	9	0.0.0.0	0	
C:\Program Files\MSN Messenger\msnmsgr.exe	TCP	0.0.0.0	1140	207.46.110.100	80	Connected
C:\Program Files\MSN Messenger\msnmsgr.exe	UDP	127.0.0.1	1136	0.0.0.0	0	
C:\Program Files\MSN Messenger\msnmsgr.exe	TCP	0.0.0.0	1135	207.46.107.158	1863	Connected
C:\Program Files\BellSouth\BellSouth Internet Security\Freedom.exe	TCP	0.0.0.0	1062	207.107.241.1...	443	Connected
C:\Program Files\BellSouth\BellSouth Internet Security\Freedom.exe	UDP	127.0.0.1	1041	0.0.0.0	0	
C:\WINNT\system32\svchost.exe	TCP	0.0.0.0	135	0.0.0.0	0	Listening
C:\Program Files\BellSouth\BellSouth Internet Security\Freedom.exe	TCP	127.0.0.1	51206	0.0.0.0	0	Listening
C:\Program Files\BellSouth\BellSouth Internet Security\Freedom.exe	TCP	127.0.0.1	51203	0.0.0.0	0	Listening
C:\Program Files\BellSouth\BellSouth Internet Security\Freedom.exe	TCP	127.0.0.1	51204	0.0.0.0	0	Listening
C:\Program Files\BellSouth\BellSouth Internet Security\Freedom.exe	TCP	127.0.0.1	51114	0.0.0.0	0	Listening

## 6. View Log

When the BellSouth® Firewall blocks an incoming or outgoing connection, the information of the blocked connection is logged to a text file on the hard drive.

The following packets were blocked:

Protocol	Direction	Source IP	S. Port	Destination IP	D. Port
tcp	Outgoing	192.168.0.101	1063	207.107.241.36	80
tcp	Outgoing	192.168.0.101	1063	207.107.241.36	80
tcp	Outgoing	192.168.0.101	1063	207.107.241.36	80
tcp	Outgoing	192.168.0.101	1063	207.107.241.36	80
tcp	Incoming	207.107.241.97	80	192.168.0.101	1114
tcp	Outgoing	192.168.0.101	1063	207.107.241.36	80
icmp	Outgoing	192.168.0.101	0	205.152.132.235	0

Details:

Protocol:	tcp	Packet:	
Source IP:	207.107.241.97	Dest. IP:	192.168.0.101
Source Port:	80 [World Wide Web]	Dest. Port:	1114 [Mini SQL]
Trojan:		Date:	1/12/2005 8:53:50 PM

Clear Log View Log as Web Page

[Help about this page](#) Back

The Blocked Packets Log will display the type of protocol used, the source IP and the destination IP. These will help the user track down the source of the blocked packets. Please note that the majority of blocked packets are harmless, as they are not purposefully directed to user.